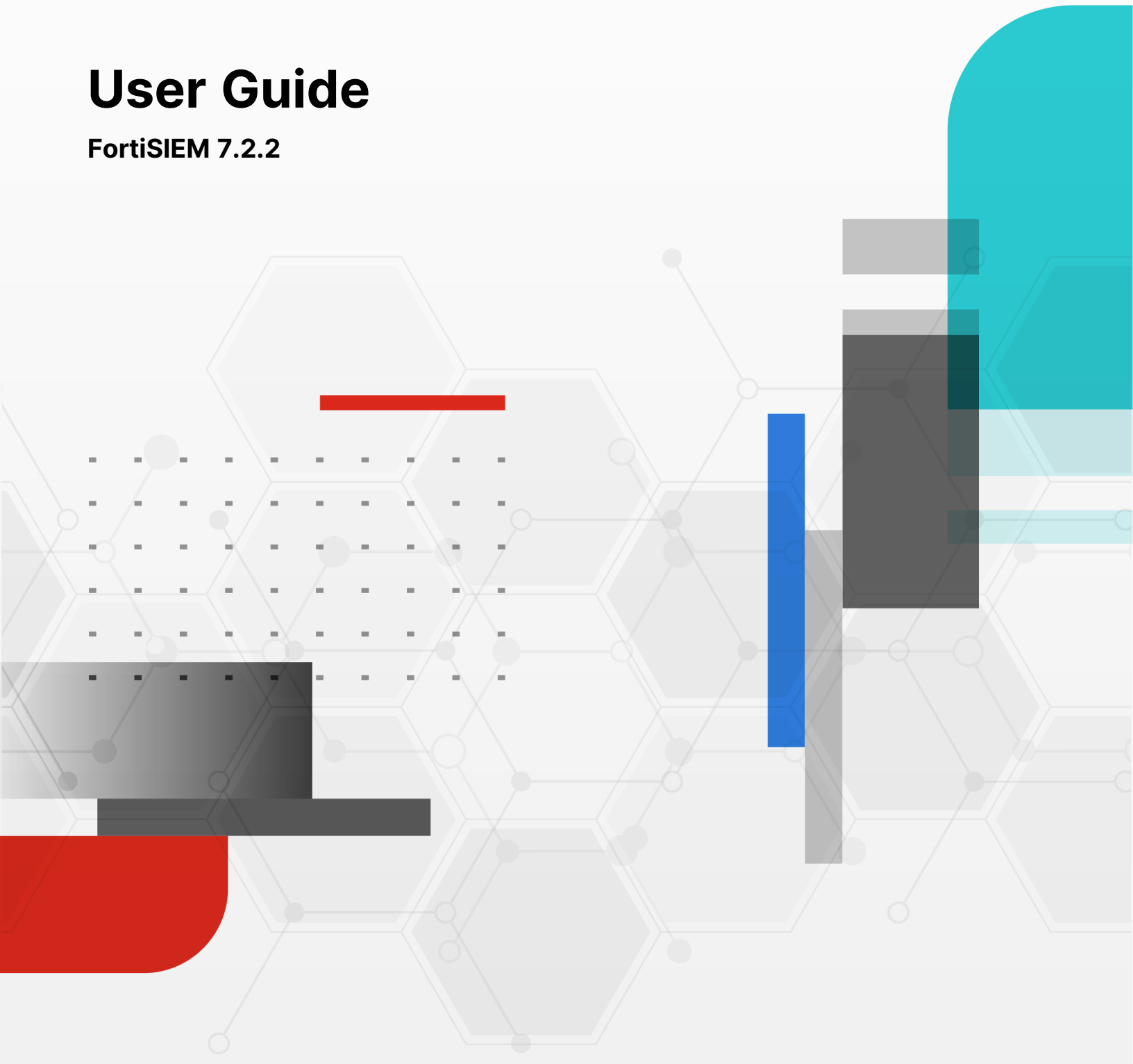
FORTINET

User Guide

FortiSIEM 7.2.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

03/05/2026
FortiSIEM 7.2.2 User Guide

TABLE OF CONTENTS

Overview **48**
Scale-Out Architecture 48
Multi-tenancy 48
Infrastructure Discovery and Automated CMDB 48
High Performance Log Collection and Flexible Parsing 49
Performance and Availability Monitoring 49
Network Configuration and File Integrity Monitoring 49
Custom Device and Application Support 50
User Identity and Location Tracking 50
External Threat Intelligence Integration 50
Distributed Event Correlation and Threat Detection – the Rule Engine 50
Device and User Risk Scoring 51
Incident Response and Mitigation 51
Search, Threat Hunting, Compliance Reports and Dashboards 51
Internal Ticketing System and Two-way Third-party Ticketing Integration 51
Business Service Analytics 52
FortiSIEM Releases **53**
What's New in 7.2.2 ..... **54**
New Features 54
Raw Event Size based Licensing 54
Exporting QRadar Logs to FortiSIEM 55
Enhancements 55
Dashboard Query Optimization (for ClickHouse) 55
Rocky Linux Update 55
Bug Fixes 56
Implementation Notes 60
PostGreSQL Related 61
Collector HA Related 61
Identity and Location Related 62
Post-Upgrade ClickHouse IP Index Rebuilding 63
What's New in 7.2.1 ..... **64**
Bug Fixes 64
Important Considerations 67
PostGreSQL v13.14 Update 67
Post-Upgrade ClickHouse IP Index Rebuilding 67
Implementation Notes and Known Issues 68
What's New in 7.2.0 ..... **70**
New Features 70
Automated Case Management 70
Collector High Availability 71
Search Field Analytics 73
Custom SIGMA Rule Import 73

Key Enhancements 73
Rocky Linux Update 74
Enhanced Host and User Risk Scoring 74
Increase Non-aggregated Search Result limit up to 1 Million (ClickHouse only) 74
Enable FortiSIEM 500G Hardware Appliance to run as a ClickHouse Keeper 74
GUI Improvements 75
FortiAI (previously Fortinet Advisor) Improvements 75
Support for 34 Additional External Threat Intelligence Sources 75
Miscellaneous Enhancements 76
External Log Source Integration 77
Bug Fixes 77
Important Considerations 82
PostGreSQL v13.14 Update 82
Post-Upgrade ClickHouse IP Index Rebuilding 82
Implementation Notes and Known Issues 82
What's New in 7.1.9 85
System Update 85
Linux Agent Update 85
Bug Fixes and Enhancements 85
Implementation Notes 86
PostGreSQL Related 86
Post-Upgrade ClickHouse IP Index Rebuilding 86
Upgrade Related 86
What's New in 7.1.8 87
System Update 87
Bug Fixes and Enhancements 87
Implementation Notes 88
PostGreSQL Related 88
Post-Upgrade ClickHouse IP Index Rebuilding 88
Upgrade Related 88
What's New in 7.1.7 89
Bug Fixes 89
PostGreSQL Update 89
Post-Upgrade ClickHouse IP Index Rebuilding 90
What's New in 7.1.6 91
OS Updates 91
Rocky Linux Update 91
PostGreSQL Update 91
Bug Fixes 92
Post-Upgrade ClickHouse IP Index Rebuilding 96
What's New in 7.1.5 97
Key Enhancements 97
Rocky Linux Update 97
PostGreSQL Update 97
Bug Fixes 98

Post-Upgrade ClickHouse IP Index Rebuilding ... 99
What's New in 7.1.4 ... 100
New Feature ... 100
ClickHouse Archive to Google Cloud Storage (GCS) ... 100
Key Enhancements ... 100
Rocky Linux Update ... 100
Windows Agent Log Handling Performance Improvement ... 101
ClickHouse Data Movement Algorithm Change ... 102
Incident Actions Added to all Incident Pages ... 102
Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields ... 103
Bug Fixes and Enhancements ... 104
What's New in 7.1.3 ... 109
Known Issue ... 109
What's New in 7.1.2 ... 112
Known Issues ... 112
Installation / Upgrade Related ... 112
ClickHouse Related ... 114
What's New in 7.1.1 ... 117
Key Enhancements ... 117
Rocky Linux 8.9 ... 117
Redis Memory Usage Optimization ... 117
Support for Trend Vision One ... 118
More SOC Queries via Fortinet Advisor ... 118
SIGMA Rule Fixes ... 118
Public REST API Throttling ... 118
Bug Fixes and Enhancements ... 119
Known Issue ... 123
What's New in 7.1.0 ... 126
New Features ... 126
Fortinet Advisor ... 126
Scheduled Rules for ClickHouse based Deployments ... 127
Windows Certificate Monitoring via Agent ... 128
Windows Osquery via Agent ... 128
User Alias in Risk Calculation ... 129
New Machine Learning Models ... 129
Key Enhancements ... 129
OS Update ... 129
FortiSIEM GUI Enhancements ... 130
Dynamic Watchlist using User-to-IP Lookup ... 130
Kafka Event Collection Improvements ... 130
ClickHouse Storage Reduction for Existing Deployments ... 131
Windows Agent GUI Enhancement ... 131
Ability to Choose a Network Interface during Installation ... 131
Public REST API Enhancements ... 131
Generic STIX/TAXII 2.1 Integration for collecting External Threat Intelligence ... 132
Content Update ... 132

New Device Support 132
Device Support Enhancements 133
Bug Fixes and Enhancements 134
Known Issues 141
What's New in 7.0.4 142
System Update 142
Implementation Notes 142
Upgrade Related 142
What's New in 7.0.3 143
What's New in 7.0.2 146
Storage Space Reduction for ClickHouse Based Deployments 146
Bug Fixes and Minor Enhancements 146
Important Notes 147
What's New in 7.0.1 149
Important Notes 149
Key Enhancements 150
Rocky Linux 8.8 150
Optimized Incident Trigger Event Lookup 150
Bug Fixes 151
What's New in 7.0.0 155
Important Notes 155
New Features 157
Visual Report Designer 158
New Query Functions 158
Machine Learning Workbench 159
Incident Investigation Workspace 159
Built-in Machine Learning Models 159
ClickHouse Event Integrity 161
Fortinet Security Fabric Discovery 161
FortiEMS Discovery 161
FortiEMS Endpoint Tagging 162
Windows Agent 5.0.0 162
Linux Agent 7.0.0 162
Key Enhancements 162
Enhanced Entity Risk View 163
External Threat Intelligence Integration Enhancements 163
Elasticsearch 8.5.3 Support 163
FortiGate VDOM Based Mitigation 163
Rule Enhancements 163
GUI Inactivity Timeout Enforcement 163
Miscellaneous Enhancements 164
Bug Fixes and Enhancements 165
Known Issues 170
General 170
ClickHouse Related 170
Discovery Related 171

Elasticsearch Related ... 171
EventDB Related ... 172
HDFS Related ... 172
High Availability Related ... 172
Windows Agent Releases ... 174
Windows Agent 7.2.5 ... 174
Windows Agent 7.2.4 ... 174
Windows Agent 7.2.3 ... 174
Windows Agent 7.2.2 ... 175
Windows Agent 7.2.1 ... 175
Windows Agent 7.2.0 ... 175
Windows Agent 7.1.8 ... 175
Windows Agent 7.1.7 ... 175
Windows Agent 7.1.6 ... 176
Windows Agent 7.1.5 ... 176
Windows Agent 7.1.4 ... 176
Windows Agent Log Handling Performance Improvement ... 177
Windows Agent 7.1.1 ... 178
Windows Agent 7.1.0 ... 178
Windows Agent 5.0.1 ... 179
Windows Agent 5.0.0 ... 179
Windows Agent 4.4.1 ... 179
Windows Agent 4.4.0 ... 179
Support for Virtual Desktop Infrastructure (VDI) Environment ... 180
Bug Fix ... 180
Windows Agent 4.3.0 ... 180
Software Installer Improvements ... 180
Robust Detection of Event Log Restart (Event ID 1100) ... 181
Restart Event Collection from Last Position ... 181
Monitor Software Installed via Microsoft Apps ... 181
Windows Agent 4.2.7 ... 181
Windows Agent 4.2.6 ... 182
Windows Agent 4.2.5 ... 182
Windows Agent 4.2.4 ... 182
Windows Agent 4.2.3 ... 182
Windows Agent 4.2.2 ... 182
Windows Agent 4.2.1 ... 183
Windows Agent 4.2.0 ... 183
Windows Agent 4.1.6 ... 183
Windows Agent 4.1.5 ... 183
Windows Agent 4.1.4 ... 184
Windows Agent 4.1.3 ... 184
Windows Agent 4.1.2 ... 184
Windows Agent 4.1.1 ... 184
Windows Agent 4.1.0 ... 185

Windows Agent 4.0.1 ... 185
Windows Agent 4.0.0 ... 185
Windows Agent 3.3.1 ... 186
Windows Agent 3.3.0 ... 186
Windows Agent 3.2.3 ... 186
Windows Agent 3.2.2 ... 186
Windows Agent 3.2.1 ... 187
Windows Agent 3.2.0 ... 187
Windows Agent 3.1.3 ... 187
Windows Agent 3.1.2 ... 187
Windows Agent 3.1.0 ... 188
Content Pack Updates ... 189
Deployment Notes ... 189
Content Updates for 7.2.x ... 189
Content Update 720 ... 190
Content Update 718 ... 190
Content Update 717 ... 194
Content Update 713 ... 196
Content Update 712 ... 197
Content Update 711 ... 198
Content Updates for 7.2.0, 7.2.1, 7.2.2, 7.2.3, 7.2.4 and 7.2.5 ... 199
Content Update 709 ... 199
Content Updates for 7.2.0, 7.2.1, 7.2.2, 7.2.3 and 7.2.4 ... 199
Content Update 708 ... 200
Content Updates for 7.2.0, 7.2.1, 7.2.2 and 7.2.3 ... 200
Content Update 707 ... 200
Content Update 706 ... 201
Content Update 705 ... 201
Content Update 704 ... 201
Content Updates for 7.2.0, 7.2.1, and 7.2.2 ... 202
Content Update 703 ... 202
Content Updates for 7.2.0 and 7.2.1 ... 202
Content Update 702 ... 202
Content Updates for 7.2.0 ... 202
Content Update 701 ... 203
Key Concepts ... 204
Clustering Architecture ... 204
Licensing ... 205
Multi-tenancy and Organizations ... 206
Role-based Access Control ... 207
Discovery and CMDB ... 207
Windows and Linux Agents ... 208
Business Services ... 209
Parsers and Monitors ... 209
Entity Risk Score ... 210

User Identity and Location 210
Searches, Reports and Compliance 210
Rules and Incidents 211
Incident Automation Policy 211
Remediation Library 212
External Ticketing System Integration 212
Dashboards 212
Getting Started 214
Step 0 - Pre-Install Considerations 214
Step 1 - Install the Virtual or Hardware Appliance 215
Step 2 - Install License 215
Step 3 - Specify Event Database Storage 216
Step 4 - Check System Health and License 216
Step 5 - (Optional) Create Organizations for Service Provider Deployments 216
Step 6 - (Optional) Check Full Admin Organization Users for Service Provider Deployments 216
Step 7 - Add Email Gateway 216
Step 8 - (Optional) Add Collector 216
Step 9 - (Optional) Set Event Upload Destination for the Collector(s) 217
Step 10 - (Optional) Check Collector Health 217
Step 11 - Receive Syslog and Netflow 217
Step 12 – Check CMDB Devices and Run Searches for Received Events 218
Step 13 - Discover Devices 218
Step 14 - Check CMDB and Performance Monitors for Discovered Devices 218
Step 15 - Check Monitored Device Health 219
Step 16 - Check Incidents 219
Step 17 – Notify an Incident via Email 219
Step 18 – Create a Ticket in FortiSIEM 220
Step 19 - View System Dashboards 220
Step 20 - (Optional) Add Worker 220
Step 21 - (Optional) Check Worker Health 220
Step 22 - Check License Usage 220
Step 23 - Set Home Page and Complete Your User Profile 220
Step 24 – Log On to the Console and Check Status 221
Step 25 - Set up Automated CMDB Disk Space Management 221
Step 26 - Create Retention Policy 222
Step 27 - Online Documentation and FortiAI 222
Advanced Operations 223
CMDB Advanced Operations 224
Discovering Users 224
Creating FortiSIEM Users 225
Setting External Authentication 225
Setting 2-Factor Authentication 226
Assigning FortiSIEM Roles to Users 226
Creating Business Services 227
Creating Dynamic CMDB Groups and Business Services 227
Setting Device Geo-Location 228

Creating CMDB Reports 228
Incidents and Cases Advanced Operations 229
Changing the Home Country 229
Searching Incidents 229
Tuning Incidents via Exceptions 230
Tuning Incidents via Modifying Rules 230
Tuning Incidents via Drop Rules 230
Tuning Incidents by Adjusting Thresholds 231
Clearing Incidents 231
Adding Comments or Remediation Advice to an Incident 232
Remediating an Incident 232
Notifying an Incident via Email 234
For Policy based Notification 235
Creating New Rules 235
Creating a FortiSIEM Case Manually 235
Creating a Case Automatically 235
Device Support Advanced Operations 236
Checking Device Monitoring Status and Health 236
Setting Devices Under Maintenance 237
Creating Custom Monitors 237
Setting Important Interfaces and Processes 238
Modifying System Parsers 238
Creating Custom Parsers 238
Handling Multi-line Syslog 239
Creating Synthetic Transaction Monitors 239
Mapping Events to Organizations 239
Adding Windows Agents 239
Adding Linux Agents 240
Forwarding Events to External Systems 240
Rules, Reports and Dashboards Advanced Operations 241
Creating New Rules 241
Creating New Reports 241
Scheduling Reports 242
Customizing Built-in Dashboards 242
Creating Custom Dashboards 242
Creating Business Service Dashboards 243
Advanced Health System Advanced Operations 244
Monitoring System Health 244
Monitoring Collector Health 244
Monitoring Agent Health 244
Monitoring Elasticsearch Health 245
Monitoring Replication Health 245
System Errors 245

Monitoring User and Query Activity 245
Logged in Users 245
Locked Users 246
Query Status 247
Query Workload 248
Managing FortiSIEM Advanced Operations 250
Administrator Tools 250
Backing Up and Restoring FortiSIEM Directories and Databases 250
Administration 251
Setup 252
Configuring Storage 253
Configuring ClickHouse Based Deployments 253
ClickHouse Configuration Overview 253
Configuring ClickHouse Storage on Supervisor Node 254
Configuring ClickHouse Topology 255
Creating ClickHouse Archive Storage 255
Configuring EventDB Based Deployment 259
EventDB Configuration Overview 259
Creating EventDB Online Storage 259
Creating EventDB Archive Storage 260
Configuring Elasticsearch Based Deployment 260
Elasticsearch Configuration Overview 260
Creating Elasticsearch Online Storage 261
Creating Archive for Elasticsearch Based Deployments 263
Changing Event Database 264
Elasticsearch to NFS 265
Local to NFS 265
NFS to Local 266
EventDB to ClickHouse 266
Elasticsearch to ClickHouse 268
ClickHouse to EventDB 269
ClickHouse to Elasticsearch 270
Changing NFS Server IP 271
Setting Organizations and Collectors (Service Provider) 273
Creating an Organization 273
Installing a Collector 275
Registering a Collector 275
Complete these steps to add a Collector: 277
Installing a Collector 277
Registering a Collector 278
Setting Credentials 279
Creating a Credential 279
Associating a Credential to IP Ranges or Hosts 280
Testing Credentials and API Event Collection 281
Modifying Device Credentials 281

Modifying a Credential Association 282
Credentials Based on Access Protocol 282
Discovering Devices 283
Creating a Discovery Entry 283
Discovering on Demand 286
Scheduling a Discovery 287
Searching Previous Discovery Results 287
Editing a Discovery 287
Exporting Discovery Results 288
Editing Event Pulling 289
Viewing Event Pulling Jobs 289
Modifying Event Pulling Jobs 290
Checking Status of Event Pulling Jobs 291
Exporting Event Pulling Jobs into a Report 291
Viewing Event Pulling Reports 291
Editing Performance Monitors 292
Viewing Performance Monitoring Jobs 292
Enabling/Disabling Performance Monitoring Jobs 293
Modifying Performance Monitoring Jobs 293
Configuring Synthetic Transaction Monitoring 294
Creating Monitoring Definition 294
Creating an STM Test 294
Editing Monitoring Definition 295
Protocol Settings for STM Tests 295
Configuring Maintenance Calendars 303
Create a Maintenance Calendar 303
Specifying a Schedule 304
Specifying the Devices Under Maintenance 304
Viewing Existing Maintenance Calendars 304
Modifying Existing Maintenance Calendars 305
Configuring Windows Agent 306
Define the Windows Agent Monitor Templates 306
Associate Windows Agents to Templates 315
Viewing Agent Status 315
Enabling or Disabling an Agent 316
Viewing Files in FortiSIEM 316
Verifying Events in FortiSIEM 317
Service Level Protection Properties 317
Auto Restart Service Behavior 317
Configuring Debug Trace Logging without Agent Service Restart 318
Configuring the Agent Database Size 318
Agent Troubleshooting Notes 318

Configuring Linux Agent ... **320**
Define the Linux Agent Monitor Templates ... 320
Associate Linux Agents to Templates ... 323
Viewing Agent Status ... 324
Enabling or Disabling an Agent ... 324
Viewing Files in FortiSIEM ... 324
File Integrity Monitoring Logs ... 325
Agent Troubleshooting Notes ... 331
Configuring FortiSIEM Instance for FortiSIEM Manager ... **332**
Unregister FortiSIEM Manager Instance ... 332
Deleting FortiSIEM Manager Instance ... 332
Testing FortiSIEM Instance ... 332
Device Support ... **333**
Working with Devices or Applications ... **334**
Adding a Device or Application ... 334
Modifying a Device or Application ... 335
Working with Event Attributes ... **336**
Adding an Event Attribute ... 336
Modifying an Event Attribute ... 337
Working with Event Types ... **338**
Adding an Event Type ... 338
Modifying an Event Type ... 339
Working with Parsers ... **340**
Overview ... 340
Viewing all Parsers ... 341
Understanding Parser Order ... 341
Viewing a Specific Parser ... 342
Disabling a Parser ... 342
Enabling a Parser ... 343
Deleting a Parser ... 343
Modifying a Parser ... 343
Creating a New Parser ... 344
Adjusting Parser Order ... 345
Working with Custom Performance Monitors ... **347**
Creating a Custom Performance Monitor ... 347
Prerequisites ... 347
Monitoring Protocol Configuration Settings ... 348
JDBC Configuration Settings ... 349
JMX Configuration Settings ... 350
SNMP Configuration Settings for Custom Performance Monitors ... 350
WMI Configuration Settings for Custom Performance Monitors ... 352
LOGIN Configuration Settings for Custom Performance Monitors ... 352
Mapping Monitoring Protocol Objects to Event Attributes ... 354
Creating Transforms ... 355

Managing Monitoring of System and Application Metrics for Devices 355
Working with Custom Properties 356
Adding a Custom Property 356
Modifying a Custom Property 356
Creating SNMP System Object Identifiers for Devices 357
Analyzing Custom Log Files 358
Configuring Local Syslog File Ingestion from a Directory 359
Configuring Local PCAP File Ingestion from a Directory 360
Health 361
Viewing Cloud Health 362
First Frame 362
Second Frame 363
FortiSIEM Back-End Processes 364
Viewing Collector Health 368
Properties Associated with Collector Health 369
Process Properties 371
FortiSIEM Back-End Processes 372
Properties Associated with Tunnels 372
Open Tunnel Re-Configuration Required after 6.3.0 or later Upgrade/Fresh Install 373
Viewing Agent Health 374
Properties Associated with Agent Health 374
Viewing Elasticsearch Health 376
Viewing Replication Health 378
License 380
Viewing License Information 381
EPS Based Licensing 381
GB Per Day Licensing 381
Viewing License Usage 383
EPS Licensing 383
About Events Per Second 383
EPS Usage By Node 384
EPS Usage by Organization 384
Used EPS (Global) 385
Notes 385
GB Per Day Licensing 385
Violations 386
About Raw Event Usage 386
Notes 386
Working with Nodes 387
Viewing a Node 387
Adding a Node 388
Adding a Worker Node 388
Adding a Primary Follower Node (with High Availability Node) 389
Adding a Secondary Supervisor Node (with Disaster Recovery Enabled) 389

Editing a Node 389
Editing a Worker Node 389
Editing the Primary Leader Node 390
Editing a Primary Follower Node 390
Editing Secondary Supervisor (with Disaster Recovery Enabled) 390
Deleting a Node 391
Deleting Worker Node 391
Deleting Primary Follower Node 391
Configuring and Maintaining Active-Active Supervisor Cluster 392
Operational Overview 392
Configuration 394
Adding Primary Leader 394
Adding Primary Follower 394
Load Balancer Setup 397
Collecting UUID and SSH Public Key 397
External Load Balancer Configuration 398
Maintenance 401
Failover Operations 401
Checking Cluster Replication Health 403
Maintenance Operations 404
Upgrade 405
Configuring Disaster Recovery 405
Configuring Disaster Recovery for ClickHouse 405
Configuring Disaster Recovery for Elasticsearch 405
Configuring Disaster Recovery for EventDB 405
Content Update 406
Content Update Notification 406
Viewing Content Updates 406
Checking for Content Updates 407
Viewing Content Update History 407
Installing Content Update 407
Settings 409
System Settings 411
UI Settings 411
User Profile UI Settings 411
Administrator UI Settings 412
Email Settings 413
Customizing the Incident Email Template 414
Example Registering FortiSIEM with Azure via OAUTH 417
Image Server Settings 426
Upgrading Collectors 426
Upgrading Linux Agents 428
Upgrading Windows Agents 430
Custom Update 431
Cluster Config 432
Supervisor / Load Balancer Configuration 432
Event Upload Workers Configuration 432

Lookup Settings 433
Kafka Settings 433
Setting up Consumer 434
Setting Up FortiSIEM 437
Dashboard Slideshow Settings 438
Dashboard Ownership 438
PAYG Report 439
Trusted Hosts 439
FortiGuard Proxy 440
FQDN 440
Collector High Availability Configuration 441
AWS/EC2 Collector Deployments 443
Step 1 - Configure Collectors 444
Step 2 - Create IAM Policy 444
Step 3 - Create IAM Role 445
Step 4 - Associate IAM Role to all Collectors 446
Step 5 - Locate Unused VIP 447
Step 6 - Configure Collector HA Group Via VRRP 449
Azure Collector Deployments 451
Step 1 - Configure Collectors 451
Step 2 - Configure Port Rule 451
Step 3 - Create Load Balancer 452
Step 4 - Configure Load Balancer 458
Step 5 - Configure Collector HA Group Via Load Balancer 461
GCP Collector Deployments 463
Step 1 - Configure Collectors 463
Step 2 - Create Instance Group 463
Step 3 - Create Load Balancer 465
Step 4 - Check Load Balancer 471
Step 5 - Configure Load Balancer to Report Health Status 472
Step 6 - Configure Collector HA Group Via Load Balancer 473
Non-Cloud Collector Deployments 475
Step 1 - Configure Collectors 475
Step 2 - Configure Collector HA Group Via VRRP 476
Troubleshooting 477
DB Cluster Configuration 480
Analytics Settings 481
Scheduled Reports 481
Scheduling Report Alerts 481
Scheduling Report Copy 482
Incident Notification 482
Webhook Notification 482
Setting Incident HTTP Notification 483
Setting Incident SNMP Traps 483

Setting Remedy Notification 483
Setting a Subcategory 487
Creating a Subcategory 488
Modifying a Subcategory 488
Deleting a Subcategory 488
Setting Risk Filters 488
Creating a Risk Filter 489
Editing a Risk Filter 489
Deleting a Risk Filter 489
Viewing Risk Filter Results 489
Tags 490
Creating a Tag 490
Editing a Tag 490
Deleting a Tag 490
ML / AI 491
General Configuration 491
Configuring AWS ML 491
Configuring FortiAI 491
UEBA Settings 492
Setting UEBA Higher Risk Entities 492
Setting UEBA Tags 492
Cloud Machine Learning 494
Set Up AWS SageMaker 494
Configure FortiSIEM to use AWS SageMaker 495
Other Tasks 495
Checking AWS SageMaker Training Job Status 495
Checking AWS SageMaker Hyperparameter Tuning Job Status 496
Checking AWS SageMaker Inference Job Status 496
Implementation Notes 496
AWS Auto Mode Running Time 496
Discovery Settings 497
Generic 497
Device Filter 498
Application Filter 499
Location 499
CMDB Groups 500
Grouping Devices by Custom Properties 501
Monitoring Settings 502
Important Processes 502
Important Ports 502
Important Interfaces 503
Excluded Disks 503
Windows WMI Filter 504
Step 1: Create the Windows WMI Filter 504
Step 2: Apply the Filter in a Credential 504
Step 3: Discover Using the WMI Credential in Step 2 505

Event Handling Settings 506
Event Dropping 506
Event Forwarding 507
Event Forwarding by Worker 508
Event Organization Mapping 509
Multiline Syslog 509
Database Settings 511
Creating Retention Policy 512
ClickHouse Event Retention 512
How ClickHouse Event Retention Works 513
Creating ClickHouse Time Based Event Retention Policy 515
Creating ClickHouse Archive Event Retention Policy for EventDB on NFS 516
FortiSIEM EventDB Event Retention 516
How EventDB Event Retention Works 516
Creating EventDB Online Event Retention Policy 517
Creating EventDB Archive Event Retention Policy 518
Elasticsearch Event Retention 519
How Elasticsearch Event Retention Works 519
Configuring Elasticsearch Retention Threshold 520
Configuring HDFS Archive Threshold 520
Creating Elasticsearch Archive Event Retention Policy 521
Viewing Online Event Data Usage 521
Viewing Archive Event Data 521
Event Log Integrity 522
Validating Event Log Integrity for EventDB 522
Viewing EventDB Event Log Integrity Status 522
Validating EventDB Event Log Integrity 523
Exporting EventDB Event Log Integrity Status 523
Validating Event Log Integrity for ClickHouse 524
Viewing ClickHouse Event Log Integrity Status 524
Validating ClickHouse Event Log Integrity 525
Automating ClickHouse Log Integrity 525
ClickHouse Configuration 526
Role Settings 528
Adding a New Role 530
Modifying a Role 531
Example Role Setup 531
Setting Up an Incident Remediation Workflow Example 531
Viewing User Roles for AD Group Mappings 533
Mapping AD Groups to Roles 534
Step 1: Setup or Edit an Authentication Profile 534
Step 2: Create a Role to be Mapped to the AD Group 534
Step 3: Assign an AD Group 534
Step 4: Test Your Mappings 535
Principle of Least Restrictive Role 535

Compliance Settings **537**
PCI Compliance Policy **538**
Viewing PCI Policies 538
Adding a PCI Logging Policy 538
Editing a PCI Logging Policy 539
Deleting a PCI Logging Policy 539
General Settings **540**
External Authentication Settings **541**
Configure FortiSIEM Users for non-SAML External Authentication 541
Step 1: Create External Authentication Profile 541
Step 2: Associate User to External Authentication Profile 542
Configure FortiSIEM Users for SAML Authentication 543
Step 0: Overview 543
Step 1 - Preparation 544
Step 2 - Create External Authentication Profile in FortiSIEM 544
Step 3 - Create SAML Role Mappings in FortiSIEM 545
Step 4 - Create the User in CMDB 545
Example 1: Configure FortiSIEM Users for SAML Authentication with Azure AD 546
Step 1: Setup Azure 546
Step 2: Setup FortiSIEM 551
Step 3: Setup SAML Role Mapping 552
Example 2: Configuring FortiSIEM Users for RADIUS/LDAP Authentication with FortiAuthenticator (FAC) 554
Step 1: Configure AD Users 554
Step 2: Configure FortiAuthenticator 555
Step 3: Configure FortiSIEM 556
Logging In 557
Example 3: Configuring FortiSIEM Users for SAML Authentication with FortiAuthenticator (FAC) 557
Set Up FortiAuthenticator as an IdP 557
Add FortiSIEM as Service Provider 561
Set Up FortiSIEM 562
Set Up SAML Role Mapping 564
Import Users from FortiAuthenticator 564
Example 4: Configuring FortiSIEM Users for SAML Authentication with OKTA 565
Example 5: Configuring FortiSIEM Users for 2 Factor Authentication with Duo Security 569
Step 0: Obtain Keys for FortiSIEM to Communicate with Duo Security 569
Step 1: Create and Manage FortiSIEM users in Duo Security 570
Step 2: Add 2-Factor Authentication Option for FortiSIEM Users 570
Step 3: Log in to FortiSIEM Using 2-Factor Authentication 571
Troubleshooting SAML Operations 571
Plugin Tool 571
Issues after Successful Authentication 572
Common Configuration Errors 572
SAML Login Error Codes 573

Automation Policy ... **575**
Adding Automation Policy Settings ... 575
Modifying Automation Policy Settings ... 576
Enabling Automation Policies ... 576
Applying Case Creation to Automation Policy ... 577
Define Notification Action - Email/SMS/Webhook ... **578**
Configuring Notification Action for Email/SMS/Webhook ... 578
Configuring Notification Action for Email via CMDB > Users ... 579
Edit Email Template ... 579
Configuring External Integrations ... **580**
Configuring Ticketing System Integrations ... 580
ServiceNow Integration ... 581
Jira Integration ... 596
ConnectWise Integration ... 599
Salesforce Integration ... 605
CMDB Inbound Integration ... 609
Configuring Reputation System Integrations ... 611
VirusTotal Integration ... 611
FortiGuard IOC Lookup Integration ... 612
RiskIQ Integration ... 613
Configuring Communication through Proxies ... 614
Modifying an External System Integration ... 615
ServiceNow Security Operations (SecOps) Integration ... **616**
Scope and Purpose ... 616
XML Assets ... 616
Process Overview ... 616
Process and Workflow ... 617
ServiceNow FortiSIEM Integration Prerequisites ... 617
ServiceNow FortiSIEM Integration Installation ... 617
ServiceNow FortiSIEM Integration Usage ... 625
View Scheduled Jobs ... 625
Monitor Scheduled Job Execution Logs ... 625
Examine FortiSIEM Incidents, Logs, and Triggering Events ... 625
View Corresponding Security Incidents ... 626
Examine Security Incidents in Detail ... 626
Customized "FortiSIEM Incident" Page ... 627
ServiceNow FortiSIEM Integration Deletion ... 627
ServiceNow and FortiSIEM Field Mappings ... 631
FortiSIEM Closed State Mappings ... 631
FortiSIEM Incident Category Field: "phSubIncidentCategory" Mappings ... 632
FortiSIEM Incident Severity Field: "eventSeverity" Mappings ... 635
FortiSIEM Triggering Events Attributes Displayed in ServiceNow ... 635
Known Limitations ... 636
Required Permissions for ServiceNow SOAP Integration ... **637**
General Requirements ... 637
Required Table and Field Permissions for CMDB Outbound Integration ... 638

Main Table Permissions 638
Extended Table Permissions 639
Reference Table Permissions 641
Reference Field Permissions 642
Regular Field Permissions 642
Required Table and Field Permissions for Incident Outbound Integration 642
Main Table Permissions 642
Reference Table Permissions 642
Reference Field Permissions 643
Regular Field Permissions 643
Case Management 644
Adding/Editing a Case Management Policy 644
Adding/Editing Case Close Codes 646
Viewing Case Management Policy 647
Viewing Case Close Codes 647
Applying Case Creation to Automation Policy 648
Configuring SSL Socket Certificates 649
Running the SSL Configuration Script 649
Script Options 649
Script Examples 651
Disable Certificate Verification in Both Directions 651
Enable Verification in Both Directions Using a Public Certificate 651
Enable Verification in Both Directions with a Self-Signed Certificate 652
Managing CMDB 653
Devices 654
Viewing Device Information 655
Working with Device Groups 657
Adding Device Groups 657
Modifying Device Groups 657
Performing Operations on Device Groups 658
Changing Display Columns 658
Creating and Editing Devices 659
Performing Operations on Devices and Device Groups 660
Associating Parsers to a Device 662
Searching for Devices 663
Applications 664
Viewing Application Information 665
Adding an Application 665
Editing Applications 666
Working with Application Groups 667
Adding Application Groups 667
Modifying Application Groups 667

Users 668
Viewing User Information 669
Adding Users 670
Add Users Manually 670
Discover Users from Microsoft Active Directory 672
Step 1: Create LDAP Login Credentials and Associate with LDAP Server IP Address 672
Step 2: Discover Active Directory Server and Users 673
Step 3: Set FortiSIEM Attributes for Users 673
Discover Users from OKTA 674
Step 1: Prepare OKTA for Authentication 674
Step 2: Create an OKTA API Token 675
Step 3: Create OKTA Login Credentials in FortiSIEM and Associate with OKTA Server 675
Step 4: Discover OKTA Users 676
Step 5: Set FortiSIEM Attributes for Users 676
Implementation Notes 677
Editing User Information 678
Performing Operations on Users 681
Working with User Groups 682
Adding User Groups 682
Adding a FortiSIEM Analyst Team 682
Modifying User Groups 683
Business Services 684
Viewing Business Services 684
Creating Business Services 684
Working with Business Service Groups 686
Adding Business Service Groups 686
Modifying Business Service Groups 686
CMDB Reports 688
Creating CMDB Reports 691
Creating a CMDB Report 691
Cloning and Modifying a CMDB Report 692
Exporting a CMDB Report 692
Importing and Exporting CMDB Report Definitions 692

Scheduling a CMDB Report ... **694**
Running a CMDB Report ... **695**
Adding CMDB Report to Dashboard ... **696**
Managing Resources ... **697**
Reports ... **698**
Viewing System Reports ... **699**
Running System Reports ... **700**
Creating New Reports ... **701**
Creating a Report ... 701
Creating a Report Bundle ... 701
Editing a Report Bundle ... 702
Working with Report Design Templates ... **703**
Creating a Report Template ... 704
Creating Report Templates for a Report Folder or Resource Bundle ... 704
Modifying an Existing Report Template ... 704
Designing a Report Template ... 705
Overview ... 705
Cover Page ... 710
Report - Sections and Objects ... 711
Scheduling Reports ... **715**
Scheduling a Report ... 715
Scheduling a Report Bundle ... 716
Scheduling Reports Using a Workflow ... 717
Step 1 - Create Appropriate Roles for Users ... 718
Step 2 - Map Users to Appropriate Roles ... 718
Step 3 - Request Report to be Scheduled ... 718
Step 4 - Approve the Report Scheduling Request ... 718
Step 5 - View Report Scheduling Request Status ... 719
Importing and Exporting Reports ... **720**
Importing a Report ... 720
Exporting a Report Definition ... 720
Exporting Report Results ... 720
Importing and Exporting Report Definitions ... **722**
Importing a Report Definition ... 722
Exporting a Report Definition ... 722
Rules ... **723**
Viewing Rules ... **724**
Creating Rules ... **725**
Creating a Rule ... 725
Defining Rule Conditions ... 729
Defining the Incident Generated by a Rule ... 732
Defining Rule Exceptions ... 733
Defining Clear Conditions ... 733

Defining an Incident Title ... 734
To Display the Incident Title Field ... 734
Activating and Deactivating a Rule ... 736
Activating a Rule Without a Workflow ... 736
Activating a Rule Using a Workflow ... 736
Step 1 - Create Appropriate Roles for Users ... 736
Step 2 - Map Users to Appropriate Roles ... 737
Step 3 - Request Rule to be Activated/Deactivated ... 737
Step 4 - Approve the Rule Activation/Deactivation Requests ... 737
Step 5 - View the Rule Activation/Deactivation Request Status ... 738
Activating/Deactivating Multiple Rules ... 738
Testing a Rule ... 739
Exporting and Importing Rule Definitions ... 740
Exporting a Rule Definition ... 740
Importing a Rule Definition ... 740
Importing Sigma Rules ... 741
Importing via URL ... 741
Importing via File ... 742
Importing via Custom Input ... 742
Networks ... 744
Adding a Network ... 745
Modifying a Network ... 746
Deleting a Network ... 747
Watch Lists ... 748
System-defined Watch List ... 749
Creating a Watch List ... 756
Modifying a Watch List ... 757
Using a Watch List ... 758
Adding Watch List to a Rule ... 758
Using Watch Lists as Conditions in Rules and Reports ... 758
Exporting and Importing Watch Lists ... 760
Exporting a Watch List ... 760
Importing a Watch List ... 760

Protocols ... **761**
Adding a Protocol ... **762**
Modifying a Protocol ... **763**
Deleting a Protocol ... **764**
Event Types ... **765**
Adding an Event Type ... **766**
Modifying an Event Type ... **767**
Deleting an Event Type ... **768**
Working with AlienVault OTX ... **769**
Working with AlienVault OTX Malware Domains ... 769
Enabling the AlienVault OTX Service ... 769
Disabling the AlienVault OTX Service ... 769
AlienVault OTX Malware Domain Values ... 770
Working with AlienVault OTX Malware IPs ... 770
Working with AlienVault OTX Malware URLs ... 771
Working with AlienVault OTX Malware Hash ... 771
Working with Custom Threat Feeds that use HTTPS Connectivity ... **772**
Working with Dragos IOCs ... **773**
Download Dragos Worldview Malware Domains ... 773
Download Dragos Worldview Malware IPs ... 773
Download Dragos Worldview Malware Hashes ... 774
Specifying a Schedule ... 774
Working with FortiGuard IOCs ... **776**
Working with FortiGuard Malware Domains ... 776
Enabling the FortiGuard IOC Service ... 776
Disabling the FortiGuard IOC Service ... 776
Using a Proxy for the FortiGuard IOC Service ... 777
Working with FortiGuard Malware IPs ... 777
Working with FortiGuard Malware URLs ... 777
Working with Malware Patrol ... **778**
Configuring Malware Patrol Malware Domains ... 778
Configuring Malware Patrol Malware IPs ... 779
Configuring Malware Patrol Malware Hashes ... 779
Configuring Malware Patrol Malware URLs ... 780
Working with MISP Threatfeeds ... **782**
MISP Server Setup ... 782
Prerequisites ... 782
Limitation ... 782
Create API Key ... 783
FortiSIEM Setup ... 783
Malware IP Setup ... 783
Malware URL Setup ... 784
Malware Domain Setup ... 784

Malware Hash Setup 785
Working with OpenCTI Threatfeeds 786
OpenCTI Threatfeeds Setup 786
FortiSIEM Setup 788
Malware IP Setup 788
Malware URL Setup 789
Malware Domain Setup 789
Malware Hash Setup 790
Troubleshooting 791
Working with ThreatConnect IOCs 792
Download ThreatConnect Malware Domains 792
Download Other ThreatConnect IOCs 793
Specifying a Schedule 793
Malware Domains 794
Adding a Malware Domain 795
Modifying a Malware Domain 796
Deleting a Malware Domain 797
Importing Malware Domains 798
Custom Threat Feed Websites - CSV Data - One-time Manual Import 798
Custom Threat Feed Websites - CSV Data - Programmatic Import via Java 799
Custom Threat Feed Websites - Programmatic Import via Python 800
Viewing Malware Domains 801
Malware IPs 802
Adding a Malware IP 803
Modifying a Malware IP 804
Deleting a Malware IP 805
Importing Malware IPs 806
Prerequisites 806
Websites with Built-in Support 806
Custom Threat Feed Websites - CSV Data - One-time Manual Import 807
Custom Threat Feed Websites - CSV Data - Programmatic Import via Java 808
Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java 809
Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java 809
Custom Threat Feed Websites - Programmatic Import via Python 810
Viewing Malware IPs 811
Malware URLs 812
Adding a Malware URL 813
Modifying a Malware URL 814
Deleting a Malware URL 815
Importing Malware URLs 816
Prerequisites 816
Threat Feed Websites with Built-in Support 816

Custom Threat Feed Websites - CSV Data - One-time Manual Import 817
Custom Threat Feed Websites - CSV Data - Programmatic Import via Java 817
Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java818
Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java 819
Custom Threat Feed Websites - Programmatic Import via Python 819
Viewing Malware URLs 821
Malware Processes 822
Creating a Malware Process Group 823
Adding a Malware Process 824
Modifying a Malware Process 825
Deleting a Malware Process 826
Importing Malware Processes 827
Custom Threat Feed Websites - CSV Data - One-time Manual Import 827
Viewing Malware Processes 828
Country Groups 829
Creating a Country Group 830
Adding a Country Group 831
Modifying a Country Group 832
Deleting a Country Group 833
Changing the Home Country 834
Malware Hash 835
Adding a Malware Hash 836
Modifying a Malware Hash 837
Importing/Updating User-defined Malware Hash 838
Import from a CSV File 838
Custom Websites - CSV Data - One-time Manual Import 838
Update via API 839
Updating System Defined Malware Hash Group 839
Custom Threat Feed Websites - CSV Data - Programmatic Import via Java 840
Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java 841
Custom Threat Feed Websites - Non-CSV Data -STIX Formatted Data and TAXII Import via Java 841
Custom Threat Feed Websites - Programmatic Import via Python 842
Viewing Malware Hash 843
Default Password 844
Adding a Default Password 845
Modifying a Default Password 846
Importing and Exporting a Default Password 847
Importing Default Password 847
Exporting Default Password 847

Anonymity Network 848
Adding Anonymity Networks 849
Modifying Anonymity Networks 850
Updating Anonymity Networks 851
Import from a CSV File 851
Custom Websites - CSV Data - One-time Manual Import 851
Update via API 852
Websites with Built-in Support 852
Custom Websites - CSV Data - Programmatic Import 852
New Websites - Non-CSV Data - Programmatic Import 853
User Agents 854
Adding User Agents 855
Modifying User Agents 856
Importing and Exporting User Agents 857
Importing User Agents 857
Exporting User Agents 857
Remediations 858
Adding Remediations 859
Modifying Remediations 860
Deleting Remediations 861
Lookup Tables 862
Adding a Lookup Table 863
Deleting a Lookup Table 864
Working with Lookup Table Data 865
Adding Lookup Table Data 865
Deleting Lookup Table Data 865
Editing Lookup Table Data 866
Importing Lookup Table Data 866
Importing from a CSV File 866
Update via API 867
Import via Report 867
Import System Defined Lookup Table Data via Report 868

Playbooks 869
Viewing Playbooks 870
Updating Playbooks 871
Connectors 872
Viewing Connectors 873
Updating Connectors 874
Machine Learning Jobs 875
Viewing Machine Learning Jobs 876
Editing a Machine Learning Job 877
Deleting a Machine Learning Job 878
Osquery 879
Viewing osquery Templates 880
Creating Osquery Templates 881
Creating an osquery Template 881
Applying Changes to an osquery Template 881
Working with Cases 882
Creating a Case Manually 883
Step 1 - Configure an Email Server for Notifications 883
Step 2 - Create one or more FortiSIEM Analyst Teams 883
Step 3 - Create a Case Management Policy 885
Step 4 - Create a Case 886
Create a Case from an Incident 886
Add an Incident to an Existing Case 886
Create a Case from an Event 887
Add an Event to an Existing Case 887
Creating a Case Automatically 888
Step 1 - Configure an Email Server for Notifications 888
Step 2 - Create one or more FortiSIEM Analyst Teams 889
Step 3 - Create a Case Management Policy 890
Step 4 - Create Automation Policy 891
Viewing All Cases 893
Case Summary 893
Case Attributes 893
Viewing Specific Case Attributes 895
Searching Cases 896
Viewing a Case in Depth 897
Overview 897
Explore View 897
MITRE ATT&CK View 898
Investigate View 898
Case Notes 898
Case Evidence 899

Action History 900
Acting on a Case 901
Case Dashboard 903
Case Health Dashboard 903
Case KPI Dashboard 904
Case Handling Dashboard 904
Case Report 905
Steps to Update Case Escalation from 6.x-7.1.x to 7.2.x 907
Step 1 - Move or Create Prior Case Users to FortiAnalysts Groups 907
Step 2 - Update your Escalation Policy (now called a Case Management Policy) 907
Step 3 - Associate Case Management Policy with an Automation Policy 908
Working with Incidents 910
Overview View 911
List View 913
Viewing Incidents 913
List by Time View 914
List by Device View 920
List by Incident View 920
Acting on Incidents 920
Location View 920
Clearing Incidents 921
Actions 921
Searching Incidents 926
Searching Incidents 926
Searching for MITRE ATT&CK Incidents 927
Risk View 928
Pane Information 928
Left Pane for Device 928
Left Pane for User 929
Middle Pane For Device and User 929
Right Pane for Device 930
Right Pane for User 930
Explorer View 931
Using the Incident Explorer View 933
Filtering in the Incident Explorer View 933
MITRE ATT&CK® View 934
Rule Coverage View 934
ICS Attack (Tactic Categories) Table 934
IT Attack (Tactic Categories) Table 935
Using the Rule Coverage View 936
Searching Techniques in Rule Coverage View 937
Incident Coverage View 937
Using the Incident Coverage View 938
Searching Techniques in Incident Coverage View 941

Filtering in Incident Coverage View 941
MITRE ATT&CK Incident Explorer View 941
Using the MITRE ATT&CK Incident Explorer View 942
Filtering in the MITRE ATT&CK Incident Explorer View 942
Getting Detailed Information on an Incident 943
Displaying Triggering Events for an Incident 943
UEBA View 944
Incident Trend Chart 944
Attribute List 944
Related Incidents 945
Triggering Events 946
Filtering in the UEBA View 946
Investigating Incidents 947
Examining an Incident and Related Entities 947
Working with the Undirected Graph 950
Adding an Undirected Graph 950
Clearing an Undirected Graph 950
Fitting the Undirected Graph in Panel 951
Repositioning a Node 951
Repositioning the Undirected Graph 951
Zooming In/Out of the Undirected Graph 951
Automated Incident Resolution Recommendation 952
Lookups Via External Websites (e.g. VirusTotal) 953
Prerequisites 953
Performing an External Lookup on VirusTotal, RiskIQ, and/or FortiGuard 953
CVE-Based IPS False Positive Analysis 955
Requirements 955
False Positive Detection Logic 955
Running an IPS False Positive Test 956
Consequences of Running the IPS False Positive Test 957
Remediating an Incident using a Script 958
Overview 958
Requirements 959
How App Server Determines Enforce On and Run On Devices 960
Structure of a Remediation Script 960
Executing a Playbook on an Incident 962
Running a Connector on an Incident 963
Troubleshooting Incident Trigger 964
Working with Analytics Search 966
Overview 967
Running a Built-in Historical Search 968
Creating a New Search 969
Step 1 - Specify Search Filter 969

Specifying Event Keyword Based Filters ... 969
Specifying Event Attribute Based Filters ... 969
Specifying CMDB Attribute Based Filters from CMDB Reports ... 972
Step 2 - Specify Time Range ... 973
Step 3- Specify Trend Interval ... 973
Step 4 - Specify Event Source ... 974
Specify Maximum Number of Rows in the Result ... 974
Saving Filter Conditions ... 974
Step 5 - Specify Organizations for Service Provider Deployments ... 975
Step 6 - Specify Group By, Display Fields and Display Conditions ... 975
Creating a Nested Search ... 977
Outer CMDB Query, Inner Event Query ... 977
Step 1: Construct the Inner Event Query ... 977
Step 2: Construct the Outer CMDB Query by Referring to the Query in Step 1 ... 977
Outer Event Query, Inner Event Query ... 978
Step 1: Construct the Inner Event Query ... 978
Step 2: Construct the Outer Event Query ... 979
Outer Event Query, Inner CMDB Event Query ... 979
Step 1: Construct the Inner CMDB Query ... 979
Step 2: Construct the Outer Event Query ... 980
Viewing Real-time Search Results ... 981
Display Controls ... 981
Viewing Parsed Raw Events ... 981
Modifying Search Filter Criteria ... 982
Modifying Search Display Fields ... 982
Zooming-in on a Specific Time Window ... 982
Viewing Historical Search Results ... 983
Understanding Default Result Display ... 983
Choosing other Chart Displays ... 984
Viewing Parsed Raw Events ... 988
Modifying Search Filter Criteria ... 988
Modifying Search Display Fields ... 988
Zooming in on a Specific Time Window ... 988
Copying the Search to a Separate tab ... 989
Searches Using Pre-computed Results ... 990
Usage Notes ... 990
Setting Up Pre-computation ... 991
Impact of Organization and Roles ... 991
Viewing Pre-computed Results ... 992
Running a GUI Search on Pre-computed Results ... 993
Scheduling a Report Based on Pre-computed Results ... 994
Running a Report Bundle Based on Pre-computed Results ... 995
Scheduling a Report Bundle Based on Pre-computed Results ... 995

Working with Search Results ... **997**
Saving Search Definition and Results ... 997
Viewing / Deleting Saved Search Results ... 997
Exporting Search Results ... 998
Emailing Search Results ... 998
Creating a Rule ... 999
Saving Search Filter and Display Conditions ... 1000
Executing a FortiSOAR Playbook ... 1000
Running a FortiSOAR Connector ... 1001
Invoking FortiAI ... 1001
Creating a New Case ... 1002
Adding to an Existing Case ... 1003
Advanced Search ... **1004**
Overview ... **1005**
Running a Built-in Advanced Search ... **1006**
Running Advanced Search from Resources ... 1006
Running Advanced Search from Analytics ... 1006
Creating a New Advanced Search ... **1007**
General Usability Notes ... 1009
Query Performance Considerations ... 1009
Fixing Query Errors ... 1009
Fixing SQL Query Syntax Errors with FortiAI ... **1010**
Miscellaneous Advanced Search Operations ... **1011**
Saving Advanced Search Definition and/or Results ... 1011
Viewing Saved Advanced Search Results ... 1011
Exporting Search Results ... 1012
Importing and Exporting Advanced Search Definition ... 1012
Advanced Search Examples ... **1013**
Example 1 - Query Top 10 Reporting Devices by Event Count in Last 1 Hour ... 1013
Example 2 - Add the Reporting Vendor and Model of the Reporting Devices and the Last Time that They Reported an Event ... 1013
Example 3 - Show the Reporting IP and the Top Event Types for these Devices and only Include External Events ... 1014
Example 4 - Show the External Events from a Specific Reporting Device with a Specific IP ... 1015
Example 5 - Show Information from a Specific CMBD Group ... 1015
Example 6 - Show Reporting Devices Reporting External Events Today that were not Reporting External Events Yesterday ... 1016
Example 7 - Only Return Top 5 Event Types for Each Reporting Device ... 1017
Machine Learning ... **1018**
Overview ... **1019**
Anomaly Detection ... **1023**
Anomaly Detection Algorithms for Local Mode ... 1023

Running Anomaly Detection Local Mode 1027
Step 1: Design 1027
Step 2: Prepare Data 1027
Step 3: Train 1028
Step 4: Schedule 1029
Anomaly Detection Algorithms for AWS Mode 1030
Running Anomaly Detection AWS Mode 1030
Step 0: Set Up AWS 1030
Step 1: Design 1030
Step 2: Prepare Data 1031
Step 3: Train 1031
Step 4: Schedule 1032
Classification 1033
Classification Algorithms for Local Mode 1033
Running Classification Local Mode 1034
Step 1: Design 1034
Step 2: Prepare Data 1034
Step 3: Train 1035
Step 4: Schedule 1036
Classification Algorithms for Local Auto Mode 1036
Running Classification Local Auto Mode 1037
Classification Algorithms for AWS Mode 1037
Running Classification AWS Mode 1037
Step 0: Set Up AWS 1037
Step 1: Design 1037
Step 2: Prepare Data 1038
Step 3: Train 1038
Step 4: Schedule 1040
Classification Algorithms for AWS Auto Mode 1040
Running Classification AWS Auto Mode 1041
Clustering 1044
Clustering Algorithm for Local Mode 1044
Running Clustering Local Mode 1045
Step 1: Design 1045
Step 2: Prepare Data 1045
Step 3: Train 1046
Step 4: Schedule 1047
Clustering Algorithms for Local Auto Mode 1047
Running Clustering Local Auto Mode 1048
Clustering Algorithm for AWS Mode 1048
Running Clustering AWS Mode 1048
Step 0: Set Up AWS 1048
Step 1: Design 1048
Step 2: Prepare Data 1049
Step 3: Train 1049
Step 4: Schedule 1050

Forecasting ... **1052**
Forecasting Algorithms for Local Mode ... 1052
Running Forecasting Local Mode ... 1052
Step 1: Design ... 1052
Step 2: Prepare Data ... 1053
Step 3: Train ... 1053
Step 4: Schedule ... 1055
Regression ... **1056**
Regression Algorithms for Local Mode ... 1056
Running Regression Local Mode ... 1057
Step 1: Design ... 1057
Step 2: Prepare Data ... 1057
Step 3: Train ... 1058
Step 4: Schedule ... 1059
Regression Algorithms for Local Auto Mode ... 1060
Running Regression Local Auto Mode ... 1060
Regression Algorithms for AWS Mode ... 1060
Running Regression AWS Mode ... 1060
Step 0: Set Up AWS ... 1060
Step 1: Design ... 1060
Step 2: Prepare Data ... 1061
Step 3: Train ... 1062
Step 4: Schedule ... 1062
Regression Algorithms for AWS Auto Mode ... 1063
Running Regression AWS Auto Mode ... 1064
Working with Dashboards ... **1066**
General Operations ... **1067**
Viewing Built-in Dashboard Folders ... 1067
Displaying Only Dashboard Folders of Interest ... 1071
Setting a Home Dashboard Folder ... 1071
Creating a New Dashboard Folder ... 1072
Creating a New Dashboard Under a Folder ... 1072
Sharing Dashboard Folders ... 1072
Creating a Shared Dashboard ... 1073
Cloning a Shared Dashboard Folder ... 1073
Deleting a Dashboard ... 1074
Deleting a Dashboard Folder ... 1074
Starting Dashboard Slideshow ... 1074
Widget Dashboard ... **1076**
Creating a Widget Dashboard ... 1076
Data Source ... 1076
Populating a Widget Dashboard ... 1076
Modifying Widget Dashboard Layout ... 1076
Modifying Widget Information Display ... 1077
Searching in a Widget Dashboard ... 1077

Drill-down into a Widget 1078
Exporting Widget Dashboard Definition 1078
Importing a Widget Dashboard 1078
Forcing a Refresh 1078
Summary Dashboard 1079
Creating a Summary Dashboard 1079
Data Source 1079
Managing Devices in a Summary Dashboard 1079
Changing Display Columns 1080
Changing Refresh Interval 1080
Forcing a Refresh 1080
Searching a Summary Dashboard 1080
Business Service Dashboard 1081
Creating a Business Service Dashboard 1081
Data Source 1081
Adding/Removing Business Services to the Dashboard 1081
Summary View 1081
Drilldown View 1082
Filtering Summary View 1082
Filtering Drilldown View 1082
Changing Refresh Interval 1082
Forcing a Refresh 1082
Identity and Location Dashboard 1083
Data Source 1083
Adding to the Data Source 1084
Viewing Identity and Location Dashboard 1084
Searching for Specific Information 1085
Interface Usage Dashboard 1086
Data Source 1086
Adding/Removing Devices and Interfaces to the Dashboard 1088
Viewing Device Level Metrics 1089
Viewing Interface Level Metrics 1089
Viewing Application Usage 1089
Viewing QoS Statistics 1089
Drill-down from Widgets 1089
Modifying Widget Information Display 1089
Changing Refresh Interval 1090
Forcing a Refresh 1090
PCI Logging Status Dashboard 1091
Setting Up Data Source 1091
Creating a Dashboard 1095
Analyzing Dashboard Data 1095
Searching Dashboard Data 1095

Managing Tasks 1096
Requesting a De-anonymization Request 1096
Approving a De-anonymization Request 1096
FortiAI 1098
Overview 1098
OpenAI Integration and Disclaimer 1099
How to ask FortiAI to Create a Report 1100
Anonymizing Sensitive Data 1100
FortiAI GUI Interface 1101
Expand/Reduce Input Field Size 1101
Maximize/Minimize FortiAI Window 1101
FortiSIEM Manager 1102
FortiSIEM Manager Incidents 1103
FortiSIEM Manager Incidents Overview View 1104
FortiSIEM Manager Incidents - List View 1106
Viewing Incidents 1106
List by Time View 1107
List by Device View 1112
List by Incident View 1112
Acting on Incidents 1112
FortiSIEM Manager CMDB Users 1117
FortiSIEM Manager CMDB Adding Users 1118
FortiSIEM Manager - Editing User Information 1120
FortiSIEM Manager Resources 1121
FortiSIEM Manager Resources Rules 1122
Enable/Disable Rules 1122
Change Rule Severity 1122
FortiSIEM Manager Resources Connectors 1123
FortiSIEM Manager Resources Playbooks 1124
FortiSIEM Manager Resources - Event Types 1125
FortiSIEM Manager Admin 1126
FortiSIEM Manager Setup 1127
Add a FortiSIEM Instance 1127
Edit a FortiSIEM Instance 1128
Delete a FortiSIEM Instance 1128
Unregister a FortiSIEM Instance 1128
FortiSIEM Manager Health 1129
FortiSIEM Manager Cloud Health 1130
First Frame 1130
Second Frame 1131
FortiSIEM Back-End Processes 1132

FortiSIEM Manager Collector Health **1137**
Properties Associated with Collector Health 1137
Process Properties 1139
FortiSIEM Back-End Processes 1139
FortiSIEM Manager License **1141**
Appendix **1143**
Administrative Tools and Information **1144**
Adding Network Interfaces **1145**
Adding Interfaces for FortiSIEM Virtual Machine Based Deployments 1145
Step 1 – Modify VM Hardware Configuration on the Hypervisor 1145
Step 2 - Configure the Additional Interface on FortiSIEM 1145
Adding Interfaces for FortiSIEM Hardware Appliances 1147
Backing Up and Restoring Databases **1150**
Backing Up and Restoring CMDB 1150
CMDB Backup Procedure 1150
CMDB Restore Procedure 1151
Backing Up and Restoring EventDB 1151
EventDB Backup Procedure 1151
EventDB Restore Procedure 1151
Backing Up and Restoring SVN 1152
SVN Backup 1152
SVN Restore 1152
Creating and Restoring ESX Snapshots **1153**
Create FortiSIEM VM Snapshot 1153
Restoring FortiSIEM VM from Snapshot 1157
Exporting Events from FortiSIEM **1160**
phExportESEvent Tool 1160
phExportEvent Tool 1161
TestESSplitter Tool 1162
phClickHouseCSVExport Tool 1166
Importing Events into FortiSIEM **1168**
phClickHouseImport Tool 1168
Increasing Collector Event Buffer Size **1171**
Listing Event Attributes seen by Elasticsearch **1172**
listElasticEventAttributes.sh Tool 1172
Managing Events in EventDB **1173**
TestDBPurger Tool 1173
EnforceRetentionPolicy Tool 1174
TestSegmentReader Tool 1174
Managing FortiSIEM Operations **1175**
phstatus Tool 1175
phtools Tool 1175

ClickHouse Usage Notes ... **1177**
ClickHouse Index Design ... **1178**
ClickHouse Operational Overview ... **1179**
Shards and Replicas ... 1179
ClickHouse Related Processes ... 1179
Supervisor/Worker Nodes Running ClickHouse Functions ... 1180
ClickHouse Keeper Cluster Considerations ... 1181
Event Insertion Flow ... 1181
Event Replication Flow ... 1181
Query Flow ... 1181
ClickHouse Query Optimization Guidelines ... **1182**
Handling ClickHouse Node IP Change ... **1183**
Step 1: If Keeper node IP changed, then update ClickHouse Keeper registry file on all Keeper nodes to reflect the new IP address. ... 1183
Step 2: If Data/Query node IP changed, then update ClickHouse Keeper file on all ClickHouse Data/Query nodes. ... 1183
Step 3: If Keeper node IP changed, then update Redis key of ClickHouse Keeper node from Supervisor. ... 1184
Step 4: If Data/Query node IP changed, then update Redis key of ClickHouse Data/Query node. ... 1184
Step 5: If Data/Query node IP changed, then update interserver_http_host and cluster file on this node where the IP changed. ... 1185
Step 6: Test and Save from FortiSIEM GUI ... 1186
ClickHouse Backup and Restore Steps ... **1187**
Backup to Remote Server via SFTP ... 1187
Step 1: Prepare the SFTP server ... 1187
Step 2: SSH to FortiSIEM node and Copy the ClickHouse Backup Config File ... 1188
Step 3: Modify the ClickHouse Backup Config File ... 1189
Step 4: Add a Crontab Job to Run the Backup Task Daily ... 1190
Step 5: Monitor the /var/log/clickhouse-backup.log to Verify if the Backup Task Happens Correctly ... 1190
Step 6: Back up All Other Shards ... 1190
Restore from Remote SFTP Server ... 1191
Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File ... 1191
Step 2: Modify the ClickHouse Backup Config File ... 1192
Step 3: Drop Schema Objects, then Download and Restore Schema Only for the fsiem.events_replicated Table ... 1192
Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for the fsiem.events_replicated Table ... 1193
Step 5: Verify the Event Count in the FortiSIEM Setup ... 1193
Step 6: Restore Other Existing Shards ... 1193
Backup to AWS S3 ... 1194
Step 1: Prepare the S3, Modify its Permission Policy ... 1194
Step 2: SSH to FortiSIEM Node and Copy the ClickHouse Backup Config File ... 1195
Step 3: Modify the ClickHouse Backup Config File ... 1195
Step 4: Add a Crontab Job to Run the Backup Task Daily ... 1196

Step 5: Verify that the Backup Task is Happening Correctly 1197
Step 6: Back up All Other Existing Shards 1197
Restore from AWS S3 1197
Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File 1197
Step 2: Modify the ClickHouse Backup Config File 1198
Step 3: Drop Schema Objects, then Download and Restore Schema Only for fsiem.events_replicated Table 1199
Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for fsiem.events_replicated Table 1199
Step 5: Verify the Event Count in the FortiSIEM Setup 1199
Step 6: Restore All Other Shards 1200
Deleting ClickHouse Organization Data 1201
Rebalancing Shards 1202
Advanced Operations 1204
Adding a Disk or Tier 1204
Deleting a Disk 1205
Deleting a Storage Tier 1206
Moving a Worker from One Shard to Another Shard 1207
Replacing a Worker with another Worker (within the same Shard) 1208
Recovering from Complete Loss of ClickHouse Keeper Cluster 1209
Recovering from Losing Quorum in ClickHouse Keeper Cluster 1210
Recovering from Read-Only Mode 1210
Mitigating a Non-Responsive ClickHouse Keeper Node 1212
Migrating ClickHouse Events from FortiSIEM 6.5.x to 6.6.0 or Later 1213
Post-7.1.1 Upgrade ClickHouse IP Index Rebuilding 1214
Reference 1216
General Introduction 1216
Concepts and Architecture 1216
ClickHouse Keeper 1216
Performance Tuning 1216
Troubleshooting 1216
Configuration Notes 1217
Automated CMDB Disk Space Management 1218
Component Communication and Network Port Usage 1219
Configuring FortiSIEM Application Server for Proxy Connectivity 1220
Editing phoenix_config.txt File 1221
FortiSIEM Deployment Scenarios 1222
Enterprise Deployment 1222
Enterprise Deployments with Supervisor and no Collector 1222
Enterprise Deployment with Supervisor and Worker but no Collector 1222
Enterprise Deployments with Supervisor, Worker and Collector 1223
Service Provider Deployment 1224
Service Provider Deployment - Organizations with Dedicated Collector 1224

Service Provider Deployment - Organizations with Shared Multi-tenant Collector 1225
FortiSIEM OS Updates and Internet Connectivity 1228
Tuning PostgreSQL Configuration Parameters 1229
Important Configuration Parameters 1229
Additional Configuration Parameters 1230
Elasticsearch Usage Notes 1232
Configuring Elasticsearch Buffer 1233
Configuring Elasticsearch Timeout 1234
Dynamic Scripting Limits 1235
Elasticsearch Feature Compatibility 1237
Merging Small Elasticsearch Indices into a Big Index 1238
Steps 1238
Differences in Analytics Semantics between EventDB and Elasticsearch 1240
Issues 1240
Example 1 - Matching Event Types 1241
Example 2 - Matching Raw Messages 1241
Elasticsearch Support for Regex 1242
Elasticsearch Known Issues 1243
Examples of Custom Performance Monitors 1244
Custom JDBC Performance Monitor for a Custom Table 1245
Planning 1245
Adding New JDBC Performance Objects 1246
Associating Device Types to Performance Objects 1247
Testing the Performance Monitor 1248
Enabling the Performance Monitor 1248
Writing Queries for the Performance Metrics 1248
Custom SNMP Monitor for D-Link Interface Network Statistics 1249
Planning 1249
Adding the D-Link SNMP Performance Object 1251
Associating Device Types to Performance Objects 1252
Testing the Performance Monitor 1253
Enabling the Performance Monitor 1253
Writing Queries for the Performance Metrics 1253
Custom JMX Monitor for IBM Websphere 1254
Planning 1254
Adding New IBM WebSphere Performance Objects 1255
Associating Device Types to Performance Objects 1257
Testing the Performance Monitor 1258
Enabling the Performance Monitor 1258
Writing Queries for the Performance Metrics 1259
Custom SNMP Monitor for D-Link HostName and SysUpTime 1259
Planning 1259
Adding the D-Link SNMP Performance Object 1261

Associating Device Types to Performance Objects 1261
Testing the Performance Monitor 1262
Enabling the Performance Monitor 1262
Writing Queries for the Performance Metrics 1262
Custom WMI Monitor for Windows Domain and Physical Registry 1263
Planning 1263
Adding the Microsoft Windows WMI Performance Object 1264
Associating Device Types to Performance Objects 1265
Testing the Performance Monitor 1266
Enabling the Performance Monitor 1266
Writing Queries for the Performance Metrics 1266
Exporting QRadar Logs to FortiSIEM 1267
Overview 1267
Prerequisites 1268
Resource Considerations 1268
Planning the Export 1268
Export Procedure 1269
Step 1: Generate QRadar API Key for Log Export 1270
Step 2: Configure QRadar Payload Truncation of Raw Logs 1270
Step 3: Set up API Upload Credential in FortiSIEM Collector 1270
Step 4: Run Export Script 1271
Step 5: Confirm Ingested Data in FortiSIEM 1274
Export Procedure for Service Provider Deployments 1275
Validating Events Ingested 1275
FortiEMS Endpoint Tagging 1277
Overview 1277
Updated Remediation Scripts 1277
Fortinet FortiEMS (Endpoint Management Server) Discovery Setup 1278
FortiEMS Configuration 1278
FortiSIEM Configuration 1279
Best Practice Setup 1280
Additional Information on Automatically Tagging a Host 1282
Example Scenario 1283
Scheduling Automatic Tagging Example 1283
GUI Notes 1286
Flash to HTML5 GUI Mapping 1287
Dashboard 1287
Analytics 1290
Incidents 1290
CMDB 1291
Admin 1291
FortiSIEM Charts and Views 1294
FortiSOAR Integration Notes 1299
Configuring FortiSOAR for FortiSIEM Integration 1300
Set Up Authentication 1300

Writing FortiSIEM Compatible FortiSOAR Playbooks **1302**
Introduction 1302
Prerequisites 1302
Playbooks and Connectors 1302
Jinja and its Use in Playbooks 1303
Building Custom Playbooks 1306
Sample Incident JSON 1306
Sample Event JSON 1308
Sample Attribute Names 1309
Custom Playbook Requirements – API Endpoint Specification 1309
FortiSIEM Prebuilt Playbooks 1310
Content Pack Playbooks 1310
Reference Playbooks 1311
Playbook Tagging 1311
Formatting Playbook Result Data back to FortiSIEM 1311
FortiSIEM Special Playbook Response Variables 1311
References 1314
Functions in Analytics **1315**
Aggregation Functions 1315
AVG Function 1316
COUNT Function 1317
COUNT DISTINCT Function 1318
FIRST Function 1318
LAST Function 1319
MAX Function 1320
MEDIAN Function 1321
MIN Function 1322
MODE Function 1323
PctChange Function 1324
Pctile95 Function 1325
PCTILE Function 1325
STDDEV Function 1326
SUM Function 1327
VARIANCE Function 1328
CMDB Lookup Function 1329
DeviceToCMDBAttr Function 1329
Conversion Functions 1330
LOG Function 1331
TO_DOUBLE Function 1331
TO_INTEGER Function 1332
TO_STRING Function 1333
Date Conversion Functions 1333
DayOfWeek Function 1334
HourOfDay Function 1334
Evaluate and Set Function 1335
IF Function 1335
Extraction Function 1336

EXTRACT Function 1336
Lookup Table Functions 1337
LookupTableGet Function 1337
LookupTableHas Function 1338
String Manipulation Functions 1339
LEN Function 1340
LTRIM Function 1340
REPLACE Function 1341
RTRIM Function 1342
SUB_STR Function 1342
TO_LOWER Function 1343
TO_UPPER Function 1344
TRIM Function 1344
Time Window Functions 1345
EMA Function 1345
SMA Function 1347
Knowledge Base 1349
FortiSIEM Event Attribute to CEF Key Mapping 1350
FortiSIEM Event Categories and Handling 1354
Public Domain Built-in Rules 1355
License Enforcement 1402
CMDB Device License Enforcement 1402
Agent License Enforcement 1402
EPS License Enforcement 1403
Events 1403
Raw Event Size Based License Enforcement 1405
Parser Specification 1406
General Parsing Patterns 1406
Event Format Recognizer Specification 1408
Parsing Instructions 1410
Built-in Patterns 1415
Event Log Patterns 1415
FQDN Pattern 1416
Network Patterns 1416
Time Patterns 1416
Type Patterns 1417
Built-in Functions 1418
Collect and Set Functions 1419
collectFieldsByRegex 1419
collectFieldsByKeyValuePair 1420
collectAndSetAttrByKeyValuePair 1421
collectAndSetAttrByKeyValuePairMultiValue 1422
collectAndSetAttrByPos 1423
collectAndSetAttrByPosWithQuotes 1424
collectAndSetAttrByPosWithNestedSep 1425

collectFieldsByCsvFile 1426
collectFieldsByCsvValue 1427
collectFieldsBySNMPTrap 1428
collectAndSetAttrBySymbol 1429
collectAndSetAttrByXPath 1430
collectFieldsByXPath 1431
collectAndSetAttrFromAnotherEvent 1432
collectAndSetAttrByJSON 1433
collectAndSetAttrByJsonArray 1434
collectAndSetAttrByJsonSymbol 1435
collectAndSetAttrByRegex (Deprecated) 1436
collectAndSetAttrByKeyValPair (Deprecated) 1436
Compute Functions 1437
add 1437
calculateDomainEntropy 1438
calculateLatency 1438
compIntfSecVal 1439
combineMsgId 1439
compare 1440
decodeBase64 1441
decodeHex 1441
divide 1442
normalizeMAC 1443
resolveDNSName 1443
scale 1444
shiftTimeSec 1445
swap 1445
unzip 1446
URLDecode 1446
Conversion Functions 1448
calculateMSec 1448
calculateSec 1449
convertHexStrToInt 1449
convertIpDecimalToStr 1450
convertStrToIntIpPort 1450
convertStrToIntIpProto 1451
toLower 1452
toUpper 1452
toDateTime 1453
toUnixTime 1455
convertHexStrToStr (Deprecated) 1456
convertHostNameToIp (Deprecated) 1456
Extraction Functions 1457
extractHostFromFQDN 1457

getEventSeverityFromSyslogPriority 1458
DeviceToCMDBAttr 1458
extractHostFromURL 1459
String Functions 1460
replaceStringByRegex 1460
replaceStrInStr 1461
splitJsonEvent 1461
trimAttribute 1464
Python Threat Feed Framework 1466
Threat Feed Workflow 1468
Internal/Scheduled by FortiSIEM Execution Scenario: 1468
External Execution Scenario: 1469
Threatfeed Module 1469
Directory Structure 1470
Overview of Threat Feed Integrations 1470
Data Object Classes 1470
Important Member Variables of the ThreatfeedIntegration Class 1473
Important Member Functions of the ThreatfeedIntegration Class 1474
Instructions on Creating a New Python Integration 1474
Python Script 1474
Save Imported Data to Database 1476
Performance Considerations 1476
Public APIs 1477
Import API 1477
Delete API 1479
Notes about Threat Feed Authentication 1480
Installing New Python Packages 1480
Sample Windows Agent Logs 1481
Certificate Monitoring Logs 1481
Certificate Added 1481
Certificate Removed 1482
Certificate Expired 1482
Certificate Expiring 1482
System Logs 1483
System Logs generated by pre-7.1.4 Windows Agent 1483
System Logs generated by 7.1.4 and later Windows Agent 1483
Sysmon Logs 1484
Sysmon Logs generated by pre-7.1.4 Windows Agent 1484
Sysmon Logs generated by 7.1.4 and later Windows Agent 1485
PowerShell Logs 1486
PowerShell Logs generated by pre-7.1.4 Windows Agent 1486
PowerShell Logs generated by 7.1.4 and later Windows Agent 1486
Application Logs 1488
Application Logs generated by pre-7.1.4 Windows Agent 1488
Application Logs generated by 7.1.4 and later Windows Agent 1488
Security Logs 1489

Security Logs generated by pre-7.1.4 Windows Agent 1489
Security Logs generated by 7.1.4 and later Windows Agent 1489
Security Logs in French Windows generated by pre-7.1.4 Windows Agent 1490
Security Logs in French Windows generated by 7.1.4 and later Windows Agent 1490
DNS Logs 1491
DNS System Logs generated by pre-7.1.4 Windows Agent 1491
DNS System Logs generated by 7.1.4 and later Windows Agent 1491
DHCP Logs 1492
IIS Logs 1493
DFS Logs 1494
File Content Monitoring Logs 1494
File Integrity Monitoring Logs 1495
Use Case 1: File or Directory Created 1495
Use Case 2: File or Directory Deleted 1496
Use Case 3: File Content Modified 1497
Use Case 4: File Content Modified and Upload is Selected 1497
Use Case 5: File Renamed 1498
Use Case 6: File Permission Changed 1499
Use Case 7: File Ownership Changed 1500
Use Case 8: File Archive Bit Changed 1501
Use Case 9: File Baseline Changed 1502
Installed Software Logs 1502
Registry Change Logs 1503
Removeable Media Monitoring Logs 1503
WMI Logs 1504
UEBA Information 1505
Comparing UEBA Sources 1506
Windows UEBA vs Log Based UEBA 1506
UEBA Rules Trigger Based on Log Source 1508
UEBA Based on Log 1512
Windows Security logs 1512
Windows Sysmon 1512
Linux Agent 1512
UEBA Sample Logs 1513
Windows Agent System Variables 1514

Overview

FortiSIEM is an advanced Security Information and Event Management (SIEM) solution that combines advanced log and traffic analysis with performance/availability monitoring, change analysis, and accurate knowledge of the infrastructure to provide accurate threat detection, remediation, incident response and compliance reporting.

FortiSIEM can be deployed as a hardware appliance, a virtual appliance, or as a cluster of virtual appliances to scale-out to large infrastructure deployments.

Scale-Out Architecture

FortiSIEM scales seamlessly from small enterprises to large and geographically distributed enterprises and service providers.

For smaller deployments, FortiSIEM can be deployed as a single all-in-one hardware or virtual appliance that contains full functionality of the product. The virtual appliance can run on most common hypervisors including VMware ESX, Microsoft Hyper-V, and RedHat KVM, and can be deployed on premise or in Amazon AWS Cloud. For larger environments needing greater event handling throughput and storage, FortiSIEM can be deployed in cluster mode. There are three types of FortiSIEM nodes – Collector, Worker and Supervisor.

Collectors are used to scale data collection from various geo-separated network environments potentially behind a firewall. Collectors communicate to the devices, collect the data, parse the data, and send it to the Worker nodes over a compressed secure HTTP(S) channel. Supervisor and Worker nodes reside inside the data center and perform data analysis functions using distributed co-operative algorithms. For scalable event storage, FortiSIEM provides two solutions – FortiSIEM NoSQL event database with data residing on a NFS Server and Elasticsearch.

As compute or storage needs grow, you can add Collector nodes, Worker nodes, disks on the NFS server and Elasticsearch Data Nodes.

FortiSIEM also provides Windows Agents that enable log collection from a large number of Windows Servers. Windows Agents can be configured to send events to Collectors in a highly available load balanced manner.

Multi-tenancy

FortiSIEM allows you to manage multiple groups of devices and users (Organizations) within a single FortiSIEM installation. Devices and IP addresses can overlap between Organizations. FortiSIEM provides strict logical separation between organizations at the application layer. Users of one Organization cannot see another Organization's data including devices, users and logs. Users belonging to a Manage Service Provider Organization can see all Organizations.

Infrastructure Discovery and Automated CMDB

For complete situational awareness, the user needs to know the network and server infrastructure in depth. FortiSIEM's inbuilt discovery engine can explore an IT infrastructure (on premise and cloud, physical and virtual), discover and categorize network devices, servers, users and applications in

depth. A wide range of information is discovered including hardware information, serial numbers and licenses, installed software, running applications and services, and device configurations. Some special topological relationships can be discovered, for example - WLAN Access Points to WLAN Controllers, and VMware guests to physical hosts. This rich information populates an integrated configuration management database (CMDB), which is kept up to date through scheduled rediscoveries.

A novel aspect of FortiSIEM discovery is that the system automatically discovers what can be monitored and which log can be pulled using the provided credentials. This approach reduces human error, since FortiSIEM autonomously learns the true network configuration state.

High Performance Log Collection and Flexible Parsing

FortiSIEM has a flexible distributed log collection and parsing architecture. For logs pushed to FortiSIEM (such as Syslog), devices can load balance the logs across various Workers or Collectors. For logs pulled by FortiSIEM (such as Windows WMI or Cloud services via REST API), the pulling functionality is automatically load balanced across Workers and Collectors. Logs are immediately parsed at the point at which they are received. This distributed processing speeds up log collection and analysis.

FortiSIEM has a patented XML based log parsing language that is both flexible and computationally efficient. Flexibility comes from the fact that users can easily write their own parsers (XML files) or edit system provided ones using the FortiSIEM GUI. The parser XML files are compiled at run-time and executed as an efficient code. This makes log parsing very efficient, almost as efficient as writing code in native programming languages.

Performance and Availability Monitoring

Zero-day malware can create performance issues on a server, for example, malware can consume large memory, or ransomware scanning and encrypting files can slow the performance of other applications. By shutting down certain services and creating excessive network traffic, malware can cause availability issues. To properly detect and remediate security issues, an investigator needs to know the performance and availability trends of critical infrastructure services. Powered by its discovery capabilities, FortiSIEM can seamlessly collect a rich variety of performance and availability metrics to help the investigator hunt for threats. FortiSIEM can also alert users when it receives metrics outside a normal profile, correlating such violations with security issues to create high fidelity alerts.

Network Configuration and File Integrity Monitoring

Unauthorized or inadvertent changes to key system configuration files (such as httpd.conf) or router/firewall configuration can lead to security issues. Malware can modify key system files. Bad actors (for example, insider threats) can steal forbidden files. It is important to maintain control of key files and directories.

FortiSIEM provides mechanisms for tracking and detecting key file changes. It can monitor start-up and running configuration of network devices via SSH. It can monitor configuration files on servers. FortiSIEM agents can efficiently monitor large server infrastructures. An alert is created when a file changes from one version to another or deviates from a blessed hardened configuration.

Custom Device and Application Support

While FortiSIEM provides turnkey support for a large number of devices and applications, users can build their own full-fledged support from the GUI. System log parsers, performance monitors, and configuration change detectors can be modified. New device and application types, performance monitors, and configurations change detectors can be defined, and new log parsers can be integrated to work with FortiSIEM.

User Identity and Location Tracking

By combining DHCP logs, VPN logs, WLAN logs, and Domain Controller logon events, FortiSIEM is able to maintain an audit trail for IP address to user and geo-location mappings over time. While IP address to User mapping is important for look-up purposes by its own right, this feature enables FortiSIEM to detect stolen credentials as they tend to get used from distant locations over a short period of time.

External Threat Intelligence Integration

External websites can provide cyber threat information in terms of:

- Malware IP
- Malware Domain
- Malware hash
- Malware URL
- Anonymity Networks

FortiSIEM has a flexible framework to connect to a wide variety of threat sources (both free and paid), efficiently downloading this information and find matches in real-time in the environment it is running. Some threat sources can have a large number (millions) of bad IPs and URLs. FortiSIEM's distributed search and rule engines find matches with such large sets of data at a very high event rate.

Distributed Event Correlation and Threat Detection – the Rule Engine

FortiSIEM has a distributed event correlation engine that can detect complex threats in near real-time. Threats are users or machine behavioral anomalies and can be specified in terms of event patterns sequenced over time. A threat can be alternatively looked at as a SQL query evaluated in a streaming mode. FortiSIEM has an inbuilt profiling engine that can handle threats defined using statistical thresholds, using mean and standard deviation.

What makes the FortiSIEM rule engine powerful is (a) the ability to include any data in a rule, for example: performance and change metrics along with security logs, (b) distributed in-memory computation (patent-pending) involving Supervisor and Worker nodes for near real-time performance with high event rates, (c) the ability for a rule to generate a dynamic watch list which can be used recursively in a new rule to create a nested rule hierarchy, (d) use of CMDB Objects in Rule definition, and (e) unified XML based language for rules and reports which makes it easy to convert a report into a rule and vice-versa.

Several machine learning based UEBA models are part of the FortiSIEM inbuilt rule library – (a) detection of simultaneous logins from two different countries, (b) detection of simultaneous logins from two improbable geo-locations, (c) login behavior anomaly – logins to servers at times that one does not typically log on, etc., (d) detection of traffic to dynamically generated domains.

FortiSIEM has a large number of in-built behavioral anomaly rules that work out of the box, but can also be adapted by the user for their own environment. A framework is provided where the user can write new rules via the GUI, test them with real events, and then deploy in the system.

Device and User Risk Scoring

By combining with asset criticality, user role and importance, incident severity, frequency of occurrence and vulnerabilities found, FortiSIEM assigns a risk score to users and machines. This score is displayed in a dashboard with drill-down capabilities to identify the underlying factors.

Incident Response and Mitigation

FortiSIEM provides a number of mitigation scripts that can run an action when an incident happens. The scripts can be invoked automatically when an incident happens or can be invoked on-demand. Some examples include blocking an IP or a MAC, deactivating a user from active directory, removing an infected file, putting a user into a watch list, restarting a process or rebooting a server, and so on. You can also write your own mitigation scripts and deploy on a running system.

Search, Threat Hunting, Compliance Reports and Dashboards

FortiSIEM provides a flexible and unified search framework. The user can search data based on keywords or in a structured way using FortiSIEM parsed attributes. In real-time mode, the matched data streaming in from devices is displayed. In Historical mode, events in the event database are searched. Supervisor and Worker nodes perform search in a distributed manner.

A large number of inbuilt reports (search templates) are provided, based on the device type, and functionality, such as availability, performance, change and security.

Two novel aspects of FortiSIEM search are event unification and drill-down or threat hunting capabilities. With event unification, all data is analyzed and presented the same way, whether it is presentation aspects (real-time search, reports, rules) or context (performance and availability metrics, change events or security logs). Using drill-down, you can start from a specific context, such as Top Authentication Failed Users, and select attributes to further analyze data and iteratively, get to the root cause of a problem. As an example, the investigation of 'Top Authentication Failed users' could be followed by picking a specific user from the list and selecting Destination IP, and Ports to see which machines the user communicated with, followed by selecting the raw logs for real evidence.

FortiSIEM contains a wide selection of compliance reports out of the box – PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13, SANS Critical Control, NIST800-53, and NIST800-171.

FortiSIEM provides a wide variety of visual dashboards for the data it collects and for incidents that have triggered - Summary dashboards, Widget dashboards, Business Service dashboard, Incident dashboard, and Identity and Location dashboard.

Internal Ticketing System and Two-way Third-party Ticketing Integration

FortiSIEM has a built-in ticketing system for managing incidents via tickets. It supports the full ticket life cycle of opening, escalating, closing, reopening and creating cases with attachments for evidence.

FortiSIEM can also integrate with third-party ticketing systems. When an incident occurs in FortiSIEM, a ticket can be created in the external ticketing system and linked to an existing device or a new device can be created in the external system. You can customize various FortiSIEM incident fields to the

external ticketing system field. When the ticket is closed in the external ticketing system, the ticket is closed in FortiSIEM.

Several third-party external ticketing systems are supported out of the box, for example, ServiceNow, Salesforce, ConnectWise and Remedy. An API is provided so that other integrations can be built.

Business Service Analytics

Business Service enables you to prioritize incidents and view performance/availability metrics from a business service perspective. A Business Service is defined within FortiSIEM as a smart container of relevant devices and applications serving a common business purpose. Once defined, all monitoring and analysis are presented from a business service perspective.

FortiSIEM enables you to easily define and maintain a Business Service. Since FortiSIEM automatically discovers the applications running on the servers as well as the network connectivity and the traffic flow, you can easily choose the applications and respective servers and be intelligently guided to choose the rest of components of the Business Service.

FortiSIEM Releases

The following sections provide release specific information about new features, enhancements, and resolved issues:

- What's New in 7.2.2
- What's New in 7.2.1
- What's New in 7.2.0
- What's New in 7.1.9
- What's New in 7.1.8
- What's New in 7.1.7
- What's New in 7.1.6
- What's New in 7.1.5
- What's New in 7.1.4
- What's New in 7.1.3
- What's New in 7.1.2
- What's New in 7.1.1
- What's New in 7.1.0
- What's New in 7.0.4
- What's New in 7.0.3
- What's New in 7.0.2
- What's New in 7.0.1
- What's New in 7.0.0

What's New in 7.2.2

This release contains the following features, enhancements, and bug fixes.

- New Features
- Enhancements
- Bug Fixes
- Implementation Notes

New Features

- Raw Event Size based Licensing
- Exporting QRadar Logs to FortiSIEM

Raw Event Size based Licensing

This release supports a new licensing scheme for on-premises VM based deployments. License is based on:

- Total Raw event size per day (GB/Day)
- Number of Agents
- Number of UEBA Agents
- FortiGuard IOC

Important Notes:

1. The user is allowed to have 11 violations in a rolling 30-day window. After that, the **Analytics** and **Dashboard** pages are disabled for 1 day.
2. In this license scheme, users can have as many devices and events per second (EPS) as can be supported by their deployed hardware, without violating the Total Raw event size per day (GB/Day) limits.
3. If a device was **Unmanaged** because of the previous device and EPS-based license, then after applying the new GB/Day license, the user must re-discover the device as **Managed** for these devices to become managed.
4. To apply this new license type, the user must get a new license from FortiCare and upload that license to FortiSIEM Supervisor, following the same normal license procedure.

Exporting QRadar Logs to FortiSIEM

This release provides a script that can be used to export logs from IBM QRadar SIEM to FortiSIEM. The script connects to the QRadar SIEM via API on port 443 and collects raw logs along with the Reporting Device IP or Host Name and the time at which the log was received in QRadar. The script then sends the logs to a FortiSIEM Collector via HTTPS POST. The Collector parses the logs as if they were directly received from the external device and stores them in FortiSIEM.

For details see here.

Enhancements

- Dashboard Query Optimization (for ClickHouse)
- Rocky Linux Update

Dashboard Query Optimization (for ClickHouse)

In current releases, every time a user visits a Dashboard, for ClickHouse, Elasticsearch and EventDB based deployments, a separate query is run for each report in that dashboard. This may result in too many queries being submitted to the event database.

This release provides an optimization for ClickHouse based deployments. Query results are cached for a duration and users visiting a dashboard are shown the cached query results (if available). Caching duration is set by the refresh interval defined for a Dashboard report. In this release, the minimum refresh interval is set to 5 minutes.

The following queries are not cached:

1. CMDB Report Queries
2. Absolute Time Range Queries

Rocky Linux Update

This release updates FortiSIEM OS to Rocky Linux OS 8.10 and includes fixes and enhancements until July 15, 2024. Details can be found at https://rockylinux.org/news/rocky-linux-8-10-ga-release. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include Rocky Linux 8.10. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

Bug Fixes

The following issues are resolved.

Bug ID	Severity	Module	Description
1052724	Major	App Server	LDAP Re-discovery will remove externally authenticated users from FortiSIEM Analysts Group.
1063551	Minor	App Server	For an external authentication user, FortiSIEM role is not enforced correctly after upgrade to 7.1.7 or higher.
1059078	Minor	App Server	CMDB report using custom user defined properties does not work.
1059053	Minor	App Server	Rule sync error happens for user defined rule involving lookup table.
1056534	Minor	App Server	HTTP Incident notification delivery obfuscates raw events in XML automatically.
1054941	Minor	App Server	SQL query statement is incorrectly escaped in Performance Object Definition page.
1052883	Minor	App Server	PostgreSQL may throw shared memory error if there are Incidents over 1 year.
1051271	Minor	App Server	Failed to export CMDB report 'Rules with Exceptions' to both PDF and CSV.
1050861	Minor	App Server	Skip invalid data types from being added as an IOC to a malware list.
1047662	Minor	App Server	Upgrade overwrites user modified Rule Severity.
1045942	Minor	App Server	Parenthesis in filter not saved correctly in report/rules.
1045541	Minor	App Server	Cannot use special characters in Host Name field on CMDB Group Definition page (Admin > Settings > Discovery > CMDB Groups).
1013450	Minor	App Server	PAYG Report throws array out of bounds on report completion.
921322	Minor	App Server	Unable to configure FortiGuard Connectivity via Proxy without FortiGuard IOC License.

Bug ID	Severity	Module	Description
1037081	Minor	ClickHouse	Need to slow down ClickHouse insertion attempts when ClickHouse insertion fails. Otherwise, too many ClickHouse data parts may be generated, and the table may become read only.
1032484	Minor	ClickHouse Backend	Retry interval for ClickHouse data insertion failure is too short.
1059077	Minor	Data Work	The Rule "Uncommon Windows process via Sysmon" definition is incorrect with respect to LookupTable mappings.
1043134	Minor	Data Work	Notification Action Time in GitHubWebhooksJson event is not parsed correctly.
883182	Minor	Data Work	FortiSIEM FortiEDR Dashboard doesn't display information correctly.
1038259	Minor	Discovery	Discovery of large vCenter environment failing for 19k + assets.
1047317	Minor	Event Pulling Agents	Oracle DB Service name is not inserted into event when events are being pulled.
1038661	Minor	Event Pulling Agents	Mimecast support: Update argument in SIEM API; reduce logging and better error handling.
1055340	Minor	Generative AI	Sometimes, temporary files created by Generative AI may not be cleaned up and lead to /opt becoming full.
1047666	Minor	Generative AI	phGenerativeAI doesn't start in closed environment (without access to Internet).
1053453,1053095	Minor	GUI	GUI does not show Rule Incident Attributes: COUNT (Matched Events), COUNT(DISTINCT <attribute>).
1042605	Minor	GUI	Should not create a risk for a malware Domain.
1055926	Minor	GUI	Editing the Worker during EventDB to ClickHouse migration and saving the configuration throws an invalid IPV4 address error.
1054050	Minor	GUI	After software upgrade, GUI should show a pending content update if true.

Bug ID	Severity	Module	Description
1036286	Minor	GUI	Unable to save any modification in Active Directory if the user belongs to more than one LDAP group.
1030444	Minor	GUI	FortiSOAR Block IP Address Connector is missing IP address & Address group field.
1063250	Minor	Linux Agent	Linux Agent sends empty device id after restart.
1035413	Minor	REST API	For Public REST API query at /phoenix/rest/agentStatus/all, the value LastEventReceiveTime always shows 0.
1055964	Minor	Threat Intel Integration	Python STIX2.1 Threatfeed can sometimes fail if invalid ip/url/domain object is encountered.
1053245	Minor	Upgrade	Upgrade script needs to be more exact while referencing fsiem.summary table.
1049788	Minor	Upgrade	Upgrade from 6.6.4/6.7.8 failed due to 'Unknown storage policy `fsiem_storage_policy`'.
1047472	Minor	Upgrade	During upgrade, connection to ClickHouseKeeper could be lost resulting in ClickHouse database upgrade failure.
1047414	Minor	Upgrade	Upgrade from 6.7.3 to 7.2.1 failed due to 'Coordination error: Connection loss'.
1043635	Minor	Upgrade	Content Update resets to base version when upgrading between any minor version. Workaround is to immediately do a content update to the latest on the current software version.
1053996	Enhancement	App Server	Incident Queries issued by QueryMaster may be slow when there are a lot of incident partition tables.
1047969	Enhancement	ClickHouse Backend	Do not restart ClickHouse after certain configuration changes.
1053391	Enhancement	Data Work	WinOSXMLParser needs update for Event IDs 4720 & 4738.
1050300	Enhancement	Data Work	Update Oracle DB parser to parse serviceName.
1044846	Enhancement	Data Work	IOC Rules missing for CertPL Malware Domains.

Bug ID	Severity	Module	Description
1044798	Enhancement	Data work	Some FortiGate Events are missing Event Type Groups.
1040767	Enhancement	Data Work	Update VMWare VCenter Parser and VMEventParser.
1040765	Enhancement	Data Work	Add Dell Unity and Dell PowerShell Custom Parsers for Authentication Events.
1039612	Enhancement	Data Work	Update Carbon Black CEF Parser.
1033866	Enhancement	Data Work	Update FortiPAM Parser.
1023114	Enhancement	Data Work	Need a parser for FortiGate Events From SASE.
1022941	Enhancement	Data Work	Update Cisco ACI log support.
1022371	Enhancement	Data Work	Update Trend Vision One CEF event support.
1045499	Enhancement	Event Pulling Agents	Support additional date format YYYY-MM-DD hh:mm:ss in Generic Poller to support ServiceNow event pulling.
1037893	Enhancement	Event Pulling Agents	Tenable Security Center Integration requires additional API to fetch CVSS scores.
1029563	Enhancement	GUI, Query	Improved Dashboard Query Management for ClickHouse.
1027612	Enhancement	Machine Learning	Add data normalization for all ML algorithms as a standard pre-processing step.
1044001	Enhancement	New Feature	Enhancement - Provide a HTTP POST based method to import QRadar logs into FortiSIEM.
1028322	Enhancement	Remediation	Develop FortiEDR Remediation via API to Quarantine a host.
1012778	Enhancement	System	Change pgdump from gzip to pigz for multi-CPU zip processing.

Implementation Notes

- PostGreSQL Related
- Collector HA Related
- Identity and Location Related

- Post-Upgrade ClickHouse IP Index Rebuilding

PostGreSQL Related

FortiSIEM 7.2.2 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.2.2, then the patch is included and there is nothing to do.
- If you have upgraded to FortiSIEM 7.1.5 or later, then the patch is included and there is nothing to do.
- If you want to remain on FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

```
curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe
```

Collector HA Related

1. If you have FortiSIEM Windows/Linux Agents reporting through Collectors and you decide to form a HA Collector Group with those Collectors, then you need to add all the Collectors in the HA Group to **Admin > Setup > Windows Agent > Host to Template Associations** and click **Apply**.
2. If you add a new Collector to an existing HA Collector Group, then the new Collector must be added as a Follower.
3. If a Collector is part of High Availability (HA) Cluster and you want to delete the Collector, then follow these procedures.

   Case 1: If the Collector is a Follower, then follow these steps:
   a. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
   b. Click **Save**.
   c. Delete the Collector from CMDB.

   Case 2: If the Collector is a Leader, then follow these steps:
   a. Make the Collector a Follower Cluster in **Admin > Settings > System > Cluster Config**.
   b. Click **Save**.
   c. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
   d. Click **Save**.
   e. Delete the Collector from CMDB.
4. Collector High Availability (HA) Failover Triggers:
   - Logs are sent to a VIP in VRRP based Failover - In this case, when VRRP detects node failure, then Follower becomes a Leader and owns the VIP and events are sent to the new Leader. If a process is down on a node, then VRRP may not trigger a Failover.

- Logs sent to Load Balancer - In this case, the Load balancing algorithm detects logs being sent to a different Collector. If a process is down on a node, then Failover may not trigger.
- For event pulling and performance monitoring, App Server redistributes the jobs from a Collector if App Server failed to receive a task request in a 10 minute window.

Identity and Location Related

If you are upgrading to 7.2.2, then please update the following entry in the `/opt/phoenix/config/identityDef.xml` file in Supervisor and Workers to get Identity and location entries populated for Microsoft Office365 events. Then restart `IdentityWorker` and `IdentityMaster` processes on Supervisor and Workers.

Pre-7.2.2 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded</eventType>
     <eventAttributes>
        <eventAttribute name="userId" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude" reqd="no"/>
     </eventAttributes>
  </identityEvent>
```

7.2.2 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded,MS_OFFICE365_EntraID_UserLoggedIn,MS_
OFFICE365_EntraID_StsLogon_UserLoggedIn</eventType>
     <eventAttributes>
        <eventAttribute name="user" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude" reqd="no"/>
     </eventAttributes>
  </identityEvent>
```

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.2.2, then after upgrading to 7.2.2, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.2.0, or 7.2.1 and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

What's New in 7.2.1

This release contains the following bug fixes and known issues.

- Bug Fixes
- Important Considerations
- Implementation Notes and Known Issues

Bug Fixes

The following issues are resolved.

Bug ID	Severity	Module	Description
1047223	Major	App Server	If multiple Windows agents are associated with a template, the template will disappear if any one of the agents is uninstalled.
1046931	Major	App Server	Case formation by aggregating incidents may fail if one Incident Title is very long.
1046177	Major	App Server	(Service Provider Deployments) Appsvr does not correctly evaluate automation policy conditions, resulting in incorrect Incident notifications.
1047238, 1040908	Minor	App Server	Analytics query with custom attribute shows Invalid query XML error due to duplicates custom event attributes.
1043296	Minor	App Server	Fail to export Incident when Incident Detail values are null.
1040907	Minor	App Server	App Server error may happen during incident resolution inference processing if there are no new Incidents during a time period.
1039294	Minor	App Server	In Admin > Settings > Discovery > CMDB Group, the IP range in a policy does not handle CIDR (e.g. 172.30.56.1/22), IP ranges such as 172.30.56.1-172.30.56.3, 172.30.56.1,172.30.56.2,172.30.56.3.
1040422	Minor	Data work	Windows XML parser does not parse user correctly in Security Event 4624.
1016469	Minor	Data work	Sometimes Event Pulling API error logs may not be parsed correctly by FortiSIEM, the parsed event type and event name are 5830.
1026325	Minor	GUI	TypeError on console when navigating to Admin > Device Support > Parsers.

Bug ID	Severity	Module	Description
1034648	Minor	Rule	The Detection rule 'Windows: Active Directory User Backdoors' has incorrect logic.
1041837	Minor	System	Many Python IOC threatfeed scripts do not parse the datetime correctly.
1037398	Minor	Windows Agent	Sometimes Windows Agents show 'Disconnected' after power cycle.
1037186	Minor	Windows Agent	Double quotes are missing for some attributes in the AO-WUA-InstSw-Removed event.
1038780	Enhancement	App Server	Validate custId parameters for Watchlist Summary REST API: /phoenix/rest/watchlist/all/summary.
1038267	Enhancement	App Server	Add POST body validation for REST AI agentStatus/v2/all API.
1039113	Enhancement	Data work	Create outbreak rules and reports for Check Point Quantum Security Gateways Information Disclosure Attack.
1037028	Enhancement	Data work	Create outbreak rules and reports for D-link Multiple Devices Attack.
1035123	Enhancement	Data work	Improve FortiAuthenticator Parser to capture real src IP from msg section of log.
1033867	Enhancement	Data work	Support Hashicorp Vault via Syslog.
1029606	Enhancement	Data work	Create a separate FortiSandbox phishing detection rule.
1029289	Enhancement	Data work	Need to get rid of the double quotes from user when parsing the NetScreen event.
1029153	Enhancement	Data work	Enhance FortiNDR Parser to include On Prem missing fields.

Bug ID	Severity	Module	Description
1028529	Enhancement	Data work	WinOSWmiParser does not parse msg field on Security EventID 364.
1035107	Enhancement	GUI	Too much blank space in the Exported Report in PDF format, when there are no charts in the report template.
1033132	Enhancement	Performance Monitoring	Support Citrix SD-WAN link status monitoring via SNMP.

Important Considerations

- PostGreSQL v13.14 Update
- Post-Upgrade ClickHouse IP Index Rebuilding

PostGreSQL v13.14 Update

FortiSIEM 7.2.1 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.2.1, then the patch is included and there is nothing to do.
- If you have upgraded to FortiSIEM 7.1.5 or later then the patch is included and there is nothing to do.
- If you want to remain on FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

```
curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe
```

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.2.1, then after upgrading to 7.2.1, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6, 7.1.7, or 7.2.0 and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

Implementation Notes and Known Issues

1. If you have FortiSIEM Windows/Linux Agents reporting through Collectors and you decide to form a HA Collector Group with those Collectors, then you need to add all the Collectors in the HA Group to **Admin > Setup > Windows Agent > Host to Template Associations** and click **Apply**.
2. If you add a new Collector to an existing HA Collector Group, then the new Collector must be added as a Follower.
3. If you are upgrading to 7.2.1, then please update the following entry in the `/opt/phoenix/config/identityDef.xml` file in Supervisor and Workers to get Identity and location entries populated for Microsoft Office365 events. Then restart `IdentityWorker` and `IdentityMaster` processes on Supervisor and Workers.

   Pre-7.2.1 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded</eventType>
     <eventAttributes>
        <eventAttribute name="userId" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude"
reqd="no"/>
     </eventAttributes>
  </identityEvent>
```

   7.2.1 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded,MS_OFFICE365_EntraID_
UserLoggedIn,MS_OFFICE365_EntraID_StsLogon_UserLoggedIn</eventType>
     <eventAttributes>
        <eventAttribute name="user" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude"
reqd="no"/>
     </eventAttributes>
```

```
</identityEvent>
```

4. If a Collector is part of High Availability (HA) Cluster and you want to delete the Collector, then follow these procedures.

   Case 1: If the Collector is a Follower, then follow these steps:

   a. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
   b. Click **Save**.
   c. Delete the Collector from CMDB.

   Case 2: If the Collector is a Leader, then follow these steps:

   a. Make the Collector a Follower Cluster in **Admin > Settings > System > Cluster Config**.
   b. Click **Save**.
   c. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
   d. Click **Save**.
   e. Delete the Collector from CMDB.

5. Collector High Availability (HA) Failover Triggers:
   - Logs are sent to a VIP in VRRP based Failover - In this case, when VRRP detects node failure, then Follower becomes a Leader and owns the VIP and events are sent to the new Leader. If a process is down on a node, then VRRP may not trigger a Failover.
   - Logs sent to Load Balancer - In this case, the Load balancing algorithm detects logs being sent to a different Collector. If a process is down on a node, then Failover may not trigger.
   - For event pulling and performance monitoring, App Server redistributes the jobs from a Collector if App Server failed to receive a task request in a 10 minute window.

What's New in 7.2.0

This release contains the following features, enhancements, device support and bug fixes.

- New Features
- Key Enhancements
- External Log Source Integration
- Bug Fixes
- Important Considerations
- Implementation Notes and Known Issues

New Features

- Automated Case Management
- Collector High Availability
- Search Field Analytics
- Custom SIGMA Rule Import

Automated Case Management

In FortiSIEM, administrator can create a Case consisting of one or more incidents and assign the Case to a user to resolve the case. Currently the Case creation and assignment process is manual. This release provides an option to automate this process.

Automated Case Management involves the following steps:

1. **Create Analyst Teams** under **CMDB > Users**. Each Team has a Team Lead, a Team Queue along with FortiSIEM users as team members. Work schedule and Time off schedule can be defined for each team member.
2. **Create Case Management Policy Templates** under **Admin > Settings > Case Management**. A policy involves specifying the following aspects:
   - SLA Violation and Escalation policy
   - Auto-assignment policy
   - Case Change Notifications policy
   - Case Change Permissions policy
   - Case Auto Close policy
3. **Create one or more Case Assignment Policies** under **Admin > Settings > Automation Policy**. A Case Assignment Policy determines how the Case should be assigned and managed. A policy involves specifying a Condition and an Action.

- A Case Assignment Policy **Condition** is specified in terms of Incident Severity, Rule Name, Time Range, Affected Items, Affected Orgs (for Service Provider deployments).
- A Case Assignment Policy **Action** specifies a Case Management Policy and an ordered list of Teams.

Automated Case Creation and Assignment works as follows: When an Incident triggers, FortiSIEM will attempt to find an existing Open Case with matching IP address or host name. If found, then the Incident is simply added to that Case. Otherwise, FortiSIEM goes through the list of Case Assignment Policy Conditions **in rank order** looking for a match. If a match is found, then a new Case is created:

- An Assignee is found from the list of Teams in the matching Case Management Policy.
- Subsequently, the Case is managed following the Case Assignment Policy templates.

A Case can also be created manually as follows:

1. **Create Analyst Teams** under **CMDB > Users**.
2. **Create Case Management Policy Templates** under **Admin > Settings > Case Management**. The Auto-Assignment rules do not need to be specified.
3. Pick an Incident and create a Case or assign to an existing Case. The Assignee needs to be chose from the Analyst team and a Case Management Policy Template should be chosen, but is optional. During the assignment process, the list of related Incidents is provided to help the user to group related incidents into one Case.

All Cases can be viewed in **Cases > List View**. Each Case has a Drill Down View that includes Explore Dashboard, Investigation Dashboard and MITRE ATT&CK Dashboard specific for the Incidents included in this Case.

Cases > Overview provides 3 dashboards to view Overall Case Health, Case KPIs, Case Handling Statistics.

Other features include:

- In User Profile > UI Settings, user can customize the Case Home page.
- Audit events prefixed by PH_AUDIT_CASE with System Event Category = 2, which can be seen from **Resources > Event Types** by searching for PH_AUDIT_CASE.
- CMDB Reports to report on Case Progress, e.g. all cases that are open for more than 15 days.
- Ability to export and import a Case.
- Ability to create a Case from events only.
- Use FortiAI (previously Fortinet Advisor) to analyze a Case and add the analysis to Case Comments.

See here for details.

Collector High Availability

A FortiSIEM Collector plays the critical role of communicating with the end devices and Cloud Services for collecting logs and performance monitoring metrics, configurations, and other data. Currently if a Collector goes down, then:

- Logs sent to this Collector need to be manually resent to another Collector unless there is a Load Balancer in front.
- Events being pulled by Collector stops, until a new Collector is onboarded, and discovery is repeated to create an event pulling job for the new Collector.

This release adds the ability to deploy Collectors in *High Availability* mode – this enables Collector data collection to continue uninterrupted even when a Collector fails. This feature works differently in these environments:

- Case 1 - On premise and AWS deployments via VRRP
- Case 2 – On Azure and GCP deployments via Load Balancer

Case 1: On premise and AWS deployments via VRRP

If your Collectors are deployed on On-premise hypervisors, or on AWS, or they are hardware appliances, then High Availability (HA) is enabled via Virtual Router Redundancy Protocol (VRRP). A Collector HA Cluster needs to be created with one Leader and one or more Followers and a Virtual IP (VIP) that is always owned by the Leader.

During normal operations:

- Logs sent to the VIP are handled by the Leader Collector (which owns the VIP).
- FortiSIEM Supervisor node *distributes* event pulling and performance monitoring jobs among all Collectors in the Cluster.

If the Leader Collector goes down:

- The Follower node with highest priority will become the Leader and own the VIP. No human intervention is needed.
- Logs previously sent to the (failed) Leader Collector will automatically reach the new Leader Collector.
- FortiSIEM Supervisor node will automatically *re-distribute* event pulling and performance monitoring jobs previously assigned to the failed Leader Collector, to other Collectors in the HA Cluster.

If a Follower Collector goes down:

- App Server will distribute event pulling and performance monitoring jobs assigned to the failed Collector to other Collectors in the HA Cluster.
- If a failed Collector comes back up, then it will stay a Follower, but the event pulling jobs will be re-distributed among all the working Collectors in the HA Cluster.

Failure and Recovery:

- If the Leader Collector goes down then the Follower with the highest priority takes over. If the Leader Collector comes back up, then it will resume the Leader role due to its higher priority.
- If a Follower Collector goes down, the Leader will continue to operate. If the Follower comes back up, then it will remain a Follower while the Leader is operational.

Case 2: On Azure and GCP deployments via Load Balancer

If your Collectors are deployed on Azure or GCP, then High Availability is achieved via Load balancing mechanisms. A Collector HA Cluster needs to be created with a Load Balancer in front of the Collectors. The disadvantage of this approach is that the Customer needs to deploy a Load Balancer. However,

During normal operations:

- Logs sent to the Load Balancer are distributed among the Collectors in the Cluster.
- FortiSIEM Supervisor node *distributes* event pulling and performance monitoring jobs among all Collectors in the Cluster.

If a Collector goes down, then:

- Load Balancer will skip the failed Collector and distribute logs among other Collectors.
- FortiSIEM Supervisor node will automatically re-distribute event pulling and performance monitoring jobs previously assigned to the failed Collector, to other Collectors in the Cluster.

Defining the Collector Cluster is here, and for AWS, here.

Steps to set up Load Balancer in Azure are here, and for GCP, here.

Search Field Analytics

When an Analytics Search result spans multiple pages, it is difficult to know the values and their frequency for a Query result field, without scrolling multiple pages.

In this release, the Top and Bottom 100 values for each display field (other than Date fields and Raw Event Log, see instructions for more information on some exceptions) are shown in a separate left pane next to the Query result. User can also select one or more values and see the related search results and the trends for selected values. This feature enables the user to quickly sharpen the Search results for creating effective rules and reports.

This feature is available for ClickHouse based deployments only. Instructions on how to use this feature is here.

Custom SIGMA Rule Import

FortiSIEM already includes many SIGMA security rules as described here. However, the SIGMA rules change frequently. This release enables you to import a new SIGMA rule from the FortiSIEM GUI. FortiSIEM will automatically convert the SIGMA rule format to FortiSIEM Rule format. It is always advisable to check the correctness of the imported rule and test the rule before deploying.

You can import in one of 3 ways:

- By providing the URL for the SIGMA Rule.
- By uploading a SIGMA Rule file.
- By typing in a rule in SIGMA YAML file format as specified here.

Instructions on how to import a SIGMA Rule is here.

Key Enhancements

- Rocky Linux Update
- Enhanced Host and User Risk Scoring
- Increase Non-aggregated Search Result limit up to 1 Million (ClickHouse only)
- Enable FortiSIEM 500G Hardware Appliance to run as a ClickHouse Keeper
- GUI Improvements
- FortiAI (previously Fortinet Advisor) Improvements

- Support for 34 Additional External Threat Intelligence Sources
- Miscellaneous Enhancements

Rocky Linux Update

This release updates FortiSIEM OS to Rocky Linux OS 8.10 and includes fixes and enhancements until May 30, 2024. Details can be found at https://rockylinux.org/news/rocky-linux-8-10-ga-release. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include Rocky Linux 8.10. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

Enhanced Host and User Risk Scoring

The current Risk scoring framework is enhanced by including Incident Rarity, which captures how often an incident happens in the network. Rare incidents contribute more towards the risk score than frequent incidents. Other factors in the Risk score are Incident Severity, Incident Resolution and Asset Criticality.

Both Device and Host Risk Scores are calculated and displayed in the GUI when a host and user information are displayed. Case Risk score is shown in the Cases page. A Risk explanation is also provided. The **Incidents > Risk** page is also updated to show this information.

Increase Non-aggregated Search Result limit up to 1 Million (ClickHouse only)

Currently, up to 100K results can be displayed in the GUI and exported as CSV files. This limit is increased to 1 million for ClickHouse based deployments. This feature needs at least 32GB of RAM in Supervisor.

Enable FortiSIEM 500G Hardware Appliance to run as a ClickHouse Keeper

Currently, only FortiSIEM 2000F, 2000G, 2200G, 3500F, 3500G, and 3600G hardware appliances can be run as a Worker node and deployed as ClickHouse Keeper. These appliances have a large amount of storage and compute resources that a ClickHouse Keeper node does not need. This release enables you to deploy a FortiSIEM 500G hardware appliance as a stand-alone ClickHouse Keeper node.

To do this, install FortiSIEM 500G appliance as a FortiSIEM Worker node and add to ClickHouse Keeper cluster.

GUI Improvements

This release provides several GUI improvements:

- Vertical Slide in for CMDB pages.
- Threat Analysis tab on the Incident detail slide in . This includes automated analysis of an IOC (IP, Domain, URL, Hash) based on External Threat Intel sources, including FortiGuard IOC Lookup, VirusTotal, configured Resources > Malware IP/Domain/URL/Hash, FortiSIEM Incidents, Watch Lists, Fortinet GeoDB and Whois Information.
- Risk Score display for Hosts and Users throughout the GUI.
- Threat Analysis Result display throughout GUI for IP, Domain, URL and Hash fields.
- Redesigned Risk page.
- Improved PDF Reports – charts and tables.
- Fortinet Advisor - Ability to clear old conversations and show anonymized OpenAI requests *before* sending out to OpenAI.
- Allow Osquery execution from CMDB and add a device filter on the Resources Osquery section.

FortiAI (previously Fortinet Advisor) Improvements

This release provides more use cases to use Generative AI to respond to the following SOC questions:

- Get Incidents involving specific IP, host, user, domain in the last 1 day.
- Tell me what you know about a specific IP, host, user, domain.
- What is the health of specific IP, host, user based on Incidents seen in the last 1 day
- Elaborate on Incident <*id*> and give me details about the entities involved.
- Get more details about a CVE ID.
- Are there are any logs or Incidents related to a specific CVE in my environment?

Support for 34 Additional External Threat Intelligence Sources

IP Threat Feeds:

1. Blocklist DE - https://lists.blocklist.de/lists/all.txt
2. C2 Tracker - https://raw.githubusercontent.com/montysecurity/C2-Tracker/main/data/all.txt
3. CINS Score blacklist - https://cinsscore.com/list/ci-badguys.txt
4. Cisco Talos blacklist - http://www.talosintelligence.com/documents/ip-blacklist
5. Firehol Github based feed - https://raw.githubusercontent.com/ktsaou/blocklist-ipsets/master/firehol_level1.netset
6. Greensnow blocklist - https://blocklist.greensnow.co/greensnow.txt
7. IPSum threat Intelligence - https://raw.githubusercontent.com/stamparm/ipsum/master/ipsum.txt
8. Proofpoint compromised IP - https://rules.emergingthreats.net/blockrules/compromised-ips.txt
9. Snort IP blocklist - https://snort.org/downloads/ip-block-list

10. Abuse.ch Botnet C2 IP Blacklist - https://sslbl.abuse.ch/blacklist/sslipblacklist.txt
11. DigitalSide Threat-Intel IPs - https://osint.digitalside.it/Threat-Intel/lists/latesturls.txt
12. MISP IP threat feed
13. FortiSOAR IP threat feed
14. OpenCTI Threat Intel framework via STIXV2
15. FortiRecon Malware IP

URL Threat Feeds:

1. OpenPhish threat URLs - https://openphish.com/feed.txt
2. Abuse.ch - https://threatfox.abuse.ch/export/csv/urls/recent/
3. Tweetfeed.live IOCs shared by the infosec community at Twitter
   a. (Today) https://raw.githubusercontent.com/0xDanielLopez/TweetFeed/master/today.csv
   b. (Last week) https://raw.githubusercontent.com/0xDanielLopez/TweetFeed/master/week.csv
4. DigitalSide Threat-Intel URLs - https://osint.digitalside.it/Threat-Intel/lists/latesturls.txt
5. MISP URL threat feed
6. FortiSOAR URL threat feed
7. OpenCTI Threat Intel framework via STIXV2
8. FortiRecon Malware URL

Domain Threat Feeds:

1. Cert.PL Phishing Domains - https://hole.cert.pl/domains/domains.csv
2. DigitalSide Threat-Intel DNS - https://osint.digitalside.it/Threat-Intel/lists/latestdomains.txt
3. MISP Domain threat feed
4. FortiSOAR Domain threat feed
5. OpenCTI Threat Intel framework via STIXV2
6. FortiRecon Malware Domain

Hash Threat Feeds:

1. Abuse.ch SHA256 hashes - https://bazaar.abuse.ch/export/txt/sha256/recent/
2. MISP Hash threat feed
3. FortiSOAR Hash threat feed
4. OpenCTI Threat Intel framework via STIXV2
5. FortiRecon Malware Hash

Miscellaneous Enhancements

- API
- Rules and Reports

API

1. REST API `/phoenix/rest/watchlist/all/summary` to list all Watchlist IDs
2. REST API `/phoenix/rest/agentStatus/v2/all` to return all agent status

Rules and Reports

Changes to Rules and Reports from FortiSIEM 7.1.0 to FortiSIEM 7.2.0 are provided as .csv files

See here for rule changes.

See here for report changes.

External Log Source Integration

1. Generic Support for Webhooks for importing logs. Earlier releases would accept only webhooks with basic authentication using a strict set of POST parameters. This release expands to a generic solution. Any application or SaaS product that supports push events/notifications via Webhooks can utilize this method to send data to FortiSIEM. See here.
2. Updated GitHub support using Webhook. See here.
3. Updated GitLab support using Webhook. See here.
4. Updated Atlassian Beacon support using Webhook. See here.
5. Akamai Support. See here.
6. Mimecast API Support. See here.
7. MS SQL Server 2022 Support. See here.
8. Eliminate the need for SNMP/WMI/OMI for JDBC Monitoring
9. Update Sysmon to v14.13
10. New reports for GCP VM and Firewall related events
    a. GCP: Set Machine Type
    b. GCP: Set Tag Activity
    c. GCP: VM Start Activity
    d. GCP: VM Stop Activity
    e. GCP: Firewall Allowed Traffic Details
    f. GCP: Firewall Denied Traffic Details
11. FortiPAM Device Support. See here.

Bug Fixes

This release includes all the bug fixes for 7.1.6. In addition, the following issues are resolved.

Bug ID	Severity	Module	Description
1029792	Minor	App Server	OpenCTI Threat Feed integration via STIX/TAXII is not working.
1012458	Minor	App Server	After disabling Disaster Recovery in (High Availability + Disaster Recovery) environment, the Secondary node would show duplicated Supervisor node in Admin > Cloud Health.
979524	Minor	App Server	LDAP Discovery missing certain groups in certain AD environment.
876788	Minor	App Server	Data obfuscation of custom attribute results in errors in Analytics page.
906336	Minor	Data Manager	Online Data Display sometimes shows multiple Supervisors.
1034161	Minor	Data work	For 4625 and 4771 windows security events, - -success and -failure gets appended to event type.
1033622	Minor	Data work	Report Bundle may not always show same results as Adhoc Reports from Analytics page.
1005257	Minor	Data work	One FortiGate Event (logid="0103020300") fails to be parsed.
1004458	Minor	Data work	Rule '\Office365: Mailbox SendAs or SendOnBehalf has occurred' not functioning as intended.
999336	Minor	Data work	Windows event 4740 parsing is case-sensitive. Some unusual windows server condition results in log channel values being in lower case rather than pascal case.
995788	Minor	Data work	Rule 'Successful Windows Dormant Account Logon' does not trigger.
993844	Minor	Data work	Rule 'Windows: External Remote SMB Logon from Public IP' triggered by server's own IPv6 address.
991684	Minor	Data work	Ransomware detected rule triggers falsely during Windows Update.
987200	Minor	Data work	"Threat Detection" event types from CiscoAMPStream fail to parse due to bp_data field having a very long value.
982483	Minor	Data work	FortiWeb event name does not match with FortiWeb log message reference id 10000017 and 11005901.

Bug ID	Severity	Module	Description
992462	Minor	Discovery	Onboarding Oracle Acme Packet Controller scz9.1.0 device via SSH fails with “Wrong Protocol Data”.
982101	Minor	Discovery	FGT recompute security posture report is not always returned as FortiSIEM requests this data to be generated every time.
985943	Minor	Event Pulling Agents	JDBC event pulling times out error for large tables.
1002849	Minor	GUI	[ClickHouse] Online Data displayed starting 1 day before the oldest data available in ClickHouse DB.
995861	Minor	GUI	Baseline rules > Step 3: Incident definition shows attribute type mismatch.
995642	Minor	GUI	Incident Title allows to save '.' even when incident definition is backed out and rule is resaved.
991653	Minor	GUI	Subpattern filter is disabled when viewing Incident details - Triggering Events tab for the first time.
976014	Minor	Parser	SFLOW packets not parsed because of unsupported BCM counter type and IPv6.
989058	Minor	Performance Monitoring	Checkpoint FW Network Interface Monitoring does not support with Real Interfaces.
932787	Minor	Performance Monitoring	In Synthetic Transaction Monitoring, HTTP type doesn't work for the response codes 3xx, 4xx, and 5xx.
818860	Minor	Performance Monitoring	Net Intf Stat missing for Cisco ASR 1000 switch.
1002448	Minor	phMonitor	phMonitor crashes when file permission for httpd.conf differs than what is expected.
954599	Minor	Query	LookupTableGet is missed in Group BY in Query XML when it is Before Last(Event Receive Time).
954731	Minor	Rule	Global constraint using simple function in rule is not working properly.
1010184	Minor	System	Unused events_non_replicated table may prevent ClickHouse from restarting - this table should be cleaned up.
938659	Minor	System	Worker upgrade may fail when Supervisor's license is renewed, but workers had expired license.
1016411	Enhancement	App Server	Deleting CMDB Device is slow.

Bug ID	Severity	Module	Description
1008053	Enhancement	App Server	HTTP to HTTPS redirect exposing URLs along with http protocol/method in access logs.
995771	Enhancement	App Server	Org admin user cannot change the report logo from Settings > UI.
970039	Enhancement	App Server	For Disaster recovery, monitor Secondary Supervisor health from Primary Supervisor GUI.
1011352	Enhancement	Data work	Fail to parse Dell Nseries switches Raw Events.
1008784	Enhancement	Data work	Cyxtera Parser - events are being parser as unknown.
1004260	Enhancement	Data work	FortiDeceptor eventFormatRecognizer does not pickup the devid for VMs.
1002977	Enhancement	Data work	Some Unix logs not recognized.
990592	Enhancement	Data work	Parser Update for RSAAuthenticationServerParser.
989000	Enhancement	Data work	Some Aruba ClearPass Policy Manager events not parsed.
988034	Enhancement	Data work	Some Cisco FirePower threat defence events are not parsed.
987122	Enhancement	Data work	Cisco Firepower Management Center events not parsed.
987108	Enhancement	Data work	Some of the events received from Palo Alto Firewall are not parsed.
984778	Enhancement	Data work	Logs received from FortiDeceptor through FAZ on FortiSIEM are showing as 'Unknown_EventType'.
978121	Enhancement	Data work	Parser Enhancements required for Cisco Firepower Defense Parser.
959604	Enhancement	Data work	Some TippingPoint SMS Events failing to be parsed.
952101	Enhancement	Data work	Added parser and event types for Microsoft Graph List Risky Users API.
927787	Enhancement	Discovery	Discovering FortiGate using DNS first name resolution will set hostname to _gateway if the FortiGate is the default gateway of discovery node.
1006187	Enhancement	Event Pulling Agents	Enable API token for GitHub Device Support.
572554	Enhancement	Event Pulling Agents	Easily support defining AWS CloudWatch multiple log streams by enabling wildcards in the logStream field of the AWS CloudWatch credential.

Bug ID	Severity	Module	Description
1030134	Enhancement	GUI	Rules with numbers as sub-pattern names causes rule editing problems for the target rule.
1000173	Enhancement	GUI	Increase the font size of table and chart legends in PDF reports.
997065	Enhancement	GUI	User scope rules do not contain a hyperlink to the MITRE technique like system scope rules have.
992653	Enhancement	GUI	Disable the ability to modify User Idle Timeout. Currently hard coded to 15 minutes for Security purposes.
992253	Enhancement	GUI	When adding an Incident to a Closed Case, show error message and ask user to reopen the Case first.
973026	Enhancement	GUI	PG_WAL file size monitoring needs to be added to Health > Replication health.
969929	Enhancement	GUI	After configuring AWS S3 archive, tell user to go to Admin > Settings > Database > ClickHouse Config and click Test and Deploy.
696734	Enhancement	GUI	Allow Import/Export and Bulk Delete of Resources > Networks.
987571	Enhancement	Parser	Parse the Group Security ID in Windows Security Event 4732 and 4728.
1008125	Enhancement	Query	Unable to use Expressions inside LookupTable functions.
1007180	Enhancement	Query	Unable to query TO_LOWER / TO_UPPER / REPLACE(user) IN/NOT IN CMDB_GROUP.
960316	Enhancement	Query	Remove the log 'Summary data missing attribute custId' as there is no impact.
995155	Enhancement	System	Elasticsearch To ClickHouse Conversion tool: Enhance phExportESEventToClickHouse to provide a --retentionDays option.
938676	Enhancement	System	Provide a very clear, actionable error message when download upgrade image fails on collector.
1017189	Enhancement	Windows Agent	For Windows User log file monitoring, Wildcard is not supported for system files.

Important Considerations

- PostGreSQL v13.14 Update
- Post-Upgrade ClickHouse IP Index Rebuilding

PostGreSQL v13.14 Update

FortiSIEM 7.2.0 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.2, then the patch is included and there is nothing to do.
- If you are upgrading to FortiSIEM 7.2, then the patch is included and there is nothing to do.
- If you want to remain on FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

```
curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe
```

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.2.0, then after upgrading to 7.2.0, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, 7.1.5 or 7.1.6, and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

Implementation Notes and Known Issues

1. For Service Provider deployments, Automation Policies (formerly known as Notification policy) may be executed for incidents that do not meet the policy definition.

   If using Service Provider mode, **before newly deploying or upgrading, please contact support to obtain the necessary patch**. If FortiSIEM has already been newly deployed or upgraded to FortiSIEM 7.2.0, please contact support to apply the patch as soon as possible.
2. If you have FortiSIEM Windows/Linux Agents reporting through Collectors and you decide to form a HA Collector Group with those Collectors, then you need to add all the Collectors in the HA Group to **Admin > Setup > Windows Agent > Host to Template Associations** and click **Apply**.
3. If you add a new Collector to an existing HA Collector Group, then the new Collector must be added as a Follower.

4. In **Admin > Settings > Discovery > CMDB Groups**, when you create a new mapping definition, the **IP Range** field currently only handles a single IP address.
5. If you are upgrading to 7.2.0, then please update the following entry in the `/opt/phoenix/config/identityDef.xml` file in Supervisor and Workers to get Identity and location entries populated for Microsoft Office365 events. Then restart `IdentityWorker` and `IdentityMaster` processes on Supervisor and Workers.

   Pre-7.2.0 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded</eventType>
     <eventAttributes>
        <eventAttribute name="userId" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude"
reqd="no"/>
     </eventAttributes>
  </identityEvent>
```

   7.2.0 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded,MS_OFFICE365_EntraID_
UserLoggedIn,MS_OFFICE365_EntraID_StsLogon_UserLoggedIn</eventType>
     <eventAttributes>
        <eventAttribute name="user" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude"
reqd="no"/>
     </eventAttributes>
  </identityEvent>
```

6. If a Collector is part of High Availability (HA) Cluster and you want to delete the Collector, then follow these procedures.

   Case 1: if the Collector is a Follower, then follow these steps:

   a. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
   b. Click **Save**.

c. Delete the Collector from CMDB.

Case 2: if the Collector is a Leader, then follow these steps:

a. Make the Collector a Follower Cluster in **Admin > Settings > System > Cluster Config**.
b. Click **Save**.
c. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
d. Click **Save**.
e. Delete the Collector from CMDB.

7. Collector High Availability (HA) Failover Triggers:
   - Logs are sent to a VIP in VRRP based Failover - In this case, when VRRP detects node failure, then Follower becomes a Leader and owns the VIP and events are sent to the new Leader. If a process is down on a node, then VRRP may not trigger a Failover.
   - Logs sent to Load Balancer - In this case, the Load balancing algorithm detects logs being sent to a different Collector. If a process is down on a node, then Failover may not trigger.
   - For event pulling and performance monitoring, App Server redistributes the jobs from a Collector if App Server failed to receive a task request in a 10 minute window.

What's New in 7.1.9

This release contains the following bug fixes and enhancements.

- System Update
- Linux Agent Update
- Bug Fixes and Enhancements
- Implementation Notes

System Update

This release includes Rocky Linux OS 8.10 patches until October 22, 2025. Details can be found at https://rockylinux.org/news/rocky-linux-8-10-ga-release. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include Rocky Linux 8.10. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

Linux Agent Update

This release updates the Linux Agent code signing certificate.

Bug Fixes and Enhancements

This release fixes the following bug:

Bug ID	Severity	Module	Description
1206464	Minor	System	"configFSM.sh" run failed on Hardware Appliances during re-installation.

Implementation Notes

- PostGreSQL Related
- Post-Upgrade ClickHouse IP Index Rebuilding
- Upgrade Related

PostGreSQL Related

FortiSIEM 7.1.9 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.1.9, then the patch is included and there is nothing to do.
- If you are upgrading to FortiSIEM 7.1.9, then the patch is included and there is nothing to do.
- If you want to remain on a version of FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.1.9, then after upgrading to 7.1.9, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6, 7.1.7 or 7.1.8, and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

Upgrade Related

You may encounter a blank Global Dashboard after upgrading to 7.1.9. There are two workarounds.

1. If you have not upgraded yet, then run the script `updateDashboard.sh` as root on Supervisor before upgrade. You can upgrade after running the script.
2. If you have upgraded to 7.1.9 and then see a blank Global Dashboard, then run the script `updateImportDashboard.sh` as root on Supervisor.

What's New in 7.1.8

This release contains the following bug fixes and enhancements.

- System Update
- Bug Fixes and Enhancements
- Implementation Notes

System Update

This release includes Rocky Linux OS 8.10 patches until March 17, 2025. Details can be found at https://rockylinux.org/news/rocky-linux-8-10-ga-release. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include Rocky Linux 8.10. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
1077901	Major	App Server	Improve App Server performance by handling PostGreSQL Idle Transaction issue.
1079987	Major	Parser	Improper TLS handling can result in phParser module consuming large memory.
1116583	Enhancement	System	Enable FortiSIEM deployment for VMware versions 7 and 8.
1012778	Enhancement	System	Change pg_dump output from gzip to pigz for faster processing.

Implementation Notes

- PostGreSQL Related
- Post-Upgrade ClickHouse IP Index Rebuilding
- Upgrade Related

PostGreSQL Related

FortiSIEM 7.1.8 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.1.8, then the patch is included and there is nothing to do.
- If you are upgrading to FortiSIEM 7.1.8, then the patch is included and there is nothing to do.
- If you want to remain on a version of FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.1.8, then after upgrading to 7.1.8, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6 or 7.1.7, and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

Upgrade Related

You may encounter a blank Global Dashboard after upgrading to 7.1.8. There are two workarounds.

1. If you have not upgraded yet, then run the script `updateDashboard.sh` as root on Supervisor before upgrade. You can upgrade after running the script.
2. If you have upgraded to 7.1.8 and then see a blank Global Dashboard, then run the script `updateImportDashboard.sh` as root on Supervisor.

What's New in 7.1.7

This document describes the content on the FortiSIEM 7.1.7 release.

- Bug Fixes
- PostGreSQL Update
- Post-Upgrade ClickHouse IP Index Rebuilding

Bug Fixes

This release contains the following fixes.

Bug Id	Severity	Module	Description
1034781	Major	Linux Agent	Failed to install 7.1.6 and 7.2.0 Linux Agent due to certificate expiration.
1034224	Minor	System	If charting redis server (Node.js-charting) remains down, then phMonitor may start many new charting processes instances, consuming high memory and CPU resources.

PostGreSQL Update

FortiSIEM 7.1.7 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.1.7, then the patch is included and there is nothing to do.
- If you are upgrading to FortiSIEM 7.1.7, then the patch is included and there is nothing to do.
- If you want to remain on a version of FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

```
curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe
```

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.1.7, then after upgrading to 7.1.7, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, 7.1.5 or 7.1.6, and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

What's New in 7.1.6

This document describes the content on the FortiSIEM 7.1.6 release.

- OS Updates
- Bug Fixes
- Post-Upgrade ClickHouse IP Index Rebuilding

OS Updates

- Rocky Linux Update
- PostGreSQL Update

Rocky Linux Update

This release includes published Rocky Linux OS 8.9 updates until May 6, 2024. The list of updates can be found at https://errata.rockylinux.org/. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until May 6, 2024. FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in FortiSIEM OS Update Procedure.

PostGreSQL Update

FortiSIEM 7.1.6 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.1.6, then the patch is included and there is nothing to do.
- If you are upgrading to FortiSIEM 7.1.6, then the patch is included and there is nothing to do.
- If you want to remain on a version of FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe

Bug Fixes

This release contains the following fixes.

Bug Id	Severity	Module	Description
1016660, 1006507	Major	App Server	Supervisor will stop uploading incidents to FortiSIEM Manager if there are too many incidents backed up on Supervisor.
1023244	Major	Disaster Recovery	For ClickHouse in Disaster Recovery Environment, after switching to Secondary, historical queries may fail.
1010268	Major	Generative AI	Fortinet Advisor response shows information from other organizations.
1022966	Major	Parser	Improve phParser Syslog over TLS server processing to handle more clients.
1013804	Major	Query	EventDB deployments: Queries with any group by large field length value (> 4K) fails with 'Search Data Error'.
1025920	Major	Rule	Improve RuleWorker to reduce event drops during heavy load. Event drops produce PH_DROP_ EVENT_FROM_SHARED_BUFFER error events.
1002055	Major	Rule	Sometimes for Service provider Organizations, disabled rules may trigger incidents after upgrade to 7.1.4.
938498	Major	Rule	Sometimes phRuleWorker crashes on workers.
1003855	Major	Rule, Report	phQueryWorker, phRuleWorker and phReportWorker processes may crash when group by attribute is too long.
1026841	Major	System	Collector may fail to upload config events due to mod_security rules.
1025670	Minor	App Server	Raw Events in email incident notification (via custom template) is truncated when Incident contains Windows Agent events.
1022684	Minor	App Server	Optimize App Server handling of incident detail and lookup-time updates in System config for Elasticsearch deployments.
1022485	Minor	App Server	Windows Agents fail authentication with Supervisor in VDI environment.
1021956	Minor	App Server	Remove Organizations from other CMDB tables (ph_drq_scope) after an Organization is deleted from CMDB. This error can cause disabled rules to get activated if the rule was active in the deleted organization.

Bug Id	Severity	Module	Description
1020274	Minor	App Server	Investigation View doesn't load some incidents if there are 2 devices in Incident with the same name.
1019109	Minor	App Server	Improve App Server Task retrieval performance from Redis. This can cause GUI to become slow with large number of collectors.
1015817	Minor	App Server	IPS CVE Check Integration is broken - Cannot get CVE list from FortiGuard Services.
1012404	Minor	App Server	Org level admin cannot create System Rule Exception from Org scope.
997457	Minor	App Server	After decommissioning an unmanaged device, create a new managed device with same IP and its logs are dropped.
995640	Minor	App Server	Rule import from XML can bypass the rule name restriction that a rule name can't start with numbers.
995638	Minor	App Server	CSV Export of Watchlist does not handle comma's inside value (even if double quoted).
987938	Minor	App Server	phRecvDate cannot be used in GroupByAttr when using rest/query/eventQuery.
978060	Minor	App Server	Notification policies with Remediation script is configured to run on the collector, but is running on Supervisor.
905928	Minor	App Server	Attachments are not received in Case email notification.
1026042	Minor	App Server, Upgrade	During Collector Upgrade, DownloadImage task for a particular collector status may stay in Inwaiting stage and may not proceed.
1025801	Minor	ClickHouse Backend	ClickHouse Log Integrity Validation does not work from Supervisor Follower.
990441	Minor	ClickHouse Backend	ClickHouse Server does not clean up old unused AWS S3 objects occupying storage space.
987286	Minor	ClickHouse Backend	ClickHouse - Add worker > Test may fail if the disk is already formatted.
1022689	Minor	Docker, System	Linux agent event can't be uploaded through Docker Collector.
1024358	Minor	GUI	Duplicate 'Incident First Seen' show under CMDB Report Attribute list.

Bug Id	Severity	Module	Description
1023547	Minor	GUI	Some Lookup Tables can not be imported in Enterprise version.
1021133	Minor	GUI	Severity of more than 1 selected system rules cannot be changed WITHOUT creating a clone rule.
1011914	Minor	GUI	Incident > 'Run External Integration' Action is missing.
1007538	Minor	GUI	During rule editing, removing an attribute from GroupBy in Filter Conditions (Step 2) does not remove this attribute from Action (Step 3) - this causes rulesync issues.
1005651	Minor	GUI	Incident Explorer View is missing 'Other' Category.
997725	Minor	GUI	User GUI timeout in background browser tab logs out active foreground tab.
983266	Minor	GUI	GUI removes spaces between words in 'Destination Organization' and likely other attributes.
956930	Minor	GUI	After deleting Organizations and creating new one, user sometimes fails to create archive policies for new organizations.
991802	Minor	Linux Agent	Linux agent on Ubuntu 22.04.3 does not start when using Supervisor FQDN. Using Supervisor IP works.
987004	Minor	Linux Agent, Parser	Linux agent 7.1.0 fails to parse Process names with spaces.
1006302	Minor	Machine Learning	The Gaussian Model and Gaussian Mixture Models algorithms do not handle large data properly because of missing data normalization.
876167	Minor	Parser	During Testing Rules, parsed event attribute values containing semicolon do not show correctly.
936491	Minor	Performance Monitoring	After cloning a JDBC Performance Object, Test may fail.
1021803, 1004011	Minor	Query	For ClickHouse, there may be result discrepancy between Search on GUI and CSV Export.
996566	Minor	Query	For ClickHouse, it is not possible to do a group by on event attributes with Uint64 values.
1025395	Minor	System	Restarting 'phMonitor' would result in the unnecessarily restarting 'ClickHouseServer'.
1018855	Minor	System	For phClickHouseCSVExport tool, device ip argument should mean reporting ip.

Bug Id	Severity	Module	Description
938732	Minor	Upgrade	When collector upgrade fails, phMonitor.pre-upgrade should move back to phMonitor.
1026025	Enhancement	Data work	FortiMail Parser does not parse logs from FortiCloud FortiMail.
1024781	Enhancement	Data work	Win-Security-4688 is not parsing CommandLine in new WinOSXmlParser.
1007504	Enhancement	GUI	Interface Usage Dashboard data cannot be sorted.
996423	Enhancement	GUI	Show Organization names in alphabetical order.
989168	Enhancement	System	Support change_ip operation for worker and non-licensed Supervisor.

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.1.6, then after upgrading to 7.1.6, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, or 7.1.5, and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

What's New in 7.1.5

This document describes the contents on the FortiSIEM 7.1.5 release.

- Key Enhancements
- Bug Fixes
- Post-Upgrade ClickHouse IP Index Rebuilding

Key Enhancements

- Rocky Linux Update
- PostGreSQL Update

Rocky Linux Update

This release includes published Rocky Linux OS 8.9 updates until April 9, 2024. The list of updates can be found at https://errata.rockylinux.org/. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until April 9, 2024. FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in FortiSIEM OS Update Procedure.

PostGreSQL Update

FortiSIEM 7.1.5 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.1.5, then the patch is included and there is nothing to do.
- If you are upgrading to FortiSIEM 7.1.5, then the patch is included and there is nothing to do.
- If you want to remain on an earlier version of FortiSIEM, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

```
curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe
```

Bug Fixes

This release contains the following fixes.

Bug Id	Severity	Module	Description
1013839	Major	App Server	Elasticsearch based deployments - The Trend Histogram in Search results is not granular.
1012448	Major	Event Pulling Agents	GCP event pulling sometimes gets duplicate events.
1010197	Major	Report	PDF export containing multibyte characters will not display correctly.
1013071	Minor	App Server	During Incident HTTP Notification, special characters (e.g. &, >, < etc.) in Incident attributes are not escaped, resulting in invalid XML when incident attribute values contains such special characters.
1012404	Minor	App Server	Org level admin cannot create exceptions to system rules.
1009809	Minor	Collector	ClickHouse Server incorrectly installed on FortiSIEM Collectors.
1016072	Minor	Discovery	Discovering a collector via SNMPv3 in its own Org doesn't update CMDB and performance jobs.
986119	Minor	Event Packager	phEventPackager module on Collector restarts crashes if it can't communicate with Worker (after retries).
1015740	Minor	Event Pulling Agents	FortiEMS Vuln Scan API called too frequently, creating high EPS for large environments.
1010975	Minor	Event Pulling Agents	When AWS S3 SQS File name contains special characters, then FortiSIEM may fail to get logs from that file.
1013844	Minor	GUI	Elasticsearch based deployments - When a user hovers over a single trend bar in the UI display Search results, the displayed trend interval is not correct.
1014757	Minor	Parser	phParser module does not properly handle a JSON field when it is an array.
1009300	Minor	Parser	User, target user and target user group not parsed for certain Windows XML formatted logs from FortiSIEM Windows Agent 7.1.5 and above.
1005694	Enhancement	App Server	App Server handling of updating Collector and Worker health need to be optimized.

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.1.5, then after upgrading to 7.1.5, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3 or 7.1.4, and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

What's New in 7.1.4

This document describes the additions for the FortiSIEM 7.1.4 release.

- New Feature
- Key Enhancements
- Bug Fixes and Enhancements

New Feature

ClickHouse Archive to Google Cloud Storage (GCS)

This release enables you to archive ClickHouse to Google Cloud Storage (GCS) in FortiSIEM Google Cloud Platform (GCP) deployments. For setting up ClickHouse Archive on GCS, see here.

Key Enhancements

- Rocky Linux Update
- Windows Agent Log Handling Performance Improvement
- ClickHouse Data Movement Algorithm Change
- Incident Actions Added to all Incident Pages
- Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields

Rocky Linux Update

This release includes published Rocky Linux OS 8.9 updates until February 15, 2024. The list of updates can be found at https://errata.rockylinux.org/. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until February 15, 2024. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in FortiSIEM OS Update Procedure.

Windows Agent Log Handling Performance Improvement

To better handle larger volume of Windows events (specially Windows forwarded events), FortiSIEM Windows Agent now uses the Windows native XML format to transfer all Windows logs (Security, System, Application, Forwarded Events, etc.) to Collector. A new FortiSIEM Windows event parser (WinOSXmlParser) now parses event attributes directly from XML fields. By transferring the parsing load from Windows Agent to Collector, Agent CPU load is reduced, and the Collector CPU load is slightly increased. Fortinet has not noticed any significant load increases in Collector. From user perspective, only Windows raw message structure changes from FortiSIEM "[Attribute]:Value, [Attribute]:Value" format to Windows XML format.

Since Windows event log structure has changed, all user-written custom Windows parsers should be upgraded to parse XML fields, prior to upgrading Windows Agent. Please follow the parsing logic in WinOSXmlParser to adapt your custom Windows parsers.

An example Security log format change is below. For other examples, see here.

Current Format:

```
2024-02-22T01:07:51Z Win10.acme.com 172.30.56.127 AccelOps-WUA-WinLog-Security
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="72f70ae7-fedf-4dc0-92e7-0c953f46f87e" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [eventName]="Security" [eventSource]="Microsoft-
Windows-Security-Auditing" [eventId]="4703" [eventType]="Information" [domain]=""
[computer]="Win10.acme.com" [user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="Feb 22
2024 01:07:51" [deviceTime]="Feb 22 2024 01:07:51" [msg]="A token right was adjusted."
[[Subject]][Security ID]="S-1-5-18" [Account Name]="GFU-WIN10$" [Account Domain]="ACME"
[Logon ID]="0x3E7" [[Target Account]][Security ID]="S-1-5-18" [Account Name]="ACME-WIN10$"
[Account Domain]="ACME" [Logon ID]="0x3E7" [[Process Information]][Process ID]="0x3348"
[Process Name]="C:\\Windows\\System32\\msiexec.exe" [Enabled Privileges]="" [Disabled
Privileges]="SeRestorePrivilege,SeTakeOwnershipPrivilege"
```

New Format:

```
2024-02-27T21:19:33Z Win10.acme.com 172.30.56.129 FSM-WUA-WinLog-Security [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="1e749ab9-bf6e-
4052-806b-02068b2d4465" [timeZone]="-0800" [extEventRecvProto]="Windows Agent"
[level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-a5ba-
3e3b0328c30d}'/><EventID>4703</EventID><Version>0</Version><Level>0</Level><Task>13317</Ta
sk><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2024-
02-
27T21:19:32.430796700Z'/><EventRecordID>9064813051</EventRecordID><Correlation/><Execution
ProcessID='4' ThreadID='5944'/><Channel>Security</Channel><Computer>FSM-GFU-Windows2019-
WIN2019-172-30-56-129</Computer><Security/></System><EventData><Data
```

```
Name='SubjectUserSid'>S-1-5-18</Data><Data Name='SubjectUserName'>FSM-GFU-
WINDOWS$</Data><Data Name='SubjectDomainName'>WORKGROUP</Data><Data
Name='SubjectLogonId'>0x3e7</Data><Data Name='TargetUserSid'>S-1-0-0</Data><Data
Name='TargetUserName'>FSM-GFU-WINDOWS$</Data><Data
Name='TargetDomainName'>WORKGROUP</Data><Data Name='TargetLogonId'>0x3e7</Data><Data
Name='ProcessName'>C:\\Windows\\System32\\svchost.exe</Data><Data
Name='ProcessId'>0xbdc</Data><Data
Name='EnabledPrivilegeList'>SeAssignPrimaryTokenPrivilege
   SeIncreaseQuotaPrivilege
   SeSecurityPrivilege
   SeTakeOwnershipPrivilege
   SeLoadDriverPrivilege
   SeSystemtimePrivilege
   SeBackupPrivilege
   SeRestorePrivilege
   SeShutdownPrivilege
   SeSystemEnvironmentPrivilege
   SeUndockPrivilege
   SeManageVolumePrivilege</Data><Data Name='DisabledPrivilegeList'>-
</Data></EventData></Event>
```

ClickHouse Data Movement Algorithm Change

Currently when a storage tier becomes 90% full, then the earliest data partition from each retention policy bucket (chosen in a round robin manner) is moved to the next storage tier, until the utilization reaches 80%. This policy may be unfair to recently created retention policies. The data movement algorithm is changed to global earliest data partition first. That means, when a storage tier becomes 90% full, then the earliest data partitions across all retention policy buckets are moved to the next storage tier, until the utilization reaches 80%.

Incident Actions Added to all Incident Pages

Currently, the Incident Action menu is available on the Incident List View and Risk pages. This menu is now added to the following pages.

- **Incidents > UEBA**
- **Incidents > Explorer**
- **Incidents > MITRE ATT&CK > IT: Incident Explorer**
- **Incidents > MITRE ATT&CK > ICS: Incident Explorer**

Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields

As noted in 7.1.3 Known Issue, after upgrading pre-7.1.1 to 7.1.2 or later, searching on IP fields in ClickHouse based deployments does not show correct results for events stored prior to upgrade. IP fields include Reporting IP, Source IP, Destination IP, and Host IP. This release provides a simple script to replace the set of commands detailed in 7.1.3 Known Issue.

If you are running FortiSIEM 7.1.2 or 7.1.3 on ClickHouse and already executed the rebuilding steps in 7.1.3 Known Issue, then nothing more needs to be done. However, if you are running FortiSIEM 7.1.1 or earlier on ClickHouse, then after upgrading to 7.1.4, you can use the following command to automate the ClickHouse index rebuilding steps:

```
/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -h
```

Usage: `./script [-h for help] [-p for 10 oldest partitions] [-m manual commands] [-r <index id> index to be rebuilt]`

Here are indexes available for rebuild. Please choose one and specify the `id` in `-r` option.

`-r <index id>` option is mandatory.

1. reptDevIpAddr
2. srcIpAddr
3. destIpAddr
4. hostIpAddr

For example, to rebuild reptDevIpAddr index, issue the following command.

```
$ ./rebuild_ip_bloom_filter.sh -r 1
```

Notes before running the script:

1. The script should be run on only one node per shard. Only one instance of the script can be run at one time on a host. This is checked and enforced by the script.
2. The rebuilding of bloom filter index is a table-wide operation and it could take some time to complete, based on the amount of data and resources available.
3. Since the script could be long-running, please use screen or tmux sessions to launch the script.
4. During the rebuilding of bloom filter index, there will be a temporary spike in storage usage as ClickHouse goes through the existing data and rebuilds indexes for the whole table. The rebuilding of bloom filter index is a non-intrusive operation. After the DROP, ADD, MATERIALIZE requests are submitted to ClickHouse, ClickHouse will schedule the various tasks in an optimized way. The user has no control over the process.
5. All nodes in the target shard should have at least 10% free space on `/data-clickhouse-hot-1`. The script will also check the 10% space requirement on all nodes of the shard and suggests partitions that should be moved to a different tier to create space. If there are no more tiers to move the partitions to, please consult with Fortinet support to identify a reasonable solution.
6. The script will show the remaining parts to be processed for both DROP and MATERIALIZE phase. If the "parts to be processed" is stuck at a specific count for more than 24 hours, please contact Fortinet support to check if there are any underlying

conditions that would have prevented the DROP or MATERIALIZE command to proceed further.

Detailed Steps are as follows:

1. Go to root shell by running the following command:
   `sudo -s`
2. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 1`
   The script will produce output similar to the following:

```
[root@server]# /opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 1
current attr is reptDevIpAddr
Materialize in progress "false" for reptDevIpAddr with 0 parts to process
Materialize in progress "false" for srcIpAddr with 0 parts to process
Materialize in progress "false" for destIpAddr with 0 parts to process
Materialize in progress "false" for hostIpAddr with 0 parts to process
drop in progress "false" for reptDevIpAddr
drop in progress "false" for srcIpAddr
drop in progress "false" for destIpAddr
drop in progress "false" for hostIpAddr
Processing index index_reptDevIpAddr_bloom_filter
Trying to rebuild index_reptDevIpAddr_bloom_filter
drop in progress "false"
There is enough storage on host 172.30.56.206.
done checking storage for index index_reptDevIpAddr_bloom_filter
dropping index index_reptDevIpAddr_bloom_filter
dropping index command issued
Start monitoring index index_reptDevIpAddr_bloom_filter for drop operation
drop index_reptDevIpAddr_bloom_filter done. Total time taken: 0 seconds
Total time to drop index_reptDevIpAddr_bloom_filter is 1 seconds
adding index_reptDevIpAddr_bloom_filter
Start monitoring index index_reptDevIpAddr_bloom_filter for materialize operation
parts left to materialize reptDevIpAddr index : 6 - time taken 0 seconds
materialize index_reptDevIpAddr_bloom_filter done. Total time taken: 10 seconds
Rebuilding index for reptDevIpAddr done. Total time taken for rebuild 13 seconds
```

3. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 2`
4. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 3`
5. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 4`

Bug Fixes and Enhancements

This release contains the following fixes and enhancements.

Bug ID	Severity	Module	Description
1000328	Major	App Server	With large (500+) number of parsers, App Server may encounter stack overflow, and fail to start up.
986665	Major	App Server	During Agent upgrade with a large number of large number of Agents, some Agents would get hung up and not finish the upgrade process.
1004319	Major	GUI	Clear condition in a Rule is not saved correctly. This may cause the correct clear conditions to be displayed correctly in GUI and may not be enforced correctly in a rule. This bug was introduced in FortiSIEM 7.1.0.
991851	Major	Performance Monitoring	`phPerfMonitor` module may crash when both STM and perf monitoring are defined.
1004357	Major	phMonitor	Adding a Worker node fails in the scenario where NFS is chosen as event archive destination.
1001969	Major	Rule Engine	With a large Malware IOC feed and high EPS, the `phRuleWorker` module may be dropping events, and Incidents may not trigger.
997357	Major	System	`snmpd.conf` has default 'public' community string enabled in the image.
990219	Minor	App Server	Adding more than 20 Incidents to a Case throws `request-uri too long` error.
984002	Minor	App Server	Duplicate Device with different Vendor/Model/Versions may be seen in CMDB after Agent registration.
982928	Minor	App Server	Running investigations in the GUI can cause `Appserver` to crash if App Server is unable to reach external servers (e.g. Whois, FortiGuard).
992974	Minor	Data Purger	ClickHouse data management module moves or purges 10% more data than it should. Instead of free disk utilization fluctuating between 10% and 20% (as needed by design), it fluctuates between 10% and 30%.
953268	Minor	Data Purger	In EventDB environment, Online data for Org 0 and Org 2 did not get purged after archive.
987019	Minor	Data work	Office365 Reports API Parser has flipped source and destination domain for Office365 Message Trace events.

Bug ID	Severity	Module	Description
994833	Minor	Discovery	Configuration pull for FortiOS via Rest API integration does not work if FQDN obtained via IP reverse lookup, and CMDB hostname are different.
1001664	Minor	Event Pulling Agents	Google App event pulling fails (caused by 3rd party library `google-api-client.jar` upgraded to version 2.1.4).
988310	Minor	Event Pulling Agents	`phAgentManager` may crash while handling incorrect Office365 credentials.
993615	Minor	GUI	In Incident List View, event attributes inside `incidentDetail` are not shown correctly if value contains ':'.
992843	Minor	GUI	Test Connectivity does not work in 7.1.x Enterprise mode.
989124	Minor	GUI	Windows Agent type in Agent health page is empty after upgrading to 7.1.2.
979734	Minor	GUI	"Set Activation Scope" from Super org does not correctly update rule status for organizations.
977174	Minor	GUI	Export PDF Report Results fails if Supervisor can't reach Internet over port 443.
992940	Minor	Machine Learning	Incident Resolution Recommendation Engine is learning from its own actions instead of only learning for user's action.
995423	Minor	Parser	`phParser` module crashes (instead of restarting) after content update on Workers.
993240	Minor	Parser	After content update to version 602, parsers are not applied correctly.
980410	Minor	Parser	Elasticsearch index creation fails when parser generates internal events for Orgs that do not exist in CMDB.
1003091	Minor	phAnomaly	The `/opt/phoenix/MachineLearning` folder size is increasing with .csv files, and may eventually fill up `/opt` partition.
990369	Minor	Query	User with full access to Analytics and View access to CMDB need additional view permission to see all parsed events.
989855	Minor	Query	Analytical searches with Raw Event Log and CONTAIN 'Code' does not run.

Bug ID	Severity	Module	Description
989751	Minor	Query	There is a known issue in release 7.1.1 or later. After upgrading to any of these releases from a pre-7.1.1 release, in ClickHouse based deployments, searching on IP fields (namely, Reporting IP, Source IP, Destination IP, and Host IP) does not show correct results for events stored prior to upgrade. Release notes provides manual steps. A script is needed to replace the manual steps.
1003621	Minor	System	FortiSIEM hardware appliance `factoryreset --force` fails when system does not have Internet access to OS repo servers.
992756	Minor	System	`phshowVersion.sh` script output does not show the data for Archive correctly if Archive and Online disk mount point uses the same disk name.
986922	Minor	System	The `phMonitor` process in Supervisor node may sometimes restart during adding Workers.
1001157	Minor	Windows Agent	In Windows Event Forwarding environment, Windows Agent which receives forwarded events and sends to Collector, may get overloaded with events and the latency for events to reach FortiSIEM Collector may increase.
972454, 975763	Minor	Windows Agent	Windows Agent has high CPU usage when it handles high volume of Windows Forwarded events.
984787	Minor	Windows Agent	Windows Agent performance monitoring shows wrong disk latency metrics.
939919	Minor	Windows Agent	File Integrity Monitoring (FIM) Event for non-Windows network drive mounted on Windows server does not contain user id and domain info.
1002302	Enhancement	Data Work	FortiMail reported "Antivirus Phishing URL found in email" is not specifically handled by existing rules.
985480	Enhancement	Data Work	Update FortiGate IPS Signatures to the latest.
975379	Enhancement	Data Work	Add Rules, Reports, Dashboard for Trend Micro Vision One integration.
998288	Enhancement	GUI	Add Action menu to Incident Explorer view, UEBA view and MITRE ATT&CK Incident Explorer view.
989845	Enhancement	GUI	In Incident slide-in display, Incident First Occur Time and Last Occur Time values need to show the full exact date.

Bug ID	Severity	Module	Description
991315	Enhancement	Machine Learning	Currently, FortiSIEM automatically clears an Incident if Machine Learning algorithm detects 'False positive' resolution with confidence greater than 90%. Provide a user option to disable this.
984748	Enhancement	Parser	For HTTPS Advanced Poller, support dot notation for json response key as the array of events is sometimes nested under several structure not at the top level.

What's New in 7.1.3

This release fixes the following issues:

- An important security issue described in Fortinet PSIRT Advisory FG-IR-23-130 impacting Supervisor and Worker nodes.
- Fixes known issue in FortiSIEM 7.1.2, where Supervisor and Worker nodes may fail to restart properly for VMs running on ClickHouse or EventDB with local disk. For more detailed information, see 7.1.2 Installation / Upgrade Related Known Issue.

Known Issue

After upgrading to 7.1.1 or later, in ClickHouse based deployments, searching on IP fields (namely, Reporting IP, Source IP, Destination IP, and Host IP) does not show correct results *for events stored prior to upgrade*. Events are still stored in ClickHouse, but searches on events *before* the upgrade do not return results, while searches on events stored *after* the upgrade work correctly. All other searches work correctly.

This issue is related to a recent change in ClickHouse version 23.3 in how IPV6 fields are represented. See the following URLs for more information.

- https://github.com/ClickHouse/ClickHouse/issues/58885
- https://github.com/ClickHouse/ClickHouse/issues/56487
- https://github.com/ClickHouse/ClickHouse/pull/57707
- https://github.com/ClickHouse/ClickHouse/issues/54162

Workaround

The workaround requires recreating old indices involving Reporting IP, Source IP, Destination IP, and Host IP that were created before the 7.1.1 upgrade. In our experiments, Fortinet has not seen any event loss or FortiSIEM service interruption during this process.

1. Go to root shell by running the following command:
   ```
   sudo -s
   ```
2. Change directory to `/tmp` by running the following command:
   ```
   cd /tmp
   ```
3. Run the following command:
   ```
   clickhouse-client
   ```
4. Ensure that `/data-clickhouse-hot-1` has at least 10% free disk space. This space is required during index re-creation (Step 5 below). If free disk space is less that 10%, then run the following SQL command (4a.) to get the list of oldest ClickHouse partitions residing on the `/data-clickhouse-hot-1` disk and either move them to another disk or tier, or delete them until `/data-clickhouse-hot-1` has at least 10% free disk space. **These commands need to be run only on ALL data nodes in every shard.** The first command (4a.), identifies the largest partitions on the `/data-`

clickhouse-hot-1 disk. The remaining commands enable you to move the data to another tier (4b.), or another disk (4c.), or delete the data (4d.).

a. Identify the largest ClickHouse partitions in Hot node:

```
SELECT disk_name, partition, extract(partition, '\(\d+,(\d+)\)') as date,
formatReadableSize(sum(bytes_on_disk)), formatReadableSize(sum(data_uncompressed_
bytes)) FROM system.parts WHERE (table = 'events_replicated') AND path LIKE
'%hot-1%' AND active GROUP BY disk_name, partition ORDER BY disk_name ASC, date
ASC limit 10
```

b. Move the data to another tier:

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION <partition expression from (a)
> TO VOLUME <next tier>
```

c. Move the data to another disk:

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION <partition expression from (a)
> TO disk <another disk>
```

d. Delete the data:

```
 ALTER TABLE fsiem.events_replicated DROP PARTITION <partition expression from
(a) >
```

Example:

Output from command in 4a.:

disk_name	partition	date	formatReadableSize(sum(bytes_on_disk))	formatReadableSize(sum(data_uncompressed_bytes))
default	(18250,20240115)	20240115	229.96 MiB	3.98 GiB
default	(18250,20240116)	20240116	399.59 MiB	6.92 GiB
default	(18250,20240118)	20240118	8.58 MiB	208.72 MiB
default	(18250,20240119)	20240119	1.87 MiB	43.64 MiB
default	(18250,20240120)	20240120	1.89 MiB	43.93 MiB
default	(18250,20240121)	20240121	1.88 MiB	44.12 MiB
default	(18250,20240122)	20240122	1012.05 KiB	22.46 MiB

To move the first partition (size 3.98 GiB) to Warm tier, issue the following command as shown in 4b.

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION (18250, 20240115) TO VOLUME
'warm'
```

To move the first partition (size 3.98 GiB) to another disk in Hot tier, issue the following command as shown in 4c.

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION (18250, 20240116) TO disk
'data_clickhouse_hot_2'
```

To delete the first partition (size 3.98 GiB), issue the following command as shown in 4d.

```
ALTER TABLE fsiem.events_replicated DROP PARTITION (18250, 20240116)
```

5. Run the following commands sequentially. This will drop/add/recreate all affected indices: Reporting IP, Source IP, Destination IP, and Host IP within ClickHouse. **These commands need to be run only on one data node per shard.** Note that the first command (drop) in every index may take some time to complete. User must wait until it completes before issuing the next command.

```
alter table fsiem.events_replicated drop index index_reptDevIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_reptDevIpAddr_bloom_filter
reptDevIpAddr TYPE bloom_filter GRANULARITY 5 AFTER index_customer_set
alter table fsiem.events_replicated materialize index index_reptDevIpAddr_bloom_filter
```

```
alter table fsiem.events_replicated drop index index_srcIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_srcIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'srcIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
collectorId_set
alter table fsiem.events_replicated materialize index index_srcIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_destIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_destIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'destIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
index_srcIpAddr_bloom_filter
alter table fsiem.events_replicated materialize index index_destIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_hostIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_hostIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'hostIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
index_user_bloom_filter
alter table fsiem.events_replicated materialize index index_hostIpAddr_bloom_filter
```

What's New in 7.1.2

This release fixes an important security issue described in Fortinet PSIRT Advisory FG-IR-23-130 impacting Supervisor and Worker nodes.

Known Issues

- Installation / Upgrade Related
- ClickHouse Related

Installation / Upgrade Related

FortiSIEM Supervisor and Worker nodes may fail to come up properly **after restart** in certain situations. This impacts VM based installs where the storage type is ClickHouse or EventDB with local disk. Hardware platforms are not affected by this issue. The root cause is that the sanitized scripts, as part of security fix, failed to insert the disk UUID in `/etc/fstab` file entries.

The failing scenarios are as follows:

Case 1: Fresh install 7.1.2, then save ClickHouse or EventDB local storage and try to reboot.

Case 2: Upgrade to 7.1.2, then save ClickHouse or EventDB local storage and try to reboot.

Workarounds are as follows:

Case 1: If you have not yet rebooted the nodes, login via SSH as root and make the following changes:

ClickHouse:

The following empty UUIDs need to be replaced with the actual value from the `blkid` command output for the corresponding disk.

1. Use the following command to print the UUID of the disk.
   `blkid <devicename> | awk '-F"' '{ print $2; }'`
   For example:
   ```
   blkid /dev/sde | awk '-F"' '{ print $2; }'
   cc111789-ead1-485c-9880-138db408b7c1
   blkid /dev/sdf | awk '-F"' '{ print $2; }'
   c877e6a7-b16c-4fd2-988e-5450b963d7c7
   ```
2. Edit `/etc/fstab` file and replace empty UUIDs as follows:
   ```
   UUID=cc111789-ead1-485c-9880-138db408b7c1 /data-clickhouse-hot-1 xfs
   defaults,nodev,noatime,inode64 0 0
   UUID=c877e6a7-b16c-4fd2-988e-5450b963d7c7 /data-clickhouse-warm-1 xfs
   defaults,nodev,noatime,inode64 0 0
   ```

3. Once the above changes are made, run the following command:
   `systemctl daemon-reload`
   Now, it is safe to reboot the system.

EventDB on Local Disk:

The following empty UUID needs to be replaced with the actual value from the `blkid` command output for the corresponding disk.

1. Use the following command to print the UUID of the disk.
   `blkid <devicename> | awk '-F"' '{ print $2; }'`
2. Edit `/etc/fstab` file and replace empty UUID as follows:
   `UUID= /data xfs defaults,nodev,noatime,inode64 0 0`
3. Once the above changes are made, run the following command:
   `systemctl daemon-reload`
   Now, it is safe to reboot the system.

Case 2: If you rebooted the system and the system appears to be hanging, then you will need to perform the following steps while the system is hung:

1. Send Ctrl+Alt+Delete or reset the VM in VCenter or Hypervisor console.
2. On the VM console, when you get to the list of boot up options (Rocky Linux ..., Rescue ...), the default is the first entry.
3. Before it boots up automatically into the first entry, hit the 'e' key to edit grub options. Then you are brought to a simple editor of grub options.
4. Scroll down to the line which starts with "linux". Go to the end of the line with Ctrl+E.
5. Remove the options "quiet" and "console=ttyS0" if running on a Hypervisor platform, such as VMWare VCenter. In the case of AWS, Azure, or GCP, if you are using the serial console, you only need to remove the "quiet" option since the console is already correctly going to the serial console ttyS0.
6. Hit Ctrl+X.
7. Now the system boots up in verbose mode, and it will hang for a few minutes attempting to mount ClickHouse hot and warm disks, or EventDB local disk as the case may be. Once it fails to mount, it will bring you to the prompt "Give root password for maintenance".
8. Enter root password. You will now be in the root prompt.
9. Use the following command to print the UUID of the disk. You need to know which disk you provided for hot and warm disk.
   `blkid <devicename> | awk '-F"' '{ print $2; }'`
   For example:
   `blkid /dev/sde | awk '-F"' '{ print $2; }'`
   `cc111789-ead1-485c-9880-138db408b7c1`
   `blkid /dev/sdf | awk '-F"' '{ print $2; }'`
   `c877e6a7-b16c-4fd2-988e-5450b963d7c7`
10. Take this UUID and edit the `/etc/fstab` hot disk entry with the UUID, and the warm disk entry (if present) or local EventDB directory.
    For example:
    `UUID=cc111789-ead1-485c-9880-138db408b7c1 /data-clickhouse-hot-1 xfs defaults,nodev,noatime,inode64 0 0`

```
UUID=c877e6a7-b16c-4fd2-988e-5450b963d7c7 /data-clickhouse-warm-1 xfs
defaults,nodev,noatime,inode64 0 0
```

11. Run the following command:
    ```
    systemctl daemon-reload
    ```
12. Reboot.

ClickHouse Related

After upgrading to 7.1.1 or later, in ClickHouse based deployments, searching on IP fields (namely, Reporting IP, Source IP, Destination IP, and Host IP) does not show correct results *for events stored prior to upgrade*. Events are still stored in ClickHouse, but searches on events *before* the upgrade do not return results, while searches on events stored *after* the upgrade work correctly. All other searches work correctly.

This issue is related to a recent change in ClickHouse version 23.3 in how IPV6 fields are represented. See the following URLs for more information.

- https://github.com/ClickHouse/ClickHouse/issues/58885
- https://github.com/ClickHouse/ClickHouse/issues/56487
- https://github.com/ClickHouse/ClickHouse/pull/57707
- https://github.com/ClickHouse/ClickHouse/issues/54162

Workaround

The workaround requires recreating old indices involving Reporting IP, Source IP, Destination IP, and Host IP that were created before the 7.1.1 upgrade. In our experiments, Fortinet has not seen any event loss or FortiSIEM service interruption during this process.

1. Go to root shell by running the following command:
   ```
   sudo -s
   ```
2. Change directory to `/tmp` by running the following command:
   ```
   cd /tmp
   ```
3. Run the following command:
   ```
   clickhouse-client
   ```
4. Ensure that `/data-clickhouse-hot-1` has at least 10% free disk space. This space is required during index re-creation (Step 5 below). If free disk space is less that 10%, then run the following SQL command (4a.) to get the list of oldest ClickHouse partitions residing on the `/data-clickhouse-hot-1` disk and either move them to another disk or tier, or delete them until `/data-clickhouse-hot-1` has at least 10% free disk space. **These commands need to be run only on ALL data nodes in every shard.** The first command (4a.), identifies the largest partitions on the `/data-clickhouse-hot-1` disk. The remaining commands enable you to move the data to another tier (4b.), or another disk (4c.), or delete the data (4d.).
   a. Identify the largest ClickHouse partitions in Hot node:
      ```
      SELECT disk_name, partition, extract(partition, '\(\d+,(\d+)\)') as date,
      formatReadableSize(sum(bytes_on_disk)), formatReadableSize(sum(data_uncompressed_
      bytes)) FROM system.parts WHERE (table = 'events_replicated') AND path LIKE
      '%hot-1%' AND active GROUP BY disk_name, partition ORDER BY disk_name ASC, date
      ASC limit 10
      ```

b. Move the data to another tier:

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION <partition expression from (a)
> TO VOLUME <next tier>
```

c. Move the data to another disk:

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION <partition expression from (a)
> TO disk <another disk>
```

d. Delete the data:

```
 ALTER TABLE fsiem.events_replicated DROP PARTITION <partition expression from
(a) >
```

Example:

Output from command in 4a.:

disk_name	partition	date	formatReadableSize(sum(bytes_on_disk))	formatReadableSize(sum(data_uncompressed_bytes))
default	(18250,20240115)	20240115	229.96 MiB	3.98 GiB
default	(18250,20240116)	20240116	399.59 MiB	6.92 GiB
default	(18250,20240118)	20240118	8.58 MiB	208.72 MiB
default	(18250,20240119)	20240119	1.87 MiB	43.64 MiB
default	(18250,20240120)	20240120	1.89 MiB	43.93 MiB
default	(18250,20240121)	20240121	1.88 MiB	44.12 MiB
default	(18250,20240122)	20240122	1012.05 KiB	22.46 MiB

To move the first partition (size 3.98 GiB) to Warm tier, issue the following command as shown in 4b.

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION (18250, 20240115) TO VOLUME
'warm'
```

To move the first partition (size 3.98 GiB) to another disk in Hot tier, issue the following command as shown in 4c.

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION (18250, 20240116) TO disk
'data_clickhouse_hot_2'
```

To delete the first partition (size 3.98 GiB), issue the following command as shown in 4d.

```
ALTER TABLE fsiem.events_replicated DROP PARTITION (18250, 20240116)
```

5. Run the following commands sequentially. This will drop/add/recreate all affected indices: Reporting IP, Source IP, Destination IP, and Host IP within ClickHouse. **These commands need to be run only on one data node per shard.** Note that the first command (drop) in every index may take some time to complete. User must wait until it completes before issuing the next command.

```
alter table fsiem.events_replicated drop index index_reptDevIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_reptDevIpAddr_bloom_filter
reptDevIpAddr TYPE bloom_filter GRANULARITY 5 AFTER index_customer_set
alter table fsiem.events_replicated materialize index index_reptDevIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_srcIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_srcIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'srcIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
collectorId_set
alter table fsiem.events_replicated materialize index index_srcIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_destIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_destIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'destIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
```

```
index_srcIpAddr_bloom_filter
alter table fsiem.events_replicated materialize index index_destIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_hostIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_hostIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'hostIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
index_user_bloom_filter
alter table fsiem.events_replicated materialize index index_hostIpAddr_bloom_filter
```

What's New in 7.1.1

This release contains the following key enhancements and bug fixes.

- Key Enhancements
- Bug Fixes and Enhancements
- Known Issue

Key Enhancements

- Rocky Linux 8.9
- Redis Memory Usage Optimization
- Support for Trend Vision One
- More SOC Queries via Fortinet Advisor
- SIGMA Rule Fixes
- Public REST API Throttling

Rocky Linux 8.9

This release updates Rocky Linux OS to 8.9 and includes published Rocky Linux OS updates until November 28, 2023. The list of updates can be found at https://errata.rockylinux.org/.

FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until July 14, 2023. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in FortiSIEM OS Update Procedure.

Redis Memory Usage Optimization

FortiSIEM uses Redis to distribute CMDB Group Objects (including Malware IP/Domain/URL/Hash objects) from Supervisor PostGreSQL database to the Worker nodes. A Malware IP or Domain group containing a large number of entries can cause Redis to hit its memory limit and cause Search queries to fail. In this release, by using compression techniques, Redis peak memory usage is reduced significantly. This enables FortiSIEM to handle more threat feed entries, and more CMDB Groups.

As an example, in Fortinet experiments with 1 million FortiGuard Malware IP, 3 million Malware Domains, 500 thousand Malware URL and with App Server Java memory set to 10GB, Redis peak memory usage is reduced from 1GB in 7.0.2 to 156MB in 7.1.1. For this case, compression resulted in more than 80% reduction of Redis peak memory.

Support for Trend Vision One

This release adds support for Trend Vision One XDR platform. See Trend Vision One in the External Systems Configuration Guide for integration details.

More SOC Queries via Fortinet Advisor

Fortinet Advisor recognizes and responds to the following Security Operations Center (SOC) questions.

Note: In 7.2.0 and later, Fortinet Advisor is known as FortiAI.

- Get my FortiSIEM environment
- Get latest 10 high severity Incidents
- Get most frequent 10 Incidents
- Get Top 10 risky users
- Get Top 10 risky devices

SIGMA Rule Fixes

This release updates several FortiSIEM rules adapted from SIGMA rules. Updates involve regular expression conversions from SIGMA format to FortiSIEM format.

Public REST API Throttling

To safeguard Supervisor performance, FortiSIEM now throttles the volume of public REST API requests. Concurrent API requests are limited per source IP and globally. Once limits are reached, error code 429 is sent in response.

The limits are defined in `/opt/phoenix/config/phoenix_config.txt`:

```
global_max_concurrent_public_api_requests=50
```

```
per_ip_max_concurrent_public_api_requests=10
```

Notes:

1. When a single source IP makes more than 10 concurrent API calls, then the 11th request will receive a 429 HTTP(S) error code. If the client retries and one or more of its earlier calls finishes and the number of active calls becomes lower than 10, then the new call will succeed.
2. If the total of all active API calls from all sources is over 50, then the 51st request will receive a 429 HTTP(S) error code.
3. When a 429 error code is encountered, API Clients should implement backoff, waiting longer between each subsequent retry.

Bug Fixes and Enhancements

This release contains the following fixes and enhancements.

Bug ID	Severity	Module	Description
971855	Major	App Server	Null pointer exception may occur during App Server incident handling.
971840	Major	App Server	App Server may hit deadlock issue in Postgres during FortiSIEM node health update.
977554	Major	ClickHouse	After upgrading to 7.1.0, adding new ClickHouse node to the same shard fails with DDL error.
914974	Major	Rule Engine	User created security incidents auto-clear after 24 hours even if `auto_clear_security_incidents=0` is set.
975345	Minor	App Server	For Windows and Linux Agents, agent monitoring attributes overwrite agentless monitoring attributes, when both agentless methods (such as OMI or SSH) are used along with agents on the same server.
973567	Minor	App Server	After cloning an existing rule and changing the evaluation mode to scheduled, Incidents are still evaluated in streaming mode.
972257	Minor	App Server	Summary Dashboards do not show performance metrics collected by Windows Agent.
971860	Minor	App Server	For Event Receive Hour/Day/Week queries, Query Result Export and Scheduled Report do not work correctly.
971276	Minor	App Server	System defined and user defined Network objects with same IP range become incorrectly linked together.
971126	Minor	App Server	Invalid Query XML for IN queries with more than 1 Individual Countries.
969372	Minor	App Server	Public REST API for Event Query and Archive Query return no events if report syntax is invalid. It should return error instead.
968983	Minor	App Server	Content update fails if there are dashboard widgets in the content update.
968751	Minor	App Server	Box.com integration may cause App Server to lock up when auth token expires.
968266	Minor	App Server	For Incident public REST API, queries for second and subsequent pages may fail with 503 error code if called too fast.
962913	Minor	App Server	Need to throttle public REST API queries by returning HTTP status code 429, when client sends in too many requests.

Bug ID	Severity	Module	Description
939273	Minor	App Server	Cannot modify device properties for multi-tenant collector.
936243	Minor	App Server	Timezone selection for Europe/Berlin is not listed in UTC+2, but it is in UTC+1.
927843	Minor	App Server	Discovering a device via FSM Agent and EMS/FGT integration results in duplicate CMDB entries.
926647	Minor	App Server	CMDB Device Report: No result for 'Property Event Receive Time Gap [Low/High] Threshold minutes'.
970594	Minor	ClickHouse Backend	Update `phClickHouseImport` tool to support event DB data import from custom directory instead of `CUSTOMER_1` only.
974846	Minor	Discovery	Test Connectivity for Cisco FireAmp fails.
970075	Minor	Discovery	GitLab discovery failure: Need to use host name as IP does not work during SSL handshake.
931808	Minor	Discovery	For standalone FortiSwitch, Network Interfaces not discovered via SNMP v3 because of lack of support for SHA-224, SHA-256, SHA-384 and SHA-512 for authentication and AES-192 and AES-256 for encryption.
976427	Minor	GUI	**Analytics > Investigation** page, Run Reports > Event Receive Time column shows epoch value instead of date formatted values.
976046	Minor	GUI	User with Dashboard only role gets empty landing page after login.
974384	Minor	GUI	In CMDB Report, Latest Monitor Time and Latest Event Pulling Time fields show epoch value instead of date formatted values.
972715	Minor	GUI	Check Reputation in Real Time/Historical Search does not work.
971557	Minor	GUI	NullPointerException in the POST SAML response after modifying the idle timeout for Azure SSO user.
966730	Minor	GUI	Name field from External Authentication shouldn't allow 'space' when the protocol is SAML.
966728	Minor	GUI	SAML Organization field for SAML Role configuration doesn't accept space + umlaut characters.

Bug ID	Severity	Module	Description
964794	Minor	GUI	For user defined rules/reports, the user cannot move rules or reports to a new custom folder without creating a copy.
963867	Minor	GUI	Malformed IP address can be successfully imported from .CSV file without error checking.
957400	Minor	GUI	CMDB Report - Rule query - Scope attribute only takes integer, but needs string.
927769	Minor	GUI	GUI allows invalid / character to be added in port field for FortiOS credentials.
887630	Minor	GUI	Widget Setting as Single Line Chart and Display Type as Text - COUNT(Matched Events) displays no count.
628705	Minor	GUI	It is better to disable 'Test' button for OKTA authentication policy instead of showing 'IP/Host is required'.
970976	Minor	Parser	In 'PH_SYSTEM_IP_EVENTS_PER_SEC' event, Reporting Device is set incorrectly.
966727	Minor	Parser	For Amazon AWS CloudWatch, CMDB is populated for each discovered device.
974448	Minor	phMonitor	Disaster recovery setup may fail with 1 hour timeout, if CMDB replication takes a long time (resulting from CMDB being large and network bandwidth being slow).
968131	Minor	Query	Query using `DevicetoCMDBAttr` does not return any result for custom property.
965081	Minor	Report	In PDF Report, legend may not always show.
971810	Minor	System	`phziplogs` does not pull `phoenix-x.log` due to file format change from `phoenix.log.x`.
966773	Minor	System	Collector fresh-install needs internet to uninstall `rpcbind`.
972752	Minor	Windows Agent	Windows Agent reports "Disk Full" for Optical Drives.
954108	Minor	Windows Agent	Agent can't talk to Collector (verification fails) when Collector has a TLS certificate.
964501	Enhancement	ClickHouse Backend	Generate an incident and system error when free disk of ClickHouse is lower than 20%.
961884	Enhancement	ClickHouse Backend	Enhancement - Procedures for incrementally adding ClickHouse storage.

Bug ID	Severity	Module	Description
972486	Enhancement	Data work	Add rule/report for Apache ActiveMQ Ransomware Attack.
971135	Enhancement	Data work	Netflow dashboards do not include all relevant traffic.
967829	Enhancement	Data work	Windows - Need to parse Logon GUID to `userID` instead of `machineGUID`.
966160	Enhancement	Data work	Need to enhance FortiEDR Rule and event parsing.
964446	Enhancement	Data work	FortiGate Events generated with logID 0100044545 needs to be parsed as `FortiGate-event-admin-delete`.
963543	Enhancement	Data work	Missing column 'appServerState' when loading Application Server dashboard.
962882	Enhancement	Data work	Update Carbon Black CEF parser.
939482	Enhancement	Data work	HPiLoParser Unknown Event due to different syslog header format.
936650	Enhancement	Data work	PANOS parser enhancement needed to parse original VM name from Panorama logs.
916555	Enhancement	Data work	'Group Policy Object Created/Modified' rules have the same event type filter.
912298	Enhancement	Data work	Parse device hostname for FortiAuthenticator parser.
869437	Enhancement	Data work	Update Zscaler log integration in JSON format.
850455	Enhancement	Data work	Update KasperskyParser, update RegEx.
964471	Enhancement	Generative AI	In ChatGPT audit log, provide visibility of user and org ID.
969605	Enhancement	Performance Monitoring	`mib2xml` enhancements to handle Dell iDRAC.
963416	Enhancement	Rule Engine	Sometimes `phRuleWorkers` drops events, while load is light and has CPU and memory resources.

Known Issue

After upgrading to 7.1.1, in ClickHouse based deployments, searching on IP fields (namely, Reporting IP, Source IP, Destination IP, and Host IP) does not show correct results *for events stored prior to upgrade*. Events are still stored in ClickHouse, but searches on events *before* the upgrade do not return results, while searches on events stored *after* the upgrade work correctly. All other searches work correctly.

This issue is related to a recent change in ClickHouse version 23.3 in how IPV6 fields are represented. See the following URLs for more information.

- https://github.com/ClickHouse/ClickHouse/issues/58885
- https://github.com/ClickHouse/ClickHouse/issues/56487
- https://github.com/ClickHouse/ClickHouse/pull/57707
- https://github.com/ClickHouse/ClickHouse/issues/54162

Workaround

The workaround requires recreating old indices involving Reporting IP, Source IP, Destination IP, and Host IP that were created before the 7.1.1 upgrade. In our experiments, Fortinet has not seen any event loss or FortiSIEM service interruption during this process.

1. Go to root shell by running the following command:
   ```
   sudo -s
   ```
2. Change directory to `/tmp` by running the following command:
   ```
   cd /tmp
   ```
3. Run the following command:
   ```
   clickhouse-client
   ```
4. Ensure that `/data-clickhouse-hot-1` has at least 10% free disk space. This space is required during index re-creation (Step 5 below). If free disk space is less that 10%, then run the following SQL command (4a.) to get the list of oldest ClickHouse partitions residing on the `/data-clickhouse-hot-1` disk and either move them to another disk or tier, or delete them until `/data-clickhouse-hot-1` has at least 10% free disk space. **These commands need to be run only on ALL data nodes in every shard.** The first command (4a.), identifies the largest partitions on the `/data-clickhouse-hot-1` disk. The remaining commands enable you to move the data to another tier (4b.), or another disk (4c.), or delete the data (4d.).
   a. Identify the largest ClickHouse partitions in Hot node:
      ```
      SELECT disk_name, partition, extract(partition, '\(\d+,(\d+)\)') as date,
      formatReadableSize(sum(bytes_on_disk)), formatReadableSize(sum(data_uncompressed_
      bytes)) FROM system.parts WHERE (table = 'events_replicated') AND path LIKE
      '%hot-1%' AND active GROUP BY disk_name, partition ORDER BY disk_name ASC, date
      ASC limit 10
      ```
   b. Move the data to another tier:
      ```
      ALTER TABLE fsiem.events_replicated MOVE PARTITION <partition expression from (a)
      > TO VOLUME <next tier>
      ```
   c. Move the data to another disk:
      ```
      ALTER TABLE fsiem.events_replicated MOVE PARTITION <partition expression from (a)
      > TO disk <another disk>
      ```
   d. Delete the data:
      ```
      ALTER TABLE fsiem.events_replicated DROP PARTITION <partition expression from
      (a) >
      ```
      Example:
      Output from command in 4a.:

disk_name	partition	date	formatReadableSize(sum(bytes_on_disk))	formatReadableSize(sum(data_uncompressed_bytes))
default	(18250,20240115)	20240115	229.96 MiB	3.98 GiB
default	(18250,20240116)	20240116	399.59 MiB	6.92 GiB
default	(18250,20240118)	20240118	8.58 MiB	208.72 MiB
default	(18250,20240119)	20240119	1.87 MiB	43.64 MiB
default	(18250,20240120)	20240120	1.89 MiB	43.93 MiB
default	(18250,20240121)	20240121	1.88 MiB	44.12 MiB
default	(18250,20240122)	20240122	1012.05 KiB	22.46 MiB

To move the first partition (size 3.98 GiB) to Warm tier, issue the following command as shown in 4b.

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION (18250, 20240115) TO VOLUME
'warm'
```

To move the first partition (size 3.98 GiB) to another disk in Hot tier, issue the following command as shown in 4c.

```
ALTER TABLE fsiem.events_replicated MOVE PARTITION (18250, 20240116) TO disk
'data_clickhouse_hot_2'
```

To delete the first partition (size 3.98 GiB), issue the following command as shown in 4d.

```
ALTER TABLE fsiem.events_replicated DROP PARTITION (18250, 20240116)
```

5. Run the following commands sequentially. This will drop/add/recreate all affected indices: Reporting IP, Source IP, Destination IP, and Host IP within ClickHouse. **These commands need to be run only on one data node per shard.** Note that the first command (drop) in every index may take some time to complete. User must wait until it completes before issuing the next command.

```
alter table fsiem.events_replicated drop index index_reptDevIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_reptDevIpAddr_bloom_filter
reptDevIpAddr TYPE bloom_filter GRANULARITY 5 AFTER index_customer_set
alter table fsiem.events_replicated materialize index index_reptDevIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_srcIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_srcIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'srcIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
collectorId_set
alter table fsiem.events_replicated materialize index index_srcIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_destIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_destIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'destIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
index_srcIpAddr_bloom_filter
alter table fsiem.events_replicated materialize index index_destIpAddr_bloom_filter

alter table fsiem.events_replicated drop index index_hostIpAddr_bloom_filter
alter table fsiem.events_replicated add INDEX index_hostIpAddr_bloom_filter metrics_
ip.value[indexOf(metrics_ip.name, 'hostIpAddr')] TYPE bloom_filter GRANULARITY 5 AFTER
index_user_bloom_filter
alter table fsiem.events_replicated materialize index index_hostIpAddr_bloom_filter
```

What's New in 7.1.0

- New Features
- Key Enhancements
- New Device Support
- Device Support Enhancements
- Bug Fixes and Enhancements
- Known Issues

New Features

- Fortinet Advisor
- Scheduled Rules for ClickHouse based Deployments
- Windows Certificate Monitoring via Agent
- Windows Osquery via Agent
- User Alias in Risk Calculation
- New Machine Learning Models

Fortinet Advisor

This release introduces OpenAI/ChatGPT-4 powered Advisor that provides the following functions:

Note: In 7.2.0 and later, Fortinet Advisor is known as FortiAI.

- **Responses to SOC Queries** by running an API. Currently, the following questions are supported.
  - *Get FortiSIEM health* – This retrieves the current health of FortiSIEM nodes including Supervisor, Worker and Collector.
  - *Get the latest known vulnerabilities* – This retrieves the list of vulnerabilities in your environment known to FortiSIEM. To get this data, you must enable FortiSIEM to collect data from FortiClient/EMS or vulnerability scanners.
- **Responses to Questions** from 7.1.0 Product documentation and internal knowledge base articles.
- **Analysis and Recommendations for logs and Incidents**: From **Incidents > List View**, **Incidents > Risk**, **Incidents > Investigation** and **Analytics > Search** pages, you can launch these requests using the Fortinet Advisor menu option. Incident analysis provided by OpenAI/ChatGPT-4 can be added to Incident Comments.
- **Automated Incident Analysis and Recommendation** using the Notification policy framework. Incident Notification email can be configured to include Incident analysis provided by OpenAI/ChatGPT-4.

- **Help in building a FortiSIEM Report**: You can ask the Fortinet Advisor to “Create a report”. After the report has been generated, the report can be uploaded to **Analytics** at the click of a button and subsequently run. You can also create a rule once you are satisfied with the Report.

Important Notes:

- Fortinet Advisor uses GPT3.5-Turbo and GPT4. Your OpenAI API key must support access to these models.
- When asking Advisor to build a report, you can describe the report using natural language, but certain keywords need to be present for accuracy. The syntax is as follows and the keywords are in bold: **Create a report** to **show** the <*comma separated list of attributes*> **where** <*filtering conditions*>, **group them by** <*list of event attributes*>, and only **show results for** <*having conditions*>, **order by** <*attribute*> in **ascending** or **descending order**. Grouping and ordering is optional. Several examples are provided in the Advisor GUI.
- For SOC Queries, you always have to use the exact question: “*Get FortiSIEM health*” and “*Get the latest known vulnerabilities*”.
- Anonymization: When you ask ChatGPT for log and Incident analysis using the Fortinet Advisor menu option, then customer specific information is anonymized before sending to ChatGPT. The returned results are converted back to the original values before displaying to the user. The full list of anonymized event attributes is here. Similar anonymization is performed when you invoke ChatGPT via Notification policy. If you manually enter log and ask ChatGPT to analyze the log, then the log fields are not anonymized.

OpenAI Integration and Disclaimer

The Fortinet Advisor lets you connect FortiSIEM to your own OpenAI account, using your own OpenAI license key. This integration will send data from your FortiSIEM to OpenAI and will show you responses from OpenAI. Fortinet does not verify or correct these responses and has no responsibility for them. OpenAI is operated by a third party, not Fortinet. You must exercise discretion and independently verify any information or recommendations you receive from OpenAI before relying on them.

Note: Fortinet Advisor uses GPT3.5-Turbo and GPT4. Your OpenAI API key must support access to these models.

For details on using the Fortinet Advisor, see here.

Scheduled Rules for ClickHouse based Deployments

This release allows users to create Incidents by running reports on periodic intervals. This is only supported for ClickHouse based deployments. In contrast to the current in-memory streaming rule engine, Scheduled rules require disk access and does not scale comparably. In-memory option is faster and a large number of rules can be evaluated concurrently. However, the new scheduled report-based approach has the following advantages:

1. Rules can be written using the complex analytic functions introduced in 7.0.
2. Rules can be evaluated over larger time intervals.

Once the scheduled rule conditions are met, Incidents are created the same way as Streaming rules.

For steps on how to define scheduled rules, see Creating a Rule.

A ClickHouse Query Management layer is introduced to enforce a priority-based scheduling between 3 types of queries: Interactive GUI queries (highest priority), Scheduled Rules (medium priority), and

Scheduled Reports (lowest priority). The status of currently running ClickHouse queries can be seen on the Query Status page.

Windows Certificate Monitoring via Agent

This release enables FortiSIEM to monitor certificates on Windows hosts via FortiSIEM Agent 7.1.0 and later. The following use-cases are handled:

- Detect when a certificate is added or deleted.
- Detect when a certificate has 7-30 days (configurable) left before expiration.
- Report on certificates that have expired (Can notify "X" number of days after certificate has expired, "X" being configurable).
- Detect self-signed certificates.

Steps on how to create a Certificate Monitoring Template and distribute to Windows agents is described in Define the Windows Agent Monitor Templates. Sample logs are available here.

Windows Osquery via Agent

Osquery (https://osquery.readthedocs.io/en/latest/) enables you to collect a variety of information from hosts. The osquery framework provides the following key advantages over logging, and can be used effectively *in addition* to log analysis.

- Osquery can provide information that is not necessarily available in logs, for example the programs that run when a machine starts up, the TCP/UDP ports that are tied to services, etc...
- Hosts can be queried for live information using osquery. This can be very useful in Incident investigations.
- Osquery is Operating system independent – the same Osquery can work for Windows and Linux. Note that FortiSIEM currently supports Osquery for Windows only.

In this release, the osquery framework is integrated into FortiSIEM Windows Agent 7.1. When the 7.1 agent installs, or you upgrade to the 7.1 version, the osquery feature is available.

- A built-in set of osqueries is provided (**Resources > Osquery**), and you can create and test your own osquery.
- An osquery can be attached to a Windows monitoring template, along with other logging and performance monitoring definitions. When the template is assigned to hosts, each host will run the osquery at specific intervals and send the osquery results as FortiSIEM events (prefixed with `PH_OSQUERY_WIN`). The events can be used in Rules and Reports. Lookup Tables can be populated using these events and Rules can be written using the Lookup Tables.
- Reports for built-in osqueries are in **Resources > Reports > Osquery**. Built-in Rules for osqueries can be found by searching for “osquery” in **Resources > Rules** in the main pane.
- The user can also run live osqueries from **Incident Investigation** View. The osquery will collect the current matching data from the hosts. The results can be saved to PDF and attached to Cases.

For steps on how to create an osquery, see here. To attach an osquery to a Windows Monitoring template, see here. Running an osquery from an Incident Investigation graph is a selectable option under Run Reports.

User Alias in Risk Calculation

Often times, a user can have multiple accounts, e.g. Active Directory, AWS, Office 365, email. This release provides a way to define aliases for the main user account in **CMDB > User> Edit > Alias**. FortiSIEM calculates the Total Risk for that user by including the incidents in which aliases appear.

New Machine Learning Models

This release adds two new Anomaly Detection Machine Learning models:

1. **Gaussian Model** - This unsupervised machine learning model approximates the probability distribution of an event attribute as a Gaussian distribution. A data point is considered anomalous if its occurrence probability is lower than the provided threshold.
2. **Gaussian Mixture Model** - As a generalization of the Gaussian model, this unsupervised machine learning model approximates the probability distribution of an event attribute as N Gaussian distributions. This is useful for modeling event attributes which has multiple peaks and valleys. A data point is considered anomalous if its occurrence probability is lower than the provided threshold.

For Details, see Anomaly Detection.

Key Enhancements

- OS Update
- FortiSIEM GUI Enhancements
- Dynamic Watchlist using User-to-IP Lookup
- Kafka Event Collection Improvements
- ClickHouse Storage Reduction for Existing Deployments
- Windows Agent GUI Enhancement
- Ability to Choose a Network Interface during Installation
- Public REST API Enhancements
- Generic STIX/TAXII 2.1 Integration for collecting External Threat Intelligence
- Content Update

OS Update

This release includes published Rocky Linux OS updates until October 24, 2023. The list of updates can be found at https://errata.rockylinux.org/.

FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until October 24, 2023. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux

versions by following the procedures described in https://docs.fortinet.com/document/fortisiem/7.0.0/fortisiem-os-update-procedure/574280/fortisiem-os-update-procedure.

FortiSIEM GUI Enhancements

This release contains several GUI enhancements:

- New consistent color scheme throughout the GUI for both Light and Dark themes.
- In the following Views, Incident detail is presented in a slide-in window from the right:
  - Incident List View
  - Incident Explorer View
  - MITRE ATT&CK Incident Explorer View
  - Incident Overview drill-down View
  - Incident Risk drill-down View
- In Incident List View, the Actions list is streamlined.
- Added a Check Reputation action for IP, Domain, URL and Hash.
- In Widget dashboard, the re-arranging of widgets is optimized. When a widget is moved from one position, the GUI shows the tentative new placement based on current position and minimizes widget movements after placing the widget in the new position.

Dynamic Watchlist using User-to-IP Lookup

There are situations where a rule triggers with only username, but remediation requires the current IP address of the user. This release provides a way for FortiSIEM to update an IP based watchlist when a rule triggers, based on the Username to IP mapping information in the Identity and Location database.

When you define a rule, you can create an IP based Watchlist even if the Rule does not have IP as an event type attribute. In **Resources > Rules**, when adding or editing a rule, go to **Step 3: Define Action**, click the **Watch List** Edit icon, and select the `LookupIpByUser` function to populate a watch list. FortiSIEM will keep track of the User to IP mapping in the Identity and Location database. If it finds an IP mapping for that User, then it will add the matching IP to the watchlist. Some important sub-cases are handled, such as

- If some other user takes that IP, then that IP is removed from the Watch List.
- If the offending user takes some other IP, then the Watch List is updated with the new IP.

Kafka Event Collection Improvements

Two improvements were done:

- **Event Collection scalability** by enabling multiple collectors to pull on the same Topic.
- **Encryption via SASL/SSL via GUI** – This feature was added to 6.7.6 and 7.0.1, but the configuration was via `phoenix_config.txt`. In this release, this configuration option is added to the GUI. If you are using this feature in 6.7.6 or 7.0.1 and upgrade to 7.1.0, you need to navigate to **Admin**

> Settings > System > Kafka in FortiSIEM GUI, change **Protocol** from `PLAINTEXT` to `SSL` and re-do Test Connectivity.

ClickHouse Storage Reduction for Existing Deployments

If you are running ClickHouse as your event database and upgrade to FortiSIEM 7.1.x, then the new events will be compressed more efficiently using ZSTD, while the old events will remain compressed using LZ4. All the events can be queried. As the older events gets purged over time, all event data will be compressed using ZSTD and the full compression potential of ZSTD will be achieved.

Windows Agent GUI Enhancement

This release enables the user to choose the network interface over which the Windows Agent will communicate with the Supervisor and Collector nodes.

For details, see the 7.1.x Windows Agent Guide.

Ability to Choose a Network Interface during Installation

In earlier releases, FortiSIEM always chose `eth0` as the primary network interface for both hardware appliances and virtual machines. This release allows you to choose *any* configured network interface, including bonded interfaces, during FortiSIEM install process.

For details, see your specific hardware or virtual machine installation guide in the FortiSIEM Document Library.

Public REST API Enhancements

The performance of the following CMDB APIs were improved:

- `/phoenix/rest/cmdbDeviceInfo/devices`
- `/phoenix/rest/cmdbDeviceInfo/devicesByPagination`
- `/phoenix/rest/config/Domain`

A new API is introduced to query archived events:

- `/phoenix/rest/query/archive`

A new API is introduced to get IP/Host/User Context

- `/phoenix/rest/context/ip`
- `/phoenix/rest/context/hostname`

- `/phoenix/rest/context/user`

A new API is introduced to query CMDB data. In other words, the API enables you to run CMDB Reports via API.

- Get the schema: `/phoenix/rest/query/cmdb/schema`
- Run a CMDB Query: `/phoenix/rest/query/cmdb`

Generic STIX/TAXII 2.1 Integration for collecting External Threat Intelligence

This release adds a python script for Collecting External Threat Intelligence feeds from any STIX/TAXII 2.1 Server. Currently supported Indicators include IP, Domain, and URL.

To use this integration, simply select **Plugin Type** as `Python` and **Plugin Name** as the script `stix21_threadfeed.py` from the Update Malware IP/Domain/URL dialog.

For details, see Custom Threat Feed Websites - Programmatic Import via Python for Malware Domain, Malware IPs, or Malware URLs.

Content Update

Each built-in Report has a Data Source field that specifies the device integration required for this report to have content. Each built-in Rule has 3 new fields: Data Source, Detection Technology and Evaluation Mode. The Data Source field specifies the device integration required for this rule to trigger. Detection Technology can be one of the following values: Correlation, Profiling, Machine Learning and Correlation Using Lookup Table. Evaluation Mode is either Streaming or Scheduled.

The SIGMA rules are now updated to match the latest from the website (https://github.com/SigmaHQ/sigma/tree/master/rules).

See here for the new rules.

See here for the new reports.

New Device Support

This release adds the following device support:

- G42 Cloud (https://www.g42cloud.com/#/) - log collection. See here for details.
- FortiNDR Cloud - log and alert collection. See here for details.
- Armis Intelligence Platform (https://www.armis.com/) - alert collection. See here for details.
- Hillstone Firewall (https://www.hillstonenet.com/) - log collection. See here for details.

Device Support Enhancements

This release provides following enhancements to already supported devices:

- Microsoft Office365
  - Email Activity Counts via Microsoft Graph API
  - Email statistics via Office 365 Reporting Web Service
  - New rules, reports and dashboard

  See here for details.
- AlienVault TAXII Server 2.1 API (https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html) to download threat intelligence information. See here for integration details.

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
954115	Major	App Server	When host status=UEBA and template configuration with only 'UEBA' is applied, then a Device license is counted.
951833	Major	ClickHouse Backend	NFS Real Time Archive for ClickHouse does not work.
953340	Major	GUI	GUI throws error when a requestor tries to activate or deactivate one rule in Enterprise mode.
955478	Major	Linux Agent	Linux Agent is auditing its own processes and system calls - resulting in large number of useless events.
951156	Major	System	In some situations, ReportWorker to ReportMaster communication issues can cause Data Manager to drop events.
953313	Minor	App Server	Audit log is not generated when rule is activated or deactivated in Enterprise mode.
953181	Minor	App Server	`PH_UPDATE_RULE_SUCCEED` audit event does not have correct ruleName event attribute, when rule is deleted (added is OK).
949130	Minor	App Server	Description column not included when importing watchlist.
944462	Minor	App Server	PDF/CSV Export fails for "Rules with Exception" CMDB Report.
937174	Minor	App Server	Upgrade and Content Updates may not complete as jobs show status as 'InWaiting'.
936858	Minor	App Server	Error occurs when disabling/enabling a new created event dropping rule.
936635	Minor	App Server	Can't update content version to 409 if content version is not configured to 400.
936224	Minor	App Server	Backend LDAP Authentication Events Shown as Unknown Events in Analytics.
930437	Minor	App Server	PostgreSQL log files are growing in number when DR has issue - create a log when this happens.
928788	Minor	App Server	Scheduling a report to run in the future runs after saving the schedule.
926547	Minor	App Server	Public Watchlist REST API (`POST /phoenix/rest/watchlist/save`) is not working.
923582	Minor	App Server	Public REST API `/phoenix/rest/device/update` returns error when updating a specific device.

Bug ID	Severity	Module	Description
923081	Minor	App Server	Public REST API to update CMDB Device System property returns NullPointer Exception.
920602	Minor	App Server	Public REST API for device maintenance (`/phoenix/rest/deviceMaint/update`) returns status code 500 even though it successfully created a maintenance schedule.
915524	Minor	App Server	Cases tab - Export Summary for all tickets is limited to 30 entries.
902079	Minor	App Server	Periodic updates are not working for AlienVault Malware Hash.
887393	Minor	App Server	FortiSIEM Incident Tags not being reflected in Incident JSON when pulled via Rest API.
881550	Minor	App Server	Malware Domain (AlienVault) doesn't pull all the domain values from AlienVault's response.
876052	Minor	App Server	Global Org view permission not honored from dashboard widget and drill down when `phEventCategory` is part of the query.
874420	Minor	App Server	Custom dashboard cannot be shared with AD group role user.
814006	Minor	App Server	Cloud Health shows wrong info after 6.5.0 for Supervisor with two NICs.
954731	Minor	App Server,GUI	Global constraint using simple function in rule is not working properly.
860610	Minor	App Server,GUI	Read-only user can still modify some values due to improper access controls.
940119	Minor	ClickHouse Backend	ClickHouse internal logs (trace_log, part_log, asynchronous_metric_log, query_log) grow to take up significant storage.
888575	Minor	ClickHouse Backend	ClickHouse encounters Signal 8 segmentation fault when all nodes in a shard are deleted.
958249	Minor	Data work	FortiGate Parser Event Type Spelling Error for NTP Status Events.
955723	Minor	Data work	Drilldown from the Server Dashboard -> Logins -> Account Lockouts widget leads to the wrong report.
932909	Minor	Data work	GitlabLogParser not functioning properly.
932801	Minor	Data work	Update Cisco Umbrella DNS parser.
904038	Minor	Data work	Update parsing for Win-Security-5136.

Bug ID	Severity	Module	Description
946373	Minor	Discovery	LDAP discovery imports contact when email field is configured.
937157	Minor	Discovery	AD Discovery completes, but cmdb GUI does not load (reason: bad group insertion in ph_group table).
958820	Minor	Event Pulling Agents	Agent Manager has high memory when reading large files for Generic AWS S3 integration.
958363	Minor	Event Pulling agents	Missing some Proofpoint events due to vendor's data format changes.
951615	Minor	Event Pulling Agents	For Tenable Security Agent, duplicate events may be seen if `phAgentManager` process is restarted.
949554	Minor	Event Pulling Agents	CrowdStrike event stream is getting reset every 5 minutes.
956515	Minor	GUI	Cases with overlapping incidents does not work. If a Case is opened for an Incident which is already part of a Case, then the existing case is updated.
954050	Minor	GUI	FortiGuard CTS external lookup results not added to result history in Investigation.
934291	Minor	GUI	Altering critical interfaces list in CMDB is only possible for the first selected device.
933843	Minor	GUI	Allow Parser Test to proceed even if there are more than 10 test events.
928561	Minor	GUI	Need to add OMI in **Resources > Remediation**, since Windows Remediation scripts require OMI credential.
946758	Minor	Identity & Location	Sometimes `phIpIdentityWorker` module crashed in `libcurl` module.
915091	Minor	Linux Agent	Linux agent `audit.log` folder filling up with denied write messages for user fsmadmin.
951409	Minor	Machine Learning	Viewing Scatter Plot from Machine Learning > Prepare causes GUI corruption.
951408	Minor	Machine Learning	Report for ML job built from ad-hoc report is saved in Ungrouped folder instead of Machine Learning.
934545	Minor	Notification	Case automatically created from incident without any notification policy configured.
899393	Minor	Notification	No subject line in SMS Incident Notification.

Bug ID	Severity	Module	Description
943849	Minor	Parser	Two `PH_SYSTEM_EPS_ORG` events generated for Super organization when there are Super local collectors.
936757	Minor	Parser	EPS calculation mismatch because (a) unknown events not counted towards license and (b) type casting error.
931868	Minor	Parser	Collector Name is not set correctly in events.
925100	Minor	Query	ClickHouse Queries referring custom network range object returns no data.
937564	Minor	Report	Report Designer only allows one Legend per Page, even if you add multiple Charts to the same page.
952241	Minor	Rule	Occasional NullPointerException error when testing a rule.
925899	Minor	Rule	`phRuleMaster` process crashes due to event size 65k buffer overflow.
938995	Minor	System	In Redis cache and clickhouse, ingestionnodesonline key missing for datamanager and querymaster, causing queries to fail - happens on migrating other databases to ClickHouse.
938739	Minor	System	PostgreSQL symbolic link was missing for psql 13 (6.4.x -> 6.7.2).
938735	Minor	System	Upgrade failed due to httpd process that did not start (6.7.1 -> 6.7.3).
938675	Minor	System	Upgrade to 6.7.4 could not uninstall python package pyyaml (6.6.3 -> 6.7.4).
921597	Minor	System	Reboot extremely slow and /tmp files removal errors after upgrade to v7.0.0.
902108	Minor	System	Installing on VMware ESX8 reports a certificate error.
952305	Minor	Windows Agent	UEBA File printed events comes through as '?' when printing files with Arabic characters.
947196	Minor	Windows Agent	Windows agent events are not parsed, when agent moves from offline > online.
902941	Minor	Windows Agent	Windows Agent always uses Windows proxy settings automatically and ignores /noproxy settings.
954539	Enhancement	App Server	Add Audit log when user runs a query and exports data from GUI.

Bug ID	Severity	Module	Description
951444	Enhancement	App Server	Extend the public Incident API to pull Incidents by specific event types.
937666	Enhancement	App Server	Remove unnecessary elements from Rule and Report Definition XML file during export from GUI.
919278	Enhancement	App Server	Provide IP + User based lockout for shared system accounts.
908586	Enhancement	App Server	FortiSIEM nodes discovered as a separate CMDB Group.
877664	Enhancement	App Server	Handle AlienVault new native API.
808565	Enhancement	App Server	Provide feedback on GUI when importing malware ip/hash, etc. from CSV files.
955721	Enhancement	Data work	Proofpoint parser update for URLs.
958363	Enhancement	Data work	Proofpoint parser needs update.
955949	Enhancement	Data work	Update FortiMail Cloud event parser.
953321	Enhancement	Data work	Enhance Pulse Secure VPN events to parse User, Source IP and Source Country fields.
953213	Enhancement	Data work	Sophos XG Firewall Parser update.
951972	Enhancement	Data work	Win-Sysmon-22-DNS-Query Event needs enhancement.
949904	Enhancement	Data work	Wrong Incident Title - Concurrent VPN Authentications To Same Account From Different Cities.
949563	Enhancement	Data work	Ingestion JSON Formatted Event from BitdefenderGravityZoneParser does not populate Reporting Ip.
947118	Enhancement	Data work	Add case to Generic DHCP Parser to resolve 'unknown' events.
943724	Enhancement	Data work	Fortimanager v7.2.3 parsing fails.
943106	Enhancement	Data work	Update FortiClient parser.
940666	Enhancement	Data work	Update FortiEDR parser.
936898	Enhancement	Data work	Several parsers incorrectly use applicationId of type UINT32 as a string field.
935755	Enhancement	Data work	Need to update UbiquityParser for new event types.
933472	Enhancement	Data work	Parse VMware vSAN Trace Logs.
926545	Enhancement	Data work	Update McAfeeXmlParser Parser.

Bug ID	Severity	Module	Description
925683	Enhancement	Data work	Create two rules for Dragos Worldview IP Traffic.
924510	Enhancement	Data work	FortiGate Parser doesn't parse when FortiGate serial number begins with 'FD'.
911349	Enhancement	Data work	WinOSWmiParser not parsing Application Name as attribute for event ids : 5154, 5158.
901988	Enhancement	Data work	NSX-T events are not being parsed correctly.
885730	Enhancement	Data work	FortiWeb Cloud Parser via syslog.
885316	Enhancement	Data work	Sourcefire2Parser is not parsing the HTTP Response Code field to httpStatusCode in the Raw Event Log.
884548	Enhancement	Data work	FortiAI/NDR parser update.
881333	Enhancement	Data work	Add Support to parse events received from FortiAuthenticator.
879396	Enhancement	Data work	Windows Security Event IDs 1200,1201,1206,1207,1210 are missing fields in 'RequestAuditComponent' via windows agent.
876847	Enhancement	Data work	McAfee Web Gateway parser update.
873640	Enhancement	Data work	Additional SNMP SysObjIds needed for Dell switches.
926726	Enhancement	Discovery	Add support for JBOSS 7.1.
829081	Enhancement	Discovery	For Agent/WMI/OMI - provide user option to set FQDN or shortname in discovery, perf monitoring and logs.
930821	Enhancement	Event Pulling Agents	Enhance HTTPS Advanced Generic Poller to support raw JSON post to support APIs similar to Cortex XDR.
937127	Enhancement	GUI	Add capability to Search on Discover > Include/Exclude Types.
927632	Enhancement	GUI	Allow users to choose number of rows/page in tables.
916266	Enhancement	GUI	Prevent users from changing incident severity category by mistake.
942641	Enhancement	Linux Agent	Add FortiSIEM Linux Agent support for Debian 11 and Debian 12.
941337	Enhancement	Performance Monitoring	Add CPU and Memory Monitoring via SNMP for Huawei VRP.

Bug ID	Severity	Module	Description
922131	Enhancement	Rule	Create a System Error in GUI when FortiSIEM starts to throttle Incidents (Rate limiting threshold is hit).
938679	Enhancement	System	Need to verify FSM RPM before upgrade (6.7.x -> 6.7.7).
938672	Enhancement	System	Clean up old upgrade images from `/opt/upgrade` to save space and make new upgrade succeed.
926490	Enhancement	System	Enhance phziplogs to include `phoenix_config.txt` and dmesg output.
880535	Enhancement	System	Enable Content update Docker Collector.
933390	Enhancement	Upgrade	Before beginning upgrade, ensure that `/opt` has enough free disk for CMDB backup.

Known Issues

1. Kafka encryption via SASL/SSL is set from the GUI. This feature was added to 6.7.6 and 7.0.1, but the configuration was via `phoenix_config.txt`. If you are using this feature in 6.7.6 or 7.0.1 and upgrade to 7.1.0, you need to navigate to **Admin > Settings > System > Kafka** in FortiSIEM GUI, change **Protocol** from PLAINTEXT to SSL and re-do Test Connectivity.
2. Special steps for upgrading 6.2.0 Collector with 7.1.0 Supervisor are required. A bug was introduced in 6.2.0 but fixed in 6.2.1, which will cause the Collector upgrade from 6.2.0 to 7.1.0 to fail, unless the following steps are taken:
   a. Download the upgrade package, `FSM_Upgrade_All_7.1.0_build####.zip`.
   b. Unzip the package:
      `unzip FSM_Upgrade_All_7.1.0_build####.zip`
   c. Go to the upgrade package folder:
      `cd FSM_Upgrade_All_7.1.0_build###`
   d. Decompress the python 3.9 package:
      `tar xf Py39-compiled-install.tar.xz`
   e. Move the python 3.9 folder to `/usr/local`:
      `mv py39/ /usr/local/`
   f. Create symlink for python 3.9:
      `ln -s /usr/local/py39/bin/python3.9 /usr/bin/python3.9`
   g. Continue with upgrade from Supervisor.

What's New in 7.0.4

This release contains the following updates.

- System Update
- Implementation Notes

System Update

This release includes Rocky Linux OS 8.10 patches until March 17, 2025. Details can be found at https://rockylinux.org/news/rocky-linux-8-10-ga-release. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include Rocky Linux 8.10. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

Implementation Notes

Upgrade Related

You may encounter a blank Global Dashboard after upgrading to 7.0.4. There are two workarounds.

1. If you have not upgraded yet, then run the script `updateDashboard.sh` as root on Supervisor before upgrade. You can upgrade after running the script.
2. If you have upgraded to 7.0.4 and then see a blank Global Dashboard, then run the script `updateImportDashboard.sh` as root on Supervisor.

What's New in 7.0.3

This release fixes an important security issue described in Fortinet PSIRT Advisory FG-IR-23-130 impacting Supervisor and Worker nodes.

This release includes published Rocky Linux OS updates until January 16, 2024. The list of updates can be found at https://errata.rockylinux.org/. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until January 16, 2024. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in FortiSIEM OS Update Procedure.

This release also includes the following bug fixes and enhancements.

Bug ID	Severity	Module	Description
914974	Major	App Server	User created Security Incidents auto clear after 24 hours.
991851	Major	Performance Monitoring	`phPerfMonitor` module crashes when both STM and perf monitoring are defined.
993070	Minor	App Server	FortiGuard IOC download may fail because of inability to update malware update history.
992940	Minor	App Server	Incident Resolution Recommendation Engine is learning from its own actions, instead of only learning from user actions.
937174	Minor	App Server	During Upgrade and Content Update, GUI shows many Collector status as 'inwaiting'.
927843	Minor	App Server	Discovering a Windows machine both via FortiSIEM Agent and Fortinet EMS/FGT integration results in duplicate CMDB entries.
968983	Minor	Content Update	Content update fails if there are dashboard widgets in the content update package.
974448	Minor	Disaster Recovery	`phMonitor` may time out if DR configuration takes more than 1 hour.
970075	Minor	Discovery	GitLab discovery failure: Need to use host name as IP does not work during SSL handshake.
958820	Minor	Event Pulling Agents	Agent Manager has high memory usage when reading large files for Generic AWS S3 integration.
971557	Minor	GUI	NullPointerException in the POST SAML response after modifying the idle timeout for Azure user.
966730	Minor	GUI	Name field from External Authentication shouldn't allow 'space' when the protocol is SAML.
966728	Minor	GUI	SAML Organization field for SAML Role configuration doesn't accept space and umlaut characters.
955478	Minor	Linux Agent	Linux Agent is auditing its own processes and system calls - this may result in a very high number of useless events.
963550	Minor	Parser	Collector may stop writing event to buffer after 2 hours if Collectors are unable to offload.
961619	Minor	System	Incorrect `/etc/hosts` configuration during Worker addition may result in larger than normal DNS traffic.
958991	Minor	System	The `factoryreset` procedure on hardware appliances may cause all directories under `/opt` installed from the FSM rpm to be owned by root.

Bug ID	Severity	Module	Description
965077	Enhancement	App Server	Handle AlienVault new native STIX/TAXII 2.1 API.
967927	Enhancement	ClickHouse Backend	Use ZSTD for ClickHouse compression.
958363	Enhancement	Event Pulling Agents	Proofpoint integration misses some events due to Proofpoint API internal JSON structure changes.

What's New in 7.0.2

- Key Enhancement
- Bug Fixes and Minor Enhancements
- Important Notes

Key Enhancement

Storage Space Reduction for ClickHouse Based Deployments

This release reduces the storage space for storing events in ClickHouse based deployments. This is achieved in two ways:

- By removing a derived event attribute that included the list of all parsed attributes. This attribute was added to quickly show all parsed attributes in raw message queries, but required additional storage. Now GUI performs optimized adhoc queries to get this information from ClickHouse database.
- By changing the compression algorithm to Zstandard (ZSTD) level 6. Note that only new installations from 7.0.2 onwards can use the ZSTD level 6 compression. Existing customers will use the current LZ4 algorithm. See the ClickHouse Sizing Guide for new storage requirements.

Bug Fixes and Minor Enhancements

This release includes the following bug fixes:

- Several security related code improvements in Linux Agent area
- Fix for Bug 946202: FortiSIEM Supervisor and Worker makes excessive DNS lookups due to missing entries in `/etc/hosts` file. This bug was introduced in 7.0.0.
- Fix for Bug 934773: The runtime directory of `phAnomaly` process under `/tmp` would be deleted after certain time, resulting in `phAnomaly` process to not run after 10 days. This bug was introduced in 7.0.0.
- phAnomaly process to not run after 10 days. This bug was introduced in 7.0.0.
- Fix for Bug 921597: Reboot may be slow after upgrading to 7.0.0. This bug was introduced in 7.0.0.
- Fix for Bug 948701: Machine Learning Clustering job failed to handle inference output without `hostName` id attribute. This bug was introduced in 7.0.0.

This release includes Rocky Linux OS 8.8 updates until September 3, 2023. The list of updates can be found at https://errata.rockylinux.org/.

FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until September 3, 2023. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in the FortiSIEM OS Update Procedure Guide.

Important Notes

1. For native Elasticsearch and Elastic Cloud deployments, FortiSIEM 7.0.0 or higher supports Elasticsearch versions 7.17 and 8.5. If you are running a lower Elasticsearch version and upgrade to FortiSIEM 7.0.0 or higher, then Elasticsearch Queries will not work. Follow these steps to properly upgrade your infrastructure.
   a. Upgrade FortiSIEM to 7.0.0 or higher.
   b. Upgrade Elasticsearch version to 7.17 or 8.5.
   c. In **Admin > Setup > Storage > Online**, redo **Test** and **Deploy**.
2. AWS Elasticsearch is not supported in FortiSIEM 7.0.0 or higher, since they only support Elasticsearch 7.10, which is lower than the required 7.17.
3. AWS Opensearch is not supported in FortiSIEM 7.0.0 or higher.
4. To support new analytical functions in Elasticsearch, the Painless scripting language is used. See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/modules-scripting-painless.html for reference. If you are running Elasticsearch, then add the following line to the `Elasticsearch.yml` file in every Elasticsearch node and restart the cluster for the changes to take effect. Otherwise, queries will fail.

   ```
   script.painless.regex.enabled: true
   ```
5. 5.x Collector will not work with FortiSIEM 6.7.2 or later. This step is taken for improved security. Follow these steps to make the 5.x Collectors operational after upgrade.
   a. Upgrade the Supervisor to the latest version: 7.0.0 or higher.
   b. Copy phProvisionCollector.collector from the Supervisor to all 5.x Collectors.
      i. Login to Supervisor.
      ii. Run the following command.

      ```
      scp /opt/phoenix/phscripts/bin/phProvisionCollector.collector
      root@<Collector_IP>:/opt/phoenix/bin/phProvisionCollector
      ```
   c. Update 5.x Collector password.
      i. SSH to the Collector.
      ii. Run the following command.

      ```
      phProvisionCollector --update <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
      ```
      iii. Make sure the Collector ID and password are present in the file `/etc/httpd/accounts/passwds` on Supervisors and Workers.
   d. Reboot the Collector.
6. FortiSIEM 7.0.0, 7.0.1 and 7.0.2 cannot be installed with FIPS option.
7. For Windows and Linux Agents monitoring host performance, **CMDB > Monitor Status** tab is not populated in GUI.

8. FortiSIEM 7.0.0 and later API documentation is transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. Fortinet recommends checking this link first for the latest API updates.

What's New in 7.0.1

- Important Notes
- Key Enhancements
- Bug Fixes

Important Notes

1. For native Elasticsearch and Elastic Cloud deployments, FortiSIEM 7.0.0 supports Elasticsearch versions 7.17 and 8.5. If you are running a lower Elasticsearch version and upgrade to FortiSIEM 7.0.0, then Elasticsearch Queries will not work. Follow these steps to properly upgrade your infrastructure.
   a. Upgrade FortiSIEM to 7.0.0.
   b. Upgrade Elasticsearch version to 7.17 or 8.5.
   c. In **Admin > Setup > Storage > Online**, redo **Test** and **Deploy**.
2. AWS Elasticsearch is not supported since they only support Elasticsearch 7.10, which is lower than the required 7.17.
3. AWS Opensearch is not supported.
4. To support new analytical functions in Elasticsearch, the Painless scripting language is used. See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/modules-scripting-painless.html for reference. If you are running Elasticsearch, then add the following line to the `Elasticsearch.yml` file in every Elasticsearch node and restart the cluster for the changes to take effect. Otherwise, queries will fail.

   ```
   script.painless.regex.enabled: true
   ```
5. 5.x Collector will not work with FortiSIEM 6.7.2 or later. This step is taken for improved security. Follow these steps to make the 5.x Collectors operational after upgrade.
   a. Upgrade the Supervisor to the latest version: 7.0.0 or higher.
   b. Copy `phProvisionCollector.collector` from the Supervisor to all 5.x Collectors.
      i. Login to Supervisor.
      ii. Run the following command.

      ```
      scp /opt/phoenix/phscripts/bin/phProvisionCollector.collector
      root@<Collector_IP>:/opt/phoenix/bin/phProvisionCollector
      ```
   c. Update 5.x Collector password.
      i. SSH to the Collector.
      ii. Run the following command.

      ```
      phProvisionCollector --update <Organization-user-name> <Organization-user-
      password> <Supervisor-IP> <Organization-name> <Collector-name>
      ```
      iii. Make sure the Collector ID and password are present in the file `/etc/httpd/accounts/passwds` on Supervisors and Workers.

   d. Reboot the Collector.
6. This release cannot be installed with FIPS option.
7. For Windows and Linux Agents monitoring host performance, **CMDB > Monitor Status** tab is not populated in GUI.
8. FortiSIEM 7.0.0 and later API documentation is transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. Fortinet recommends checking this link first for the latest API updates.

Key Enhancements

- Rocky Linux 8.8
- Optimized Incident Trigger Event Lookup

Rocky Linux 8.8

This release updates Rocky Linux OS to 8.8 and includes published Rocky Linux OS updates until July 14, 2023. The list of updates can be found at https://errata.rockylinux.org/.

FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include fixes until July 14, 2023. Therefore, FortiSIEM customers in versions 6.4.1 and above, can upgrade only their Rocky Linux versions by following the procedures described in https://docs.fortinet.com/document/fortisiem/7.0.0/fortisiem-os-update-procedure/574280/fortisiem-os-update-procedure.

Optimized Incident Trigger Event Lookup

Incident Trigger Event lookup in GUI is optimized for long running Incidents. In previous releases, the trigger events are searched over the First Seen Time and Last Seen Time window, which can be very large, if the incident is constantly triggering and is not resolved. In such cases, GUI may fail to display trigger events. In the new design, for an Incident, the latest 100 trigger events are shown over a maximum 30-day period. For ClickHouse, in addition, the eventType field is stored for every trigger event and used in the queries. Since eventType is a ClickHouse Primary Index, queries are faster (See ClickHouse Index Design), but the additional speedup will impact newer incidents. Consider these examples:

- If 100 trigger events occur in last 1 day, then only these trigger events are shown.
- If 50 trigger events occur in each of last 2 days, then only these trigger events over last 2 days are shown.
- If 1 trigger event occur on each of last 100 days, then 30 trigger events are shown.

Bug Fixes

This release contains the following fixes and enhancements.

Bug Id	Severity	Module	Description
929885	Major	App Server	Test Connectivity & Discovery may get stuck with Database update 0% when a few discoveries are running.
922978	Major	Report	`ReportWorker` on EventDB environments may be slow in processing events and sending summaries to `ReportMaster`.
914571	Minor	Agent Manager	`phAgentManager` process memory grows, while receiving Kafka events, caused by a memory leak in the 3rd party librdkafka module. In this release, librdkafka module has been upgraded to the latest version. Our tests show that a FortiSIEM Collector with 8 vCPU and 24GB memory, can collect up to 4K EPS from Kafka.
923024	Minor	App Server	In GUI, switching user from Super Global to a specific Organization does not work unless the user belongs to all Organizations.
921351	Minor	App Server	Multiple Incident REST API issues are fixed: • JSON APIs return error responses in JSON format, instead of XML format • POST API filtering allow these event attributes: `eventSeverity`, `eventSeverityCat`, `phIncidentCategory`, `incidentStatus`, `customer`, `phCustId`, `incidentReso`, `incidentId` • Two parameters are required for Trigger event queries - `timeFrom` and `timeTo`, to provide response to trigger event queries in reasonable time. These two parameters should not be more than 1 day apart. For details, see FortiSIEM REST API.
918854	Minor	App Server	`AppServer` incorrectly invalidates older log integrity XML data, resulting in these files not written to database.
917625	Minor	App Server	During CMDB Merge for Windows Agents, Windows GUID is considered for merging. This causes two different Windows Servers with different names but same IP or GUID to be merged into the same entry in CMDB.
921662	Minor	Data Purger	Excessive logging by `phDataPurger` when it hits a Value Group lookup error, fills up `/opt` disk.

Bug Id	Severity	Module	Description
921628	Minor	Elasticsearch	In Elasticsearch, the nesting of SUM and IF functions doesn't work when IF operator is (>,<,>= or <=). An example is SUM(IF((Event Severity >= 4),1,0)).
921451	Minor	Event Pulling Agents	Azure for US Govt does not work - (fails with correct credential).
928179	Minor	GUI	Machine Learning Report: Windows Process Interaction Ratio does not display correct data.
927794	Minor	GUI	If a nested function has aggregation but outer function is non-aggregate (e.g. LOG(SUM(X))), then whole function is treated as non-aggregate and included in GroupBY attribute list. This results in an invalid Query.
924367	Minor	GUI	New Entity Risk View in 7.0 shows only 10 Incidents in the time window. Now it shows all Incidents.
919768	Minor	GUI	Two issues are resolved for assigning Custom Design Templates assigned to a Report Folder under **Resources > Reports**: (a) If you are migrating from pre-7.0.0 release and you have Custom Design Templates assigned to a Report Folder under **Resources > Reports**, then Report Design Template migration process will not complete, (b) Cannot assign a custom Report Design Template to a Report Folder.
918931	Minor	GUI	Cannot execute FortiSOAR Playbook and run FortiSOAR Connector from Analytics page.
923667	Minor	Machine Learning	The Machine Learning algorithm fails to predict Incident Resolution for some new Incidents.
921060	Minor	Machine Learning	The Machine Learning algorithm to predict Incident Resolution does not work in Service Provider installations.
929009	Minor	Parser	The EPS in event `PH_SYSTEM_EPS_GLOBAL` is calculated incorrectly.
928414	Minor	Parser	`phParser` CPU may be high if event size is very large. This was noticed when receiving larger than 800KB events.
918150	Minor	System	Upgrade can fail when Rocky Linux OS repo DNS Name resolution fails.

Bug Id	Severity	Module	Description
918654	Enhancement	Parser	Make `phParser` EoL character recognition configurable for TLS syslog. The following `phoenix_config.txt` entry is added: `tcp_syslog_delimiter=0x0a # or 0x00,0x0a`

743793	Enhancement	Parser	Enable SASL_SSL (authentication plus encryption) for Kafka producer and consumer. In this release, there is no GUI support for this. Customer needs to choose SASL_PLAINTEXT on GUI and configure this in `phoenix_config.txt`.
			
			`sasl_ssl_ca_cert=/etc/pki/kafka/ca-cert`
			`sasl_ssl_cert_file=/etc/pki/kafka/client_client.pem`
			`sasl_ssl_key_file=/etc/pki/kafka/client_client.key`
			`sasl_ssl_password=`
			`sasl_ssl_verify=true`
			
			See the **Appendix > Configuration Notes > Editing phoenix_config.txt File** for guidance on changing the file. Specifically, on the Collector, you need to make the same change in 2 places:
			• Change the `/opt/config/phoenix_config.txt` file on the Collector and restart the Collector.
			• Make the same change on `/opt/phoenix/config/collector_config_template.txt`. This ensures that new Collectors registering will get the new parameters and the changes are preserved across upgrades.

914960	Enhancement	Systems	Reduce the number of CMDB backups to 1 per day to conserve space and facilitate upgrade.

What's New in 7.0.0

- Important Notes
- New Features
- Key Enhancements
- Bug Fixes and Enhancements
- Known Issues

Important Notes

1. For native Elasticsearch and Elastic Cloud deployments, FortiSIEM 7.0.0 supports Elasticsearch versions 7.17 and 8.5. If you are running a lower Elasticsearch version and upgrade to FortiSIEM 7.0.0, then Elasticsearch Queries will not work. Follow these steps to properly upgrade your infrastructure.
   a. Upgrade FortiSIEM to 7.0.0.
   b. Upgrade Elasticsearch version to 7.17 or 8.5.
   c. In **Admin > Setup > Storage > Online**, redo **Test** and **Deploy**.
2. AWS Elasticsearch is not supported since they only support Elasticsearch 7.10, which is lower than the required 7.17.
3. AWS Opensearch is not supported.
4. To support new analytical functions in Elasticsearch, the Painless scripting language is used. See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/modules-scripting-painless.html for reference. If you are running Elasticsearch, then add the following line to the `Elasticsearch.yml` file in every Elasticsearch node and restart the cluster for the changes to take effect. Otherwise, queries will fail.

   ```
   script.painless.regex.enabled: true
   ```
5. 5.x Collector will not work with FortiSIEM 6.7.2 or later. This step is taken for improved security. Follow these steps to make the 5.x Collectors operational after upgrade.
   a. Upgrade the Supervisor to the latest version: 7.0.0 or higher.
   b. Copy `phProvisionCollector.collector` from the Supervisor to all 5.x Collectors.
      i. Login to Supervisor.
      ii. Run the following command.

      ```
      scp /opt/phoenix/phscripts/bin/phProvisionCollector.collector
      root@<Collector_IP>:/opt/phoenix/bin/phProvisionCollector
      ```
   c. Update 5.x Collector password.
      i. SSH to the Collector.
      ii. Run the following command.

      ```
      phProvisionCollector --update <Organization-user-name> <Organization-user-
      password> <Supervisor-IP> <Organization-name> <Collector-name>
      ```

iii. Make sure the Collector ID and password are present in the file `/etc/httpd/accounts/passwds` on Supervisors and Workers.

d. Reboot the Collector.

6. In pre-7.0.0 releases, you can define a Report Design Template for an individual Report, a Report Bundle or a Report Folder under **Resources > Reports**. In this release, assigning a Report Design Template to a Report and a Report Bundle works correctly, but *assigning to a Report Folder does not work*. This means:
   - In 7.0.0, you cannot assign a custom Report Design Template to a Report Folder.
   - If you are migrating from an earlier release and you have Custom Design Templates assigned to a Report Folder under **Resources > Reports**, then the pre-7.0.0 -> 7.0.0 Template migration process will not complete. Note that Template migration happens under the hood, when user logs on to the system for the first time after upgrading to 7.0.0. In this case, you will see the following error message, "Another User is updating all Report Templates on this machine. Please try again later.".

   The following workaround is suggested:

   a. Before upgrading, check if you have any Custom Design Templates assigned to a Report Folder. This can be checked in one of two ways:
      - Login to GUI, go to **Resources > Reports**, and visit each folder and see if there is a Custom Design Template defined.
      - Alternatively, you can download a zip file with the bash script from here, SSH to the Supervisor as root, copy the script to `/tmp` and run the command:

        `/tmp/GetCustomFolderReportDesignTemplate`

        If you get "Permission denied" error while running the script, then run the following command as root.

        `chmod 755 /tmp/GetCustomFolderReportDesignTemplate`
      - If there no Custom Design Template defined for a Report folder, then the script output will be "No Custom Folder Report Design Template Found. You may proceed to regular upgrade."
      - If there are Custom Design Templates defined for a Report folder, then the script output will be something like:

        ```
        Found 2 Custom Folder Report Design Templates:
          testFolder1
          testFolder2
        ```

   b. Before upgrading, if there are Custom Design Templates defined for a Report folder, then you need to delete them. This can be done in one of two ways:
      - Login to GUI, Go to **Resources > Reports**, select each folder with Custom Folder Report Design Template, select **More > Report Design** and click "Revert to Default".
      - Alternatively, you can download a zip file with the bash script from here, SSH to the Supervisor as root, copy the script to `/tmp` and run the command:

        `/tmp/RemoveAllCustomFolderReportDesignTemplate`

        The script output will be something like:

        ```
        Deleted 2 Custom Folder Report Design Templates:
          testFolder1
          testFolder2
        ```

   You may proceed to regular upgrade. If you have already upgraded, then reload the GUI.

c. If you have already upgraded without doing the procedures 1 and 2 above, then there are two cases:
   - If you do not have any Custom Design Templates assigned to a Report Folder, then the system will work normally.
   - If you do have Custom Design Templates assigned to one or more Report Folders, then you will see the error when you visit Reports page: "Another User is updating all Report Templates on this machine. Please try again later." In this case, you can download a zip file with the bash script from here, SSH to the Supervisor as root, copy the script to `/tmp` and run the following command:

     ```
     /tmp/RemoveAllCustomFolderReportDesignTemplate
     ```

     The script output will be:

     ```
     Deleted 2 Custom Folder Report Design Templates:
       testFolder1
       testFolder2
     ```

   You may proceed to regular upgrade. If you have already upgraded, then reload the GUI.

   After running the script, simply reload the GUI.

7. This release cannot be installed with FIPS option.
8. For Enterprise deployments, while creating a custom Report Bundle, you will see an Error: *NumberFormat Exception: For input string: "undefined"*. You can close this error and proceed to create the report bundle. The error has no impact.
9. The Report Design Templates from pre-7.0.0 releases will be migrated to the new format as required by the new Visual Report Design Editor in 7.0. If your pre-7.0.0 Report Design Template contained a PDF attachment in the middle of the template, then after migration, the PDF attachment will be moved to the end of the PDF document.
10. For Windows and Linux Agents monitoring host performance, **CMDB > Monitor Status** tab is not populated in GUI.
11. FortiSIEM 7.0.0 and later API documentation is transitioning to https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/. Fortinet recommends checking this link first for the latest API updates.
12. Starting with this release, the following communication ports changed to gRPC protocol. If you deployed firewalls between Workers and Supervisor nodes, then you may need to adjust the firewall policies accordingly.
    - ReportWorker and ReportMaster communicate on port 27934
    - QueryWorker and QueryMaster communicate on port 27918
    - RuleWorker and RuleMaster communicate on port 27922

    For details, see here.

New Features

This release contains the following new features:

- Visual Report Designer
- New Query Functions
- Machine Learning Workbench

- Incident Investigation Workspace
- Built-in Machine Learning Models
- ClickHouse Event Integrity
- Fortinet Security Fabric Discovery
- FortiEMS Discovery
- FortiEMS Endpoint Tagging
- Windows Agent 5.0.0
- Linux Agent 7.0.0

Visual Report Designer

This release provides a report design editor that shows how the report will look in the PDF document. This is often referred to as a WYSIWYG (What you see is what you get) editor. All the features in the current report designer are available with the following exceptions:

- Sub-section from earlier versions is not supported in 7.0.0
- An image/text can be placed side-by-side with another item (image/chart/text) in 7.0.0

For details on creating and editing reports using the Visual Report Designer, see Designing a Report Template.

When a user logs in for the first time to an upgraded FortiSIEM 7.0.0, existing pre-7.0.0 report and report bundle templates will be automatically converted to the new format. The new format will be identical to the old format except in one case: if a user chose 2 charts for the same report in the pre-7.0.0 template, then the charts will be placed next to each other with a shared legend, in the new 7.0.0 format. If there are 4 or more charts for the same report in the pre-7.0.0 template, then the new 7.0.0 format will display multiple rows of charts, with 2 charts in one row, and a common legend at the end.

New Query Functions

The following enhancements are provided for querying events:

1. **Aggregation Functions**: COUNT, MEDIAN, MODE, PCTILE, STDDEV, and VARIANCE. These compute specific functions in group-by queries and provide additional insights compared to existing aggregation functions: SUM, AVG, MIN, MAX.
2. **Time Window Functions**: SMA, EMA. These compute simple and exponential moving averages over a time window.
3. **String Manipulation Functions**: LEN, TO_UPPER, TO_LOWER, REPLACE, TRIM, LTRIM, RTRIM, SUB_STR, URL_DECODE. These do various string manipulations and may be needed to regularize string valued event attributes.
4. **Conversion Functions**: TO_INTEGER, TO_DOUBLE, TO_STRING, LOG
5. **Extraction Function**: EXTRACT. This can extract a value from an event attribute, in case the parser missed this attribute in historical data.
6. **Evaluation Function**: IF. This function can be used to set a new variable based on whether a logical condition based on event attributes is true or false.
7. Allow functions to be nested up to 5 levels, e.g. COUNT DISTINCT (TO_UPPER(user)))

These functions are only available for ClickHouse and Elasticsearch Queries. See the full description link below for limitations of nesting operations.There is no support for EventDB queries and rules.

For full description of the functions and examples, see Functions in Analytics.

Machine Learning Workbench

This release provides a workflow for users to create machine learning tasks based on the events stored in FortiSIEM. You can run a report to create a dataset for a machine learning task, and then train FortiSIEM to create a machine learning model. Then you schedule an inference job to run periodically, which can detect deviations from the model and create incidents, or send emails. The model can be re-trained periodically or on demand. 4 machine learning tasks are supported: Regression, Classification, Anomaly Detection and Forecasting. Classification will only work if there is a labeled field in the event. For Forecasting jobs, email is sent instead of creating incidents.

Four machine learning jobs can be run locally on the Supervisor/Worker cluster, or on AWS. Each platform supports different machine learning tasks and algorithms. When run locally, machine learning jobs are distributed across the Supervisor/Worker cluster - this means that any of Supervisor or Worker nodes can do the training and inference jobs. In each mode, the user can choose a specific machine learning algorithm or run in Auto mode, where FortiSIEM tries to choose the best algorithm with the optimal parameters. Auto mode takes longer to train as various algorithms and parameter sets are attempted during the optimization process.

For details on how to create a machine learning job, see Machine Learning.

Incident Investigation Workspace

Currently, users investigate an Incident within the List View. It is not easy in this view to correlate this Incident with other related Incidents and the entities involved. In this release, a separate Incident Investigation workspace is provided in **Analytics > Investigation**. Starting with a root Incident, the user can build a link graph relating that Incident to involved entities (IP, Host, user, process, file) and then recursively to other incidents and related entities. The user can view the timeline of these Incidents and play them in a time ordered fashion to visualize how an attack kill chain is developing. Context is provided for every entity based on information in CMDB, external lookups and events in the FortiSIEM Event Database. It is also possible to run reports, run FortiSOAR playbooks and Connectors to gain further insight into an investigation. Finally, the user can also take a remediation action, create a case locally or in an external ticketing system and clear the Incident. In summary, this Workspace enables the user to stay on this page and fully investigate an Incident and take it to closure.

For details on working with Incident Investigation Workspace, see Investigating Incidents.

Built-in Machine Learning Models

The following specialized Machine Learning models are provided:

1. **Login Anomaly Detection via Bipartite Graph Edge Anomaly Algorithm**

   This release includes a proprietary Machine Learning algorithm that detects login anomalies by learning the user-to-workstation login patterns and forming dynamic peer user groups with similar login patterns. Users and Workstations are represented using a Bipartite graph. In a Bipartite graph, the sets of nodes can be split into two disjoint sets, in such a way that there are no edges between the nodes within the same set. In this example, Users and Workstations form a Bipartite graph, the edge between a User and a Workstation represents a login, and the edge weight represents the number of logins during a time interval.

   This algorithm is part of the FortiSIEM Machine Learning Workbench, introduced in this release. A system defined Machine Learning job including a login report and the Bipartite Graph Edge Anomaly algorithm, is included in this release. The user needs to train the algorithm using the login data from their environment and then schedule the job to run at periodic intervals to detect anomalies. An Incident triggers when an anomaly is detected, along with a visualization of the anomaly.

   For details on the Bipartite Graph Edge Anomaly algorithm, see Anomaly Detection Algorithms for Local Mode.

   For details on how to train and schedule the Login anomaly detection job, see Running Anomaly Detection Local Mode.

2. **Incident Resolution Recommendation**

   FortiSIEM provides 2 attributes to record Incident status

   - **Incident Resolution**: None, True Positive, False Positive
   - **Incident Status**: Active, System Clear and Manually Cleared

   When an Incident triggers, **Incident Status** is Active and **Incident Resolution** is None. There are 3 ways an Incident can get resolved:

   1. If the Incident turns out to be a false positive, then the user can set **Incident Resolution** to False Positive and **Incident Status** to Manually Cleared.
   2. The Incident may clear itself because of a clearing condition in the rule. In that case, **Incident Resolution** is set to True Positive and Incident Status is set to System Cleared.
   3. The Incident may be a real issue. In that case, after working through the Issue, the user can set **Incident Resolution** to True Positive and Incident Status to Manually Cleared.

   In this release, FortiSIEM uses a Machine Learning Classification algorithm to learn the **Incident Resolution** set by the user for Incidents over the last 2 days, and recommends **Incident Resolution** for new Incidents as they happen. The algorithm runs daily at midnight (12AM) to cover Incidents over the last 2 days. Recommendation is done only for new incidents in real time:

   - **Incident Resolution** is set to True Positive or False Positive.
   - A new Incident attribute called **Confidence** (between 0 and 100) is set, with a higher confidence number implying high confidence on the result.
   - **Incident Comment** is updated with the comment "Resolution set by Machine Learning".

Notes:

1. Only **Incident Resolution** is set and **Incident Status** is not modified.
2. This algorithm always runs in the background, and cannot be disabled. It uses a set of Incident attributes as features (including Event Receive Time, Event Type, Reporting Device, Source, Target, Category and MITRE Attack Technique) to make its recommendation.

ClickHouse Event Integrity

This release provides a mechanism to check if event data in ClickHouse has been altered after it is first written to database. This feature is resource intensive and turned off by default. When turned on, checksums are computed per shard and per partition from that day onwards and stored in PostgreSQL database. From **Admin > Settings > Database > Event Integrity**, the user can check the various checksums and ask FortiSIEM to validate them. If some changes were made to the event data, the on-demand checksum would not match the checksum stored in PostgreSQL database.

For details about configuring and validating ClickHouse Event Integrity, see here.

A tool is provided to calculate checksum for historical data. The tool will compute checksums and store them in PostgreSQL database.

Fortinet Security Fabric Discovery

In earlier releases, FortiSIEM can discover a FortiGate firewall via REST API. The attached FortiSwitches, FortiAPs along with the FortiGate firewall and its configuration are discovered. In this release, this discovery is enhanced to a Security Fabric Discovery, where the following *additional* items are also discovered:

- Security Risk Rating for the entire Fabric, if the discovered FortiGate firewall is a Fabric root firewall.
- FortiClient User Store for the discovered FortiGate firewall, which is the list of FortiClient devices passing through the firewall.
- Shallow discovery of other FortiGate firewalls in the Fabric. Shallow discovery includes basic information about the firewall and does not include detailed information such as FortiClient User Store, configuration, etc.

In this release, the recommended way to discover the full Security Fabric is to *individually discover each FortiGate firewall via REST API*. The information from various discoveries is merged and displayed in CMDB.

For details about Security Fabric Discovery, see Fortinet FortiGate Firewall in the External Systems Configuration Guide.

FortiEMS Discovery

In this release, FortiSIEM can discover FortiEMS Servers, managed FortiClient endpoint devices and detailed vulnerabilities for each managed FortiClient endpoint. The vulnerability information is normalized to similar information found by vulnerability scanners.

For details about FortiEMS Discovery, see FortiClient EMS in the External Systems Configuration Guide.

FortiEMS Endpoint Tagging

When an Incident triggers in FortiSIEM and it involves a FortiClient endpoint managed by FortiEMS, then user can associate a tag to the FortiClient endpoint in FortiEMS. A tag can be associated with a rule or manually defined. Tagging/Untagging is done via the remediation framework and can be done Adhoc or automated via the notification policy framework. For automation to work correctly, Fortinet Security fabric Discovery must be performed to associate FortiClient endpoint to the FortiEMS that it is registered to.

For details about FortiEMS endpoint tagging, see the Appendix - FortiEMS Endpoint Tagging.

Windows Agent 5.0.0

1. In previous releases, discovery and performance monitoring for Windows Servers had to be performed via WMI/OMI only, which needed an account to be created on the server for FortiSIEM use. In this release, Windows Agent can perform discovery and performance monitoring, this feature has parity with WMI/OMI based discovery and performance monitoring.

   For configuring discovery and performance monitoring for Windows Agent, see Configuring Windows Agent - Monitor settings.
2. DNS Analytical logs are now collected via real time Events Tracing for Windows (ETW) provider. This is done to overcome an issue with the old design where DNS analytical logs can stop when the log size is full, requiring the agent to restart in order to pick up new analytical logs.

Linux Agent 7.0.0

In previous releases, discovery and performance monitoring for Linux Servers had to be performed via SNMP and SSH only, which needed configuration changes on the server for FortiSIEM to setup SNMP and SSH connections. In this release, Linux Agent can perform discovery and performance monitoring, this feature has parity with SNMP and SSH based discovery and performance monitoring.

For configuring discovery and performance monitoring for Linux Agent, see Configuring Linux Agent - Monitor settings.

Key Enhancements

- Enhanced Entity Risk View
- External Threat Intelligence Integration Enhancements
- Elasticsearch 8.5.3 Support
- FortiGate VDOM Based Mitigation
- Rule Enhancements
- GUI Inactivity Timeout Enforcement
- Miscellaneous Enhancements

Enhanced Entity Risk View

The Risk Page is re-designed to provide more context for impacted entity (user or host) along with an activity timeline. See Risk View for more information on the Risk Page.

External Threat Intelligence Integration Enhancements

Two enhancements are included in this release.

1. A python-based framework that can be used to integrate new threat intelligence sources. For details see Python Threat Feed Framework in the Appendix.
2. GUI to show the health of threat intelligence integrations. Information includes Status, Feed, Last Updated, Pulling Schedule, Integration Type, Action and missed data polls because of errors. This enables users to make sure that integrations are running correctly.

Elasticsearch 8.5.3 Support

This release adds support for Elasticsearch 8.5.3.

FortiGate VDOM Based Mitigation

The FortiGate mitigation scripts now work if FortiGate has Virtual Domains (VDOMs) defined. User provides VDOM information and the script uses the VDOM during execution. See step 4 in Creating a Remediation Action for more information.

Rule Enhancements

1. Ability to compare event attributes within the same event, e.g. Source IP = Destination IP or Source IP != Destination IP.
2. Allow expression on the Right hand side of query/rule operator.

GUI Inactivity Timeout Enforcement

GUI inactivity time out is specified in **CMDB > User > Idle Timeout**. This is correctly enforced in this release. Unless the user is in **Dashboard**, the user is automatically logged out after the specified timeout if the user does not move the mouse or press a key.

Miscellaneous Enhancements

1. Create a CMDB entry for Cloud Service in CMDB and alert when logs are not being received. Host name is used as the IP Address in the logs. Merge discovered Cloud Services in the CMDB if the IP addresses of the service changes.
2. Show Collector ID in the Org Definition screen.
3. Expand AWS S3 Generic Log ingestion to handle multi-line JSON events (if extension is .json.gz or .json).
4. Support SMTP over SSL on ports 587 and 465.
5. Incident and Case PDF Export content improvements.
6. Added heads up display for **CMDB > Users** and **CMDB > Applications** to show the most prevalent users and applications.
7. Create a default **CMDB > Users** group called "FortiSIEM Users" containing administrative users defined locally in FortiSIEM.

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
885349	Major	App Server	FortiGuard Malware URL entries with special characters may result in App Server exceptions, which may fill up disk and the Supervisor may stop.
885206	Major	App Server	User may not be able to login to FortiSIEM Manager, due to excessive incident updates from instances.
880937	Major	App Server	When customer has user defined parsers, parser order may change unexpectedly after content update or regular upgrade.
891289	Minor	App Server	In notification email, Identity and Location lookup data is merged across organizations.
879916	Minor	App Server	Unable to view adhoc queries from the Query Status tab when the online storage is Elasticsearch.
877909	Minor	App Server	In **CMDB > Device**, items cannot be sorted globally.
869411	Minor	App Server	Schedule CMDB Report is blank, if Copy to remote host option is chosen and email setting is not configured.
865069	Minor	App Server	For a user defined via AD Group Role, the manually added Contact information will be deleted after user logs out.
859557	Minor	App Server	Unable to delete user defined Dashboard Slideshow in super/global and orgs.
851691	Minor	App Server	CMDB Report: Sometimes the returned number of rows may depend on the combination of display columns used.
843342	Minor	App Server	Incident Title and name are empty for auto clear incidents triggered by OSPF Neighbor Down Rule.
840694	Minor	App Server	AGENT method disappears from CMDB Discovery Method column when SNMP discovery is re-ran.
803284	Minor	App Server	Customer defined Default email sender in Notification Email gets overwritten after upgrade.
797247	Minor	App Server	A user that logs in via AD Group Role config cannot change the Date Format.
795247	Minor	App Server	A CMDB Device Groups can be deleted if there are devices belonging to this group.
749788	Minor	App Server	Delete/Edit CMDB AD User groups with 100k users fails with 'Undefined' error.
799463	Minor	Data Purger	Detect when Elasticsearch Alias is not created, and then try to create again.

Bug ID	Severity	Module	Description
817151	Minor	Disaster Recovery	When removing Disaster Recovery (DR) from cluster, cloud health page is not cleaned up; it contains the old cluster data.
876027	Minor	Discovery	FortiGate discovery API fails due to missing 'status' parameter on one of the API calls.
801608	Minor	Discovery	SNMP SysObjectId cannot be applied when a system defined 'Device Type' is used.
892781	Minor	Event Pulling Agents	Failed to Pull ELB forwarded logs using AWS-S3-WITH-SQS.
862020	Minor	Event Pulling Agents	Generic HTTPS Advanced Poller incorrectly sets lastPollTime window to local time instead of UTC.
788696	Minor	Event Pulling Agents	Azure Compute not working to government cloud; No Azure instance found.
690309	Minor	Event Pulling Agents	Unable to receive logs from Cloud-based Endpoint Solutions such as Bitdefender GravityZone via API.
912165	Minor	GUI	Interface Usage Dashboard: Wrong interface values are mapped when selecting interfaces from second table.
897192	Minor	GUI	When sorting a column in a Resource folder, then going to another Resource folder without that column, a Query Exception will occur.
895959	Minor	GUI	Searching function in Parser XML Editor does not work properly.
885293	Minor	GUI	Users are incorrectly redirected to 'Password reset page' even though password is still valid.
881317	Minor	GUI	Some UEBA tags are not applied.
862834	Minor	GUI	Application Monitoring does not show the correct message when you click on Monitor from CMDB.
860518	Minor	GUI	In Incident List View, switching incidents before trigger event query finishes will show the old incident's triggered events.
847236	Minor	GUI	Kafka Configuration - GUI shows an error when hostname is being saved as a Kafka broker.
845231	Minor	GUI	Elasticsearch Query that uses 'CONTAIN' with value ending with '\' will not complete.
807427	Minor	GUI	Incident HTTP notification test fails due to ':' in protocol string.

Bug ID	Severity	Module	Description
806694	Minor	GUI	Collector health page does not update 'collector type' column when the value has changed.
796076	Minor	GUI	In org level, **Admin > Device Support > Device Apps** -> Group list shows natural ID of custom group instead of Display names.
792520	Minor	GUI	Bar color in **CMDB> Devices> Summary> Health Overview** does not match with thresholds.
791298	Minor	GUI	VirusTotal connector does not complete when adding 'relationship to include' drop down.
853461	Minor	Linux Agent	Linux Agent fails to start up when IPv6 is disabled on Ubuntu 20.04.5.
905514	Minor	Parser (Data)	FortiGateParser stopped recognizing some FGT messages because of unexpected devid format in log.
893761	Minor	Parser (Data)	WinOSWmiParser parses different 'Process Name' for Security 4624 event.
889725	Minor	Parser (Data)	PaloAltoParser does not parse Source IP, Reason & User for PAN-OS-SYSTEM-generic.
886338	Minor	Parser (Data)	FortiGate parser update because of new devid format.
884941	Minor	Parser (Data)	FortiNAC parser needs to be extended.
877268	Minor	Parser (Data)	Event Type 'Google_Apps_moderator_action_add_user' needs to have more attributes to be parsed.
869873	Minor	Parser (Data)	FortiWeb Event Types contains incorrect description.
865141	Minor	Parser (Data)	Microsoft NPS event not fully parsed.
863302	Minor	Parser (Data)	3 Event Types have severity above 10.
846007	Minor	Parser (Data)	Parsed event type 'SentinelOne-EPP-Generic' missing event attributes.
842119	Minor	Parser (Data)	File Name' attribute incorrect or blank for FortiSandbox Syslog.
840182	Minor	Parser (Data)	WinOSWmiParser does not parse events with id 18456, if there is no user defined at the raw event log.
811131	Minor	Parser (Data)	CiscoIOS Parser has an unknown event.
809815	Minor	Parser (Data)	Palo Alto Threat ID 34261 miscategorized. Should be for cobalt strike, not a benign definition.

Bug ID	Severity	Module	Description
798684	Minor	Parser (Data)	Parse Cisco AMP for Endpoints API V0 raw logs for more information.
754074	Minor	Parser (Data)	Update Microsoft Network Policy Manager Parser for Windows Agent Collection.
907902	Minor	Performance Monitoring	Custom Perf Monitors always returns numerical data as DOUBLE, even when it is specified to be of a different data type.
898371	Minor	Performance Monitoring	Fail to monitor WebLogic 12c memory.
871853	Minor	Query	PctChange function is not working.
861224	Minor	RuleWorker	phRuleWorker randomly crashes due to possible memory corruption.
876849	Minor	System	For Disaster Recovery in EventDB based deployments, if NFS takes a long time to respond, replication health page responds incorrectly.
874222	Minor	System	FortiSIEM install fails since Red Hat hypervisor is not explicitly supported in install scripts.
867999	Minor	System	Changing the IP of the Supervisor using configFSM.sh will cause svn_url to change to repos/cmdb/.
857752	Minor	System	Include all cert formats during the Upgrade certificate backup and restore procedures.
729023	Minor	System	SQLite header and source version mismatch causes upgrade failure.
881225	Minor	Windows Agent	Unable to collect Windows DHCP logs with traditional Chinese characters in DhcpSrvLog-Mon.log.
799857	Minor	Windows Agent	XML key is truncated in Windows security events 1202/1203.
856691	Enhancement	Data	For the scenario - Administrator is added to FortiGate, the event type should be properly parsed and a rule should be created.
814287	Enhancement	DataPurger	Enhance Elasticsearch Event Export tool phExportESEvent to include org ID as an argument.
814145	Enhancement	Event Pulling Agents	Support Gzip compressed files on HTTP POST feature.
813609	Enhancement	Event Pulling Agents	Support Tenable Nessus Security Scanner via Nessus10 API.

Bug ID	Severity	Module	Description
796857	Enhancement	GUI	Support LookupTableGet() and event attribute on right side of Filter condition.
796453	Enhancement	GUI	Azure EventHub integration missing mapping to organization.
878826	Enhancement	Linux Agent	Add support for Ubuntu 22.04 LTS.
868661	Enhancement	Linux Agent	Add support for CentOS 9, RHEL 9 and Rocky Linux 9.
871607	Enhancement	Parser (Data)	Extend FortiDeceptor parser to include MITRE ATTACK TTP information.
845671	Enhancement	Parser (Data)	Event Severity' is not being parsed and evaluated properly in the KasperskyParser.
811438	Enhancement	Parser (Data)	Add support for cronyd events.
802206	Enhancement	Parser (Data)	Add parser for TSV formatted Zeek log.
845685	Enhancement	System	Unable to update FortiSandbox Malware Hash and URL In STIX v2 format.

Known Issues

- General
- ClickHouse Related
- Discovery Related
- Elasticsearch Related
- EventDB Related
- HDFS Related
- High Availability Related

General

See issues mentioned in Important Notes.

ClickHouse Related

1. If you are running ClickHouse event database and want to do Active-Active Supervisor failover, then your Supervisor should not be the **only** ClickHouse Keeper node. In that case, once the Supervisor is down, the ClickHouse cluster will be down and inserts will fail. It is recommended that

you have 3 ClickHouse Keeper nodes running on Workers.

2. If you are running ClickHouse, then during a Supervisor upgrade to FortiSIEM 6.7.0 or later, instead of shutting down Worker nodes, you need to stop the backend processes by running the following command from the command line.

   `phtools --stop all`

3. If you are running Elasticsearch or FortiSIEM EventDB and switch to ClickHouse, then you need to follow two steps to complete the database switch.
   a. Set up the disks on each node in **ADMIN > Setup> Storage** and **ADMIN > License > Nodes**.
   b. Configure ClickHouse topology in **ADMIN > Settings > Database > ClickHouse Config**.
4. In a ClickHouse environment, Queries will not return results if none of the query nodes within a shard are reachable from Supervisor and responsive. In other words, if at least 1 query node in every shard is healthy and responds to queries, then query results will be returned. To avoid this condition, make sure all Query Worker nodes are healthy.

Discovery Related

Test Connectivity & Discovery may get stuck with Database update 0% when a few discoveries are running.

Elasticsearch Related

1. In Elasticsearch based deployments, queries containing "IN Group X" are handled using Elastic Terms Query. By default, the maximum number of terms that can be used in a Terms Query is set to 65,536. If a Group contains more than 65,536 entries, the query will fail.

   The workaround is to change the “max_terms_count” setting for each event index. FortiSIEM has been tested up to 1 million entries. The query response time will be proportional to the size of the group.

   Case 1. For already existing indices, issue the REST API call to update the setting

   ```
   PUT fortisiem-event-*/_settings
   {
     "index" : {
       "max_terms_count" : "1000000"
     }
   }
   ```

   Case 2. For new indices that are going to be created in the future, update fortisiem-event-template so those new indices will have a higher max_terms_count setting

   a. `cd /opt/phoenix/config/elastic/7.7`
   b. Add `"index.max_terms_count": 1000000` (including quotations) to the “settings” section of the `fortisiem-event-template`.

      Example:

      ...

```
"settings": {
  "index.max_terms_count": 1000000,
```

...

c. Navigate to **ADMIN > Storage > Online** and perform **Test** and **Deploy**.

d. Test new indices have the updated terms limit by executing the following simple REST API call.

`GET fortisiem-event-*/_settings`

2. FortiSIEM uses dynamic mapping for Keyword fields to save Cluster state. Elasticsearch needs to encounter some events containing these fields before it can determine their type. For this reason, queries containing `group by` on any of these fields will fail if Elasticsearch has not seen any event containing these fields. Workaround is to first run a non-group by query with these fields to make sure that these fields have non-null haves.

EventDB Related

Currently, Policy based retention for EventDB does not cover two event categories: (a) System events with phCustId = 0, e.g. a FortiSIEM External Integration Error, FortiSIEM process crash etc., and (b) Super/Global customer audit events with phCustId = 3, e.g. audit log generated from a Super/Global user running an adhoc query. These events are purged when disk usage reaches high watermark.

HDFS Related

If you are running real-time Archive with HDFS, and have added Workers after the real-time Archive has been configured, then you will need to perform a **Test** and **Deploy** for HDFS Archive again from the GUI. This will enable `HDFSMgr` to know about the newly added Workers.

High Availability Related

If you make changes to the following files on any node in the FortiSIEM Cluster, then you will have to manually copy these changes to other nodes.

1. FortiSIEM Config file (`/opt/phoenix/config/phoenix_config.txt`): If you change a Supervisor (respectively Worker, Collector) related change in this file, then the modified file should be copied to all Supervisors (respectively Workers, Collectors).
2. FortiSIEM Identity and Location Configuration file (`/opt/phoenix/config/identity_Def.xml`): This file should be identical in Supervisors and Workers. If you make a change to this file on any Supervisor or Worker, then you need to copy this file to all other Supervisors and Workers.
3. FortiSIEM Profile file (`ProfileReports.xml`): This file should be identical in Supervisors and Workers. If you make a change to this file on any Supervisor or Worker, then you need to copy this file to all other Supervisors and Workers.
4. SSL Certificate (`/etc/httpd/conf.d/ssl.conf`): This file should be identical in Supervisors and Workers. If you make a change to this file on any Supervisor or Worker, then you need to copy this file to all other Supervisors and Workers.

5. Java SSL Certificates (files `cacerts.jks`, `keyfile` and `keystore.jks` under `/opt/glassfish/domains/domain1/config/`): If you change these files on a Supervisor, then you have to copy these files to all Supervisors.
6. Log pulling External Certificates: Copy all log pulling external certificates to each Supervisor.
7. Event forwarding Certificates define in FortiSIEM Config file (`/opt/phoenix/config/phoenix_config.txt`): If you change on one node, you need to change on all nodes.
8. Custom cron job: If you change this file on a Supervisor, then you have to copy this file to all Supervisors.

Windows Agent Releases

Some Windows Agent 7.2.x, 7.1.x, Windows Agent 5.x.x, Windows Agent 4.4.x, Agent 4.3.x and 4.2.x features are only supported on FortiSIEM 6.4.0 or later.

Make sure you have the latest content update before installing/upgrading Windows Agent.

Windows Agent 7.2.5

Published November 11, 2024

This release resolves the following issue:

- OSQuery.exe, invoked by the FortiSIEM windows agent, may use significant memory to process event logs (Bug 1090576).

Windows Agent 7.2.4

Published September 11, 2024

This release resolves the following issue:

- DISABLEPROXY setting is not carried over during upgrade (Bug 1071795).
  Note: This fix applies to future upgrades from 7.1.11 or 7.2.4. If you are running a lower version and want to upgrade to 7.1.11 or 7.2.4 and want to keep the proxy settings, then you need to manually enter the following entry to the registry before running the upgrade via the GUI.
  ```
  reg add "HKLM\Software\Fortinet\FortiSIEM" /v DISABLEPROXY /t REG_DWORD /d 1 /f
  ```

Windows Agent 7.2.3

Published August 27, 2024

This release resolves the following issues:

- Sometimes Agent can fail to render message description which can result in the Agent failing to send events to Collector. This behavior has been observed for HyperV logs (Bug 1058897).
- Agent does not correctly send events in case there are multiple Virtual Collectors and name resolution failures. The Agent may get stuck if one Virtual Collector name to IP resolution fails (Bug 1067554).

Windows Agent 7.2.2

Published July 29, 2024

This release resolves the following issue:

- Windows Agent has a memory leak when processing non-security event logs (Bug 1048352).

Windows Agent 7.2.1

Published June 28, 2024

This release contains the following fixes.

- Windows Agent status in FortiSIEM GUI may show "Disconnected" after power cycling the Windows Server (Bug 1037398).
- Double quotes are missing for some attributes in the 'AO-WUA-InstSw-Removed' raw event (Bug 1037186).

Windows Agent 7.2.0

Published June 04, 2024

This release resolves the following issue:

- Windows System Event Log ID 1074 is not reported on Windows restart (Bug 1031491).

Windows Agent 7.1.8

Published June 28, 2024

This release contains the following fix.

- Windows Agent status in FortiSIEM GUI may show "Disconnected" after power cycling the Windows Server (Bug 1037398).

Windows Agent 7.1.7

Published May 01, 2024

This release resolves the following issues:

- Windows Agent leaves a few files in system (C:\Program Files\Fortinet\FortiSIEM) after uninstall (Bug 1018385).
- Windows Agent does not work with multiple Supervisors in High Availability mode, when using Collector Proxy (Bug 1023056).

Note: This requires FortiSIEM 7.1.4 or later with content update 607.

Windows Agent 7.1.6

Published April 12, 2024

This release resolves the following issue:

Windows Agent adds an extra escaping for \ and " characters in the XML event sent to the Collectors. As an example, "C:\\Windows\\ServiceProfiles\\LocalService\\AppData\\Local\\lastalive1.dat" instead of "C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat".

As a result, some rules that use strict file patterns may not trigger (Bug 1016204).

Windows Agent 7.1.5

Published March 25, 2024

This release contains the following fixes.

1. Resolves a situation where Windows System and Application Event Logs can contain empty `<Message>` nodes, resulting in incomplete logs, since `<Message>` contains useful information.
2. The system parser for Windows Agent events in XML format (WinOSXmlParser) has been improved to handle all Event logs. The parsed attributes are now comparable to the Windows OMI based parser. To get this fix, you must also install Content Update version 606 for all FortiSIEM 7.1.x versions.

Windows Agent 7.1.4

Published March 05, 2024

Windows Agent Log Handling Performance Improvement

To better handle larger volume of Windows events (specially Windows forwarded events), FortiSIEM Windows Agent now uses the Windows native XML format to transfer all Windows logs (Security, System, Application, Forwarded Events, etc.) to Collector. A new FortiSIEM Windows event parser (WinOSXmlParser) now parses event attributes directly from XML fields. By transferring the parsing load from Windows Agent to Collector, Agent CPU load is reduced, and the Collector CPU load is slightly increased. Fortinet has not noticed any significant load increases in Collector. From user perspective, only Windows raw message structure changes from FortiSIEM "[Attribute]:Value, [Attribute]:Value" format to Windows XML format.

Since Windows event log structure has changed, all user-written custom Windows parsers should be upgraded to parse XML fields, prior to upgrading Windows Agent. Please follow the parsing logic in WinOSXmlParser to adapt your custom Windows parsers.

An example Security log format change is below. For other examples, see here.

Current Format:

```
2024-02-22T01:07:51Z Win10.acme.com 172.30.56.127 AccelOps-WUA-WinLog-Security
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="72f70ae7-fedf-4dc0-92e7-0c953f46f87e" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [eventName]="Security" [eventSource]="Microsoft-
Windows-Security-Auditing" [eventId]="4703" [eventType]="Information" [domain]=""
[computer]="Win10.acme.com" [user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="Feb 22
2024 01:07:51" [deviceTime]="Feb 22 2024 01:07:51" [msg]="A token right was adjusted."
[[Subject]][Security ID]="S-1-5-18" [Account Name]="GFU-WIN10$" [Account Domain]="ACME"
[Logon ID]="0x3E7" [[Target Account]][Security ID]="S-1-5-18" [Account Name]="ACME-WIN10$"
[Account Domain]="ACME" [Logon ID]="0x3E7" [[Process Information]][Process ID]="0x3348"
[Process Name]="C:\\Windows\\System32\\msiexec.exe" [Enabled Privileges]="" [Disabled
Privileges]="SeRestorePrivilege,SeTakeOwnershipPrivilege"
```

New Format:

```
2024-02-27T21:19:33Z Win10.acme.com 172.30.56.129 FSM-WUA-WinLog-Security [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="1e749ab9-bf6e-
4052-806b-02068b2d4465" [timeZone]="-0800" [extEventRecvProto]="Windows Agent"
[level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-a5ba-
3e3b0328c30d}'/><EventID>4703</EventID><Version>0</Version><Level>0</Level><Task>13317</Ta
sk><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2024-
02-
27T21:19:32.430796700Z'/><EventRecordID>9064813051</EventRecordID><Correlation/><Execution
ProcessID='4' ThreadID='5944'/><Channel>Security</Channel><Computer>FSM-GFU-Windows2019-
WIN2019-172-30-56-129</Computer><Security/></System><EventData><Data
```

```
Name='SubjectUserSid'>S-1-5-18</Data><Data Name='SubjectUserName'>FSM-GFU-
WINDOWS$</Data><Data Name='SubjectDomainName'>WORKGROUP</Data><Data
Name='SubjectLogonId'>0x3e7</Data><Data Name='TargetUserSid'>S-1-0-0</Data><Data
Name='TargetUserName'>FSM-GFU-WINDOWS$</Data><Data
Name='TargetDomainName'>WORKGROUP</Data><Data Name='TargetLogonId'>0x3e7</Data><Data
Name='ProcessName'>C:\\Windows\\System32\\svchost.exe</Data><Data
Name='ProcessId'>0xbdc</Data><Data
Name='EnabledPrivilegeList'>SeAssignPrimaryTokenPrivilege
   SeIncreaseQuotaPrivilege
   SeSecurityPrivilege
   SeTakeOwnershipPrivilege
   SeLoadDriverPrivilege
   SeSystemtimePrivilege
   SeBackupPrivilege
   SeRestorePrivilege
   SeShutdownPrivilege
   SeSystemEnvironmentPrivilege
   SeUndockPrivilege
   SeManageVolumePrivilege</Data><Data Name='DisabledPrivilegeList'>-
</Data></EventData></Event>
```

Windows Agent 7.1.1

Published December 19, 2023

This release resolves the following issues.

1. Improve the memory usage of Windows Agent during event log process restart (Bug 968139).
2. When Collector has a TLS certificate, Windows Agent fails to communicate with Collector certificate verification failure error (Bug 954108).
3. Windows Agent reports Disk Full for (read only) Optical Drives (Bug 972752).
4. The field "Is Certificate Authority" should not show Null for expired certificates (Bug 965418).

Windows Agent 7.1.0

Published November 06, 2023

1. Windows Agent now offers the use of osquery to poll Windows devices. System and user defined osquery templates can be created and executed by Windows Agent on a regular schedule to gather data from Windows devices. For information on osquery, see osquery. For information on configuring osquery, see Configuring Windows Agent step 3j.
2. Certificate Monitoring has been added to give administrators more visibility into certificates that include alerts when an certificate has been added, deleted, is about to expire, and has expired. For information on configuring Certificate Monitoring, see Configuring Windows Agent step 3i.

3. When installing Windows Agent, the user can now select their interface by entering it in the **Network Adapter Name** field in the FortiSIEM LogAgent Setup.

Windows Agent 5.0.1

This Windows Agent release resolves the following issue:

If the Windows Agent loses network connection to the Collector for a period of time, then the performance monitoring events can have unknown event type. This can result in high Collector CPU (Bug 947196).

Windows Agent 5.0.0

This release contains the following features and enhancements:

1. In previous releases, discovery and performance monitoring for Windows Servers had to be performed via WMI/OMI only, which needed an account to be created on the server for FortiSIEM use. In this release, Windows Agent can perform discovery and performance monitoring, this feature has parity with WMI/OMI based discovery and performance monitoring.

   For configuring discovery and performance monitoring for Windows Agent, see Configuring Windows Agent - Monitor settings.
2. DNS Analytical logs are now collected via real time Events Tracing for Windows (ETW) provider. This is done to overcome an issue with the old design where DNS analytical logs can stop when the log size is full, requiring the agent to restart in order to pick up new analytical logs.

Windows Agent 4.4.1

This release includes the following bug fix.

For French locale, Windows Security, System and Application Event logs are incorrectly formatted, leading to important fields not being parsed (Bug 901252).

Windows Agent 4.4.0

This release contains the following new feature and bug fix.

Support for Virtual Desktop Infrastructure (VDI) Environment

Windows Agents can work in VDI environments using the following steps:

1. The administrator first installs the Windows Agent onto the VDI Golden image. See Installing Windows Agent in VDI Environment for details.
2. When user logs on to the VDI environment and downloads a VM from the VDI Server, the VM contains a VDI transient image (containing the Windows Agent). The agent automatically registers to the FortiSIEM Supervisor node, with host name set to <DOMAIN>__<USERNAME> in CMDB.
3. When user logs off from the VDI environment, the agent automatically unregisters to the FortiSIEM Supervisor node. The agent's status is decommissioned, so that it does not consume an agent license.

Bug Fix

Command line arguments in 'new process created' events are lowercased affecting base64 decoding of command line arguments (Bug 873700).

Windows Agent 4.3.0

This release provides the following features and improvements.

Software Installer Improvements

In earlier versions, FortiInsight User Entity Behavior Analysis (UEBA) was installed as a separate package and installer and showed up as a separate Windows service. Starting with this release, FortiInsight runs as an integrated module within FortiSIEM Windows Agent. This also means that FortiInsight will no longer be running in the background when the UEBA license, and template associations are not enabled.

Three installation options are provided: x86 MSI, x64 MSI and a bundled exe that automatically detects the correct MSI to use.

Installation paths, log files and registries have been renamed from AccelOps to FortiSIEM:

- Installation path has been updated from C:/Program Files/AccelOps to **C:/Program Files/Fortinet/FortiSIEM**
- ProgramData paths have been updated from C:/ProgramData/AccelOps to **C:/ProgamData/FortiSIEM/**
- Registry entries have been moved from HKLM/Software/AccelOps to **HKLM/Software/Fortinet/FortiSIEM**
- Log files have been added to **C:/Program Files/Fortinet/FortiSIEM/logs**

- ProxyTrace.log has been updated to **C:/ProgramData/FortiSIEM/logs/Trace.log**
- All libraries have been renamed from AccelOps to FortiSIEM.
  - AccelOps.Common > FortiSIEM.Common
  - AccelOps.Security > FortiSIEM.Security
  - AccelOps.Utilities > FortiSIEM.Utilities
  - AccelOps.WebProxy > FortiSIEM.WebProxy

Robust Detection of Event Log Restart (Event ID 1100)

In previous versions, Event Log restart was detected by tracking the Process ID (PID) of the Windows Event Log service. The assumption is that when Windows Event Log service restarts, the PID gets recycled. In some cases, however, the Windows Event Log “restart” does not recycle the PID, but just invalidates the handles.

This release adds a robust restart check by looking for the security Event ID 1100, which indicates a restart has occurred.

Restart Event Collection from Last Position

In previous versions, event collection starts from Agent startup time. This causes the Agent to miss events, especially in case of restart. In this release, the Windows Agent will store its last processed event and on restart, will begin event collection from that point. Restart will not result in Event loss.

Monitor Software Installed via Microsoft Apps

In previous versions, FortiSIEM Windows Agent would detect installed software when the user installed via standard installation mechanisms such as Control Panel or MSIs. This release adds support for the Microsoft App store, which has become more the standard for installing, and distributing Microsoft software. FortiSIEM Windows Agent 4.3 can now detect installed/removed software when the user installs software via the Microsoft App store.

Windows Agent 4.2.7

This release fixes the following issue.

Windows Agent process stops after enabling UEBA on Windows OS French language pack version (Bug 821479).

Windows Agent 4.2.6

This release fixes the following issue.

Virtual Collector configuration in Windows Agent Host to Template Association does not work correctly. Agent does not send events to the configured Virtual Collectors (Bug 812009).

Windows Agent 4.2.5

This release fixes the following issue.

Windows security logs with XML keyword are truncated. Examples are Windows Security Event ID 1202, 1203 for Active Directory Federation Service (ADFS) (Bug 799857).

Windows Agent 4.2.4

This release resolves the following issue.

Allow the following characters in the Windows Agent user name during registration: space, dollar, plus, minus, dot, at the rate of, underscore, left parenthesis, right parenthesis, in other words, these characters between double quote " $*+-.@_()" (contains space) (Bug 790304).

Windows Agent 4.2.3

This release provides a way to install FortiSIEM Windows Agent so that the Administrator can stop the Agent Service if needed. To accomplish this, the user must install the Agent via the command line with the `UNPROTECT = 1` option. For details, see Installing with the Ability to Stop Agent Service in the Windows Agent Guide.

Windows Agent 4.2.2

This release adds support for the full special characters set in specifying Windows Agent passwords. Supported character set is specified at this website:

https://owasp.org/www-community/password-special-characters

Specifically, it includes (between double quotes): " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~"

These characters can be input both via the Windows Agent command line and the GUI.

Windows Agent 4.2.1

This release fixes the following three issues for FortiSIEM Windows Agent.

1. The Agent may not capture Windows Event Forwarding (WEF) logs when WEF is configured to write forwarded logs to any folder other than the Forwarded Events folder on the forwarded server. In addition, the Agent's performance of WEF log handling is improved. (Bug 766939)
2. The Agent limits the Collectors' name to only 50 characters, which may not work in AWS where FQDN can be long. (Bug 770632)
   Note: The name is now 253 characters.
3. The Agent stops sending logs after killing or restarting Windows Event Log Process. (Bug 744891)

Windows Agent 4.2.0

This release contains two enhancements.

1. A GUI is provided for installing the Agent. See Installing FortiSIEM Windows Agent 4.2.x in the Windows Agent 4.x.x Installation Guide.
2. Ability to upgrade multiple agents in parallel from the Supervisor. See here.

Windows Agent 4.1.6

This release fixes the following three issues for FortiSIEM Windows Agent.

1. The Agent may not capture Windows Event Forwarding (WEF) logs when WEF is configured to write forwarded logs to any folder other than the Forwarded Events folder on the forwarded server. In addition, the Agent's performance of WEF log handling is improved. (Bug 766939)
2. The Agent limits the Collectors' name to only 50 characters, which may not work in AWS where FQDN can be long. (Bug 770632)
   Note: The name is now 253 characters.
3. The Agent stops sending logs after killing or restarting Windows Event Log Process. (Bug 744891)

Windows Agent 4.1.5

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 4.1.4

This release resolves two issues:

1. File handle leak while interfacing with local SQLite database. This can cause Windows Agent memory usage to grow overtime. (Bug 746978)
2. File handle leak while interfacing with Windows registry. This can cause Windows Agent memory usage to grow over time. (Bug 748252)

Windows Agent 4.1.3

This release resolves two issues:

1. When FortiSIEM monitors DNS Analytical logs, Windows EventLog service memory utilization maybe high. (Bug 723147)
2. Windows Agent may stop sending events if both the Supervisor and Collector go down for more than 10 minutes and then come up. (Bug 727842)

Windows Agent 4.1.2

This release adds the ability to work with FortiSIEM Management Extension Application (MEA) Collector released as part of FortiSIEM 6.3.0.

Windows Agent 4.1.1

This release fixes the following issues:

1. Windows Agent does not generate events when a monitoring template is chosen with a large set of comma separated eventIDs. Previous limit of 50 eventIDs or 250 characters is now extended to 1200 characters including comma separating characters. If you need more than this limit, you can always create multiple monitoring templates. (Bug 702090)

2. When Windows Event Forwarding is configured, FortiSIEM Agent running on the forwarded server may sometimes fail to get the message in Security Events. A new API is now used to collect the events from the Windows Forwarded Events folder. (Bug 710074)

Windows Agent 4.1.0

This release adds the following enhancements.

1. Agent will restart automatically after 1 minute if it is killed.
2. Service protection – user cannot Stop, Restart or Pause the agent from Windows Service Manager.
3. Users can change the logging level without restarting service by changing the registry key. Registry key instructions follow:
   a. Open HKEY_LOCAL_MACHINE\SOFTWARE\AccelOps\Agent key
   b. To update with trace logging, set “LogLevel” value to “2”
   c. To update with debug logging, set “LogLevel” value to “1”
4. Agent Database is used to store Agent configuration parameters and to store events when connectivity to collectors is lost. The default size for your Agent Database is 1GB. This can be changed by modifying the MaxDBSizeInMB entry in your Registry Editor.

Details are in the Windows Agent Guide.

Windows Agent 4.0.1

This release fixes three issues:

1. Agent status became disconnected on Windows server 2012R2. (Bug 672660)
2. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
3. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 4.0.0

This release provides User Entity Behavior Analysis (UEBA) by embedding a Kernel Agent that detects anomalies on these 10 user activities.

- Log on and log off
- Machine on and off
- File create
- file delete

- file read
- file write
- file rename
- file move
- file upload
- file download
- drive mount
- drive un-mount

Windows Agent 3.3.1

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 3.3.0

This release fixes the following issue:

Windows Agent fails to send events to Collector after service restart or machine reboot. (Bug 659782)

Windows Agent 3.2.3

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 3.2.2

This release fixes the following issue:

Windows Agent on certain platforms, including Windows10 Pro, may crash while doing File Integrity Monitoring checks. This can cause Agents to get disconnected from FortiSIEM GUI and cause events to stop coming. (Bug 653943)

Windows Agent 3.2.1

This release fixes the following issue:

Windows Agent service stops after a while with File Integrity Monitoring (FIM) turned on. (Bug 636060)

Windows Agent 3.2.0

This release includes several enhancements for File Integrity Monitoring (FIM) when using Windows Agents:

- Detect File Permission and Ownership changes.
- Ability to push monitored files from agents to the FortiSIEM Supervisor where an audit trail of file changes are kept in SVN. The user can then examine the differences between the files.
- Ability to detect file changes from a baseline.

Windows Agent 3.1.3

This release resolves two security issues:

1. The log file contains plain text password used to register the agent to the Supervisor. This password is not used for any other purposes. (Bug 749499)
2. An authenticated windows user can run arbitrary Powershell scripts with Admin permissions. (Bug 749499)

Windows Agent 3.1.2

This release adds the following new features and enhancements:

- Signed Agent binary: Windows Agent binaries are now cryptographically signed by Fortinet.
- Ability to specify host name: The user can specify a host name during Windows Agent installation. The Agent will register to the Supervisor with that host name. CMDB will show that host name.
- Virtual Collector Support: Agents can send events to a Virtual Collector (such as an F5 Load balancer) located between Agents and Collectors. Virtual Collectors can be defined in the Agent

definition on the Supervisor.
- Agent fails to install if there is a file or folder named Program under C:\.

Windows Agent 3.1.0

This release contains the following Windows Agent specific enhancements, in addition to the ability to work without Agent Manager functionality described earlier.

- Support for Windows Event Forwarding: Windows can forward logs using Windows mechanisms to a Central Windows Server. A FortiSIEM agent on the central server can then bring all the events from the various windows servers to FortiSIEM. This is an alternative to running FortiSIEM agent on every Windows server. The disadvantage of this approach is that Windows (Security, application and system) event logs can be collected in this way, while FortiSIEM agent can collect other information such as FIM, Custom log, Sysmon etc. This release is able to parse the forwarded Windows events so that actual reporting Windows server is captured and all the attributes are parsed as sent by native agents.
- Support of Windows FIPS enabled mode: In earlier releases, the agent did not work properly if FIPS mode was turned on. This issue is addressed in this release.
- File hash for File Integrity Monitoring computed using SHA256: The file hash value for file/folder monitoring is now reported using SHA256 algorithm instead of MD5. This enables direct match with external threat intelligence malware file hashes.

Content Pack Updates

This document provides details about Content updates for various 7.2.x releases.

- Content Updates for 7.2.x
- Content Updates for 7.2.0, 7.2.1, 7.2.2, 7.2.3, 7.2.4 and 7.2.5
- Content Updates for 7.2.0, 7.2.1, 7.2.2, 7.2.3 and 7.2.4
- Content Updates for 7.2.0, 7.2.1, 7.2.2 and 7.2.3
- Content Updates for 7.2.0, 7.2.1, and 7.2.2
- Content Updates for 7.2.0 and 7.2.1
- Content Updates for 7.2.0

Deployment Notes

- Content Pack Updates require the use of FortiSIEM version 6.4.0 or later. Procedures related to Content Updates can be found here.
- Content Pack Updates are available for the latest major release and the most recent prior three major releases. For example, If the latest release was 7.2.0, Content Pack Updates would include 7.2.0, 7.1.x, 7.0.x, and 6.7.x releases.
- 7.2.0 Content Pack Updates release begin with Content Update 701, and increments. If your FortiSIEM does not contain an older content update, it is automatically downloaded and added during your content update.
- Content Pack Updates must be done in the following order:
  a. Update FortiSIEM Supervisor.
  b. Update FortiSIEM Worker.

Content Updates for 7.2.x

- Content Update 720
- Content Update 718
- Content Update 717
- Content Update 713
- Content Update 712
- Content Update 711

Note: There is no content update 719, 716, 715, 714 or 710.

Content Update 720

Published January 14, 2026

This content update contains the following:

1. 3 * Outbreak Rules and Reports:
   - Outbreak: Cisco ASA and FTD Firewall RCE Detected on Network
   - Outbreak: UNC1549 Critical Infrastructure Espionage Attack Detected on Network
   - Outbreak: React2Shell Remote Code Execution Detected on Network
2. Parser Updates & Enhancements:
   - ArmisParser: Updated to parse additional csX labels.
   - BindDNSParser: Updated to handle new log format.
   - CheckpointCEFParser: Updated to parse additional custom string csX labels.
   - CiscoASAParser: Updated to parse server ip for event 113005.
   - FalconStreamingParser: Updated to handle new log format for DetectionSummaryEvent.
   - FortiADCParser: Updated event format recognizer to include new Forti ADC serial numbers.
   - FortiGateParser: Updated event format recognizer to exclude Forti ADC serial numbers.
   - FortiReconParser: Added parsing for breach date in FortiRecon-easm_leaked_creds events.
   - FortiSandboxParser: Updated to support events with devid FSA[A-Z0-9] and the corresponding event type definitions.
   - HillstoneNGFWParser: Updated to parse log id, source ip, destination ip and some additional event attributes.
   - IronportMailParser: Updated to parse new labels for sender reputation domain events.
   - UnixParser: Updated parser to handle postponed ssh auth events and the corresponding event type definition.
   - VMwareEventParser: Event type definitions added for various events.
3. CrowdStrike rules and reports updated to handle new format for DetectionSummaryEvent.
4. Fixed typo in rule incident title for the following rule:
   - End User DNS Queries to Unauthorized DNS Servers
5. New Rules added for Cisco Email Security Appliance (formerly Cisco IronPort)
   - Cisco Email Security: Mail Permitted from a Untrusted Domain
   - Cisco Email Security: Mail Permitted from a Questionable Domain
   - Cisco Email Security: Excessive Emails Detected from a Untrusted Domain
   - Cisco Email Security: Excessive Emails Detected from a Questionable Domain
6. Latest GeoDB Updates.

Content Update 718

Published November 20, 2025

This content update contains the following:

1. 3 x Outbreak Rules and Reports:
   - Outbreak: Fortra GoAnywhere MFT Attack Detected on Network
   - Outbreak: Fortra GoAnywhere MFT Attack Detected on Host
   - Outbreak: Oracle E-Business Suite RCE Zero-day Detected on Network
2. New Device & Integration Support:
   - DynatraceAuditLogParser – Adds parsing of Dynatrace Audit Logs.
   - ESETProtectCEFParser – Adds support for ESET Protect CEF-formatted logs.
   - FortiMailWorkspaceAPIParser – Supports API-based ingestion from FortiMail Workspace (Perception Point).
   - FortiMailWorkspaceCEFParser – Adds CEF parser for FortiMail Workspace Security (Perception Point) syslog events.
   - ManageEngineEndpointCentralParser – Adds support for ManageEngine Endpoint Central device logs.
   - ManageEnginePAM360Parser – Adds support for ManageEngine PAM360 platform logs.
3. Parser Updates & Enhancements:
   - BindDNSParser - Updates for new log header format.
   - CiscoASAParser - Parsing fixes for events 302020 and 420002.
   - CiscoIOSParser - Fixed unhandled issue in parsing event IPACCESSLOGRP.
   - CiscoMerakiParser - Added new event attributes and event type definitions.
   - CloudTrailParser - Enhanced to normalize usernames correctly across all logon types for consistent event correlation.
   - FalconStreamingParser - Added support for additional fields.
   - FortiClientParser - Updated to extract CVE information from vulnerability name descriptions in FortiClient Vulnerability Scan logs.
   - FortiGateParser - Updated to parse the new devID format.
   - MicrosoftATAParser - Updated to parse logs in the new event format.
   - UnixParser - Added handling to catch generic nmbd process logs.
   - VMwareVCenterParser - Parser enhancement to support parsing for sshd-session, Fdm, doat, and lsud events.
   - WinOSXmlParser - Updated to map IpAddress and IpPort correctly to source or destination based on context.
   - ZeekParser - Updated to parse zeek-intel events.
   - ZscalerJsonParser - Enhanced to handle NSS/LSS logs using on-prem NSS or Cloud NSS for ZIA, or LSS for ZPA.

     Note: ZscalerNSSParser has been removed.
   - General Updates - Various parsers now map Event ID to msgId instead of eventId, preventing incorrect event triggers caused by the previous internal eventId mapping.
4. Lookup Table Rule/Report updated to include additional event types:
   - Uncommon Office365 Mail Login
   - Top O365 Mail login
5. New reports added:
   - AWS S3 Data: Total Event Count
   - AWS S3 Data: Total Reads
   - AWS S3 Data: Total Creates

- AWS S3 Data: Total Deletes
- AWS S3 Data: Read Objects
- AWS S3 Data: Create Objects
- AWS S3 Data: Delete Objects
- AWS S3 Data: Total Updates
- AWS S3 Data: Update Objects
- AWS S3 Data: Latest bucket object activities
- AWS S3 Data: Total bytes out over time
- AWS S3 Data: Total bytes in over time
- AWS S3 Management: Total Event Count
- AWS S3 Management: Total Creates
- AWS S3 Management: Total Reads
- AWS S3 Management: Create Bucket
- AWS S3 Management: Update Bucket
- AWS S3 Management: Delete Bucket
- AWS S3 Management: Total Deletes
- AWS S3 Management: Total Updates
- AWS S3 Management: Read Bucket
- AWS S3 Management: Bucket Update Details
- AWS S3: Total Event Count
- AWS S3: Top Operations
- AWS S3: Top Buckets
- AWS S3: Top Source Countries
- AWS S3: Top Principal Amazon Resource Names
- AWS S3: Top Users
- AWS S3: Total Bytes
- AWS S3: Resource type and Bucket actions over time
- AWS ECS: Total Event Count
- AWS ECS: Top ECS Clusters
- AWS ECS: Top ECS Tasks
- AWS ECS: Top Source Countries
- AWS ECS: Total Creates
- AWS ECS: Total Deletes
- AWS ECS: Total Updates
- AWS ECS: Total Lists
- AWS ECS: Operations
- AWS ECS: Top Principal Amazon Resource Names
- AWS ECS: Cluster Details
- AWS ECS: Create Details
- AWS ECS: Update Details
- AWS ECS: Delete Details
- AWS ECS: Top Users
- AWS WAF: Total Event Count

- AWS WAF: Top Source Countries
- AWS WAF: Top HTTP Methods
- AWS WAF: Top Source IPs
- AWS WAF: Top URI Stems
- AWS WAF: Total ALLOW Events
- AWS WAF: Total BLOCK Events
- AWS WAF: Total CAPTCHA Events
- AWS WAF: Top Sources by URI STems
- AWS WAF: Top Web ACLs
- AWS WAF: Top Events
- AWS WAF: Web Traffic details
- AWS WAF: Top Http Source Names
- Zscaler ZIA: Top DNS Actions
- Zscaler ZIA: Top Blocked DNS Queries
- Zscaler ZIA: Top Allowed DNS Queries
- Zscaler ZIA: Top Blocked DNS Queries by Source IP and Destination Domain
- Zscaler ZIA: Top Blocked DNS Requests by User
- Zscaler ZIA: Top Blocked DNS Requests by Web Category
- Zscaler ZIA: DNS Blocked Traffic Details
- Zscaler ZIA: Top Firewall Blocked Actions
- Zscaler ZIA: Top Firewall Permitted App Protocols
- Zscaler ZIA: Top EDLP Firewall Actions
- Zscaler ZIA: Top EDLP Threat Levels
- Zscaler ZIA: Top Blocked Destination IPs
- Zscaler ZIA: Top Blocked Source IPs
- Zscaler ZIA: Top Threats
- Zscaler ZIA: FW Blocked Traffic Details
- Zscaler ZIA: Top Web Blocked URL Categories
- Zscaler ZIA: Top Permitted Web Apps
- Zscaler ZIA: Top Web Actions
- Zscaler ZIA: Top HTTP Status Codes
- Zscaler ZIA: Top Blocked Web Users
- Zscaler ZIA: Top Blocked Web Sources and Destination Domains
- Zscaler ZIA: Web Blocked Traffic Details
- Zscaler ZPA: User Activity Details
- Zscaler ZPA: User Status Details
- Zscaler ZPA: Top Users
- Zscaler ZPA: Top Destination Domains
- Zscaler ZPA: Top User Activity Policies
- Zscaler ZPA: Top User Activity Source IPs
- Zscaler ZPA: Audit Details
- Zscaler ZPA: Top Audit Operations
- Zscaler ZPA: Top Audit Changes by User and Operation

- Zscaler ZPA: Top Audit Users
- Zscaler ZPA: Audit Sign In Details
- Zscaler ZPA: Top Browser Access Destinations by Sent and Recv Bytes
- Zscaler ZPA: Top Browser Access Source IPs and Destination Domains
- Zscaler ZPA: Top Browser Access Source IPs by Sent and Recv Bytes
- Zscaler ZPA: Top Connectors by Traffic Volume
- Zscaler ZPA: Top Browser Access Application Protocols
- Zscaler ZPA: Top Browser Access HTTP Status Codes
- Zscaler ZPA: Top Connectors
- Zscaler ZPA: Browser Access Allowed Traffic Details
- Zscaler ZPA: Browser Access Blocked Traffic Details
- FortiMail Workspace: Top Mail Sender and Receivers Domains
- FortiMail Workspace: Total Clean Email Count
- FortiMail Workspace: Total Email Scan Count
- FortiMail Workspace: Total Malicious Email Count
- FortiMail Workspace: Total Restricted Email Count
- FortiMail Workspace: Total Spam Email Count
- FortiMail Workspace: Total Suspicious Email Count
- FortiMail Workspace: Top Scanned URLs
- FortiMail Workspace: Top Scanned Files
- FortiMail Workspace: Audit Details
- FortiMail Workspace: Top Malicious Mail by Sender and Receiver
- FortiMail Workspace: Top Suspicious Mail by Sender and Receiver
- FortiMail Workspace: Top Spam Senders

6. New rules added:
   - Zscaler ZIA: Critical Risk Firewall Traffic Allowed
   - Zscaler ZIA: Critical Risk Web Traffic Allowed
   - Zscaler ZIA: High Risk Firewall Traffic Allowed
   - Zscaler ZIA: High Risk Web Traffic Allowed
   - Zscaler ZIA: High Severity EDLP Detection Allowed
   - Zscaler ZPA: New Administrator Created
   - FortiMail Workspace: Admin User Added
   - FortiMail Workspace: Malicious Email Permitted
   - FortiMail Workspace: Suspicious Email Permitted
7. Latest GeoDB Updates.

Content Update 717

Published September 30, 2025

This content update contains the following:

1. Outbreak Rules and Reports:
   - Outbreak: ShadowSilk Data Exfiltration Attack Detected on Network
2. New Device Support:
   - DarkTraceWebhookParser - DarkTrace SaaS platform support
   - WallixBastionParser - Wallix Bastion PAM support
   - SAPEnterpriseThreatDetectionCloudParser - SAP ETD Cloud alerts via Generic Poller
   - SiemensSimaticPLCParser - Siemens Simatic PLC support
   - SentinelOneSingularityParser - HTTPS Advanced event puller for SentinelOne
3. Parser Updates & Enhancements:
   - AwsSQSParser - Additional event attributes and event type definitions added for S3 events
   - CheckpointCEFParser - Event parsing and event type definitions added for SmartConsole and WEB_API events
   - CiscoDuoParser - Updated to parse source IP field
   - CiscoFirepowerCEFParser - Additional event attributes and event type definitions for Firepower Connection Statistics events
   - CiscoIOSParser - Support for IOS XR SSH events
   - CitrixNetScalerParser - Parsing Client_ip to srcIpAddr instead of hostIpAddr
   - F5Big-IP-LTMParser - Updated to parse client IP field
   - FortiGateParser - Updated to parse user and source for malformed log 22903
   - KasperskyParser - Improved time parsing (epoch millis → seconds for timestamp)
   - MS365DefenderParser - Updated to parse urlEvidence field
   - MSDefAdvancedHuntingParser - Additional event attributes and event type definitions added
   - PaloAltoParser - Additional event attributes and event type definitions added
   - TrendMicroVisionOneParser - Parsing Hostname and HostIP fields
   - WinDefATPParser - ThreatName field parsed to virusName instead of attackName
4. FortiNDR On-Premise Rules (now organized by Severity):
   - FortiNDR: Critical IOC Detected
   - FortiNDR: High IOC Detected
   - FortiNDR: Medium IOC Detected
   - FortiNDR: High Severity Attack Chain Permitted
   - FortiNDR: Medium Severity Attack Chain Permitted
   - FortiNDR: Low Severity Attack Chain Permitted
   - FortiNDR: High Severity Botnet Detected
   - FortiNDR: Medium Severity Botnet Detected
   - FortiNDR: Low Severity Botnet Detected
   - FortiNDR: High Severity Attack Permitted
   - FortiNDR: Medium Severity Attack Permitted
   - FortiNDR: Low Severity Attack Permitted
5. MS 365 Defender (Defender for XDR) Rules Updates:
   - Existing rules have been enhanced and additional rules added to account for the severity of each event. Every rule now has Medium and High severity.
   - FortiSIEM supports more than one event ingestion method (HTTPS Advanced via Graph API or Event Hub) for Defender audit logs.

- The rules prefixed with \"MS 365 Defender\" have been updated to allow triggering from either source.

6. Additional Rules for Armis Centrix & SentinelOne Singularity:
   - Armis Device Risk Level Medium
   - Armis Device Risk Level High
   - Armis Network Policy Violation
   - SentinelOne: Analyst Marked Malicious Threat Verdict as True Positive
   - SentinelOne: New Malicious Threat not Mitigated
   - SentinelOne: New Suspicious Threat not Mitigated
   - SentinelOne: STAR Response Marked Event as Malicious
   - SentinelOne: STAR Response Marked Event as Suspicious
   - SentinelOne Cloud Alert: New Malicious Threat not Mitigated
   - SentinelOne Cloud Alert: New Suspicious Threat not Mitigated
7. New Reports for SentinelOne Singularity:
   - SentinelOne Singularity: Distinct Malware Hosts Count
   - SentinelOne Singularity: Distinct Ransomware Hosts Count
   - SentinelOne Singularity: Malware Host Details
   - SentinelOne Singularity: Ransomware Host Details
   - SentinelOne Singularity: Top Blocked Traffic by Host and Destination
   - SentinelOne Singularity: Top Classifiers
   - SentinelOne Singularity: Top Device Control Approved Devices
   - SentinelOne Singularity: Distinct Suspicious Hosts Count
   - SentinelOne Singularity: Suspicious Host Details
   - SentinelOne Singularity: Threat not mitigated details
8. Latest GeoDB Updates.

Content Update 713

Published August 11, 2025

This content update contains the following:

1. 8 x Outbreak Rules and Reports:
   - Outbreak: SimpleHelp Support Software Attack Detected on Network
   - Outbreak: SimpleHelp Support Software Attack Detected on Host
   - Outbreak: TBK DVRs Botnet Attack Detected on Network
   - Outbreak: SonicWall Secure Mobile Access Attack Detected on Network
   - Outbreak: Microsoft SharePoint Zero-day Attack Detected on Network
   - Outbreak: Microsoft SharePoint Zero-day Attack Detected on Host
   - Outbreak: Langflow Unauth RCE Attack Detected on Network
   - Outbreak: Citrix Bleed 2 Detected on Network
2. New Parser added:
   - VeeamBackupSyslogParser

3. New Reports added:
   - Veeam: Top Failed Backup Jobs
   - Veeam: VM Backup Jobs by Status
   - Veeam: Total Backup and Backup Copy Jobs
   - Veeam: Total Event Count
   - Veeam: Total Malware Activity Detected
   - Veeam: Backup Job Details
   - Veeam: Total Failed Backup Jobs
   - Veeam: Total Successful Backup Jobs
   - Veeam: Backup Task Details
   - Veeam: Top Malware Activity
4. Updates to the following parsers:
   - AWSELBParser
   - CiscoASAParser
   - CiscoFTDParser
   - ClarotyParser
   - FalconDataRepParser
   - FalconStreamingParser
   - FortiGateParser
   - GoogleGCPParser
   - Office365Parser
   - PaloAltoParser
   - TrendMicroVisionOneParser
   - WinOSWmiParser
5. Additional rule for CrowdStrike Falcon:
   - Crowdstrike: Detection Occurred but was allowed
6. Updates to event type groups for Windows MSI Installer events.
7. Latest GeoDB updates.

Content Update 712

Published June 11, 2025

This content update contains the following:

1. 8 x Outbreak Rules:
   - Outbreak: CrushFTP Authentication Bypass Attack Detected on Network
   - Outbreak: CrushFTP Authentication Bypass Attack Detected on Host
   - Outbreak: Microsoft DOTNET Framework Information Disclosure Detected on Network
   - Outbreak: Microsoft DOTNET Framework Information Disclosure Detected on Host
   - Outbreak: Apache Tomcat RCE Detected on Network
   - Outbreak: Apache Tomcat RCE Detected on Host
   - Outbreak: Langflow Unauth RCE Attack Detected on Network

- Outbreak: Earth Lamia APT Attack Detected on Network

2. 8 x Outbreak Reports:
   - Outbreak: CrushFTP Authentication Bypass Attack Detected on Network
   - Outbreak: CrushFTP Authentication Bypass Attack Detected on Host
   - Outbreak: Microsoft .NET Framework Information Disclosure Detected on Network
   - Outbreak: Microsoft .NET Framework Information Disclosure Detected on Host
   - Outbreak: Apache Tomcat RCE Detected on Network
   - Outbreak: Apache Tomcat RCE Detected on Host
   - Outbreak: Langflow Unauth RCE Attack Detected on Network
   - Outbreak: Earth Lamia APT Attack Detected on Network
3. New Parser added to support FortiSRA - Secure Remote Access for OT.
4. Updates to the following parsers:
   - FortiGateParser
   - FortiManagerParser
   - NutanixParser
   - SquidParser
   - WinOSXmlParser
5. Enhancement to FortiEDR rules to add Message ID in GroupBy clause.
6. Latest GeoDB updates.

Content Update 711

Published May 07, 2025

This content update contains the following:

1. 1 x Outbreak Rules and Reports:
   - Outbreak: Commvault Command Center Path Traversal Vuln Detected on Network
2. Updates to the following parsers:
   - FortiDeceptorParser
   - Office365Parser
   - WinOSXmlParser
3. Renamed Ransomware detected on a host rule to Excessive file changes on a host: Potential Ransomware.
4. Updated several FortiGate event types to fix event type group mismatch.
5. Latest GeoDB updates.

Note: Please note that in the FortiSIEM GUI, item 3 - "Updates to Windows SIGMA rules to remove false positives", was mistakenly added. It is NOT included in this Content Update. The corrected Content Update information is provided here.

Content Updates for 7.2.0, 7.2.1, 7.2.2, 7.2.3, 7.2.4 and 7.2.5

- Content Update 709

Content Update 709

Published March 5, 2025

This content update contains the following:

1. 2 x Outbreak Rules and Reports:
   - Outbreak: Ivanti Cloud Services Appliance Zero-Day Attack Detected on Network
   - Outbreak: PTZOptics NDI and SDI Cameras Attack Detected on Network
2. Updates to the following parsers:
   - FortiEDRParser
   - CiscoNxOSParser
   - SonicwallFirewallParser
   - CiscoASAParser
   - CiscoFTDParser
   - Office365Parser
   - AkamaiSIEMParser
   - AwsKinesisParser
   - CloudPassageParser
   - DocuSignParser
   - FalconStreamingParser
   - FireAMPCloudParser
   - OracleCASBParser
   - ProofpointParser
   - WinDefATPParser
3. Updated several FortiGate VPN event types with vpn logon success group.
4. Latest GeoDB updates.

Content Updates for 7.2.0, 7.2.1, 7.2.2, 7.2.3 and 7.2.4

- Content Update 708

Content Update 708

Published January 7, 2025

This content update contains the following:

1. 7 x Outbreak Rules and Reports:
   - Outbreak: Palo Alto Networks Management Interface Attack Detected on Network
   - Outbreak: Palo Alto Expedition Missing Authentication Vuln Detected on Network
   - Outbreak: Progress Kemp LoadMaster OS Command Injection Vulnerability Detected on Network
   - Outbreak: Mitel MiCollab Unauthorized Access Attack Detected on Network
   - Outbreak: Mitel MiCollab Unauthorized Access Attack Detected on Host
   - Outbreak: Apache Struts 2 RCE Attack Detected on Network
   - Outbreak: Apache Struts 2 RCE Attack Detected on Host
2. Latest GeoDB updates.

Content Updates for 7.2.0, 7.2.1, 7.2.2 and 7.2.3

- Content Update 707
- Content Update 706
- Content Update 705
- Content Update 704

Content Update 707

Published November 11, 2024

This content update contains the following:

1. 2 x Outbreak Rules and Reports:
   - Outbreak: Mallox Ransomware Detected on Network
   - Outbreak: Mallox Ransomware Detected on Host
2. New indicators added to FortiManager Rules/Reports.
   - Outbreak: FortiManager Command Execution Vulnerability Detected on Network
   - Outbreak: FortiManager Command Execution Vulnerability Detected on Device
3. Updates to FortiGate Reports.
   - FortiGate: Top Applications by Bandwidth
   - FortiGate: Top non-HTTP Applications by Bandwidth
4. Updates to Access Violation Rules.

- Concurrent Successful Authentications To Same Account From Multiple Cities
- Concurrent Failed Authentications To Same Account From Multiple Countries
- Concurrent Failed Authentications To Same Account From Multiple Cities

5. Latest GeoDB updates.

Content Update 706

Published October 29, 2024

This content update contains the following:

1. 2 x Outbreak Rules and Reports:
   - Outbreak: FortiManager Command Execution Vulnerability Detected on Network
   - Outbreak: FortiManager Command Execution Vulnerability Detected on Device
2. Latest GeoDB updates.

Content Update 705

Published October 17, 2024

This content update contains the following:

1. 2 x Outbreak Rules and Reports:
   - Outbreak: Synacor Zimbra Collaboration Command Execution Vuln Detected on Network
   - Outbreak: Synacor Zimbra Collaboration Command Execution Vuln Detected on Host
2. Enhancements to FortiGate and WinOSXml parsers.
3. New parser for FortiAuthenticator Debug Logs.
4. Latest GeoDB updates.

Content Update 704

Published September 24, 2024

This content update contains the following:

1. 3 x Outbreak Rules and Reports:
   - Outbreak: CISA Alert AA24-249A Russian Cyber Espionage Attack Detected on Network
   - Outbreak: CISA Alert AA24-249A Russian Cyber Espionage Attack Detected on Host
   - Outbreak: GeoServer RCE Attack Detected on Network
2. Additional event attributes to support new parsing.
3. Enhancements to Apache, CiscoDuo, FortiClient, FortiMail, FortiRecon, Sendmail, TenableVuln, Unix, VMwareVCenter, WinOSWmi, and WinOSXml parsers.
4. Updated descriptive metadata for several rules.
5. Latest GeoDB updates.

Content Updates for 7.2.0, 7.2.1, and 7.2.2

- Content Update 703

Content Update 703

Published August 28, 2024

This content update contains the following:

1. 4 x Outbreak Rules and Reports:
   - Outbreak: ServiceNow Remote Code Execution Attack Detected on Network
   - Outbreak: Apache OFBiz RCE Attack Detected on Network
   - Outbreak: Jenkins RCE Attack Detected on Network
   - Outbreak: Jenkins RCE Attack Detected on Host
2. Enhancements to Okta, LinuxAudit, Unix, and BlueCatAddressManager parsers.
3. Latest GeoDB updates.

Content Updates for 7.2.0 and 7.2.1

- Content Update 702

Content Update 702

Published August 1, 2024

1. Enhancements to parsers: Office365, FortiPAM, FortiEDRRest, CitrixNetScaler, Dragos, VMwareVCenter, VMwareEvent, CiscoNxOS, OracleDB, FortiGate, PHBox, GitHubWebhooksJson, CarbonBlackCEF, TenableVuln, TrendMicroApexCentral, and WinOSXml.
2. New parsers added: ADAuditPlusParser, BlueCatAddressManagerParser, CiscoACISyslogParser, DellUnityParser, DellPowerEdgeParser, HashiCorpVaultParser, and TrendMicroVisionOneCEFParser.
3. Updated report "Slow FortiSIEM Queries".
4. Latest GeoDB updates.

Content Updates for 7.2.0

- Content Update 701

Content Update 701

Published June 17, 2024

This content update contains the following:

1. 3 x Outbreak Rules and Reports:
   - Outbreak: Dlink Multiple Devices Attack Detected on Network
   - Outbreak: Check Point Quantum Security Gateways Information Disclosure Attack Detected on Network
   - Outbreak: PHP CGI OS Command Injection Vuln Detected on Network
2. Enhancements to WinOSWmi, WinOSXml, FortiSandbox, FortiNDR, FortiAuthenticator, and JunipSSGFirewallLog parsers.
3. Updated Windows rule to fix incorrect logic.
   - Windows: Active Directory User Backdoors
4. Dedicated FortiSandbox rule to detect phishing URLs.
   - FortiSandbox detects Phishing URL
5. Latest GeoDB updates.

Key Concepts

This section describes several key concepts used in FortiSIEM.

- Clustering Architecture
- Licensing
- Multi-tenancy and Organizations
- Role-based Access Control
- Discovery and CMDB
- Windows and Linux Agents
- Business Services
- Parsers and Monitors
- Entity Risk Score
- User Identity and Location
- Searches, Reports and Compliance
- Rules and Incidents
- Incident Automation Policy
- Remediation Library
- External Ticketing Systems Integration
- Dashboard

Clustering Architecture

FortiSIEM scales seamlessly from small enterprises to large and geographically distributed enterprises and service providers.

- For smaller deployments, FortiSIEM can be deployed as a single all-in-one hardware or virtual appliance that contains full functionality of the product. This is the Supervisor node.
- For larger environments that need greater event handling throughput, FortiSIEM can be deployed in a cluster of Supervisor and Worker Virtual Appliances. Collector nodes are also used to distribute event collection to Collectors for performance and also architecture reasons such as collecting events from remote networks and different network segments.
- For larger distributed environments where there are multiple instances of FortiSIEM, the FortiSIEM Manager can be used to monitor separate FortiSIEM instances and manage Incidents. FortiSIEM Manager is a separately licensed product to FortiSIEM. Unless there is a requirement to manage multiple FortiSIEM Instances (Supervisors), then please begin with installing the Supervisor which will manage Worker nodes, Collector nodes and Agents.

There are four types of FortiSIEM nodes – Collector, Worker, Supervisor and Manager. Collectors are used to scale data collection from various geographically separated network environments potentially behind firewalls. Collectors communicate to the devices, collect, parse and compress the data and then send this information to the Worker nodes over a secure HTTP(S) channel in a load balanced manner. Supervisor and Worker nodes reside inside the data center and perform data analysis functions using distributed co-operative algorithms.

A FortiSIEM instance consists of Supervisor, multiple Workers and Collectors. A FortiSIEM Manager can be used to monitor and manage multiple FortiSIEM instances over HTTPS REST API channel. Incidents, License and Health information are forwarded from each FortiSIEM instance to the FortiSIEM Manager. From FortiSIEM Manager, you can Clear/Resolve/Change Severity/Add comments to one or more Incidents, disable one or more rules and change their severity, run FortiSOAR Playbooks and Connectors to update Incident Status and Comments. A one-click operation to log you into the appropriate FortiSIEM instance where an Incident occurred. This enables you quickly to investigate an Incident in depth.

There are five primary data analysis tasks:

1. Data indexing and storing in an event database
2. Data searching
3. Correlating data in streaming mode to trigger rules (behavioral anomalies)
4. Creating a user identity and location database to add context for data
5. Creating baselines for anomaly detection

For scalability, each of these tasks is divided into a heavyweight Worker component executed by the Worker nodes and a lightweight Master component executed by the Supervisor node. The Supervisor nodes, accessible via the GUI is comprised of a self-contained three-tier model – the GUI, the Application Server containing the business logic, and a relational database for holding the FortiSIEM application state.

For scalable event storage, FortiSIEM provides three options:

- Local disk
- FortiSIEM NoSQL event database with data residing on an NFS Server
- Elasticsearch distributed database

Hardware appliance and All-in-one virtual appliance solutions use the local disk option while the NoSQL or Elasticsearch options can be exploited by a FortiSIEM cluster of Supervisor and Workers.

The NoSQL event database option is a purpose built FortiSIEM proprietary solution. The Supervisor and Worker nodes create and maintain the database indices. To scale event insertion and search performance in this mode requires (a) a fast communication network between the Supervisor/Worker nodes and the NFS Server and (b) high NFS IOPS that can be achieved using fast RAID disk or tiered SSD and magnetic disks.

Elasticsearch provides a true distributed, redundant columnar database option for scale-out database performance at the expense of higher storage needs. In this option, FortiSIEM Worker nodes push the data in real time to Elasticsearch cluster, which maintains the event database. FortiSIEM has developed an intermediate adaptation layer, so that the same GUI can run seamlessly on both Elasticsearch and FortiSIEM NoSQL event database.

Licensing

FortiSIEM is licensed based on the following:

- Number of devices FortiSIEM monitors or receives logs from
- Number of Windows Agents and Linux Agents
- Aggregate Events per Second (EPS) it receives

Note that FortiSIEM licensing is not based on storage - you can store and query the data as needed for your compliance needs without any concern regarding licensing. The license parameters can be perpetual or subscription based. Maintenance and FortiGuard Threat Intelligence are subscription based.

You can have unlimited devices in CMDB. However, the total number of devices that send logs to FortiSIEM or are monitored by FortiSIEM cannot exceed the device license. The devices under license are called 'Managed' while the remaining devices are called 'Unmanaged'. If you do a discovery and the number of newly discovered devices combined with Managed CMDB devices exceed the license, then the extra devices are tagged in CMDB as 'Unmanaged'. You can either buy more device license or exchange an Unmanaged device with a Managed device.

FortiSIEM calculates Events per Second (EPS) over a 3-minute period as the total number of events received over a 3-minute period divided by 180. FortiSIEM is a distributed system where events can be received at any node - Collector, Worker, or Supervisor. The EPS licensing is enforced as follows:

At the end of every 3-minute interval, Incoming EPS is calculated at each event entry node (Collector, Worker, or Supervisor) and the value is sent to the central decision-making engine on the Supervisor node.

1. The Supervisor node takes all Incoming EPS values and based on the Licensed EPS, computes the Allocated EPS for the next 3-minute interval for every node and communicates those values to every node.
2. For the next 3-minute interval, each node accepts up to (Allocated EPS * 180) events. It also reports Incoming EPS for the current interval to the Supervisor node.
3. The continuous EPS reallocation process continues.

FortiSIEM includes some additional refinements to EPS enforcement as follows:

- Each Collector has a Guaranteed EPS. The Allocated EPS for this Collector is always greater than the Guaranteed EPS.
- FortiSIEM keeps track of Unused EPS as the sum of positive differences of Allocated EPS and Incoming EPS over all nodes. At the beginning of the day (12:00 am), Unused EPS is set to 50% of previous day's Unused EPS and then Unused EPS accumulates throughout the day before maxing out at five times Licensed EPS. Unused EPS can be used for bursting during attacks or other event surge periods, beyond Licensed EPS.

For details on License Enforcement, see here.

Multi-tenancy and Organizations

Multi-tenancy enables you to manage multiple groups of devices (Organizations) within a single installation. FortiSIEM provides logical separation between Organizations at an application layer. The users of one Organization cannot see another Organization's data, which includes devices, users and logs.

You have to choose the Service Provider Installation type when you first install FortiSIEM. Organizations can be defined in two ways:

- *By adding a Collector to an Organization* – all devices sending logs to a Collector or all devices monitored by a Collector are automatically assigned to the Organization to which the Collector belongs. Device Names and IP Addresses can overlap between two Organizations. This situation can be used to model Remote Managed Service Providers.
- *By assigning IP ranges to Organizations* – there are no Collectors and devices will be discovered from Supervisor node and send logs to Supervisor or Worker nodes. If the IP addresses of ALL interfaces of a device are wholly included within the IP range for an Organization, then the device is assigned to that Organization. Else, the device is assigned to the Super/Local Organization (see below).

In addition to user-defined Organizations, FortiSIEM creates two Organizations for ease of management:

- **Super/Local Organization** – this can be used to model a Service Provider's own network.
  - For Organizations with Collectors, if a device sends logs directly to Supervisor or Worker nodes or is discovered from the Supervisor node, then it belongs to the Super/Local Organization.
  - For Organizations without Collectors, if all the IP addresses of a device (being discovered or sending logs) are not wholly included within the IP range for any Organization, then that device is assigned to the Super/Local Organization.
- **Super/Global Organization** – this is a virtual Organization that can 'see' all the other Organizations. This is useful for Service Provider administrative users.

FortiSIEM Multi-tenancy principles are as follows:

1. Users belonging to Super/Global Organization can see other organizations and their data.
2. Users belonging to Super/Local Organization and user-defined Organizations can only see their own Organization.
3. Devices and events are automatically tagged by FortiSIEM with the Organization Id and Name.
4. Rules can be written at a Global level or for a specific Organization. Incidents trigger when rule conditions are met and they trigger independently for each organization. Each Incident is labeled with Customer Id and Name.
5. Searches/Reports can be executed from Super/Global Organization for any combinations of Organizations.
6. From a specific user-defined Organization or Super/Local Organization, Searches/Reports can run on that Organization.
7. Viewing Incidents is simply a specific Search and follows the same principles as specified in 5 and 6.

Role-based Access Control

After installation, FortiSIEM automatically creates an admin user with Full Admin rights for Super/Global and Super/Local Organization. When the user creates a new Organization, FortiSIEM creates an admin user for that Organization. These are accounts with Full Admin rights. FortiSIEM users with Full Admin rights can create Roles and then create users and assign them a role.

A FortiSIEM role is based on the following aspects:

- What the user can see:
  - Restrict GUI visibility by hiding parts of the GUI
  - Restrict some Organizations for Service Provider installations
  - Restrict data by writing filters on device type, event type and any parsed event attribute
- What the user can do:
  - Restrict or even hide Admin tab where most of the configuration takes place
  - Restrict any other GUI tab
  - Restrict write capability on certain parts of the GUI

FortiSIEM has a few built-in roles that the users can customize to meet their own needs.

Discovery and CMDB

Discovery is a key differentiator for FortiSIEM as it enables users to seamlessly discover their infrastructure (the 'truth') and auto-populate the CMDB, which can then be used to facilitate analytics.

Discovery can be of two types:

- **Simple LOG discovery** – FortiSIEM has mappings for device type to parse logs for all its in-built log parsers. When it sees a log that matches a parser, it associates the corresponding device type to that device and creates a CMDB entry.
- **Detailed device discovery** – LOG discovery is very basic since only the Vendor and Model can be guessed (for example: Cisco IOS, Fortinet FortiGate, Microsoft Windows, Generic Linux). It is not possible to deduce more details about the device, for example: Operating System version, hardware model, installed patches, installed software, running processes, network device configurations, interfaces, monitor-able performance metrics, etc. In addition to discovering all of the above, FortiSIEM can also discover certain inter-device relationships, for example, Virtualization Guest to Host mappings, WLAN AP to Controller mappings, Multi-context device to physical device mappings, network topology etc. Devices in the AWS Cloud and MS Azure Cloud can be discovered as well.

Discovered information is used to automatically populate a CMDB. As new devices get added or deleted from the infrastructure, scheduled rediscoveries can keep FortiSIEM CMDB up to date. The user can also define some rules to map certain groups of devices to certain CMDB device groups.

The key advantages of FortiSIEM Discovery and CMDB are as follows:

1. The customer has an *accurate picture of the infrastructure* and its relationships from a simple discovery. If a new rogue device is added to the network, FortiSIEM rediscovery learns immediately of the new device and can send an alert of this potential security issue. If an inadvertent configuration change to a key file is made, FortiSIEM rediscovery or configuration monitoring also detects and alerts.
2. *Performance and availability monitoring is automated* since FortiSIEM simply learns what can be monitored and starts monitoring immediately. This approach eliminates human error from the process.
3. *Certain key CMDB Objects such as Business Services can remain up to date against infrastructure changes* as they can be auto-populated by discovery.
4. *CMDB Objects make rules and reports easy to create*. First, no long explicit list of IP addresses or host names are needed for rules or reports. Secondly, rules do not need to be rewritten as devices get added or deleted.
5. *Discovery enables configuration change detection* for both day-to-day changes and changes to golden versions.

Windows and Linux Agents

Some logs and performance metrics can be collected remotely from Windows servers via WMI and by running the Winexe command. Some key performance metrics and file monitoring on Linux servers can be done via SSH. However, the following limitations exist:

For Windows Servers:

- Not all metrics can be collected from a FortiSIEM Linux platform via WMI (for example: Sysmon, Generic Event Logs in the Event Log navigation tree, Registry changes). WMI can be used to collect only Windows Event logs.
- *File Integrity Monitoring Data collected via Windows Security logs is very verbose* (~8 logs per file operation) and creates unnecessary noise in FortiSIEM.
- Remotely running *some programs such as Winexe start services on the servers* may trigger security alerts in certain environments.
- A domain account is required to collect certain logs. A regular account does not provide all logs.
- WMI Service often creates CPU load on the servers when a large number of logs are pulled via WMI.

- *Collecting logs via polling from thousands of servers is not efficient*. If a server is not responsive or slow, you have to wait for the connection to timeout and this wastes resources.

Linux Servers send log via syslog. However, if you want to collect File Integrity Monitoring Data, then a certain configuration is required for this to be done remotely.

Agents provide a clean and efficient way to collect exactly the data that is needed. FortiSIEM Agents are very lightweight and do not consume more than 5% of system CPU and memory. FortiSIEM Windows Agents have the following functionality:

- Collect any Windows Event log including Security, Application and Performance event logs, DHCP/DNS logs, Sysmon logs, etc.
- Collect Custom log files
- Detect registry changes
- Detect File read, write and edits (FIM) with added user context
- Run any PowerShell command and send the output as logs – this allows users to capture any data at periodic intervals and send it to FortiSIEM.
- Detect removable media insertion, deletion, read and write

FortiSIEM can manage a large number of FortiSIEM Windows Agents using configuration templates. The user needs to create a template and associate it with servers. Windows Agents can be configured to send logs to FortiSIEM collectors in a round robin fashion. If one collector is not available, the Agent can send it to the next Collector in the list. This provides a robust and scalable way to collect logs from a large number of servers.

Linux Agents can be used to detect file reads, writes, and edits (FIM functionality) with added user context.

Business Services

A Business Service provides a collection of devices and applications serving a common business purpose. You can define a Business Service in FortiSIEM either manually or by the Dynamic CMDB Group framework that adds it to the Business Service once a device matching certain criteria appears in CMDB.

The primary objective of a Business Service is to assist in incident triage. Once a Business Service is defined, every incident is tagged with the impacted Business Services. A Business Service dashboard provides a top-level Incident-centric view of Business Services. The user can take care of incidents for critical Business Services and ensure that they stay up.

Parsers and Monitors

The ability to parse any log to any depth is a key SIEM functionality. FortiSIEM comes inbuilt with over 2,500 event attributes, 175,000 event types and 250 parsers for various device types and applications. In addition, it has a flexible GUI based framework for customers to enhance existing log parsers, and create completely new device types, event attributes, event types and log parsers. The user can test parser changes on a live system and apply them to become effective immediately on all nodes – so changes take effect without any downtime. Parsers can also be exported out of one system and imported into another system. In Service Provider environments, a parser change can be created at a global level and deployed to all organizations.

FortiSIEM also comes with a number of built-in performance monitors and configuration pulling scripts for device types and applications. Discovery automatically enables the applicable monitors and the user can adjust some parameters, such as polling intervals. Similar to log parsers, the user can create and test performance monitors on a live system and apply them to become effective immediately on all

nodes – so changes take effect without any downtime. Performance Monitors can also be exported out of one system and imported into another system.

FortiSIEM tracks changes to installed software and network device configuration. If a new configuration file needs to be monitored and can be obtained via a script, then the user can add them to the system. FortiSIEM monitors changes from a current version to a previous version, deviation from a blessed file, and changes between running config and startup config for certain devices.

Entity Risk Score

FortiSIEM displays devices and users (entities) ranked by risk, providing entity risk scores in Risk View. An entity risk score is calculated based on triggering incidents using a proprietary algorithm that incorporates asset criticality, incident severity, frequency of incident occurrence, and vulnerabilities found. In addition, scores are color coded to quickly identify high risk (red), medium risk (yellow) and low risk (green), and also show occurrence trends, such as whether a risk has gone up or down. Each entity can be selected to show a more detailed risk score trend, along with timeline incident data.

User Identity and Location

FortiSIEM creates an Audit trail of User Identity and Location data in real time by associating a network identity (for example: an IP address, or MAC address) to user identity (for example: a user name, computer name, or domain or Cloud logon) and tying that to a location (like a wired switch port, a wireless LAN controller, or VPN gateway or geo-location for VPN logins). The associations are generated by piecing together various pieces of information from Windows Active Directory events, DHCP events, WLAN and VPN logon events and various Cloud service logon events, with discovery results.

FortiSIEM Supervisor and Worker nodes collaborate in a distributed manner to create User Identity and Location records. The IdentityWorker module on Worker nodes keep a partial User Identity and Location in-memory database based on the events that they see. Whenever the IdentityWorker module on a specific Worker sees new information, for example: a new IP address to User association, it updates the database and communicates to the IdentityMaster module on the Supervisor node. The global User Identity and Location database is created by the IdentityMaster module on the Supervisor node by combining information from all IdentityWorker modules. Whenever the IdentityMaster module sees new information, it sends a signal to parser modules in all nodes, which then gets the latest updates from the Supervisor node. The parser module injects IP to User meta-data into events in real time so that this information can be searched without complicated database join operations.

Searches, Reports and Compliance

FortiSIEM provides a unified way to search the data it collects from various devices. All data whether it is system logs, performance metrics, or configuration changes, is converted to an event with parsed event attributes to make it easy to search.

Searches can be done for real-time data or historical data. In real time mode, search occurs in a streaming node on incoming data without touching the event database. In historical mode, the user specifies a time period and data residing in the event database is searched for that time period. Searches can be specified on raw logs or parsed attributes. A rich variety of grouping and aggregation constructs are supported to display data at various granularity. The raw log data is saved into the same event database as the parsed attributes and any attributes added via enrichment are also added to the event and stored in the event database.

FortiSIEM comes pre-built with a large number of reports that can be used as starting points. The user can customize these reports and save them as their own reports for later use. Reports can be scheduled to run at specified times and be delivered in various formats, such as PDF and CSV, via

email. FortiSIEM provides a large number of compliance reports, each with reference to specific compliance mandates. To run these reports, the user simply needs to add devices to the specific compliance device group (Business Service) and then run the report.

All searches run in a distributed fashion in FortiSIEM. For deployments with FortiSIEM NoSQL database, the Supervisor node distributes each search query to Worker nodes and summarizes the partial results sent back from the Worker nodes. Assuming you have sufficient NFS IOPS, searches can be made faster up by adding Worker nodes. Worker nodes can be added to a live system. Since event data is centrally stored in NFS, newly added Workers can participate in queries.

For deployments with Elasticsearch, the Supervisor node sends each search query to the Elasticsearch Coordinating node, which then distributes each search query to Elasticsearch Data Node and summarizes the partial results sent back from the Data Node to the Supervisor node. Adding Elasticsearch Data Nodes can make up searches faster. Since each Data Node has its own storage, it takes some time for data to be distributed to the newly added Data Node. However, since data is stored locally on each Data Node, this solution scales horizontally.

Rules and Incidents

Rules detect bad behavioral anomalies for machines and users in real time. FortiSIEM has developed SQL-like XML based rule specification language. The user creates a rule from the GUI, tests it using real events, and then deploys the rule. The XML language is quite powerful and uses CMDB Objects (e.g. Device, Network and Application Groups, Event Type Groups, Malware Objects, Country groups, Watch Lists) to keep the rules concise.

A rule specification involves multiple sub-patterns of events connected by temporal operators (AND, OR, AND NOT, FOLLOWED BY, and NOT FOLLOWED BY). Each sub-pattern is like a SQL Query with filters, group by attributes and thresholds on aggregates. The thresholds can be static or dynamically specified based on statistics. A rule can be nested, meaning a rule can be set to trigger another rule. A rule can also create a watch list that, like a CMDB Object, can be used in another rule.

Rule computation happens in a streaming mode using distributed in-memory computation involving Super and Worker nodes. Latest rule definitions are distributed to Super and Worker nodes. Worker nodes evaluate each rule based on the events it sees and periodically sends partial rule results to the Supervisor node. The Supervisor node keeps the global rule state machine and creates an incident when rule conditions are met. When a rule involves a statistical attribute (for example: mean or standard deviation), a baseline report is created which computes the statistics and updates the rule conditions. The baseline report also runs in a streaming mode using in-line distributed computation. When a CMDB Object changes, an App Server module on the Supervisor node sends a change signal to the Worker nodes, which then downloads the changes. This distributed in-memory computation enables FortiSIEM to scale to near real time performance with high EPS and a large number of rules.

Since FortiSIEM analyzes all data including logs, performance and availability metrics, flows and configuration changes, the rule engine can detect suspicious behavior. This ability to cross correlate across different functional IT domains is what makes the FortiSIEM rule framework powerful.

Incident Automation Policy

Once an incident triggers, the user may want to take an action, for example: send an email, create a ticket or initiate a remediation action. Rather than attaching an action to an incident, which does not scale, FortiSIEM takes a policy-based approach. You can write Incident Automation policies involving Time Of Day, Incident Severity, Affected Items, and Affected Organization and attach actions to policies. This allows you to create corporate wide policies on who works on what and on which time of day. Affected items are specified using CMDB Groups and Assigned Users can be specified using CMDB Users – this makes incident automation policies easy to specify and maintain.

Remediation Library

You may want to remediate an incident by running a script. In FortiSIEM, this amounts to creating an Incident Automation Policy and attaching the Remediation Script as an Action to the Automation Policy. The remediation script may run on the Supervisor node or on the Collectors since the enforced devices may be behind a firewall.

When an incident triggers and a Remediation Action has to be taken, the App Server sends a signal to the involved enforcement points (Supervisor and Collectors). The enforcement point first retrieves necessary information (such as enforced on device IP or Host name, enforced on device credentials and incident details) from the Supervisor node and passes that information to the Remediation Script. After the script executes, the Remediation results are attached to the Incident.

FortiSIEM provides a wide collection of inbuilt Remediation Scripts. The user can create new Remediation Scripts in FortiSIEM.

External Ticketing System Integration

This feature allows you to manage a FortiSIEM incident in an external ticketing system. Several API based built-in integrations are available – ServiceNow, Salesforce and ConnectWise. A Java based framework is available for the user to create integrations to other ticketing systems.

There are four types of integrations available – Device or Incident and Inbound or Outbound.

- *Incident Outbound Integration* is used to create a ticket in an external ticketing system.
- *Incident Inbound Integration* is used to update the external ticket status in FortiSIEM of a ticket opened previously using Incident Outbound Integration. If a ticket is closed in external ticketing system, the ticket status is also updated in FortiSIEM.
- *Device Outbound Integration* is used to update CMDB in an external ticketing system from FortiSIEM CMDB. Every ticketing system needs a CMDB.
- *Device Inbound Integration* is used to update FortiSIEM device attributes from an external CMDB.

To use built-in *Incident Outbound* and *Device Outbound Integrations*, define an appropriate integration and attach it as an Action to an Incident Automation Policy. You can use extensive field mappings to customize how the ticket will appear in the external ticketing system. Incident Inbound and Device Inbound integrations have to be scheduled to run at periodic intervals.

Dashboards

FortiSIEM offers various types of dashboards for the user to understand the data it collects and the incidents that are triggering in the system:

- Summary Dashboards
- Widget Dashboards
- Business Service Dashboards
- Identity and Location Dashboards
- Incident Dashboards
- Interface Usage Dashboards
- PCI Logging Dashboards

Summary Dashboards

Summary dashboards show a near real time view of health, up-time, incidents and other key performance metrics of many devices in a single spreadsheet format – each row is a device and each

column is a metric. Cells are color-coded (Red, Yellow, Green) to highlight the values when they cross certain customizable limits. The advantage of this type dashboard is that user can simultaneously compare many metrics of many devices from a single view and instantaneously spot issues. The user can customize the groups of devices and the corresponding metrics. Additionally, the user can build multiple Summary dashboards. FortiSIEM has developed an in-memory database that powers this dashboard – continuous querying event database does not scale. For more information, see Summary Dashboards.

Widget Dashboards

Widget dashboards offer the more traditional Top N dashboard view – one chart for one metric. A wide variety of chart types are available and are described in FortiSIEM Charts and Views.

Any FortiSIEM Report – whether it is reported on Events or on CMDB – can be added to a Widget dashboard. FortiSIEM Widget Dashboards have these distinct advantages.

- Color Coding – Items in each widget can be color coding based on thresholds – this can quickly help the user to spot problems
- Dynamic Search – The user can filter the entire dashboard by Host Name or IP Address to quickly locate what they're searching for
- Streaming Computation – The reports in the widget dashboard are computed in a streaming mode without making repeated queries to the event database. This makes the dashboards fast to load.

For more information, see Widget Dashboards.

Business Service Dashboards

Business Service Dashboards provide a top-down view of Business Service health. The user can see the incidents related to each Business Service and then drill down on the impacted devices and incidents. For more information, see Business Service Dashboards.

Identity and Location Dashboards

Identity and Location dashboards provide a tabular view of network identity to user identity mappings. For more information, see Identity and Incident Dashboards.

Incident Dashboards

FortiSIEM provides two Incident Dashboards – Overview and Risk View.

- The Overview dashboard shows a top-down view into Incidents By Category, Top Incidents and where they are triggering, and Top Impacted Devices and what Incidents they are triggering.
- The Risk View dashboard organizes devices and users by Risk.

For more information, see Overview and Risk View.

Interface Usage Dashboards

This dashboard provides an overview of individual interface usage for Router and Firewall devices. You can obtain metrics at three levels:

device level, interface level and application level. For more information, see Interface Usage Dashboards.

PCI Logging Dashboards

A PCI Logging Status dashboard provides an overview of which devices in PCI are logging. The devices are displayed by CMDB Device Groups (for example Windows, Linux, Firewalls and so on) and by Business Units. For more information, see PCI Logging Dashboards.

Getting Started

Following are the basic steps for getting started with FortiSIEM:

- Step 0 - Pre-Install Considerations
- Step 1 - Install the Virtual or Hardware Appliance
- Step 2 - Install License
- Step 3 - Specify Event Database Storage
- Step 4 - Check System Health and License
- Step 5 - (Optional) Create Organizations for Service Provider Deployments
- Step 6 - (Optional) Check Full Admin Organization Users for Service Provider Deployments
- Step 7 - Add Email Gateway
- Step 8 - (Optional) Add Collector
- Step 9 - (Optional) Set Event Upload Destination for the Collector(s)
- Step 10 - (Optional) Check Collector Health
- Step 11 - Receive Syslog and Netflow
- Step 12 - Check CMDB Devices and Run Searches for received events
- Step 13 - Discover Devices
- Step 14 - Check CMDB and Performance Monitors for discovered devices
- Step 15 - Check Monitored Device health
- Step 16 - Check Incidents
- Step 17 - Notify an Incident via Email
- Step 18 - Create a Ticket in FortiSIEM
- Step 19 - View System Dashboards
- Step 20 - (Optional) Add Worker
- Step 21 - (Optional) Check Worker Health
- Step 22 - Check License Usage
- Step 23 - Set Home Page and Complete Your User Profile
- Step 24 - Log On to the Console and Check Status
- Step 25 - Set up Automated CMDB Disk Space Management
- Step 26 - Create Retention Policy
- Step 27 - Online Documentation and FortiAI

Step 0 - Pre-Install Considerations

FortiSIEM can run in the following modes:

- Single node all in one Virtual Appliance (Supervisor node) running on a wide variety of Hypervisors with local event database storage
- Virtual Appliance Cluster – Supervisor and Worker nodes - external event database storage

- Dedicated hardware appliances – single node with local event database storage or cluster with external event database storage

Before starting the installation process, make the following decisions:

- Installation type: Hardware appliance or Virtual appliance
- If Virtual Appliance, then decide:
  - Hypervisor type – ESX, KVM, Hyper-V, AWS, Azure, Nutanix, Google Cloud Platform, Oracle Cloud Infrastructure
  - Enterprise version or Service Provider version
  - Single node (All-in-one Supervisor) or a Cluster (single Supervisor and multiple Workers)
  - Local event database or External storage (cluster requires external storage)
  - External storage type - FortiSIEM event database or Elasticsearch
  - Whether Collectors are needed
- If hardware appliance, then decide:
  - Enterprise version or Service Provider version
  - Single node (All-in-one Supervisor Appliance) or a Cluster (single Supervisor Appliance e.g. 3500F and multiple Workers e.g. 2000F)
  - Local event database or External storage (cluster requires external storage)
  - External storage type - FortiSIEM event database or Elasticsearch
  - Whether Collectors are needed

Step 1 - Install the Virtual or Hardware Appliance

You can choose to use all-in-one FortiSIEM Hardware Appliance or a Virtual Appliance based solution.

To install FortiSIEM Hardware Appliance (FSM-2000F, FSM-2000G, FSM-2200G, FSM-3500F, FSM-3500G, FSM-3600G, FSM-500F, FSM-500G), see here.

To install a FortiSIEM Virtual Appliance based solution:

- Select the hypervisor (VMWare ESX, AWS, Azure, Hyper-V, KVM, Nutanix, Google Cloud Platform, Oracle Cloud Infrastructure) on which FortiSIEM is going to run
- Select event database storage – local or NFS or Elasticsearch or ClickHouse
  Note: ClickHouse is recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
- Set up external storage if needed: NFS and Elasticsearch
  See *NFS Storage Guide* and *Elasticsearch Storage Guide*
- Install FortiSIEM Virtual Appliance (See the installation guides here.)

Step 2 - Install License

Apply the license provided by Fortinet. Note that for Virtual appliance install, the UUID of the Supervisor node must match the license while for hardware appliance, the hardware serial numbers must match the license.

After applying the license, the system will reboot and provide a login page.

Login with the following default values:

- **USER ID** - admin
- **PASSWORD** - admin*1
- **CUST/ORG ID** - super

- **DOMAIN** - LOCAL

For more information about FortiSIEM Licensing, see the *Licensing Guide* here.

Step 3 - Specify Event Database Storage

If you chose Virtual Appliances, then specify storage option (see here – **ADMIN** > **Setup** > **Storage**).

Hardware appliances only support local disk event database storage.

Step 4 - Check System Health and License

Ensure that:

- All the system components are up and in good health (**ADMIN** > **Health** > **Cloud Health** – see here)
- The license matches your purchase by visiting the **ADMIN** > **License** > **License** page – see here

Step 5 - (Optional) Create Organizations for Service Provider Deployments

A Service Provider would consist of multiple Organizations.

These Organizations can be defined in two ways:

- **Case 1** - By associating one or more collectors to an Organization – any log received by those Collectors or any devices discovered by those collectors will belong to that Organization. This typically makes sense for remote management scenarios.
- **Case 2** - By associating an IP range to an Organization – this typically makes sense for hosted scenarios

In both cases, create organizations by visiting **ADMIN** > **Setup** > **Organizations** (see here).

The system will create default system users with Full Admin functionality for each created organization.

Step 6 - (Optional) Check Full Admin Organization Users for Service Provider Deployments

FortiSIEM will automatically create a Super-global Full Admin user and one Full Admin user for each Organization. Ensure that you are able to log in to:

- each Organization using the system created Full Admin users
- Super-Global mode using Super-global Full Admin user and then switch to any Organization

Step 7 - Add Email Gateway

FortiSIEM will send notifications for incidents via email. Setup the email gateway by visiting **ADMIN** > **Settings** > **System** > **Email** (see here for details).

Step 8 - (Optional) Add Collector

If your monitored devices are behind a firewall or in a distant location across the Internet, then you will need a Collector to collector to collect logs and performance metrics from that location.

FortiSIEM Collectors can be Hardware Appliances or Virtual Appliances. Hardware Appliances are easiest to install.

- For FSM-500F

See *500F Collector Configuration Guide* for the installation above.

Install the FortiSIEM Collector Virtual appliance based on the Hypervisor of your choice:

- VMWare ESX
- AWS
- Azure
- KVM
- Microsoft Hyper-V
- Nutanix
- Google Cloud Platform
- Oracle Cloud Infrastructure

See the specific Installation Guides here for the installations above.

Register the Collector to the FortiSIEM Supervisor node.

See the section *Registering Collectors* for the registration process.

Step 9 - (Optional) Set Event Upload Destination for the Collector(s)

You must specify the FortiSIEM nodes where the Collector will upload events to, in **ADMIN** > **Settings** > **System** > **Worker Upload** (see here). There are three options:

- In a simple setup with one Supervisor node, specify the Supervisor node. This is not recommended in larger setups as this will make the Supervisor node busy.
- You may want to specify one or more Worker nodes, listed by Worker IP addresses. The Collectors will load balance across the specified Worker nodes. In this manner, streaming analytics like inline reports and rule are distributed over Worker nodes.
- You may specify a load balancer name that sits in front of the Worker nodes. Note that in this case, you have to carefully tune the load balancing configuration to get optimum performance.

The second option works the best in most cases.

Step 10 - (Optional) Check Collector Health

You want to make sure that Collectors are up and running properly. Go to **ADMIN** > **Health** > **Collector Health** to check (see here for details).

At this point, the system is ready to receive events or perform discovery.

Step 11 - Receive Syslog and Netflow

First check the list of supported devices whose logs are parsed by FortiSIEM out of the box. The list is **ADMIN** > **Device Support** > **Parsers**. See also the external device support document for further details (see here). If your device is in that list, then FortiSIEM will likely parse your logs out of the box.

Note that with every new version, vendors add new log types or sometimes, even change the log format in a non-backward compatible manner. In that case, the built-in parser may need to be adjusted (this topic will be covered in Advanced Operations). If your device is not on the list of built-in parsed devices, then a custom parser needs to be written. This topic will be covered in Advanced Operations.

Configure your device to send logs to FortiSIEM. If your device is behind a Collector, then the logs will be sent to the Collector. Otherwise, logs can be sent to Supervisor or Worker node. For devices with high event rates, it is recommended to add a Worker node (Step 19) and send logs directly to Worker node. Most vendors have straightforward methods to send syslog to external systems – see here but be aware that the information may be a little out of date. Consider your vendor's manual in that case.

FortiSIEM automatically receives Netflow variations of well-defined ports.

Step 12 – Check CMDB Devices and Run Searches for Received Events

If the logs in Step 11 are received correctly in FortiSIEM, then you should see the sending devices in the correct CMDB device and application group.

You can also search for the logs and see how they are parsed. Go to **ANALYTICS** > **Shortcuts** from the folder drop-down and run 'Raw Messages', 'Top Reporting Devices' or 'Top Event Types' queries (see here for details).

Step 13 - Discover Devices

Some systems (for example, Linux based servers) have generic log patterns – so logs cannot precisely identify the Operating system. If you want to get accurate information from such systems, then you must discover them via protocols such as SNMP, SSH. For Windows servers, if you want to collect logs via WMI, then you must discover them via WMI only or SNMP and WMI.

To perform discovery first go to **ADMIN** > **Setup** > **Credentials** and set up credentials and then go to **ADMIN** > **Setup** > **Discovery** and run discoveries. For Service Provider deployments with collectors, do the discoveries from each organization because IP addresses and names can be overlapping.

You can run the discovery in the foreground or in the background. If you run in the foreground, then you will know when it finishes. If you run in the background, then you must go to Tasks section to see the discovery completion percentages and status. Note that ill-defined discoveries can take a long time to complete – see here for guidelines.

To see the benefits of discovery, see the *External Systems Configuration Guide* here and search your device type.

Step 14 - Check CMDB and Performance Monitors for Discovered Devices

After discovery is complete, you will see the CMDB populated with the discovered devices in the correct device, application and network segment folders.

Note the following:

- If the number of devices is within your license limits, then the discovered devices will be in managed and Pending state. Otherwise, a set of (randomly chosen) devices exceeding license limit will be in the Unmanaged state. FortiSIEM will not receive logs from unmanaged devices, nor they can be monitored. You can flip a device from Unmanaged to Managed and vice-versa. You can also buy additional licenses to rectify this situation.
- If devices have overlapping IP addresses, then they will be merged. Check for this incident “PH_RULE_DEVICE_MERGED_OVERLAP_IP” to look for merged devices. To correct this situation, you have two choices:
  - Change the overlapping IP address on the device, delete the device from CMDB and rediscover.
  - If the overlapping IP is a Virtual IP (VIP), then add this IP to the VIP list in **ADMIN** > **Settings** > **Discovery**. Delete the device from **CMDB** and re-discover.

After you have corrected the situation, make sure that devices are not merged and appear correctly in **CMDB**.

Note that in the enterprise mode, discoveries are done by the Supervisor node. In the Service Provider version, there are two possibilities, depending on how organizations are defined (see Step 5)

- For Organizations defined by IP addresses, discoveries are done by the Supervisor node. After discovery, the devices should belong to the correct organization.
  - If all interfaces of a device belong to the specified Organization IP range, then the device belongs to that Organization.
  - On the other hand, if at least one IP does not belong to specified Organization IP range, then the device belongs to the Super/local Organization (representing the Hosting Service Provider Organization).
- For Organizations with Collectors, discoveries are done by the associated Collector node. Check **CMDB** to see that the devices are marked with the correct Organization and Collector.

As part of discovery, FortiSIEM also discovers which performance metrics it can collect and which logs it can pull. See **ADMIN** > **Setup** > **Pull Events** and **ADMIN** > **Setup** > **Monitor Performance** tabs (see here for details). You can turn off log/performance metric collection or tune the polling intervals.

Performance monitoring and log collection is a continuous process. If you tested the credentials before running discoveries (**ADMIN** > **Setup** > **Credentials** > **Test Connectivity**) and fixed the errors showing up in Discovery error tab, then the metric/log collection should not have errors. After running for some time, there can be errors – some reasons being (a) network connectivity issues from FortiSIEM to the devices, (b) someone changed the credentials or access policies on the device, (c) the device can have performance issues. Please check for errors in the **ADMIN** > **Setup** > **Pull Events** and **ADMIN** > **Setup** > **Monitor Performance** tabs (see here for details) and fix them. If credentials have changed, then you must change the credentials in **ADMIN** > **Setup** > **Credentials** and rediscover the corresponding devices.

Step 15 - Check Monitored Device Health

You can watch the current health of a device in CMDB by selecting the device and choosing the Device health option from the menu. To see the performance metrics in real time, select the device in CMDB and choose the Real time performance option from the menu.

Step 16 - Check Incidents

FortiSIEM provides a large number of built-in machine and user behavior anomalies in the form of rules. These rules are active by default and will trigger incidents. See here on how to navigate incidents. Advanced Operations describes how to tune these rules for your environment.

Step 17 – Notify an Incident via Email

You may want to notify users via email when an incident trigger. This is achieved in one of two ways.

- Create an Incident Automation Policy and specify the incident matching criteria and the receiver email address. See here for details.
- Select an incident from **INCIDENTS** > **List** view, go to **Actions** and select **Notify via Email**. See here for details.

Note that many other advanced actions are possible such as:

- Customizing the email template
- Remediating the incident by running a script
- Opening a ticket in an external ticketing system and so on.

See Advanced Operations for details.

Step 18 – Create a Ticket in FortiSIEM

You can use FortiSIEM built-in ticketing system to handle tickets. Currently, this is handled outside of the notification policy concept (Step 17).

To create a FortiSIEM ticket, select one or more incidents from **INCIDENTS** > **List** view, go to **Actions** and select **Create Ticket**.

Step 19 - View System Dashboards

FortiSIEM provides several built-in dashboards:

- Incident Dashboard – Overview and Risk View
- Incident Location View - (see here for details)
- Incident and Location Dashboard – select **DASHBOARD** > Incident and Location Dashboard (this requires you to collect DHCP, Active Directory logon events – see here for details

Go to **DASHBOARD** and select the dashboard of your choice.

Step 20 - (Optional) Add Worker

For larger software based deployments that involve multiple collectors or large number of monitored devices or devices with high event rates, it is highly recommended to deploy one or more Workers to distribute the Supervisor node's workload. Note that Workers cannot be added to Hardware-based appliances.

Workers can be added by visiting **ADMIN** > **License** > **Nodes** - see here for details.

After adding the Worker(s), remember to add the workers to the collect event upload destination list (**ADMIN** > **Settings** > **System** > **Worker Upload** - see here for details).

Step 21 - (Optional) Check Worker Health

Check the health of the Workers by visiting **ADMIN** > **Health** > **Cloud Health**.

- The health of all nodes should be Normal, load average should be within bounds (typically less than the number of cores), CPU should not be pegged at 99%, and little swap should be used.
- Click on any node and check the health of individual processes running on that node in the bottom pane. Status should be Up with large Up times and reasonable CPU and memory usage.

Step 22 - Check License Usage

Check whether the system is operating within licensed parameters (Monitored device count and EPS) by visiting **ADMIN** > **License** > **Usage** (see here for details).

Step 23 - Set Home Page and Complete Your User Profile

Click the **User Profile** icon ( ) in the upper right corner of the UI. The dialog box contains three tabs:

Basic - Use the **Basic** tab to change your password into the system.

Contact - Use the **Contact** tab to enter your contact information.

UI Settings - Use the **UI Settings** tab to set the following:

Settings	Guidelines
Home	Select the tab which opens when you log in to the FortiSIEM UI.
Incident Home	Select the Overview, List, Risk, Explorer, or MITRE ATT&CK display for the **INCIDENTS** tab.
Case Home	Select the Overview or List display for the **Cases** tab.
Dashboard Home	Select the Dashboard to open by default under the **DASHBOARD** tab from this drop-down list.
Dashboard Settings	Select the type of dashboards to be visible/hidden using the left/right arrows. The up/down arrows can be used to sort the Dashboards.
Language	Specify which language will be used for the UI display. Many UI items have been translated into the languages in the drop-down list, including buttons, labels, top-level headings, and breadcrumbs. Items that are data-driven are not translated.
Theme	Select Dark or Light theme for FortiSIEM UI. Save and refresh the browser to view the change.

Step 24 – Log On to the Console and Check Status

In rare situations when the GUI is not responding, you may need to SSH in to the system console of Supervisor, Worker and Collector nodes and issue some commands. The list of node IP addresses are available in **ADMIN > License > Nodes**, **ADMIN > Health > Cloud Health** and **ADMIN > Health > Collector Health**.

You can login as root for the first time using the password: `ProspectHills`. After the first login, you are forced to change this password.

The following commands are available:

`phstatus`: shows the status of all FortiSIEM processes

`phstatus -a`: shows the detailed status of all FortiSIEM processes along with events per second and local I/O rates

The following Linux commands can be useful:

`top`: shows the CPU, memory usage of all Linux processes

`iostat -x 2`: shows the I/O statistics for local disk

`nfsiostat -x 2`: shows the NFS I/O statistics for Supervisor and Worker for NFS based deployments

`tail -300f /opt/phoenix/log/phoenix.log`: See the C++ module log

Step 25 - Set up Automated CMDB Disk Space Management

If the CMDB disk partition becomes full, then the system may not work correctly. To prevent this from happening, 6.3.2 introduced a CMDB disk space management framework.

Three parameters are introduced in `phoenix_config.txt`.

- `month_retain_limit`: Number of months for which incidents on the Supervisor node should be retained (default value 6 months).

- `cmdb_disk_space_low_threshold` (in MB): When free CMDB disk space falls below this defined threshold, disk management kicks in (default value 50MB).
- `cmdb_disk_space_high_threshold` (in MB): When disk management kicks in, incidents are purged until CMDB disk space reaches this defined threshold (default value 100MB).

Two audit events are introduced.

- `PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and old incidents and identity / location data were pruned to bring the free CMDB disk space above the high threshold (`cmdb_disk_space_high_threshold`).
- `PH_AUDIT_CMDB_DISK_PRUNE_FAILED`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and in spite of pruning older incidents and identity / location data, free CMDB disk space stays below the high threshold (`cmdb_disk_space_high_threshold`). To remedy this situation, the user must reduce the number of months of incidents and identity / location data in CMDB (`month_retain_limit`).

Two system defined rules are included.

- FortiSIEM: CMDB Disk space low - Prune successful.
- FortiSIEM: CMDB Disk space low - Prune failed to keep free disk space above high threshold.

Adjust the CMDB disk management values if necessary.

Step 26 - Create Retention Policy

After the event database has been set up, if you haven't done so already, you may want to create retention policies to optimize how your storage is managed. To do so, follow the steps in Creating a Retention Policy.

Step 27 - Online Documentation and FortiAI

The upper right corner of the UI has two icons that you may find helpful.

- Click the Online Documentation icon ( ) in the upper right corner of the UI to access the FortiSIEM User Guide.
- Click the FortiAI icon ( ) in the upper right corner of the UI to access FortiAI. FortiAI can be configured by following the instructions here.

  FortiAI allows you to enter English language questions, and returns a response. In the case of a report query, validated XML code is provided. You can push this code to the **Analytics** page by clicking on the **Action** drop-down option, selecting "Run on Analytics" (which will take you to the **Analytics** page). On the **Analytics** page, click **Run** to run the provided report.

  For more details, see FortiAI.

Advanced Operations

FortiSIEM enables you to perform advanced operations for the following:

- CMDB
- Incidents and Cases
- Device Support
- Rules, Reports, and Dashboards
- Advanced Health System
- Managing FortiSIEM

CMDB Advanced Operations

FortiSIEM enables you to perform the following CMDB advanced operations.

- Discovering Users
- Creating FortiSIEM Users
- Setting Eternal Authentication
- Setting 2-Factor Authentication
- Assigning FortiSIEM Roles to Users
- Creating Business Services
- Creating Dynamic DMDB Groups
- Setting Device Geo-Location
- Creating CMDB Reports

Discovering Users

Users can be discovered via LDAP, OpenLDAP, or they can be added manually. Discovering users via OpenLDAP or OKTA are similar.

To discover users in Windows Active Directory, discover the Windows Domain Controller:

1. Go to **ADMIN** > **Setup** > **Credentials**.
2. Click **New** to create an LDAP discovery credential by entering the following in the Access Method Definition dialog box:
   a. **Name** for the credential
   b. **Device Type** as "Microsoft Windows Server 2012 R2"
   c. **Access Protocol** as "LDAP"
   d. **Used For** as "Microsoft Active Directory"
   e. Enter the **Base DN** and **NetBios Domain**
3. Test the LDAP Credentials.
4. Run discovery.
5. Go to **CMDB > Users**.
6. Click the "Refresh" icon on left panel and see the users displayed on the right panel.

To add users manually:

1. Go to **CMDB > Users**.
2. Click **New** and add the user information.

For details about Discovering Users, see here (Refer to the table by searching: Credentials for Microsoft Windows Server)

For details about Adding Users, see here.

Creating FortiSIEM Users

To create users that access FortiSIEM:

1. Login as a user with "Full Admin" rights.
2. Create the **user** in CMDB.
3. Set a password – after logging in, the user can set a new password.
4. Select the user and click **Edit**.
5. Select **System Admin** and enter the following:
   a. **Authentication Mode** - "Local" or "External"
   b. **Enterprise case** - select the Role
   c. **Service Provide Case** - select the Role for each Organization

For details about creating users, see here.

To change the password:

1. Login as the user.
2. Click the "User Profile" icon on the top-right corner.
3. Click **Save**.

Setting External Authentication

FortiSIEM users can be authenticated in two ways:

- **Local** authentication – user credentials are stored in FortiSIEM
- **External** authentication – user credentials are stored in an external database (AAA Server or Active Directory) and FortiSIEM communicates with the external database to authenticate the user

Step 1: Set up an Authentication Profile

1. Login as a user with **Full Admin** rights.
2. Create an authentication profile by visiting **ADMIN** > **Settings** > **General** > **External Authentication**.
3. Click **New**.
4. Provide the following information in the External Authentication Profile dialog box:
   a. Enter a Name for the profile
   b. Select an **Organization** from the drop-down list
   c. Set **Protocol** appropriately (for example, LDAP, LDAPS, or LDAPTLS for Active Directory)
   d. Enter the **IP/Host** and **Port** number
5. Make sure the credentials are defined in **ADMIN** > **Setup** > **Credentials**.
6. Select the entry and click **Test** to ensure it works correctly.

Step 2: Attach the Authentication Profile to the user

1. Select the user under **CMDB** > **User** and click **Edit**.
2. Select **System Admin** and click the edit icon.
3. Set **Mode** to "External" and set the Authentication Profile created.

For details about Setting up Authentication Profiles, see here.

For details about Editing Users, see here.

Setting 2-Factor Authentication

FortiSIEM supports Duo as 2-factor authentication for FortiSIEM users:

Step 1: Set up an Authentication Profile

1. Login as a user with **Full Admin** rights.
2. Create an authentication profile by visiting **ADMIN** > **Settings** > **General** > **External Authentication**:
   a. Set **Protocol** to "Duo"
   b. Make sure the credentials are defined in **ADMIN** > **Setup** > **Credentials**
   c. Select the entry and click **Test** to make sure it works correctly

Step 2: Attach the Authentication Profile to the user

- Select the user **CMDB** > **Users** and click **Edit**
- Select **System Admin** and click the edit icon
- Set **Mode** to "External" and set the Authentication Profile created

For details about Setting up Authentication Profiles, see here.

For details about Editing Users, see here.

Assigning FortiSIEM Roles to Users

FortiSIEM allows the admin user to create Roles based on what data the user can see what the user can do with the data. To set up Roles:

Step 1: Create a Role of your choice

1. Login as a user with **Full Admin** rights.
2. Go to **ADMIN** > **Settings** > **Role** > **Role Management**.
3. Make sure there is a Role that suits your needs. If not, then create a new one by clicking **New** and entering the required information. You can also Clone an existing Role and make the changes.

Step 2: Attach the Role to the user

1. Select the user **CMDB** > **Users** and click **Edit**.
2. Select **System Admin** and click the edit icon.

3. Set **Default Role**:
   a. Enterprise case – select the **Role**
   b. Service Provide Case – select **Role** for each Organization

For details about Setting up Roles, see here.

For details about Editing Users,see here.

Creating Business Services

Business Service is a smart grouping of devices. Once created, incidents are tagged with the impacted Business Service(s) and you can see business service health in a custom Business Service dashboard.

For details about creating a Business Service, see here.

For details about setting up Dynamic Business Service, see here.

For details about viewing Business Service health, see here.

Creating Dynamic CMDB Groups and Business Services

CMDB Groups are a key concept in FortiSIEM. Rules and Reports make extensive use of CMDB Groups. While inbuilt CMDB Groups are auto-populated by Discovery, user-defined ones and Business Services are not. You can use the Dynamic CMDB Group feature to make mass changes to user-defined CMDB Groups and Business Services.

To create Dynamic CMDB Group Assignment Rules:

1. Login as a user with **ADMIN** tab modification rights.
2. Go to **ADMIN** > **Settings** > **Discovery** > **CMDB Group**.
3. Click **New**.
4. Enter CMDB Membership Criteria based on **Vendor**, **Model**, **Host Name** and **IP Range**.
5. Select the CMDB group (**Groups**) or Business Services (**Biz Services**) to which the Device would belong if the criteria in Step 3 is met.
6. Click **Save**.

You can now click **Apply** to immediately move the Devices to the desired CMDB Groups and Business Services. Discovery will also honor those rules – so newly discovered devices would belong to the desired CMDB Groups and Business Services.

For details about Setting up Dynamic CMDB Groups and Business Services, see here.

Setting Device Geo-Location

FortiSIEM has location information for public IP addresses. For private address space, you can define the locations as follows:

1. Login as a user with **ADMIN** tab modification rights.
2. Go to **ADMIN** > **Settings** > **Discovery** > **Location**.
3. Click **New**.
4. Enter **IP/IP Range**.
5. Specify the Corresponding **Location** for the IP address Range.
6. Select **Update Manual Devices** if you want already discovered device locations to be updated.
7. Click **Save**.
   You can now click **Apply** to set the geo-locations for all devices matching the IP ranges.

For details about Setting Device Location, see here.

Creating CMDB Reports

If you want to extract data from FortiSIEM CMDB and produce a report, FortiSIEM can run a CMDB Report and display the values on the screen and allows you to export the data into a PDF or CSV file.

For details about Creating CMDB Reports, see here.

Incidents and Cases Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

- Changing the Home Country
- Searching Incidents
- Tuning Incidents via Exceptions
- Tuning Incidents via Modifying Rules
- Tuning Incidents via Drop Rules
- Tuning Incidents by Adjusting Thresholds
- Clearing Incidents
- Adding Comments or Remediation Advice to an Incident
- Remediating an Incident
- Notifying an Incident via Email
- Creating New Rules
- Creating a FortiSIEM Case Manually
- Creating a Case Automatically

Additional Incident related information: Automated Incident Resolution Recommendation

Changing the Home Country

Many rules and reports use the My Home CMDB Object as defined in **RESOURCES** > **Country Groups** > **My Home**. By default, it is set to United States of America.

For details on changing this, see here.

Searching Incidents

If you want to search for specific incidents, go to **INCIDENTS** > **List** > **Actions** > **Search**. A Search Windows appears on left. First, select the Time Window of interest. Then by clicking on any of the criteria, you can see the current values. You can select values to see matches incidents in the right pane.

For details about Searching Incidents, see here.

Tuning Incidents via Exceptions

If you do not want a rule to trigger for a specific Incident Attribute, then you can create an exception.

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incident shows in the right pane.
3. Highlight the Incident.
4. Click **Actions** > **Edit Rule Exception**.
5. Enter the exception criteria – attribute based or time-based.

For details about Tuning Incidents via Exceptions, see here.

Tuning Incidents via Modifying Rules

Sometimes modifying the rule is a better idea than creating exceptions. For example, if you do not want a rule to trigger for DNS Servers, simply modify the rule condition by stating something like “Source IP NOT CONTAIN DNS Server”. To do this:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incident shows in the right pane.
3. Highlight the Incident.
4. Click **Actions** > **Edit Rule**.
5. Edit the Rule.
   If it is a System Rule, then you must save it as a User Rule. Deactivate the old System Rule and activate the new User Rule.

For details, see here.

Tuning Incidents via Drop Rules

Sometimes the rule can be prevented from triggering by dropping the event from rule considerations. There are two choices - (a) store the event in database but not trigger the rule or (b) drop the event completely.

To do this:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incident shows in the right pane.
3. Highlight the Incident.
4. Click **Actions** > **Create Event Dropping Rule**.
5. Specify event drop criteria and action. Events can be dropped on certain parsed fields (like Reporting/Source/Destination IP and Regex filter on the content).

For details, see here.

Tuning Incidents by Adjusting Thresholds

Some performance rules are written using global thresholds, for example - the Rule “High Process CPU: Server” uses the global threshold “Process CPU Util Critical Threshold” defined in **ADMIN** > **Device Support** > **Custom Property**.

You have two choices – (a) modify the global threshold or (b) modify the threshold for a specific device or a group of devices. If you change the global threshold, then the threshold will change for all devices.

To modify the global threshold, follow these steps:

1. Go **ADMIN** > **Device Support** > **Custom Property**.
2. Select the property and click **Edit**.
3. Enter the new value and click **Save**.

For details, see here.

To modify the threshold for one device, follow these steps:

1. Go to **CMDB**.
2. Select the device and click **Edit**.
3. In the **Properties** tab, enter the new value and click **Save**.
   To modify the threshold for a group of devices, repeat the above step for all devices.

Clearing Incidents

In some cases, the Incident may not be happening anymore as the exception condition was corrected.

To clear one or more Incidents:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Clear Incident**.
5. Enter **Reason** and click **OK**.

For details, see here.

Adding Comments or Remediation Advice to an Incident

To add a comment to an Incident:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Edit Comment**.
5. Enter the **Comment** and click **OK**.

For details, see here.

Sometimes, it is necessary to add Remediation advice for the recipient of an Incident, so he can take some action to remediate the Incident. This has to be done by editing the Rule.

1. Go to **RESOURCES** > **Rules**.
2. Select a Rule and click **Edit**.
3. Enter **Remediation Note** text and click **Save**.

For details, see here.

The Remediation text can be added to the Incident Notification email template.

For details, see here.

Remediating an Incident

You can use the following commands to enable Windows Remote Management (WinRM) and set authentication on the target Windows Servers. See Remediations for information on adding, editing, and deleting a remeditation from the FortiSIEM UI.

In the remediation script:

1. When you initiate the WinRM session, set `transport` parameter to `ssl`.
2. Set the `server_cert_validation` option accordingly. If you do not need to validate the certificate, set to `ignore`. For example:
   ```
   session = winrm.Session(enforceOn, auth = (user, password), transport="ssl", server_cert_validation = "ignore")
   ```

In the target Windows server:

Note: You might need to disable Windows Firewall before running remediation.

1. Create the self-signed certificate in the certificate store, for example:
   ```
   New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "mySubjectName.lan"
   ```
   where `Cert:\LocalMachine\My` is the location of the certificate store and `mySubjectName.lan` is the subject alternate name extension of the certificate.

2. Create an HTTPS listener, for example:
   ```
   winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Port
   ="5986";Hostname="{your host name}"; CertificateThumbprint="
   {CertificateThumbprint}"}'
   ```
3. Start the WinRM service and set the service `startup` type to `auto-start`. The `quickconfig` command also configures a listener for the ports that send and receive WS-Management protocol messages using either HTTP or HTTPS on any IP address.
   ```
   winrm quickconfig -transport:https
   ```
4. Validate the WinRM service configuration and Listener.
   a. Check whether basic authentication is allowed, for example:
      ```
      winrm get winrm/config/service
      ```
   b. Check whether a listener is running, and verify the default ports, for example:
      ```
      winrm get winrm/config/listener
      ```

Remediation can be done either on an ad hoc basis (for example, user selects an Incident that has already occurred to Remediate) or using an Automation Policy where the system takes the Remediation action when Incident happens. First, make sure the Remediation script for your scenario is defined. Check the existing Remediation scripts in **ADMIN** > **Settings** > **General** > **Automation Policy** > Remediation settings. If your device is not in the list, add the needed Remediation script.

To set ad hoc remediation:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incident you want to remediate (you can remediate only one Incident at a time)..
4. Click **Actions** > **Remediate Incident**.
5. In the **Run Remediation** dialog box:
   a. Select the script in the **Remediation** drop-down list that you want to run.
   b. Select the role that the script will run on from the **Run On** drop-down list.
   c. Open the **Enforce On** drop-down list to choose which devices the remediation script will run on. In the **Run Remediation** dialog box, open the **Device** tree. Select individual devices and shuttle them to the **Selections** column. (You can choose only individual devices; you cannot choose device groups.)
6. Click **Run** in the **Run Remediation** dialog box.

For details, see here.

To set policy-based remediation:

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New**.
3. Under **Action**, click the edit icon next to **Run Remediation/Script**.
4. In the **Automation Policy - Define Script/Remediation** dialog box click New.
5. In the dialog box that opens, click either **Legacy Script** or **Remediation**:
   - **Legacy Script**:
     - Enter the name and path to the script in the **Script** field.
     - Select the role the script will run on from the **Run On** drop-down list.

- **Remediation**:
  - Select a remediation script from the **Script** drop-down list.
  - Select the role that the script will run on from the **Run On** drop-down list.
  - Open the **Enforce On** drop-down list to choose which devices the remediation script will run on. In the**Automation Policy - Define Script/Remediation - Enforce On** dialog box, open the **Device** tree. Select individual devices and shuttle them to the **Selections** column. (You can choose only individual devices; you cannot choose device groups.)

6. Click **Save**.

For details, see here.

To see the Notification history of an Incident:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Show Notification History**.

For details, see here.

Notifying an Incident via Email

Notifying an Incident can be done either on ad hoc basis (for example - user selects an Incident that has already occurred to notify) or using an Automation Policy where the system takes the notification action when Incident happens.

First, make sure that Email Server has been properly defined in **ADMIN** > **Settings** > **Email** > **Email Settings**.

FortiSIEM has a built-in Incident Notification Email template. If you want a different one, please define it under **ADMIN** > **Settings** > **Email** > **Incident Email Template**.

For details, see here.

To set ad hoc notifications:

1. Go to **INCIDENTS** > **List** view.
2. Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
3. Highlight the Incidents.
4. Click **Actions** > **Notify via Email**.
5. Choose Receive Email Address and Email Template.
6. Click **Send**.

For details, see here.

For Policy based Notification

To send policy-based notifications:

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New**.
3. Specify the Incident Filter Conditions (**Severity**, **Rules**, **Time Range**, **Affected Items**, **Affected Organizations**) carefully to avoid excessive emails.
4. Under **Action**, click **Send Email/SMS to Target Users**.
5. Enter **Email Address** or Users from CMDB.
6. Click Save.

For details, see here.

To see the Notification history of an Incident:

- Go to **INCIDENTS** > **List** view.
- Search the Incident (**Actions > Search**) or make sure that Incidents show in the right pane.
- Highlight the Incidents.
- Click **Action** > **Show Notification History**

For details, see here.

Creating New Rules

Sometime, you may want to create a new rule from scratch.

For details, see here. For additional Incident related information, see Automated Incident Resolution Recommendation .

Creating a FortiSIEM Case Manually

See Creating a FortiSIEM Case Manually.

Creating a Case Automatically

To create an automation policy for automatic case creation, see here.

Device Support Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

- Checking Device Monitoring Status and Health
- Setting Devices Under Maintenance
- Creating Custom Monitors
- Setting Important Interfaces and Processes
- Modifying System Parsers
- Creating Custom Parsers
- Handling Multi-line Syslog
- Creating Synthetic Transaction Monitors
- Mapping Events to Organizations
- Adding Windows Agents
- Adding Linux Agents
- Forwarding Events to External Systems

Checking Device Monitoring Status and Health

For Performance Monitoring scenarios, you would like to know:

- Is FortiSIEM is able to monitor the devices on time? Is FortiSIEM falling behind?
- Are there monitoring errors?
- What is the current health of monitored devices?

To check whether FortiSIEM is able to collect monitoring data on time:

1. Go to **CMDB**.
2. Search for the device and by typing in a string in the search window.
3. Check the **Monitor Status** column.
4. If Monitor Status Warning or Critical, then select the Device and check the Monitor sub-tab in the bottom pane to find out the reason.

FortiSIEM is an optimized multi-threaded solution. If one node is given too many devices to monitor, each device with many metrics, then it may not be able to keep up. If FortiSIEM is not able to keep up (e.g. polling interval is 1 minute and last poll was 3 minutes ago), then you can do one of the following:

1. Check the Monitored Device resources (CPU, memory) and the network between FortiSIEM and the Monitored Device. Many monitoring protocols such as SNMP, WMI will not operate under WAN type latencies (greater than 10 msec).
2. Increase the polling intervals by visiting **ADMIN** > **Setup** > **Monitor Performance** > **More** > **Edit Intervals**.
   Note: If you increase polling intervals, some performance monitoring rules that require a certain

number of polls in a time window may not trigger. Please adjust those rules either by reducing the number of polls or increasing the time window. For example, if a rule needs 3 events (polls) for a 10 min time window with original polling interval as 3 min, the rule will not trigger if polling interval is changed to 4 min or higher. To make the rule trigger again, either reduce the number of events needed (for example, from 3 to 2) or increase the time window (for example, from 10 min to 15 min).

3. Turn off some other jobs by visiting **ADMIN** > **Setup** > **Monitor Performance** > **More** > **Edit Intervals**.
4. Deploy Collectors close to the Monitored Devices or deploy more Collectors and distribute performance monitoring jobs to Collectors by doing re-discovery.

To check for Monitoring errors:

- Go to **ADMIN** > **Setup** > **Monitor Performance** > **More** > **Errors**.

For details see here.

To see current health of a monitored device:

1. Go to **CMDB**.
2. Search for the device and by typing in a string in search window.
3. Choose **Actions** > **Device Health**.

For details, see here.

Setting Devices Under Maintenance

If a device will undergo maintenance and you do not want to trigger performance and availability rules while the device is in maintenance, then

1. Go to **ADMIN** > **Setup** > **Maintenance**.
2. Select the Maintenance Schedule.
3. Select the Group of Devices or Synthetic Transaction Monitors (STM) for maintenance.
4. Make sure the **Generate Incidents for Devices under Maintenance** is checked.

For details, see here

Creating Custom Monitors

Although FortiSIEM provides out of the box monitoring for many devices and applications, user can add monitoring for custom device types or add monitoring for supported device types.

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Click **Enter Performance Object** > **New** and enter the specification of the Performance Object.
3. Select the Performance Object and click **Test**.
4. Click **Enter Device Type to Performance Object Association** > **New** and choose a set of Device Types and associated Performance Objects.
5. Go to **ADMIN** > **Setup** > **Credentials** and enter the Device Credentials for a set of device types specified in Step 4.
6. Go to **ADMIN** > **Setup** > **Discovery** and discover these devices.
7. FortiSIEM will pick the customer monitors defined in Step 2 if the Tests in Step 3 succeeded.
8. Go to **ADMIN** > **Setup** > **Monitor Performance** and see the monitors
   From the same tab, Select one or more devices and Click **More** > **Report** and check whether the monitoring events are generated correctly.

Steps 1-4 are described here.

Steps 5 is described here.

Steps 6 is described here.

Step 8-9 are here.

Setting Important Interfaces and Processes

A network may have hundreds of interfaces and you have may have hundreds of network devices. Not all interfaces may not be interesting for up/down and utilization monitoring. For example, you may only want to monitor WAN links and trunk ports and leave out Access Ports. This saves you lots of CPU and storage. Similar logic applies to critical processes on servers.

Since FortiSIEM discovers interfaces and processes, it is easy to select Critical Interfaces and Processes for Monitoring.

1. Go to **ADMIN** > **Settings** > **Monitoring**.
2. Click **Important Interfaces**> **Enable** > **New** and select the Interfaces.
3. Click **Important Processes**> **Enable**> **New** and select the Processes.

Note that once you select Important Interfaces and Processes, only these Interfaces and Processes will be monitored for availability and performance.

For details, see here.

Modifying System Parsers

If you want to modify a built-in log parser, then do the following steps:

1. Go to **ADMIN** > **Device Support** > **Parsers**.
2. Select a Parser and click **Disable** since you have two parsers for the same device.
3. Select the same Parser and click **Clone**.
4. Make the required modifications to the parser.
5. Click **Validate** to check the modified Parser syntax.
6. Click **Test** to check the semantics of the modified Parser.
7. If both Validate and Test pass, then click **Enable** and then **Save**.
   The modified Parser should show **Enabled**
8. Click **Apply** to deploy the modified Parser to all the nodes.

For details, see here.

Creating Custom Parsers

If you want to create a completely new log parser, then do the following steps:

1. Go to **ADMIN** > **Device Support** > **Parsers**.
2. Parsers are evaluated serially from top to bottom in the list. Select the parser just before the current custom parser and click **New**.
3. Fill in the parser details – **Name**, **Device Type**, test Events and the parser itself.
4. Click **Validate** to check the syntax
5. Click **Test** to check the semantics of the modified parser.
6. If all passes, then click **Enable** and then click **Save**.
   The newly added parser should show **Enabled**.
7. Click **Apply** to deploy the change to all the nodes.

For details, see here.

Handling Multi-line Syslog

When devices send the same log in multiple log messages, you can combine them into one log in FortiSIEM to facilitate analysis and correlation.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Multiline Syslog**.
2. Click **New** to begin a multi-line syslog handling rule.
3. Enter a **Protocol** – TCP or UDP.
4. Enter a **Begin Pattern** and **End Pattern** regular expressions.
   All the logs matching a begin pattern and an end pattern are combined into a single log
5. Click **Save**.

For details, see here.

Creating Synthetic Transaction Monitors

You can define a Synthetic Transaction Monitor to monitor the health an application or a web service. To do this:

1. Go to **ADMIN** > **Setup** > **STM**.
2. **Step 1: Create a monitoring definition**, click **New** and enter the required fields. When the protocol is HTTP, then a Selenium script can be input. Specify the timeout values for detecting STM failures.
3. **Step 2: Apply the monitoring definition to a host**
4. **Step 3: Make sure it is working correctly** - click **Monitor Status**.

For details, see here.

Mapping Events to Organizations

In most cases, the events received by a Collector is tagged with the Organization to which the Collector belongs. In some cases, events for multiple Organizations are aggregated by an upstream device and then forwarded to FortiSIEM. In this case, FortiSIEM needs to map events to organizations based on some parsed event attribute. An example is the FortiGate VDOM attribute.

This is accomplished as follows:

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Event Org Mapping**.
2. Click **New** to create an Event Org mapping definition.
3. Select a **Device Type** from the drop-down list.
4. Specify the **Event Attribute** that contains the Organization information.
5. Specify the **Collector** that will do this Event Org Mapping.
6. Specify an **IP** or **IP Range**.
7. Specify the mapping rules by clicking the edit icon next to **Org mapping**. In the Event Organization Mapping dialog box, map Event Attribute values to Organizations.

For details, see here.

Adding Windows Agents

FortiSIEM Windows Agents provides a scalable way to collect performance metrics, logs and other audit violations from a large number of Windows servers. Windows Agents (version 3.1 onwards) can be configured and managed from the FortiSIEM GUI. Windows Agent Manager is not required. As long as license is available, you can install Windows Agents and register to the FortiSIEM Supervisor node.

For details about Installing Windows Agents, see the latest Windows Agent Installation Guide.

For details about Configuring Windows Agent in FortiSIEM, see here.

Adding Linux Agents

Starting release 5.2.1, Linux Agent requires a license. Install a Linux Agent and register to the FortiSIEM Supervisor node. As long as the license is available, you can install Linux Agent and register to the FortiSIEM Supervisor node. Linux Agents can be configured and managed from the FortiSIEM GUI.

For details about Installing Linux Agents, see Linux Agent Installation Guide.

For details about Configuring Linux Agent in FortiSIEM, see here.

Forwarding Events to External Systems

Events received by FortiSIEM can be forwarded to external systems. FortiSIEM provides a flexible way to define forwarding criteria and forwarding mechanism such as syslog, Kafka and Netflow.

For details, see here.

Rules, Reports and Dashboards Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

- Creating New Rules
- Creating New Reports
- Scheduling Reports
- Customizing Built-in Dashboards
- Creating Custom Dashboards
- Customizing Business Service Dashboards

Creating New Rules

To create new Rules, go to **RESOURCES** > **Rules**, choose a folder and click **New**. Remember to test and activate the rule.

For details, see here.

Rules can also be created from **ANALYTICS** tab. Once you have run a search, create a rule from it by clicking **Actions** > **Create Rule.**

For details, see here.

Creating New Reports

New Reports can be created from **RESOURCES** > **Reports** > Choose a Folder > Click **New**.

For details, see here.

Reports can also be created from **ANALYTICS** tab. Once you have run a search, you can save it as a Report by clicking **Actions** > **Save as Report**.

For details, see here.

Scheduling Reports

Reports can be scheduled to run at later time and contain data for a specific period of time. Go to **RESOURCES** > **Reports** > Choose a Report > **More** > **Schedule**.

For details, see here.

Customizing Built-in Dashboards

FortiSIEM Built-in Dashboards are organized in Folders with multiple Dashboards in each Folder. You can add dashboards to any Folder or modify the dashboards in any built-in folder. Dashboard modification can include – modifying chart layout, chart settings or even adding new widgets for widget dashboards.

For details, see here.

You can also choose to display only a set of Dashboard Folders by visiting **ADMIN** > **Settings** > **System** > **UI** > **Dashboard Settings**.

Creating Custom Dashboards

You can either create a new Dashboard Folder and move dashboards in it or add dashboards to an existing folder.

To create a new Dashboard folder:

1. Click **DASHBOARD**
2. Open the Dashboard Folder drop-down list.
3. Click **New**.

To create a new Dashboard for the folder:

1. Select the Dashboard Folder from the drop-down list.
2. Click **+** to the right of the selected folder.
3. Enter a **Name** and Dashboard **Type** from the drop-down list in the Create New Dashboard dialog box.
4. If you created a Widget Dashboard, click **+** beneath the folder name to add Widgets to the Dashboard.

For details, see here.

Creating Business Service Dashboards

After creating a new Dashboard, choose Type = Business Service Dashboard. Then select the Business Service Selector on the top right to add Business Services to the Dashboard.

For details, see here.

Advanced Health System Advanced Operations

FortiSIEM enables you to perform the following advanced operations:

- Monitoring System Health
- Monitoring Collector Health
- Monitoring Agent Health
- Monitoring Elasticsearch Health
- Monitoring Replication Health
- System Errors
- Monitoring User and Query Activity

Monitoring System Health

To see the system level health of every FortiSIEM Supervisor/Worker node, go to **ADMIN** > **Health** > **Cloud Health**. The top pane shows the overall health of various nodes – Supervisor and Workers. Click any one node and the bottom pane shows the health of the various processes in that node.

For details, see here.

Monitoring Collector Health

To see the system level health of every FortiSIEM Collector node, go to **ADMIN** > **Health** > **Collector Health**.

For details, see here.

Monitoring Agent Health

To see agent health information, go to **ADMIN** > **Health** > **Agent Health**.

For details, see here.

Monitoring Elasticsearch Health

To see the Elasticsearch health information, go to **ADMIN** > **Health** > **Elasticsearch Health**.

For details, see here.

Monitoring Replication Health

To see the Replication health information, go to **ADMIN** > **Health** > **Replication Health**.

For details, see here.

System Errors

To see the system errors, click the **Jobs/Errors** icon on the top-right corner of FortiSIEM GUI and select the **Error** tab. You can also run a report in **ANALYTICS** > click the **Folders** icon > **Shortcuts** > **Top FortiSIEM Operational Errors**.

Monitoring User and Query Activity

To see FortiSIEM User and Query Activity, click the **User Activity** icon ( ) on the top-right corner of FortiSIEM GUI. The User Activity dialog box contains these tabs:

- Logged in Users
- Locked Users
- Query Status
- Query Workload

All of the tabs in the User Activity dialog box contain the time of the last refresh and the number of seconds until the next automatic refresh. By default, the automatic refresh interval is 60 seconds. To refresh the table on demand, click the **Refresh** button.

Logged in Users

This tab displays a table listing the users currently logged in to FortiSIEM. You can perform the following operations on this tab:

- **Log Out** - Select one or more users in the table and click **Log Out**. The selected users will be logged out of FortiSIEM.
- **Log Out and Lock Out** - Select one or more users in the table and click **Log Out and Lock Out**. The selected users will be logged out of FortiSIEM and prevented from logging back in.

The Logged in Users table contains the following information:

Column	Description
Organization	The Organization to which the user belongs.
User	The name of the user.
Full Name	The full name of the user.
Login IP	The IP address from which the user logged in.
Role	The name of the user's role.
Login Time	The date and time when the user logged in.
Session ID	The ID of the user's FortiSIEM session.
Supervisor	The supervisor of the user.

Locked Users

This tab displays a table listing the users currently locked out of FortiSIEM. Typically, user access to FortiSIEM can be locked due to multiple login failures. You can perform the following operations on this tab:

- **Unlock** - Select one or more users in the table and click **Unlock**.

Note: Users can also be unlocked by going to **CMDB > Users > Actions > Unlock**.

The Locked Users table contains the following information:

Column	Description
Organization	The Organization to which the user belongs.
User	The name of the user.
Full Name	The full name of the user.
Login IP	The IP address from which the user logged in.
Role	The name of the user's role.
Locked Time	The date and time when the user was locked out of FortiSIEM.

Query Status

This tab displays a table listing the status of current and recent queries. You can perform the following operations on this tab:

- **Stop Query** - Select a query from the table and click **Stop Query**. The selected query will be stopped remotely. If the query was sent from the **ANALYTICS** page, you should see a warning message saying this query was stopped manually. You should also be able to see the partial results you received before it was stopped.
- **Search** - Click the **Search** button to search for queries by Query name (plain text search), User name (multiple options selected via a checkbox), and/or query Type (multiple options selected via a checkbox).
- **Sort** - Click a column name. You can sort the column data in ascending or descending order.
- **Job Distribution for Query** - Click a query in the Query Status table to see the Job Distribution for Query <*query_name*> table. This table identifies the Worker nodes employed in processing the query and their status. For more information, see Obtaining Job Distribution for Query.

The Query Status table contains the following information:

Column	Description
Query ID	The ID of the query.
Query Name	The name of the query.
Organization	The organization that the query came from.
User	The name of the user who issued the query.
Status	The value of Status can be: • **Running** - The query is currently running. • **Waiting** - The query is waiting in the queue because the maximum number of running queries has been reached.
Type	The value of Type can be: • **Interactive** - Queries executed directly from the **ANALYTICS** page. • **Scheduled Query** - Queries scheduled from **RESOURCES > Reports**. • **Scheduled Rule** - Rule scheduled from **RESOURCES > Rules**.
Submit Time	The date and time when the query was submitted.
Start Time	The date and time when the query was issued.
Progress	The percent of progress the query has made towards completion.
Elapsed	The time, in seconds, that the query has run.
Supervisor	The Supervisor where the query was initiated.

Obtaining Job Distribution for Query

To see how the query job is distributed between nodes, click a query in the Query Status table. The Job Distribution for Query <*query_name*> table appears beneath the Query Status table.

- **Sort** - Click a column name. You can sort the column data in ascending or descending order.

The Job Distribution for Query <*query_name*> table contains the following information:

Column	Description
Node	The node's IP address.
Role	The FortiSIEM handling the query.
Status	The value of Status can be: • **Unknown** - The query process is in an unknown state. • **Starting** - The query has started processing. • **Running** - The query is currently processing. • **Pausing** - The query is in the process of pausing processing. • **Resuming** - The query has resumed processing. • **Stopping** - the query is in the process of stopping processing. • **Paused** - The query has temporarily paused processing. • **Stopped** - The query has stopped processing. • **Completed** - The query has completed processing.
Interactive Tasks	The number of interactive tasks (that is, sent from the **ANALYTICS** page) assigned to the node.
Scheduled Tasks	The number of scheduled tasks assigned to the node.
Task Workload	The total number of tasks assigned to the node.
Progress	The percent of progress the query has made towards completion.
Running For	The time (in seconds) elapsed since the Start Time. *Note: This value is calculated from the last refresh time, not the Last Update minus the Start Time.*
Start Time	The date and time when the query began processing.
Last Update	The data and time when the node last reported a progress update.

Query Workload

This tab displays a table listing the available nodes for a query job. You can perform the following operations on this tab:

- **Sort** - Click a column name. You can sort the column data in ascending or descending order.
- **Status of Running Tasks** - Click a node row in the Query Workload table to display the Tasks Running On <*IP_address*> table. For more information, see Obtaining Running Tasks.

The Query Workload table contains the following information:

Column	Description
Node	The node's IP address.
Role	The role of the node.
Status	The value of Status can be: • **Online** - The node is currently online. • **Offline** - The node is currently offline.
Interactive Tasks	The number of interactive tasks (that is, sent from the **ANALYTICS** page) assigned to the node.
Scheduled Tasks	The number of scheduled tasks assigned to the node.
Task Workload	The total number of tasks assigned to the node.

Obtaining Running Tasks

To see the status of running tasks, click a node in the Query Workload table. The Tasks Running On <*IP_address*> table appears beneath the Query Workload table. You can perform the following operations on this tab:

- **Sort** - Click a column name. You can sort the column data in ascending or descending order.

The Tasks Running On <*IP_address*> table contains the following information:

Column	Description
Query ID	The ID of the query.
Query Name	The name of the query.
User	The name of the user who issued the query.
Type	The value of Type can be: • **Interactive** - Queries executed directly from the **ANALYTICS** page. • **Scheduled** - Queries scheduled from **RESOURCES > Reports**.
Start Time	The date and time when the query began processing.
Status	See Status in Obtaining Job Distribution for Query.
Progress	The percent of progress the query has made towards completion.
Range Start Time	The time the ranged query started.
Range End Time	The time that the ranged query ends.

Managing FortiSIEM Advanced Operations

FortiSIEM provides the following advanced operations to manage your FortiSIEM:

- Administrator Tools
- Backing Up and Restoring FortiSIEM Directories and Databases

Administrator Tools

For information on Administrator Tools, see here.

Backing Up and Restoring FortiSIEM Directories and Databases

For information on Backing Up and Restoring FortiSIEM Directories and Databases, see here.

Administration

The **Admin** tab provides the tools required to setup and monitor FortiSIEM.

The following tools are available:

- Setup
- Device Support
- Health
- License
- Content Update
- Settings

Setup

Before initiating discovery and monitoring of your IT infrastructure, configure the following settings:

- Configuring Storage
- Setting Organizations and Collectors (Service Provider)
- Setting Collectors (Enterprise)
- Setting Credentials
- Discovering Devices
- Editing Event Pulling
- Editing Performance Monitors
- Configuring Synthetic Transaction Monitors
- Configuring Maintenance Calendars
- Configuring Windows Agent
- Configuring Linux Agent
- Configuring FortiSIEM Manager

Configuring Storage

FortiSIEM provides 3 options for storing event data.

- ClickHouse
- EventDB
- Elasticsearch

This document provides separate configuration steps for three event databases.

- Configuring ClickHouse Based Deployments
- Configuring EventDB Based Deployments
- Configuring Elasticsearch Based Deployments
- Changing Event Database
- Changing NFS Server IP

Configuring ClickHouse Based Deployments

This section covers the following topics.

- ClickHouse Configuration Overview
- Configuring ClickHouse Storage on Supervisor Node
- Configuring ClickHouse Topology
- Creating ClickHouse Archive Storage

ClickHouse Configuration Overview

It may be helpful to review the concepts in ClickHouse Operational Overview and the ClickHouse Sizing Guide. First you need to design your ClickHouse Online Cluster and the role of supervisor and worker nodes. There are 3 cases:

1. **Small deployments**: All-in-one deployment using Supervisor Virtual Machine or a hardware appliance like FortiSIEM 2000G or 3500G.
2. **Medium sized deployments**: Supervisor is a member of Keeper Cluster but not the Data Cluster. Workers are members of both Keeper and Data Clusters.
3. **Large deployments**: Supervisor is not a part of Keeper or Data Clusters. Workers entirely form the Keeper and Data Clusters.

The configuration steps involve:

1. Creating storage on Supervisor and Worker nodes depending on their role.
2. Creating a ClickHouse topology to specify the Supervisor and Worker nodes belonging to Keeper cluster and Data cluster.

Next, you need to configure the Archive, where events will be stored after the Online data stores become full. Here are the following options:

- For on-premises deployments, you can use a large Warm disk tier as Archive; or real-time archive to NFS.
- For AWS Cloud deployments, you can use AWS S3 for Archive.
- For GCP deployments you can use GCS for Archive.

After configuring the online and archive storage, you need to specify the retention policies. See How ClickHouse Event Retention Works for details.

Information on Online event database usage can be seen at Viewing Online Event Data Usage.

Information on Archive event database usage can be seen at Viewing Archive Data.

For Advanced Configuration Operations, see Advanced Operations in the Appendix.

Configuring ClickHouse Storage on Supervisor Node

Follow these steps:

Note: Make sure license has been uploaded. This can be done by navigating to **ADMIN > License** and clicking **Upload** to load license. For more information, refer to FortiSIEM Licensing Guide.

1. Navigate to **ADMIN > Setup > Storage** and click **Online** to choose storage.
2. From the **Event Database** drop-down list, select **ClickHouse**.
3. Set **Storage Tiers** and disks following the guidelines below.
4. If your hardware model is 3600G or 2200G or 2000G:
   - **Storage Tiers** count is set to 2 (Hot Tier and Warm Tier).
   - The **Hot and Warm Tier** disks are pre-configured.
   - If you want to add to add more storage, then you can add storage to 3rd Tier. Set **Storage Tiers** to 3 and add NFS mounted storage in **Cold Tier**.

   Note: You cannot mount NFS storage for Hot and Warm tiers.
5. If your hardware model is 3500G or 2000F or 500G:
   - **Storage Tiers** count is set to 1 (Hot Tier).
   - **Hot Tier** disks are pre-configured.
   - If you want to add to add more storage, then you can add storage to 2nd and 3rd Tiers. Set **Storage Tiers** to 2 or 3 and add NFS mounted storage in **Warm Tier** or **Cold Tier** as needed.
6. If you are running on VM, then you can set **Storage Tiers** to 1, 2 or 3 and add disks to each Tier. Note that NFS mounted disks cannot be added to Hot Tier for performance reasons.
   - To add a disk at any tier, click **+** and enter the **Disk Path**.
   - To specify a **locally attached Disk Path**, run `lsblk` command to find **Disk Path**, which should be of the form '/dev/<disk>'
   - To specify a **NFS mounted Disk Path**, enter in the following format:
     `<NFS Server IP or HostName>:<exported mount point>.`
     Example: `192.0.20.0:/mnt/warm`
     For more information, see steps 1 and 2 in the NFS Storage Guide.

Notes:
1. **The mount point should be different for each Worker node and each tier, else the data is going to be overwritten.**
2. **You cannot mount NFS storage for Hot Tier.**
3. If you are planning on using Worker nodes for add storage, see Adding a Worker Node for details.

7. Click **Test** and if successful then **Deploy**.

Configuring ClickHouse Topology

After configuring storage, you need to set up the ClickHouse topology. This involves:

- Selecting the Supervisor or Worker nodes that belong to the ClickHouse Keeper Cluster.
- Choosing the number of shards for the ClickHouse Data cluster.
- Selecting the Worker nodes that belong to the ClickHouse Data cluster.

See ClickHouse Configuration for details.

Creating ClickHouse Archive Storage

Here are the following options:

- For on-premises deployments, you can use a large Cold disk tier as Archive, or you can use real-time archive to NFS.
- For AWS Cloud deployments, you can use AWS S3 for Archive.
- For GCS deployments, you can use GCS for Archive.

Case 1: If you want ClickHouse Cold tier as archive, then configure Cold storage tier in each of the nodes in the ClickHouse Data Cluster. See Adding a Worker Node for details.

Case 2: To configure real-time archive using NFS, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **NFS**.
3. Enter the following parameters:
   a. **IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
   b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Case 3: To configure AWS S3 for Archive, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **AWS S3**.
3. For **Credential Type**, select **Environmental Credentials** or **Explicit Credentials**.
   a. If **Environmental Credentials** is selected, you will need to have an Identity and Access Management. Follow the instructions in Creating IAM Policy for AWS S3 Explicit Credentials to create an IAM Policy
   b. If **Explicit Credentials** is selected, then enter the following information:
      i. **Access Key ID**: Access Key ID required to access the S3 bucket(s)
      ii. **Secret Access Key**: The Secret Access Key associated with the Access Key ID to access the S3 bucket(s)
4. For Buckets:
   a. In the **Bucket** field, enter the bucket URL.
   b. In the **Region** field, enter the region. For example, "us-east-1".
   Note: To minimize any latency, enter the closest region.
   c. If more Buckets are required, click **+** to add a new row.
5. Click **Test**.
6. If the test succeeds, click **Deploy**.
7. Configure each ClickHouse Worker to use the configured S3 bucket.
   a. Navigate to **Admin > License > Nodes**, edit each Worker, check **AWS S3** and choose the Bucket from the drop-down.
   b. Click **Test**, and if the test succeeds, click **Deploy**.
8. If the Supervisor is used as ClickHouse node, take the following steps:
   a. Navigate to **Admin > Setup > Storage**, click **Online**, check **AWS S3** and choose the Bucket from the drop-down.
   b. Click **Test**, and if the test succeeds, click **Deploy**.
9. Apply AWS S3 as the new storage policy to the ClickHouse cluster by taking the following steps.
   a. Navigate to **Admin > Settings > Database > ClickHouse Config**.
   b. Add the AWS S3 bucket(s) to your ClickHouse Cluster Configuration using the appropriate Shard # > Replica # drop-down list.
   c. Click **Test**, and if the test succeeds, click **Deploy**.

Implementation Notes:

1. AWS S3 buckets MUST be created prior to this configuration.
2. When storing ClickHouse data in AWS S3, Fortinet recommends turning Bucket Versioning off, or suspending it (if it was previously enabled). This is because data in ClickHouse files may change and versioning will keep both copies of data - new and old. With time, the number of stale objects may increase, resulting in higher AWS S3 costs. If versioning was previously enabled for the bucket, Fortinet recommends suspending it and configuring a policy to delete non-current versions.
3. Archive data will NOT be automatically purged by FortiSIEM or ClickHouse.
4. S3 archive folder will not be generated until the worker performs its first archive into S3.

Case 4: To configure GCS for Archive, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **GCS**.

3. Enter the following information:
   a. **Access Key ID**: Access Key ID required to access the GCS bucket(s)
   b. **Secret Access Key**: The Secret Access Key associated with the Access Key ID to access the GCS bucket(s)
   Note: See Google IAM documentation here for more information about keys.
4. For Buckets:
   a. In the **Bucket** field, enter the bucket.
   b. If more Buckets are required, click **+** to add a new row.
   Note: See Google Cloud Storage documentation here for more information about buckets.
5. Click **Test**.
6. If the test succeeds, click **Deploy**.
7. Configure each ClickHouse Worker to use the configured GCS bucket.
   a. Navigate to **Admin > License > Nodes**, edit each Worker, check **Archive GCS** and choose the Bucket from the **GCS Bucket** drop-down.
   b. Click **Test**, and if the test succeeds, click **Deploy**.
8. If the Supervisor is used as ClickHouse node, take the following steps:
   a. Navigate to **Admin > Setup > Storage**, click **Online**, check **Archive GCS** and choose the Bucket from the **GCS Bucket** drop-down.
   b. Click **Test**, and if the test succeeds, click **Deploy**.
9. Apply GCS as the new storage policy to the ClickHouse cluster by taking the following steps.
   a. Navigate to **Admin > Settings > Database > ClickHouse Config**.
   b. Add the GCS bucket(s) to your ClickHouse Cluster Configuration by using the appropriate Shard # > Replica # drop-down list.
   c. Click **Test**, and if the test succeeds, click **Deploy**.

Implementation Notes:

1. GCS buckets MUST be created prior to this configuration.
2. When storing ClickHouse data in GCS, Fortinet recommends turning Bucket Versioning off, or suspending it (if it was previously enabled). This is because data in ClickHouse files may change and versioning will keep both copies of data - new and old. With time, the number of stale objects may increase, resulting in higher GCS costs. If versioning was previously enabled for the bucket, Fortinet recommends suspending it and configuring a policy to delete non-current versions.
3. Archive data will NOT be automatically purged by FortiSIEM or ClickHouse.

Creating IAM Policy for AWS S3 Explicit Credentials

Take the following steps from your AWS console.

1. From your **EC2 Dashboard**, select your instance.
2. Navigate to the **IAM dashboard**.
   Note: You can go there by clicking the **IAM** button, or by clicking on **Services** and selecting **IAM**.
3. Click **Policies** to navigate to the **Policies** page, and click **Create policy**.
4. From the **Create policy** page, click the **JSON** tab.

5. Paste the following JSON code into the editor to configure your policy.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "s3:ListStorageLensConfigurations",
            "s3:ListAccessPointsForObjectLambda",
            "s3:GetAccessPoint",
            "s3:PutAccountPublicAccessBlock",
            "s3:GetAccountPublicAccessBlock",
            "s3:ListAllMyBuckets",
            "s3:ListAccessPoints",
            "s3:PutAccessPointPublicAccessBlock",
            "s3:ListJobs",
            "s3:PutStorageLensConfiguration",
            "s3:ListMultiRegionAccessPoints",
            "s3:CreateJob"
         ],
         "Resource":"*"
      },
      {
         "Sid":"VisualEditor1",
         "Effect":"Allow",
         "Action":"s3:*",
         "Resource":[
            "arn:aws:s3:::demo-bucket",
            "arn:aws:s3:::demo-bucket/*"
         ]
      }
   ]
}
```

6. Click the **Next: Tags** button.
   Note: Tags does not need to be configured.
7. Click the **Next: Review** button.
8. On the **Create policy** page, in the **Name** field, enter a name for the policy.
9. Click the **Create policy** button. Your policy has been created.
10. Navigate back to the **IAM dashboard** and click **Roles**, and click **Create role**.
11. For **Select trusted entity**, select **AWS service**.
12. Under **Use case**, select **EC2**.
13. Click **Next**, and then click **Next** again.
14. On the **Name**, **review**, and **create** page, in the **Role name** field, enter a name for the role.
15. Under **Step 2: Add permissions**, click the **Edit** button, and select the policy you created earlier, and click **Next**.
16. Click **Create role**.
17. Navigate to the **Instances** page, select your instance and click the **Security** tab.

18. Click **Actions** (located upper left), and select **Security > Change security groups > Modify IAM role**.
19. Select the role you just created, and click **Update IAM role**.

Configuring EventDB Based Deployment

This section covers the following topics:

- EventDB Configuration Overview
- Creating EventDB Online Storage
- Creating EventDB Archive Storage

EventDB Configuration Overview

EventDB requires a file location for storing events.

- For all-in-one based deployments, you need to create a disk and enter that disk path in the GUI. (Case 1)
- For hardware-based deployments, the disk is already created, and you need to enter specific information in the GUI. (Case 1)
- For cluster-based installations using Workers, you must set up NFS and provide the mount point in the GUI. (Case 2)

You can set up separate Online and Archive EventDB, with separate file locations.

For managing Online and Archive event retention, see How EventDB Event Retention Works.

Information on Online event database usage can be seen at Viewing Online Event Data Usage.

Information on Archive event database usage can be seen at Viewing Archive Data.

Creating EventDB Online Storage

Case 1: If your deployment is on all-in-one node or a hardware appliance, then follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **EventDB Local Disk**.
3. Enter the following information for **Disk Name**.
   a. Hardware appliances: enter “hardware”
   b. Software installs: enter the 4th or 5th disk name that you configured (Refer to your specific Installation Guide in the FortiSIEM Document Library) during FortiSIEM installation. Use the command `fdisk -l` to find the disk name.
4. Click **Test**.

5. If the test succeeds, click **Deploy**.

Case 2: If your deployment has Worker nodes, then you must configure event database on NFS. Make sure you have NFS server setup and then follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **EventDB on NFS**.
3. Enter the following parameters:
   a. **Server IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
   b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Creating EventDB Archive Storage

Follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **NFS**.
3. Enter the following parameters:
   a. **IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
   b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Configuring Elasticsearch Based Deployment

This section covers the following topics:

- Elasticsearch Configuration Overview
- Creating Elasticsearch Online Storage
- Creating Archive for Elasticsearch Based Deployments

Elasticsearch Configuration Overview

FortiSIEM supports 3 Elasticsearch deployments

- Native Elasticsearch – You deploy your own Elasticsearch (Case 1)
- AWS Opensearch (previously known as AWS Elasticsearch) (Case 2)

- Elastic Cloud (Case 1)

Creating Elasticsearch Online Storage

This assumes that you have already deployed Elasticsearch or have an AWS Opensearch or Elastic Cloud account.

Case 1: To configure Native Elasticsearch or Elastic Cloud, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **Elasticsearch**, and from the **ES Service Type** drop-down list, select **Native** or **Elastic Cloud** depending on your Elasticsearch set up.
3. Enter the following parameters.
   a. **Org Storage**: This is relevant for FortiSIEM Multi-tenant deployments. Select one of the following from the drop-down list.
      i. **All Orgs in One Index** – In this option, events from all Organizations are mixed in every Elasticsearch index. This is the most cost-effective option as Elasticsearch does not scale when there are many Organizations with high events per sec, and each Organization being in a separate index may lead to an excessive number of indices (note that Elasticsearch has been observed to have approximately 15K index limit per cluster).
      ii. **Each Org in its own Index** – In this option, events from each Organization is in its own Elasticsearch index. This is a flexible option that provides event isolation among Organizations, but Elasticsearch does not scale when there are many Organizations with high events per sec and each Organization being in a separate index may lead to an excessive number of indices.
      iii. **Custom Org Assignment** – In this option, Organizations can be grouped into Groups (maximum 15 allowed). Organizations belonging to the same group have their events in the same index. This is a balanced approach that provides some amount of event isolation, but does not let the number of indices grow excessively. To create and deploy a custom Organization to Group Mapping, follow these steps:
         i. Click **Edit**.
         ii. In the follow up dialog, click **Add**.
         iii. In the Mapping table, select an Organization in the left column and select the mapped Group in the right column. The 15 specific Groups are numbered 50,001-50,015. Any Organization that is not explicitly mapped, is mapped to the default Group numbered 50,000. A common use case, map 15 of your important customers to the specific groups and the rest to the default groups. Currently, the number of groups (15) is fixed and cannot be changed.
         iv. Click **Deploy**.
   b. **Endpoint**: Click **Edit** and enter the following information:
      i. **URL**: Enter Elasticsearch Coordinator node URL.
      ii. **Ingest/Query** checkbox: If this Coordinator node is to be used for Ingesting Events then check Ingest. If this Coordinator node is going to be used for Querying events, then check the Query flag. If you have multiple Coordinator nodes, then click **+** and select the URL and

Ingest/Query flags. This flexibility enables FortiSIEM to separate a set of Coordinator nodes for Query and Ingest functionalities.

c. **Port**: The TCP port for the URL above (set to HTTPS/443 by default)
d. **User Name**: Enter the username for basic authentication to be used with the URL
e. **Password**: Enter the password for basic authentication to be used with the URL
f. **Shard Allocation**:
    i. If you set it to **Fixed**, then you enter the number of fixed **Shards**, FortiSIEM will not create new shards, even if a Shard reaches its size limit during event surge. You can set the Shard Allocation to Fixed only if you know your system well.
    ii. If you set it to **Dynamic**, then you enter the number of fixed Starting **Shards** (default 5) and FortiSIEM will dynamically adjust the number of shards based on event rate. **This is the recommended method.**
g. **Replicas**: If you set it to N, then there will be N+1 copies of every index in Elasticsearch. The most common value is Replicas = 1. A higher number of replicas can increase query speed and resiliency against failures, but may slow down event ingest and will use more storage space.
h. **Event Attribute Template**: This defines how FortiSIEM Event Attributes are mapped to Elasticsearch Event Attribute Types. This mapping is used to store events in Elasticsearch. If you set it to **Default**, then FortiSIEM will use the default mapping. The default mapping maps all (currently 2000+) FortiSIEM Event Attributes and can be a large file. Since this mapping is stored in every index, the global Elasticsearch state also becomes large. It is possible to use a smaller file by including only the FortiSIEM Event Attributes used in your environment. In that case, set this field to **Custom** and enter the custom mapping file.

4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Case 2: To configure AWS Opensearch, follow these steps:

1. Go to **ADMIN > Setup > Storage**.
2. Click **Online**, and from the **Event Database** drop-down list, select **Elasticsearch**, and from the **ES Service Type** drop-down list, select **Amazon**
3. Enter the following parameters.
    a. **Endpoint**: Click **Edit** and the enter the following information:
        i. **URL**: Enter the AWS Opensearch URL.
        ii. **Ingest/Query** checkbox: If this endpoint is to be used for Ingesting Events, then check Ingest. If this endpoint is going to be used for Querying events, then check the Query flag. If you have multiple endpoints, then click + and select the URL and Ingest/Query flags. This flexibility enables to separate a set of endpoints for Query and Ingest functionalities.
    b. **Port**: The TCP port for the URL above (set to HTTPS/443 by default).
    c. **Access Key ID**: Enter the Access Key ID for use with this endpoint.
    d. **Secret Key**: Enter the Secret Key to be used with this endpoint.
    e. **Shard Allocation**:
        i. If you set it to **Fixed**, then you enter the number of fixed **Shards**, FortiSIEM will not create new shards, even if a Shard reaches its size limit during event surge. You can set the Shard Allocation to Fixed only if you know your system well.

ii. If you set it to **Dynamic**, then you enter the number of fixed Starting **Shards** (default 5) and FortiSIEM will dynamically adjust the number of shards based on event rate. **This is the recommended method.**

f. **Replicas**: If you set it to N, then there will be N+1 copies of every index in Elasticsearch. The most common value is Replicas = 1. A higher number of replicas can increase query speed and resiliency against failures, but may slow down event ingest and will use more storage space.

g. **Event Attribute Template**: This defines how FortiSIEM Event Attributes are mapped to Elasticsearch Event Attribute Types. This mapping is used to store events in Elasticsearch. If you set it to **Default**, then FortiSIEM will use the default mapping. The default mapping maps all (currently 2000+) FortiSIEM Event Attributes and can be a large file. Since this mapping is stored in every index, the global Elasticsearch state also becomes large. It is possible to use a smaller file by including only the FortiSIEM Event Attributes used in your environment. In that case, set this field to **Custom** and enter the custom mapping file.

4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Creating Archive for Elasticsearch Based Deployments

There are 3 archive options

- HDFS Archive from Elasticsearch
- Real-time HDFS Archive from FortiSIEM
- Real-time Archive to NFS

Configuring HDFS Archive from Elasticsearch

In this option, FortiSIEM HDFSMgr process creates Spark jobs to directly pull events from Elasticsearch and store in HDFS. Follow these steps.

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **HDFS**.
3. Enter the following parameters:
   a. Uncheck **Real Time Archive**.
   b. For **Spark Master Node**:
      i. Select **IP** or **Host** and enter the IP address or Host name of the Spark Cluster Master node.
      ii. Set **Port** to the TCP port number for FortiSIEM to communicate to the Spark Master node.
   c. For **HDFS Name Node**:
      i. Select **IP** or **Host** and enter the IP address or Host name of the HDFS Name node. This is the machine which stores the HDFS metadata: the directory tree of all files in the file system, and tracks the files across the cluster.
      ii. Set **Port** to the TCP port number for FortiSIEM to communicate to the HDFS Name node.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Configuring Real-time HDFS Archive from FortiSIEM

In this option, FortiSIEM HDFSMgr process creates Spark jobs to pull events from FortiSIEM Supervisor and Worker nodes. Follow these steps.

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **HDFS**.
3. Enter the following parameters:
   a. Check **Real Time Archive**. Set a Start time (in the future) when the real time archive should begin
   b. For **Spark Master Node**:
      i. Select **IP** or **Host** and enter the IP address or Host name of the Spark Cluster Master node.
      ii. Set **Port** to the TCP port number for FortiSIEM to communicate to Spark Master node.
   c. For **HDFS Name Node**:
      i. Select **IP** or **Host** and enter the IP address or Host name of the HDFS Name node. This is the machine which stores the HDFS metadata: the directory tree of all files in the file system, and tracks the files across the cluster.
      ii. Set **Port** to the TCP port number for FortiSIEM to communicate to HDFS Name node.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Configuring Real-time Archive to NFS

In this option, FortiSIEM Supervisor and Worker nodes store events in NFS managed by FortiSIEM EventDB. This happens while events are getting inserted into Elasticsearch. This approach has no impact in Elasticsearch performance, but events are stored in both Elasticsearch and EventDB and managed independently. Follow these steps.

1. Go to **ADMIN > Setup > Storage**.
2. Click **Archive**, and select **NFS**.
3. Enter the following parameters:
   a. **IP/Host**: [Required] Select **IP** or **Host** and enter the IP address/Host name of the NFS server.
   b. **Exported Directory**: [Required] Enter the file path on the NFS Server which will be mounted.
4. Click **Test**.
5. If the test succeeds, click **Deploy**.

Changing Event Database

It is highly recommended to chose a specific event storage option and retain it. However, it is possible to switch to a different storage type.

Note: In all cases of changing storage type, the old event data is not migrated to the new storage. Contact FortiSIEM Support if this is needed - some special cases may be supported.

For the following cases, simply choose the new storage type from **ADMIN** > **Setup** > **Storage**.

- Local to Elasticsearch
- NFS to Elasticsearch
- Elasticsearch to Local

The following storage change cases need special considerations:

- Elasticsearch to NFS
- Local to NFS
- NFS to Local
- EventDB to ClickHouse
- Elasticsearch to ClickHouse
- ClickHouse to EventDB
- ClickHouse to Elasticsearch

Elasticsearch to NFS

1. Log in to FortiSIEM GUI.
2. Select and delete the existing Workers from **ADMIN** > **License** > **Nodes** > **Delete**.
3. Go to **ADMIN** > **Setup** > **Storage** and update the Storage type as **NFS** server
4. Go to **ADMIN** > **License** > **Nodes** and **Add** the recently deleted Workers in step #2.

Local to NFS

If you are running a single Supervisor, then follow these steps.

1. SSH to the Supervisor and stop FortiSIEM processes by running:
   `phtools --stop all`
2. Unmount `/data` by running:
   `umount /data`
3. Validate that /data is unmounted by running:
   `df -h`
4. Edit /etc/fstab and remove /data mount location.
5. Log in to FortiSIEM GUI, go to **ADMIN** > **Setup** > **Storage** and update the Storage type as **EventDB on NFS**.

If you are running multiple Supervisors in Active-Active cluster, then follow these steps.

1. Log on to Leader.
2. Run steps 1-4 in the single Supervisor case described above.
3. Log on to each Follower and repeat steps 1-4 in the single Supervisor case described above.
4. Log on to Leader, go to **ADMIN > Setup > Storage** and set the Storage type to **EventDB on NFS**.
5. Log on to any node and make sure that all processes are up on all Supervisors.

NFS to Local

1. SSH to the Supervisor and stop FortiSIEM processes by running:
   `phtools --stop all`
2. Unmount /data by running:
   `umount /data`
3. Validate that `/data` is unmounted by running:
   `df -h`
4. Edit /etc/fstab and remove /data mount location.
5. Connect the new disk to Supervisor VM.
6. Log in to FortiSIEM GUI, go to **ADMIN** > **Setup** > **Storage** and update the Storage type as **Local Disk**.

EventDB to ClickHouse

- Single Node Deployment
- Single Supervisor with Workers Deployment
- Multiple Supervisors and Workers Deployment

Assuming you are running FortiSIEM EventDB on a single node deployment (e.g. 2000F, 2000G, 3500G and VMs), the following steps shows how to migrate your event data to ClickHouse.

Follow these steps to migrate events from EventDB to ClickHouse.

1. Stop all the processes on Supervisor by running the following command.
   `phtools --stop all`
   Note: This will also stop all events from coming into Supervisor.
2. Edit `/etc/fstab` and remove all */data* entries for EventDB.
3. If the same disk is going to be used by ClickHouse (e.g. in hardware Appliances), then copy out events from FortiSIEM EventDB to a remote location. You can bring back the old data if needed (See Step 7).
   a. Mount a new remote disk for the appliance, assuming the remote server is ready, using the following command.`# mount -t nfs <remote server ip>:<remote share point> <local path>`
   b. Copy the data, using the following command.
      `# rsync -av --progress /data /<local path>`
      Example: `# rsync -av --progress /data /mnt/eventdb`
4. If the same disk is going to be used by ClickHouse (e.g. in hardware Appliances), then delete old data from FortiSIEM, by taking the following steps.
   a. Remove the data by running the following command.
      `# rm -rf /data/*`
   b. Unmount, by running the following commands.
      `# note mount path for /data`
      `# umount /data`
   c. For 2000G, run the following additional command.
      `# lvremove /dev/mapper/FSIEM2000G-phx_eventdbcache: y`

5. For VM based deployments, create new disks for use by ClickHouse by taking the following steps.
   a. Edit your Virtual Machine on your hypervisor.
   b. Add a new disk to the current disk controller.
   c. Run the following in your FortiSIEM Supervisor Shell if the disk is not automatically added.
   ```
   # echo "- - -" > /sys/class/scsi_host/host0/scan
   # echo "- - -" > /sys/class/scsi_host/host1/scan
   # echo "- - -" > /sys/class/scsi_host/host2/scan
   # lsblk
   ```
6. Log into the GUI as a full admin user and change the storage to ClickHouse by taking the following steps.
   a. Navigate to **ADMIN > Setup > Storage > Online**.
   b. From the **Event Database** drop-down list, select **ClickHouse**.
   c. From the **Storage Tiers** drop-down list, select **1**.
   d. In the Disk Path field, select the disk path.
   Example: `/dev/sde`
   e. Click **Test**.
   f. Click **Deploy**.
   g. Navigate to **Admin > Settings > Database > ClickHouse Config**, and click **Test** and then click **Deploy**.
7. (Optional) Import old events. For appliances they were copied out in Step 3 above. For VMs, they may be mounted remotely. To do this, run the following command from FortiSIEM.
   `# /opt/phoenix/bin/phClickHouseImport --src [Source Dir] --starttime [Start Time] --endtime [End Time] --host [IP Address of ClickHouse - default 127.0.0.1] --orgid [Organization ID (0 – 4294967295)`
   More information on `phClickHouseImport` can be found here.
   Note the valid time format:
   <time> : *"YYYY-MM-DD hh:mm:ss"* (notice the quotation marks, they need to be included.)
   Example:
   `phClickHouseImport --src /test/sample --starttime "2022-01-27 10:10:00" --endtime "2022-02-01 11:10:00"`
   Example with import all organizations:
   ```
   [root@SP-191 mnt]# /opt/phoenix/bin/phClickHouseImport --src /mnt/eventdb/ --starttime "2022-01-27 10:10:00" --endtime "2022-03-9 22:10:00"
   Found 32 days' Data
   [▉ ] 3% 3/32 [283420]▉
   ```
8. Log into FortiSIEM GUI and use the **ANALYTICS** tab to verify events are being ingested.
   Note: If your Single Node deployment also contains Workers, proceed to the next section for Worker configuration.

If you are running a single Supervisor with Workers, take the following steps for your Workers, after following the prior steps for your Supervisor in Single Node Deployment.

1. Navigate to **Admin > License**.
2. Click the **Nodes** tab.
3. From the **License > Nodes** page, take the following steps for each Worker.
   a. Select a Worker, and click **Edit**.
   b. Add disks.
   c. Click **Test**.
   d. Click **Save**.

   e. Repeat steps 3.a-3.d for each Worker. Proceed to step 4 after all Workers have been configured.
4. Navigate to **Admin > Settings > Database > ClickHouse Config**, and click **Test** and then click **Deploy**.

If you are running multiple Supervisors, Workers with EventDB on NFS and want to switch to ClickHouse, take the following steps:

1. Power off all Supervisors, Workers and add new disks for ClickHouse.
2. Power on all Supervisors, Workers.
3. Wait until all processes are up.
4. SSH to Primary Leader Supervisor node.
   a. Run the following command.
   `phtools --stop all`
   b. Unmount `/data` by running the following command.
   `umount /data`
   c. Validate that `/data` is unmounted by running the following command.
   `df -h`
   d. Edit `/etc/fstab` and remove `/data` mount location.
5. Repeat Step 4 for all Primary Follower Supervisor nodes.
6. SSH to Primary Leader Supervisor node.
   a. Configure ClickHouse following the steps in Configuring ClickHouse Based Deployments.
   b. Run the following command.
   `phtools --start all`
7. Log into FortiSIEM GUI and use the **ANALYTICS** tab to verify events are being ingested.

Elasticsearch to ClickHouse

To switch your Elasticsearch database to ClickHouse, take the following steps.

Note: Importing events from Elasticsearch to ClickHouse is currently not supported

1. Stop all the processes on Supervisor by running the following command.
   `phtools --stop all`
   Note: This command will also stop all events from coming into the Supervisor. Make sure `phMonitor` process is running.
2. Log into your hypervisor and add disks for ClickHouse by taking the following steps. You can have 3 Tiers of disks with multiple disks in each Tier. You must have at least 1 Tier one disk.
   a. Edit your Virtual Machine on your hypervisor.
   b. Add a new disk to the current disk controller.
   c. Run the following in your FortiSIEM Supervisor Shell if the disk is not automatically added.
   ```
   # echo "- - -" > /sys/class/scsi_host/host0/scan
   # echo "- - -" > /sys/class/scsi_host/host1/scan
   # echo "- - -" > /sys/class/scsi_host/host2/scan
   # lsblk
   ```

3. Set up ClickHouse as the online database by taking the following steps.Events can now come in.
   a. Navigate to **ADMIN > Setup > Storage > Online**.
   b. From the **Event Database** drop-down list, select **ClickHouse**.
   c. From the **Storage Tiers** drop-down list, select **1**.
   Note: If you wish to have a warm tier or multiple hot tier disks, additional disks are required
   d. Provide the disk path.
   e. Click **Test**.
   f. Click **Deploy** when the test is successful.
4. Log into FortiSIEM GUI and use the **ANALYTICS** tab to verify events are being ingested.

ClickHouse to EventDB

To switch your ClickHouse database to EventDB, take the following steps.

Note: Importing events from ClickHouse to EventDB is currently not supported.

1. Stop all the processes on the Supervisor by running the following command.
   `phtools --stop all`
   Note: This is will also stop all the events from coming into Supervisor.
2. Stop ClickHouse Service by running the following commands.
   ```
   systemctl stop clickhouse-server
   systemctl stop phClickHouseMonitor
   ```
3. Edit `phoenix_config.txt` in `/opt/phoenix/config` on Supervisor and set `enable = false` for ClickHouse.
4. Edit and remove any mount entries in `/etc/fstab` that relates to ClickHouse.
5. Unmount data by taking the following step depending on whether you are using a VM (hot and/or warm disk path) or hardware (2000F, 2000G, 3500G).
   a. For VM, run the following command.
   `umount /data-clickhouse-hot-1`
   If multiple tiers are used, the disks will be denoted by a number.
   Example:
   ```
   /data-clickhouse-hot-2
   /data-clickhouse-warm-1
   /data-clickhouse-warm-2
   ```
   b. For hardware, run the following command.
   `umount /data-clickhouse-hot-1`
   c. For 2000G, run the following additional commands.
   ```
   umount /data-clickhouse-warm-1
   lvremove /dev/mapper/FSIEM2000Gphx_hotdata : y
   ```
6. Delete old ClickHouse data by taking the following steps.
   a. Remove old ClickHouse configuration by running the following commands.
   ```
   # rm -f /etc/clickhouse-server/config.d/*
   # rm -f /etc/clickhouse-server/users.d/*
   ```
7. Clean up "incident" in psql, by running the following commands.
   ```
   psql -U phoenix -d phoenixdb
   truncate ph_incident;
   truncate ph_incident_detail;
   ```

8. Configure storage for EventDB by taking the following steps.
   - For VMs, proceed with Step 9, then continue.
   - For hardware appliances 2000F, 2000G, or 3500G, proceed to Step 10.
9. Set up EventDB as the online database by taking the following steps for Creating EventDB Online Storage (Local Disk) OR Creating EventDB Online Storage (NFS).
   a. For EventDB Local Disk configuration, take the following steps.
      i. Create a new disk for the VM by logging into the hypervisor and create a new disk.
      ii. Log into the FortiSIEM Supervisor GUI as a full admin user.
      iii. Navigate to **ADMIN > Setup > Storage > Online**.
      iv. From the **Event Database** drop-down list, select **EventDB Local Disk**.
      v. Target the new local disk.
      vi. Click **Test**.
      vii. Click **Deploy**.
      viii. Proceed to Step 11.
   b. For EventDB on NFS configuration, take the following steps.
      Note: Make sure remote NFS storage ready.
      i. Create a new disk for the VM by logging into the hypervisor and create a new disk.
      ii. Log into FortiSIEM Supervisor GUI as a full admin user.
      iii. Navigate to **ADMIN > Setup > Storage > Online**.
      iv. From the Event Database drop-down list, select **EventDB on NFS**.
      v. In the **IP/Host** field, select **IP** or **Host** and enter the remote NFS server IP Address or Host name.
      vi. In the **Exported Directory** field, enter the share point.
      vii. Click **Test**.
      viii. Click **Deploy**.
      ix. Proceed to Step 11.
10. Set up EventDB as the online database, by taking the following steps.
    a. Log into the FortiSIEM Supervisor GUI as a full admin user.
    b. Navigate to **ADMIN > Setup > Storage > Online**.
    c. From the **Event Database** drop-down list, select **EventDB**.
    d. Click **Test**.
    e. Click **Deploy**.
11. Make sure phMonitor process is running. Events can now come in.
12. Verify events are coming in by running Adhoc query in **ANALYTICS**.

ClickHouse to Elasticsearch

To switch your ClickHouse database to Elasticsearch, take the following steps.

Note: Importing events from ClickHouse to Elasticsearch is currently not supported.

1. Stop all the processes on Supervisor by running the following command.
   `phtools --stop all`
   Note: This is will also stop all the events from coming into Supervisor.

2. Stop ClickHouse Service by running the following commands.
   ```
   systemctl stop clickhouse-server
   systemctl stop phClickHouseMonitor
   ```
3. Edit `phoenix_config.txt` on the Supervisor and set `enable = false` for ClickHouse.
4. Edit and remove any mount entries in `/etc/fstab` that relates to ClickHouse
5. Unmount data by taking the following step depending on whether you are using a VM (hot and/or warm disk path) or hardware (2000F, 2000G, 3500G).
   a. For VM, run the following command.
      ```
      umount /data-clickhouse-hot-1
      ```
      If multiple tiers are used, the disks will be denoted by a number:
      Example:
      ```
      /data-clickhouse-hot-2
      /data-clickhouse-warm-1
      /data-clickhouse-warm-2
      ```
   b. For hardware, run the following command.
      ```
      umount /data-clickhouse-hot-1
      ```
   c. For 2000G, run the following additional commands.
      ```
      umount /data-clickhouse-warm-1
      lvremove /dev/mapper/FSIEM2000Gphx_hotdata : y
      ```
6. Delete old ClickHouse data by taking the following steps.
   a. Remove old ClickHouse configuration by running the following commands.
      ```
      # rm -f /etc/clickhouse-server/config.d/*
      # rm -f /etc/clickhouse-server/users.d/*
      ```
7. Clean up "incident" in psql, by running the following commands.
   ```
   psql -U phoenix -d phoenixdb
   truncate ph_incident;
   truncate ph_incident_detail;
   ```
8. Make sure `phMonitor` process is running.
9. Setup Elasticsearch as online database by taking the following steps.
   a. Log into the FortiSIEM Supervisor GUI as a full admin user.
   b. Navigate to **ADMIN > Setup > Storage > Online**.
   c. From the **Event Database** drop-down list, select **Elasticsearch**.
   d. From the **ES Service Type** drop-down list, select **Native**, **Amazon**, or **Elastic Cloud**.
   e. Configure the rest of the fields depending on the ES Service Type you selected.
   f. Click **Test**.
   g. Click **Deploy**.
10. Wait for `JavaQuerySever` process to start up.
11. Start new events.
12. Verify events are coming in by running Adhoc query in **ANALYTICS**.

Changing NFS Server IP

If you are running a FortiSIEM Cluster using NFS and want to change the IP address of the NFS Server, then take the following steps.

Step 1: Temporarily Change the Event Storage Type from EventDB on NFS to EventDB on Local

1. Go to **ADMIN > License > Nodes** and remove all the Worker nodes.
2. SSH to the Supervisor and stop FortiSIEM processes by running:
   `phtools --stop all`
3. Unmount `/data` by running:
   `umount /data`
4. Validate that `/data` is unmounted by running:
   `df -h`
5. Edit `/etc/fstab` and remove `/data` mount location.
6. Attach new local disk to the Supervisor. It is recommended that it is at least 50~80GB.
7. Go to **ADMIN > Setup > Storage > Online**.
8. Change the storage type to **Local Disk** and add the local disk's partition to the **Disk Name** field. (e.g. `/dev/sde`).
9. Click **Test** to confirm.
10. Click **Deploy**.

Step 2: Change the NFS Server IP Address

This is a standard system administrator operation. Change the NFS Server IP address.

Step 3: Change the Event Storage Type Back to EventDB on NFS

1. SSH to the Supervisor and stop FortiSIEM processes by running:
   `phtools --stop all`
2. Umount `/data` by running:
   `umount /data`
3. Validate that `/data` is unmounted by running:
   `df -h`
4. Edit `/etc/fstab` and remove `/data` mount location.
5. Go to **ADMIN > Setup > Storage > Online**.
6. Change the storage type to **NFS**.
7. In the **Server** field, with **IP** selected, enter the new IP address of the NFS server.
8. In the **Exported Directory** field, enter the correct NFS folder's path.
9. Click **Test** to confirm.
10. Click **Deploy**.
11. Go to **ADMIN > License > Nodes** and add back all the Worker nodes.

Setting Organizations and Collectors (Service Provider)

FortiSIEM supports multi-tenancy via Organizations in a Service Provider deployment. The devices and logs belonging to two Organizations are kept separate. Incidents trigger separately for Organizations.

A Collector enables FortiSIEM to collect logs and performance metrics from geographically disparate networks. Data collection protocols such as SNMP and WMI are often chatty and the devices may only be reachable from the Supervisor node via Internet and behind a firewall. Syslog protocol specially over UDP is unreliable and insecure. A Collector can be deployed behind the firewall to solve these issues. The Collector registers with FortiSIEM Supervisor node and then receives commands from the Supervisor regarding discovery and data collection. The Collector parses the logs and forwards the compressed logs to Supervisor/Worker nodes over an encrypted HTTPS channel. The Collector also buffers the logs locally for a period of time if the network connection to the Super/Worker is not available.

Organizations can be defined in one of two ways:

- Associating one or more Collectors to an Organization – the devices monitored by the Collector or the events sent to the Collector automatically belong to the associated Organization.
- Defining an IP range for an Organization – if the sending IP of a device belongs to the IP range, then the device and logs belong to that Organization.

This section provides the procedures to configure an Organization for a multi-tenant FortiSIEM deployment.

- Creating an Organization
- Installing a Collector
- Registering a Collector

Note: For information on Diode Collector, see the Diode Collector Installation Guide.

Make sure the Worker Upload has been configured prior to defining the Collectors.

Creating an Organization

Complete these steps to add an Organization:

1. Go to **ADMIN** > **Setup** > **Organizations** tab.
2. Click **New**.

3. In the **Organization Definition** dialog box, enter the information below.

Settings	Guidelines
Organization	[Required] Name of the Organization
Full Name	Full name of the Organization
Admin User	[Required] User name that will be used two purposes: (a) Users logging in to FortiSIEM Supervisor GUI for that Organization and (b) Collector registration to Supervisor. This user has 'Full Admin' role.
Admin Password/Confirm Admin Password	[Required] Password of the Admin user.
Admin Email	[Required] Email id of the Admin user for the Organization.
Phone	Contact number for the Organization
Include IP/IP Range	IP range for the Organization in case the Organization is defined by IP addresses. Allowed format is comma-separated individual IPs or IP range 10.10.10.1-10.10.10.8
Exclude IP/IP Range	IP range to be excluded for the Organization. Allowed format is comma-separated individual IPs or IP range 10.10.10.1-10.10.10.8
Agent User	User name used by FortiSIEM Windows and Linux Agents to register to FortiSIEM Supervisor. **Note**: An Agent User cannot be used to log into the UI.
Agent Password/Confirm Agent Password	Password of Agent User.
Max Devices	Maximum number of monitored CMDB devices for the Organization
Address	Contact address for the Organization

4. If your Organization uses Collectors, click **New** under **Collectors** and enter the information below.

Settings	Guidelines
Name	[Required] Name of the Collector
Guaranteed EPS	[Required] Events from this Collector are always accepted when its event rate is below this Guaranteed EPS. FortiSIEM will re-allocate excess EPS (license minus the sum of Guaranteed EPS over all the collectors) based on need but the allocation will never go below the Guaranteed EPS.
Upload Rate Limit (Kbps)	Maximum rate limit (in Kbps) at which a Collector can send events to all Workers.
Upload EPS Limit	Maximum events per second at which a Collector can send events to all Workers. EPS limit is enforced at periodic 3 minute intervals. When either the upload rate limit or EPS limit are hit, events are buffered at the Collector and sent later.
Start Time	[Required] Select a specific start date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.
End Time	[Required] Select a specific end date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.
Event Worker	Worker list that Collector uploads event files to.

5. Enter the **Description** about the Organization.
6. Click **Save**.

Installing a Collector

For installing Collectors, see the "Install Collector" sections in the specific Installation Guides.See also the Upgrade Guide and the Sizing Guides available in the FortiSIEM Documents Library here.

Registering a Collector

Once a Collector has been created in the GUI, the Collector needs to be installed and registered.

For registering a Collector, follow these steps:

1. SSH to the Collector.
2. Run the following command:
   phProvisionCollector --add <user> '<password>' <super IP or host> <organization> <collectorName>
   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped. In Enterprise mode, use `super` as the organization .

Refer to the tables in steps 3 and 4 here for more information about these settings: `<user>`, `<password>`, `<organization>` and `<collectorName>`

Complete these steps to add a Collector:

1. Go to **ADMIN** > **Setup** > **Collector** tab.
2. Click **New**.
3. In the **Event Collector Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Collector name
Guaranteed EPS	[Required] Events from this Collector are always accepted when its event rate is below this Guaranteed EPS. FortiSIEM will re-allocate excess EPS (license minus the sum of Guaranteed EPS over all the collectors) based on need but the allocation will never go below the Guaranteed EPS.
Upload Rate Limit (Kbps)	Maximum rate limit (in Kbps) at which a Collector can send events to all Workers. Rate limit is enforced at periodic 3 minute intervals. When either the upload rate limit or EPS limit are hit, events are buffered at the Collector and sent later.
Upload EPS Limit	Maximum events per second at which a Collector can send events to all Workers. EPS limit is enforced at periodic 3 minute intervals. When either the upload rate limit or EPS limit are hit, events are buffered at the Collector and sent later.
Start Time	[Required] Select a specific start date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.
End Time	[Required] Select a specific end date or check 'Unlimited'. Collectors will not work outside of start and end dates if specific dates are chosen.
Event Worker	Worker list that Collector uploads event files to.

4. Click **Save**.

Installing a Collector

For installing Collectors, see the "Install Collector" sections in the specific Installation Guides. See also the Upgrade and Sizing Guides available in the FortiSIEM Documents Library here.

Registering a Collector

Once a Collector has been created in the GUI, the Collector needs to be installed and registered.

For registering a Collector, follow these steps:

1. SSH to the Collector.
2. Run the following command:
   phProvisionCollector --add <user> '<password>' <super IP or host> <organization> <collectorName>
   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped. In Enterprise mode, use `super` as the organization .
   Refer to the tables in steps 3 and 4 here for more information about these settings: `<user>`, `<password>`, `<organization>` and `<collectorName>`

Setting Credentials

FortiSIEM communicates with various systems to collect operating system/hardware/software information, logs, and performance metrics. This section provides the procedures to set up a device credential and associate them to an IP or IP range. For information on generalized HTTPS based event collection, refer to "Generic Log API Poller (HTTPS Advanced) Integration" in the Appendix of the latest External Systems Configuration Guide.

- Creating a Credential
- Associating a Credential to IP Ranges or Hosts
- Testing Credentials and API Event Collection
- Modifying Device Credential
- Modifying a Credential Association
- Credentials Based on Access Protocol

Creating a Credential

Complete these steps to create a login credential:

1. Go to **ADMIN** > **Setup** > **Credentials** tab.
2. Under **Step 1: Enter Credentials** section, click **New**.
3. In the **Access Method Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Name of the credential that will be used for reference purpose.
Device Type	Type of device from the drop-down.
Access Protocol	Type of access protocol from the drop-down. Note that this list depends on the selected device type.
Port	TCP/UDP Port number for communicating to the device for the access protocol.
Password config	Choose **Manual**, **CyberArk SDK** or **CyberArk REST API**. - **Manual**: The credentials will be defined and stored in FortiSIEM. See the External Systems Configuration Guide for the corresponding device type configuration settings. - **CyberArk SDK**: FortiSIEM will get credentials from CyberArk password Vault. See "CyberArk SDK Password Configuration" in the External Systems Configuration Guide for configuration settings. -**CyberArk REST API**: FortiSIEM will get credentials from CyberArk password Vault through REST API access. See "CyberArk REST API Password Configuration" in the External Systems Configuration Guide for configuration settings.

4. Enter the options in the remaining fields that appear based on the **Device Type** selection.
5. Click **Save**.

Associating a Credential to IP Ranges or Hosts

The association is on a per-Collector basis.

1. Under **Step 2: Enter IP Range to Credential Associations** section, click **New**.
2. In the **Device Credential Mapping Definition** dialog box, enter the information below.

Settings	Guidelines
IP/Host Name	[Required] Host name, IP address or IP range to associate with a credential. Allowed IP range syntax is single IP, single range, single CIDR or a list separated by comma – e.g. 10.1.1.1, 10.1.1.2,20.1.1.0/24, 30.1.1.1-30.1.1.10. Host names are only allowed for a specific set of credentials see below.
Credentials	Select one or more credentials by name. Use **+** to add more.

3. Click **Save**.

Testing Credentials and API Event Collection

Credentials can be tested to ensure that they are working correctly and do not perform a full discovery, and therefore provide results more quickly.

Test Connectivity also has a special function for certain Device API integrations. Instead of performing separate Discovery to integrate FortiSIEM with a Device API, clicking **Test Connectivity** will test the credential and start collecting event from the API. The External System Configuration Guide details Device integrations that require only this step to collect events.

1. If the user assigns a Test Connectivity or Discovery task to a Collector, then the Collector performs those tasks. The Supervisor also assigns the performance monitoring task to the same Collector that performed discovery.
2. For environments without Collector:
   a. Supervisor does discovery and Test Connectivity.
   b. Supervisor then assigns the performance monitoring tasks to the Active Workers in a weighted round robin fashion. Some jobs like vCenter monitoring has a higher weight than simple SNMP based CPU monitoring.
   c. Workers perform the performance monitoring tasks.
   d. If a Worker is removed, its performance monitoring jobs are redistributed to other Workers.
   e. If a Worker is added, new performance monitoring jobs are assigned to that Worker.
   f. If you disable and then enable performance monitoring jobs from the GUI, then a new global job distribution takes place.

1. Select an association.
2. Click **Test** after choosing:
   - **Test Connectivity** – the device will be pinged first and then the credential will be attempted. This shortens the test connectivity process in case the device with specified IP is not present or reachable.
   - **Test Connectivity without Ping** – the credential will be attempted without pinging first.
3. Check the test connectivity result in the pop up display.

Modifying Device Credentials

Complete these steps to modify device credentials:

1. Select an association from the list and click the required option.
   - **Edit** - to modify any credential settings.
   - **Delete** - to delete a credential.
   - **Clone** - to duplicate a credential.
2. Click **Save**.

Modifying a Credential Association

Complete these steps to modify a credential association:

1. Select the credential association from the list and click the required option under **Step 2: Enter IP Range to Credential Associations**:
   - **Edit** - to edit an associated IP/IP range
   - **Delete** - to delete any association
2. Click **Save**.

Credentials Based on Access Protocol

For information on the credential configuration settings for selected devices, see the External Systems Configuration Guide.

Discovering Devices

FortiSIEM automatically discovers devices, applications, and users in your IT infrastructure and start monitoring them. You can initiate device discovery by providing the credentials that are needed to access the infrastructure component, and from there FortiSIEM will discover information about your component such as the host name, operating system, hardware information such as CPU and memory, software information such as running processes and services, and configuration information. Once discovered, FortiSIEM will also begin monitoring your component on an ongoing basis.

1. If the user assigns a Test Connectivity or Discovery task to a Collector, then the Collector performs those tasks. The Supervisor also assigns the performance monitoring task to the same Collector that performed discovery.
2. For environments without Collector:
   a. Supervisor does discovery and Test Connectivity.
   b. Supervisor then assigns the performance monitoring tasks to the Active Workers in a weighted round robin fashion. Some jobs like vCenter monitoring has a higher weight than simple SNMP based CPU monitoring.
   c. Workers perform the performance monitoring tasks.
   d. If a Worker is removed, its performance monitoring jobs are redistributed to other Workers.
   e. If a Worker is added, new performance monitoring jobs are assigned to that Worker.
   f. If you disable and then enable performance monitoring jobs from the GUI, then a new global job distribution takes place.

This section provides the procedures for discovering devices.

- Creating a Discovery Entry
- Discovering on Demand
- Scheduling a Discovery
- Searching Previous Discovery Results
- Editing a Discovery
- Exporting Discovery Results

Creating a Discovery Entry

Complete these steps to create a discovery:

1. Go to **ADMIN** > **Setup** > **Discovery** tab.
2. Click **New**.

3. In the **Range Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Name of the discovery entry that will be used for reference.
Discovery Type	Select the type of discovery: • **Range Scan** - FortiSIEM will sequentially discover each device in one or more IP ranges and CIDR subnets. • **Smart Scan** - FortiSIEM will first discover the Root IP, which will provide a list of devices that it knows about. Then FortiSIEM will discover each of the devices learnt from the Root IP device. Each of these devices will provide a list of devices they know about, which FortiSIEM will then discover. This process continues until the list of known devices is exhausted. • **AWS Scan** - FortiSIEM will discover the devices in Amazon Web Services (AWS) Cloud learnt via AWS SDK. For AWS Scan to succeed, there needs to be an AWS Credential mapped to aws.com or amazon.com in the IP to Credential mapping. • **L2 Scan** - FortiSIEM will discover only the Layer 2 connectivity of the devices. • **Azure Scan** - FortiSIEM will discover the devices in Azure Cloud learnt via Azure SDK. For Azure Scan to succeed, there needs to be a Credential mapped to azure.com in the IP to Credential mapping. • **Nozomi Scan** - FortiSIEM will discover the devices in Nozomi SCADAguardian and CMC learnt via Nozomi REST API. For Nozomi Scan to succeed, there needs to be a Credential mapped to Nozomi SCADAguardian/CMC in the IP to Credential mapping. See Setting Credentials and the FortiSIEM External Systems Configuration Guide for more information on Credential mapping.
Root IPs	IP address of the Starting device for Smart Scan. See Smart scan definition above.
Include	[Required] A list of IP addresses that will be included for discovery. Allowed IP range syntax is single IP, single range, single CIDR or a list separated by comma – e.g. 10.1.1.1, 10.1.1.2,20.1.1.0/24, 30.1.1.1-30.1.1.10.
Exclude	A list of IP addresses that will be excluded for discovery. Allowed IP range syntax is single IP, single range, single CIDR or a list separated by comma – e.g. 10.1.1.1, 10.1.1.2,20.1.1.0/24, 30.1.1.1-30.1.1.10.
Include Types	A list of device Types that will be included for discovery. Click the edit icon to configure the **Range Definition** and **Save**.
Exclude Types	A list of device Types that will be excluded for discovery. Click the edit icon to configure the **Range Definition** and **Save**.
Name Resolution	Host names can learn from DNS look up, device configuration, or SNMP/WMI. If these do not match, then choose which discovery method with higher priority. For example, if DNS is chosen then FortiSIEM will get host names from DNS. If DNS lookup fails for an IP, the host names will be obtained from SNMP/WMI.

Settings	Guidelines
Options	Select the options for this discovery: - **Do not ping before discovery**: Device will not be pinged before attempting the credentials. - **Ping only discovery**: Select this option if you are only interested in discovering whether a device or service is up or down. - **Winexe based discovery** - For Windows servers, HyperV metrics and other AD replication metrics are discovered via Winexe. However, Winexe installs a service and uninstalls the service after it finishes for certain old OS. This setting enables to control this behavior. - **Only discover devices not in CMDB** - **Discover Routes**: Routes help to discover neighboring devices for Smart Scan but “show route” can be expensive for BGP routers. This selection provides a way to control this behavior. - **Include powered off VMs**: This allows the administrator to control whether powered off VMs will be discovered during VCenter discovery - **Include VM templates**: This allows the administrator to control whether VM templates will be discovered during VCenter discovery. - **Set discovered devices as unmanaged**: This allows the administrator to set the discovered devices as unmanaged. **Discover Installed Software**:This setting allows FortiSIEM to check for installed software on devices. **Discover Installed Patches**: This setting allows FortiSIEM to check for installed patches on devices. **Get Windows Events**: This allows the administrator to control whether to retrieve Windows events.

4. Click **Save**.

Discovering on Demand

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Select the required discovery from the table.
3. Click **Discover**.
4. Click **Results** to view the discovery result.
5. Click **Errors** to check for any errors found during discovery.
   Use the **Run in Background** to run discovery in background while performing other operations.
6. After successful discovery, **Discovery Completed.** message is displayed with the discovery results.

Scheduling a Discovery

Discovery can be a long-running process when performed on a large network, or over a large IP range, and so you may want to schedule it to occur when there is less load on your network or during off hours. You may also want to set up a schedule for the process to run and discover new devices on a regular basis.

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Click **Scheduled**.
3. Under **Discovery Schedule** dialog box, click **New**.
4. Select from the available ranges.
   You can select multiple ranges and set the order in which discovery will run on them using the up and down arrows.
5. Set the time at which you want discovery to run.
   - For a one-time scheduled discovery, select the **Start Time**.
   - For recurring discoveries, select how often (hourly, daily, weekly, monthly), you want discovery to run, and then enter other scheduling options.
6. Click **Save**.

Searching Previous Discovery Results

Complete these steps to search previously discovered results:

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Select a discovery result.
3. Click **History**.
4. In the **Discovery History** dialog box, click **View Results**, **View Errors** or **View Changes** to see the related information.

Editing a Discovery

Complete these steps to modify discovery settings:

1. Select the required option from the table below.
   - **Edit** - to edit any scheduled discovery settings.
   - **Delete** - to delete any scheduled discovery.
2. Click **OK**.

Exporting Discovery Results

Complete these steps to export discovery history:

1. Click **History**.
2. In the **Discovery History** dialog box, select the discovery type.
3. Based on the type of information required, select the required option:
   - **View Results** - to see the discovery results
   - **View Errors** - to see the errors during discovery
   - **View Changes** - to see the changes in discovery
4. Click **Export** based on your selection in step#3.
5. Optional - Enter the **User Notes**.
6. Select the **Output Format** as **PDF** or **CSV**.
7. Click **Generate**.
   'Export successful message' is displayed under **Export Report** dialog box.
8. Click **View** to see the discovery results.

Editing Event Pulling

After discovery is complete, FortiSIEM starts pulling events from devices with correct credentials. Examples include Windows Servers via WMI, VMWare VCenter via VMWare SDK, AWS CloudTrail via AWS SDK, etc.

The following section describes the procedures to see the status of these event pulling jobs and turn them on/off.

- Viewing Event Pulling Jobs
- Modifying Event Pulling Jobs
- Checking Status of Event Pulling Jobs
- Exporting Event Pulling Jobs into a Report
- Viewing Event Pulling Reports

Viewing Event Pulling Jobs

Complete these steps to enable event pulling:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. See the listed jobs:
   - Enabled – the job is enabled at a device level.
   - Device name – name of the device in CMDB.
   - Access IP – IP address with which FortiSIEM accesses this device.
   - Device Type – the device type in CMDB.
   - Organization – the organization to which this device belongs (for a multi-tenant FortiSIEM install).
   - Method – the event pulling method – format - credential name (Access Protocol). An icon appears next to the method, showing the collection status. Hover your cursor over the icon/method to get more details.

Icon	Collection Status
	Data for the specific monitor is being collected normally.
	Method validated for the specific monitor, but data collection has not yet started.
	Metric collection for the specific monitor not scheduled due to test failure during the beginning of the monitoring cycle, though discovery was successful. In most situations, this is caused by missing or invalid device credentials in FortiSIEM. Recommendation is to check the access protocol credentials and restart discovery.
	Event pulling method for the specific monitor has failed.

- Maintenance – indicates if this device is in maintenance or not.

3. See **Enabled** option to view the enabled device.
4. Select **Errors** to view the list of errors, if any.

Modifying Event Pulling Jobs

Complete these steps to enable/disable event pulling at all device level (all jobs will be enabled/disabled).

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select the device from the list.
3. Select **All** check-box to enable all jobs or deselect to disable.
4. Click **Apply**.

Complete these steps to enable/disable a specific event pulling job for a device:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select the device from the list.
3. Click **Edit**.
4. Check the specific job to enable/disable.
5. Click **Apply**.

Checking Status of Event Pulling Jobs

Complete these steps to the status of event pulling jobs:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select the device from the list.
3. Hover over the method column – the tool tip shows the Execution Status.
4. To see the events generated from the event pulling job, click **Report**.
   A report is run for all the events generated by this event pulling job in the last 10 minutes.

Exporting Event Pulling Jobs into a Report

Complete these steps to export an event pulling job report:

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Click **Export**.
3. Optional - Enter the **User Notes**.
4. Select the output format to **PDF** or **CSV** and click **Generate**.
5. Click **View** to download and view the report.

Viewing Event Pulling Reports

1. Go to **ADMIN** > **Setup** > **Pull Events** tab.
2. Select **Super/Local** or **Org with collector** or use the **Search** field to view any related jobs.

Editing Performance Monitors

After the discovery is complete, FortiSIEM starts monitoring successfully discovered devices for performance, availability and change. The following section describes the procedure to see the status of these performance monitoring jobs and edit them.

- Viewing Performance Monitoring Jobs
- Enabling/Disabling Performance Monitoring Jobs
- Modifying Performance Monitoring Jobs

Viewing Performance Monitoring Jobs

1. Go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. To check the **Device Health** details, select the device from the list and click the drop-down near the device name.
3. To check the errors during the monitoring job, select the device and click **More** > **Errors**.
4. To export a Performance Monitor, select the device and click **More** > **Export Monitors**.
5. To generate a Performance Monitoring report for any device(s), select the device and click **More** > **Report**.
6. The **Monitor** column displays the following icons for a quick assessment of monitor jobs. Hover your mouse cursor over the "Not Sheduled" or "Execution Failed" icon in the **Monitor** column to get more information.

Icon	Status
	Running.
	Not Scheduled.
	Execution Failed.

Enabling/Disabling Performance Monitoring Jobs

Complete these steps to enable/disable performance monitoring at a device level – all jobs will be enabled/disabled:

1. Go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. Select the device from the list.
3. Select **Enabled** check-box to enable and select again to disable.
4. Click **Apply**.

Modifying Performance Monitoring Jobs

Complete these steps to enable/disable a specific performance monitoring job for a device:

1. Change the Scope to Local and go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. Select the device from the list.
3. Click **More** and select the required option:
   - **Edit System Monitors** to select the Protocols and click **Save**.
   - **Edit App Monitors** to select the Protocols and click **Save**.
4. Click **Save**.
5. Click **Apply**.

Another way to enable/disable a specific job or tune monitoring intervals for specific jobs for all devices:

1. Go to **ADMIN** > **Setup** > **Monitor Performance** tab.
2. Click **More** > **Edit Intervals**.
3. In the **Set Intervals** pop-up:
   - Choose the Monitor on the left panel.
   - Choose the device on the middle panel.
   - Click **>>** to move the chosen jobs on the chosen devices to the right panel.
   - Choose the new polling interval or choose **Disabled**.
   - Click **Save**.
4. Click **Apply**.

Configuring Synthetic Transaction Monitoring

A Synthetic Transaction Monitoring (STM) test lets you test whether a service is up or down, and measure the response time. An STM test can range from something as simple as pinging a service, to complex as sending and receiving an email or a nested Web transaction.

This section provides the procedures to set up Synthetic Transaction Monitoring tests.

- Create Monitoring Definition
- Create STM Test
- Edit Monitoring Definition
- Protocol Settings for STM Tests

Creating Monitoring Definition

Complete these steps to create monitor definitions:

1. Go to **ADMIN** > **Setup** > **STM** tab.
2. Under **Step 1: Edit Monitoring Definitions**, click **New**.
3. In the **Add Monitor Definition** dialog box, enter the information below.
   a. Name – enter a name that will be used for reference.
   b. Description – enter a description.
   c. Frequency – how often the STM test will be performed.
   d. Protocol - See 'Protocol Settings for STM Tests' for more information about the settings and test results for specific protocols.
   e. Timeout – when the STM test will give up when it fails.
   f. Probe Settings - enter the timeout period in seconds.
4. Click **Save**.

Creating an STM Test

Complete these steps to create an STM test:

1. Go to **ADMIN** > **Setup** > **STM** tab.
2. Under **Step 2: Create synthetic transaction monitoring entry by associating host name to monitoring definitions**, select **New**.

3. Click **New** and enter the following information:
   a. **Monitoring Definition** – enter the name of the Monitor (previous step).
   b. **Host name or IP/IP Range** – enter a host name or IP or IP range on which the test will be performed.
   c. **Service Ports** – click the Port(s) on which the test will be performed. To add/delete Ports, click **+/-**.
   d. Check **SSL** option to enable SSL for encryption.
   e. Click **Test and Save** to test and save the changes.
   f. Click **Apply**.

Editing Monitoring Definition

Complete these steps to modify monitor definition settings:

1. In the **Step 1: Edit Monitoring Definitions** dialog box, click the tab based on the required action.

Tab	Description
Edit	To modify the Monitoring Definitions.
Delete	To delete the selected Monitoring Definition.
Clone	To duplicate the selected Monitoring Definition.

2. Click **Save**.

Protocol Settings for STM Tests

This table describes the settings associated with the various protocols used for Creating Monitoring Definition.

Protocol	Description	Settings	Notes
Ping	Checks packet loss and round trip time.	**Maximum Packet Loss PCT**: tolerable packet loss. **Maximum Average Round Trip Time**: tolerable round trip time (seconds) from FortiSIEM to the destination and back. If either of these two thresholds are exceeded, then the test is considered as failed.	Make sure the device is accessible from the FortiSIEM node from which this test is going to be performed.
LOOP Email	This test sends an email to an outbound SMTP server and then attempts to receive the same email from a mailbox via IMAP or POP. It also records the end-to-end time.	**Timeout**: the time limit by which the end to end LOOP EMAIL test must complete. **Outgoing Settings**: these specify the outgoing SMTP server account for sending the email. • **SMTP Server**: name of the SMTP server. • **User Name**: user account on the SMTP server. • **Email Subject**: content of the subject line in the test email.	Before you set up the test you must have set up access credentials for an outbound SMTP account for sending email, and an inbound POP/IMAP account for receiving email.

Protocol	Description	Settings	Notes
		Incoming Settings: These specify the inbound IMAP or POP server account for fetching the email. • **Protocol Type**: choose IMAP or POP. • **Server**: name of the IMAP or POP server. • **User Name**: user account on the IMAP or POP server. • **Email Subject**: content of the subject line in the test email.	
HTTP(S) - Selenium Script	This test uses a Selenium script to play back a series of website actions in FortiSIEM.	**Upload**: select the java file you exported from Selenium. **Total Timeout**: the script must complete by this time or the test will be considered failed. **Step Timeout**: each step must complete by this time.	**How to export**: • Make sure Selenium IDE is installed within Firefox browser. • Open Firefox. • Launch Tools > Selenium IDE. From now on, Selenium is recording user actions. • Visit websites. • Once done, stop recording. • Click File > Export Test case as > Java / Junit 4 /WebDriver. • Save the file as .java in your desktop. This file has to be inputted in FortiSIEM.

Protocol	Description	Settings	Notes
HTTP(S) - Simple	This test connects to a URI over HTTP(s) and checks the response time and expected results.	**URI**: the URI to connect to. **Authentication**: any authentication method to use when connecting to this URI. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails. **Contains**: an expected string in the test results. **Does Not Contain**: a string that should not be contained in the test results. The format should be a list of words, separated with a space, e.g. “fortinet firewall”. If **All** is selected, then every listed word is expected, e.g. “fortinet” AND “firewall” are expected to be found within the web page. If **Any** is selected, then any of the listed words are expected, e.g. “fortinet” OR “firewall” is expected to be found within the web page.	

Protocol	Description	Settings	Notes
		Response Code: an expected HTTP(S) response code in the test results. The default is set to **200 - 204**.	
TCP	This test attempts to connect to the specified port using TCP.	**Timeout**: this is the single success criterion. If there is no response within the time specified here, then the test fails.	
DNS	Checks response time and expected IP address.	**Query**: the domain name that needs to be resolved. **Record Type**: the type of record to test against. **Result**: specify the expected IP address that should be associated with the DNS entry. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails.	
SSH	This test issues a command to the remote server over SSH, and checks the response time and expected results.	**Remote Command**: the command to run after logging on to the system **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test	You must set up an SSH credential on the target server before setting up this test. As an example test, you could set **Raw Command** to `ls`, and then set **Contains** to the name of a file that should be returned when that command executes on the target server and directory.

Protocol	Description	Settings	Notes
		fails. **Contains**: an expected string in the test results.	
LDAP	This test connects to the LDAP server, and checks the response time and expected results.	**Base DN**: an LDAP base DN you want to run the test against. **Filter**: any filter criteria for the Base DN. **Scope**: any scope for the test. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails. **Number of Rows**: the expected number of rows in the test results. **Contains**: an expected string in the test results. **Does Not Contain**: a string that should not be contained in the test results.	You must set up an access credential for the LDAP server before you can set up this test
IMAP	This tests checks connectivity to the IMAP service.	**Timeout**: this is the single success criterion - if there is no response within the time specified here, then the test fails.	
POP	This test checks connectivity to the IMAP service.	**Timeout**: this is the single success criterion - if there is no response within the time specified here, then the test	

Protocol	Description	Settings	Notes
		fails.	
SMTP	This test checks connectivity to the SMTP service.	**Timeout**: this is the single success criterion - if there is no response within the time specified here, then the test fails.	
JDBC	This test issues a SQL command over JDBC to a target database, and checks the response time and expected results.	**JDBC Type**: the type of database to connect to. **Database Name**: the name of the target database. **SQL**: the SQL command to run against the target database. **Timeout**: this is the primary success criterion - if there is no response within the time specified here, then the test fails. **Number of Rows**: the expected number of rows in the test results. **Contains**: an expected string in the test results. **Does Not Contain**: a string that should not be contained in the test results.	
FTP	This test issues a FTP command to the server and checks expected results.	**Anonymous Login**: choose whether to use anonymous login to connect to the FTP directory. **Remote Directory**: the remote directory to connect to.	

Protocol	Description	Settings	Notes
		Timeout: this is the primary success criterion - if there is no response within the time specified here, then the test fails.	
TRACE ROUTE	This test issues a trace route command to the destination and parses the results to create PH_DEV_MON_ TRACEROUTE events, one for each hop.	**Timeout**: If there is no response from the system within the time specified here, then the test fails. **Protocol Type**: Specifies the IP protocol over which trace route packets are send - current options are UDP, TCP and ICMP. **Max TTL**: Max time to live (hop) value used in outgoing trace route probe packets. **Wait Time**: Max time in seconds to wait for a trace route probe response.	For the trace route from AO to destination D via hops H1, H2, H3, FortiSIEM generates 3 hop by hop PH_ DEV_MON_TRACEROUTE events. **First event:** Source AO, destination H1, Min/Max/Avg RTT, Packet Loss for this hop. **Second event:** Source H1, destination H2, Min/Max/Avg RTT, Packet Loss for this hop. **Third event:** Source H2, destination H3, Min/Max/Avg RTT, Packet Loss for this hop. **Fourth event:** Source H3, destination D, Min/Max/Avg RTT, Packet Loss for this hop **Fourth event:** Source H3, destination D, Min/Max/Avg RTT, Packet Loss for this hop.

When an STM test fails, three system rules are triggered, and you can receive an email notification of that failure by creating an automation policy for these rules:

- **Service Degraded - Slow Response to STM**: Detects that the response time of an end-user monitored service is greater than a defined threshold (average over 3 samples in 15 minutes is more than 5 seconds).
- **Service Down - No Response to STM:** Detects a service suddenly went down from the up state and is no longer responding to synthetic transaction monitoring probes.
- **Service Staying Down - No Response to STM**: Detects a service staying down, meaning that it went from up to down and did not come up, and is no longer responding to end user monitoring probes.

Configuring Maintenance Calendars

A Maintenance Calendar displays when a device is undergoing maintenance (likely due to hardware and software upgrades). When a device is in maintenance, it is not monitored for performance, availability and change and the corresponding rules do not trigger.

This section provides the procedures to set up maintenance calendars.

- Create a Maintenance Calendar
  - Specifying a Schedule
  - Specifying the Devices Under Maintenance
- Viewing Existing Maintenance Calendars
- Modifying Existing Maintenance Calendars

Create a Maintenance Calendar

Complete these steps to schedule maintenance:

1. Go to **ADMIN** > **Setup** > **Maintenance** tab.
2. Click **New** and specify the following:

Settings	Guidelines
Name	[Required] Name of the Calendar. This will be displayed on the Calendar.
Description	Description or details about this schedule.
Schedule	[Required] Specify the times during which devices will be in maintenance.
Groups/Devices	Specify the groups/devices and Synthetic Transaction Monitoring (STM) tasks that will be in maintenance.

3. Optional - To generate incidents during maintenance, enable **Generate Incidents for Devices under Maintenance**.
4. Click **Save**.

Specifying a Schedule

1. Click the **Schedule** drop-down list in the **Device Maintenance** window.
2. Enter values for the following options:
   - **Time Range** specifies start time (within the day) and the duration of the maintenance window.
   - **Recurrence Pattern** specifies if and how the maintenance window will repeat.
     - If the maintenance window is one time:
       i. Select **Once** for **Recurrence Pattern**.
       ii. Select the specific date on the **Recurrence Range**.
     - If the maintenance window should repeat on certain days of the week:
       i. Select **Recurring Days** and select the Repeat Days and Repeat months.
       ii. Select the start and end dates for Recurrence Range.
     - If the maintenance window should repeat on certain months of the year:
       i. Select **Recurring Months** and select the Repeat Months.
       ii. Select the **Start From**/**End By** dates for Recurrence Range or select **No end date** to continue the recurrance forever.
3. Click **Save** to apply the changes.

Specifying the Devices Under Maintenance

1. Click the **Groups/Devices** drop-down list in the **Device Maintenance** dialog box.
2. From the **Folders** on the left pane, select either the Devices folder or the STM folder of all the STM jobs defined so far.
3. From the devices/STM jobs shown in the middle pane, select the appropriate ones and click **>** for them to appear in the right **Selections** pane.
4. To select all devices in a folder, select the folder on the left windows and click **>>** to move the folder into the right window.
5. Click **Save**.

Viewing Existing Maintenance Calendars

The existing maintenance calendars can be displayed in various time windows. These options are available on the top-right:

- Monthly view - click **Month**.
- Weekly view - click **Week** or **List (Week)**.
- Day view - click **Day**.

You can navigate to a specific month on the Calendar, click the **<** and **>** buttons on the top-left of the Calendar. To view the current Maintenance, click **Current**.

Modifying Existing Maintenance Calendars

Complete these steps to modify a maintenance schedule:

1. Select the schedule from the Calendar.
2. Click the tab based on the required action:
   - Edit - to edit the scheduled maintenance settings.
   - Delete - to delete the scheduled maintenance.
3. Click **Save**.

Configuring Windows Agent

Before proceeding, follow the instructions in the Windows Agent Installation Guide to complete these steps:

1. Install the Windows Agent using the correct installation file.
2. Make sure the Agent appears in the CMDB page of the FortiSIEM GUI, using the host name defined in the installation file.
3. Configure the Windows Server to receive the types logs of interest (see Microsoft Windows Servers via Agent in the External Systems Configuration Guide).

To receive logs from Windows Agent, you must complete the following steps:

1. Define Windows Agent Monitor Templates
2. Associate Windows Agents to Templates

Once these steps are completed, the Supervisor node will distribute monitoring policies to the Agents and you will be able to see events in FortiSIEM.

This section also covers these topics:

- Viewing Agent Status
- Enabling or Disabling an Agent
- Viewing Files in FortiSIEM
- Verifying Events in FortiSIEM
- Service Level Protection Properties
- Auto Restart Service Behavior
- Configuring Debug Trace Logging without Agent Service Restart
- Configuring the Agent Database Size
- Agent Troubleshooting Notes

Note: Sample Windows Agent logs can be found in the Appendix here.

Define the Windows Agent Monitor Templates

A Windows Monitoring Template consists of:

- Log Settings: Windows Event Logs and Log Files
- Change Settings: File Integrity Monitoring, Registry Changes, Installed Software Changes, Removable media
- Script Settings: WMI Classes and PowerShell Scripts

Complete these steps to add a Windows Agent Monitor Template:

1. Go to **ADMIN** > **Setup** > **Windows Agent** tab.
2. Click **New** under the section **Windows Agent Monitor Templates**.

3. In the **Windows Agent Monitor Template** dialog box, enter the information under each tab with reference to the tables below.
   a. Configure the Generic settings with reference to the table below:

Generic settings	Guidelines
Name	Enter the name of the Windows Agent Monitor Template. This name is used as a reference in Template associations. Note: The template name cannot contain a space (" ") character.
Description	Enter a description of the Windows Agent Monitor Template.

   b. Configure the Monitor settings for Windows Agent using the table below. When done, click Save.

Monitor settings	Guidelines
Discover	To configure Discover settings: Click the Discover checkbox to enable Windows Agent discovery. In the Hour(s) field, enter the frequency (in number of hours) that discovery will be done.
Monitor	To configure Monitor settings: Click the appropriate Monitor checkboxes to enable specific monitoring performance of Windows Agents. • Uptime - Select to monitor uptime of Windows Agent. • CPU - Select to monitor CPU utilization. • Memory - Select to monitor memory utilization. • Disk - Select to monitor disk utilization. • Network - Select to monitor network utilization. • Application - Select to monitoring running applications. In the time field, enter a numeric value for the monitoring frequency. The drop-down time field allows you to choose the frequency in Hour(s) or Minute(s).

   c. Configure the **Event** settings with reference to the table below. Make sure you have completed these steps from the Windows Agent Installation Guide:
      - To enable DNS logging, follow the steps in Collecting Windows DNS Logs.
      - To enable DHCP logging, follow the steps in Collecting Windows DHCP Logs.
      - To enable IIS logging, follow the steps in Collecting Windows IIS Logs.
      - To get sysmon events, follow the steps in Collecting Windows Sysmon Logs.
      - To get security log events, follow the steps in Collecting Windows Security Logs.
      - To get system and application events, follow the steps in Collecting Windows System and Application Logs.

Event settings	Guidelines
Event Log	To configure **Event log** settings: **1.** Select the **Type** of log from the drop-down: • **Application** — Events that are logged by Windows Application. Select All, Exchange Server or SQL Server as Source. • **Security** — Log that contains records of login/logout activity or other security-related events specified by the system's audit policy. • **System** — Events that are logged by the operating system components. • **DFS** — Logs to identify the users who accessed the Distributed File System. • **DNS** — DNS Debug logs and Name Resolution Activity logs. • **Hardware Events** — Events related to hardware. • **Key Management Service** — Events related to creation and control of keys used to encrypt your data. • **Setup** — Log files for all actions that occur during installation. • Sysmon - Logs related to Sysmon. • **Windows PowerShell** — Logs related to Windows PowerShell. • **Other** — Any other log type (specify the name under **Event Name** setting.) **2.** Enter the events to be included under **Include Event** and the ones to exclude under **Exclude Event** by entering each event ID followed by a semicolon as a separator.

d. Select UEBA to turn on UEBA functionality for all hosts running Windows 4.0 or later that are permitted by the UEBA license. For example, if you have 10 UEBA licenses and you applied the template to 100 hosts, system will apply the UEBA license to 10 random hosts. You can turn on/off UEBA on hosts via CMDB.

e. Configure the **User Log** settings with reference to the table below:

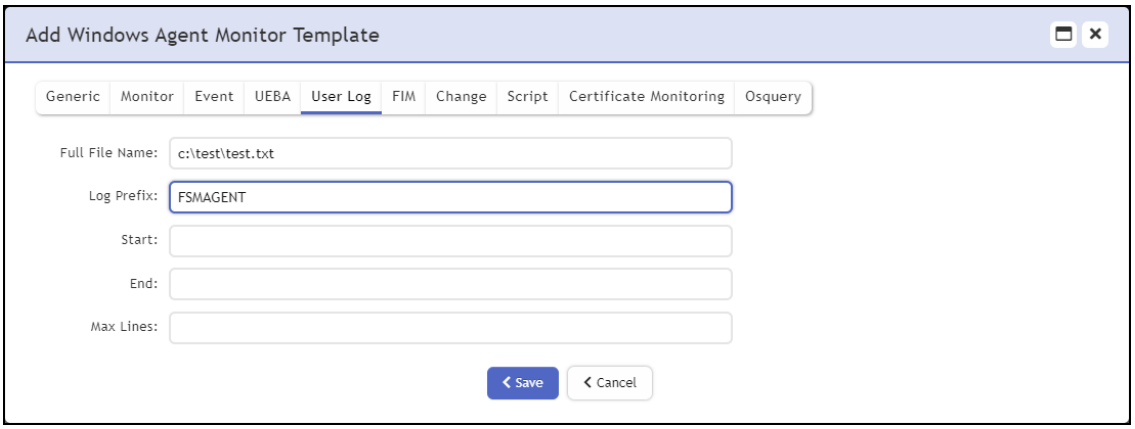
User Log settings	Guidelines
User Log	Click **New** to add the custom log files that must be monitored: • **Full File Name**—(Required) Enter the full file name (including path) to be monitored. Note: Windows System variables are also supported as part of this path. For example, `%WINDIR%` can be placed as part of the file path. The agent will then expand this property when evaluating the template, and use the correct path. For the full list of supported system variables, see Appendix - Windows Agent System Variables. • **Log Prefix**—(Required) Any prefix to the identify events from this file for better accessibility.

Example:

The contents of the file `C:\test\test.txt` needs to be brought into FortiSIEM for analysis. The log prefix FSMAGENT was chosen. To configure the Windows Agent template in FortiSIEM, from the User Log tab, you would take the following steps.

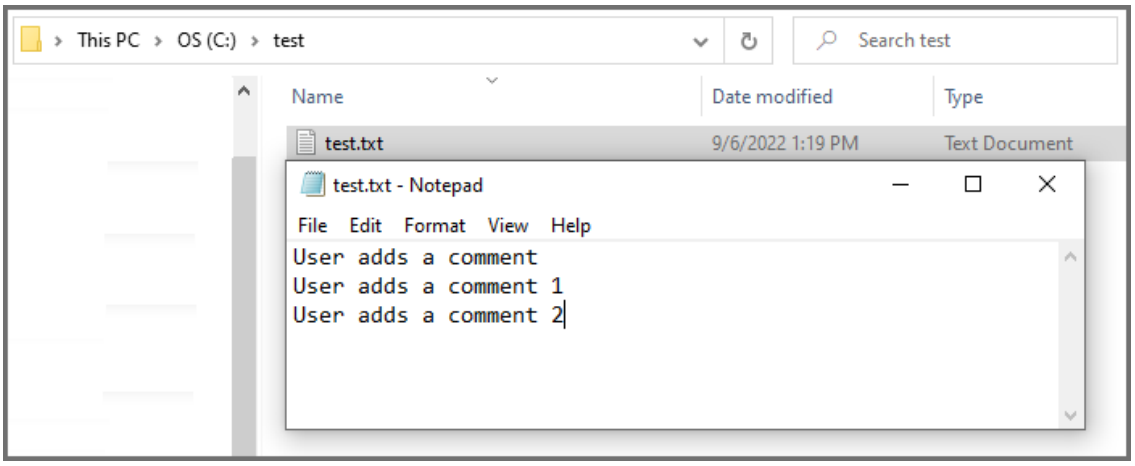
In the Full File Name field, you would enter "C:\test\test.txt".

In the Log Prefix field, you would enter "FSMAGENT".



Suppose the contents of the file C:\test\test.txt looks like this.

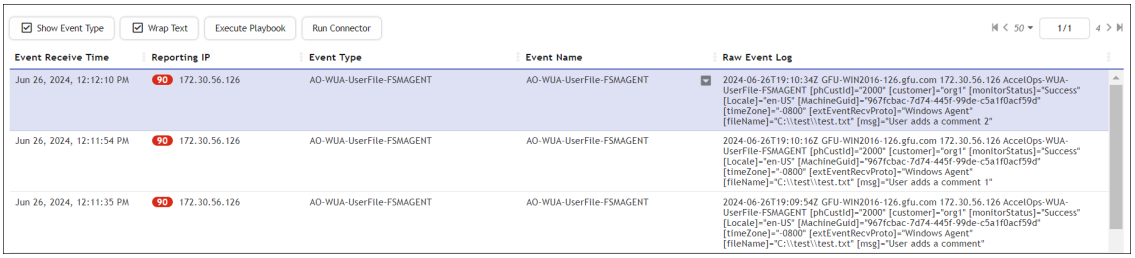
```
User adds a comment
User adds a comment 1
User adds a comment 2
```



FortiSIEM agent will send each line in a separate event.

```
2024-06-26T19:09:54Z GFU-WIN2016-126.gfu.com 172.30.56.126 AccelOps-WUA-UserFile-
FSMAGENT [phCustId]="2000" [customer]="org1" [monitorStatus]="Success"
[Locale]="en-US" [MachineGuid]="967fcbac-7d74-445f-99de-c5a1f0acf59d" [timeZone]="-
0800" [extEventRecvProto]="Windows Agent" [fileName]="C:\\test\\test.txt"
[msg]="User adds a comment"

2024-06-26T19:10:16Z GFU-WIN2016-126.gfu.com 172.30.56.126 AccelOps-WUA-UserFile-
FSMAGENT [phCustId]="2000" [customer]="org1" [monitorStatus]="Success"
[Locale]="en-US" [MachineGuid]="967fcbac-7d74-445f-99de-c5a1f0acf59d" [timeZone]="-
0800" [extEventRecvProto]="Windows Agent" [fileName]="C:\\test\\test.txt"
[msg]="User adds a comment 1"

2024-06-26T19:10:34Z GFU-WIN2016-126.gfu.com 172.30.56.126 AccelOps-WUA-UserFile-
FSMAGENT [phCustId]="2000" [customer]="org1" [monitorStatus]="Success"
[Locale]="en-US" [MachineGuid]="967fcbac-7d74-445f-99de-c5a1f0acf59d" [timeZone]="-
0800" [extEventRecvProto]="Windows Agent" [fileName]="C:\\test\\test.txt"
[msg]="User adds a comment 2"
```

The event type will be AO-WUA-UserFile-FSMAGENT.



f. Configure the **FIM** settings with reference to the table below. Make sure you have completed these steps from the Microsoft Windows Server via Agent section in the External Systems Configuration Guide:

- To enable logging appropriately, follow the steps in Configure Security Audit Logging Policy.
- To get user meta data in the file auditing logs, follow the steps in Configure File Auditing Policy.

- To enable change events for permission and/or ownership changes to files and/or directories, follow the steps in Configure Audit File System Policy.

FIM settings	Guidelines
FIM	To include the file directory details: 1. Click **New** to add the file directory details: • **File/Directory**— Enter the full path of the file directory: • **Include Subfolder(s)** — Select if you must include the directory sub-folders. • **Exclude Subfolder(s)** — Enter any sub-folders to exclude, if any. • **Include File Type** — Enter the file types to include separated by a semi-colon. • **Exclude File Type** — Enter the file types to exclude, if any, separated by a semi-colon. • **On Modify:** • **Push Files**—Select this if you want Windows Agent to push files to FortiSIEM whenever there is a change. File/Directory must specify a specific file and not a directory. Also, the absolute file name, including the path, must be specified. For example `C:\temp\fileToBeMonitored.txt`. The files are stored in SVN and are accessible from the Supervisor. These files are displayed in **CMDB > Device > File**. Send only important files, as this can fill up disk space. Note: Windows System variables are also supported as part of this path. For example, `%WINDIR%` can be placed as part of the file path. The agent will then expand this property when evaluating the template, and use the correct path. For the full list of supported system variables, see Appendix - Windows Agent System Variables. • **Compare Baseline**—Select this if you want to be alerted when the file changes from a baseline. File/Directory must specify a specific file and not a directory. Also, the absolute file name, including the path, must be specified. For example `C:\temp\fileToBeMonitored.txt`. This is common for configuration files that rarely change. If you choose this option, you will be asked to provide a copy of the baseline file. Click **Choose File** and upload the file from your workstation. The Supervisor will compute the MD5 checksum and distribute the checksum to the agents for comparison. 2. Click Save.

FIM settings	Guidelines
	Use the **Edit**/**Delete** buttons to modify/remove any file directory information.

g. Configure the **Change** settings with reference to the table below:

Change settings	Guidelines
Registry Change	Select the required key(s) to monitor: • **HKEY_CLASSES_ROOT**—key that contains file extension association information, as well as a programmatic identifier, Class ID, and Interface ID data. • **HKEY_CURRENT_USER**—key that contains configuration information for Windows and software specific to the currently logged in user. • **HKEY_LOCAL_MACHINE**—hive that contains the majority of the configuration information for the software you have installed, as well as for the Windows Operating System. • **HKEY_USERS**—key that contains user-specific configuration information of all currently active users on the computer. • **HKEY_CURRENT_CONFIG**—key that acts as a shortcut to a registry key which keeps information about the hardware profile currently used.
Check Every	Set the time period to check the Registry Change in Minute (s) or Hour(s).
Installed Software Change	Select to enable monitoring of any installed software change.
Removable Drive	Select the removable drive to track: • Track USB drive(s) • Track CD-DVD drive(s)

h. Configure the **Script** settings with reference to the table below:

Script settings	Guidelines
WMI Classes	To include a WMI Class: 1. Click **New** to add a new WMI Class. Select the **Name**, **WMI Class**, and **Attributes** from the drop-down lists (Use ';' as the separator). 2. Set the time period to monitor in Minute(s) or Hour(s) under **Check Every** setting. Use the **Edit**/**Delete** buttons to modify/remove any WMI Classes.
PowerShell Script	To include a PowerShell Script: Click **New** to add a new PowerShell Script and enter the **Name** and **Script**. Use the **Edit**/**Delete** buttons to modify/remove any PowerShell Script.

i. Configure the Certificate Monitoring settings with reference to the table below for each Certificate Folder:

Certificate Monitoring settings	Guidelines
Store Name	Select the following to monitor: Add - Event generated when certificate is added to store. Delete - Event generated when certificate is removed from store. Expired (Days) - From the drop-down list, select the number of days to receive notification when a certificate has expired. Expiry (Days) - From the drop-down list, select the period of days to receive notification prior to when a certificate is about to expire.

j. Configure the Osquery settings with reference to the table below:

Osquery settings	Guidelines
osquery	From the Osquery drop-down list, select the osquery template to include in the Windows Agent Monitor Template. Click + to add a new entry. Select the osquery template to use. Click - to remove an existing entry.

4. Click Save.
Use the **Edit** button to modify any template or **Delete** button to remove any Windows Agent Monitor template.

Associate Windows Agents to Templates

After defining the monitoring templates, you must associate hosts to templates. To scale to a large number of hosts, this is done via Policies. A Policy is a mapping from Organization and Host to Templates and Collectors. Policies are evaluated in order (lower order or rank is higher priority) and the policy that matches first is selected. Therefore, define the exceptions first followed by broad policies. Hosts are defined in terms of CMDB Device Groups or Business Services. Multiple templates can be used in one Policy and the system detects conflicts, if any.

Complete these steps to associate a Host to Template:

1. Click **New** under the section **Host To Template Associations**.
2. In the **Host To Template Associations** dialog box, enter the information below.

Settings	Guidelines
Name	Name of the Host to Template Association.
Organization	Select the organization.
Host	Use the drop-down list to browse the folders and select the **Devices** or/and **Business Services** to monitor and click **Save**.
Template	Select one or more monitoring templates from the list or select **All Templates** to include all. You can also use the search bar to find any specific template.
Collector	Select the Collector from the list or select **All Collectors** to include all. Agents forward events to Collectors via HTTP(S). A Collector is chosen at random and if that Collector is not available or non-responsive, then another Collector in the list is chosen.

3. Click **Save** and **Apply**.
   A **Rank** is automatically assigned to the association.

You can use the **Edit** button to modify or **Delete** button to remove any template association.

Viewing Agent Status

Complete these steps to view the Windows Agent status for any specific device:

1. Go to **CMDB** > **Devices** and select the device.
   The following fields display the information related to the Agent:
   - Agent Status: status of the Agent on the device
   - Agent Policy: agent policy name
   - Monitor Status: status of monitoring

   The Agent Status indicates the following:

Status	Description
Registered	Agent has completed registration but has not received the monitoring template.
Running Active	Agent has received a monitoring template and it is performing properly.
Running Inactive	Agent is running but does not have a monitoring template – the reasons can be (a) no license or (b) incomplete definition - no Collector or Template is defined for that host.
Stopped	Agent is stopped on the Linux Server.
Disconnected	Supervisor did not receive any status from the Agent for the last 10 minutes.

Enabling or Disabling an Agent

Complete these steps to enable or disable Agent for a specific device:

1. Go to **CMDB** > **Devices** and select the required device.
2. Select the **Action** drop-down menu and click **Enable Agent** to enable or **Disable Agent** to disable Agent monitoring for the selected device.

Viewing Files in FortiSIEM

If the FortiSIEM Agent is running on a Server and a FIM policy is enabled with **Push Files On Modify**, then the FortiSIEM Agent will send the files to FortiSIEM when a change is detected. FortiSIEM stores the files in SVN on the Supervisor.

1. Go to the **CMDB** page. Make sure that **AGENT** is one of the **Methods**.
2. Search for the device in CMDB by name.
   Use the host name that you used in the `InstallSettings.xml` file to install the Windows Agent.
3. Click **File** beneath the device table.
   You will see all of the files that were changed since the monitoring template was applied.
4. Select a file.
   If you need to search for a file, set the **From** and **To** dates. The files which changed between those dates will be displayed.
5. Click the file name on the left and its contents will be displayed in the right hand window.
   Each file has a header containing file meta data followed by the actual file content.
   - FILEPATH: The full file name, including the path.
   - ARCHIVE: Set to true if ArchiveBit is set; set to false if it is not.
   - HASHCODE: The file hash.

- HASHALGO: The algorithm used to compute file hash.
- OWNER: The file owner.
- USER, PERMIT, DENY: Permissions are specified as a (User, Permit, Deny) triple. This describes the actions that the user is allowed to perform.
- MODIFIED_TIME: The time when the file was last modified.

6. To see the differences between two files, select two files on left and click **Diff**.

Verifying Events in FortiSIEM

Follow the steps below to verify the events in FortiSIEM:

1. Go to **ANALYTICS** tab.
2. Click the Filters field.
3. Create the following condition: Attribute= **Raw Event Log**, Operator = CONTAIN, Value = AccelOps-WUA and click **Save & Run.**
   Note: All event types for all Windows Server generated logs are prefixed by AccelOps-WUA.
4. Select the following **Group By**:
   a. Reporting Device Name
   b. Reporting IP
5. Select the following **Display Fields:**
   a. Reporting Device Name
   b. Reporting IP
   c. COUNT(Matched Events)
6. Run the query for the last 15 minutes.
   The query will return all hosts that reported events in the last 15 minutes.

Service Level Protection Properties

When Windows Agent is running, the FSMLogAgent is shown as part of your services on your Windows machine. The ability to Start, Stop, Pause, or Resume this service is disabled. This is intentional, to provide service level protection.

Auto Restart Service Behavior

In the event of a Windows Agent crash, Windows Agent will automatically restart itself after 60 seconds has passed.

Configuring Debug Trace Logging without Agent Service Restart

To enable/disable debug trace logging, you will need to modify the `LogLevel` entry in your Registry Editor. Take the following steps:

1. Using the Registry Editor (Regedit), navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FortiSIEM`.
2. Select `LogLevel` to edit.
   - Select Decimal for Base and change Value data to 2 to enable trace logging. Both "DBGTRACE" and "TRACE" information will be logged.
   - Select Decimal for Base and change Value data to 1 to enable debug logging. Only "DBGTRACE" information will be logged.

     Note: It will take about 2-3 minutes for your change to take effect.

Go to your log folder, typically `C:\ProgramData\FortiSIEM\Logs`, and examine your `FSMLogAgent.log` file with any text editor.

Configuring the Agent Database Size

The default size for your Agent Database is 1GB. If you wish to change this, you will need to modify the `MaxDBSizeInMB` entry in your Registry Editor. Take the following steps:

1. Using the Registry Editor (Regedit), navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FortiSIEM`.
2. Select `MaxDBSizeInMB` to edit.
3. Select Decimal for Base and change Value data to the number of MB you wish to apply as the maximum capacity.

Agent Troubleshooting Notes

A Windows Agent can be in following states (shown in CMDB):

- Registered
- Running Inactive
- Running Active
- Disabled
- Disconnected

When an Agent is installed and registered, then it is in Registered state. The following audit event is generated: `PH_AUDIT_AGENT_INSTALLED`.

When a monitoring template is assigned to the device, then the state moves to Running Inactive. When the agent receives the template and starts monitoring, then the state moves to Running Active. In both cases, the following audit event is generated: `PH_AUDIT_AGENT_RUNNING`.

Agent periodically sends heartbeat messages. When a heartbeat not received for 10 minutes, the state moves to Disconnected and the audit event `PH_AUDIT_AGENT_NOTRESPONDING` is generated. Status is checked every 1 hour. At that time, if we heard from the Agent in the last 15 minutes, the state moves back to Running Inactive and a `PH_AUDIT_AGENT_RUNNING` audit event is generated.

If the Agent is disabled from the GUI, the state moves to Disabled and `PH_AUDIT_AGENT_DISABLED` audit event is generated.

If the Agent is uninstalled or the service is stopped, then the state moves to Disconnected and the audit event `PH_AUDIT_AGENT_NOTRESPONDING` is generated.

Audit events are generated at state transitions, however, the event `PH_AUDIT_AGENT_NOTRESPONDING` is generated every hour to identify all agents that are currently disconnected. A nested query can be run to detect Agents that did not report in the last N hours. Note that `PH_AUDIT` events must be queried with `System Event Category = 2`. Rules do not need this condition.

Configuring Linux Agent

Linux Agents can be configured and managed from the FortiSIEM Supervisor node.

Before proceeding, install the Linux Agent following the instructions in the Linux Agent Installation Guide.

To receive logs from the Linux Agent, you must complete the following steps

1. Define the Linux Agent Monitoring Templates.
2. Associate Linux Agents to Templates.

Once these steps are completed, the Supervisor node will distribute monitoring policies to the Linux Agents and you will be able to see events in FortiSIEM.

Note: FortiSIEM Linux Agent will not perform file integrity monitoring on the /root directory.

This section also covers these topics.

- Viewing Agent Status
- Enabling or Disabling an Agent
- Viewing Files in FortiSIEM
- File Integrity Monitoring Logs
- Agent Troubleshooting Notes

Define the Linux Agent Monitor Templates

Complete these steps to add a Linux Agent Monitor Template:

1. Go to **ADMIN** > **Setup** > **Linux Agent** tab.
2. Click **New** under the section **Linux Agent Monitor Templates**.
3. In the **Linux Agent Monitor Template** dialog box, enter the information below.

Generic tab:

Configure the **Generic** settings with reference to the table below:

Generic Settings	Guidelines
Name	[Required] Enter the name of the FortiSIEM Linux Agent. This name is used as a reference in Template associations. Note: The template name cannot contain a space (" ") character.
Description	[Required] Enter the description about the FortiSIEM Linux Agent.

Monitor tab

Configure the **Monitor** settings with reference to the table below:

Monitor Settings	Guidelines
Discover	To configure Discover settings: Click the Discover checkbox to enable Linux Agent discovery. In the Hour(s) field, enter the frequency (in number of hours) that discovery will be done.
Monitor	To configure Monitor settings: Click the appropriate Monitor checkboxes to enable specific monitoring performance of Linux Agents. • Uptime - Select to monitor uptime of Linux Agent. • CPU - Select to monitor CPU utilization. • Memory - Select to monitor memory utilization. • Disk - Select to monitor disk utilization. • Network - Select to monitor network utilization. • Running Applications - Select to monitoring running applications. In the time field, enter a numeric value for the monitoring frequency. The drop-down time field allows you to choose the frequency in Hour(s) or Minute (s).

Syslog tab:

Configure the **Syslog** settings with reference to the table below:

Syslog Settings	Guidelines
Syslog	Select the **Facility** with the corresponding Syslog levels: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Info** • **Debug**

Log File tab:

Configure the **Log File** settings with reference to the table below:

Log File Settings	Guidelines
Log Files	Click **New** to add the custom log files to monitor: • **File**—(Required) Enter the full file name (including path) to be monitored. • **Log Prefix**—(Required) Any prefix to the identify events from this file for better accessibility.

If you cannot collect logs from the specified log file, please check if SELinux is enabled and that the SELinux context configuration for the file is correct. The `var_log_t` type is needed for the log file.

To check for SELinux context, assuming `/testLinuxAgent/testLog.log` is the log file, run the following command:

```
ls -Z /testLinuxAgent/testLog.log
```

The expected result should have `var_log_t` in the output, as shown here:

```
system_u:object_r:var_log_t:s0 /testLinuxAgent/testLog.log
```

If you need to set `var_log_t` type to the log file, run the following commands:

```
chcon –t var_log_t /testLinuxAgent
chcon –t var_log_t /testLinuxAgent/testLog.log
```

FIM tab:

Configure the **FIM** settings with reference to the table below:

FIM Settings	Guidelines

FIM	Click **New** to add the files to monitor:
	• **Include File/Directory**—Enter the file or directory to monitor.
	• **Exclude File/Directory**—Enter the file or directory to exclude from monitoring using a semi-colon (;) as a separator.
	• Action—Select the actions to monitor when there is an event in the included file or directory:
	  • **All**—All of the following actions will be monitored.
	  • **Open**—One or more of the monitored files or directories has been opened.
	  • **Close**—One or more of the monitored files or directories has been closed.
	  • **Create**—A file or directory has been created in one or more of the monitored files or directories.
	  • **Modify**—One or more of the monitored files or directories has been edited.
	  • **Delete**—One or more of the monitored files or directories has been deleted.
	  • **Attribute Change**—An attribute belonging to one or more of the monitored files or directories has been changed.
	• **On Modify** (appears only if All or Modify is selected):
	  • **Push Files**—Select this if you want Linux Agent to push files to FortiSIEM whenever there is a change. The files are stored in SVN and are accessible from the Supervisor. These files are displayed in **CMDB > Device > File**. Send only important files, as this can fill up disk space.
	  • **Compare Baseline**—Select this if you want to be alerted when the file changes from a baseline. This is common for configuration files that rarely change. If you choose this option, you will be asked to provide a copy of the baseline file. Click **Choose File** and upload the file from your workstation. The Supervisor will compute the MD5 checksum and distribute the checksum to the agents for comparison.

Process Monitoring tab:

Configure the **Process Monitoring** settings with reference to the table below:

Process Monitoring Settings	Guidelines
Process Monitoring	Check the Process Monitoring checkbox to collect Linux Server related performance metrics.

4. Click **Save**

Associate Linux Agents to Templates

After defining the monitoring templates, associate the hosts to templates. To scale to large number of Hosts, this is done via Policies. A Policy is a mapping from Organization and Host to Templates and Collectors. Policies are evaluated in order (lower order or rank is higher priority) and the policy that matches first is selected. Therefore, define the exceptions first followed by broad policies. Hosts can be defined in terms of CMDB Device Groups or Business Services. Multiple templates can be used in one Policy and the system detects conflicts, if any.

Complete these steps to associate a Host to Template:

1. Click **New** under the section **Host To Template Associations**.
2. In the **Host To Template Associations** dialog box, enter the information below.

Settings	Guidelines
Name	Name of the Host to Template Association.
Organization	Select the organization.
Host	Use the drop-down list to browse the folders and select the items.
Template	Select one or more monitoring templates from the list or select **All Templates** to select all. You can also use the search bar to find a specific template.
Collector	Select the Collector from the list or select **All Collectors** to select all. Agents forward events to Collectors via HTTP(S). A Collector is chosen at random and if that Collector is not available or non-responsive, then another Collector in the list is chosen.

3. Click **Save** and **Apply**.
   A **Rank** number is automatically assigned to the association.

You can use the **Edit** button to modify or **Delete** button to remove any template association.

Viewing Agent Status

Complete these steps to view the Agent status for any specific device:

1. Go to **CMDB** > **Devices** and select the device.
   The following fields displays the information related to the Agent:
   - Agent Status: status of the Agent running on the device.
   - Agent Policy: agent policy.
   - Monitor Status: status of monitoring.

   The **Agent Status** indicates the following:

Status	Description
Registered	Agent has completed registration but has not received the monitoring template.
Running Active	Agent has received a monitoring template and it is performing properly.
Running Inactive	Agent is running but does not have a monitoring template – the reasons can be (a) no license or (b) incomplete definition - no Collector or Template is defined for that host.
Stopped	Agent is stopped on the Linux Server.
Disconnected	Supervisor did not receive any status from the Agent for the last 10 minutes.

Enabling or Disabling an Agent

Complete these steps to enable or disable Linux Agent for a specific device:

1. Go to **CMDB** > **Devices** and select the required device.
2. Select the **Action** drop-down menu and click **Enable Agent** to enable or **Disable Agent** to disable Agent monitoring for the selected device.

Viewing Files in FortiSIEM

If the FortiSIEM Agent is running on a Server and a FIM policy is enabled with **Push Files On Modify**, then the FortiSIEM Agent will send the files to FortiSIEM when a change is detected. FortiSIEM stores the files in SVN on the Supervisor.

1. Go to the **CMDB** page. Make sure that **AGENT** is one of the **Methods**.
2. Search for the device in CMDB by name.
   Use the host name that you used to install the Linux Agent.

3. Click **File** beneath the device table.
   You will see all of the files that were changed since the monitoring template was applied.
4. Select a file.
   If you need to search for a file, set the **From** and **To** dates. The files which changed between those dates will be displayed.
5. Click the file name on the left and its contents will be displayed in the right hand window.
   Each file has a header containing file meta data followed by the actual file content.
   - **OWNER**: The name of the file owner
   - **GROUP**: User group for specifying file permissions.
   - **PERMISSION=USER: "OWNER", PERMIT: "..."**: The file owner's permissions.
   - **PERMISSION=GROUP: "MEMBER", PERMIT: "...":**: The group member's file permissions.
   - **PERMISSION=GROUP: "OTHER", PERMIT: "...":**: Other group file permissions.
   - FILEPATH: The full file name, including the path.
   - HASHCODE: The file hash.
   - HASHALGO: The algorithm used to compute file hash.
   - MODIFIED_TIME: The time when the file was last modified.
6. To see the differences between two files, select two files on left and click **Diff**.

File Integrity Monitoring Logs

The following sections describe various use cases that can be detected by File Integrity Monitoring Logs.

- Use Case 1: File Created
- Use Case 2: File Deleted
- Use Case 3: File Attributes Changed
- Use Case 4: File Modified
- Use Case 5: File Modified and Upload is Selected
- Use Case 6: File Baseline Changed
- Use Case 7: File Renamed
- Use Case 8: File Accessed
- Use Case 9: File Opened
- Use Case 10: File Closed
- Agent Troubleshooting Notes

Use Case 1: File Created

Event Type

`FSM_LINUX_FILE_CREATE`

Important Event Attributes

- `targetOsObjType`: The type of object that was created: `File` or `Directory`.
- `targetOsObjName`: The name of the file or directory.

- user: The name of the user who made the change.
- hashCode: The hash code of the file.
- hashAlgo: The algorithm used to create the file.

Reports

Agent FIM: Linux File/Directory Creation/Deletion/Movement/Unmount Activity

Rules

Agent FIM - Linux File or Directory Created

Sample Log

```
Fri Mar 27 09:39:25 2020 centos7: [FSM_LINUX_FILE_CREATE]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=CREATE,[targetObjType]=File,[targetObjName]="/mlm/a.log",
[hashCode]="d41d8cd98f00b204e9800998ecf8427e",[hashAlgo]="MD5",[user]=root
```

Use Case 2: File Deleted

Event Type

FSM_LINUX_FILE_DELETE

Important Event Attributes

- targetOsObjType: The type of object that was created: File or Directory.
- targetOsObjName: The name of the file or directory.
- user: The name of the user who made the change.

Reports

Agent FIM: Linux File/Directory Creation/Deletion/Movement/Unmount Activity

Rules

Agent FIM - Linux File or Directory Deleted

Sample Log

```
Fri Mar 27 09:43:11 2020 centos7: [FSM_LINUX_FILE_DELETE]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=DELETE,[targetObjType]=File,[targetObjName]="/mlm/k.log",
[user]=root
```

Use Case 3: File Attributes Changed

Event Type

FSM_LINUX_FILE_ATTRIB_CHANGE

Important Event Attributes

- targetOsObjType: The type of object: File or Directory.
- targetOsObjName: The name of the file or directory.
- user: The name of the user who made the change.

- `fileOwner`: The name of the owner of the file or directory.
- `userGrp`: The name of the user group for the file or directory.
- `userPerm`: The permission granted to the owner.
- `groupPerm`: The permission granted to the user group.
- `otherPerm`: Other permissions.

Reports

`Agent FIM: Linux File/Directory Ownership or Permission Changes`

Rules

- `Agent FIM - Linux Directory Ownership or Permission changed`
- `Agent FIM - Linux File Ownership or Permission Changed`

Sample Log

```
Fri Mar 27 09:45:27 2020 centos7: [FSM_LINUX_FILE_ATTRIB_CHANGE]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=ATTRIBUTE_CHANGE,[targetObjType]=File,
[targetObjName]="/mlm/mlm.txt",[fileOwner]="root",[groupName]="mlm",
[userPerm]="READ,WRITE,EXEC",[groupPerm]="READ,EXEC",[otherPerm]="READ,EXEC",[user]=root
```

Use Case 4: File Modified

Event Type

`FSM_LINUX_FILE_MODIFY`

Important Event Attributes

- `targetOsObjName`: The name of the file.
- `user`: The name of the user who made the change.
- `hashCode`: The hash code of the file.
- `hashAlgo`: The algorithm used to create the file.

Reports

`Agent FIM: Linux File Content Modified`

Rules

`Agent FIM - Linux File Content Modified`

Sample Log

```
Fri Mar 27 09:47:06 2020 centos7: [FSM_LINUX_FILE_MODIFY]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=MODIFY,[targetObjType]=File,
[targetObjName]="/mlm/mlm.txt",[hashCode]=5d71f074cf9a75e0324f210160d4b9cb,[hashAlgo]=md5,
[user]=root
```

Use Case 5: File Modified and Upload is Selected

Event Type

PH_DEV_MON_FILE_CONTENT_CHANGE

Important Event Attributes

- userId: The ID of the user who modified the file.
- domain: The user's domain for a Domain computer.
- fileName: The name of the file that was modified.
- procName: The Windows process that was used to modify the file.
- hashCode, hashAlgo: The file hash after modification and the algorithm used to calculate the hash.
- oldSVNVersion: The SVN revision number of the file before change.
- newSVNVersion: The SVN revision number of the file after change.
- addedItem: The lines that were added to the file.
- deletedItem: The lines that were removed from the file.

Reports

Agent FIM: Linux File Content Modified in SVN

Rules

Audited file or directory content modified in SVN

Sample Log

```
<14>Mar 27 09:51:30 sp3 phPerfMonitor[6340]: [PH_DEV_MON_FILE_CONTENT_CHANGE]:
[eventSeverity]=PHL_INFO,[procName]=phPerfMonitor,[fileName]=phSvnUpdate.cpp,
[lineNumber]=306,[phCustId]=2000,[hostName]=centos7,[hostIpAddr]=10.30.3.39,
[fileName]=/mlm/mlm.txt,[hashCode]=ac399331afa9d1f13618c9eff36ed51c,[oldSVNVersion]=53,
[newSVNVersion]=54,[deletedItem]=(none),[addedItem]=retest;,[user]=root,[hashAlgo]=MD5,
[phLogDetail]=
```

Use Case 6: File Baseline Changed

Event Type

FSM_LINUX_FILE_CHANGE_BASELINE

Important Event Attributes

- targetOsObjName: The name of the baseline file.
- user: The name of the user who made the change.
- hashCode: The hash code of the file after modification.
- hashAlgo: The algorithm used to create the file hash.
- targetHashCode: The hash code of the baseline file.

Reports

Agent FIM: Linux File Change from Baseline

Rules

Agent FIM - Linux File Changed From Baseline

Sample Log

```
Fri Mar 27 09:51:23 2020 centos7: [FSM_LINUX_FILE_CHANGE_BASELINE]:
[fileName]=/mlm/mlm.txt,[targetHashCode]="aa63e826654915e0e2e1da385e6d14f8",
[hashCode]="ac399331afa9d1f13618c9eff36ed51c",[hashAlgo]="MD5",[user]=root
```

Use Case 7: File Renamed

Event Types

- `FSM_LINUX_FILE_MOVED_TO`
- `FSM_LINUX_FILE_MOVED_FROM`

Important Event Attributes

- `targetOsObjType`: The file type: `File` or `Directory`.
- `targetOsObjName`: The file or directory name.
- `user`: The name of the user who renamed the file.

Reports

`Agent FIM: Linux File/Directory Creation/Deletion/Movement/Unmount Activity`

Rules

None

Sample Logs

```
Fri Mar 27 09:57:42 2020 centos7: [FSM_LINUX_FILE_MOVED_FROM]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=MOVED_FROM,[targetObjType]=File,
[targetObjName]="/mlm/bb.log",[user]=root
```

```
Fri Mar 27 09:57:42 2020 centos7: [FSM_LINUX_FILE_MOVED_TO]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=MOVED_TO,[targetObjType]=File,
[targetObjName]="/mlm/cc.log",[user]=root
```

Use Case 8: File Accessed

Event Type

`FSM_LINUX_FILE_ACCESS`

Important Event Attributes

- `targetOsObjType`: The file type: `File` or `Directory`.
- `targetOsObjName`: The file or directory name.
- `user`: The name of the user who accessed the file.

Reports

None

Rules

None

Sample Log

```
Fri Mar 27 10:05:28 2020 centos7: [FSM_LINUX_FILE_ACCESS]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=ACCESS,[targetObjType]=File,
[targetObjName]="/mlm/mlm.txt",[user]=root
```

Use Case 9: File Opened

Event Type

`FSM_LINUX_FILE_OPEN`

Important Event Attributes

- `targetOsObjType`: The file type: `File` or `Directory`.
- `targetOsObjName`: The file or directory name.
- `user`: The name of the user who opened the file.

Reports

None

Rules

None

Sample Log

```
Fri Mar 27 09:57:40 2020 centos7: [FSM_LINUX_FILE_OPEN]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=OPEN,[targetObjType]=Directory,[targetObjName]="/mlm",
[user]=root
```

Use Case 10: File Closed

Event Types

- `FSM_LINUX_FILE_CLOSE_WRITE`
- `FSM_LINUX_FILE_CLOSE_NOWRITE`

Important Event Attributes

- `targetOsObjType`: The file type: `File` or `Directory`.
- `targetOsObjName`: The file or directory name.
- `user`: The name of the user who closed the file.

Reports

None

Rules

None

Sample Logs

```
Fri Mar 27 09:57:36 2020 centos7: [FSM_LINUX_FILE_CLOSE_WRITE]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=CLOSE_WRITE,[targetObjType]=File,
[targetObjName]="/mlm/bb.log",[user]=root
```

```
Fri Mar 27 10:05:28 2020 centos7: [FSM_LINUX_FILE_CLOSE_NOWRITE]: [objectType]=Directory,
[objectName]=/mlm,[objectAction]=CLOSE_NOWRITE,[targetObjType]=File,
[targetObjName]="/mlm/mlm.txt",[user]=root
```

Agent Troubleshooting Notes

A Linux Agent can be in following states (shown in CMDB):

- Registered
- Running Inactive
- Running Active
- Disabled
- Disconnected

When an Agent is installed and registered, then it is in Registered state. The following audit event is generated: `PH_AUDIT_AGENT_INSTALLED`.

When a monitoring template is assigned to the device, then the state moves to Running Inactive. When the agent receives the template and starts monitoring, then the state moves to Running Active. In both cases, the following audit event is generated: `PH_AUDIT_AGENT_RUNNING`.

Agent periodically sends heartbeat messages. When a heartbeat not received for 10 minutes, the state moves to Disconnected and the audit event `PH_AUDIT_AGENT_NOTRESPONDING` is generated. Status is checked every 1 hour. At that time, if we heard from the Agent in the last 15 minutes, the state moves back to Running Inactive and a `PH_AUDIT_AGENT_RUNNING` audit event is generated.

If the Agent is disabled from the GUI, the state moves to Disabled and `PH_AUDIT_AGENT_DISABLED` audit event is generated.

If the Agent is uninstalled or the service is stopped, then the state moves to Disconnected and the audit event `PH_AUDIT_AGENT_NOTRESPONDING` is generated.

Audit events are generated at state transitions, however, the event `PH_AUDIT_AGENT_NOTRESPONDING` is generated every hour to identify all agents that are currently disconnected. A nested query can be run to detect Agents that did not report in the last N hours. Note that `PH_AUDIT` events must be queried with `System Event Category = 2`. Rules do not need this condition.

Configuring FortiSIEM Instance for FortiSIEM Manager

To configure a FortiSIEM instance to connect with FortiSIEM Manager, take the following steps from Supervisor.

Note: Make sure the FortiSIEM instance has been added to Manager before registering. For more information on adding a FortiSIEM instance to Manager, see Add a FortiSIEM Instance.

1. In the **FortiSIEM Manager FQDN/IP** field, enter the FortiSIEM Manager Fully Qualified Domain Name (FQDN) or IP address.
2. In the **FortiSIEM Instance Name** field, enter the name for this instance.
3. In the **Account** field, enter your account user name for FortiSIEM Manager that you created while adding the instance.
4. In the **Password** field, enter the password associated with the account.
5. In the **Confirm Password** field, re-enter your password.
6. Click **Test** to validate the configuration.
7. Click **Register**.

Unregister FortiSIEM Manager Instance

To unregister the FortiSIEM instance from FortiSIEM Manager, click **Unregister**.

Deleting FortiSIEM Manager Instance

To delete the FortiSIEM Manager instance, click **Delete**.

Testing FortiSIEM Instance

To test the FortiSIEM instance connection, click **Test**.

Device Support

The following sections provide procedures to configure device support:

- Working with Devices and Applications
- Working with Event Attributes
- Working with Event Types
- Working with Parsers
- Working with Custom Performance Monitors
- Working with Custom Properties
- Creating SNMP System Object Identifiers for Devices
- Analyzing Custom Log Files
- Configuring Local Syslog File Ingestion from a Directory
- Configuring Local PCAP File Ingestion from a Directory

Working with Devices or Applications

You can create a device/application if it is not available in the list for creating a parser or monitoring under **ADMIN** > **Device Support** > **Devices/Apps**.

This section provides the procedure to configure devices or applications.

- Adding a Device or Application
- Modifying a Device or Application

Adding a Device or Application

Complete these steps to add a new device or application:

1. Go to **ADMIN** > **Device Support** > **Devices/Apps** tab.
2. Click **New**.
3. In the **Device/Application Type Definition** dialog box, enter the information below.

Settings	Guidelines
Category	[Required] Select the **Device** or **Application** from the drop-down list.
Vendor	[Required] Vendor of the device or application.
Model	[Required] Device or application model.
Version	[Required] Version number of the device or application.
Device/App Group	[Required] Select the group where you want to add this new device/application
Biz Service Group	Select the Biz Service group.
Access Protocol	Select the Access Protocol from the drop-down.
App Package Group	This setting is applicable only for 'Application' category. Enter the app package group here.
Description	Description about the device or application.

4. Click **Save**.
   The new device(s)/application(s) appears in the list.
5. Select the device(s)/application(s) from the list and click **Apply**.

You can clone an existing device/application by clicking **Clone** and modify as necessary.

Modifying a Device or Application

Complete these steps to modify a device or application:

1. Select one or more device(s)/application(s) to edit from the list.
2. Click the required option:
   - **Edit** to modify any device/application setting.
   - **Delete** to remove any device /application.
3. Click **Save**.

Working with Event Attributes

Event attributes are used to capture parsed information from events. Create a new attribute if the one you want to use for your custom parser or monitor is not listed in **ADMIN** > **Device Support** > **Event Attributes**.

This section provides the procedure to create event attributes.

- Adding an Event Attribute
- Modifying an Event Attribute

Adding an Event Attribute

Complete these steps to add a new event attribute:

1. Go to **ADMIN** > **Device Support** > **Event Attributes** tab.
2. Click **New**.
3. In the **Add Event Attribute Type Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] Event attribute name
Display Name	[Required] Display name of the event attribute
Value Type	[Required] Select the value type from the drop-down to associate with the event attribute type.
Display Format	Units in which the event attribute has to be displayed
Description	Description of the event attribute

4. Click **Save**.
   The new event attribute appears in the list.
5. Select the event attribute(s) from the list and click **Apply**.

You can clone an existing event attribute type to use as the basis for a new one. Select the event attribute type you want to use, click **Clone** and modify as necessary.

Modifying an Event Attribute

Complete these steps to modify an event attribute setting:

1. Select one or more event attribute(s) to edit from the list.
2. Click the required option:
   - **Edit** to modify the settings of an event attribute(s).
   - **Delete** to remove an event attribute(s).
3. Click **Save**.

Working with Event Types

After parsing an event or log, FortiSIEM assigns a unique event type to that event/log. When you create a new custom parser for device logs, you have to add a new event type to FortiSIEM so the log events can be identified.

This section provides the procedure to create event types.

- Adding an Event Type
- Modifying an Event Type

Adding an Event Type

Complete these steps to add an event:

1. Go to **ADMIN** > **Device Support**> **Event Types** tab.
2. Click **New**.
3. In the **Event Definition** dialog box, enter the information below.

Settings	Guidelines
Name	[Required] If the event will be used for Custom Monitoring, the Event Type name must begin with `PH_DEV_MON_CUST_`. See here for more details on Custom Monitoring.
Device Type	[Required] Select a device from the drop-down list.
Event Type Group	[Required] Select the type of group for the event.
Severity	[Required] Severity (0 - lowest) to 10 (highest).
Description	Description of the event type.

4. Click **Save**.
   The new event appears in the table.
5. Select the event(s) from the list and click **Apply**.

You can also use the **Clone** option to duplicate and modify an existing event type.

Modifying an Event Type

Complete these steps to modify an event type:

1. Select one or more event attribute(s) to edit from the list.
2. Click the required option from the following table.
   - **Edit** - To modify the settings of a selected event(s).
   - **Delete** - To delete an event type.
3. Click **Save**.

Working with Parsers

- Overview
- Viewing all Parsers
- Understanding Parser Order
- Viewing a Specific Parser
- Disabling a Parser
- Enabling a Parser
- Deleting a Parser
- Modifying a Parser
- Creating a New Parser
- Adjusting Parser Order
- Appendix: Parser Specification
- Appendix: Built-in Patterns
- Appendix: Built-in Functions

Overview

A Parser (file) contains instructions for the FortiSIEM Parser module to parse a log into event attributes. Written in XML format, a parser file contains parsing instructions for one device type (e.g. FortiGate firewall, Cisco IOS based devices, Windows OS logs, etc.) or an application type (such as Windows IIS, Apache Web server, etc.). The Parser module complies the XML formatted parsers into C++ code that enables it to parse logs at high speed.

FortiSIEM comes with many built-in Parser files. Customers can modify the built-in Parser files or create their own.

Once a log is received by the Parser module, the Parser files are inspected in the **top-to-bottom order** specified in **Admin > Device Support > Parsers**. A Parser appearing earlier in the order is examined first for a match. The match is determined by the **Event Format Recognizer** regular expression inside each Parser file. If a match is found, then the **Parsing instructions** inside that file are executed to parse this log. All logs received from this IP address are parsed using the matched Parser file. If no matching Parser file is found, then the event type for this event is set to **`Unknown_Event_Type`**.

A Parser file is written using XML syntax. It consists of the following sections:

- **Event Format Recognizer**: This section specifies the condition that a log must match to be able to be parsed by the instructions in this file.
- **General Parsing Patterns**: This is a list of regular expressions of parsing patterns that can be used in parsing instructions.
- **Parsing Instructions**: This specifies instructions for parsing the logs matching the Event Format Recognizer.

The overall structure of a Parser XML file is

```
<patternDefinitions> </patternDefinitions>
<eventFormatRecognizer> </eventFormatRecognizer>
<parsingInstructions> </parsingInstructions>
```

Viewing all Parsers

1. Logon to GUI.
2. Go to **Admin > Device Support > Parsers**.

The list of parsers is shown in a tabular format.

- **Enabled**: If Enabled is checked, then this parser will be used to parse logs.
- **Name**: The name of the parser.
- **Device Type**: This specifies the device or application type whose logs will be parsed.
- **Scope**: For system defined parsers, **Scope** is set to **System**. For user defined parsers, **Scope** is set to **User**.

System defined parsers cannot be modified by user. To modify, you must take the following steps:

1. **Clone** the system defined parser.
2. Make your changes to the new user defined parser (Scope = User).
3. **Validate** and **Test** the new user defined parser.
4. **Disable** the system defined parser and **Enable** the user defined parser.
5. Apply the changes.

Understanding Parser Order

Logs from devices that have a specific differentiating keyword should appear earlier in the list of parsers. For example: Apache logs have differentiating keywords:

- Apache_AccessLog
- Apache_ErrorLog
- ApacheLog

This can be seen in the logs below:

```
<142>Sep 17 13:27:37 example.com ApacheLog 192.168.20.35 - - [17/Sep/2009:13:27:37 -0700]
"GET /icons/apache_pb2.gif HTTP/1.1" 200 2414 "http://192.168.0.30/" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)".
```

```
<182>Mar 22 19:00:14 lab1.example.com Apache_ErrorLog: [Tue Mar 22 16:17:41.711593 2022]
[proxy_http:error] [pid 1029463:tid 140695402702592] (104)Connection reset by peer: [client
192.168.0.30:59703] AH01102: error reading status line from remote server localhost:8181,
referer: https://192.168.1.1/phoenix/html/analytics
```

In contrast, Unix logs have no differentiating keywords and are identified by the process names e.g. sshd, sudo, etc.

```
<86>Dec 14 16:53:39 abc-desktop sshd[14666]: pam_unix(sshd:session): session opened for
user joeUser by (uid=0)
```

```
<86>Dec 14 16:54:22 abc-desktop sshd[14666]: pam_unix(sshd:session): session closed for
user joeUser
```

```
<85>Dec 20 13:58:12 abc-desktop sudo: joeUser : TTY=pts/1 ; PWD=/home/joeUser ; USER=root ;
COMMAND=/bin/vi /var/log/messages
```

Therefore, ApacheParser appears in the 4th position from top, while UnixParser appears in 3rd position from the bottom.

Viewing a Specific Parser

Follow these steps:

1. Logon to GUI.
2. Go to **Admin > Device Support > Parsers**.
3. Select the parser you wish to view and click **Clone**. The parser content will be visible in the popup window. You can **Search** for specific string in the parser body.
4. Click **Cancel** to return to the list view.

Disabling a Parser

Follow these steps to disable a specific parser:

1. Logon to GUI.
2. Go to **Admin > Device Support > Parsers**.
3. Select the parser you wish to disable. If **Enabled** is checked, then click the **Enabled** checkbox.
4. In the Disable Parser dialog, click **Yes**.
5. From the main list view, click **Apply**. This pushes this change to all the FortiSIEM nodes.

Enabling a Parser

Follow these steps to enable a specific parser:

1. Logon to GUI.
2. Go to **Admin > Device Support > Parsers**.
3. Select the parser you wish to enable. If **Enabled** is not checked, then click the **Enabled** checkbox.
4. You will be asked to **Test** the parser. This makes sure that the test events defined in this parser are only parsed by this parser and no other parser above it in the list.
   a. The Test Event(s) are shown in the top portion of the window. You can add one or more Test Events by clicking **New**.
   b. Click **Test**. The parsing results will be shown in the middle and bottom portions of the window.
   c. The middle portion of the window shows the overall parsing result for each Test event.
      i. **Result**: This will appear as either **Passed** or **Failed**.
      ii. **Event**: Shows the Test Event used in testing.
      iii. **Expected Parser**: This should be this parser that you are trying to enable.
      iv. **Used Parser**: This should be this parser if the Test passed. On the other hand, if the Test failed and this event is parsed by another parser, then Used Parser will show that parser.
   d. Select one Test Event from the middle portion of the window and the bottom portion of the window shows the full list of parsed event attributes of the selected event.
   e. Once Test has passed, click **Enable**.
5. From the main list view, click **Apply**. This pushes this change to all the FortiSIEM nodes.

Deleting a Parser

You can only delete a user defined parser. System defined parsers can only be disabled.

Follow these steps to delete a specific user defined parser:

1. Logon to GUI.
2. Go to **Admin > Device Support > Parsers**.
3. Select the parser you wish to delete. Click **Delete**.
4. From the main list view, click **Apply**. This pushes this change to all the FortiSIEM nodes.

Modifying a Parser

You might want to modify a parser when you want to extend or correct the parsing of an existing parser. To create a totally new parser for a different device or application type, follow the steps in Creating a New Parser.

Follow these steps to modify a specific parser:

1. Logon to GUI.
2. Go to **Admin > Device Support > Parsers**.
3. Select the parser.
   a. If it is a *user defined* parser, click **Edit**.
   b. If it is a *system defined* parser,
      i. Click **Clone**. In the display window, enter a name for the cloned parser and click **Save**.
      ii. The cloned parser will be added *right after* the parent parser.
      iii. Disable the parent parser following the steps in Disabling a Parser.
      iv. Select the Cloned parser for editing, and click **Edit**.
   c. Make any changes as needed. You can click the expand/reduce ( ) button to toggle the size of the work area.
   d. Click **Validate** to check the XML syntax. If the Validate step shows any errors, then fix the errors.
   e. After the Validate step, click **Test** to go to the Test window. Then click **Test** to make sure that the test events defined in this parser are only parsed by this parser and no other parser above it in the list.
   f. **Test result** will be shown in the middle and bottom portion of the window.
      i. The middle portion of the window shows the overall parsing result for each Test event.
         i. **Result**: This will appear as either **Passed** or **Failed**.
         ii. **Event**: Shows the Test Event used in testing.
         iii. **Expected Parser**: This should be this parser that you are trying to enable.
         iv. **Used Parser**: This should be this parser if the Test passed. On the other hand, if the Test failed and this event is parsed by another parser, then Used Parser will show that parser.
      ii. Select one Test Event from the middle portion of the window and the bottom portion of the window shows the full list of parsed event attributes of the selected event.
   g. Once Test has passed, click **< Back** and then click **Save**.
4. Click **Enable**.
5. Click **Apply**. This pushes this change to all the FortiSIEM nodes.

Creating a New Parser

You might want to create a new parser when you want to add support to a new device type or support logs collected via a different access method.

Follow these steps to create a brand-new parser:

1. Logon to GUI.
2. Go to **Admin > Device Support > Parsers**.
3. From the main list view, select an existing parser where you wish to **insert the new parser afterward**. Note the discussion around Parser Order in Understanding Parser Order. Then click **New**. The new parser will be added right after the selected parser and it will be disabled. It can only be enabled after it has passed the Validate and Test steps below.

4. Write the parser.
   a. In the **Name** field, enter a name for the parser.
   b. From the **Device Type** drop-down, select a device type. The parser applies for all logs for this device type. If the device type is not present, then you can create it from **Admin > Device Support > Devices/Apps > New**.
   c. You can click the expand/reduce (🗔) button to toggle the size of the work area. Enter **Pattern Definitions** (Optional). This is a list of regular expressions of parsing patterns that can be used as part of parsing instructions. You can see the `<patternDefinitions>` section in each system defined parser for examples.
   d. Enter **Event Format Recognizer**: This specifies the condition that must be matched by all logs parsed by this file. You can see the `<eventFormatRecognizer>` section in each system defined parser for examples. You can also see Parser Specification for more details.
   e. Enter **Parsing Instructions**. You can see the `<parsingInstructions>` section in each system defined parser for examples. You can also see Parser Specification for more details.
   f. Click **Validate** to check the XML syntax. If the Validate step shows any errors, then fix the errors.
   g. After Validate step, click **Test** to make sure that the test events defined in this parser are only parsed by this parser and no other parser above it in the list.
   h. **Test result** will be shown in the middle and bottom portions of the window.
      i. The middle portion of the window shows the overall parsing result for each Test event.
         i. **Result**: This will appear as either **Passed** or **Failed**.
         ii. **Event**: Shows the Test Event used in testing.
         iii. **Expected Parser**: This should be this parser that you are trying to enable.
         iv. **Used Parser**: This should be this parser if the Test passed. On the other hand, if the Test failed and this event is parsed by another parser, then Used Parser will show that parser.
      ii. Select one Test Event in the middle portion of the window and the bottom portion of the window shows the full list of parsed event attributes of the selected event.
   i. Once Test has passed, click **< Back** and then click **Save**.
5. Click **Enable**.
6. Click **Apply**. This pushes this change to all the FortiSIEM nodes.

Adjusting Parser Order

Note from the discussion in Understanding Parser Order that parsers are applied in the top to bottom order in the parser list in **Admin > Device Support > Parsers**. Therefore, *parsers for devices that have a specific differentiating keyword should appear earlier in the list of parsers*.

If parsers were not ordered correctly, that is, a parser with a loose Event Format Recognizer was placed earlier in the list than a parser with a specific Event Format Recognizer, then **Parser Test** will fail.

FortiSIEM will not allow you to enable a parser until the parser order is correct, which means that all the Test Events inside a specific parser will be parsed by the parsing instructions in that parser and not by one above in the list. There are two ways to fix the parser order:

1. Reorder the parsers by clicking **Up** and/or **Down**. For example, suppose the parser order is P1 -> P2-> P3 and enabling P3 is failing as its events are being parsed by P2. Select P3 and click **Up**. Then the order will be P1 -> P3-> P2. Try enabling P3 after this change. Click **Apply** to push the changes to all FortiSIEM nodes.
2. If there are too many orders to fix, then you can take the following approach. Click **Fix Order**. This will arrange the parsers with system-defined parsers at the top of the list in their original order, and user-defined parsers at the bottom. You can then place the user-defined parsers in the correct position. Click **Apply** to push the changes to all FortiSIEM nodes.

Working with Custom Performance Monitors

Creating a custom performance monitor involves creating a performance object that specifies the monitoring access protocol to use, maps event attributes available for that protocol to FortiSIEM event attribute types, and then associates those attributes to an event type. You can use system or user-defined device types, event attribute types, and event types when creating the performance object. The following sections provide information about working with Performance Monitors:

- Creating a Custom Performance Monitor
- Monitoring Protocol Configuration Settings
- Mapping Monitoring Protocol Objects to Event Attributes
- Managing Monitoring of System and Application Metrics for Devices
- Appendix: Examples of Custom Performance Monitors

Creating a Custom Performance Monitor

You can create Custom Performance Monitors by defining the performance object that you want to monitor, including the relationship between the performance object and FortiSIEM events and event attributes, and then associating the performance object to a device type.

In Service Provider FortiSIEM deployments, custom performance monitors have to be created by the Super/Global account, and apply to all organizations. In enterprise deployments, custom performance monitors can be created by any user who has access to the **ADMIN** tab.

Prerequisites

- You should review the configuration settings for the monitoring protocols that you will use in your monitor, and be ready to provide the appropriate OIDs, classes, or database table attributes for the access protocol.
- You should have created any new device/application types, event attributes, or event types that you want to use in your Performance Monitor.
- You should have the IP address and access credentials for a device that you can use to test the monitor.

Creating the Performance Object and Applying it to a Device

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Click **New**.

3. Enter a **Name** for the Performance Monitor.
4. For **Type**, select either **System** or **Application**.
5. For **Method**, select the monitoring protocol for the performance monitor.
   See the topics under Monitoring Protocol Configuration Settings for more information about the configuration settings for each type of monitoring protocol.
6. Click **New** next to **List of Attributes**, and create the mapping between the performance object and FortiSIEM event attributes.
   Note that the Method you select will determine the name of this mapping and the configuration options that are available. See Mapping Monitoring Protocol Objects to Event Attributes for more information.
7. Select the **Event Type** that will be monitored. Event Types used for Custom Monitoring must begin with `PH_DEV_MON_CUST_`.
8. Enter the **Polling Frequency** for the monitor.
9. Enter a **Description**.
10. Click **Save**.
11. Under **Enter Device Type to Performance Object Association** section, click **New**.
12. Enter a **Name** for the mapping.
13. Select the **Device Type** from the drop-down for which you want to apply the monitor.
    Whenever a device belonging to the selected device type is discovered, FortiSIEM will attempt to apply the performance monitor to it.
14. Click **Perf Objects** drop-down to select or search the Performance Objects.
15. Click **Save**.

Testing the Performance Monitor

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Select the Performance Monitor.
3. Click **Test**.
4. For **IP**, enter the IP address of the device that you want to use to test the monitor.
   Testing for Multi-Tenant Deployments: If you have a Service Provider FortiSIEM, select the Supervisor or Collector where the device is monitored.
5. Click **Test**.If the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

After you have successfully tested and applied the performance monitor, you should initiate discovery of the device that it will monitor, and then make sure that the new monitor is enabled as described in Managing Monitoring of System and Application Metrics for Devices.

Monitoring Protocol Configuration Settings

These topics describe the configuration settings for monitoring Protocols such as SNMP, WMI, and JDBC that are used for creating custom Performance Monitors.

- JDBC Configuration Settings
- JMX Configuration Settings
- SNMP Configuration Settings for Custom Performance Monitors
- WMI Configuration Settings for Custom Performance Monitors
- Login Configuration Settings for Custom Performance Monitors

JDBC Configuration Settings

Use these settings when configuring JDBC as the access protocol for a custom performance monitor. You might want to review the topic Custom JDBC Performance Monitor for a Custom Table as an example of how to set up a custom performance monitor using JDBC.

Field	Setting/Notes
Method	JDBC
Database Type	Select the type of database to connect to
SQL Query	The SQL Query to execute when connecting
List of Columns	This creates the mapping between columns in the database and FortiSIEM event attributes. See Mapping Monitoring Protocol Objects to Event Attributes for more information.
Where Clause	This indicates whether the database table being queried has a fixed set of rows, or whether it is growing over time. An example of this would be a table containing logs, in which case FortiSIEM would keep track of the last entry and only pull the new ones. There are three options here: **1.** There is a fixed set of rows and all rows are needed. Leave all options cleared. **2.** There is a fixed set of rows and a fixed number of rows are needed. Select **Fixed records** and enter the number of required rows. **3.** The table is growing and only new values are needed. Select **Retrieve all new values since last retrieve time of column**, and enter the name of the column that represents time in the database. FortiSIEM will keep track of the largest value in this column and only pull entries greater than that value during the next polling interval.
Event Type	Select the **Event Type** from the drop-down for which you want to apply the monitor. Whenever a event belonging to the selected method is discovered, FortiSIEM will attempt to apply the performance monitor to it.
Polling Frequency	Enter the **Polling Frequency** for the monitor.

JMX Configuration Settings

When configuring JMX as the monitoring protocol for a custom performance monitor, use these settings. You may also want to review the topic Custom JMX Monitor for IBM Websphere as an example of creating a custom JMX performance monitor.

Field	Setting/Notes
Method	JMX
MBean	Enter the MBean interface that you want to monitor, or click the downward arrow to browse the JMX tree and select it. Note that the option you select here will determine the objects that are available when you select an **Object Attribute** for the **List of Attributes**. See the next section in this topic for information on how to find MBeans
Event Type	Select the **Event Type** from the drop-down for which you want to apply the monitor. Whenever a event belonging to the selected method is discovered, FortiSIEM will attempt to apply the performance monitor to it.
Polling Frequency	Enter the **Polling Frequency** for the monitor.

Identifying MBean Names and Attributes for Custom Applications

This section discusses how to get MBean names and attributes for custom J2EE based applications.

1. Launch JConsole on your workstation and connect to the application.
2. Select the **MBeans** tab.
3. Browse to the application you want to monitor, and select it.
4. In the right pane, you will see the `MBeanInfo`. Note the `ObjectName`, while the attributes for the application will be listed in the tree view.

SNMP Configuration Settings for Custom Performance Monitors

When configuring SNMP as the access protocol for a custom performance monitor, use these settings. You may also want to review the topics Custom SNMP Monitor for D-Link Interface Network Statistics and Custom SNMP Monitor for D-Link HostName and SysUpTime as example of how to set up a custom performance monitor using SNMP.

Field	Settings/Notes
Method	SNMP
Parent OID	The parent Object Identifier (OID) is used to optimize the number of SNMP GETs required

Field	Settings/Notes
	for pulling the various individual OIDs. You can enter this directly, or click the downward arrow to select it from an MIB file. Several different MIB files are available to select from, see Importing OID Definitions from a MIB File for more information.
Parent ID is table	Select **is table** if the OIDs you want to monitor are in a table with at least one row. An example would be interface metrics, such as `ifInOctets` and `ifOutOctets`, since there is an interface metric for each interface.
List of OIDs	The OIDs you want to monitor mapped to FortiSIEM event attributes. The selection you make for **Parent OID** determines the options available in the **OID** menu when you select **New**.

Importing OID Definitions from a MIB File

Many devices include MIB files that you can then use to create a custom performance monitor for the device. This involves creating a configuration file based on information in the MIB file, using that file as input for the `mib2xml` executable, and then placing the resulting output file in the `/data/mibXml` directory of your Supervisor. Once placed in this directory, you can select the file from the **MIB File List** menu to select the parent OID, which will then also affect which OIDs you can select for the OID to event attribute mapping.

Procedure

1. Collect the device OID files you want to use and place them in a directory where the mib2XML resides.
2. Create the input config file with these fields, and name it with the `.cfg` file extension.
   See the attached alcatel.cfg file for an example. (**Note:** the link is available only in the HTML version of the User Guide.)

Field	Description
`group`	This is the number of MIB file group. MIB files must be analyzed as a group because of cross-references within them. The group attribute specifies an ID for each group and needs to be unique for every group.
`mibFile`	The name of the MIB file being analyzed. There can be multiple entries. Be sure to specify the path to the MIB files.
`vendor`	The name of the device vendor for the MIB file.
`model`	The model name or number for the device.
`evtPrefix`	As SNMP trap notification definitions in the MIB file are parsed, an event file is generated for each SNMP trap. This field specifies the event type prefix.
`enterpriseId`	The enterprise ID number for this vendor, which is used for generating the SNMP trap parser.

3. Run `mib2XML <filename>.cfg`.
4. Move the resulting `.mib.xml` file to the `/data/mibXml` directory of your Supervisor.

Example

In this example, a set of MIB files from an Alcatel 7x50 device are used to generate the XML output file. (**Note:** the following links are available only in the HTML version of the User Guide.)

1. Sample MIB files:
   TIMETRA-CHASSIS-MIB.mib
   TIMETRA-GLOBAL-MIB.mib
   TIMETRA-SYSTEM-MIB.mib
   TIMETRA-TC-MIB.mib
2. Information in these files, and the paths to them, are then used to create this config file.
   alcatel.cfg
3. Running `mib2xml alcatel.cfg` generates both an output and an mib2XML file.
   alcatel.out
   TIMETRA-TC-MIB.mib.xml

WMI Configuration Settings for Custom Performance Monitors

When configuring WMI as the monitoring protocol for a custom performance monitor, use these settings. You may also want to review the topic Custom WMI Monitor for Windows Domain and Physical Registry as example of how to set up a custom performance monitor using WMI.

Field	Settings
Method	WMI
Parent Class	WMI metrics are defined in the form of a parent class having multiple attributes. For example, the parent class `Win32_ComputerSystem` has the attributes `Domain` and `TotalPhysicalMemory`.
Is Table	If the parent WMI class is a table with one or more rows, select this option.

LOGIN Configuration Settings for Custom Performance Monitors

From the **Used For** drop-down list, choose **File Monitor**, **Target File**, **Command Output Monitoring**, or **Configuration Monitoring**.

Used For: File Monitor

Field	Settings
File Path	This setting is pre-populated with the **Parent OID/Class/File Path** value.

Used For: Target File

Field	Settings
File Path	This setting is pre-populated with the **Parent OID/Class/File Path** value.
Upload Target File	Click **Upload** and browse to the file you want to upload.

Used For: Command Output Monitoring

Field	Settings
Command	
Regular Expression	Enter a regex expression.
Matched Attribute Count	
Apply Regular Expression to	Select Single Line or Multiple Lines.
List of Attributes	Click **Edit** to edit an existing attribute or **New** to create a new attribute. See Adding Attributes for Command Output Monitoring.

Used For : Configuration Monitoring

Field	Settings
Upload Expect Script	Click **Upload** to browse for the script you want to use.

Adding Attributes for Command Output Monitoring

Click **New** to add a new attribute or **Edit** to modify an existing attribute.

Field	Settings
Matched Position	
Format	Select either **INTEGER**, **DOUBLE**, or **STRING** from the drop-down list.
Type	Select **Counter** or **Raw Value** from the drop-down list.
Event Attribute	Click the drop-down list and select an event attribute from the table.
Transform	For information on adding transforms, see Creating Transforms.

Mapping Monitoring Protocol Objects to Event Attributes

When you select a monitoring protocol for your custom performance monitor, you must also establish the relationship between the objects used by that protocol and event attributes in FortiSIEM. For example, creating a performance monitor that uses SNMP to monitor a device requires that you create a mapping between the SNMP OIDs that you want to monitor, and set of event attributes. This topic describes the configuration settings that you will use to create these object-to-event attribute relationships.

1. When creating your custom performance monitor, after you have selected the **Method**, click **New** next to **List of Attributes**.
   Depending on the monitoring protocol that you select, this table may be named **List of Oids** (SNMP), or **List of Columns** (JDBC).
2. In the first field, enter or select the monitoring protocol object that you want to map to FortiSIEM event attribute.
   Your options depend on the monitoring protocol you selected for Method.

Monitoring Protocol	Field name	Settings/Notes
SNMP	**OID**	Select an MIB file from the **MIB File List**, and then select the OID that you want to create the mapping for.You must enter an **Event Type** and a **Polling Frequency**.
WMI	**Attributes**	Enter an attribute of the WMI class you entered for **Parent Class**. You must enter an **Event Type** and a **Polling Frequency**.
JMX	**Object Attribute**	The **MBean** you select determines the attributes you can select. You must enter an **Event Type** and a **Polling Frequency**. You will also have to enter a **Name** and **Private Key** for the MBean attribute.
JDBC	**Column Name**	Select the **Database Type**, the **SQL Query** and specify the list of columns. You must enter an **Event Type** and a **Polling Frequency**.
WINEXE	**Matched Position**	Enter the Matched Position. You must enter an **Event Type** and a **Polling Frequency**.
LOGIN	**Used For**	Select **File Monitor**, **Target File**, **Command Output Monitoring**, or **Configuration Monitoring** from the drop-down list.

3. Select the **Format** for the object attribute.
   Your options will depend on the monitoring protocol you selected for Method.
4. For **Type**, select **Raw Value** or **Counter**.
5. For **Event Attribute**, select the FortiSIEM event attribute that the monitoring protocol object should map to.
   If you must create a new event attribute, see Adding an Event Attribute.

6. Create any **Transforms** of the values returned for the monitoring protocol object.
   See the next section for more information how to configure transforms.
7. Click **Save** when you are done creating the mappings, and complete the configuration of your custom performance monitor.

Creating Transforms

You can use a transform to convert the value returned for your monitoring project object into a more physically meaningful or usable metric. You an create multiple transforms, and they will be evaluated in the order shown in the table. Multiple transforms can be selected – they are evaluated in sequential order as shown in the display table.

1. Next to **Transforms**, click **New**.
2. For **Type**, select **system** or **custom**.
3. For **Formula**, either select a system-defined transformation formula from the menu if you selected **System** for **Type**, or enter a formula if you selected **custom**.
4. Click **Save**.

You can use the **Edit**, **Delete** or **Clone** buttons to modify, remove or clone a Transform respectively.

Managing Monitoring of System and Application Metrics for Devices

When FortiSIEM discovers devices, it also discovers the system and application metrics that can be monitored for each device, and displays these in the **Monitor Performance** tab of **ADMIN** > **Setup**. Here you can also disable the monitoring of specific metrics for devices, disable devices from being monitored, and change the polling interval for specific metrics. See Checking status of event pulling jobs for checking the status.

1. Go to **ADMIN > Setup > Monitor Performance**.
2. Click **Refresh** icon to make sure you have the latest list of devices.
3. To disable monitoring for a device, clear the **Enable** option for it.
4. To enable or disable monitoring of a specific metrics for a device, click a device to select it, then click **More** and select **Edit System Monitors** or **Edit App Monitors**to view the list of metrics associated with that monitor and device. You can also enable or disable the metrics for a device's monitor type by clicking on the **Edit System Monitoring** or **Edit Application Monitoring** section for the device.
5. To change the polling interval for a metric, in the **More** menu, select **Edit Intervals**. Select the **Monitor Type** and **Device**, and then set the interval.
6. When you are done making changes, click **Save**.

Working with Custom Properties

FortiSIEM includes over 30+ pre-defined global threshold properties that you can edit and use in rules, but you can also create custom threshold properties.

This section provides the procedure to configure Custom Properties.

- Adding a Custom Property
- Modifying a Custom Property

Adding a Custom Property

Complete these steps to add a custom property:

1. Go to **ADMIN** > **Device Support** > **Custom Properties**.
2. Click **New**.
3. Enter a **Name** and **Display Name** for the new property.
4. Enter the **Default Value** for the threshold.
5. Select the **Value Type** of threshold value.
   For most global threshold values, select **Double**. For **Map** thresholds, which apply to disks and interfaces, select the **Item Type** for the threshold value, and select the **Component Type** to which it applies.
6. Click **Save**.

Modifying a Custom Property

Complete these steps to modify a custom property:

1. Select one or more property from the list.
2. Click the required option:
   - **Edit** to modify a property setting.
   - **Delete** to remove a property.
3. Click **Save**.

Creating SNMP System Object Identifiers for Devices

If a new device has to be identified using SNMP System Object Identifiers (OIDs) during discovery, you can create a device type and add the SNMP System OID or this device from the FortiSIEM UI.

Complete these steps to create SNMP Object Identifiers for device discovery:

1. Go to **ADMIN** > **Device Support** > **SNMP SysObjectId**.
2. Click **New**.
3. Select the **Device Type** from the drop-down which lists all the devices added in the system under **Device Support** > **Device/Apps**.
4. Enter the **Hardware Model** of the device.
5. Enter an **SNMP SysObjectId** for the device.
6. Click **Save**.

Analyzing Custom Log Files

Custom CSV formatted log files can be uploaded from the FortiSIEM GUI for detailed analysis. For this, a mapping has to be defined from the CSV file columns to the event attributes. This generates a FortiSIEM event that can be searched, similar to an externally received event.

Complete these steps to upload a custom log file for analysis:

1. Set up a Parsing template:
   a. Go to **ADMIN** > **Device Support** > **Upload File**.
   b. Click **New**.
   c. Upload the log file under **Step 1: CSV file**:
      i. Browse to select the **Sample File** to upload.
      ii. Enter the **Separator** used in the CSV file.
      iii. To include the header, select **Header**.
      iv. Click **Next**.
   d. Map the CSV file columns to the event attributes under **Step 2: Attribute Mapping**:
      i. Select the event attributes to map to the CSV file columns.
      ii. Click **Next**.
   e. Set the template details under **Step 3: Template Details**:
      i. Enter a **Name** for the Template.
      ii. The **Event Type** is automatically updated based on the name.
      iii. Enter any **Description** about the Template.
      iv. Click **Save**.
2. Upload the file.
3. Run Reports.

Configuring Local Syslog File Ingestion from a Directory

Currently, FortiSIEM handles logs either (a) sent to it via Protocols such as Syslog, SNMP trap and so on or (b) pulled from devices via Protocols such as WMI, Checkpoint LEA and so on.

FortiSIEM can process log files copied to a directory on one of the FortiSIEM nodes:

- Copy the files to a specific directory named by the reporting device IP. For Service Provider installations, create this directory on the Collector of the Organization to which these log files belong. The attribute `event_sftp_directory` in `phoenix_config.txt` defines the path. For example, to handle logs from a device with IP: `1.2.3.4`, create log files in `<event_sftp_directory>/1.2.3.4`. A typical example is `opt/phoenix/cache/syslog/1.2.3.4`.
- Each log in the files should be formatted exactly in the same way as sent by the device. If this is a new log source, a new parser may need to be defined.
- Each file should have a distinct time stamp to prevent files from being overwritten.
- Set `event_eps_limit_controls in phoenix_config.txt` to control the EPS burst.
  - If `event_eps_limit_controls` is set to '10', FortiSIEM will process 30 events from this file in 3 seconds.
  - If `event_eps_limit_controls` is set to '0', FortiSIEM will process as many log files as possible and this may inhibit the overall EPS license usage.
  - If you change a `phoenix_config.txt` parameter, then reload the parser on that node.

Note the following:

- The log file is deleted once it has been read. Keep a separate backup if required.
- The system requires write access to the log file directory in order to delete the log file once read. This is important because if the log file cannot be deleted, it is repeatedly read and consumed by FortiSIEM resulting in many duplicate events and extra EPS consumption.

Configuring Local PCAP File Ingestion from a Directory

The configure local PCAP file ingestion from a directory, take the following steps:

Update the phoenix_config file.

1. Go to `/opt/phoenix/config/`.
2. Edit the `/opt/phoenix/config/phoenix_config.txt` file as follows:
   Change:
   ```
   # FSM upgrade preserves customer changes to parameter value
   pcap_file_directory= #/opt/phoenix/cache/PCAP
   ```
   to
   ```
   # FSM upgrade preserves customer changes to parameter value
   pcap_file_directory=/opt/phoenix/cache/PCAP
   ```
3. Save the file.
4. Create and chown the directory by running the following commands.
   ```
   [root@fortisiem ~]# mkdir /opt/phoenix/cache/PCAP
   [root@fortisiem ~]# chown admin:admin /opt/phoenix/cache/PCAP
   ```
5. Restart the application processes to read the configuration changes using the following commands. Note that this will cause a few minutes interruption to event processing, resulting in new events received being lost as the phParser process is restarted.
   ```
   [root@fortisiem PCAP]# phtools --stop phParser
   [root@fortisiem PCAP]# phtools --start phParser
   ```
6. Copy the .pcap file to the directory `/opt/phoenix/cache/PCAP`, using SCP or SFTP to copy the PCAP file to the directory. **Note**: the file will be deleted once ingested, keep another copy if required.
7. Search for the PCAP data by performing an Analytics query for 'Event Type = PH_DEV_MON_PCAP_DATA'. PCAP data is written as JSON formatted events with event type `PH_DEV_MON_PCAP_DATA`. Various attributes are also parsed, and can be used in advanced queries.

Health

The following sections provide procedures to view health information:

- Viewing Cloud Health
- Viewing Collector Health
- Viewing Agent Health
- Viewing Elasticsearch Health
- Viewing Replication Health

Viewing Cloud Health

The **ADMIN** > **Health** > **Cloud Health** page displays the status of the nodes in your deployment and the processes running on them. The top frame displays all of the available clouds and the lower frame provides information about the applications that are contained in the cloud selected in the main frame.

Complete these steps to view the information about Cloud health:

1. Go to **ADMIN** > **Health** > **Cloud Health** tab.
2. Click any node in the first frame to view its process details in the second frame.
   See the FortiSIEM Back-End Processes table for more information about the system role played by each process.

First Frame

Settings	Description
Name	Name of the node
IP Address	IP address of the node
Module Role	Module role, for example, 'Super' for Supervisor.
HA/DR Role	The role of the node, for example Primary Leader.
Health	Current health of node
Last Status Updated	The date and time when status was last updated.
Version	FortiSIEM version running on node
EPS	Events per second
Load Average	Average load of the node
CPU	Percentage CPU used
Memory	Percentage Memory used
Swap	Percentage Swap space used
Disk	Percentage Disk used
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	The current upload buffer size (KB) and queue.
Content Version	The current content version that the node is on.
Content Update Status	The status of the content update

Second Frame

Settings	Description
Process Name	Name of the process
Owner	The owner of the process
Status	Status of the process
Uptime	Total up time of the process
CPU	Measure of the CPU that the process is using
Memory	Measure of the Memory that the process is using
Resident Memory	The amount of memory the process is allocated
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)
SharedStore Type	SharedStore type (reader, writer)
SharedStore Position	SharedStore location
SharedStore Percent	SharedStore utilization percentage

FortiSIEM Back-End Processes

Process	Function	Present in Supervisor	Present in Worker	Present in Collector
Apache	Webserver for front-ending http (s) requests to AppSvr or other FortiSIEM nodes	x	x	x
AppSvr	Middleware for handling GUI requests, storing and managing PostgreSQL database and serving REST API requests from FortiSIEM nodes	x		
DBSvr	PostgreSQL Database for storing information displayed in FortiSIEM GUI other than events	x		
Node.js-charting	Message			
Node.js-pm2				
phAgentManager	Collects logs and metrics from devices or servers using protocols other than SNMP and WMI.	x	x	x
phCheckpoint	Collects logs from Checkpoint firewalls via LEA			
phDataManager	Stores the parsed events to event store (FortiSIEM EventDB or Elasticsearch)	x	x	
phDataPurger	Archives online event store (FortiSIEM EventDB or Elasticsearch). Implements event retention policy for FortiSIEM EventDB - both online FortiSIEM EventDB and archive.	x		
phDiscover	Discovers devices using various protocols such as SNMP, WMI and SSH	x		x
phEventForwarder	Forwards events from FortiSIEM to external Systems	x	x	x
phIpIdentityMaster	Merges Identity and location audit trails from multiple phIpIdentityWorker modules to produce the final Identity and location audit trail. Stores the trail in PostgreSQL Database.			

Process	Function	Present in Supervisor	Present in Worker	Present in Collector
phIpIdentityWorker	Produces Identity and location audit trail based on its own view of events	x	x	
phMonitor	Monitors the health of FortiSIEM processes. Distributes tasks from AppSvr to various processes on Supervisor and to phMonitor on Worker for further dustribution to processes on Worker nodes.			
phParser	Parses raw events and preparses them for storing into event store (FortiSIEM EventDB or Elasticsearch)	x	x	x
phPerfMonitor	Continually collects performance monitoring and configuration change data after discovery completes	x	x	x
phQueryMaster	Handles Adhoc queries from GUI for FortiSIEM EventDB. Paralellizes queries by sending them to phQueryWorkers and merges individual results to produce the final result.	x		
phQueryWorker	Handles individual FortiSIEM EventDB queries from phQueryMaster	x	x	
phReportLoader	Loads Report data into Report Server.	x		
phReportMaster	Handles individual FortiSIEM EventDB inline reports. Produces results every 5 minutes.	x		
phReportWorker	Handles inline event reports FortiSIEM EventDB.Merges individual inline report results multiple phReportMaster modules to produce the final result. Rolls up results from 5 minute intervals to 15 minute intervals and then to 60 minute intervals.	x		

Process	Function	Present in Supervisor	Present in Worker	Present in Collector
phRuleMaster	Triggers a rule in real time by evaluating rule summaries from individual phRuleWorker modules	x		
phRuleWorker	Evaluates a rule in real time based on events seen by the worker and sends a summary to the phRuleMaster module	x	x	
Redis	In-memory distributed database for holding results returned by Elasticsearch and for distributing CMDB objects between Supervisor and Worker nodes.	x	x	
SVNLite	A light weight version of Subversion, this file revision management tool stores the file change history for windows/linux servers, routers/switches and windows/linux agents. **Note**: • Files are stored in `/svn/repos`. • To conserve space, files are automatically deleted when the disk gets full based on thresholds defined in `svnlite.revisions.purge` on the Supervisor.	x		

Viewing Collector Health

If your FortiSIEM deployment includes Collectors, you can monitor the status of the Collectors in the **ADMIN** > **Health** > **Collector Health** page. You can also upgrade Collectors from this page. Select a Collector and click **Show Processes** to see the processes running on that Collector. Click **Tunnels** to open a Tunnels window to view any open tunnels. If you have upgraded or performed a fresh install of FortiSIEM 6.3.0, you will need to re-configure Tunnels to open them. See Open Tunnel Re-Configuration Required after 6.3.0 or later Upgrade/Fresh Install.
Refer to the 'FortiSIEM Back-End Processes' table below for information about the processes that run on Collectors.

The **Action** menu provides the operations you can perform on a Collector:

- **Start** - to start the Collector.
- **Stop** - to stop the Collector.
- **Download Image** - to download a Collector image.
- **Install Image** - to install a Collector image.
- **Download Update** - to download a Collector image update.
- **Install Update** - to install a Collector image update.

From the Tunnels window (appears when Tunnels is selected), the following operations are available.

- **Close Tunnel** - Select a tunnel, and click **Close Tunnel** to close the tunnel.
- **Close All** - Click to close all open tunnels.

For information on the table, see Properties associated with Tunnels.

Properties Associated with Collector Health

Collector Property	Description
Organization	Name of the organization to which the Collector belongs.
Collector ID	ID of the Collector.
Collector Name	Name of the Collector.
IP Address	IP address of the Collector.
Health	Health of the Collector based on the health of the modules running on it. If Health is **Critical**, it means that one of the modules is not running on the Collector.
Last Status Updated	The time when the Collector last reported its status to the cloud.
Last File Received	The time when the Collector last reported its performance status to the cloud.
Collector Type	The Collector type is displayed.
Version	The FortiSIEM version running on the Collector.
Cores	Number of cores Collector has.
Memory Size	Memory allocated for Collector.
Swap Size	Swap space allocated for Collector.
Uptime	Total time that the Collector has been up.
EPS	Overall Events per second (EPS) running on Collector.
CPU	Overall CPU utilization of the Collector.
Memory	Overall memory utilization of the Collector.
Swap	Percentage Swap space used
Disk	Percentage Disk used
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	Upload buffer size utilized.
Last Event Time	The time when the Collector last reported events to the cloud.
Upgrade Version	If the Collector has been upgraded, the new version.
Build Date	Date on which the version of FortiSIEM the Collector is running on was built.
Content Version	Version of FortiSIEM the Collector is running on.
Content Update Status	The status of the content update is displayed.
Install Status	If you upgrade the Collector, the status of the upgrade is shown here as either **Success** or **Failed**.

Collector Property	Description
Download Status	If an image was downloaded to the Collector, the status of the download is shown here as **Success** or **Failed**.
Group Name	Check - doesn't exist yet - guessing it will be called group name. The group name that the VIP Collector is part of.
Virtual IP	The virtual internet protocol (VIP) address used by the Collector.
VIP Active	The connectivity status of the VIP Collector.
VIP Interface	The interface used by the VIP Collector.
VIP Role	The VIP Collector's role (Leader or Follower).
VIP Priority	The priority number configured to the VIP Collector. The larger the number, the greater the priority.
VIP Router Id	The router ID of the VIP Collector.

Process Properties

Process Property	Description
Process Name	Name of the process.
Owner	The owner of the process.
Status	Status of the process as either **Up** or **Down**.
Uptime	Total time that the process has been up.
CPU	Measure of the CPU that the process is using
Memory	Measure of the Memory that the process is using
Resident Memory	The amount of memory the process is allocated
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)

FortiSIEM Back-End Processes

Process	Function	Used by Supervisor	Used by Worker	Used by Collector
phAgentManager	Execute event pulling job	X	X	X
phCheckpoint	Execute checkpoint monitoring	X	X	X
phDiscover	Pulling basic data from target	X		X
phEventForwarder	Responsible for forwarding events and incidents from FortiSIEM to external systems	X	X	X
phEventPackage	Uploading event/SVN file to Supervisor/Worker			X
phMonitorAgent	Monitoring other processes	X	X	X
phParser	Parsing event to shared store (SS)	X	X	X
phPerfMonitor	Execute performance job	X	X	X
rsyslogd	Responsible for forwarding locally generated logs to FortiSIEM	X	X	X

Properties Associated with Tunnels

Collector Property	Description
Host IP	The Host IP address of the tunnel.
Super Port	The supervisor port.
Protocol	The protocol used by the tunnel.
Protocol Port	The port used by the protocol.
Collector	The collector with the open tunnel.
PID	The Process ID.
Opened Time	The amount of time the tunnel is open.

Open Tunnel Re-Configuration Required after 6.3.0 or later Upgrade/Fresh Install

After upgrading or doing a fresh install of 6.3.0 and later, the feature - "Connect to" a CMDB device via 'Open Tunnel' will no longer work without a configuration change. When users connect via a tunnel, it will appear that the tunnel is opened. However, the displayed Supervisor's port on which the tunneled connection is running is actually not open so users will not be able to connect either via plugin or directly.

To re-enable this feature, take the following steps:

Edit `sshd_config.tunneluser` on the Supervisor by changing the entry `AllowTcpForwarding` to `yes`.

```
AllowTcpForwarding yes
```

Reload the tunnel sshd configuration using the following command:

```
kill -HUP $(pgrep -f sshd_config.tunneluser)
```

If you have tunnels you had opened after the upgrade, but prior to making the above change, you will need to click on the **Close All** button from **ADMIN > Health > Collector Health > Tunnels** page.

This fix was done to address bug 602294: CVE-2004-1653 SSH port forwarding exposes unprotected internal services.

Viewing Agent Health

If your FortiSIEM deployment includes agents, you can monitor the status of your Windows and Linux agents in the **ADMIN** > **Health** > **Agent Health** page. You can also install and upgrade your Windows and Linux agents here.

The **Search...** field allows you to filter agents by name.

The **Action** menu provides the operations you can perform on an Agent:

- **Download Image** - to download a Windows Agent or Linux Agent image.
- **Install Image** - to install a Windows Agent or Linux Agent image.

The **Columns** drop-down list allows you select what agent properties you want to appear in the table.

You can filter agents by organization that appear in the table by using the drop-down list next to the **Columns** drop-down list.

The refresh drop-down list allows you to refresh the status with any of the following options: Refresh Now, 15 seconds, 30 seconds, 1 minute, 2 minutes, 3 minutes.

Properties Associated with Agent Health

Agent Property	Description
Name	The name of the agent device is displayed. Clicking on the name will take you to the **CMDB > Devices** page for that device, where you can edit the device's configuration or view other information.
IP Address	The IP address of the agent is displayed.
Device Type	The operating system running the agent is displayed.
Agent Type	The agent server type is listed.
Agent Version	The version that the agent is running on is displayed.
Agent Status	The agent's current status is displayed.
Event Status	The event status reported by the agent is displayed.
Monitor Status	The monitor status is displayed. This is for performance monitoring.
Agent Policy	The name of the policy configured for the agent is displayed.
Status	The status of an agent's last action is displayed.
Discovered	The date when an agent was discovered is displayed.
Agent ID	The ID of the agent is displayed.
Upgrade Status	The status of the upgrade is displayed.

Event Receive Status

Displays device receiving event status metric information.

Monitor Status

Monitor Status displays metric information based on your server and protocol configuration. See **What is Discovered and Monitored** for your specific server in the External Systems Configuration Guide for more information.
Note: This table does not appear if there is no monitoring configuration.

Viewing Elasticsearch Health

The Elasticsearch Health page displays two frames of information.

Complete these steps to view Elasticsearch health details:

1. Go to **ADMIN** > **Health** > **Elasticsearch Health** tab.
2. Click **Columns** tab under both frames to select the required information to display.

Frame 1 Column Name	Description
Cluster	The name of the Elasticsearch cluster.
IP Address	The IP address of the Elasticsearch cluster.
Status	The current status of the Elasticsearch cluster.
Nodes	The number of nodes in the Elasticsearch cluster.
Data Nodes	The number of data nodes.
Shards	The number of shards in Elasticsearch cluster.
Active Shards	The number of active shards in Elasticsearch cluster.
Configured Nodes	The number of configured nodes.
Indices	The number of indices in the Elasticsearch cluster.

Frame 2 Column Name	Description
Name	The name of the node.
IP Address	The IP address of the node.
Role	The node's roles are listed.
Status	The current status.
Version	The version of Elasticsearch running on the node.
Uptime	The period of time the node has been operational.
Load	The load setting for the node.
OS	The OS being used.
Total Memory	The total memory of the node.
Used Memory	The used amount of memory of the node.
Used Swap	The used swap space.
FS Total	The total file system space.
Available	The amount of available space for the node.

Viewing Replication Health

Disaster Recovery involves replicating CMDB (in PostgreSQL database), Configuration (in SVN-lite), Profiles (in SQLite database) and Event data (in FortiSIEM EventDB or Elasticsearch) from Primary to Secondary. This page shows the replication health in terms of delay in synching these databases from Primary to Secondary.

Note: This page is not continuously updated. To manually refresh, click the refresh button on the top right.

Complete these steps to view Replication health details:

1. Go to **ADMIN** > **Health** > **Replication Health** tab.

CMDB Replication	Description
Status	The status can be Critical, Warning, or Normal. **Critical**: If replication paused or delay greater than 30 minutes **Warning**: Delay between 15 minutes and 30 minutes **Normal**: Delay less than 15 minutes
Last Synched	The time when PostgreSQL database was last synched.
Delay	Displays how many bytes remained to be synched and the amount of time needed to synch.

Configuration Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%
Last Synched	The time when SVN-lite was last synched.
Delay	Displays how many bytes remained to be synched .

Profile Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%
Last Synched	The time when SQlite was last synched.
Delay	Displays how many bytes remained to be synched .

EventDB Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%
Last Synched	The time when FortiSIEM EventDB was last synched.
Delay	Displays how many bytes remained to be synched .

Elasticsearch Replication	Description
Status	The status is based on the progress calculated as the ratio of Secondary Bytes and Primary Bytes. **Critical**: Progress less than 10% **Warning**: Progress between 10% and 75% **Normal**: Progress greater than 75%
Last Synched	The time when Elasticsearch indices were last synched.
Delay	Displays how many bytes remained to be synched .

License

The following sections provide procedures to view License information:

- Viewing License Information
- Viewing License Usage
- Working with Nodes
- Configuring and Maintaining Active-Active Supervisor Cluster
- Configuring Disaster Recovery

Viewing License Information

FortiSIEM offers two types of licenses, one based on EPS usage, and another based on GB used per day. The License displays information associated with your current FortiSIEM license under **ADMIN** > **License** > **General** tab.

Additional information on license enforcement is available here.

Information about license usage is available here.

- EPS Based Licensing
- GB Per Day Licensing

EPS Based Licensing

For EPS based licensing, the Top Heading shows you the following:

- Serial Number
- Hardware ID
- License Type
- FIPS Mode

The table displays the value and expiry date for each of the following attributes.

- Devices
- Endpoint Devices
- Additional EPS
- Total EPS
- Agents
- UEBA
- IOC Service
- Maintenance and Support

You can use the **Upload License** button on the top-right to upload a new License. For more information, refer to FortiSIEM Licensing Guide.

GB Per Day Licensing

GB Per Day Licensing is available for any FortiSIEM version except FortiSIEM Cloud and FortiSIEM hardware appliances. It can used with EventDB, Elasticsearch and ClickHouse. A top banner

appears with the number of violations found in the last 30 days. The Top Heading shows you the following:

- Serial Number
- Hardware ID / License Hardware ID
- License Type
- FIPS Mode

The table displays the value and expiry date for each of the following attributes.

- Raw Event GB Per Day
- Agents
- UEBA
- IOC Service
- Maintenance and Support
- High Availability Service

You can use the **Upload License** button on the top-right to upload a new License. For more information, refer to FortiSIEM Licensing Guide.

Viewing License Usage

Depending on the type of FortiSIEM License you have, the License Usage page will display the appropriate information.

- EPS Licensing
- GB Per Day Licensing

EPS Licensing

The **Usage** tab displays information on your license usage. Select the desired time period from the top-right drop-down to **Last 15 Minutes**, **Last 1 Hour**, **Last 1 Day**, or **Last 1 Week**.

The current License information is displayed under various tabs:

- **Device Usage** - Organization, Licensed, and Used devices
- **Agent Usage** - Organization, Windows Agents, Linux Agents, and total agents used for an organization
- **EPS Usage** - Total Licensed EPS, Used EPS and Unused Events
- **EPS Usage by Node** - EPS Usage based on each Node
- **EPS Usage by Organization** - EPS Usage based on each Organization

To print the monthly usage report, select an Organization under **Device Usage**, then click the **Print Monthly Usage Report** button on the top-right corner.

- About Events Per Second
- EPS Usage By Node
- EPS Usage by Organization
- Used EPS (Global)
- Notes

About Events Per Second

Events per second (EPS) is a key monitoring metric. Since it is tied to licensing, only the following events are included in EPS:

1. External logs – includes logs sent directly to FortiSIEM, logs pulled via FortiSIEM nodes, e.g. AWS CloudTrail, and logs sent by FortiSIEM Windows/Linux agents.
2. Performance monitoring logs (e.g. event type beginning with PH_DEV_MON)

EPS Usage By Node

This metric provides the MAX EPS handled by a FortiSIEM node, over the chosen time period in GUI. The trend line shows the MAX EPS over smaller intervals in the trend graph.

For a Collector node, EPS Usage is the incoming EPS at the Collector. For Supervisor/Worker node, EPS Usage consists of two elements:

1. EPS sent by the Collectors to Supervisor/Worker node
2. EPS from external devices that may be directly sending to that Supervisor/Worker node.

Every 3 minutes, the event PH_SYSTEM_EPS_NODE is generated. The data shown on this page is based on the system report "FortiSIEM Received EPS By Node" that uses this event.

See PH_SYSTEM_EPS_NODE in the Log Reference Guide for a description of the event.

Examples

3 Collectors 25 EPS each, sending to 2 Workers in a load balanced way. Then EPS usage of each Collector is 25. EPS Usage of Worker is 3*25/2 = 37.5. EPS Usage of Supervisor is 0.

3 Collectors 25 EPS each, sending to Supervisor. External devices are sending 10 EPS to Supervisor. Then, EPS usage of each Collector is 25, and EPS Usage of Supervisor is 85.

EPS Usage by Organization

For Enterprise case, there is only one Org - Supervisor/Local. For Service Provider case, there can be many Orgs. Typically, a Collector belongs to one Org. But a Collector belonging to Supervisor/Local Organization may handle many Orgs. EPS Usage by Org is derived by mapping the EPS usage of each Collector to Orgs they belong to.

Every 3 minutes, the event PH_SYSTEM_EPS_ORG is generated. The data shown on this page is based on the system report "FortiSIEM Received EPS By Organization" that uses this event.

See PH_SYSTEM_EPS_ORG in the Log Reference Guide for a description of the event.

Example

3 Collectors receiving 25 EPS each. Each Collector sends to 2 Workers in a load balanced way. 2 Collectors belong to Org1 and 1 Collector belongs to Org2. Then:

- EPS Usage of Org1 is 50
- EPS Usage of Org2 is 25
- EPS Usage of Supervisor/Local is 0.

Used EPS (Global)

This is the total EPS handled by the FortiSIEM cluster.

Every 3 minutes, the event PH_SYSTEM_EPS_GLOBAL is generated. The data shown on this page is based on the system report "FortiSIEM Event Processing Statistics" using this event.

See PH_SYSTEM_EPS_GLOBAL in the Log Reference Guide for a description of the event.

Example

3 Collectors receives 25 EPS each and then sends to 2 Workers in a load balanced way. Each Worker receives 10 EPS each from external devices. In this case, the Used EPS is 95.

Notes

1. Using MAX EPS versus Average EPS: EPS varies over time and has many peaks and valleys. Reasons are varied: Because of peaks and valleys, Avg EPS is typically much smaller than MAX EPS. Since a SIEM is designed to not lose events, MAX EPS over smaller intervals is a better way to judge the system usage than Average EPS.
   a. During business hours, EPS is high while it goes down after hours. During the early part of the day, say 8AM - 9AM, EPS tends to be higher than the rest of the day.
   b. If there is a new device that is brought under management and the device generates significant EPS, then it will immediately show a spike.
   c. If events are pulled from AWS S3 bucket, then it may depend on how often it is written to the buckets.
2. Being a distributed system, the EPS is calculated in different nodes in 3 minute intervals, but the intervals at different nodes may not always line up. So, the aggregate numbers may be a little off.

GB Per Day Licensing

The **Usage** tab displays information on your license usage. Select the desired time period from the top-right drop-down to **Last 15 Minutes**, **Last 1 Hour**, **Last 1 Day**, or **Last 1 Week**.

The current License information is displayed under various tabs:

- **Agent Usage** - Organization, Windows Agents, Linux Agents, and total agents used for an organization
- **Raw Event Usage** - A bar graph displays the GB used per day. Use the top-right drop-down to view the bar graph for a period of **Last 10 Days**, **Last 30 Days**, or **Last 60 Days**. A top 20 Organizations by Usage, top 20 Devices by Usage and top 20 Event Types by Usage list is provided to determine where the greatest amount of raw events is coming from, and what are the most common raw events. Click on to go to the Analytics page for the "top 20" item you wish to analyze further.

  Click on / to view the "top 20" item information as a list or pie chart respectively.

To print the monthly usage report, select an Organization under **Agent Usage**, then click the **Print Monthly Usage Report** button on the top-right corner.

- Violations
- About Raw Event Usage
- Notes

Violations

GB Per Day Licensing allows 10 violations within a span of the most current 30 days before triggering. The number of violation s is color coded as:

- 0-3 Violations: Green
- 4-6 Violations: Yellow
- 7-10 Violations: Red

After the 11th violation (12 days total within a 30 day period), **Dashboard** and **Analytics** are disabled for each day that a violation occurs. FortiSIEM also allows you to easily recognize the general GB Per Day usage for the Last 10 Days through color coding -

- 75% of License Utilized : Green
- 76%-90% of License Utilized: Yellow
- 90% or more of License Utilized : Red

About Raw Event Usage

GB Per Day License is based on:

- Total Raw event size per day (GB/Day)
- Number of Agents
- Number of UEBA Agents
- FortiGuard IOC

Notes

1. In this license scheme, users can have as many devices and events per second (EPS) as can be supported by their deployed hardware, without violating the Total Raw event size per day (GB/Day) limits.
2. If a device was **Unmanaged** because of the previous device and EPS-based license, then after applying the new GB/Day license, the user must re-discover the device as **Managed** for these devices to become managed.
3. To apply this new license type, the user must get a new license from FortiCare and upload that license to FortiSIEM Supervisor, following the same normal license procedure.

Working with Nodes

A FortiSIEM node is part of an Analytics cluster and can be of four types:

- Supervisor node: this can be of 3 sub-types
  - Primary Leader - this node is instantiated when the system is installed
  - Primary Follower (can be instantiated if High Availability is enabled)
  - Secondary Supervisor (can be instantiated if Disaster Recovery is enabled)
- Worker node

The following features are available from the **License > Nodes** page.

- Viewing a Node
- Adding a Node
- Editing a Node
- Deleting a Node

Viewing a Node

The **Nodes** tab displays information on your existing nodes. You can refresh this page by clicking on the refresh icon. If you are working with nodes for ClickHouse, see the ClickHouse Configuration page for specific ClickHouse information on handling nodes.View, add, edit, or delete nodes from this page.

The Nodes table allows you to view the following information.

Settings	Description
Host Name	The host name of the node.
IP Address	The IP address of the node.
Mode	Displays what the node is working as - Worker or Supervisor.
HA/ DR Role	High Availability (HA) Role shows what role a node is acting as in a Supervisor Cluster. A node will either be **Primary Leader**, or a **Primary Follower** in an Supervisor Cluster configuration. Disaster Recovery (DR) Role shows what role a node is acting as in Disaster Recovery, either **Primary** or **Secondary**.
HA/DR Status	Displays the status of the node. For Disaster Recovery, **Active** indicates that the Primary and Secondary nodes are in sync and that Disaster Recovery is working. If the status is **Inactive** in either the Primary or Secondary nodes involved with Disaster Recovery, it means that the Primary and Secondary are NOT in sync, and that Disaster Recovery is not working. For a Supervisor node not in Disaster Recovery or a Worker node, the Replication Status appears as **N/A**.
Leader	Displays who the leader node is for the follower node in a High Availability Supervisor Cluster configuration.
Licensed	Displays the current license status of the node.

Adding a Node

When the system is installed, a Primary Leader node is instantiated.

- Adding a Worker Node
- Adding a Primary Follower Node (with High Availability Node)
- Adding a Secondary Supervisor Node (with Disaster Recovery Enabled)

Adding a Worker Node

Complete these steps to add a Worker:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Click **Add**.
3. From the **Type** drop-down list, select **Worker**.
4. In the **Worker IP Address** field, enter the Worker IP Address.
5. If your storage solution is ClickHouse, the following options are available:
   a. From the **Storage Tiers** drop-down list, select the number of storage tiers.
   b. In Hot Tier, under **Disk Path**, enter the mount point.

c. In Warm Tier, under **Disk Path**, if multiple storage tiers is selected, under Disk Path, enter the mount point.
d. Click **+** to add another Hot Tier or Warm Tier field.
e. Click **Test** to verify the mount point(s).
f. Click **Save** when done.

6. Click **OK**.

Note: If you are doing Real time Archive to HDFS, then remember to go to **ADMIN > Setup > Storage > Archive** and click **Test** and **Save**. This will prepare the newly added worker for real time archive.

Adding a Primary Follower Node (with High Availability Node)

See Adding Primary Follower in Configuring and Maintaining Active-Active Supervisor Cluster.

Adding a Secondary Supervisor Node (with Disaster Recovery Enabled)

See Disaster Recovery.

Editing a Node

- Editing a Worker Node
- Editing the Primary Leader Node
- Editing a Primary Follower Node
- Editing Secondary Supervisor (with Disaster Recovery Enabled)

Editing a Worker Node

Complete these steps to edit a Worker:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select a Worker.
3. Click **Edit**.
4. Make any changes needed.
5. If your storage solution is ClickHouse, the following options are available:
   Click **+** to add another Hot Tier or Warm Tier field.
   Click **-** to remove a Hot Tier or Warm Tier field.

   a. From the **Storage Tiers** drop-down list, select the number of storage tiers.
   b. In Hot Tier, under **Disk Path**, enter the mount point.
   c. In Warm Tier, under **Disk Path**, if multiple storage tiers is selected, under Disk Path, enter the mount point.
   d. Click **Test** to verify the mount point(s).
   e. Click **Save** when done.
6. Click **OK**.

Editing the Primary Leader Node

Complete these steps to edit your Primary Leader.

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select the Primary Leader.
3. Click **Edit**.
4. Make any necessary changes needed to the available fields.
5. Click **Save**.

Editing a Primary Follower Node

1. Go to **ADMIN > License > Nodes** tab.
2. Select the Primary Follower.
3. Click **Edit**.
4. Make any necessary changes needed to the available fields.
5. Click **Save**.

Editing Secondary Supervisor (with Disaster Recovery Enabled)

Complete these steps to edit your Disaster Recovery Setup:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select the Secondary.
3. Click **Edit**.
4. Make any changes needed to the Disaster Recovery Setup. See Configuring Disaster Recovery for more information.
5. Click **OK**.

Deleting a Node

- Deleting Worker Node
- Deleting Primary Follower Node

Deleting Worker Node

Complete these steps to delete a Worker:

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select a Worker.
3. Click **Delete**.
4. Click **OK**.

Deleting Primary Follower Node

1. Go to **ADMIN** > **License** > **Nodes** tab.
2. Select the Primary Follower.
3. Click **Delete**.
4. Ensure the Supervisor node is shut down.
5. Click **Yes** to confirm the deletion.

Configuring and Maintaining Active-Active Supervisor Cluster

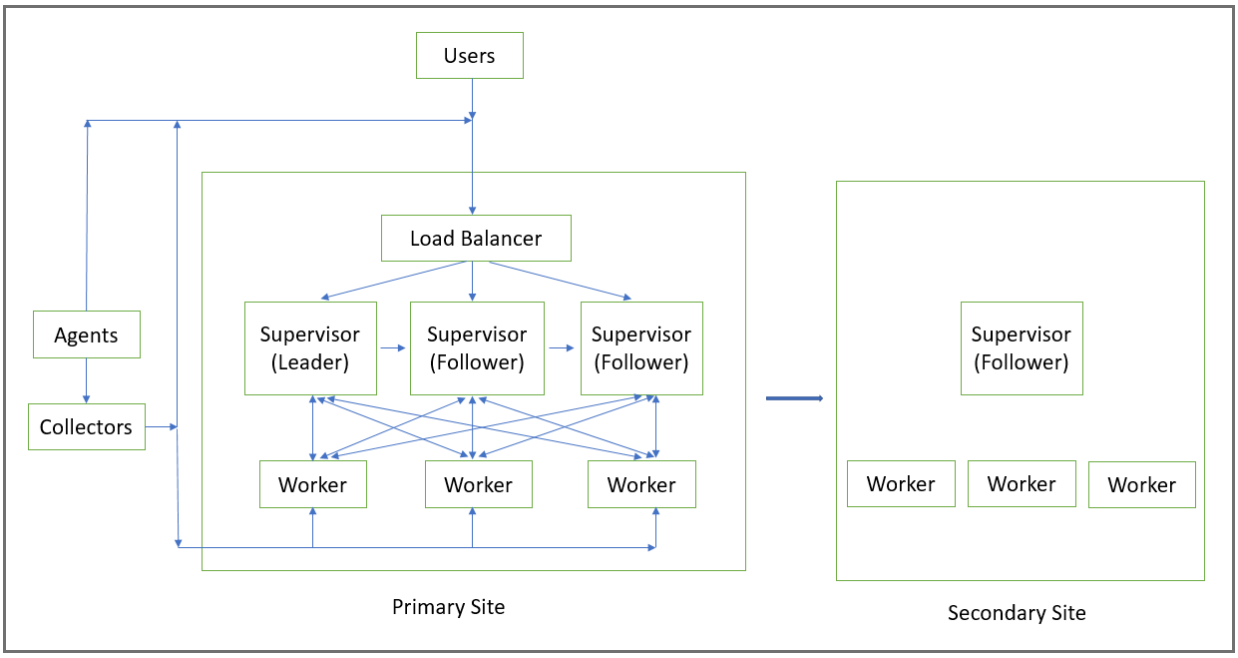
You can setup multiple Supervisors in Active-Active mode with an external Load Balancer in front. This enables you to log in to any Supervisor node and perform any GUI operation. Supervisor node functionalities are distributed across the available Supervisor nodes. An Active-Active Supervisor Cluster provides resilience against Supervisor failures, allows higher number of GUI users, Agents, Collectors, and higher volume of rule and query processing.

This document covers the following topics:

- Operational Overview
- Configuration
  - Adding Primary Leader
  - Adding Primary Follower
  - Load Balancer Setup
  - Collecting UUID and SSH Public Key
  - External Load Balancer Configuration
- Maintenance
  - Failover Operations
  - Adding a Failed Supervisor back to Cluster
  - Checking Cluster Replication Health
  - Maintenance Operations
  - Upgrade

Operational Overview

An Active-Active Supervisor cluster is built around the concept of Leader and Follower Supervisor nodes, set up as a linked list.



1. The first Supervisor where you install License, is the Leader. The Leader's UUID matches the UUID in the installed FortiCare License. On the Leader, Redis and PostGreSQL database services run in Master mode. That means that all PostGreSQL database writes from all Supervisors go to the Leader node.
2. Next, you add a Primary Follower, which follows the Leader, in the sense that its PostGreSQL database is replicated from that of the Leader. On the Follower node, both Redis and PostGreSQL database services run in Follower (that is, read only) mode.
3. You can add another Primary Follower and it will follow the Supervisor node added in Step 2. Its PostGreSQL database is replicated from the Supervisor created in Step 2. On this node, both Redis and PostGreSQL database services run in Follower (that is, read only) mode. A replication chain is formed: Leader -> Follower in Step 2 -> Follower in Step 3.
4. You can add more Primary Follower nodes by successfully chaining from the last Follower node in the chain (in this case, the Follower node created in Step 3).

It is recommended that you put a Load Balancer in front of the Active-Active Supervisor cluster and define the Load Balancer in FortiSIEM GUI (**ADMIN > Settings > Cluster Config > Supervisors**). Then Collectors, Agents and GUI users can reach any of the Supervisors through the Load Balancer. Make sure that the Load Balancer address or host name is reachable from the Collectors, Agents and GUI users.

If you decide to not use a Load Balancer, you can list the Supervisors individually in **ADMIN > Settings > Cluster Config > Supervisors**. Make sure that the Supervisor addresses or host names are reachable from the Collectors, Agents and GUI users. A GUI user can log in to any Supervisor and use FortiSIEM.

Note that Workers to Supervisors communication is maintained internally – Workers are aware of the Supervisors and their Leader/Follower role and communicate to the appropriate node in a load balanced manner.

If the Leader Supervisor fails, then you need to login to the Follower Supervisor in the chain and promote that node to be the Leader by following the instructions in Failover Operations.

The Disaster Recovery feature works with Active-Active Supervisor Cluster. You can login to any Active-Active Supervisor and define the Supervisor for Disaster Recovery. The Primary Leader will replicate the PostGreSQL database, Profile database and SVN-lite files to the Secondary.

FortiSIEM Manager feature also works with Active-Active Supervisor Cluster. You can login to any Active-Active Supervisor and define the FortiSIEM Manager.

To upgrade an Active-Active Supervisor cluster, upgrade the Leader first and then the Followers. See the Upgrade Guide for more information.

Configuration

The following topics are available for configuration.

- Adding Primary Leader
- Adding Primary Follower
- Load Balancer Setup
- Collecting UUID and SSH Public Key
- External Load Balancer Configuration

Adding Primary Leader

Installation

Follow the appropriate Installation Guide, available at the FortiSIEM Doc Library here. During the installation process, select **1 Supervisor** at the **Config Target** window and complete the Installation.

Configuration

When the license is installed, the FortiSIEM unit will be recognized as the Leader. No special configuration is required. For steps on acquiring the UUID, see Collecting UUID and SSH Public Key.

Adding Primary Follower

Installation

Note that you need a High Availability License to add a Follower.

Follow the appropriate Installation Guide, available at the FortiSIEM Doc Library here. During the installation process, select **5 Supervisor Follower** at the **Config Target** window and complete the installation.

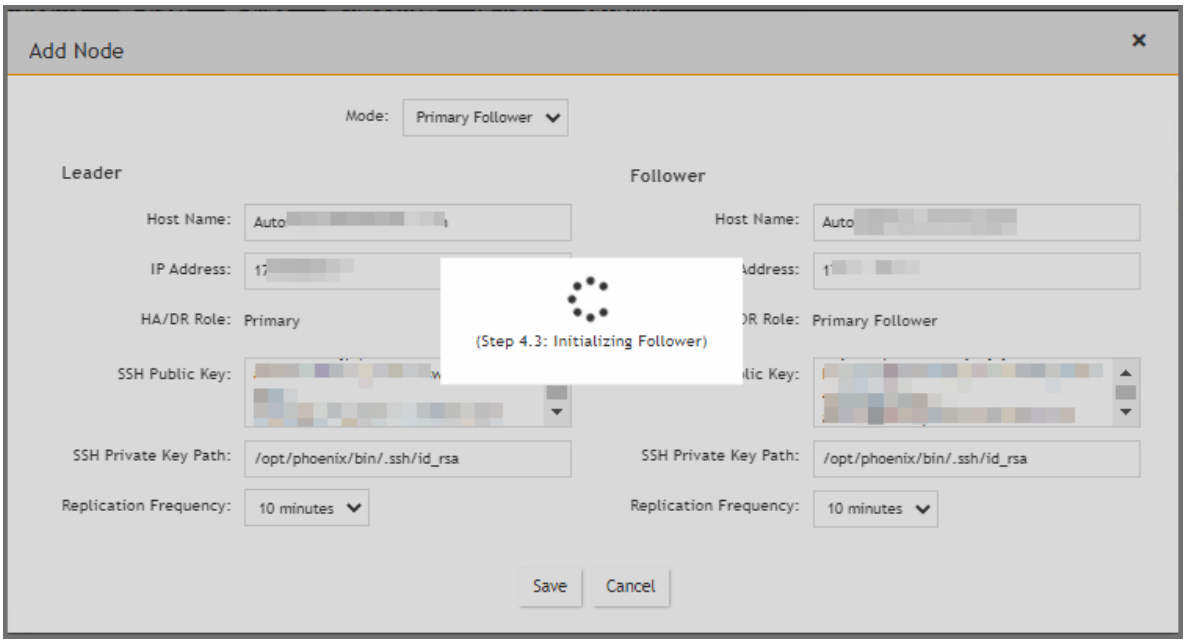
Configuration

Note that the Primary Follower node will be added to the end of linked list of currently configured Supervisors. For example, if you currently have only one Supervisor node, then the new Follower node will follow the currently installed Supervisor (which is the Leader). If you currently have one Supervisor and one Follower node, e.g. Leader -> Follower1, then the new Follower node will follow the last Follower node, e.g. Leader -> Follower1 -> Follower2.

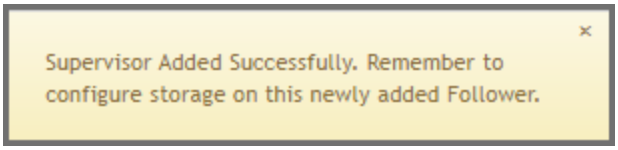
When you add a Follower node via the GUI, FortiSIEM will automatically detect the last Follower node and configure the new node to follow the last Follower node, which can be considered its Leader. The new Follower node needs to get the Profile database and SVN-Lite configuration from the Leader via rsync (using SSH keys). Before you begin to add the Follower node, please obtain its UUID and SSH public key using the information described. See Collecting UUID and SSH Public Key for the steps to acquire this.

To add a Follower node, take the following steps.

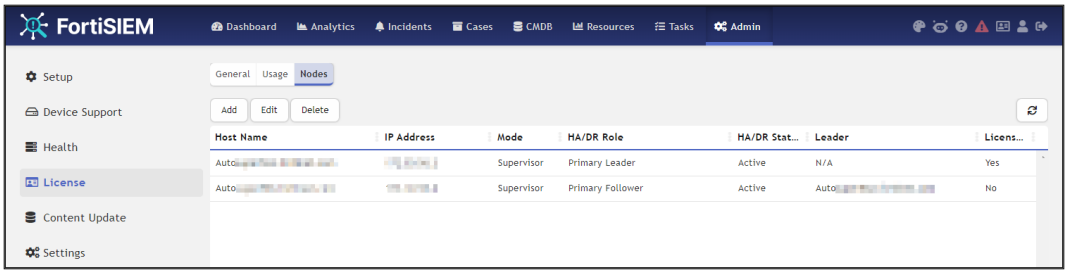
1. Login to GUI and navigate to **ADMIN > License > Nodes**.
2. On the **Add Node** window, in the **Mode** drop-down list, select **Primary Follower**. FortiSIEM will automatically detect the Leader for this new node. The Leader node configuration fields appear in the left column, and the Follower node configuration fields appear in the right column.
3. Under the **Follower** column, enter the following information.
   a. In the **Host Name** field, enter the host name of the Follower node.
   b. In the **IP Address** field, enter the IP of the Follower node.
   c. In the **SSH Public Key** field, enter/paste the SSH Public Key of the Follower node that you obtained earlier.
4. For the **SSH Private Key Path**, enter the following into the field:
   `/opt/phoenix/bin/.ssh/id_rsa`
5. For **Replication Frequency**, select a value indicating how frequently Profile database and SVN-lite files will be rsynced by the Follower node. The default 10 minutes is adequate for most operations.
6. Click **Save**.
   At this point, the Primary Follower is being linked to the Primary Leader. The progress will be displayed in the GUI.



When completed, the message "Supervisor Added Successfully" will appear.



The Follower node will be added in the **ADMIN > License > Nodes** page.



7. If you are running ClickHouse or a Local disk setup, then you need to set up Local disk for the Primary Follower. In these cases, the Primary Follower local disk setup should be identical to that of the Primary Leader. Take the following steps:
   a. Login to GUI and navigate to **ADMIN > Setup > Storage**.
   b. Click **Online** and add a Local disk.
   c. Click **Test**, then **Deploy**.
8. If you have NFS Archive setup, then you need to set up NFS Archive on the Primary Follower. The setup should be identical to that of the Primary Leader. Take the following steps:
   a. Login to GUI and navigate to **ADMIN > Setup > Storage**.
   b. Click **Archive**, choose **NFS** and add the mount point.
   c. Click **Test**, then **Deploy**.
9. If you are running real-time Archive with HDFS, and have added Workers after the real-time Archive has been configured, then you will need to perform a **Test** and **Deploy** for HDFS Archive again from the GUI. This will enable `HDFSMgr` to know about the newly added Workers.

   If you have set up real-time to HDFS, then you need to take the following steps to let HDFSMgr

know about the Primary Follower.

a. Login to GUI.
b. Navigate to **ADMIN > Setup > Storage**.
c. Click **Archive**, and choose **HDFS**.
d. Click **Test**, then **Deploy**.

Load Balancer Setup

1. First set up an external Load Balancer in front of the Active-Active Supervisors. See External Load Balancer Configuration for a sample FortiWeb Load Balancer configuration.
2. Login to GUI and navigate to **ADMIN > Settings > Cluster Config > Supervisors** and add Load Balancer Host Name or IP.

Collecting UUID and SSH Public Key

1. For the UUID, obtain the Hardware ID value through an SSH session by running the following command on FortiSIEM.
   `phLicenseTool --show`
2. Enter/paste the Hardware ID into the UUID field for FortiSIEM.
3. Under Configuration and Profile Replication, generate the SSH Public Key and SSH Private Key Path by entering the following in your SSH session from FortiSIEM:
   ```
   su – admin
   ssh-keygen -t rsa -b 4096
   ```

   Leave the file location as default, and press enter at the passphrase prompt.
   The output will appear similar to the following:

   ```
   Generating public/private rsa key pair.
   Enter file in which to save the key (/opt/phoenix/bin/.ssh/id_rsa):
   Created directory '/opt/phoenix/bin/.ssh'.
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /opt/phoenix/bin/.ssh/id_rsa.
   Your public key has been saved in /opt/phoenix/bin/.ssh/id_rsa.pub.
   The key fingerprint is:
   a9:43:88:d1:ed:b0:99:b5:bb:e7:6d:55:44:dd:3e:48 admin@site1.fsmtesting.com
   The key's randomart image is:
   +--[ RSA 4096]----+
   |      ....|
   |      . .     E. o|
   ```

4. For the SSH Public Key, enter the following command, and copy all of the output.
   `cat /opt/phoenix/bin/.ssh/id_rsa.pub`
5. Exit the admin user in the SSH session by entering the following command.
   `exit`

External Load Balancer Configuration

This section provides guidance on how to configure FortiWEB load balancer to work with FortiSIEM Active-Active Supervisor cluster. Most load balancers can also be used. For additional information on FortiWEB configuration, see the FortiWeb documentation library. The example configuration here assumes FortiWeb will have at a minimum, two interfaces.

Port1: External network / subnet - This is where collector / user traffic connects to.

Port2: Internal network / subnet - This is where appServers and Workers reside.

In this example, VMware interfaces map to FortiWeb virtual interfaces when you deploy OVF

Virtual interface 1 is port1 in FortiWeb - 172.30.57.88/22 .1 GW

Virtual interface 2 is port2 in FortiWeb - 10.65.148.3/22

The default route: 172.30.56.1

The general configuration step are:

- Define Virtual IPs
- Define Virtual Server
- Define Supervisor Health Check
- Define Server Pool
- Define Server Policy
- Define Static Routes in FortiWeb

Define Virtual IPs

1. Navigate to **Network > Virtual IP**.
   This is the Load Balancer IPs.
2. Define one unique free IP in the external subnet for AppServer Load Balancer and Worker Load Balancer
3. Click **Create New**.
4. In the **Name** field, enter a name, for example, " AppServerLB".
5. In the **IPV4 Address** field, enter your IP address. In our example, "172.30.57.89/32".
6. In the **Interface** field, enter/select your port. In our example,"port1".
7. Repeat steps 1 through 7 here in Define Virtual IPs for the Worker Load Balancer, then proceed to Define Virtual Server.

Define Virtual Server

1. Navigate to **Server Objects > Server > Virtual Server**.
2. Click **Create New**.
3. In the **Name** field, enter a name for the virtual server, for example, "AppServer_VS".
4. Click **OK**.

5. Under this setup, click **Create New**.
6. Select the Virtual IP that was created earlier.
7. Click **OK**.
8. In **Status** select **Enable**.
9. Leave other options default, and click **OK**.

Define Supervisor Health Check

1. Navigate to **Server Objects > Server > Health Check**.
2. Click **Create New**.
3. In the **Name** field, enter a name for the Health Check trigger, for example, "AppServerHealthCheck".
4. For **Relationship**, select **And**.
5. Click **OK**.
6. In **Rule List**, click **Create New**.
7. For **Type**, select **TCP SSL** and leave the options as default.
8. Click **OK**.
9. In **Rule List**, click **Create New** again.
10. For **Type**, select **HTTP**.
11. In the **URL Path** field, enter "/phoenix/login.html"
12. For **Method** , select **GET**.
13. For **Match Type**, select **Response Code**.
14. For **Response Code**, enter "200".
15. Click **OK** on each page.

Define Server Pool

1. Navigate to **Server Objects > Server > Server Pool**.
2. Click **Create New**.
3. In the **Name** field, enter a name for the server pool, for example, "AppServerPool".
4. For **Proto** , select **HTTP**.
5. For **Type**, select Reverse Proxy.
6. For **Single Server / Server Balance**, select **Server Balance**.
7. For **Server Health Check**, from the drop-down list, select the server health check you created in Define Supervisor Health Check.
8. For **Load Balancing Algorithm**, from the drop-down list, select **Least Connection** or **Round Robin**.
9. Click **OK**.
10. At the bottom of the page, click **Create New**.
11. For each Server in your server pool, in this example AppServer Pool, do the following.
    a. For **Status**, select **Enable**.
    b. For **Server Type**, select **IP**.
    c. For **IP / Domain**, enter the IP address range, for example, "#.#.#.#/32".

d. For **Port**, enter "443".
e. For **SSL**, check it, but ignore client certificate.
f. Click **OK**.

Define Server Policy

1. Navigate to **Policy > Server Policy**.
2. In the **Name** field, enter a name for the server policy, for example, "AppServerPolicy".
3. For **Deployment Mode**, select **Single Server/Server Balance**.
4. For **Virtual Server**, select the virtual server you created in Define Virtual Server.
5. For **Server Pool**, select the server pool you created in Define Server Pool.
6. For **HTTP Service**, select **HTTP**.
7. For **HTTPS Service**, select **HTTPS**.
8. For **Monitor Mode**, enable it.
9. For **Enable Traffic Log**, enable it.
10. Click **OK**.

Define Static Routes in FortiWeb

For FortiWeb to route non HTTP/HTTPS traffic through FortiWeb, create two policy routes.

1. Navigate to **Network > Route**. (See https://docs.fortinet.com/document/fortiweb/7.0.2/administration-guide/55130/configuring-the-network-settings)
2. Select **Policy Route**.
3. Configure the following rules to allow non HTTP/HTTPS traffic inbound.
   a. For **If traffic matches** Incoming Interface, select your port.
   b. For If traffic matches Source address/mask (IPv4/IPv6), enter the IP range.
   c. For If traffic matches Destination address/mask (IPv4/IPv6), enter the IP range.
   d. For **Force traffic to** Action, select **Stop Policy Routing**.
   e. For **Force traffic to** Priority, enter "200".
   f. Click **OK**.
4. Configure the following rules to allow outbound traffic.
   a. For **If traffic matches** Incoming Interface, select your port.
   b. For If traffic matches Source address/mask (IPv4/IPv6), enter the IP range.
   c. For If traffic matches Destination address/mask (IPv4/IPv6), enter the IP range.
   d. For **Force traffic to** Action, select **Stop Policy Routing**.
   e. For **Force traffic to** Priority, enter "100".
   f. Click **OK**.

For each "AppServerIP" defined in the server pool, a FortiSIEM leader/follower cluster should use those IPs.

Maintenance

The following maintenance topics are available:

- Failover Operations
- Adding a Failed Supervisor back to Cluster
- Checking Cluster Replication Health
- Planned Shutdown Procedures
- Upgrade

Failover Operations

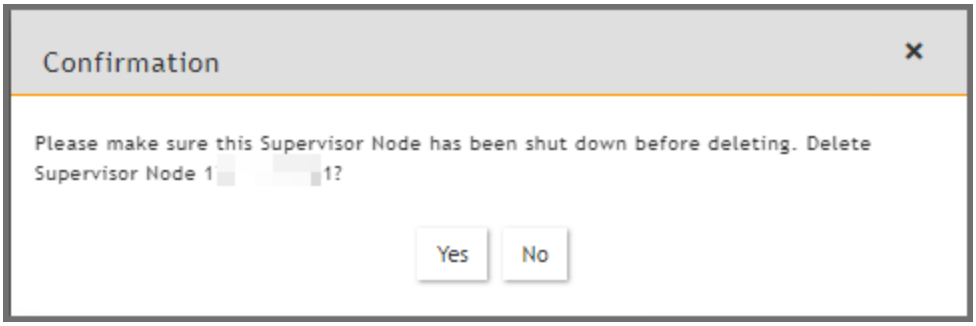
Note that the Supervisors are set up as a linked list: Leader -> Follower1 -> Follower2 -> Follower3...

Case 1: Leader Node Fails

If the Leader node fails, for example, because of a hardware issue, then you need to take the following steps.

Step 1: Promote Follower1 as new Leader by following these steps.

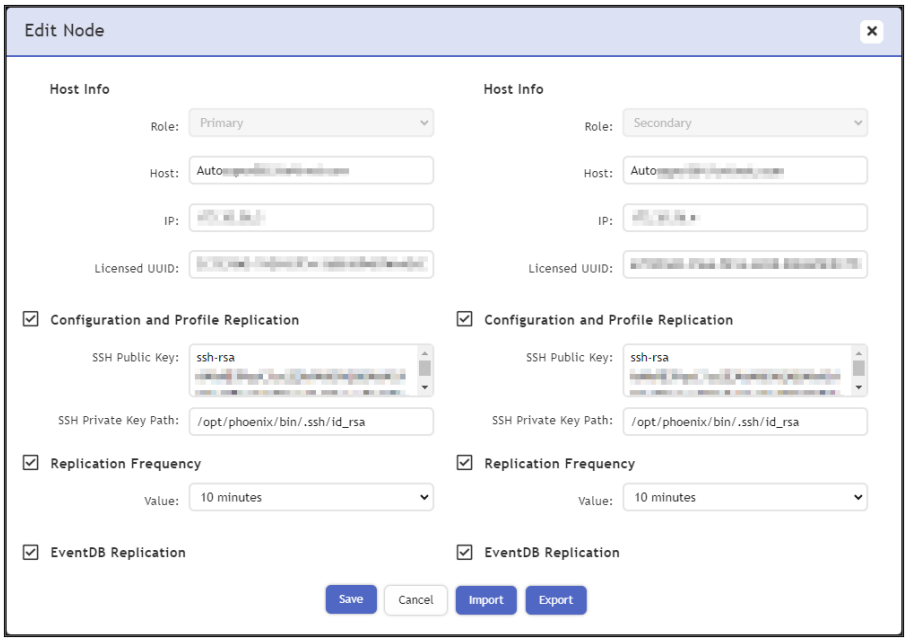
1. SSH to Follower1 and run the following command.
   `phfollower2primary <ownIP>`
   After the script finishes, Follower1 will be the new Leader and the chain becomes: Leader (old Follower1) -> Follower2 -> Follower3
2. Login to GUI. Load Balancer will likely route to any Follower.
3. Navigate to **ADMIN > License > Nodes**.
4. Select the old Leader node and click **Delete**.
5. Click **Yes** to confirm.



Step 2: If Disaster Recovery is enabled, then change Leader for Secondary node.

1. Login to (new Leader) Follower1 GUI.
2. Navigate to **ADMIN > License > Nodes**.
3. Choose Secondary node, and click **Edit**.

4. Enter the (new Leader) Follower1 information in the Primary column.
   a. Change the **Host Name** field to the Follower1 Host Name.
   b. Change the **IP Address** field to the Follower1 IP Address.
   c. DO NOT change the License UUID yet. Do this after you have done a new license with Follower1's UUID in Step 4.4.
   d. Set **SSH Parameters** (SSH Public Key, SSH Private Key Path) to that of Follower1.
   e. Click **Save**.



Step 3: Install a new license with new Leader (Follower1) UUID.

Since the license is tied to failed Leader's UUID, you will repeatedly see a message prompting you to install a new license with new Leader's UUID within a 2 weeks grace period from the time of failure. To resolve this, take the following steps.

1. Login to (new Leader) Follower1 GUI. If you go through Load Balancer, then you may end up in Follower2 GUI which does not allow this operation.
2. Navigate to **ADMIN > License > General**.
3. Click **Upload** and provide the license file with matching (new leader) Follower1's UUID.
   Note: You cannot add new Followers to the system during the 2 weeks grace period when the Primary Leader's UUID does not match the License.

Step 4: If Disaster Recovery is enabled, update Licensed Primary UUID for Secondary node.

1. Login to (new Leader) Follower1 GUI.
2. Navigate to **ADMIN > License > Nodes**.
3. Choose Secondary node and click **Edit**.
4. Update the Licensed UUID for the Primary node.

Case 2: Follower Node Fails

If any follower node fails, take the following steps.

Step 1: Remove the failed Follower node from the Cluster.

1. Login to GUI and navigate to **ADMIN > License > Nodes**.
2. Select the node
3. Click **Delete**.

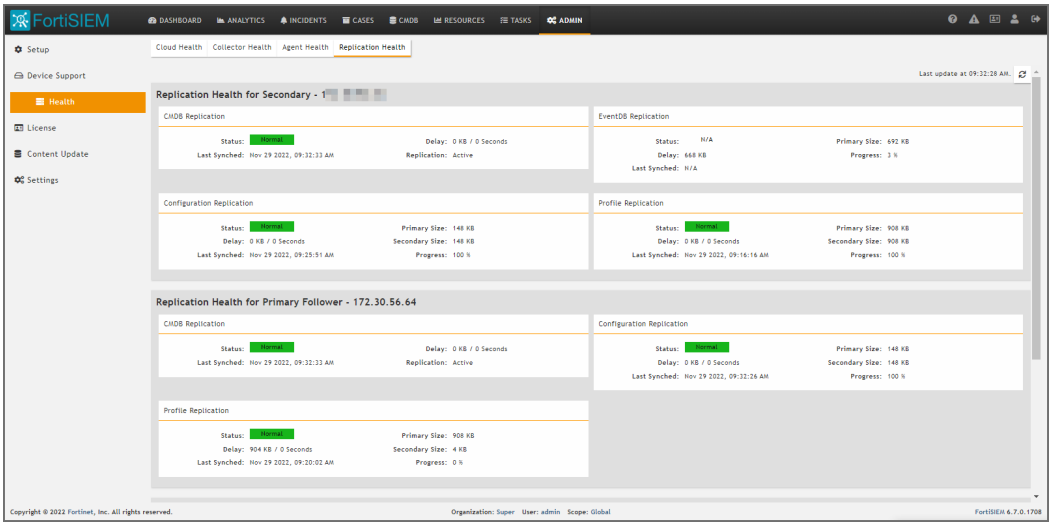
Case 3: Adding a Failed Supervisor back to Cluster

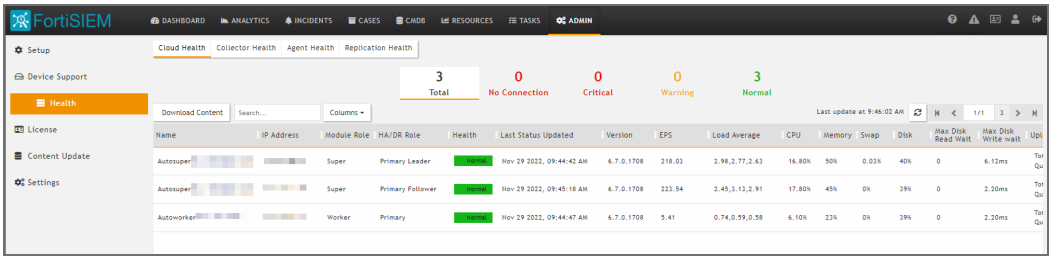
If you want to add a failed Supervisor back to the Cluster, then follow these steps.

1. Navigate to `/opt/phoenix/deployment/jumpbox`.
2. Clean the state data by running the following script, using its own IP.
   `phresetclusternode <myip>`
   Note: After completion, this script will reboot your appliance.
3. Once this appliance is up and running again, if the storage is Local, format the disk if you would like to reuse it, otherwise add a new disk.
4. Add the node as a Follower by following the steps in Adding Primary Follower.

Checking Cluster Replication Health

Cluster Replication health can be viewed in **ADMIN > Health > Replication Health** and **ADMIN > Health > Cloud Health**.





Maintenance Operations

Extra care must be taken to restart or shutdown a Leader node, since it contains the Master PostGreSQL database.

Case 1: Restarting Supervisor Leader

This should be avoided as much as possible, since the Leader contains the Master PostGreSQL database. App Server or any other modules on the Leader can be restarted normally.

1. Check Cluster health to make sure that Leader and Follower health are good and replication is up to date.
2. Make sure users are logged out.
3. Shutdown or Reboot the Leader node.
4. After Leader is up (that is, all processes are up), then users can login to the Leader.
5. Log on to each Follower and restart the App Server process on that node. After the App Server process is up on a Follower, users can log on to the Follower node.

Case 2: Restarting Supervisor Follower

This can be done normally. The user can login to any other Supervisor node. While the Follower node is down, the local PostGreSQL database will fall behind. If the Follower node comes back up within a reasonable time period, then PostGreSQL database replication will catch up and the system will become normal.

Case 3: Restarting a Process on any Supervisor

For any process other than DB Server on the Primary Leader, this can be done normally, and the Cluster should be up and users should be able to login. To restart the DB Server on Primary Leader, follow these steps:

1. Check Cluster health to make sure that Leader and Follower health are good and replication is up to date.
2. Make sure users are logged out.
3. Restart the DB Server on the Leader node.
4. After the DB Server on the Leader is up, restart the App Server. After both App Server and DB Server are up, then users can login to the Leader.
5. Log on to each Follower and restart the App Server process on that node. After the App Server process is up on a Follower, users can log on to the Follower node.

Case 4: Restarting Worker

This can be done normally.

Upgrade

Follow the Upgrade 6.x/7.x Cluster Deployment section from the Upgrade Guide here.

Configuring Disaster Recovery

Configuring Disaster Recovery for ClickHouse

For ClickHouse based deployments, see the following topics from the High Availability and Disaster Recovery - ClickHouse Guide:

General Information: High Availability and Disaster Recovery - ClickHouse

Configuration: Configuring Disaster Recovery

Operation: Disaster Recovery Operations

Configuring Disaster Recovery for Elasticsearch

For Elasticsearch based deployments, see the following topics from the High Availability and Disaster Recovery - Elasticsearch Guide:

General Information: High Availability and Disaster Recovery - Elasticsearch

Configuration: Configuring Disaster Recovery

Operation: Disaster Recovery Operations

Configuring Disaster Recovery for EventDB

For EventDB based deployments, see the following topics from the High Availability and Disaster Recovery - EventDB Guide:

General Information: High Availability and Disaster Recovery - EventDB

Configuration: Configuring Disaster Recovery

Operation: Disaster Recovery Operations

Content Update

The **ADMIN** > **Content Update** page displays the FortiSIEM version that is running and can be used to check if there are available updates. If any updates are available, they can be downloaded and installed. Content Updates must be done in the following order:

1. Upgrade FortiSIEM Supervisor.
2. Upgrade FortiSIEM Worker.

Specific Content Pack Updates information can be found here.

The following topics are available:

- Content Update Notification
- Viewing Content Updates
- Checking for Content Updates
- Viewing Content Update History
- Installing Content Update

Content Update Notification

If a Content Update is available, the following icon will appear in the top header:

Clicking this icon anywhere from the FortiSIEM GUI will redirect the user to the **ADMIN > Content Update** page.

Viewing Content Updates

The current running version is displayed in **Running Version**. Any available versions that can be applied in an update are displayed in **Available Versions**.

The Content Update table provides the following information.

Settings	Description
Version	The version of released content is displayed.
Release Date	The release date of the content is displayed.
Content Description	Information about a content update is provided here.

Checking for Content Updates

To check for any available content updates, click the **Check Now** button. If any content update is available, the **Install** button will be active. If more than one new version is found, then the button name will appear as **Install All**.

Viewing Content Update History

To check your FortiSIEM content update history, take the following steps:

1. Click the **History** button. A **Content Update History** window will appear.
2. Select **Relative** or **Absolute Time**, and input or select the time frame you wish to view.
   Click **OK**.
   The following information is provided, if available.

Settings	Description
Update Time	The time the content update was applied is displayed.
Source IP	The IP address from where the update was downloaded is displayed.
User	The user who performed the update is displayed.
Version	The version of the content update is displayed.

3. When done viewing the information, click **Close**.

Installing Content Update

This section allows you to update content for your Supervisor, Workers and Collectors without needing to update your FortiSIEM version. When the content installation occurs, all new content is pushed to all available nodes (Supervisor, Workers, Collectors).

- Content Update Installation for Supervisor and Workers
- Content Update Installation for Collectors

Content Update Installation for Supervisor and Workers

Install Content Updates for Supervisor and Workers

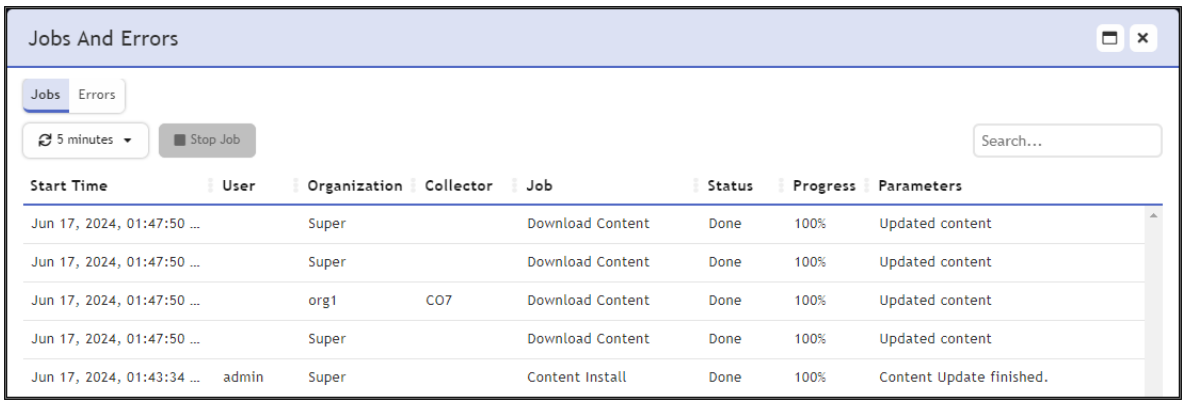
Note: Any changes that have occurred during an installation CANNOT be reverted.

1. Click the **Install** button.
   Note: If more than one update is available an **Install All** button will appear instead. In this situation, click **Install All** to perform all installations.

   A progress bar will appear as installation begins. When the progress bar is complete, the installation is done.

You can also click on the Jobs/Errors icon ( ) and select the **Jobs** tab to view the progress of the content installation. When the **Status** column shows "Done", and **Progress** column is "100%", installation for the Supervisor and Workers is complete.

Example: The Supervisor and Worker content update (The first and second lines) are shown as "Done".



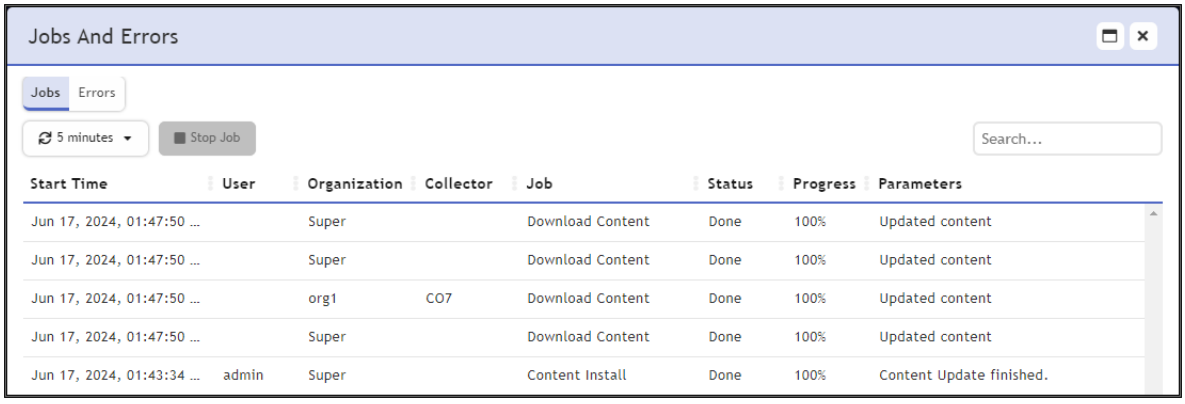
If you register/power on any Collector after the Supervisor has had a Content Update, then proceed to Content Update Installation for Collectors.

Note: You can click **Abort** to stop the installation.

Content Update Installation for Collectors

Install Content Updates to Collectors

1. Navigate to **ADMIN > Health > Collector Health**.
2. Click on the **Action** drop-down list and select **Download Content**.
   Click on the Jobs/Errors icon ( ) and select the **Jobs** tab to view the progress of the content installation. When the **Status** column shows "Done", and **Progress** column is "100%", for the Collector job, the content update is complete.
   Example: The third line shows the Collector Content Update as "Done" for Collector CO7.



Settings

This section contains information on monitoring the health of your FortiSIEM deployment, general system settings such as language, date format, and system logos, and how to add devices to a maintenance calendar.

- System Settings
  - UI Settings
  - Email Settings
  - Image Server Settings
  - Cluster Config
  - Event Worker Settings
  - Query Worker Settings
  - Lookup Settings
  - Kafka Settings
  - Dashboard Slideshow Settings
  - Dashboard Ownership
  - PAYG Report
  - Trusted Hosts
- Analytics Settings
  - Scheduled Reports
  - Incident Notification
  - Setting a Subcategory
  - Setting Risk Filters
  - UEBA Higher Risk Entities
  - UEBA Tags
  - Tags
  - ML / AI
- Discovery Settings
  - Generic
  - Device Filter
  - Application Filter
  - Location
  - CMDB Groups
- Monitoring Settings
  - Important Processes
  - Important Ports
  - Important Interfaces
  - Excluded Disks
  - Windows WMI Filter

- Event Handling Settings
  - Event Dropping
  - Event Forwarding
  - Event Organization Mapping
  - Multiline Syslog
- Event Database Settings
  - Creating Retention Policy
  - Viewing Online Event Data
  - Viewing Archive Event Data
  - Validating Event Log Integrity
  - ClickHouse Configuration
- Role Settings
  - Mapping AD Groups to Roles
- Compliance Settings
  - PCI
- General Settings
  - External Authentication Settings
  - Automation Policy Settings
  - External System Integration Settings
  - Configuring SSL Socket Certificates
  - Case Management Settings

System Settings

The following section describes the procedures for system settings:

- UI Settings
- Email Settings
- Image Server Settings
- Cluster Config
- Lookup Settings
- Kafka Settings
- Dashboard Slideshow Settings
- Dashboard Ownership
- PAYG Report
- Trusted Hosts
- FortiGuard Proxy
- FQDN

UI Settings

There are two locations where you can change UI settings in FortiSIEM. One location is in the user profile. The other is in the administrator settings.

- User Profile UI Settings
- Administrator UI Settings

User Profile UI Settings

The initial view of FortiSIEM UI after login can be configured using the UI settings including dashboard, logos, and theme.

Click the **User Profile** icon ( ) in the upper right corner of the UI. The dialog box contains three tabs:

Basic - Use the **Basic** tab to change your password into the system.

Contact - Use the **Contact** tab to enter your contact information.

UI Settings - Use the **UI Settings** tab to set the following:

Settings	Guidelines
Home	Select the tab which opens when you log in to the FortiSIEM UI.
Incident Home	Select the Overview, List (by Time, by Device, by Incident), Risk, Explorer, or MITRE ATT&CK ICS or IT (Rule Coverage, Incident Coverage, Incident Explorer) display for the **INCIDENTS** tab.
Dashboard Home	Select the Dashboard to open by default under the **DASHBOARD** tab from this drop-down list.
Dashboard Settings	Select the type of dashboards to be visible/hidden using the left/right arrows. The up/down arrows can be used to sort the Dashboards.
Language	Specify which language will be used for the UI display. Many UI items have been translated into the languages in the drop-down list, including buttons, labels, top-level headings, and breadcrumbs. Items that are data-driven are not translated.
Theme	Select Dark or Light theme for FortiSIEM UI. Save and refresh the browser to view the change.
Date Format	Select one of the following formats for displaying date and time information. • Local/Simple Date Format - Display the time in AM/PM format. • ISO 8601 - Display the date and time in ISO 8601 format, the International Standards Organization's standard for date and time representation. • UTC - Display the date and time in Coordinated Universal Time (UTC).

When done configuring, click **Save**.

Note: All of the above settings will take effect when you log in again or when you refresh the browser in the same login session.

Administrator UI Settings

Click **ADMIN > Settings > System > UI** to access the administrator UI settings.

FortiSIEM only accepts SVG format for Report Logo. All other image formats must be converted to SVG format first.

The following site can be used to help convert PNG/JPG/GIF into SVG: https://onlineconvertfree.com/convert/svg/

Settings	Guidelines
UI Logo	Click the edit icon to enter the path to the image file for the logo that will be used in the UI. UI Logo image file must be in .PNG format.
Report Logo	Click the edit icon to enter the path to the image file for the logo that will be used in reports. Report Logo image file must be in .SVG format.
Google Maps API Key	Click the edit icon to enter the API key to access Google Maps.
Lockout Users	In the number of days field, enter the number of inactive days required before a user is automatically locked out.
Login Banner	Administrators can choose a login banner to display to users after login. Click the **Enabled** checkbox to display a login banner. In the field below **Login Banner**, enter the text that you want to appear. Some simple BBCode tags are allowed in this message input: “b” - bold “i” - italic “u” - underline “url” - url HTML tags are not allowed. Nested tags are not allowed. When done, click **Save**. In addition to the banner, the user will see the following: • Last login time and IP address location • Changes to the account (if any) since last login. This includes whether the user was assigned a new role for any organization, or if a role definition has changed. Changes appear in the next login. This is a global setting for all users.

Email Settings

The system can be configured to send email as an incident notification action or send scheduled reports. Use these fields to specify outbound email server settings.

Complete these steps to customize email settings:

1. Go to **ADMIN** > **Settings** > **System** > **Email** tab.
2. Enter the following information under **Email Settings**:

Settings	Guidelines
Email Gateway Server	[Required] Holds the gateway server used for email.
Server Port	Port used by the gateway server.
Secure Connection (TLS)	Protocol used by the gateway server. This can be Exchange or SMTP.
Server Account ID	[Required] The account name for the gateway.
Default Email Sender	Default email address of the sender.
Authentication	Select **Basic** or **OAuth**. If **Basic** is selected, the following field must be configured. • **Account password** - Enter the password for the account. If **OAuth** is selected, the following fields must be configured. • **OAuth Provider** - Select the OAuth Provider from the drop-down list. • **Client ID** - Enter the Client ID for OAuth. • **Client Secret** - Enter the Client Secret associated with the Client ID. After OAuth configuration, click **Re-authenticate** to confirm authentication settings.
Enable S/MIME	Add a check mark to enable Secure/Multipurpose Internet Mail Extensions (S/MIME) to encrypt your emails. To add a S/MIME certificate, go to **CMDB > Users > Ungrouped**, create or edit a user, select **Contact Info**, ensure the **Email** field is filled out, and upload the certificate in the **Certificate** field.
Send Without Key	If this option is selected, then email is sent to a user, even if no S/MIME certificate is defined for that user. The email is encrypted with a default certificate and the user cannot read this email. If this option is unselected, then email is not sent to the user without a S/MIME certificate. Therefore, to use the S/MIME option, **certificates must be defined for all users configured to receive email**.

3. Click **Test Email** button to test the new email settings.
4. Click **Save**.

Customizing the Incident Email Template

Use the following procedure to customize the incident email template.

1. Click **New** under the section **Incident Email Template**.
2. Enter the **Name** of the template.
3. Select the **Organization** from the list.

4. Enter the **Email Subject**. You can also choose the incident attribute variables from **Insert Content** drop-down as part of Email Subject.
5. Enter the **Email Body** by selecting the attribute variables from **Insert Content** drop-down into your template, rather than typing. If required, enable **Support HTML** for HTML content support.

Incident Attribute	Description
Affected Business Service	Comma separated list of all business services to which Incident Source, Incident Target or Reporting Device belongs
Device Annotation	Annotation for the device in Incident Target – set in CMDB
Device Description	Description for the device in Incident Target – set in CMDB
Device Location	Location for the device in Incident Target – set in CMDB
First Seen Time	First time the incident occurred
Host Name	Host Name from Incident Target. If not found then gathered from Incident Source
Identity	Identity and Location for Incident Source
Incident Category	Security, Performance, Availability or Change
Incident Cleared Reason	Value set by user when clearing a rule
Incident Comments	Comments inputted by user for Incident
Incident Count	Number of times the same incident has happened with the same group by parameters
Incident Detail	Any group by attribute in an Incident other than those in Incident Source and Incident Target
Incident ID	Incident ID – assigned by FortiSIEM and is unique – this attribute has an URL which takes user to this incident after login
Incident ID Without Link	Incident ID – assigned by FortiSIEM and is unique – this attribute does not have an URL
Incident Resolution	None, True Positive, False Positive
Incident Severity	A number from 0-10
Incident Severity Category	HIGH (9-10), MEDIUM (5-8) and LOW (1-4)
Incident Source	Source IP, Source Name in an Incident
Incident Sub Category	Specific for each category – as set in the Rule definition
Incident Tactics	MITRE ATT&CK® tactic(s) involved with incident

Incident Attribute	Description
Incident Tag	Rule tag linked to Incident
Incident Target	Destination IP, Destination Host Name, Host IP, Host Name, User in an Incident
Incident Technique	MITRE ATT&CK® technique involved with incident
Incident Time	Time incident occurred
Incident Title	A system default title or a user-defined title for an incident.
Last Seen Time	Last time the incident occurred
Notify Policy ID	Automation Policy ID that triggered this email notification
Organization	Organization to which this Incident belongs.
Raw Events	Triggering events in raw format as sent by the device (up to 10)
Rule Description	Rule Description
Rule Name	Rule Name
Rule Remediation Note	Remediation note defined for each rule
Status	Incident Status – Active (0), Auto Cleared (1), Manually Cleared (2), System Cleared (3)
Triggering Attributes	List of attributes that trigger a rule – found in Rule > Sub pattern > Aggregate

6. Click **Preview** to preview the email template.
7. Click **Save** to apply the changes.

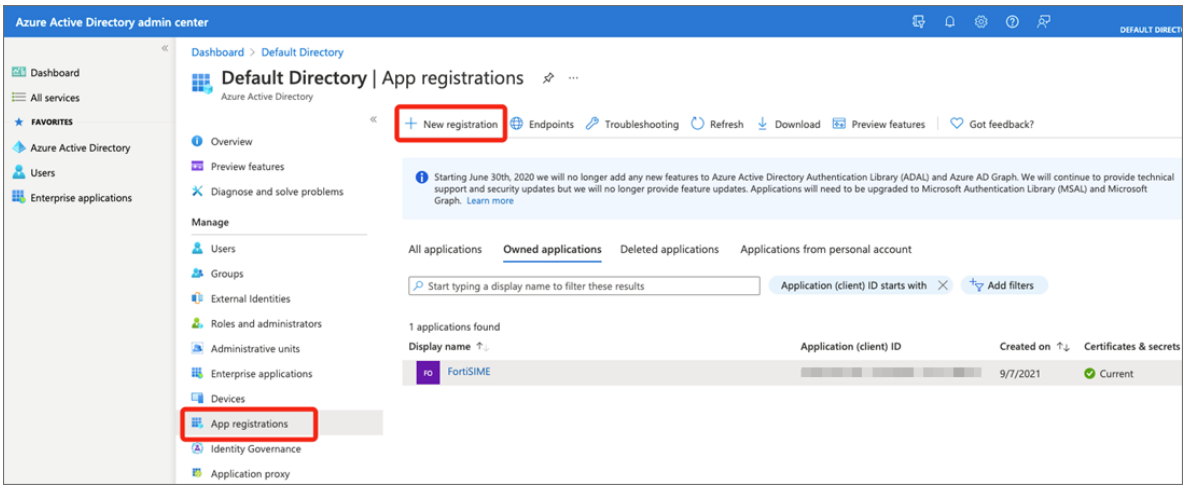
To set an email template as default, select the template in the list, and then click **Set as Default**. When you are creating an automation policy and must select an email template, if you leave the option blank, the default template will be used. For Service Provider deployments, to select a template as default for an Organization, first select the Organization, then set the default email template for that organization.

Example Registering FortiSIEM with Azure via OAUTH

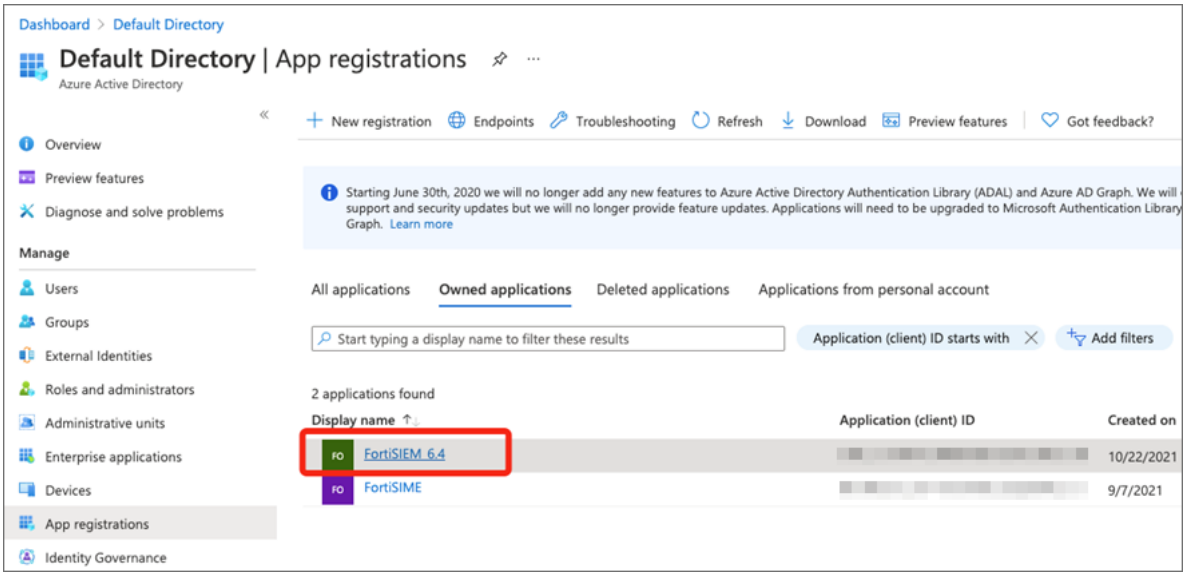
Here is an example of registering FortiSIEM to use Azure email server via OAUTH.

1. Login to Microsoft 365.
2. Go to **App registrations**.

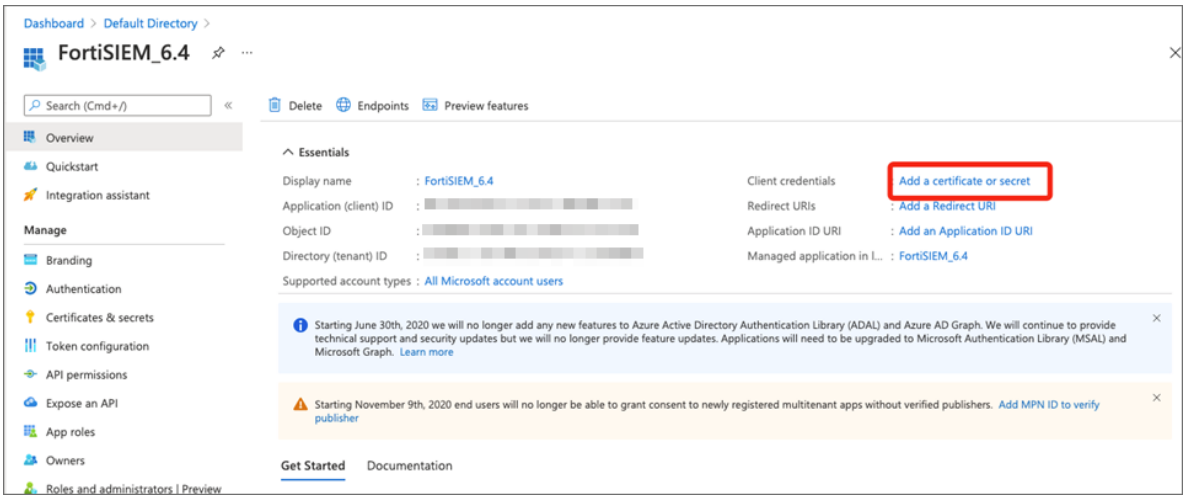
3. Click **+ New registration**.



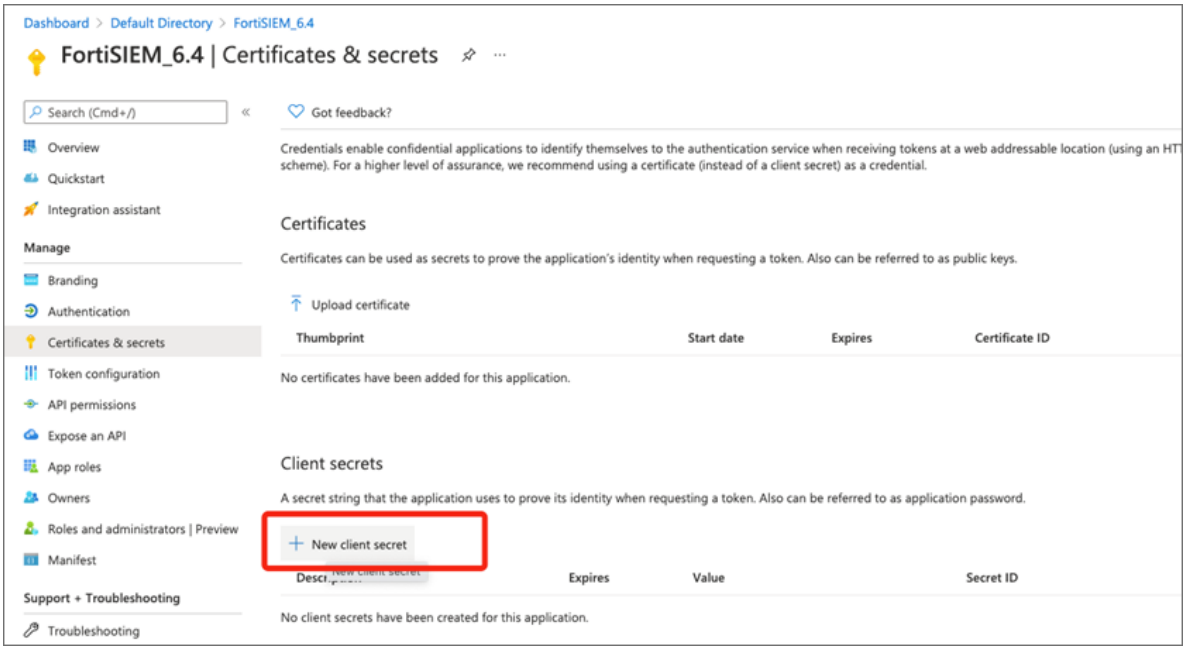
4. In the **Name** field, enter a name, such as "FortiSIEM", and choose an account type.
5. Under **Owned applications**, select your FortiSIEM application.



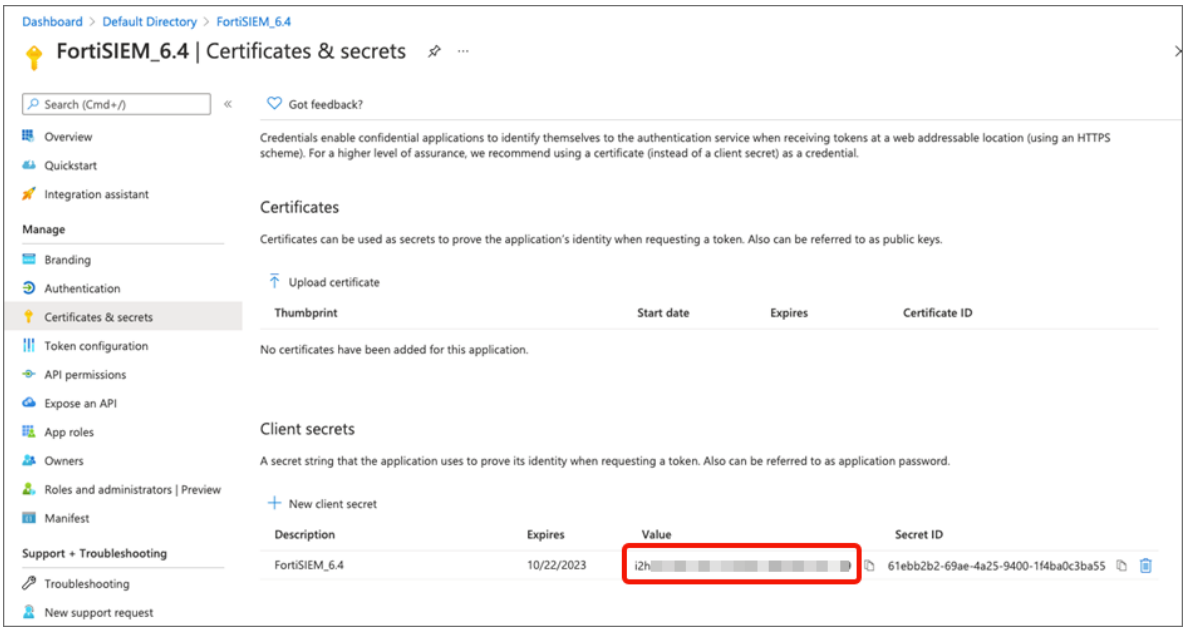
6. On the App registration page for your app, make note of the **Application (client) ID** for your FortiSIEM configuration. Then, at **Client credentials**, click **Add a certificate or secret**.



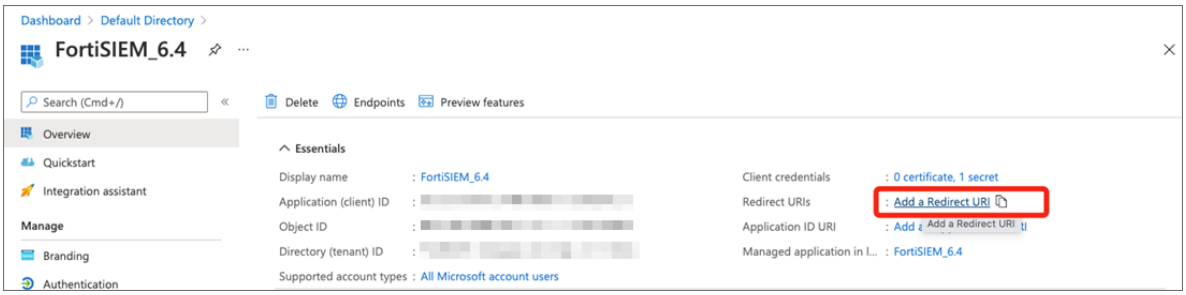
7. Under **Client secrets**, click **+ New client secret**.



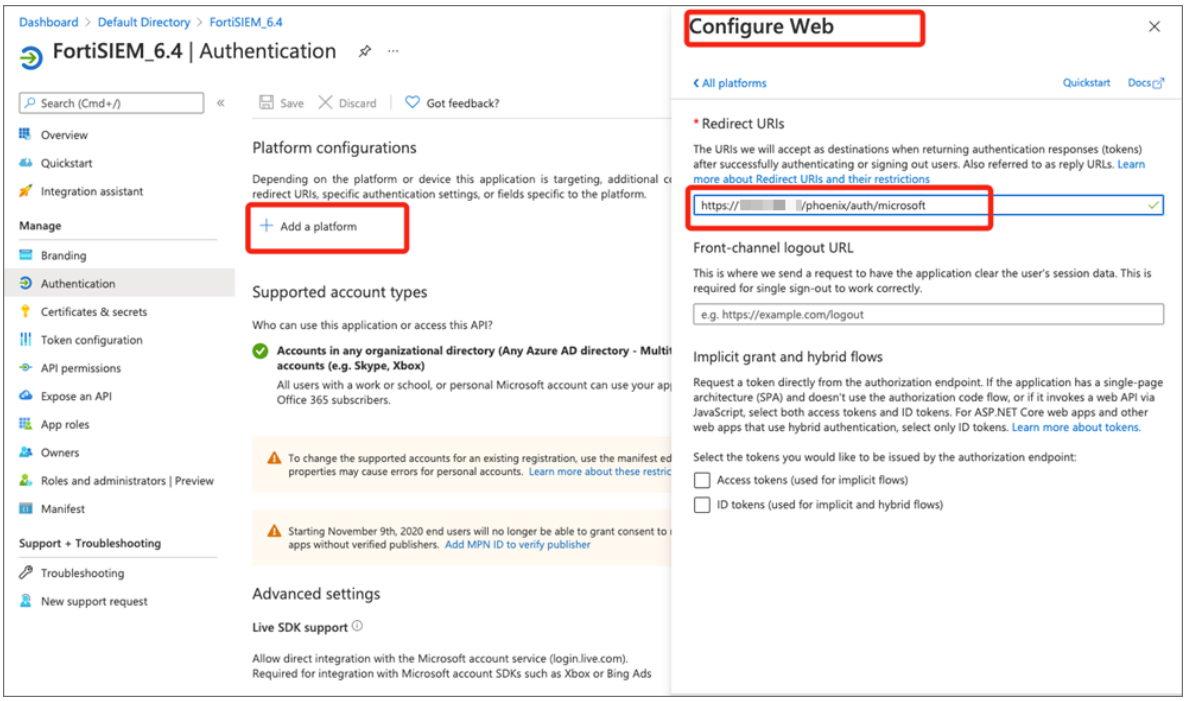
8. Copy the value from the **Value** column. This is your Client Secret for authentication.



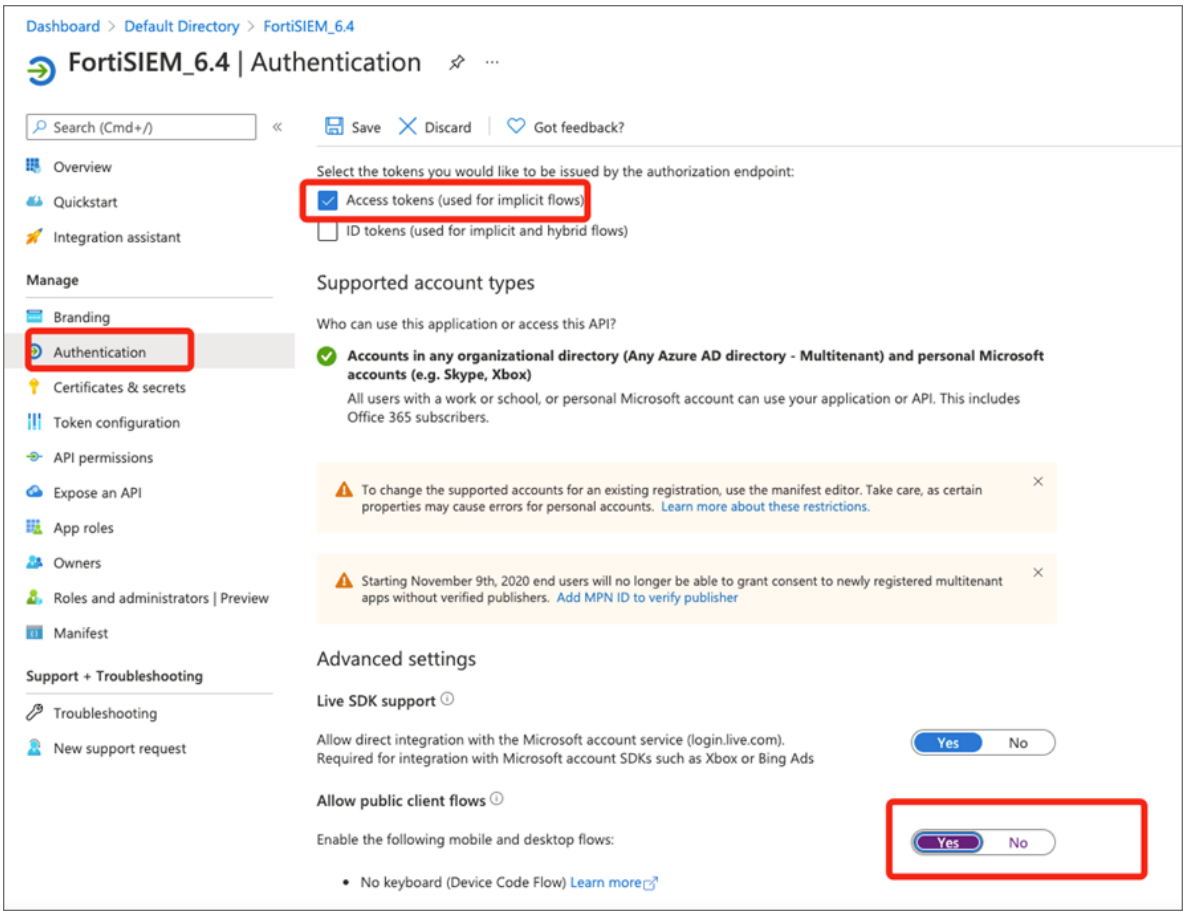
9. At **Redirect URIs**, click **Add a Redirect URI**.



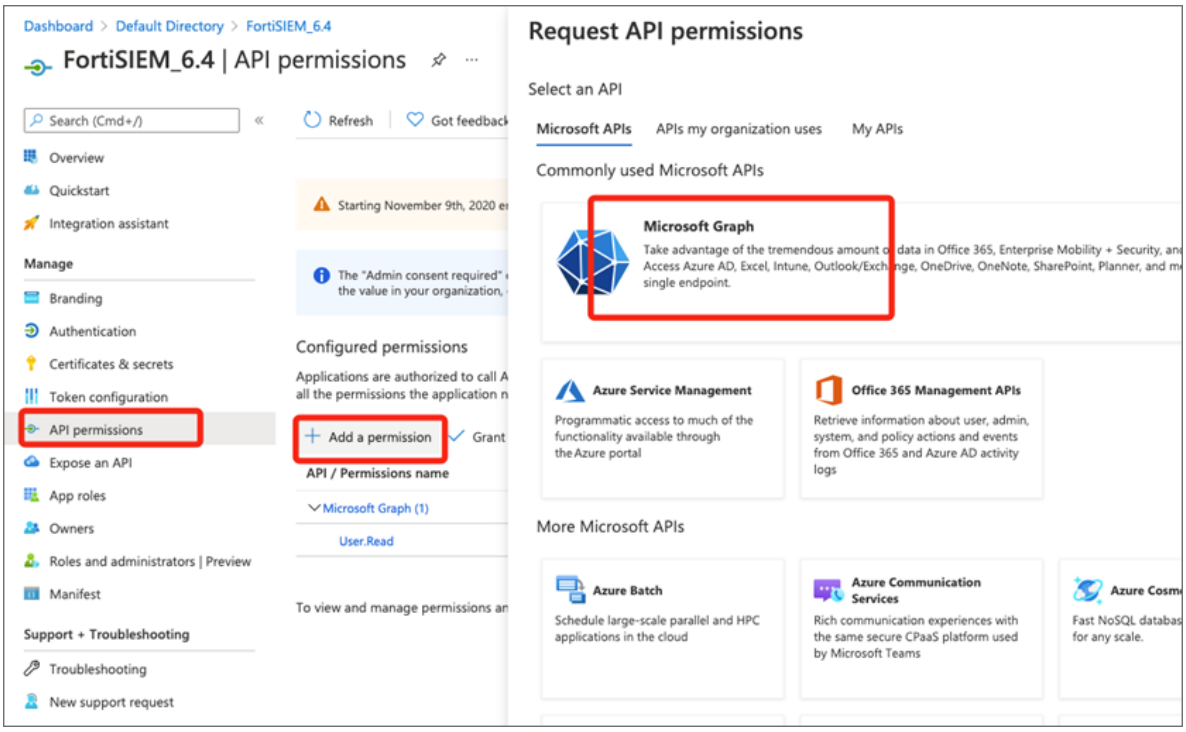
10. Under **Platform configurations**, click **+ Add a platform**.
11. Click **Web**.
12. In the **Redirect URIs** section, enter/paste the URI, which is your FortiSIEM Supervisor IP or host name.



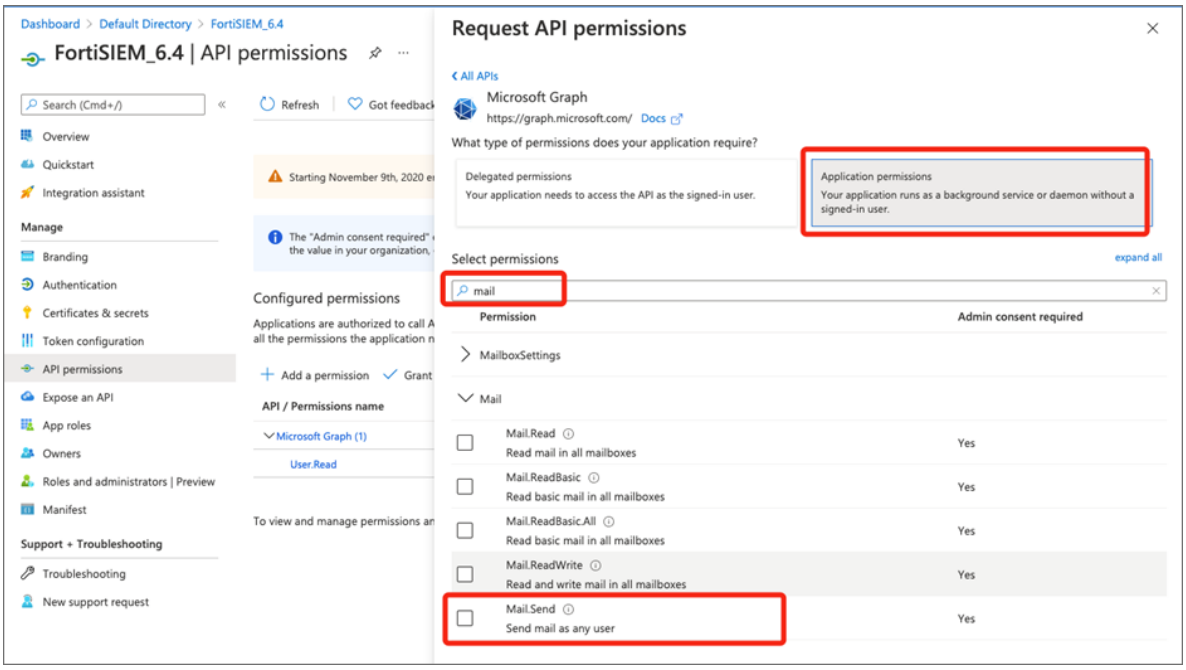
13. In the left pane, navigate to **Manage > Authentication**.
14. Configure the two following Authentication settings:
    - **Access tokens (used for implicit flows)** checkbox must be checked.
    - Under **Advanced settings**, **Allow public client flows** must be set to **Yes**.



15. Navigate to **Manage > API permissions**.
16. Under **Configured permissions**, click **+ Add a permission**.
17. From the **Request API permissions** pane, select the **Microsoft APIs** tab, and click **Microsoft Graph**.

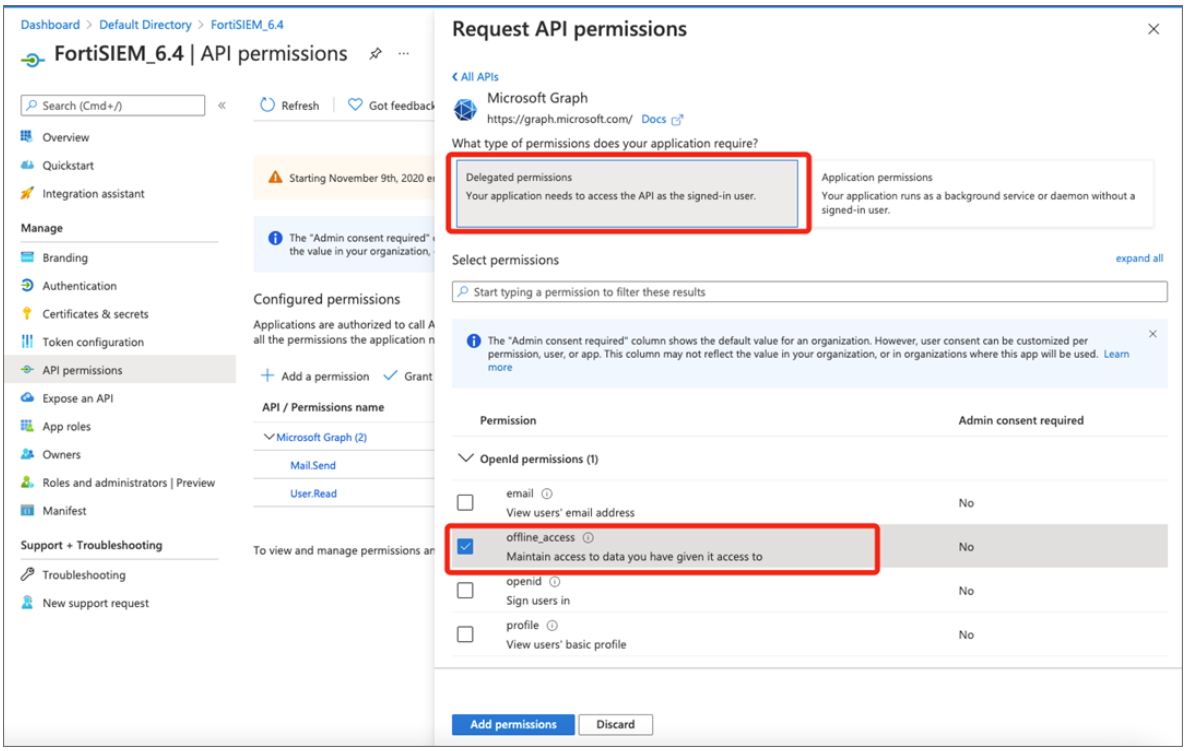


18. Under **What type of permissions does your application require?** select **Application permissions**.
19. In the **Select permissions** search field, enter "mail".
20. From the **Permission** column, expand **Mail**, and configure Mail.Send (Send mail as any user) so **Admin consent required** is set to **Yes**.



21. Now, under **Microsoft Graph > What type of permissions does your application require?** select **Delegated permissions**.
22. Under the **Permission** column, expand **OpenId permissions**.

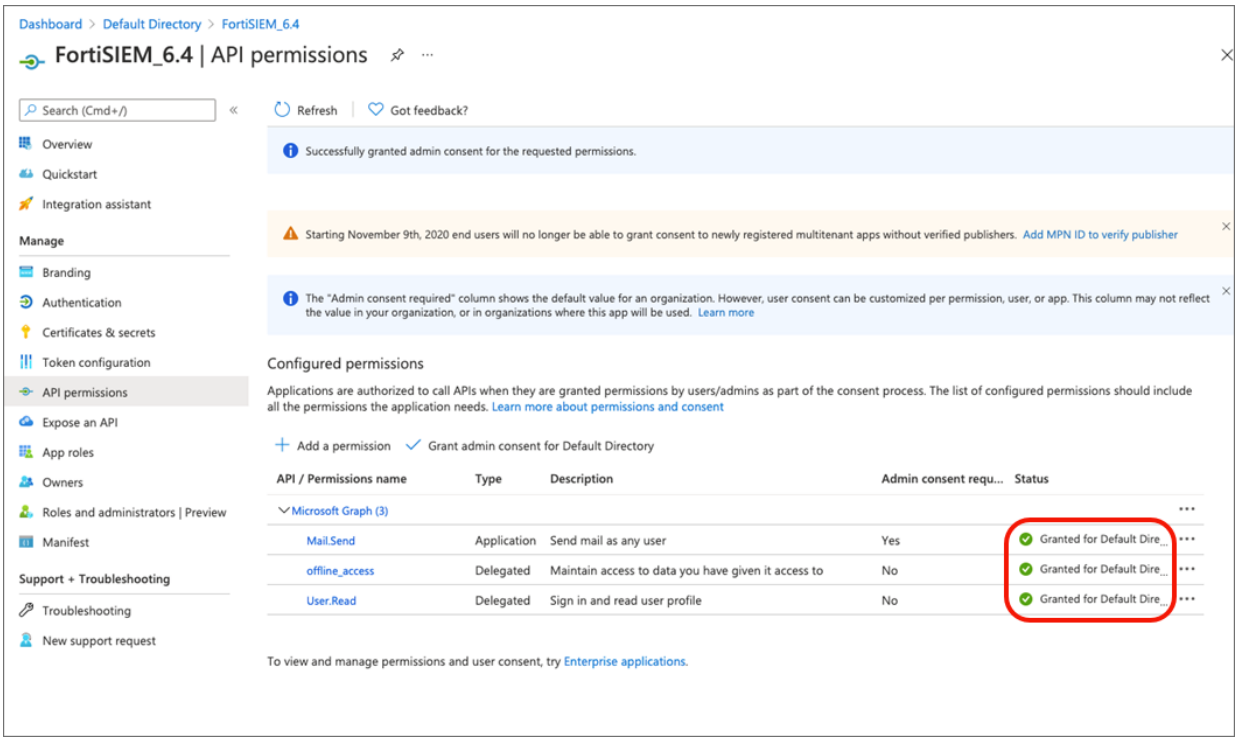
23. Click the **offline_access** checkbox so that **offline_access** is checked.



24. Under **Configured permissions**, click **Grant admin consent for Default Directory**.

Check the **Status** column. The following permissions should be granted.

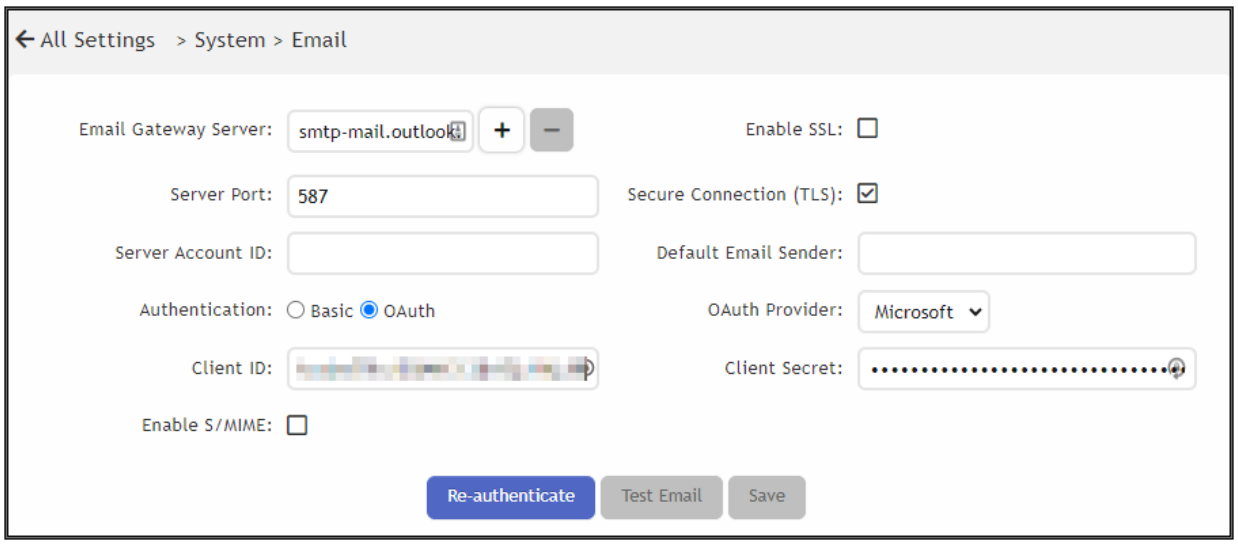
- Mail.Send
- offline_access
- User.Read



On FortiSIEM, take the following steps:

1. Navigate to **Admin > Settings > System > Email**.
2. In the **Email Gateway Server** field, enter the IP address/host name of your email gateway server.
3. In the **Server Port** field, enter the Server Port number.
4. In the **Server Account ID** field, enter the server account ID.
5. For **Authentication**, select **OAuth**.
6. In the **OAuth** drop-down list, select **Microsoft**.
7. In the **Client ID** field, enter/paste the Application (Client) ID of the App from Step 6 in Example Registering FortiSIEM with Azure via OAUTH.
8. In the **Client Secret** field, enter/paste the value from Step 8 in Example Registering FortiSIEM with Azure via OAUTH.
9. Click **Re-authenticate**, **Test Email** then **Save**.

Your OAuth settings should look similar to the following in FortiSIEM.



If you still receive a "SendAs" in "SendAsDeniedException" error, you may need to go to your Office365 account and configure "Send email on behalf of another user". This error occurs if the email address used for authentication is different than the FROM email address. The solution is to update your Office365 account settings to allow for sending on behalf of the FROM email address.

Image Server Settings

This section allows you to set up the Supervisor as an Image Server for upgrading Collectors and Agents. This mechanism provides an easy way to upgrade a large number of Collectors and Agents from one place.

- Upgrading Collectors
- Upgrading Linux Agents
- Upgrading Windows Agents
- Custom Update

Upgrading Collectors

Step 1: Download the Correct Collector Image from the Fortinet Support Site into your Workstation

As an example, Collector 6.4.0 image file name is `FSM_Upgrade_All_6.4.0_build1412.zip` and matches the hash in the support site to the locally computed hash. This ensures that the file has not been corrupted in transit.

Step 2: Upload the Image to the Supervisor Node

Note: In this step, you will upload the image to the Supervisor, which will then internally create a URL for the Collectors to download the image. It is critical to set the host name in the URL correctly so that a Collector can resolve the host name. Otherwise, the image download in Step 3 will fail.

There are two solutions.

Solution 1	By default, the Supervisor's host name in **ADMIN > License > Nodes** is used to create the URL. If the host name is a Fully Qualified domain name and is resolvable by the Collectors, then there is nothing to do. For example, a host name like `c2-52-35-20-68.us-west-2.compute.amazonaws.com` is resolvable to an external IP address. A host name like `2-52-35-20-68.us-west-2.compute` is likely not resolvable.
	If the hostname is not resolvable, either create a DNS entry to allow the Collector to resolve the hostname, or add an entry to the Collector `/etc/hosts` file in the following format:
	`<ip> <host name>`
	For example:
	`10.0.1.21 2-52-35-20-68.us-west-2.compute`

Solution 2	If there is a load balancer in front of the Supervisors, or you want to override the Supervisor host name in the default image download URL, then you can enter the appropriate host name or IP after going to **ADMIN > Settings > Systems > Image Server > Custom Update** and then clicking **Save**. If you have entered a host name here, make sure that it is a Fully Qualified domain name and is resolvable by Collectors. Do this step first before proceeding to the remaining of Step 2. Note that if you create an entry in Custom Update, then it applies to ALL Collectors and Agents. This means that every Collector and Agent will get the URL with the Custom Update entry.

1. Go to **ADMIN > Settings > Systems > Image Server**.
2. Under **Collector**, in the **Version** field, enter the version you downloaded in Step 1. The format is #.#.#. Example: 6.4.0.
3. Under **Collector**, click **Select File** and select the Collector upgrade image you downloaded in Step 1.
4. Under **Collector**, click **Upload File** to upload the Collector upgrade image to the Supervisor. This may take a while depending on the network connection between your workstation and Supervisor node. FortiSIEM will validate the image hash and upload the image to Supervisor if the hash matches.
5. Run the following SQL and make sure ImageSetup task is completed.

```
# psql phoenixdb phoenix -c "select type, progress from ph_task where type =
'ImageSetup'"
    type | progress
------------+----------
 ImageSetup | 100
 ImageSetup | 100
 ImageSetup | 100
(3 rows)
```

Step 3: Download the Image to the Collector

1. Go to **ADMIN > Health > Collector Health**.
2. From the **Columns** drop-down list, ensure **Download Status** is selected. If not, select it so the **Download Status** column is displayed.
3. Select the Collector(s) you wish to download the image to.
   Note: Starting with release 6.4.0, you can choose multiple Collectors for downloading images.
4. From the **Action** drop-down list, select **Download Image**.
5. Check that the **Download Status** column shows **finished** to confirm that the download has been completed for the selected Collectors.

Step 4: Upgrade the Collector

1. Go to **ADMIN > Health > Collector Health**.
2. From the **Columns** drop-down list, ensure **Version** is selected. If not, select it so the **Version** column is displayed.
3. Select the Collector(s) you wish to upgrade.
   Note: Starting with release 6.4.0, you can choose multiple Collectors for installing images.
4. From the **Action** drop-down list, select **Install Image**.
5. Check that the **Version** column shows the correct version number, in this example 6.4.0, to confirm that the Collector(s) have upgraded successfully.

Upgrading Linux Agents

Step 1: Download the Correct Linux Agent Image from the Fortinet Support Site into your Workstation.

As an example, a Linux Agents 6.4.0 image file name is `fortisiem-linux-agent-installer-6.4.0.1412.sh` and matches the hash in the support site to the locally computed hash. This ensures that the file has not been corrupted in transit.

Step 2: Upload the Image to the Supervisor Node

Note: In this step, you will upload the image to the Supervisor, which will then internally create a URL for the Agents to download the image. It is critical to set the host name in the URL correctly, so that an Agent can resolve the host name. Otherwise, the image download in Step 3 will fail.

There are two solutions.

Solution 1	By default, the Supervisor host name in **ADMIN > License > Nodes** is used to create the URL. If the host name is a Fully Qualified domain name and is resolvable by the Agents, then there is nothing to do. For example, a host name like `c2-52-35-20-68.us-west-2.compute.amazonaws.com` is resolvable to an external IP address. A host name like `2-52-35-20-68.us-west-2.compute` is likely not resolvable.
Solution 2	If there is a load balancer in front of the Supervisors, or you want to override the Supervisor host name in the default image download URL, then you can enter the appropriate host name or IP after navigating to **ADMIN > Settings > Systems > Image Server > Custom Update**, and then clicking **Save**. If you have entered a host name here, make sure that it is a Fully Qualified domain name and is resolvable by Agent. Do this step first before proceeding to the remaining of Step 2. Note that if you create an entry in Custom Update, then it applies to ALL Collectors and Agents. This means that every Collector and Agent will the get the URL with the Custom Update entry.

1. Go to **ADMIN > Settings > Systems > Image Server**.
2. Under **Linux Agent**, in the **Version** field, enter the version you downloaded in Step 1. The format is #.#.#. Example: 6.4.0.
3. Under **Linux Agent**, click **Select File** and select the Linux Agent upgrade image you downloaded in Step 1.
4. Under **Linux Agent**, click **Upload File** to upload the Linux Agent upgrade image to the Supervisor. This may take a while depending on the network connection between your workstation and Supervisor node. FortiSIEM will validate the image hash and upload the image to Supervisor if the hash matches.

Step 3: Download the Image to the Linux Agent

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Upgrade Status** is selected. If not, select it so the **Upgrade Status** column is displayed.
3. Select the Linux Agent(s) you wish to download the image to.
   Note: Starting with release 6.4.0, you can choose multiple Linux Agents for downloading images.
4. From the **Action** drop-down list, select **Download Image**.
5. Check that the **Upgrade Status** column shows **Download Succeeded** to confirm that the download has been completed for the selected Linux Agents.

Step 4: Upgrade the Linux Agents

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Version** is selected. If not, select it so the **Version** column is displayed.
3. Select the Linux Agent(s) you wish to upgrade.
   Note: Starting with release 6.4.0, you can choose multiple Linux Agents for installing images.
4. From the **Action** drop-down list, select **Install Image**.
5. Check that the **Upgrade Status** column shows **Upgrade Succeeded** to confirm that the Linux Agent(s) have upgraded successfully. Check that the **Version** column shows the correct version number, in this example 6.4.0, to confirm that the Linux Agent(s) have upgraded to the correct version.

Upgrading Windows Agents

Step 1: Download the Correct Windows Agent Images from the Fortinet Support Site into your Workstation.

1. Download the image file into your desktop. It is a .zip file, e.g. `FSMLogAgent-v4.2.1-build0225.zip`.
2. Compute the MD5 checksum and make sure that locally, the computed checksum matches the checksum in the Support Site. This ensures that the file is not corrupted in transit.
3. Unzip the file. You will see that there are two files – `AutoUpdate.exe` and `FSMLogAgent.exe`. You will need to upload these files in Step 2.3 and Step 2.4 below.

Step 2: Upload the Image to the Supervisor Node

Note: In this step, you will upload the image to the Supervisor, which will then internally create a URL for the Agents to download the image. It is critical to set the host name in the URL correctly, so that an Agent can resolve the host name. Otherwise, the image download in Step 3 will fail.

There are two solutions.

Solution 1	By default, the Supervisor host name in **ADMIN > License > Nodes** is used to create the URL. If the host name is a Fully Qualified domain name and is resolvable by the Agents, then there is nothing to do. For example, a host name like `c2-52-35-20-68.us-west-2.compute.amazonaws.com` is resolvable to an external IP address. A host name like `2-52-35-20-68.us-west-2.compute` is likely not resolvable.
Solution 2	If there is a load balancer in front of the Supervisors or you want to override the Supervisor host name in the default image download URL, then you can enter the appropriate host name or IP after going to **ADMIN > Settings > Systems > Image Server > Custom Update**, then clicking **Save**. If you have entered a host name here, make sure that it is a Fully Qualified domain name and is resolvable by Agent. Do this step first before proceeding to the remaining of Step 2. Note that if you create an entry in Custom Update, then it applies to ALL Collectors and Agents. This means that every Collector and Agent will the get the URL with the Custom Update entry.

1. Go to **ADMIN > Settings > Systems > Image Server**.
2. Under **Windows Agent**, in the **Version** field, enter the version you downloaded in Step 1. The format is #.#.#. Example: 4.2.1.
   Note: For Windows Agent, two files are required, the FSMLogAgent executable (FSMLogAgent.exe) and an AutoUpdate executable (AutoUpdate.exe, or AutoUpdate32.exe).
3. Under **Windows Agent**, click **Select File** and select one of the two Windows Agent upgrade image you downloaded in Step 1.
4. Under **Windows Agent**, click **Select File** and select the second Windows Agent upgrade image you downloaded in Step 1.
5. Under **Windows Agent**, click **Upload File** to upload the Windows Agent upgrade images to the Supervisor. This may take a while depending on the network connection between your workstation and Supervisor node. FortiSIEM will validate the image hash and upload the image to Supervisor if the hash matches.

Step 3: Download the Images to the Windows Agent

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Upgrade Status** is selected. If not, select it so the **Upgrade Status** column is displayed.
3. Select the Windows Agent(s) you wish to download the image to.
   Note: Starting with release 6.4.0, you can choose multiple Windows Agents for downloading images.
4. From the **Action** drop-down list, select **Download Image**.
5. Check that the **Upgrade Status** column shows **Download Succeeded** to confirm that the download has been completed for the selected Windows Agents.

Step 4: Upgrade the Windows Agents

1. Go to **ADMIN > Health > Agent Health**.
2. From the **Columns** drop-down list, ensure **Version** is selected. If not, select it so the **Version** column is displayed.
3. Select the Windows Agent(s) you wish to upgrade.
   Note: Starting with release 6.4.0, you can choose multiple Windows Agents for installing images.
4. From the **Action** drop-down list, select **Install Image**.
5. Check that the **Upgrade Status** column shows **Upgrade Succeeded** to confirm that the Windows Agent(s) have upgraded successfully. Check that the **Version** column shows the correct version number, in this example 4.2.1, to confirm that the Windows Agent(s) have upgraded to the correct version.

Custom Update

To allow Load Balancers in front of the Supervisor to work, Fortinet allows you to perform a custom upgrade through a configured IP/Host Name.
Note: The current upgrade URL for Collectors and Agents were auto generated by the App Server based on the Supervisor host name.

To perform a custom update, take the following steps.

1. Navigate to **ADMIN > Settings > System > Image Server**.
2. Under **Custom Update**, in the **IP/Host Name** field, enter the IP address or host name to use as the public download URL. **Note**: Make sure the Collector or Agent can either ping the new IP address or host name.
3. Click **Save**.
4. Upload the secure image file. (Following the steps from the appropriate instructions: Upgrading Collectors, Upgrading Linux Agents, Upgrading Windows Agents.)
   Note: If you re-update to a new URL/host name, the secure image must be re-uploaded, otherwise downloading the image will fail because the previously uploaded image retains the old IP/Hostname.
5. Download Image file. (Following the steps from the appropriate instructions: Upgrading Collectors, Upgrading Linux Agents, Upgrading Windows Agents.)
6. Install Image. (Following the steps from the appropriate instructions: Upgrading Collectors, Upgrading Linux Agents, Upgrading Windows Agents.)

Cluster Config

A Load Balancer or Supervisors, and Collectors can be added into a cluster configuration here.

- Supervisor / Load Balancer Configuration
- Event Upload Workers Configuration
- Collector High Availability Configuration
- DB Cluster Configuration

Supervisor / Load Balancer Configuration

For Supervisors or Load Balancer configuration, take the following steps:

1. Navigate to **ADMIN > Settings > System > Cluster Config**.
2. Under **Supervisors**, in the **Address** field, enter the Supervisor or Load Balancer Host Name or IP address.
3. (Optional) Click **+** to add a Supervisor, or **-** to remove one, and repeat step 2 to configure any additional Supervisor or Load Balancer.
4. Click **Save** when done.

Event Upload Workers Configuration

Collectors upload events and configurations to Worker nodes.

There are three cases:

- Explicit list of Worker IP addresses or host names - Collector forwards to this list in a round robin manner.
- If you are not using Workers and using only a Supervisor and Collector(s) – specify the Supervisor IP addresses or host name. The Collectors will upload directly to the Supervisor node.
- Host name of a load balancer - Collector forwards this to the load balancer which must be configured to distribute events to the workers.

Any Hostnames specified in the Worker Upload must be resolvable by the Collector and similarly, any specified IP addresses must have connectivity from the Collector.

Complete these steps to configure Worker upload settings:

1. Navigate to **ADMIN > Settings > System > Cluster Config**.
2. Under **Event Upload Workers**, in the **Address** field, enter the Worker Host Name or IP address.
3. (Optional) Click **+** to add a Worker, or **-** to remove one, and repeat step 2 to configure any additional Workers.
4. Click **Save** when done.

Note: Virtual IP should be done here, not through Host To Template Associations under Admin > Setup > Windows Agent or Admin > Setup > Linux Agent.

Lookup Settings

Lookup setting can be used to find any IP or domain by providing the link.

Complete these steps for lookup:

1. Go to **ADMIN** > **Settings** > **System** > **Lookup** tab.
2. Enter the **Name**.
3. Select the **Client Type** to **IP** or **Domain**.
4. Enter the **Link** for look-up.

   You must enter "<ip>" in the link. FortiSIEM will replace "<ip>" with a proper IP during lookup.

   For example, to lookup the following URL:

   `http://whois.domaintools.com/8.8.8.8`

   Enter the following link in FortiSIEM:

   `http://whois.domaintools.com/<ip>`
5. Click **Save**.

Kafka Settings

FortiSIEM events found in system event database can be exported to an external system via Kafka message bus.

FortiSIEM supports both forwarding events to an external system via Kafka message bus as a 'Producer' and receiving events from a third-party system to FortiSIEM via Kafka message bus as a 'Consumer'.

As a Producer:

- Make sure you have set up a Kafka Cloud (here) with a specific Topic for FortiSIEM events.
- Make sure you have identified a set of Kafka brokers that FortiSIEM is going to send events to.
- Make sure you have configured Kafka receivers which can parse FortiSIEM events and store in a database. An example would be Logstash receiver (see here) that can store in an Elastic Search database.
- Configure event forwarding in order for FortiSIEM to send events to an external Kafka consumer.
- Supported Kafka version: 0.8

As a Consumer:

- Make sure you have set up a Kafka Cloud (here) with a specific Topic, Consumer Group and a Consumer for sending third party events to FortiSIEM.
- Make sure you have identified a set of Kafka brokers that FortiSIEM will receive events from.
- Supported Kafka version: 0.8

Setting up Consumer

Complete these steps to configure Kafka for authentication.

Note: Tested with

- kafka_2.13-3.4.0.tgz

1. Download the source code tarball.
   https://archive.apache.org/dist/kafka/3.4.0/kafka_2.13-3.4.0.tgz
2. Generate SSL key

```
# sudo mkdir /opt/kafka
# chown -R admin.admin /opt/kafka
# cd /opt/kafka
# wget https://github.com/confluentinc/librdkafka/raw/master/tests/gen-ssl-certs.sh
# bash gen-ssl-certs.sh ca ca-cert CA_CN
# bash gen-ssl-certs.sh -k server ca-cert broker_ $(hostname)
# bash gen-ssl-certs.sh -k client ca-cert client_ client
# bash gen-ssl-certs.sh client ca-cert client_ client
```

3. Uncompress the files and enter the "config" folder.
4. Modify the configuration files by appending the following to the end of the files:
   Note: In the following example, the following is used:
   `username=alice`
   `password=alice-secret`
   `SSL password=abcdefgh`
   Remember to replace <*Kafka Server IP Address*> with your actual Kafka Server IP address.

```
# zookeeper.properties
authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
requireClientAuthScheme=sasl

# zookeeper_jaas.conf
Server {
org.apache.zookeeper.server.auth.DigestLoginModule required
   user_super="zookeeper"
   user_alice="alice-secret";
};

# server.properties
listeners=SASL_SSL://<Kafka Server IP Address>:9092
advertised.listeners=SASL_SSL://<Kafka Server IP Address>:9092

sasl.enabled.mechanisms=SCRAM-SHA-512
sasl.mechanism.inter.broker.protocol=SCRAM-SHA-512
security.inter.broker.protocol=SASL_SSL
ssl.endpoint.identification.algorithm=

authorizer.class.name=kafka.security.authorizer.AclAuthorizer
allow.everyone.if.no.acl.found=true
```

```
auto.create.topics.enable=true
ssl.client.auth=none
ssl.protocol = TLS
ssl.enabled.protocols=TLSv1.3,TLSv1.2
ssl.keystore.type=JKS
ssl.truststore.type=JKS
ssl.secure.random.implementation=SHA1PRNG

ssl.keystore.location=/opt/kafka/broker_server.keystore.jks
ssl.keystore.password=abcdefgh
ssl.key.password=abcdefgh
ssl.truststore.location=/opt/kafka/broker_server.truststore.jks
ssl.truststore.password=abcdefgh

# kafka_server_jaas.conf
KafkaServer {
org.apache.kafka.common.security.scram.ScramLoginModule required
username="alice"
password="alice-secret"
user_alice="alice-secret";
};
Client {
org.apache.zookeeper.server.auth.DigestLoginModule required
username="alice"
password="alice-secret";
};

# consumer.properties
security.protocol=SASL_SSL
sasl.mechanism=SCRAM-SHA-512
sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule required
username="alice" password="alice-secret";
ssl.truststore.location=/opt/kafka/client_client.truststore.jks
ssl.truststore.password=abcdefgh
ssl.endpoint.identification.algorithm=

# producer.properties
security.protocol=SASL_SSL
sasl.mechanism=SCRAM-SHA-512
sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule required
username="alice" password="alice-secret";
ssl.truststore.location=/opt/kafka/client_client.truststore.jks
ssl.truststore.password=abcdefgh
ssl.endpoint.identification.algorithm=

# kafka_client_jaas.conf
KafkaClient {
org.apache.kafka.common.security.scram.ScramLoginModule required
username="alice"
password="alice-secret"
user_alice="alice-secret";
```

```
};
Client {
org.apache.zookeeper.server.auth.DigestLoginModule required
username="alice"
password="alice-secret";
};

# topic.conf
sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule required
username="alice" password="alice-secret";
security.protocol=SASL_SSL
sasl.mechanism=SCRAM-SHA-512
ssl.truststore.location=/opt/kafka/client_client.truststore.jks
ssl.truststore.password=abcdefgh
ssl.endpoint.identification.algorithm=

# zookeeper.properties
authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
requireClientAuthScheme=sasl
jaasLoginRenew=3600000
```

5. Start zookeeper.

```
cd ..
export KAFKA_OPTS="-Djava.security.auth.login.config=$(\pwd)/config/zookeeper_
jaas.conf"
bin/zookeeper-server-start.sh config/zookeeper.properties

(In another shell window)
bin/kafka-configs.sh --zookeeper localhost:2181 --alter --add-config 'SCRAM-SHA-512=
[password=alice-secret]' --entity-type users --entity-name alice
```

6. Start the server (In another shell window)

```
export KAFKA_OPTS="-Djava.security.auth.login.config=$(\pwd)/config/kafka_server_
jaas.conf"
bin/kafka-server-start.sh config/server.properties
```

7. Create topic (name=test1) (In another shell window)

```
bin/kafka-topics.sh --create --topic test1 --bootstrap-server <Kafka Server IP
Address>:9092 --partitions 3 --replication-factor 1 --command-config config/topic.conf
```

8. Start consumer.

```
export KAFKA_OPTS="-Djava.security.auth.login.config=$(\pwd)/config/kafka_client_
jaas.conf"
bin/kafka-console-consumer.sh --topic test1 --bootstrap-server=<Kafka Server IP
Address>:9092 --consumer.config=config/consumer.properties
```

   At this point, when FortiSIEM forwards events to this client, contents can be seen in the consumer window.

9. (Optional) Start producer.

```
export KAFKA_OPTS="-Djava.security.auth.login.config=$(\pwd)/config/kafka_client_
jaas.conf"
bin/kafka-console-producer.sh --topic test1 --broker-list <Kafka Server IP
Address>:9092 --producer.config config/producer.properties
```

On FortiSIEM, take the following actions.

1. Copy the following files to `/etc/pki/kafka` to your FortiSIEM Supervisor and to every FortiSIEM Collector.
   - ca-cert
   - client_client.pem
   - client_client.key
2. On the FortiSIEM Supervisor and Collector, make sure to set up the value properly in `/opt/phoenix/config/phoenix_config.txt` for the path of the above files, so FortiSIEM can query the Simple Authentication and Security Layer (SASL) with correct results for the Supervisor and each Collector.

```
grep sasl /opt/phoenix/config/phoenix_config.txt
sasl_ssl_ca_cert=/etc/pki/kafka/ca-cert
sasl_ssl_cert_file=/etc/pki/kafka/client_client.pem
sasl_ssl_key_file=/etc/pki/kafka/client_client.key
sasl_ssl_password=abcdefgh
sasl_ssl_verify=false
```

Setting Up FortiSIEM

Complete these steps for configuring Kafka settings in FortiSIEM:

1. Go to **ADMIN** > **Settings** > **System** > **Kafka** tab.
2. Click **New**.
3. Enter the **Name** and **Topic**.
4. Select or search the **Organization** from the drop-down.
5. Add **Brokers** by clicking **+** icon.
   a. Enter IP address or Host name of the broker.
   b. Enter Broker port (default 9092).
6. Click **Save**.
7. Select the **Client Type** to **Producer** or **Consumer**.
8. If the Consumer is selected in step 7, enter the **Consumer Name** and **Group Name** fields.
9. Enable Authentication if you want to apply Kafka authentication by adding a checkmark to the **Authentication** checkbox, then take the following steps:
   a. Select your **Protocol**: **SASL_PLAINTEXT**, **SASL_SSL**.
   b. Select your authentication mechanism: **PLAIN**, **SCRAM-SHA-256**, or **SCRAM-SHA-512**.
   c. In the **User Name** field, enter the user name to authenticate for the Kafka servers.
   d. In the **Password** field, enter the password associated with the user name to authenticate for the Kafka servers.

e. In the **Confirm Password** field, re-enter the password associated with the user name to authenticate for the Kafka servers.

10. Click **Save**.

Dashboard Slideshow Settings

Dashboard Slideshow settings are used to select a set of dashboards and display them in a slideshow mode on big monitors to cover the entire display. This is useful for Network and Security Operation Centers.

Complete these steps to create a Dashboard Slideshow:

1. Go to **ADMIN** > **Settings** > **System** > **Dashboard Slideshow** tab.
2. Click **New** to create a slideshow.
3. Enter a **Name** for the slideshow.
4. Select the **Interval** for switching between dashboards.
5. Select the **Dashboards** from the list and move to the **Selected** list.
   These dashboards will be displayed in a slideshow mode.
6. Click **Save**.

For all the above System settings, use the **Edit** button to modify or **Delete** button to remove any setting from the list.

Dashboard Ownership

Dashboard Ownership settings are used to transfer editing rights from the current owner of a shared dashboard to another person. It requires that the owner to whom the rights are being transferred to, to have the same exact role permissions as the current owner. This feature can be useful if the current owner is no longer available, and another person is required to handle the shared dashboard of that individual.

Complete these steps to transfer Dashboard Ownership:

1. Go to **ADMIN** > **Settings** > **System** > **Dashboard Ownership** tab.
2. Select the Dashboard you wish to transfer ownership of.
3. Click **Transfer**.
4. In the Transfer Ownership window, select the new owner from the **To:** drop-down list.
5. Click **Save**.

You can verify the transfer by looking at the user in the **User** column.

PAYG Report

If applicable, you can generate a daily or monthly Pay as you Go (PAYG) report.

Note: This option is disabled for GB per Day licensing.

Complete these steps to generate a daily or monthly PAYG report:

1. Go to **ADMIN** > **Settings** > **System** > **PAYG Report** tab.
2. In the **Partner ID** field, enter the Partner ID.
3. Take the following steps to enable Daily Reports.
   a. Check the Daily Report checkbox.
   b. In the **Email** field, enter the email address for a person to whom a daily report should be sent.
   c. Click **+** to add another Email field entry.
   d. Repeat steps b and c to input additional entries.
4. Take the following steps to enable Monthly Reports.
   a. Check the Monthly Report checkbox.
   b. In the **Email** field, enter the email address for a person to whom a monthly report should be sent.
   c. Click **+** to add another Email field entry.
   d. Repeat steps b and c to input additional entries.
5. When done, click **Test** to verify your email address distribution.
6. Click **Save**.
7. To enable Month Reports, click the Monthly Report checkbox.
8. In the Transfer Ownership window, select the new owner from the **To:** drop-down list.
9. Click **Save** to finish.

Trusted Hosts

You can restrict GUI Login by defining a set of IP addresses here. If the field is empty, then GUI login from any IP addresses are allowed. However once defined, new logins are disallowed from IP addresses outside of the defined range. Existing logins are not affected. To force a logout, click on in the GUI, select a user, and click **Log Out** or **Log Out and Lock Out**.

Note: If you have defined Trusted Hosts, then remember to include the Collectors and the Agents, else they will not be able to register.

Take the following steps to configure:

1. Navigate to **ADMIN > Settings > System > Trusted Hosts**.
2. In the **Trusted Hosts** field, enter a single IP address or CIDR range, for example 172.0.20.1/24.
3. Click **+** to add another Trusted Hosts field to configure if needed.
   Note: Click **-** to remove an existing Trusted Hosts field.
4. Click **Save** when done.

FortiGuard Proxy

You can add a FortiGuard proxy by taking the following steps to configure:

1. Navigate to **ADMIN > Settings > System > FortiGuard Proxy**.
2. Uncheck the **Disable Proxy** checkbox.
3. In the **IP/Host** field, enter the IP address/hostname of the FortiGuard proxy server.
4. In the **Port** field, enter the port number used to access the server.
5. In the **User Name** field, enter the username account for access.
6. In the **Password** field, enter the password associated with the username.
7. Click **Save** when done.

FQDN

To configure a fully qualified domain name (FQDN) take the following steps.

1. Navigate to **Admin > Settings > System > FQDN**.
2. In the **Host** field, enter the FQDN.
3. Click **Save**.

Collector High Availability Configuration

A FortiSIEM Collector plays the critical role of communicating with the end devices and Cloud Services for collecting logs and performance monitoring metrics, configurations, and other data. Currently if a Collector goes down, then:

- Logs sent to this Collector need to be manually resent to another Collector unless there is a Load Balancer in front.
- Events being pulled by Collector stops, until a new Collector is onboarded, and discovery is repeated to create an event pulling job for the new Collector.

This release adds the ability to deploy Collectors in *High Availability* mode – this enables Collector data collection to continue uninterrupted even when a Collector fails. This feature works differently in these environments:

- Case 1: On premise and AWS deployments via VRRP
- Case 2: On Azure and GCP deployments via Load Balancer

Case 1: On premise and AWS deployments via VRRP

If your Collectors are deployed on On-premise hypervisors, or on AWS, or they are hardware appliances, then High Availability (HA) is enabled via Virtual Router Redundancy Protocol (VRRP). A Collector HA Cluster needs to be created with one Leader and one or more Followers and a Virtual IP (VIP) that is always owned by the Leader.

During normal operations:

- Logs sent to the VIP are handled by the Leader Collector (which owns the VIP).
- FortiSIEM Supervisor node *distributes* event pulling and performance monitoring jobs among all Collectors in the Cluster.

If the Leader Collector goes down:

- The Follower node with highest priority will become the Leader and own the VIP. No human intervention is needed.
- Logs previously sent to the (failed) Leader Collector will automatically reach the new Leader Collector.
- FortiSIEM Supervisor node will automatically *re-distribute* event pulling and performance monitoring jobs previously assigned to the failed Leader Collector, to other Collectors in the HA Cluster.

If a Follower Collector goes down:

- App Server will distribute event pulling and performance monitoring jobs assigned to the failed Collector to other Collectors in the HA Cluster.

If a failed Collector comes back up, then it will stay a Follower, but the event pulling jobs will be re-distributed among all the working Collectors in the HA Cluster.

Case 2: On Azure and GCP deployments via Load Balancer

If your Collectors are deployed on Azure or GCP, then High Availability is achieved via Load balancing mechanisms. A Collector HA Cluster needs to be created with a Load Balancer in front of the Collectors. The disadvantage of this approach is that the Customer needs to deploy a Load Balancer. However,

During normal operations:

- Logs sent to the Load Balancer are distributed among the Collectors in the Cluster.
- FortiSIEM Supervisor node *distributes* event pulling and performance monitoring jobs among all Collectors in the Cluster.
- Job distribution is handled via Round Robin.

If a Collector goes down, then:

- Load Balancer will skip the failed Collector and distribute logs among other Collectors.
- FortiSIEM Supervisor node will automatically re-distribute event pulling and performance monitoring jobs previously assigned to the failed Collector, to other Collectors in the Cluster.

Follow the appropriate configuration for your environment:

- Non-Cloud Collector Deployments
- AWS Collector Deployments
- GCP Collector Deployments
- Azure Collector Deployments

AWS/EC2 Collector Deployments

This Case covers the situation where your Collectors are deployed on AWS/EC2.

To configure Collector HA on AWS/EC2, you will need to configure your collectors as normal. Each Collector will need to have a specifically configured IAM Role. To configure an IAM Role to be later associated with each instance, you will need an IAM Policy. An IAM Policy contains the permissions needed for FortiSIEM to create VIP to handle Collector HA group. After the IAM Policy has been created, you will create the IAM Role then associate it to all the Collectors. Next, you will locate an unused VIP, and finally configure Collector HA on FortiSIEM using that VIP. The Collector HA Cluster needs to be created with one Leader and one or more Followers and a Virtual IP (VIP) that is always owned by the Leader. High Availability (HA) is then enabled via Virtual Router Redundancy Protocol (VRRP).

During normal operations:

- Logs sent to the VIP are handled by the Leader Collector (which owns the VIP).
- FortiSIEM Supervisor node distributes event pulling and performance monitoring jobs among all Collectors in the Cluster.

If the Leader Collector goes down:

- The Follower node with highest priority will become the Leader and own the VIP.
- Logs previously sent to the (failed) Leader Collector will automatically reach the new Leader Collector.
- FortiSIEM Supervisor node will automatically re-distribute event pulling and performance monitoring jobs previously assigned to the failed Leader Collector, to other Collectors in the HA Cluster.

If a Follower Collector goes down:

- App Server will distribute event pulling and performance monitoring jobs assigned to the failed Collector to other Collectors in the HA Cluster.
- If a failed Collector comes back up, then it will stay a Follower, but the event pulling jobs will be re-distributed among all the working Collectors in the HA Cluster.

Failure and Recovery:

- If the Leader Collector goes down then the Follower with the highest priority takes over. If the Leader Collector comes back up, then it will resume the Leader role due to its higher priority.
- If a Follower Collector goes down, the Leader will continue to operate. If the Follower comes back up, then it will remain a Follower while the Leader is operational.

- Step 1 - Configure Collectors
- Step 2 - Create IAM Policy
- Step 3 - Create IAM Role
- Step 4 - Associate IAM Role to all Collectors
- Step 5 - Locate Unused VIP
- Step 6 - Configure Collector HA Group Via VRRP

Step 1 - Configure Collectors

Configure Collectors as normal.

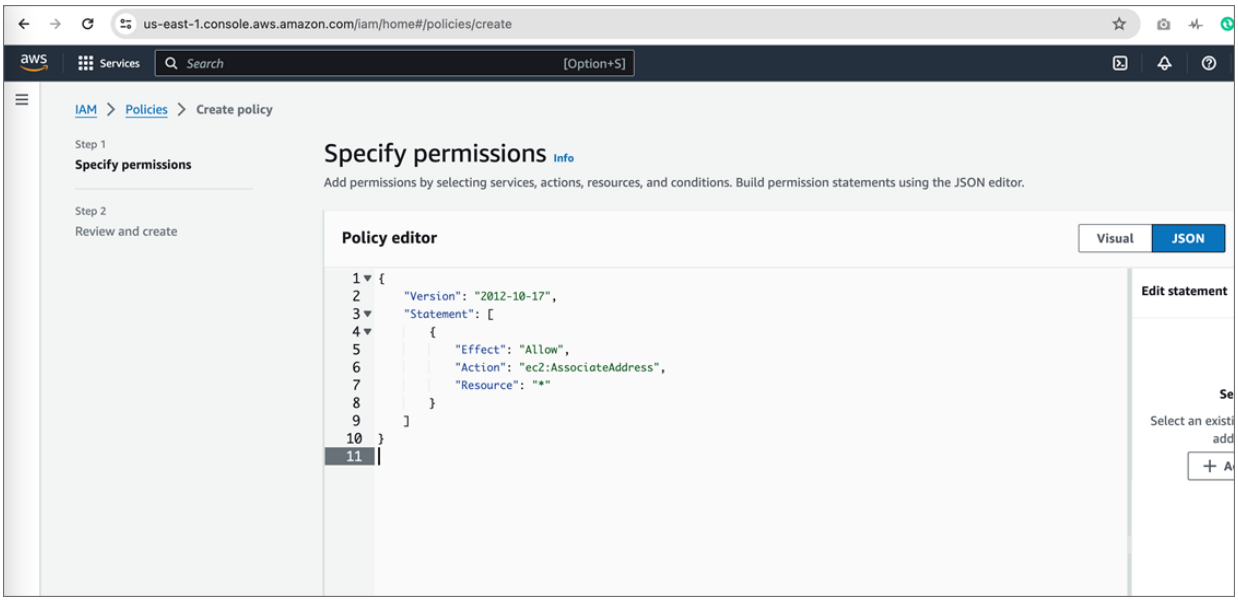
Step 2 - Create IAM Policy

To create an IAM policy, take the following steps.

Note: For more information, see https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create-console.html#access_policies_create-json-editor

1. Sign in to https://console.aws.amazon.com/iam/
2. From the left pane, select **Policies**.
3. Click **Create policy**.
4. From the **Policy editor** section, select **JSON**.
5. In the **Policy editor** pane, paste the following information:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:AssociateAddress",
            "Resource": "*"
        }
    ]
}
```

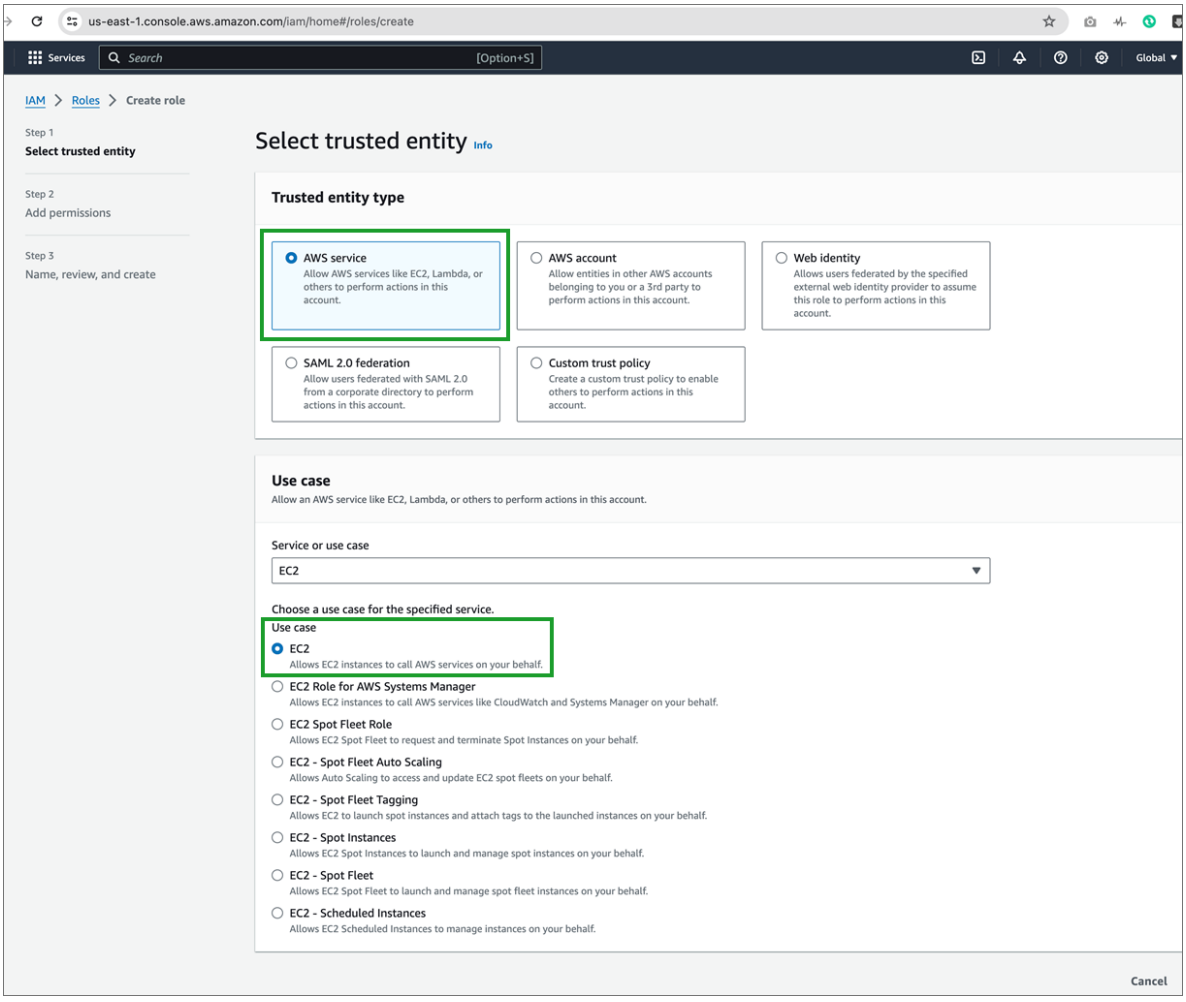


6. Click **Next**.
7. Under Policy name, enter a name for the policy, such as "AssociateAddress".
8. Click **Create Policy**.

Step 3 - Create IAM Role

To create an IAM role, take the following steps.

1. Sign in to https://console.aws.amazon.com/iam/.
2. From the left pane, select **Roles**.
3. Click **Create role**.
4. Under **Trusted entity type**, select **AWS service**.
5. From the **Service or use case** drop-down list, select **EC2**.
6. Under **Use case**, select **EC2**.



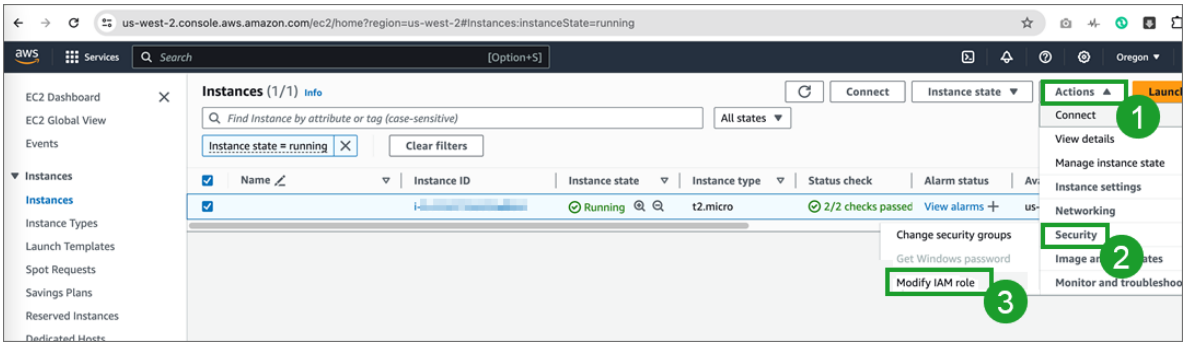
7. Click **Next**.

8. In the search field under **Permissions policies**, enter the name of the policy you created in Create IAM Policy.
9. Add a checkmark to the checkbox to attach that policy to the role we're creating.
10. Click **Next**.
11. Under the **Role** name field, enter a name for this role, such as "AssociateAddress".
12. (Optional) In the **Role description** field, enter an explanation of this role, such as "Allows EC2 instances to call AWS services on your behalf."
13. Click **Create role**.

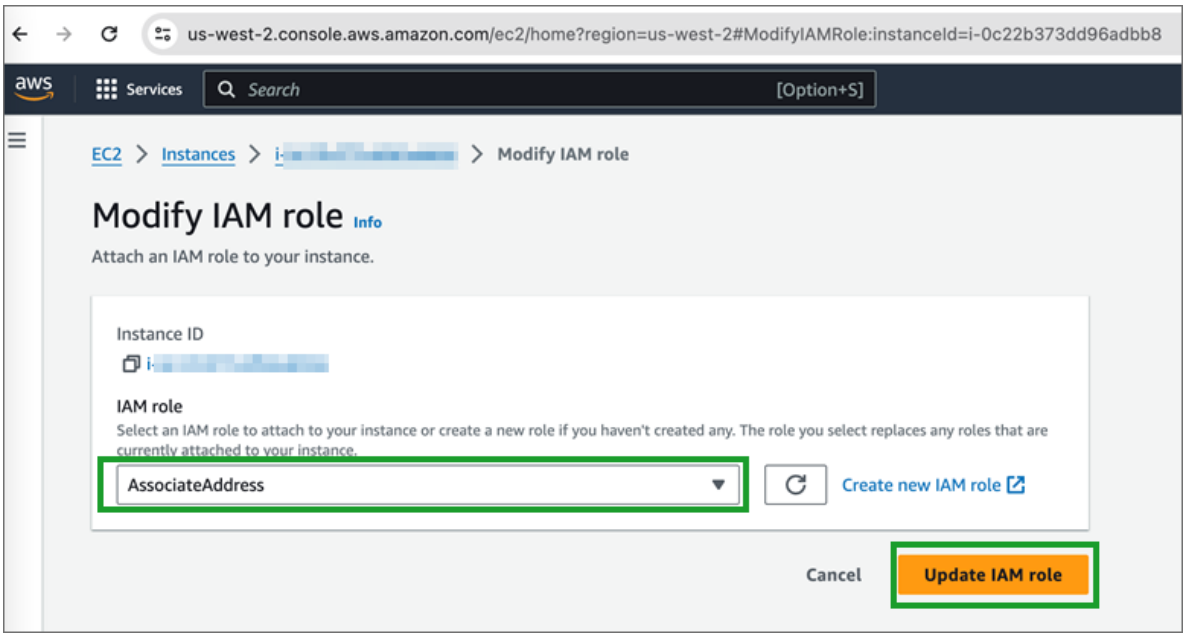
Step 4 - Associate IAM Role to all Collectors

For each collector to be part of the Collector HA group, take the following steps.

1. Sign in to the EC2 Dashboard (https://console.aws.amazon.com/ec2/v2/home).
2. From the left pane, select **Instances**.
3. Select Collector.
4. Open the **Actions** drop-down list, and select **Security > Modify IAM role**.



5. Under **IAM role**, select the role you created in Create IAM Role, and click **Update IAM role**.

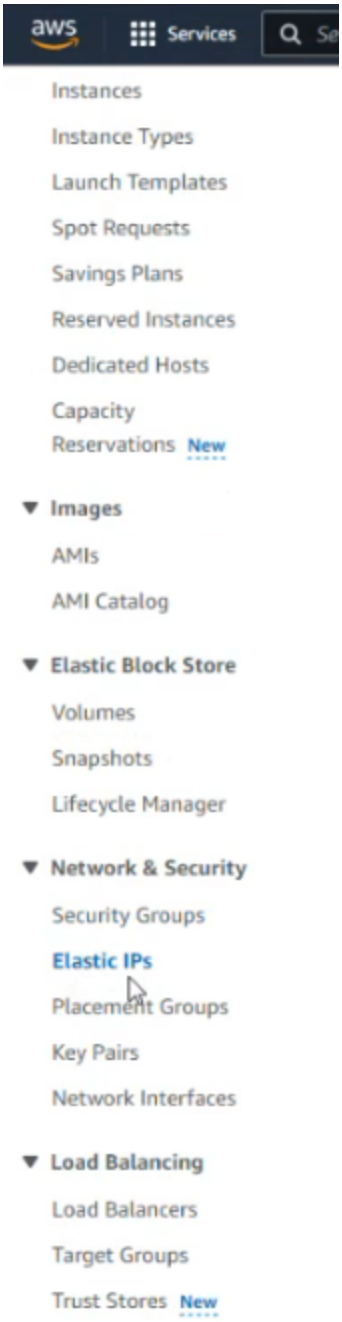


6. Repeat steps 3-5 for any remaining collectors you with to include as part of the Collector HA group.

Step 5 - Locate Unused VIP

A public IP address is required to configure a Collector HA group. To locate a public IP address to use, take the following steps.

1. Sign in to the EC2 Dashboard (https://console.aws.amazon.com/ec2/v2/home).
2. From the left pane, expand **Network & Security**, and select **Elastic IPs**.



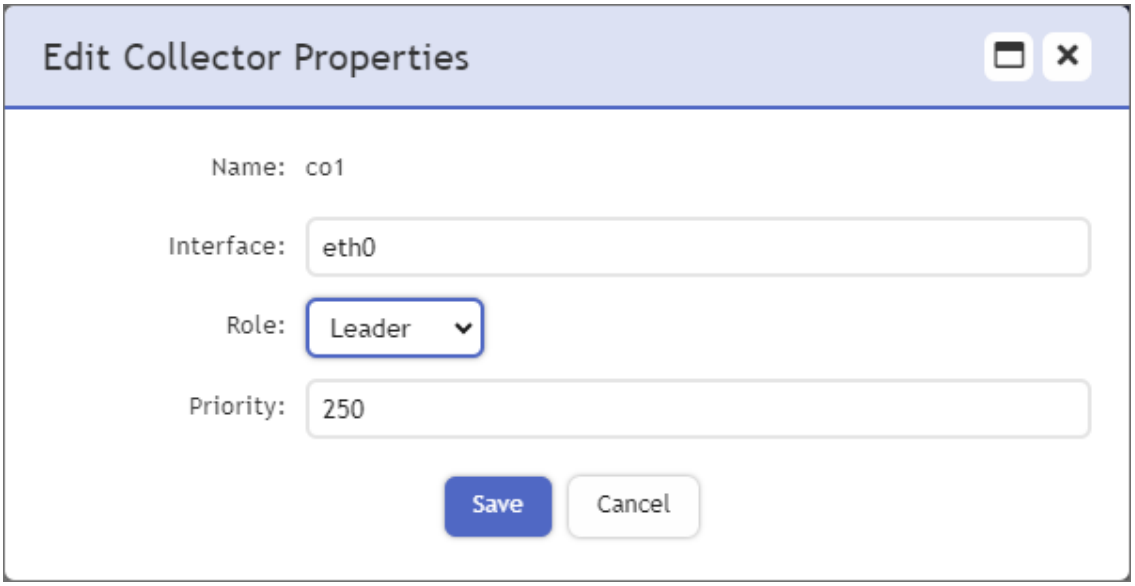
3. Under Elastic IP addresses, look for an available IP address that is Type Public IP and its Associated instance ID, Private IP address, and Association ID are all empty.
4. Ping the IP address. If it is not pingable, then it can be used as a VIP, as it confirms that the VIP is not in use. Record this VIP address. You will need it later, and need to input this into the **VIP** field in Step 6 - Configure Collector HA group Via VRRP.

Step 6 - Configure Collector HA Group Via VRRP

To create a new Collector High Availability configuration, take the following steps:

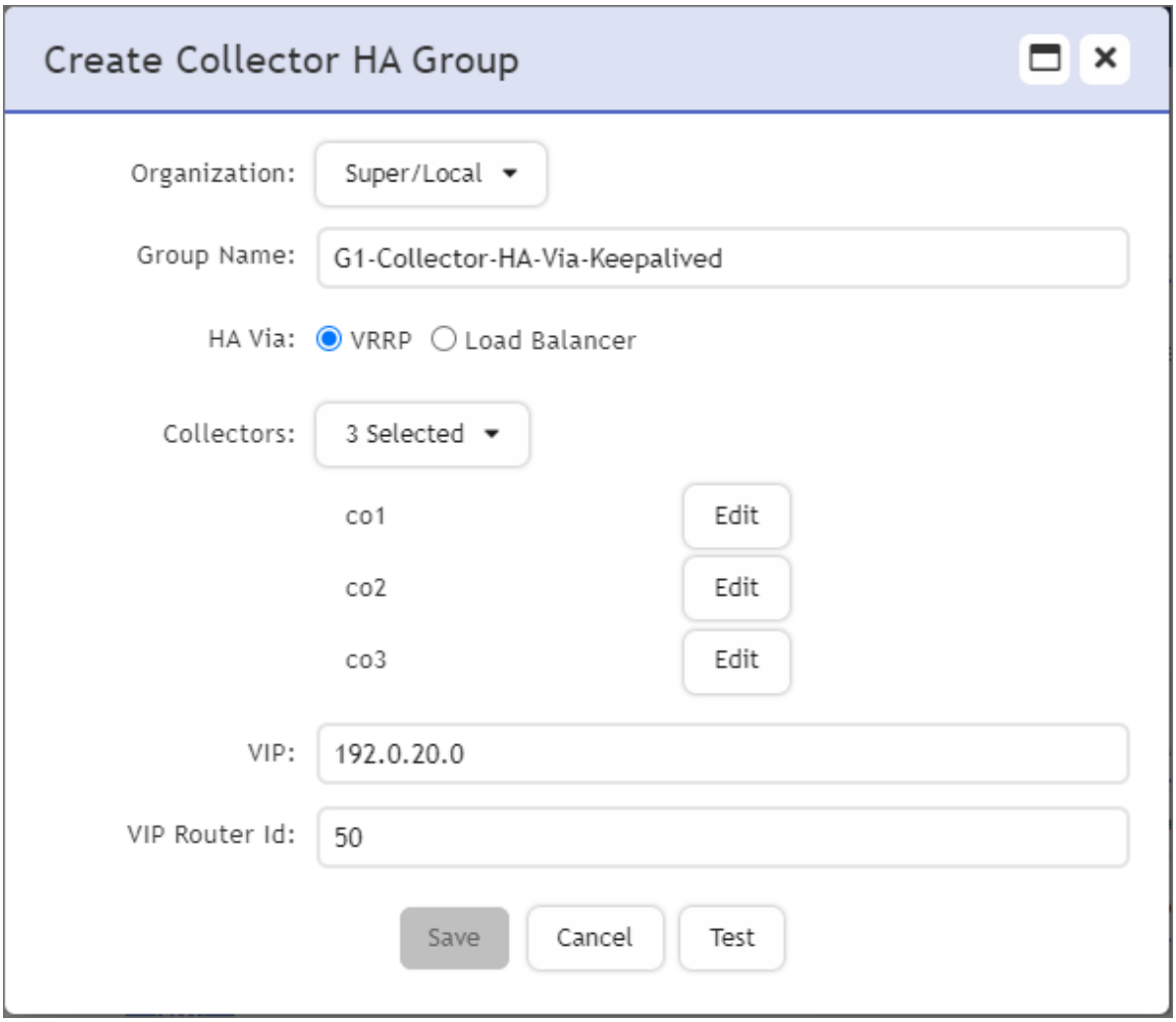
Ensure that the VIP and Collectors in a Collector HA group are on the same network. This is required for High Availability to work.

1. Navigate to **Admin > Settings > System > Cluster Config**.
2. Under Collector High Availability, click **New**. The **Create Collector HA Group** window appears. Take the following steps.
   a. From the **Organization** drop-down list, select your Organization with your collectors.
   b. In the **Group Name** field, enter the name of your Collector group.
   c. From **HA Via**, select **VRRP**.
   d. From the **Collectors** drop-down list, select the Collectors to include in the group.
   Note: The available Collectors displayed are those from the same Organization selected earlier.
   e. In the **VIP** field, enter the Virtual Internet Protocol address.
   Note: This VIP can be internal.
   f. In the **VIP Router ID** field, enter the VIP Router ID number (1-255).
3. For each collector, click Edit, and take the following steps.
   a. In the **Interface** field, enter the name of the interface. For example, eth0.
   b. From the **Role** drop-down list, select the Collector's role (Leader, Follower).
   Note: Only one collector from the HA group can be assigned as a Leader.
   c. In the **Priority** field, enter the numeric priority of the Collector, with the high number being the greater priority (1-254).
   Note: The Collector Leader Priority should be higher than all of its Followers.
   d. Click **Save**.



   e. Repeat step 3a-e for each Collector. When done, proceed to step 4.

4. Click **Test**. If the test succeeds, proceed to step 5. If it fails, check your earlier configurations.
5. Click **Save**.



Azure Collector Deployments

This Case covers the situation where your Collectors are deployed on Azure.

To use the Collector HA feature with Azure, you will need to configure your collectors, configure port rules for all your VM Collectors, create a load balancer, configure the load balancer so FortiSIEM can monitor and report the load balancer's health status, then add the load balancer to your FortiSIEM configuration. High Availability is then achieved via load balancing mechanisms.

During normal operations:

- Logs sent to the Load Balancer are distributed among the Collectors in the Cluster.
- FortiSIEM Supervisor node *distributes* event pulling and performance monitoring jobs among all Collectors in the Cluster.
- Job distribution is handled via Round Robin.

If a Collector goes down, then:

- Load Balancer will skip the failed Collector and distribute logs among other Collectors.
- FortiSIEM Supervisor node will automatically re-distribute event pulling and performance monitoring jobs previously assigned to the failed Collector, to other Collectors in the Cluster.

- Step 1 - Configure Collectors
- Step 2 - Configure Port Rule
- Step 3 - Create Load Balancer
- Step 4 - Configure Load Balancer
- Step 5 - Configure Collector HA Group Via Load Balancer

Step 1 - Configure Collectors

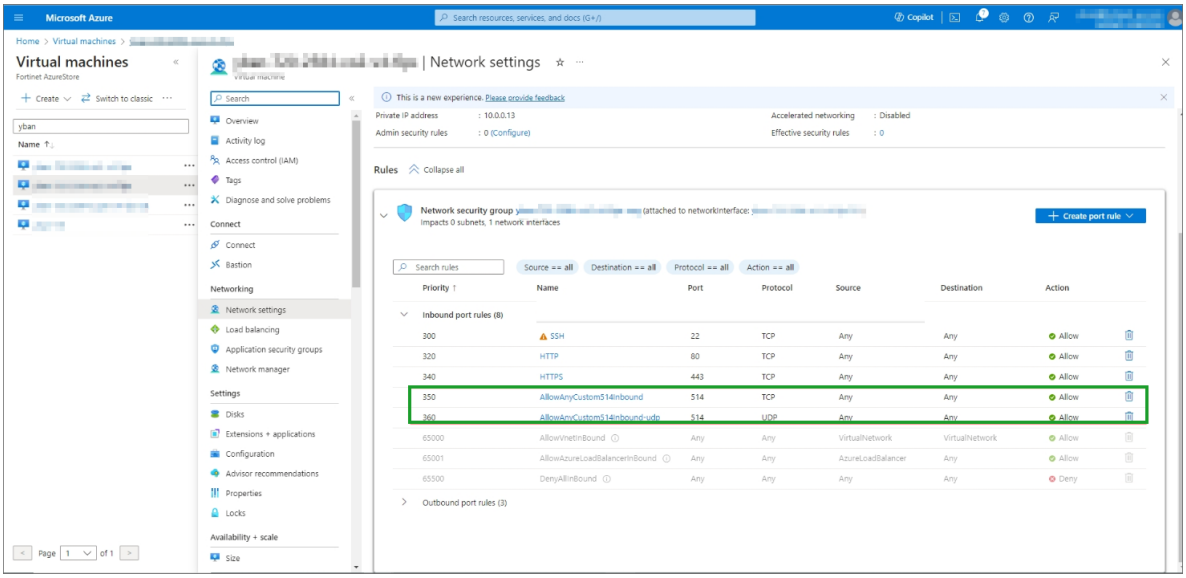
Configure Collectors as normal.

Step 2 - Configure Port Rule

For **each** VM Collector, take the following steps to create a TCP and UDP port rule for your Azure collectors.

1. Log into Microsoft Azure and go to Home > Virtual machine > <*Collector VM*>.
2. From your VM page, go to **Network Settings > Rules** and click **+ Create port rule**, then select **Inbound port rule**.
3. In the **Name** field, enter the name of the port rule, such as "514-tcp-inbound".
4. In the **Destination port ranges** field, enter "514".

5. From the **Protocol** selection, select **TCP**.
6. From the **Action** selection, select **Allow**.
7. Click **Save**.
8. Click **+ Create port rule**, then select **Inbound port rule**.
9. In the **Name** field, enter the name of the port rule, such as "514-udp-inbound".
10. In the **Destination port ranges** field, enter "514".
11. From the **Protocol** selection, select **UDP**.
12. From the **Action** selection, select **Allow**.
13. Click **Save**.



Repeat these steps for any additional Collectors you wish to include into your Collector HA group. When all Collectors have been configured with the port rules, continue with Step 3 - Create Load Balancer.

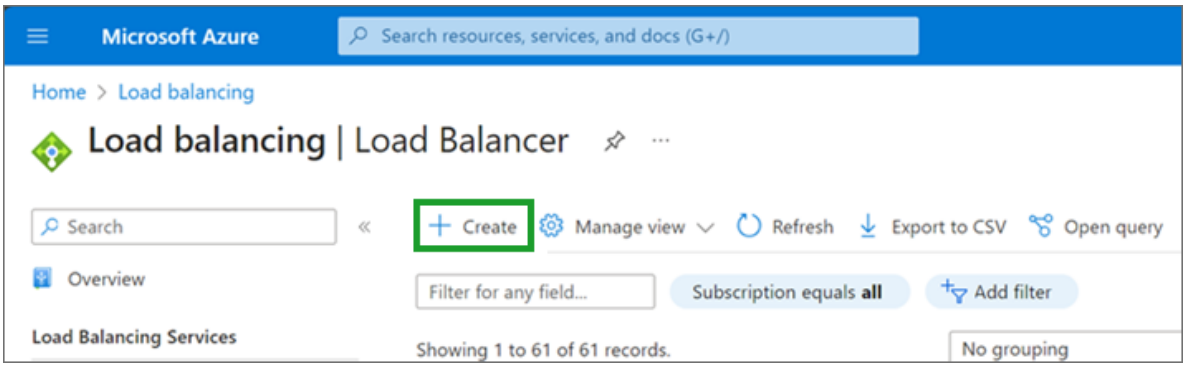
Step 3 - Create Load Balancer

To create a load balancer, take the following steps.

Note: Additional information on creating a load balancer on Azure is available at https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal

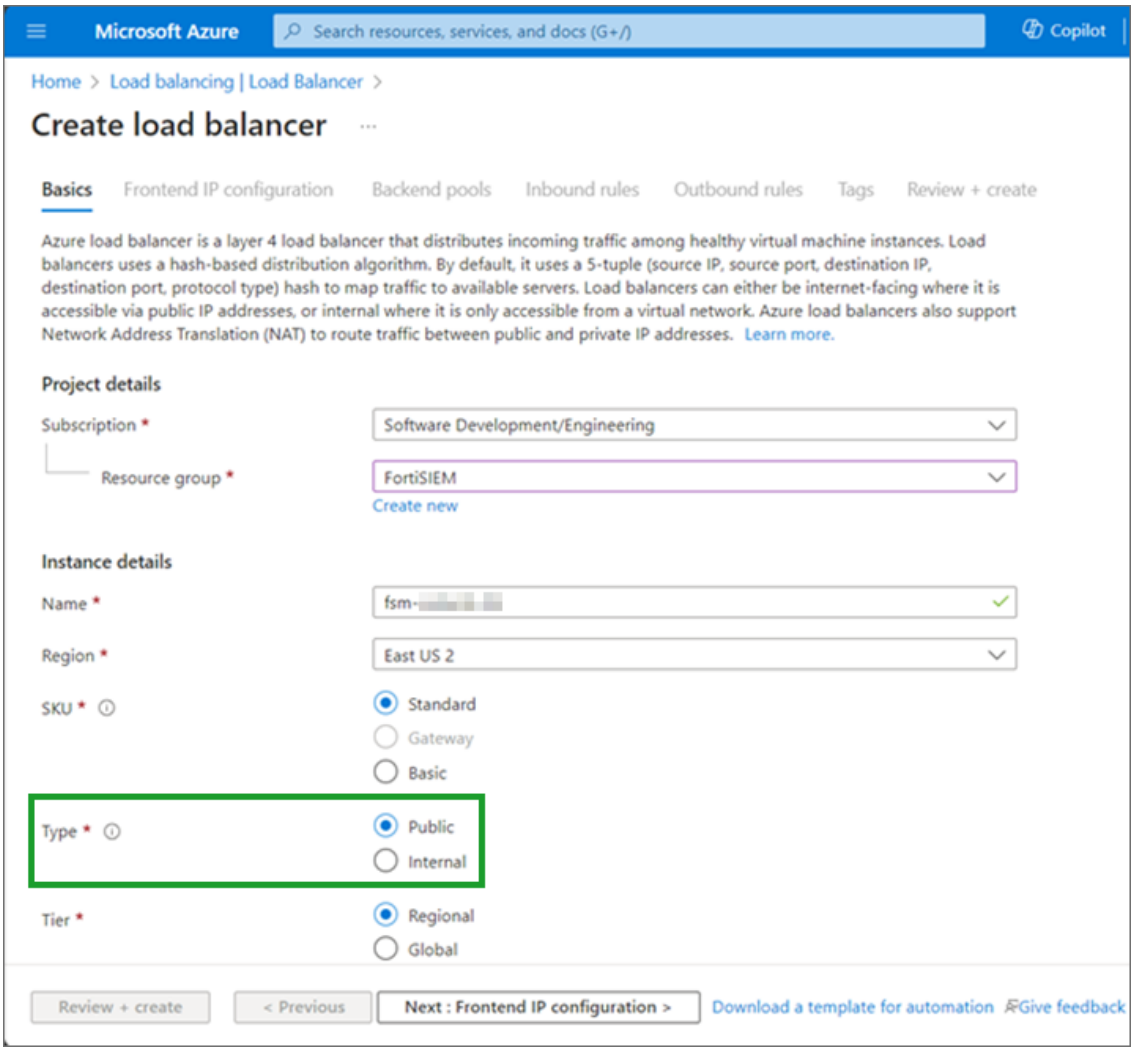
1. Log into Microsoft Azure.
2. From the search field, enter **Load balancer**, and select **Load Balancer**.

3. Click **+ Create**.



4. Under **Project details**, take the following steps.
   a. From the **Subscription** drop-down list, select your Subscription.
   b. At **Resource group**, search and select the group that the Collector instances are in.
5. Under **Instance details**, take the following steps.
   a. In the **Name** field, enter a name for the load balancer, like "load-balancer".
   b. For **Region**, select the region that the Collector instances are in.
   c. For **SKU**, leave as the default, **Standard**.

d. For **Type**, select **Public**.



e. For **Tier**, leave as the default, **Regional**.

f. Click **Next: Frontend IP configuration >**

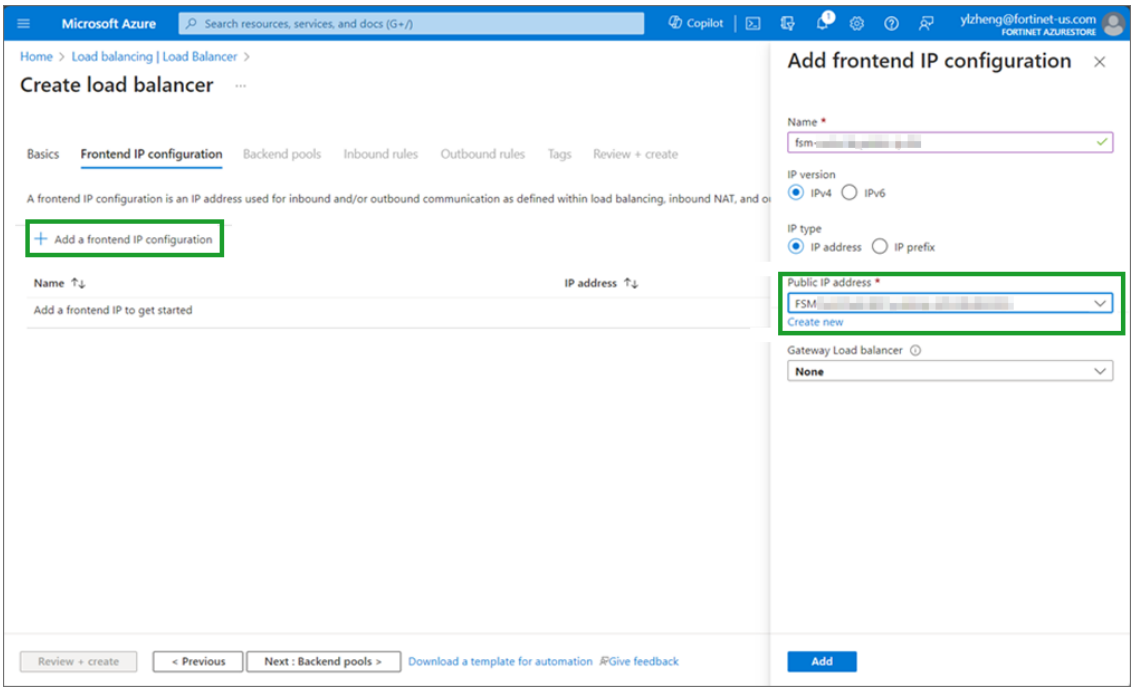
6. Under **Frontend IP configuration**, click **+ Add a frontend IP configuration**.

a. In the **Name** field, enter a name for the Frontend IP configuration.

b. For **IP version**, select **IPv4**.

c. For **IP type**, select **IP address**.

d. Under **Public IP address**, use the drop-down list to select an available public IP address. This will be the IP address in your Collector HA configuration.



e. Click **Save**.

f. Click **Next: Backend pools**.

7. From **backend pools**, click **+ Add a backend pool**.

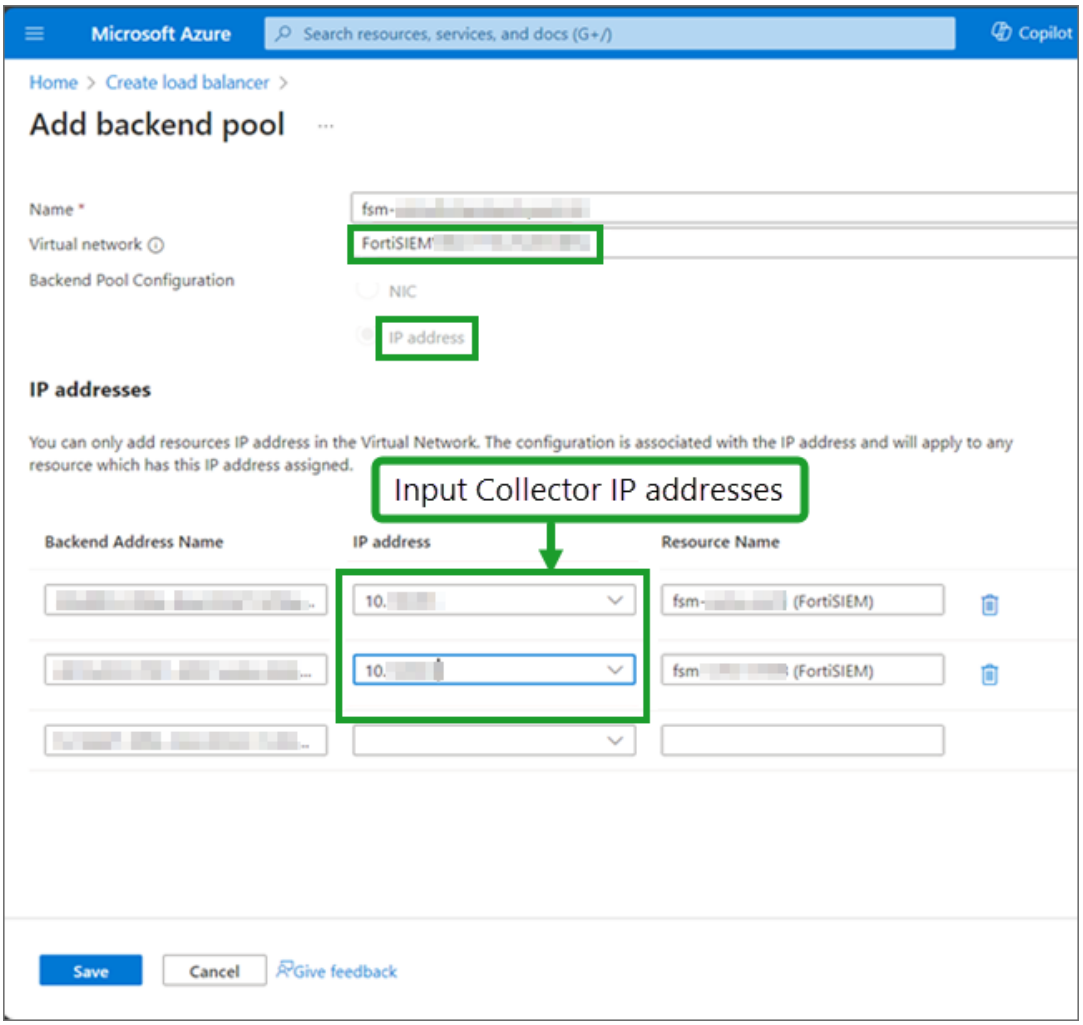
a. In the **Name** field, enter a name for backend pool.

b. From the **Virtual network** drop-down list , select a virtual network where the Collectors are.

c. For **Backend Pool Configuration**, select **IP address**.

d. From **IP addresses**, take the following steps.

i. For each **IP address** drop-down list, enter/select a Collector IP address for each Collector you wish to add to the Collector HA group.
Note: To find your existing FortiSIEM Collector IP addresses, go to the FortiSIEM GUI, navigate to **Admin > Health**, click the **Collector Health** tab, look at the **IP Address** column, and check the private IP address of the Collectors.

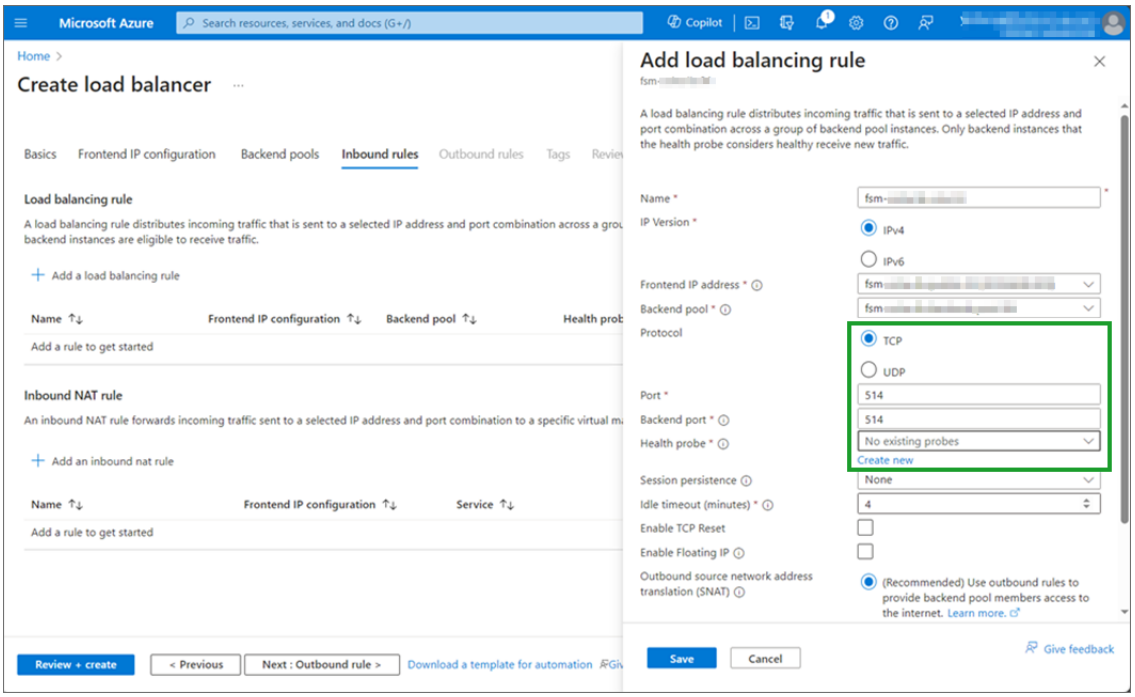


ii. When done, click **Save**.

e. Click **Next: Inbound rules**.

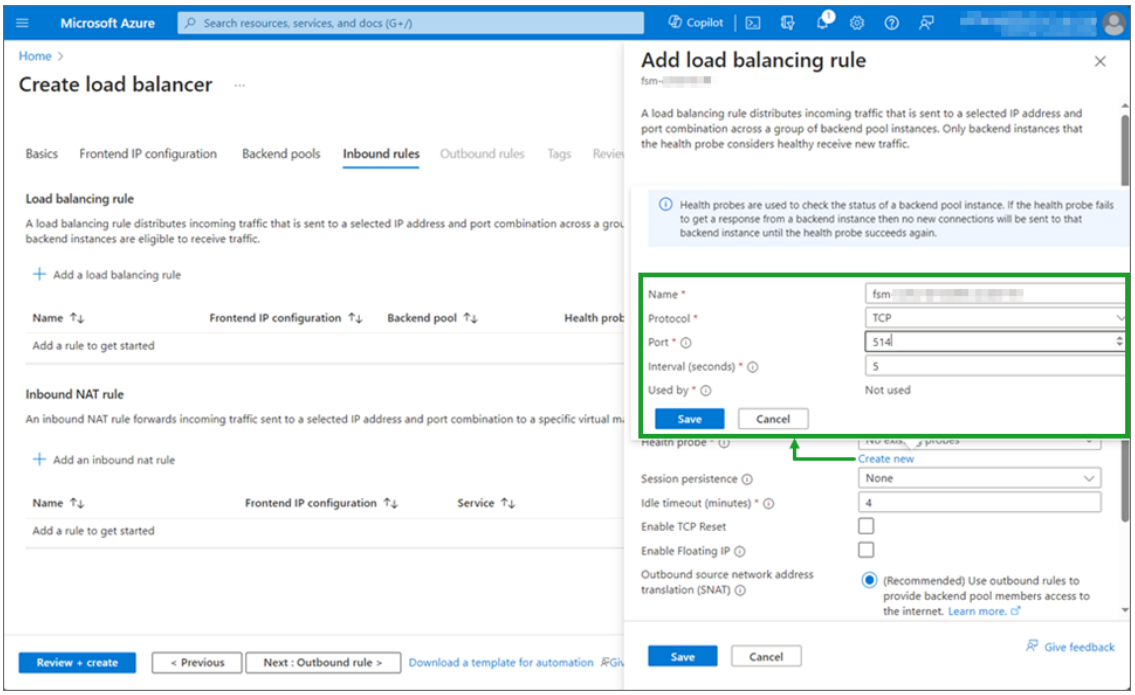
8. From **Load balancing rule**, click **+ Add a load balancing rule**, then under **Add load balancing rule**, take the following steps.
   a. In the **Name** field, enter a name for the load balancing rule.
   b. For **IP Version**, select **IPv4**.
   c. From the **Frontend IP address** drop-down list, select the Frontend IP address you created.
   d. From the **Backend pool** drop-down list, select the Backend pool that you created.
   e. For **Protocol**, select **TCP**.

f. In the **Port** field, enter 514.



g. In the **Backend port** field, enter 514.

h. Under **Health probe**, click **Create new**.



i. In the **Name** field, enter a name for the health probe.

ii. From the **Protocol** drop-down list, select **TCP**.

iii. In the **Port** field, enter 514.

iv. Click **Save**.

i. Click **Save**.

9. From Load balancing rule, click **+ Add a load balancing rule**, then under Add load balancing rule, take the following steps.
   a. In the **Name** field, enter a name.
   b. For **IP Version**, select **IPv4**.
   c. For **Protocol**, select **UDP**.
   d. In the **Port** field , enter 514.
   e. In the **Backend port** field, enter 514.
   f. Under **Health probe**, select the existing Health probe create in step 8.
   g. Click **Save**.
   h. Click **Review + create**.
10. Click **Create**.

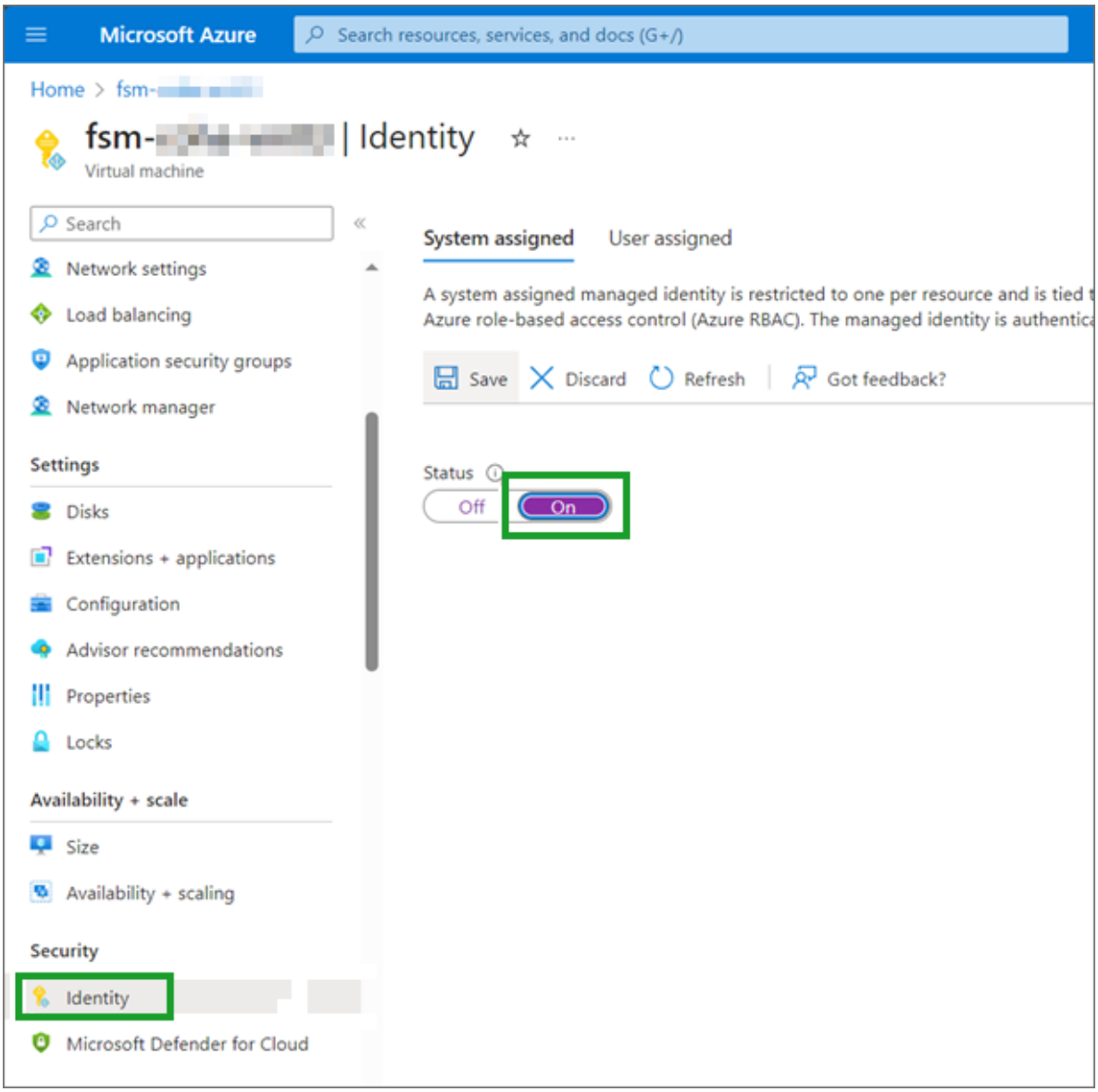
Proceed to Step 4 - Configure Load Balancer.

Step 4 - Configure Load Balancer

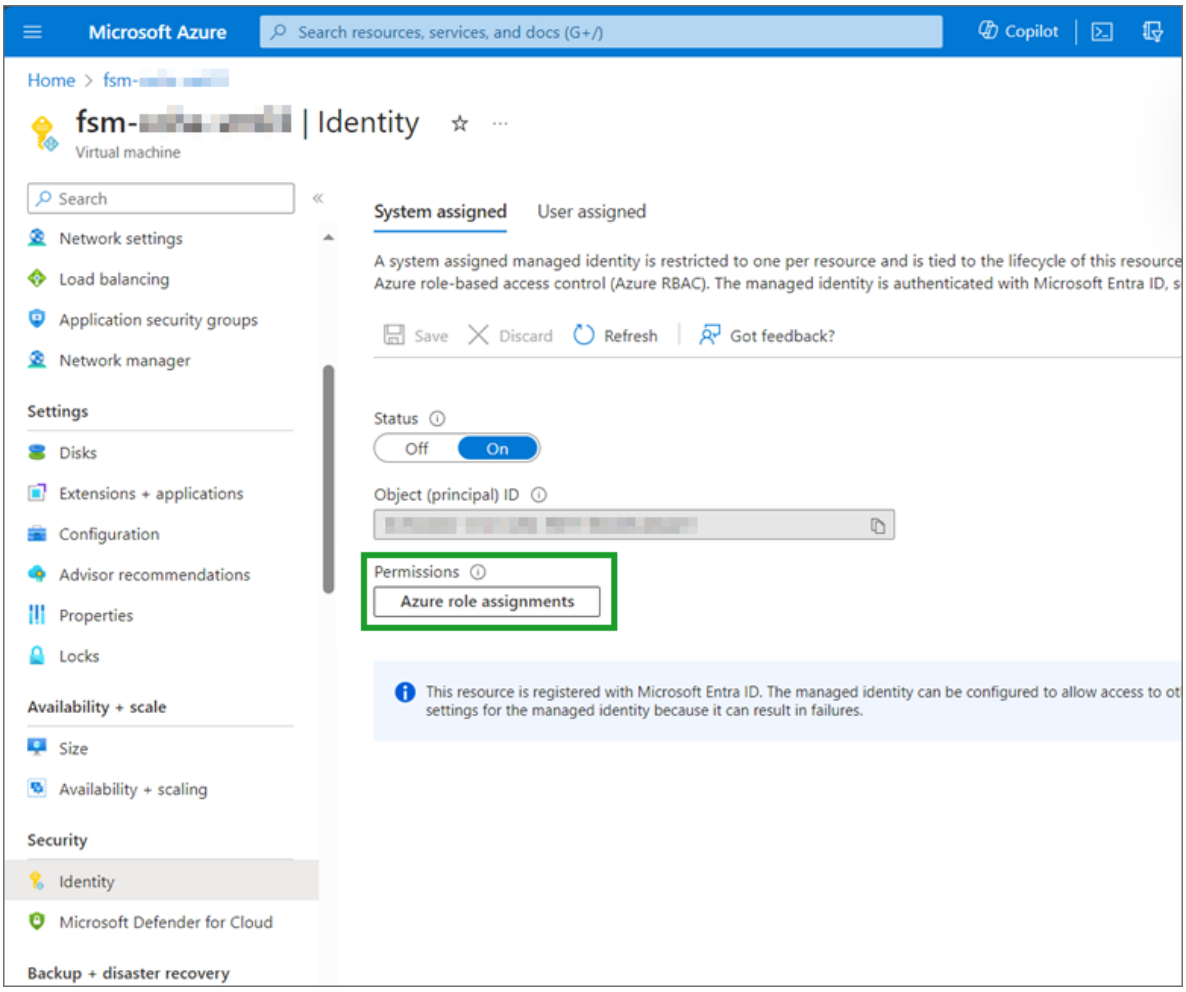
More information can be found at https://learn.microsoft.com/en-us/azure/deployment-environments/how-to-configure-managed-identity

1. Log into Microsoft Azure.
2. Navigate to the VM being used as a collector.
3. From the left pane, under **Security**, select **Identity**.

4. Change **Status** toggle so it is **On**.

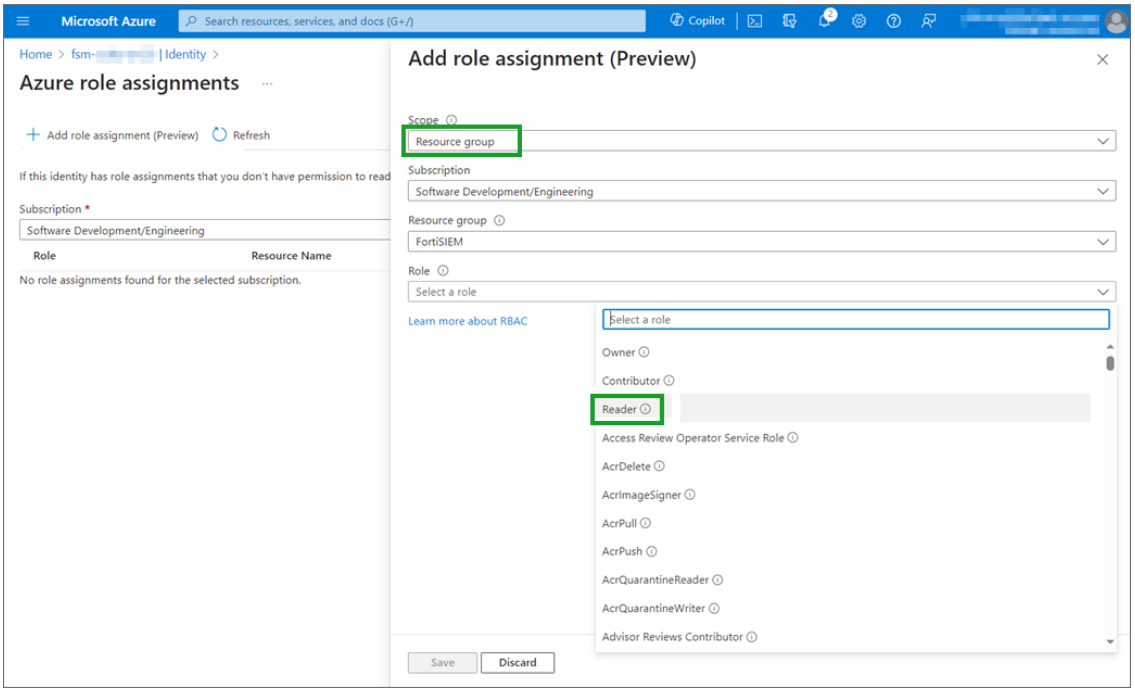


5. Click **Azure role assignments**.



6. Click **+ Add role assignment (Preview)**.
7. In the **Add role assignment (Preview)** window, take the following steps.Under **Azure role assignments**, there should now be a role of Reader.

a. From the **Scope** drop-down list, select **Resource group**.
b. From the **Role** drop-down list, select **Reader**.



c. Click **Save**.

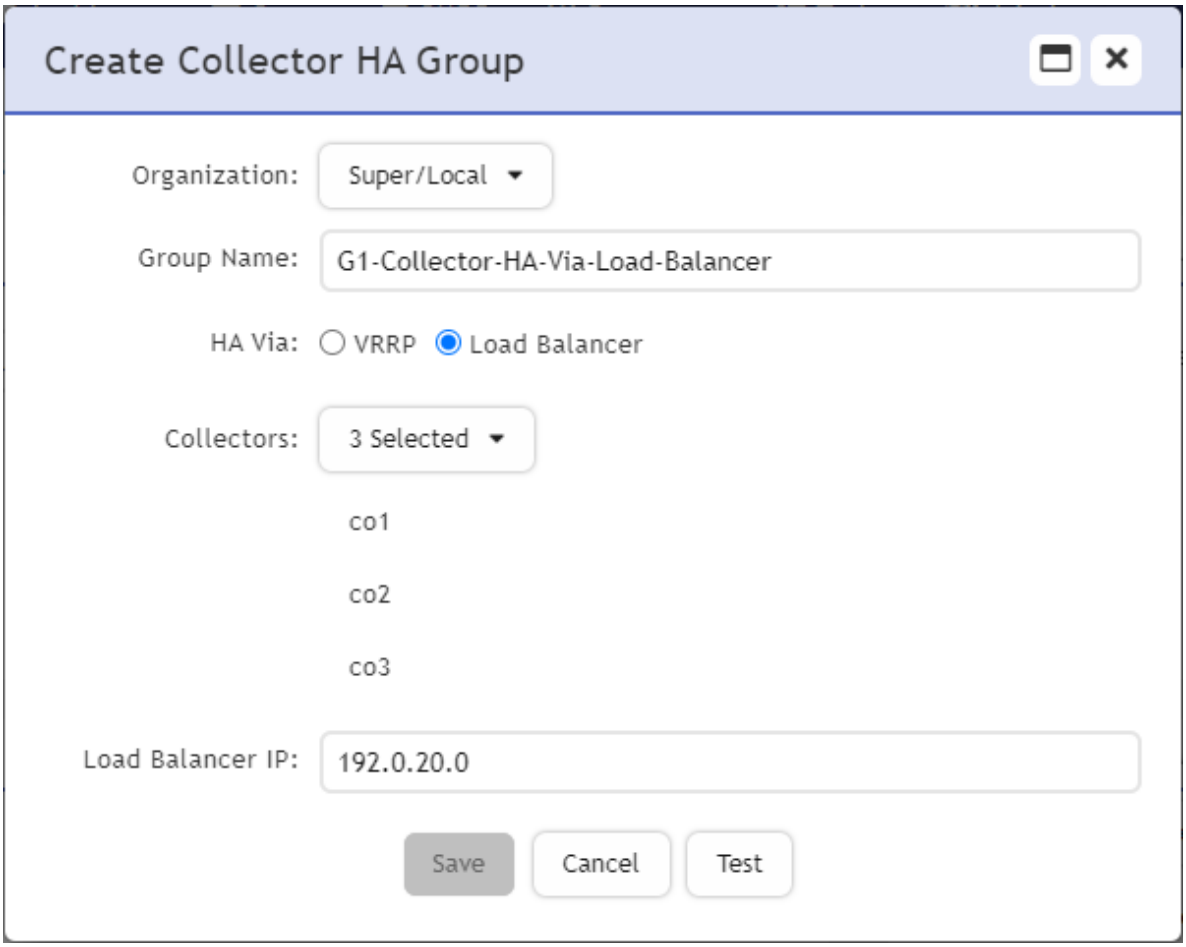
8. Go to Step 5 - Configure Collector HA Group Via Load Balancer for FortiSIEM configuration.

Step 5 - Configure Collector HA Group Via Load Balancer

To create a new Collector High Availability configuration, take the following steps:

1. Navigate to **ADMIN > Settings > System > Cluster Config**.
2. Under **Collector High Availability**, click **New**. The **Create Collector HA Group** window appears. Take the following steps.
   a. From the **Organization** drop-down list, select your Organization.
   b. In the **Group Name** field, enter the name of your Collector group.
   c. From **HA Via**, select **Load Balancer**.
   d. From the **Collectors** drop-down list, select the Collectors to include in the group.
   Note: The available Collectors displayed are those from the same Organization selected earlier.
   e. In the **Load Balancer IP** field, enter the Load Balancer frontend IP address.
   f. Click **Test** to confirm it is working correctly. If it succeeds, proceed to the next step.

3. Click **Save**.


Create Collector HA Group
Organization:
Super/Local
Group Name:
G1-Collector-HA-Via-Load-Balancer
HA Via:
VRRP
Load Balancer
Collectors:
3 Selected
co1
co2
co3
Load Balancer IP:
192.0.20.0
Save
Cancel
Test

GCP Collector Deployments

This Case covers the situation where your Collectors are deployed on GCP.

To use the Collector HA feature with GCP, after configuring your collectors, you will need to create an instance group, create a load balancer, and apply the instance group, check and configure the load balancer so FortiSIEM can monitor and report the load balancer's health status. The final step is to add the load balancer to your FortiSIEM configuration so High Availability is achieved via load balancing mechanisms.

During normal operations:

- Logs sent to the Load Balancer are distributed among the Collectors in the Cluster.
- FortiSIEM Supervisor node *distributes* event pulling and performance monitoring jobs among all Collectors in the Cluster.
- Job distribution is handled via Round Robin.

If a Collector goes down, then:

- Load Balancer will skip the failed Collector and distribute logs among other Collectors.
- FortiSIEM Supervisor node will automatically re-distribute event pulling and performance monitoring jobs previously assigned to the failed Collector, to other Collectors in the Cluster.

- Step 1 - Configure Collectors
- Step 2 - Create Instance Group
- Step 3 - Create Load Balancer
- Step 4 - Check Load Balancer
- Step 5 - Configure Load Balancer to Report Health Status
- Step 6 - Configure Collector HA Group Via Load Balancer

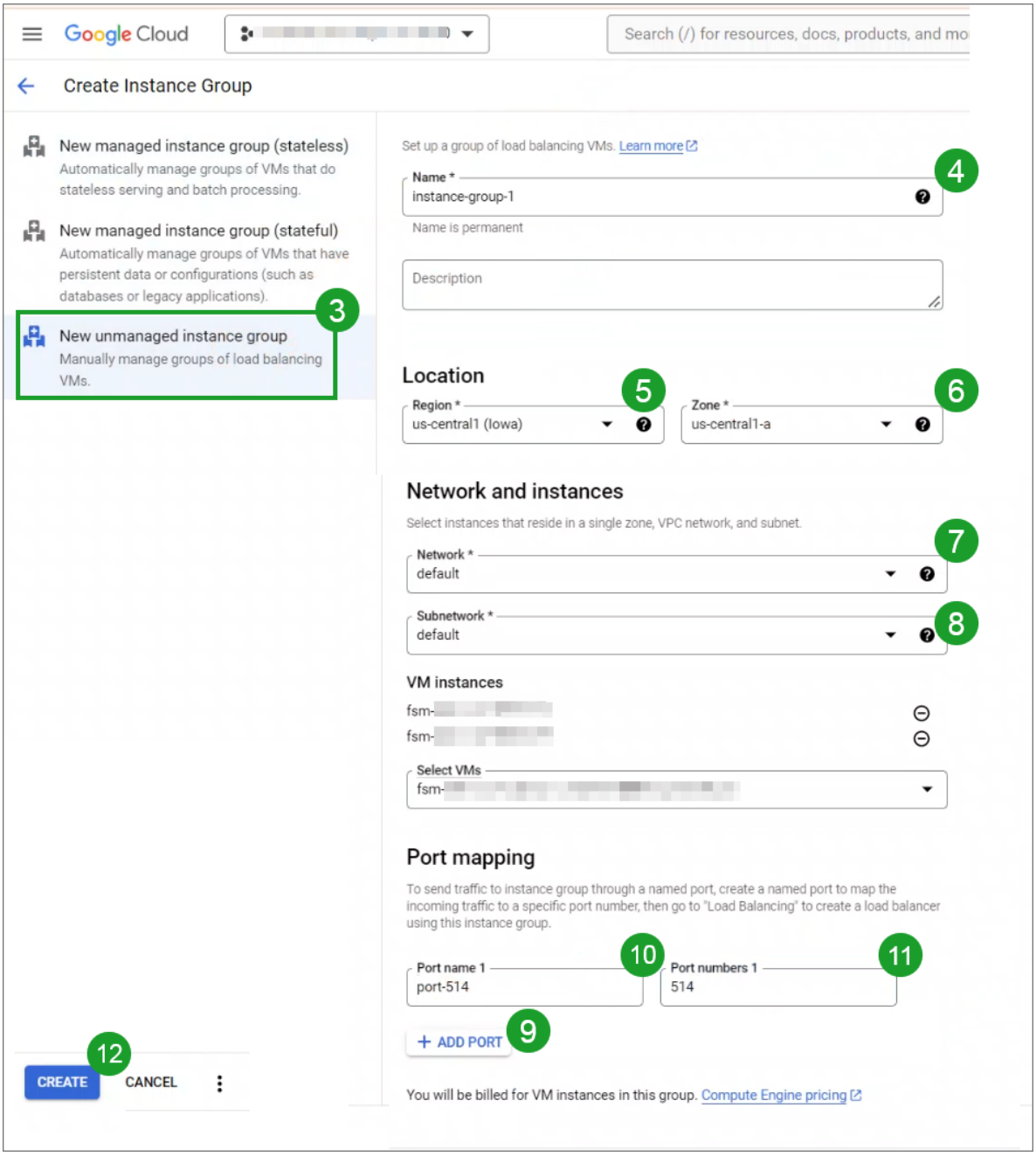
Step 1 - Configure Collectors

Configure Collectors as normal.

Step 2 - Create Instance Group

1. Go to the Instance Group page - https://console.cloud.google.com/compute/instanceGroups?_ga=2.213011796.1727950196.1712175609-895679178.1667947390
2. Click **CREATE INSTANCE GROUP**.
3. In the left pane, select **New unmanaged instance group**.
4. In the **Name** field, enter a name for the instance group.

5. From the **Location** drop-down list, select a region.
6. From the **Zone** drop-down list, select a zone.
7. From the **Network** drop-down list, select **default**.
8. From the **Subnetwork** drop-down list, select **default**.
9. From the **VM instances** drop-down list, select the collectors you wish to include as part of your Collector HA group.
10. Under **Port mapping**, click **+ ADD PORT**.
11. In the **Port name 1** field, enter a name for the port.
12. In the **Port numbers 1** field, confirm "514" appears. If it isn't, input 514.
13. Click **CREATE**.



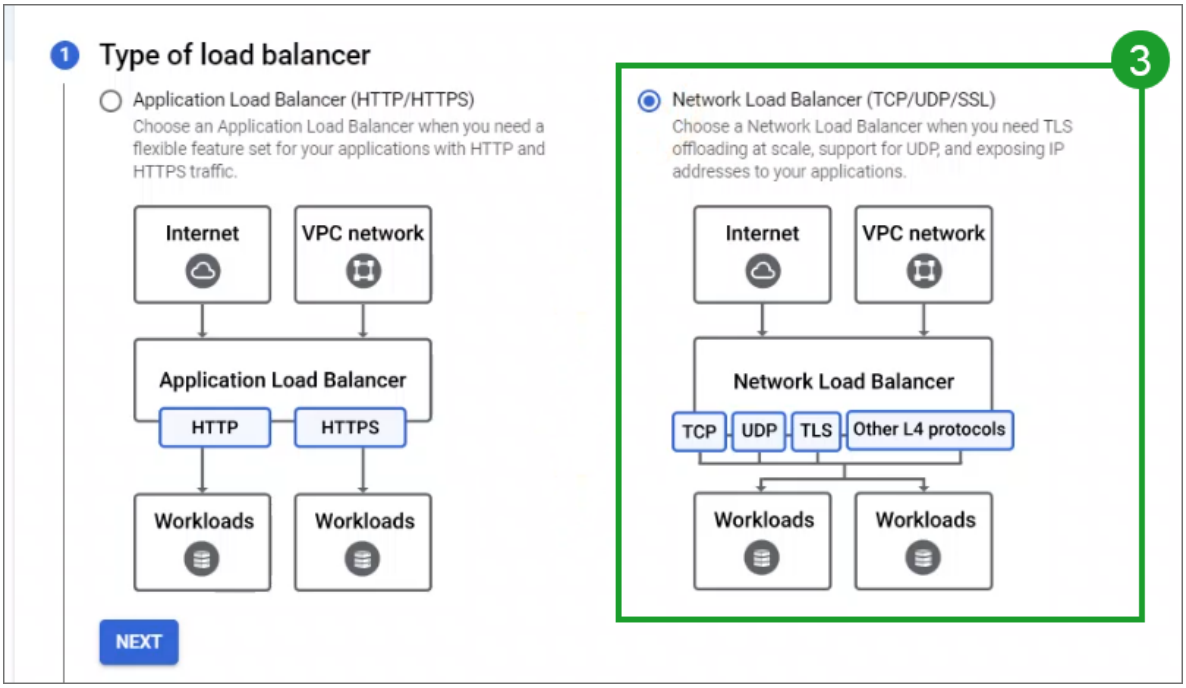
Your Instance Group is now created, and you can go to the next step to create a load balancer.

Step 3 - Create Load Balancer

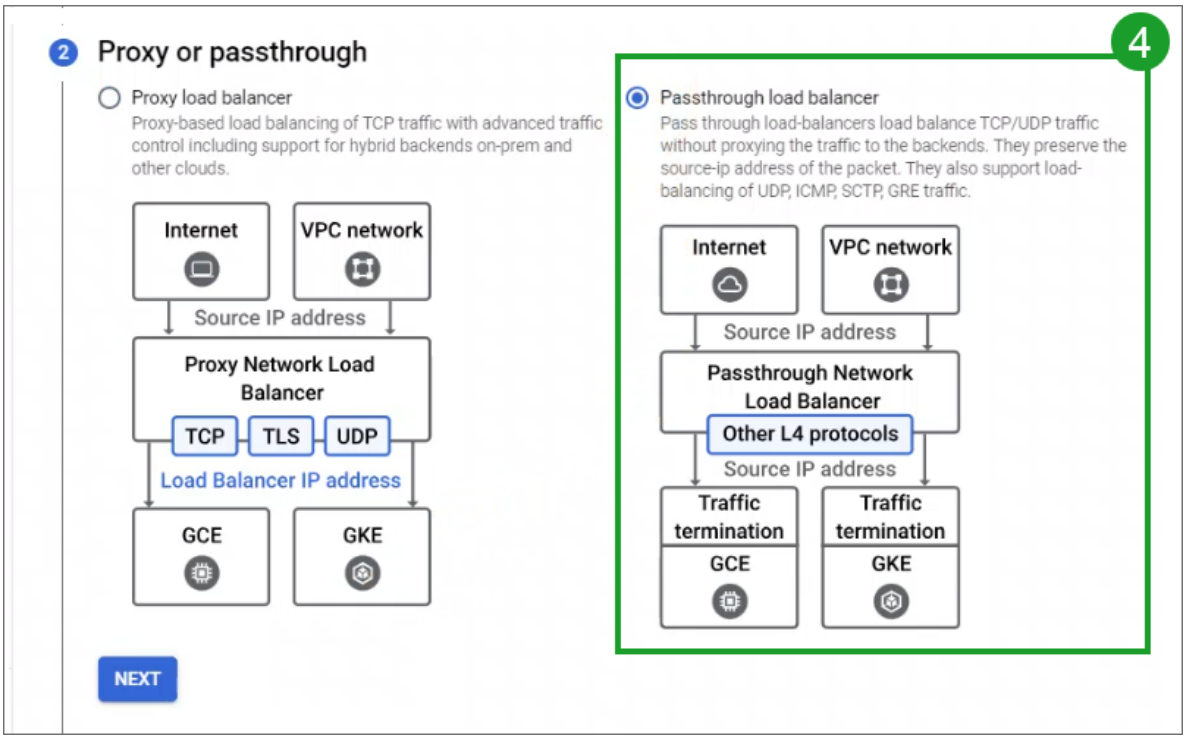
Reference: https://cloud.google.com/load-balancing/docs/https/ext-https-lb-simple#load-balancer

To create a load balancer, take the following steps.

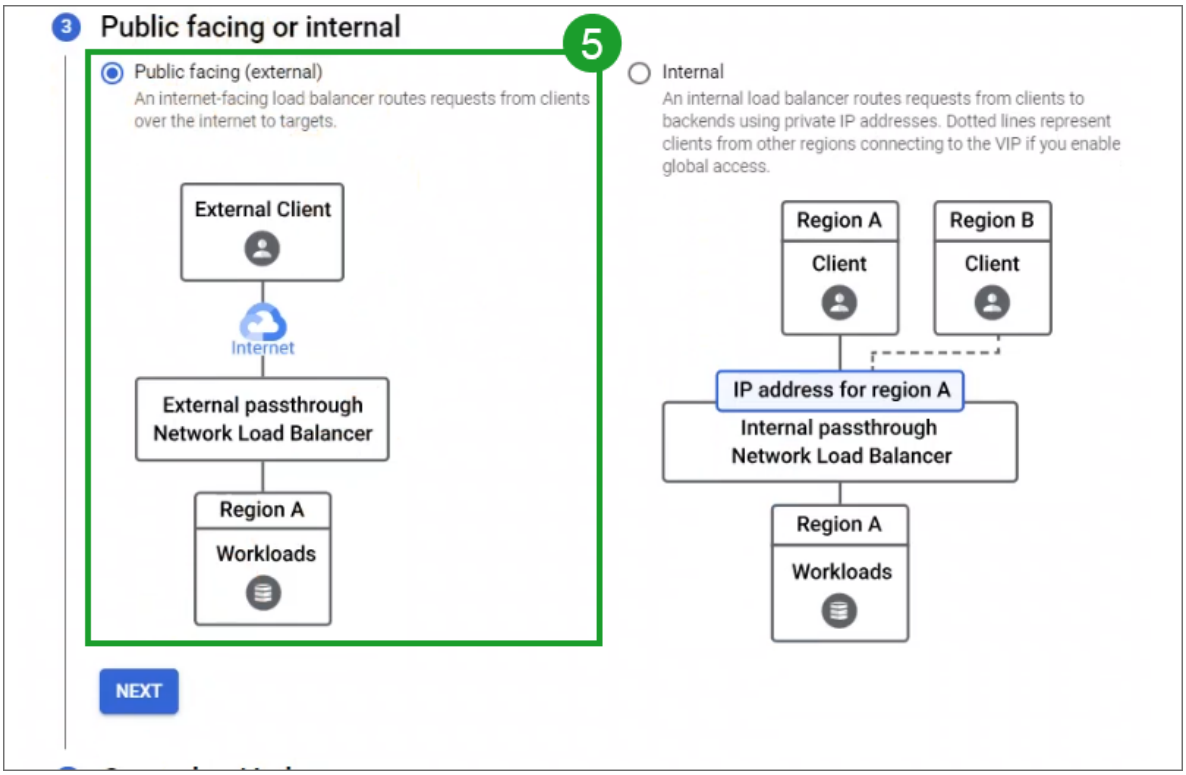
1. Use https://console.cloud.google.com/net-services/loadbalancing/list?_ga=2.221907288.1727950196.1712175609-895679178.1667947390.
   or
   Navigate to **Network services > Load balancing** .
2. Click **+CREATE LOAD BALANCER**.
3. Under **Type of load balancer**, select **Network Load Balancer (TCP/UDP/SSL)**, then click **NEXT**.



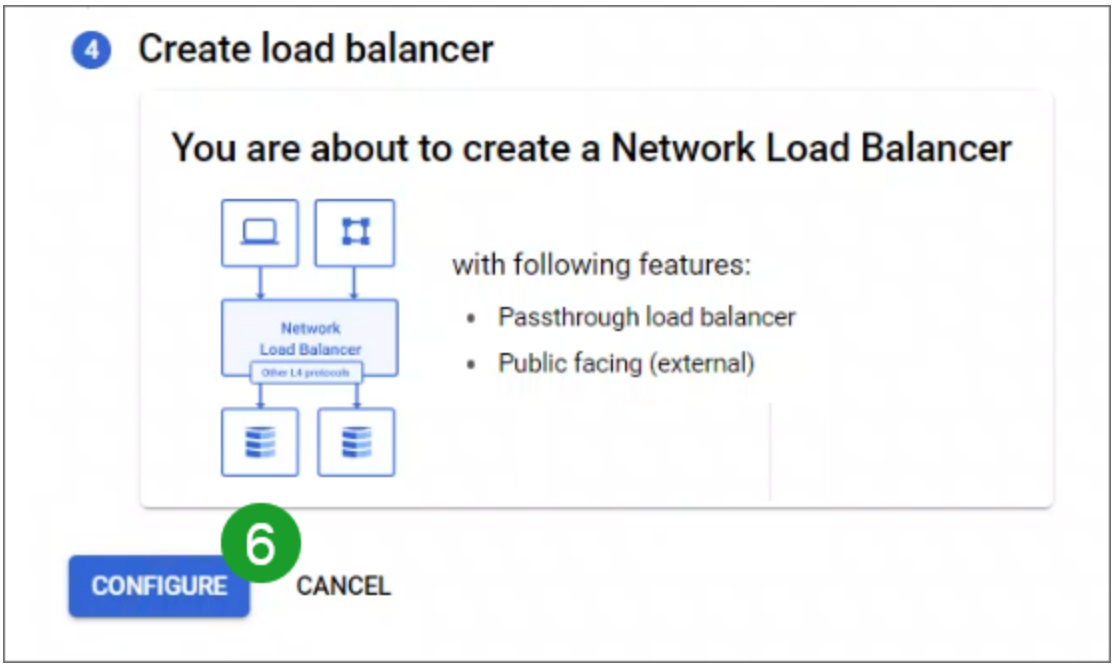
4. Under **Proxy or passthrough**, select **Passthrough load balancer**, and click **NEXT**.



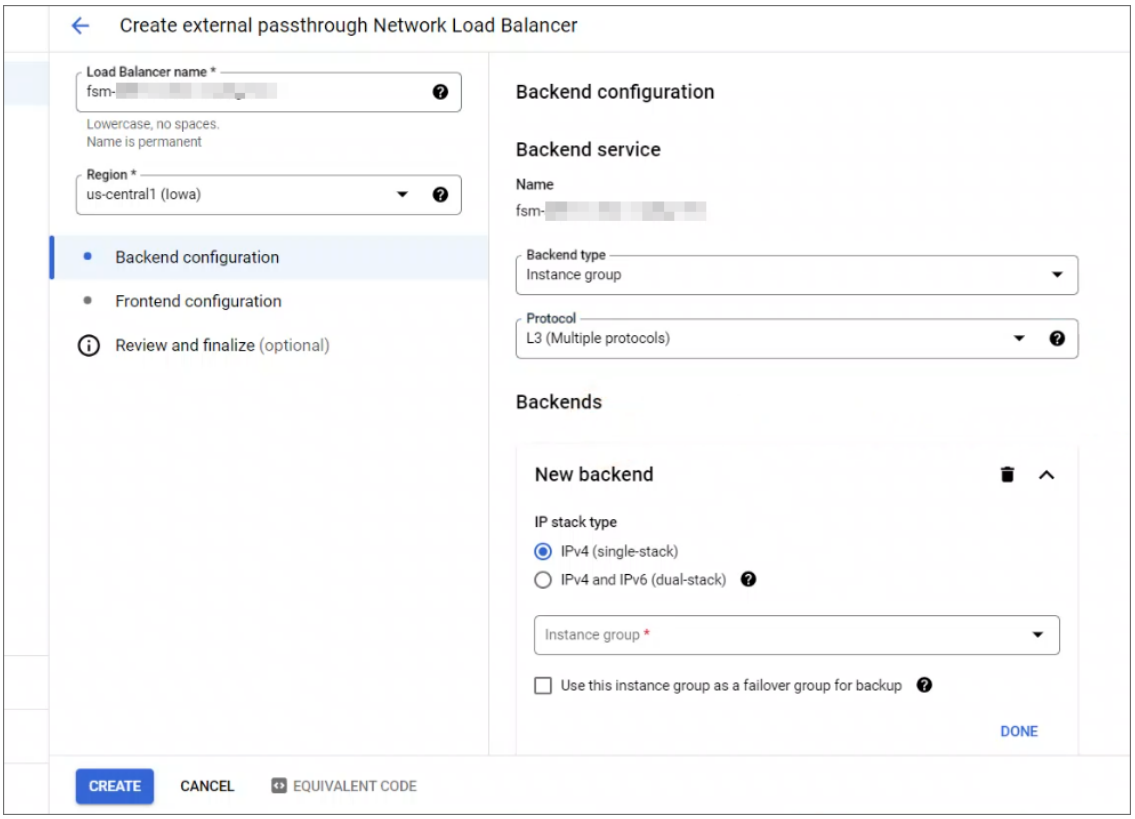
5. Under **Public facing or internal**, select **Public facing (external)** and click **NEXT**.



6. Click **CONFIGURE**.

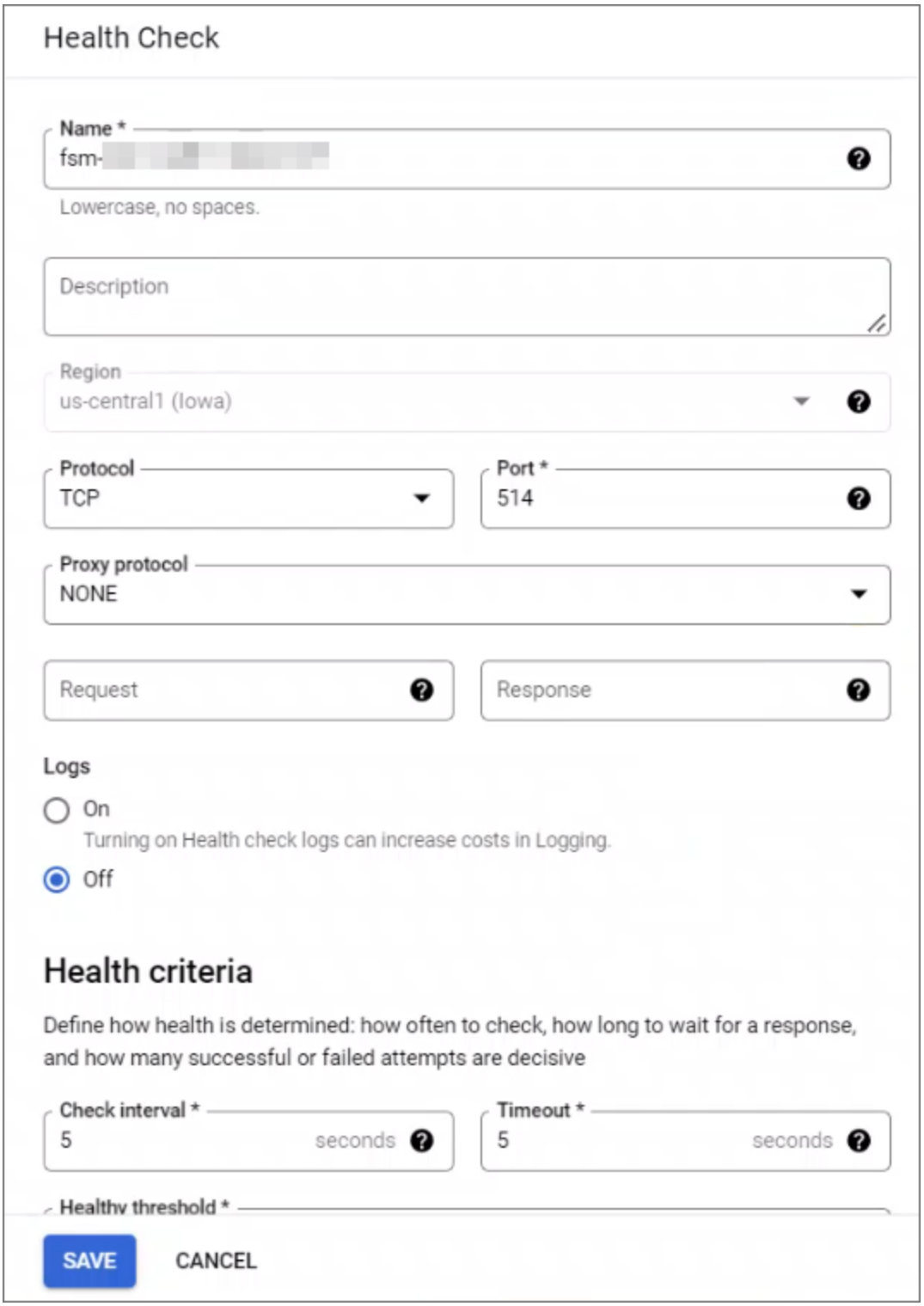


7. In the **Load Balancer name** field, enter a name for the load balancer.
8. From the **Region** drop-down list, select a region.
9. From the **Backend configuration** column, take the following steps.
   a. From the **Protocol** drop-down list, select **L3 (Multiple protocols)**.
   b. From the **Instance group** drop-down list, select the instance group you created in Create Instance Group, and click **DONE**.

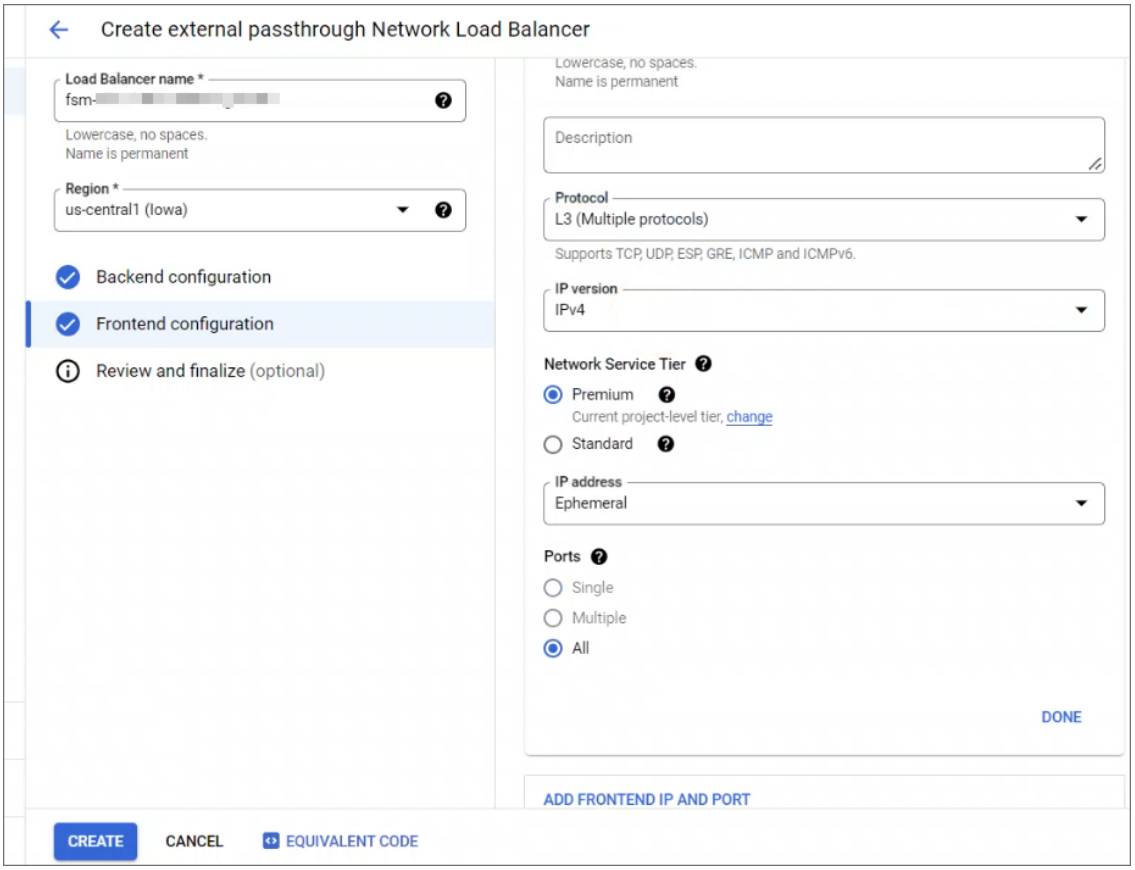


c. Click the **Health check** drop-down list.
d. Click **CREATE A HEALTH CHECK**.
e. From the **Health Check** window, take the following steps.
   i. In the **Name** field, enter a name for the health check.
   ii. From the **Protocol** drop-down list, select **TCP**.
   iii. In the **Port** field, enter "514".

iv. Click **SAVE**.

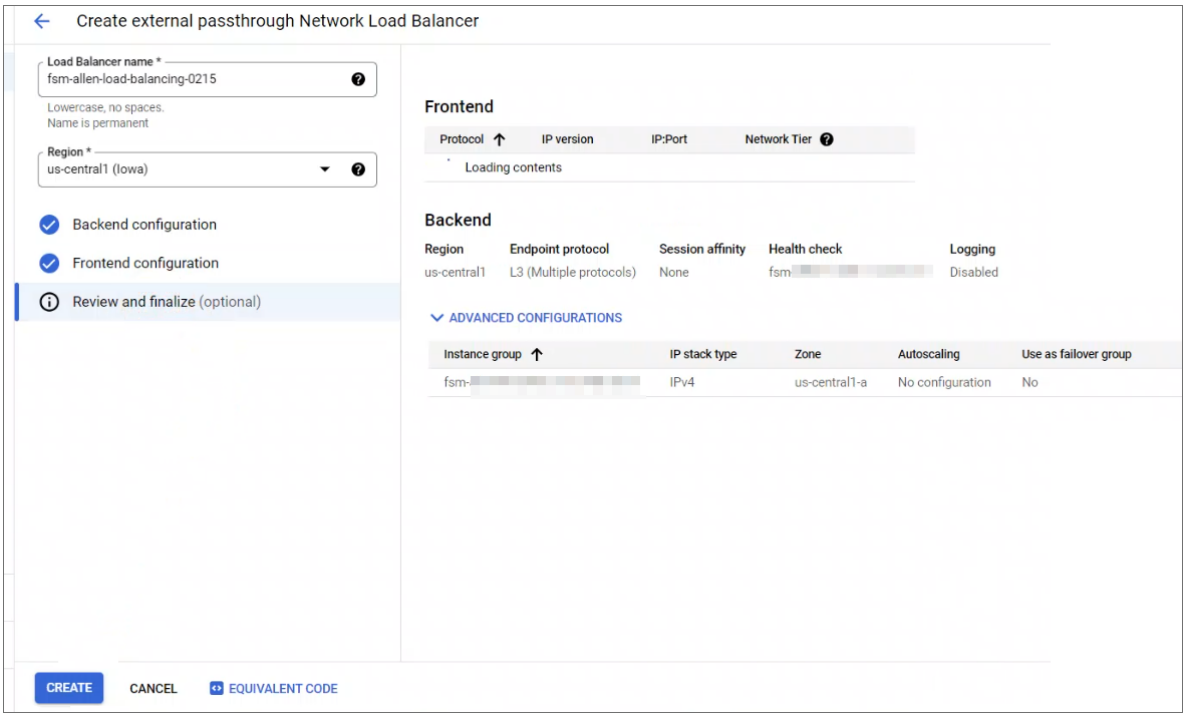


10. Select **Frontend configuration**.
    a. From the **Protocol** drop-down list, select **L3 (Multiple protocols)**.
    b. Click **DONE**.



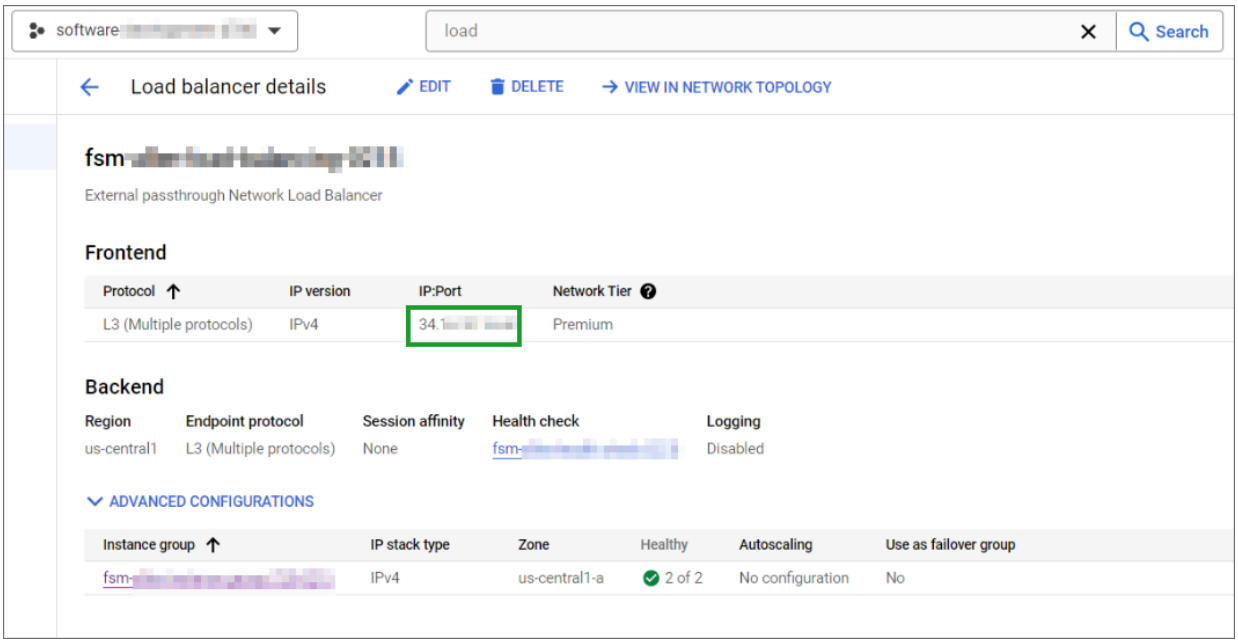
11. Click **Review and finalize**. You can review your configuration.

12. Click **CREATE**.



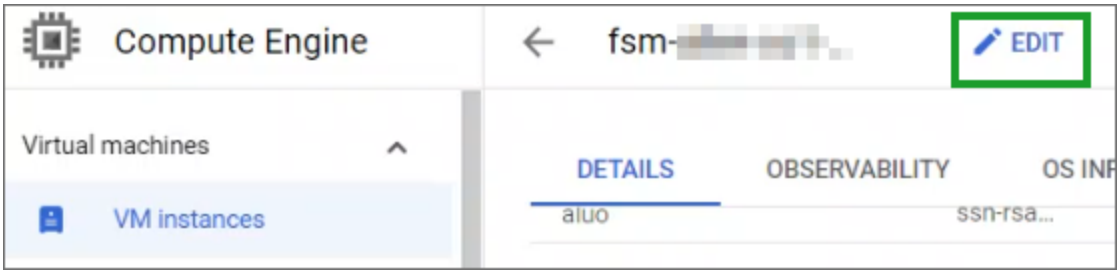
Step 4 - Check Load Balancer

Select your load balancer and confirm whether Collectors can receive data from Load balancer external IP. This IP address is displayed under the **IP:Port** column in the **Frontend** table. This is also the IP address you will need to use when configuring Collector HA in FortiSIEM.



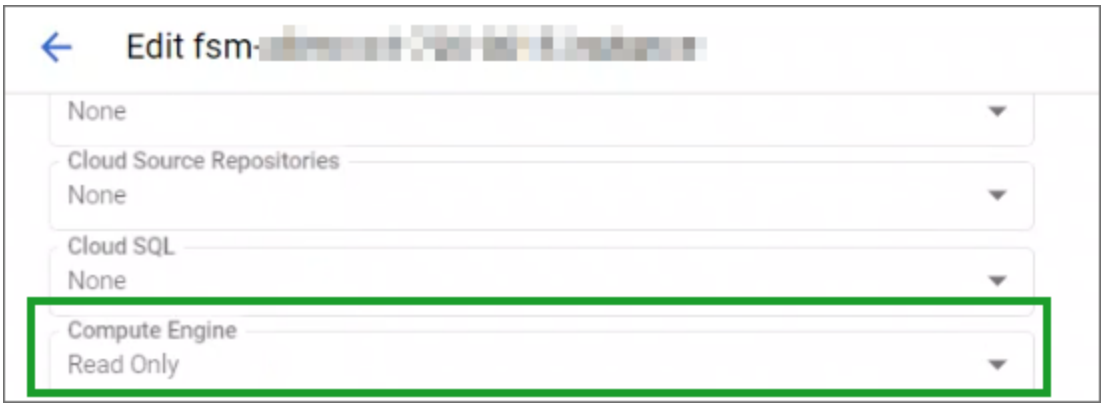
Step 5 - Configure Load Balancer to Report Health Status

1. Go to your VM instances, using https://console.cloud.google.com/compute/instances?_ga=2.191581290.1727950196.1712175609-895679178.1667947390/.
2. Select a Collector instance that you intend to use as part of your HA Collector group.
3. Shut down the instance, then click **EDIT**.
   Note: The instance must be shut down in order to edit.



4. Navigate to **Access scopes**, and locate **Compute Engine**.

5. From the **Compute Engine** drop-down list, select **Read Only**.



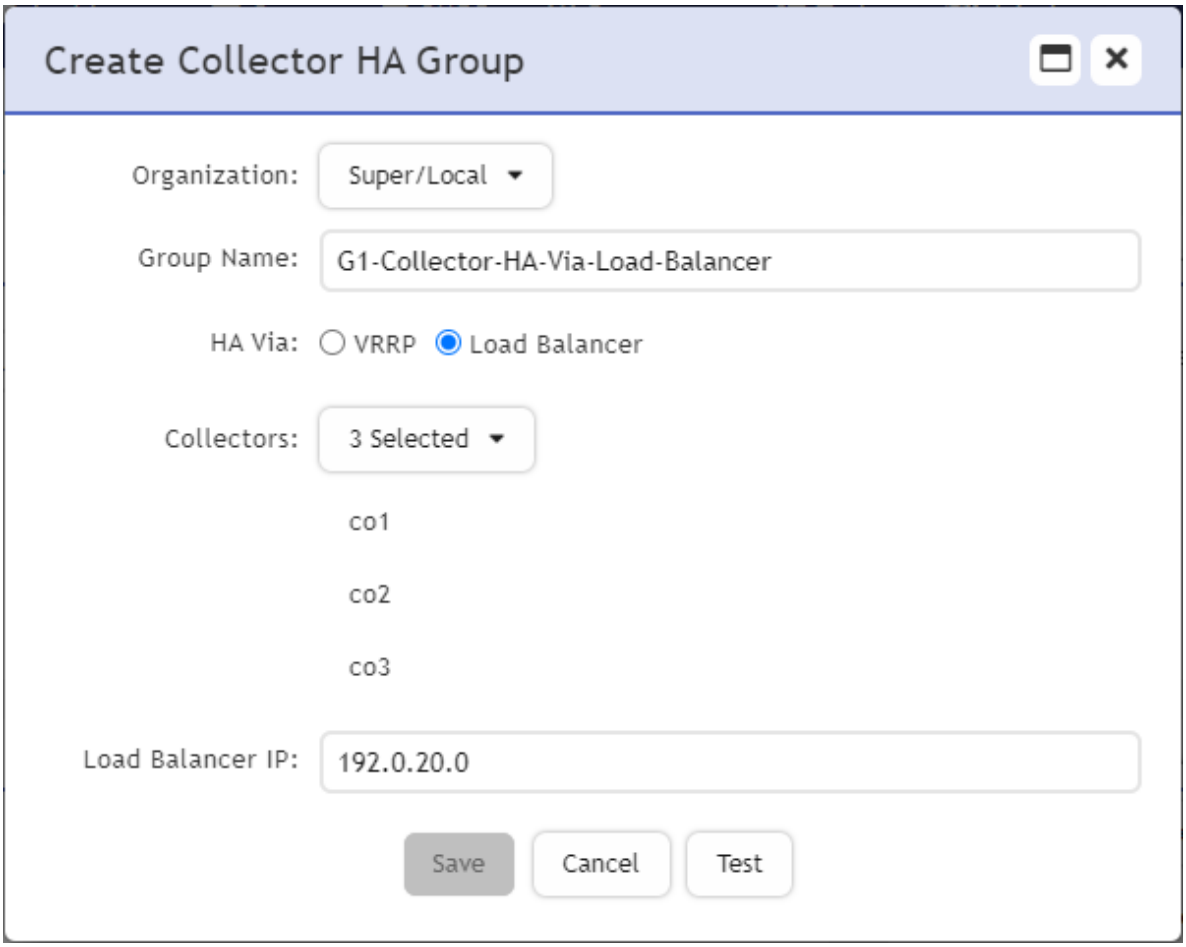
6. Click **SAVE**.
7. Repeat steps 2-6 for any additional collectors that are part of your load balancer.
   After all your collectors have **Compute Engine** configured to **Read Only**, your load balancer is now ready to report its health status.
8. Go to Configure Collector HA Via Load Balancer for FortiSIEM configuration.

Step 6 - Configure Collector HA Group Via Load Balancer

To create a new Collector High Availability configuration, take the following steps:

1. Navigate to **ADMIN > Settings > System > Cluster Config**.
2. Under **Collector High Availability**, click **New**. The **Create Collector HA Group** window appears. Take the following steps.
   a. From the **Organization** drop-down list, select your Organization.
   b. In the **Group Name** field, enter the name of your Collector group.
   c. From **HA Via**, select **Load Balancer**.
   d. From the **Collectors** drop-down list, select the Collectors to include in the group.
      Note: The available Collectors displayed are those from the same Organization selected earlier.
   e. In the **Load Balancer IP** field, enter the Load Balancer frontend IP address.
   f. Click **Test** to confirm it is working correctly. If it succeeds, proceed to the next step.

3. Click **Save**.


Create Collector HA Group
Organization:
Super/Local
Group Name:
G1-Collector-HA-Via-Load-Balancer
HA Via:
VRRP
Load Balancer
Collectors:
3 Selected
co1
co2
co3
Load Balancer IP:
192.0.20.0
Save
Cancel
Test

Non-Cloud Collector Deployments

This Case covers the situation where your Collectors are deployed on On-premise hypervisors, or on AWS, or they are hardware appliances. High Availability (HA) is enabled via Virtual Router Redundancy Protocol (VRRP). A Collector HA Cluster needs to be created with one Leader and one or more Followers and a Virtual IP (VIP) that is always owned by the Leader.

During normal operations:

- Logs sent to the VIP are handled by the Leader Collector (which owns the VIP).
- FortiSIEM Supervisor node distributes event pulling and performance monitoring jobs among all Collectors in the Cluster.

If the Leader Collector goes down:

- The Follower node with highest priority will become the Leader and own the VIP.
- Logs previously sent to the (failed) Leader Collector will automatically reach the new Leader Collector.
- FortiSIEM Supervisor node will automatically re-distribute event pulling and performance monitoring jobs previously assigned to the failed Leader Collector, to other Collectors in the HA Cluster.

If a Follower Collector goes down:

- App Server will distribute event pulling and performance monitoring jobs assigned to the failed Collector to other Collectors in the HA Cluster.
- If a failed Collector comes back up, then it will stay a Follower, but the event pulling jobs will be re-distributed among all the working Collectors in the HA Cluster.

Failure and Recovery:

- If the Leader Collector goes down then the Follower with the highest priority takes over. If the Leader Collector comes back up, then it will resume the Leader role due to its higher priority.
- If a Follower Collector goes down, the Leader will continue to operate. If the Follower comes back up, then it will remain a Follower while the Leader is operational.

- Step 1 - Configure Collectors
- Step 2 - Configure Collector HA Group Via VRRP
- Troubleshooting

Step 1 - Configure Collectors

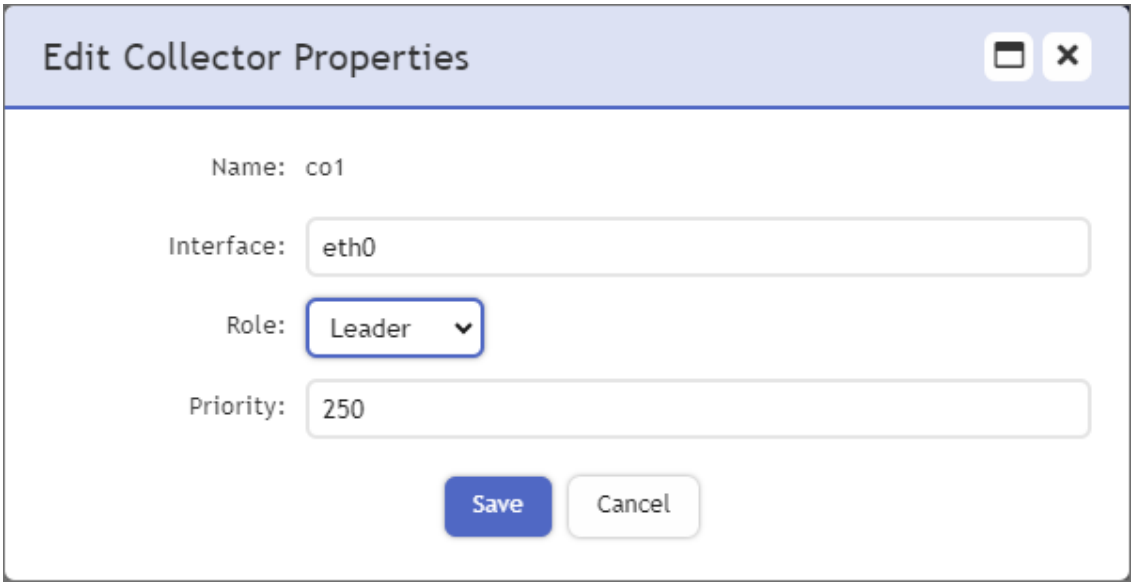
Configure Collectors as normal.

Step 2 - Configure Collector HA Group Via VRRP

To create a new Collector High Availability configuration, take the following steps:

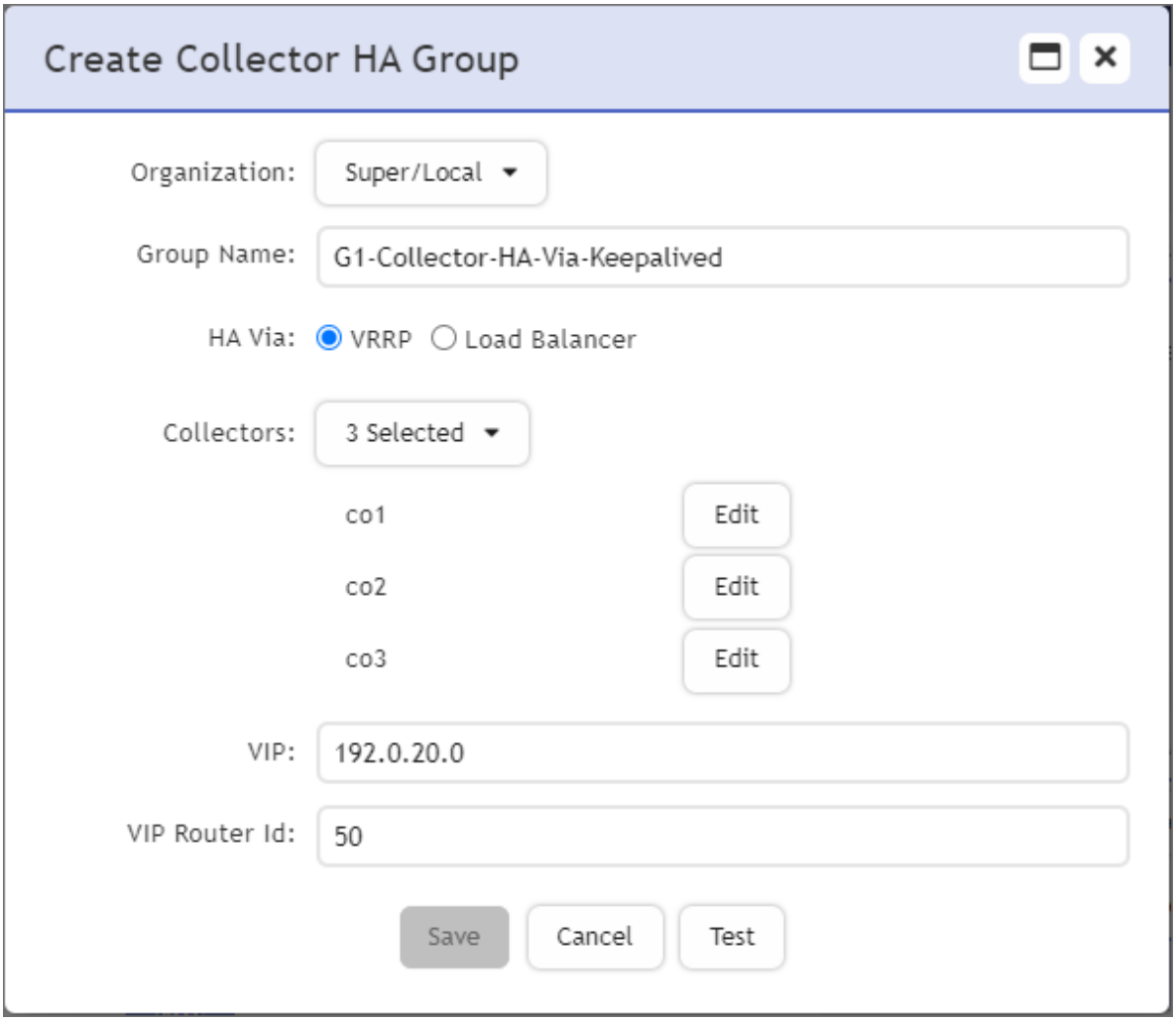
> Ensure that the VIP and Collectors in a Collector HA group are on the same network. This is required for High Availability to work.

1. Navigate to **Admin > Settings > System > Cluster Config**.
2. Under Collector High Availability, click **New**. The **Create Collector HA Group** window appears. Take the following steps.
   a. From the **Organization** drop-down list, select your Organization with your collectors.
   b. In the **Group Name** field, enter the name of your Collector group.
   c. From **HA Via**, select **VRRP**.
   d. From the **Collectors** drop-down list, select the Collectors to include in the group.
   Note: The available Collectors displayed are those from the same Organization selected earlier.
   e. In the **VIP** field, enter the Virtual Internet Protocol address.
   Note: This VIP can be internal.
   f. In the **VIP Router ID** field, enter the VIP Router ID number (1-255).
3. For each collector, click Edit, and take the following steps.
   a. In the **Interface** field, enter the name of the interface. For example, eth0.
   b. From the **Role** drop-down list, select the Collector's role (Leader, Follower).
   Note: Only one collector from the HA group can be assigned as a Leader.
   c. In the **Priority** field, enter the numeric priority of the Collector, with the high number being the greater priority (1-254).
   Note: The Collector Leader Priority should be higher than all of its Followers.
   d. Click **Save**.



e. Repeat step 3a-e for each Collector. When done, proceed to step 4.

4. Click **Test**. If the test succeeds, proceed to step 5. If it fails, check your earlier configurations.
5. Click **Save**.



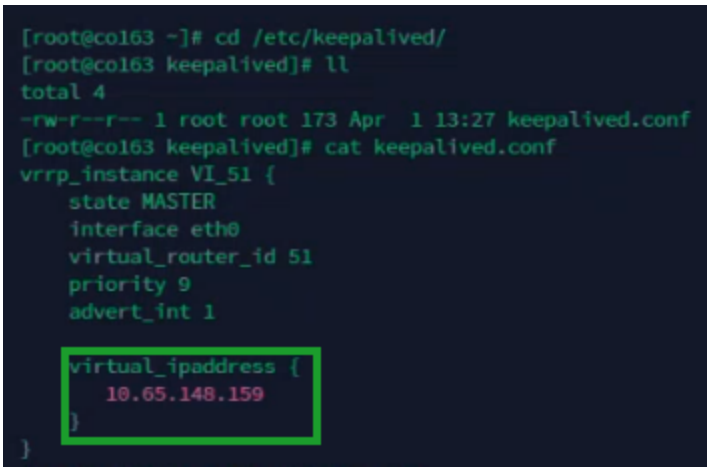
Troubleshooting

FortiSIEM creates the network for the Collector HA Group with the configuration provided. You can verify if the network has been set up correctly by checking the following.

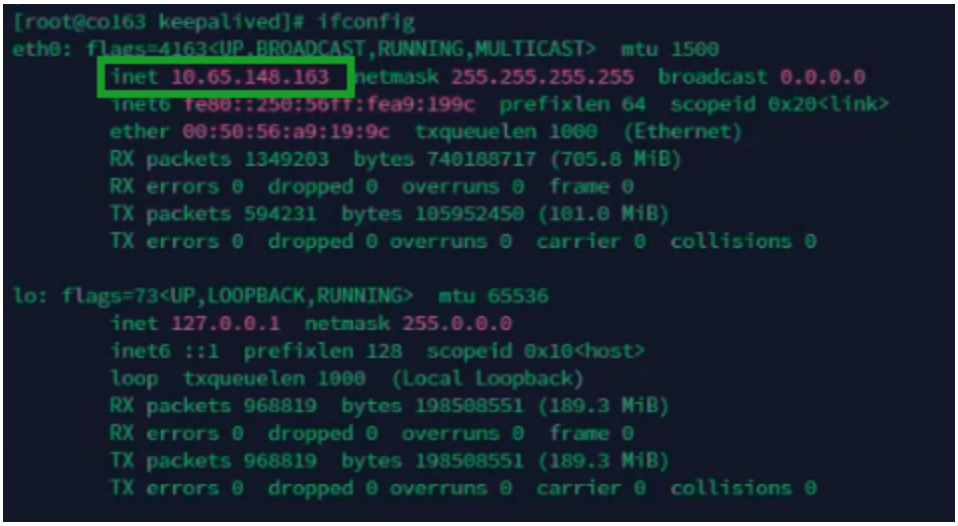
1. Check for the VIP address by executing an SSH to the Collector Leader, and run the following commands:
   a. `cd /etc/keepalived`
   b. `cat keepalived.conf`

   A virtual_ipaddress should appear.
   Example
   ...

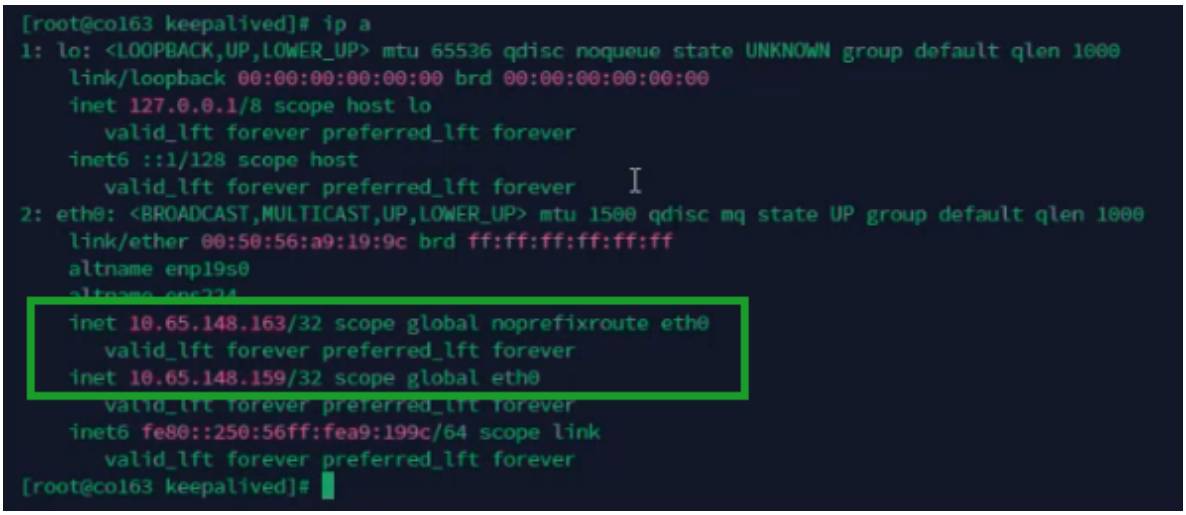
```
virtual_ipaddress {
10.65.148.159
}
...
```



2. Run `ifconfig` to check your physical IP address.



3. Next, run `ip a` to confirm that the physical IP address and virtual IP address are bound to your interface.


[root@co163 keepalived]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 00:50:56:a9:19:9c brd ff:ff:ff:ff:ff:ff
altname enp19s0
inet 10.65.148.163/32 scope global noprefixroute eth0
valid_lft forever preferred_lft forever
inet 10.65.148.159/32 scope global eth0
inet6 fe80::250:56ff:fea9:199c/64 scope link
valid_lft forever preferred_lft forever
[root@co163 keepalived]#

DB Cluster Configuration

The DB Leader is automatically selected. Select a DB Follower from the drop-down list. To add an additional DB Follower to select, click **+**. When your DB Cluster configuration is complete, enter the Virtual IP Address to use in the **VIP** field, then click **Save**.

Analytics Settings

The following section describes the procedures for Analytics settings:

- Scheduled Reports
  - Scheduling Report Alerts
  - Scheduling Report Copy
- Incident Notification
  - Setting Webhook Notification
  - Setting Incident HTTP Notification
  - Setting Incident SNMP Traps
  - Setting Remedy Notification
- Setting a Subcategory
- Setting Risk Filters
- Setting UEBA Higher Risk Entities
- UEBA Tags
- Tags
- ML / AI

Scheduled Reports

Scheduled Reports allows you to schedule report notifications when a scheduled report is run, and also send a copy of a report to a remote location when a scheduled report is sent.

- Scheduling Report Alerts
- Scheduling Report Copy

Scheduling Report Alerts

You can schedule reports to run and send email notifications to specific individuals. This setting is for default email notifications that will be sent when any scheduled report is generated.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Scheduled Report** tab.
2. Select the required action under **Scheduled Report Alerts** section.
   - **Do not send scheduled emails if report is empty** - Sometimes a report may be empty because there are no matching events. If you don't want to send empty reports to users, select this option. If you are running a multi-tenant deployment, and you select this option while in the Super/Global view, this will apply only to Super/Global reports. If you want to suppress delivery of empty reports to individual Organizations, configure this option in the Organizational view.

3. Enter the email address in **Deliver notification via** filed. Click **+** to add more than one email address, if needed.
4. Click **Save**.
5. To receive email notifications, go to **ADMIN** > **Settings** > **System** > **Email** and configure your mail server.

Scheduling Report Copy

Reports can be copied to a remote location when the scheduler runs any report. Note that this setting only supports copy to Linux remote directory.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Scheduled Report** tab.
2. Enter the following information under **Scheduled Report Copy** section.
3. Enter the **Host** - IP address or name.
4. Enter the **Path** - absolute path, such as `/abc/def`.
5. Enter the **User Name** and **Password**, and enter **Confirm Password** to reconfirm the password.
6. Click **Test** to check the connection.
7. Click **Save**.

Note: For all of the above configurations, use the **Edit** button to modify any setting or **Delete** to remove any setting.

Incident Notification

Incident Notification allows you configure incident notifications in the following ways.

- Webhook Notification
- Incident HTTP Notification
- Incident SNMP Traps
- Remedy Notification

Webhook Notification

You can configure a webhook notification using application by taking the following steps.

1. Navigate to **Admin > Settings > Analytics > Incident Notification**.
2. Under **Webhook Notification**, click **New**.
3. In the **Name** field, enter a name for the Webhook notification.
4. From the **Application** drop-down list, select the Webhook Notification utilizing application.
5. In the **URL** field, enter the webhook URL. Ensure you include "https://" or "http://" as part of the URL.
6. (Optional) In the **Description** field, enter a description for the webhook notification.
7. Click **Save**.

Notifications will be sent by the application if added to your Automation Policy using the "Send Email/SMS/Webhook to the target users" Action. See here for more information.

Setting Incident HTTP Notification

You can configure FortiSIEM to send an XML message over HTTP(s) when an incident is triggered by a rule.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Incident Notification** tab.
2. Enter the following information under **Incident HTTP Notification** section.
3. For **HTTP(S) Server URL**, enter the URL of the remote host where the message should be sent.
4. Enter the **User Name** and **Password** to use when logging in to the remote host, and enter **Confirm Password** to reconfirm the password.
5. Click **Test** to check the connection.
6. Click **Save**.

Incidents are sent out in XML format. For details, see here.

Setting Incident SNMP Traps

You can define SNMP traps that will be notified when an event triggers an incident.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Incident Notification** tab.
2. Enter the following information under **Incident SNMP Traps** section.
   a. **SNMP Trap IP Address**
   b. **SNMP Community String** - to authorize sending the trap to the SNMP trap IP address.
3. Select the **SNMP Trap Type** and **SNMP Trap Protocol** options.
4. Click **Test** to check the connection.
5. Click **Save**.

For the SNMP MIB definition, see here.

Setting Remedy Notification

You can set up Remedy to accept notifications from FortiSIEM and generate tickets from those notifications.

Configuring Remedy to Accept Tickets from FortiSIEM Incident Notifications

Before configuring Remedy to accept tickets, make sure you have configured the Remedy Notifications in FortiSIEM.

1. In Remedy, create a new form, **FortiSIEM_Incident_Interface**, with the incident attributes listed in the table at the end of this topic as the form fields.

2. When you have defined the fields in the form, right-click the field and select the **Data Type** that corresponds to the incident attribute.
3. After setting the form field data type, click in the form field again to set the **Label** for the field.
4. When you are done creating the form, go to **Servers** > **localhost** > **Web Service** in Remedy, and select **New Web Service**.
5. For **Base Form**, enter **FortiSIEM_Incident_Interface**.
6. Click the **WSDL** tab.
7. For the **WSDL Handler URL**, enter `http://<midtier_server>/arsys/WSDL/public/<servername>/FortiSIEM_Incident_Interface`.
8. Click the **Permissions** tab and select **Public**.
9. Click **Save**.

You can test the configuration by opening a browser window and entering the WSDL handler URL from step 7 above, substituting the Remedy Server IP address for `<midtier_server>` and `localhost` for `<servername>`. If you see an XML page, your configuration was successful.

Incident Attributes for Defining Remedy Forms

Incident Attribute	Data type	Description
biz_service	text	Name of the business services affected by this incident
cleared_events	text	Events which cleared the incident
cleared_reason	text	Reason for clearing the incident if it was cleared
cleared_time	bigint	Time at which the incident was cleared
cleared_user	character varying (255)	User who cleared the incident
comments	text	Comments
cust_org_id	bigint	Organization id to which the incident belongs
first_seen_time	bigint	Time when the incident occurred for the first time
last_seen_time	bigint	Time when the incident occurred for the last time
incident_count	integer	Number of times the incident triggered between the first and last seen times
incident_detail	text	Incident Detail attributes that are not included in incident_src and incident_target
incident_et	text	Incident Event type
incident_id	bigint	Incident Id
incident_src	text	Incident Source
incident_status	integer	Incident Status
incident_target	text	Incident Target
notif_recipients	text	Incident Notification recipients
notification_action_status	text	Incident Notification Status
orig_device_ip	text	Originating/Reporting device IP
ph_incident_category	character varying (255)	FortiSIEM defined category to which the incident belongs: Network, Application, Server, Storage, Environmental, Virtualization, Internal, Other

Incident Attribute	Data type	Description
rule_id	bigint	Rule id
severity	integer	Incident Severity 0 (lowest) - 10 (highest)
severity_cat	character varying (255)	LOW (0-4), MEDIUM (5-8), HIGH (9-10)
ticket_id	character varying (2048)	Id of the ticket created in FortiSIEM
ticket_status	integer	Status of ticket created in FortiSIEM
ticket_user	character varying (1024)	Name of the user to which the ticket is assigned to in FortiSIEM
view_status	integer	View status
view_users	text	View users

Complete these steps to set up the routing to your Remedy server.

1. Go to **ADMIN** > **Settings** > **Analytics** > **Incident Notification** tab.
2. Enter the following information under **Remedy Notification** section.
3. For **WSDL**, enter the URL of the Remedy Server.
4. Enter the **User Name** and **Password** associated with your Remedy server, and enter **Confirm Password** to reconfirm the password.
5. Click **Test** to check the connection.
6. Click **Save**.

Setting a Subcategory

FortiSIEM Incidents are grouped into different categories – Availability, Change, Performance, Security and Other. A Category is assigned to every Rule and you can search any Incidents using these Categories. FortiSIEM extends this concept to include Subcategories. A Subcategory is defined for every system-defined rule. You can add a Subcategory for custom rules and also create new Subcategories. Incidents can be searched using both Categories and Subcategories.

Creating a Subcategory

1. Go to **ADMIN > Settings > Analytics > Subcategory**.
2. Select the **Category** from the left-hand panel where you want to create a Subcategory.
3. Click **Add** in the right-hand panel.
4. Enter a name for the new Subcategory.
5. Click the checkmark icon or click **Save All**.

Modifying a Subcategory

You can modify only user-defined Subcategories. You cannot modify system-defined Subcategories.

1. Select the Subcategory you want to modify.
2. Click the edit icon.
3. Modify the name in the **Subcategory** field.
4. Click the checkmark icon or **Save All**.

Deleting a Subcategory

You can delete only user-defined Subcategories. You cannot delete system-defined Subcategories.

1. Select the Subcategory you want to delete.
2. Click the **-** icon.
3. Click **Save All**.

Setting Risk Filters

A Risk Filter allows you to include or exclude certain rules from the Risk Score calculation. For more information on Risk Scores, see Risk View. (Note we also have an Entity Risk Score topic which is empty)

In the SP model, you can create a global Risk Filter or filters for individual organizations. A global Risk Filter can include only system rules, and is available to all organizations. You can create only one Risk Filter for an organization. Multiple filters are not allowed. This Risk Filter includes the filter defined for the organization itself and the global filter if one exists.

The VA model allows only one filter.

The Risk Filter view contains a table with three columns. The **Scope** column lists the organization the filter belongs to. The **Included Rules** column lists the rules that will be included in the calculation of the risk score. The **Excluded Rules** columns lists the rules that will not be included in the calculation of the Risk Score.

Creating a Risk Filter

Follow these steps to create a Risk Filter.

1. Go to **ADMIN > Settings > Analytics > Risk Filter** to open the Risk Filter view.
2. Click **New**.
3. In the New Risk Filter dialog box, select **Super/Local** or the name of an organization from the **Add filter for** drop-down list.
4. Click **Next**.
5. In the next dialog box, **Include** is selected by default. Open the **Rules** tree under **Groups** and shuttle the rules you want to include in the filter from the **Rules** column to the **Selection** column.
6. Select **Exclude** and repeat the process described in the previous step to exclude rules from the filter.
7. Click **Save**. Your rule selections will appear in the **Included Rules** and **Excluded Rules** columns of the table.

Editing a Risk Filter

Follow these steps to edit a Risk Filter.

1. Go to **ADMIN > Settings > Analytics > Risk Filter** to open the Risk Filter view.
2. Click **Edit**.
3. In the dialog box, **Include** is selected by default. Shuttle the rules you do not want to be included in the Risk Score from the **Selection** column to the **Rules** column.
4. Select **Exclude** and repeat the process described in the previous step to exclude rules from the filter.
5. Click **Save**.

Deleting a Risk Filter

Follow these steps to delete a Risk Filter.

1. Go to **ADMIN > Settings > Analytics > Risk Filter** to open the Risk Filter view.
2. Select the row in the table containing the filter you want to delete.
3. Click **Delete**.

Viewing Risk Filter Results

To see the impact of the filters you defined, go to **INCIDENTS**. Click the Risk icon (Risk) to open the Risk View. For a description of the Risk View, see Risk View.

Tags

Tags allow you to create a keyword or phrase, the "tag", that can be associated with rules that trigger incidents. After creating a tag, you associate it with a rule (See Creating a Rule: Step 3: Define Actions). After this configuration, you can view tags on the Incidents List View page by doing any of the following.

- Add the **Tag** column to view tags that were part of a rule triggered incident.
- Search for tag related incidents by including **Incident Tag** as part of your search.

Creating a Tag

Follow these steps to create a new tag.

1. Navigate to **ADMIN > Settings > Analytics > Tags**.
2. Click **New**.
3. In the **Add New Tag** window, take the following steps:
   a. In the **Tag** field, enter your the name of the tag you wish to create.
   b. In the **Color** field, select a color for the tag: Red, Yellow, or Green.
   c. (Optional) In the **Description** field, add any information you wish to convey about the tag, such as its intent.
   d. When done, click **Save**.

At this point, you tag will be saved, and be available from the Tags drop-down list when creating or editing a Rule.

Editing a Tag

Follow these steps to edit a tag.

1. Navigate to **ADMIN > Settings > Analytics > Tags**.
2. Select the tag you wish to edit, and click **Edit**.
3. In the **Edit Tag: *<Name of Tag>*** window, make any changes to the **Tag**, **Color**, and **Description** fields.
4. When done, click **Save**.

Deleting a Tag

Follow these steps to delete a tag.

1. Navigate to **ADMIN > Settings > Analytics > Tags**.
2. Select the tag you wish to delete.
3. Click **Delete**.

ML / AI

- General Configuration
- Configuring AWS ML
- Configuring FortiAI

General Configuration

To configure FortiAI to automatically clear incidents within a certain percentage, take the following steps.

1. Navigate to **Admin > Settings > Analytics > ML / AI**.
2. Click on the **General** tab.
3. In the percentage field, enter the percentage to be applied to automatically clear incidents.
4. Check the **Auto Clear Incidents** check box.
5. Click **Save** to save the configuration.

Configuring AWS ML

See Cloud Machine Learning for set up.

Configuring FortiAI

To configure FortiAI, take the following steps.

1. Navigate to **Admin > Settings > Analytics > ML / AI**.
2. Click on the **FortiAI** tab.
3. In the **ChatGPT Key** field, enter your ChatGPT Key.
4. Click **Save** to save the configuration.

UEBA Settings

The AI module runs on Super and Worker nodes. All Agent activity is routed to one node in a sticky manner. If a Worker is down, Agent events are routed to another Worker. If a Worker is added, then new Agents are routed to that Worker. Additionally, AI models are now persisted across AI module restarts.

AI alerts can be monitored in the **UEBA** View in the **INCIDENTS** page. See UEBA View.

- Setting UEBA Higher Risk Entities
- Setting UEBA Tags

Setting UEBA Higher Risk Entities

UEBA Higher Risk Entities allow you to prioritize AI alerts that are most relevant to you by increasing the weight of events to High. This weighting will influence the AI model, similar to UEBA Tags. You can identify high-risk or business-critical entities, including file types, file paths, users, and groups.

Follow these steps to specify important entities:

1. Click **ADMIN > Settings > Analytics > UEBA Higher Risk Entities**.
2. The **UEBA Higher Risk Entities** dialog box contains the following fields. All of the fields are optional. In each field, use the **+** and **-** buttons to add or remove entries.
   - **File Types** - Enter the type of file you want to monitor, for example, `.exe`.
   - **File Paths** - Enter the path to the folder you want to monitor.
   - **User Accounts** - Enter the name of the Windows Agent-side user account you want to monitor.
   - **Group Names** - Enter the name of the Windows Agent-side group you want to monitor.
3. Click **Save**.

Setting UEBA Tags

AI inspects the events for specific characteristics, as defined in the AI tag definitions, and applies the appropriate tags to events that match.

Follow these steps to set tags:

1. Click **ADMIN > Settings > Analytics > UEBA Tags**.
2. Provide values for the following fields:
   a. **Enabled** - Select this option to allow FortiSIEM to monitor the alert.
   b. **ID** (required) - A user-defined ID. Only these characters are allowed: **a-z**, **A-Z**, **0-9**, and the underbar character (**_**).

c. **Name** (required) - The user-defined name for the entity. Only these characters are allowed: **a-z**, **A-Z**, **0-9**, and white space.
d. **Description** - An optional description of the alert.
e. **Weight** - Select a value from the drop-down list. The values can range from **Never Alert** (-5) to **Always Alert** (+5).
f. **Rules**
    i. **Field** - Choose a value from the drop-down list. Available values are **Machine ID**, **User**, **Application**, **Activity**, **Resource**, and **Resource Filename**.
    ii. **Relation** - Choose a value from the drop-down list. Available values are **=**, **!=**, **CONTAIN**, **NOT CONTAIN**, **MATCH**, **NOT MATCH**, **START WITH**, **NOT START WITH**, **END WITH**, and **NOT END WITH**.
    iii. **Value** - A comma-separated list of values. These values can be user-defined.
    iv. Click **+** or **-** to add or delete rows in the **Rules** list.

3. Click **Save**.

Cloud Machine Learning

This document describes how to configure AWS SageMaker for running FortiSIEM Machine Learning jobs in AWS.

- Set Up AWS SageMaker
- Configure FortiSIEM to use AWS SageMaker
- Other Tasks
  - Checking AWS SageMaker Training Job Status
  - Checking AWS SageMaker Hyperparameter Tuning Job Status
  - Checking AWS SageMaker Inference Job Status
- Implementation Notes
  - AWS Auto Mode Running Time

Set Up AWS SageMaker

To set up AWS SageMaker, take the following steps.

Step 1: Create an AWS Account

If you already have an AWS account, proceed to Step 2. Make sure you have your AWS account ID for the next step.

To create an AWS account, navigate to https://portal.aws.amazon.com/billing/signup, follow the instructions there, and record your AWS account ID for use in Step 2.

Step 2: Create an IAM Administrator User and Group

When you create an AWS account, you get a single sign-in identity that has complete access to all of the AWS services and resources in the account. This identity is called the AWS account root user. Signing in to the AWS console using the email address and password that you used to create the account gives you complete access to all of the AWS resources in your account. Fortinet strongly recommends that you not use the root user for everyday tasks, even administrative ones. Instead, adhere to the Security best practices in IAM.

To create an administrator user, follow the instructions here: Creating Your First IAM User and Administrators Group.

Step 3: Create SageMaker Execution Role and Policy

To create a SageMaker execution role and policy, take the following steps.

1. Open your IAM console at https://console.aws.amazon.com/iam/.
2. In the left pane, under **Access management**, select **Roles**, then click **Create role**.
3. Click on the **SageMaker** drop-down list, select **SageMaker - Execution**, then click **Next** to go to "Step 2 Add permissions".

4. Select **Next** to go to "Step 3 Name, review, and create".
   Note: The IAM managed policy, AmazonSageMakerFullAccess, is automatically attached to the role being created. To see the permissions included in this policy, click the carat next to the policy name.
5. In the **Role name** field, enter a name for the role, then click **Create role**.
6. On the Roles section of the IAM console, select the role you just created.
   Note: You can locate your role name by entering it partially in the *Search* field.
7. Select **Add permissions**, then click **Create inline policy**.
8. Click **Choose a service**.
9. In the **Service** field, enter "s3", then select s3.
10. Under **Actions**, under **Access level**, select **List**, **Read** and **Write**.
11. Under **Resources**, locate **bucket**, check the **Any** checkbox, then click **Review policy**.
12. Under **Review policy**, in the **Name** field, enter the name of your policy, then click **Create policy**.

Configure FortiSIEM to use AWS SageMaker

Note: Ensure Amazon SageMaker is set up first.

To configure AWS for Cloud Machine Learning, take the following steps:

1. Navigate to **Admin > Settings > Analytics > ML / AI**.
2. Click on the **AWS ML** tab.
3. In the **Access Key** field, enter the Access Key for your AWS Cloud account.
4. In the **Secret Access Key** field, enter the Secret Access Key of your AWS Cloud account.
5. In the **Region** field, enter the region where your AWS resides.
6. In the **S3 Bucket** field, enter the S3 bucket.
7. In the **SageMaker Execution Role** field, enter the SageMaker Execution role.
8. Click **Test**, to test the configuration.
9. If Test is successful, click **Save**.

Other Tasks

- Checking AWS SageMaker Training Job Status
- Checking AWS SageMaker Hyperparameter Tuning Job Status
- Checking AWS SageMaker Inference Job Status

Checking AWS SageMaker Training Job Status

To monitor your SageMaker training jobs, take the following steps.

1. Navigate to https://console.aws.amazon.com/sagemaker/.
2. In the left navigation pane, expand **Training**, select **Training jobs**, and from the center pane, choose the relevant task name.

Checking AWS SageMaker Hyperparameter Tuning Job Status

To check on the status of your SageMaker Hyperparameter tuning jobs, take the following steps.

1. Navigate to https://console.aws.amazon.com/sagemaker/.
2. In the left navigation pane, expand **Training**, select **Hyperparameter tuning jobs**, and from the center pane, choose the relevant task name.

Checking AWS SageMaker Inference Job Status

1. Navigate to https://console.aws.amazon.com/sagemaker/.
2. In the left navigation pane, expand **Inference**, select **Batch transform jobs**, and from the center pane, choose the relevant task name.

Implementation Notes

- AWS Auto Mode Running Time

AWS Auto Mode Running Time

Training time for AWS Auto mode is relatively long and only suitable for large amounts of data (e.g. more than 20K rows).

Discovery Settings

This section describes the procedures for the following Discovery settings:

- Generic
- Device Filter
- Application Filter
- Location
- CMDB Groups

Generic

Before you initiate discovery, you should configure the Discovery Settings in your Supervisor as required for your deployment.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Generic** tab.
2. Enter the following information under **Generic Settings** section. In a SP deployment, you must define all these settings for each Organization by logging in to the Organization directly.

Setting	Description
Virtual IPs	Often a common virtual IP address will exist in multiple machines for load balancing and fail-over purposes. When you discover devices, you must have these virtual IP addresses defined within your discovery settings for two reasons: • Listing the virtual IP addresses ensures that two or more devices with the same virtual IP will not be merged into one device during device discovery, so each of the load-balanced devices will maintain their separate identity in the CMDB • The virtual IP will not be used as an access IP during discovery, since the identity of the device when accessed via the virtual IP is unpredictable Enter the **Virtual IP** and click **+** to add more, if required.
Excluded Shared Device IPs	An enterprise often has servers that share credentials, for example mail servers, web proxies, and source code control servers, and a large number of users will authenticate to these servers to access their services. Providing a list of the IP addresses for these servers allows FortiSIEM to exclude these servers from user identity and location calculations in

Setting	Description
	the **Analytics** > **IdentityandLocation** report. For example, suppose user A logs on to server B to retrieve his mail, and server B authenticates user A via Active Directory. If server B is not excluded, the **Analytics > Identity and Location Report** will contain two entries for user A: one for the workstation that A logs into, and also one for server B. You can eliminate this behavior by adding server B to the list of Server IPs with shared credentials. Enter the **Excluded Shared Device IPs** and click **+** to add more, if required.
Virtual Device Hardware Serial Numbers	If two or more devices have identical hardware serial number, specify them here. In general, hardware serial number is used to uniquely identify a device and therefore two devices with identical hardware serial number is merged into a single device in CMDB. If a hardware serial number is present in the Virtual Hardware Serial Numbers list, then it is excluded for merging purposes. Enter the **Virtual Device Hardware Serial Numbers** and click **+** to add more, if required.
Allow Incident Firing on	This setting allows you to control incident firings based on approved device status. If the **Approved Devices Only** option is selected, the following logic is used: (a) If at least one Source, Destination or Host IP is approved, the incident triggers. (b) Else if at least one incident reporting device is approved, the incident triggers. (c) Else the incident does not trigger. **Note:** System devices (Super, Worker, and Collectors) will always be considered to be approved devices. In other words, incidents will fire for these system devices even if **Approved Devices Only** option is selected. Select **All Devices** or **Approved Devices Only** accordingly.

3. Click **Save**.

Device Filter

This setting allows you to limit the set of devices that the system automatically learns from logs and Netflows. After receiving a log from a device, the system automatically learns that device and adds it to

CMDB. When a TCP/UDP service is detected running on a server from Netflow analysis, the server along with the open ports are added to CMDB.

Sometimes, you may not want to add all of these devices to CMDB. You can create filters to exclude a specific set of devices from being added to CMDB. Each filter consists of a required **Excluded IP Range** field and an optional **Except** field.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Device Filter** tab.
2. Click **New**.
3. In the **Range Definition** dialog box, enter the following information:You can add multiple values for these fields by clicking the **+** icon or remove an entry by clicking the **-** icon.
   a. **Excluded IP Ranges** - A device will not be added to CMDB if it falls in the range defined in the Excluded IP Range field. For example, if you wanted to exclude the `172.16.20.0/24` network from CMDB, add a filter with `172.16.20.0-172.16.20.255` in its **Excluded IP Range** field.
   b. **Except** - This field allows you to specify some exceptions in the excluded range. For example, if you wanted to exclude the `172.16.20.0/24` network without excluding the `172.16.20.0/26` network, add a filter with `172.16.20.0-172.16.20.255` in the **Excluded IP Range** field, and `172.16.20.192-172.16.20.255` in the **Except** field.
4. Click **Save**.

Application Filter

This setting allows you to limit the set of applications/processes that the system automatically learns from discovery. You may be more interested in discovering and monitoring server processes/daemons, rather than client processes, that run on a server. To exclude client processes from being discovered and listed in the CMDB, enter these applications here. An application/process will not be added to CMDB if it matches one of the entries defined in this table.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Application Filter** tab.
2. Click **New**.
3. In the **Process Definition** dialog box, enter the **Process Name** and any **Parameters** for that process that you want to filter.
   Matching is exact and case-insensitive based on Process Name and Parameter. If **Parameter** is empty, then only **Process Name** is matched.
4. Select the **Organization** from the drop-down list.
5. Click **Save**.

Location

This setting allows you to set location information for devices in CMDB. Location information can be defined for a set of IP addresses. When applied, this information will overwrite the existing Location information in the CMDB. Future discoveries will not overwrite this information. Use this method to update locations of multiple devices with private IP addresses only. It is not necessary to update

locations for public address space in this manner, because this information can also be obtained from a separate built-in database location.

1. Go to **ADMIN** > **Settings** > **Discovery** > **Location** tab.
2. Click **New**.
3. In the **Location Definition** dialog box, select or enter the following information:
   - Organization Type
   - IP/IP Range
   - Location
   - Update Manual Devices (This enables the system to overwrite the location information for manually defined devices in CMDB.)
4. Click **Save**.
5. Select the new location from the list and click **Apply**.

CMDB Groups

This setting allows you to write rules to add devices in CMDB Device Group and Business Service Groups of your choice. When a device is discovered, the policies defined here are applied and the device is assigned to the group(s) defined in the matching policies. This device grouping does not overwrite the CMDB Device group assigned during discovery. The grouping defined here is in addition to the discovery defined CMDB group.

1. Go to **ADMIN** > **Settings** > **Discovery** > **CMDB Groups** tab.
2. Click **New**.
3. In the **CMDB Group Definition** dialog box, select or enter the following information:
   - **Organization** - the organization which this rule applies to
   - **Vendor** - the matching device vendor
   - **Model** - the matching device model
   - **Host Name** - matching device host name via regular expression match
   - **IP Range** - matching device access IP - format is single IP, IP range, CIDR
   - **Custom Properties** - see Grouping Devices by Custom Properties
   - **Groups** - specify the groups which the matching devices will be added to
   - **Biz Services**- specify the business services which the matching devices will be added to
4. Click **Save**.
5. Select the new CMDB group from the list and click **Apply**.

Conditions are matched in ANDed manner: Both the actions are taken, that is, if both a Group and a Business Service is specified, then the device will be added to both the specified Group and Business Service.

To apply one or more CMDB Group policies:

1. Select one or more policies and click **Apply** or click **Apply All** to apply all policies.
2. Once a policy is saved, then next discovery will apply these policies. That means, discovered devices will belong to the groups and business services defined in the policies.

Note: For all the above configurations, use the **Edit** button to modify any setting or **Delete** to remove any setting.

Grouping Devices by Custom Properties

FortiSIEM allows you to define device groups based on IP address, host name, or device type. You can also group devices based on custom properties. These steps assume that you have already defined the custom properties you are interested in. See Working with Custom Properties.

To group devices by custom properties:

1. In the **CMDB Group Definition** dialog box, click the edit icon next to **Custom Properties**.
2. Click **+** to add a new group definition based on the custom property.
3. Select a custom property from the **Property** drop-down list.
4. Enter a **Value** for the property. You can add multiple values by clicking the **+** button.
5. Click **Save**, then click **Save** again to return to the **CMDB Group Definition** dialog box.
6. In the **Add To** section of the dialog box, select the group to which the CMDB Group will be added from the **Groups** drop-down list.

Monitoring Settings

The following sections describe the procedures for Monitoring settings:

- Important Processes
- Important Ports
- Important Interfaces
- Excluded Disks
- Windows WMI Filter

Important Processes

This setting allows you to always get process resource utilization reports and UP/DOWN alerts on a set of important processes across all device types.

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Important Processes** tab.
2. Click **Enable**.
   This will stop monitoring all processes.
3. Click **New**.
4. Enter a **Process Name**, **Parameter**, and select an **Organization** from the drop-down.
5. Click **Save**.
6. Select the processes from the table and click **Apply**.
   FortiSIEM will start monitoring only the selected processes in this tab.
7. If you want to disable this and return to ALL process monitoring, then click **Disable**.

Important Ports

This setting allows you to get TCP/UDP port UP/DOWN status only for a set of important critical ports. Always reporting UP/DOWN status for every TCP/UDP port on every server can consume a significant amount of resources. A port's UP/DOWN status is reported only if the port belongs to this list defined here.

Matching is exact based on port number and IP protocol.

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Important Ports** tab.
2. Click **New**.
3. Enter the **Port Number** and select the **Port Type** and **Organization** from the drop-down.
4. Click **Save**.
5. Select the new ports from the list and click **Apply**.

Important Interfaces

This setting allows you to always get interface utilization reports on a set of important network interfaces across all device types.

1. Create a list of all Important interfaces.
2. Go to **ADMIN** > **Settings** > **Monitoring** > **Important Interfaces** tab.
3. Click **Enable**.
   This will stop monitoring all interfaces.
4. Click the icon left to search field to select either **Show Device Table** or **Show Interface only**.
5. Click **Select** to add the selected interface to the list. The **Critical** and **Monitor** columns will be automatically checked.
6. Check the WAN box if applicable. If checked, the interface utilization events will have the `isWAN = "yes"` attribute.
   You can use this to run a report for all WAN interfaces.
7. Select the interfaces from the table and click **Apply**.
   FortiSIEM will start monitoring only the selected interfaces in this tab.
8. If you want to disable this and return to ALL process monitoring, click **Disable**.

By default, this feature is disabled regardless of whether it is upgraded or newly installed. If this feature is disabled, FortiSIEM monitors all interface util and up/down events. The `isHostIntfCritical` attribute will be set to false for all interfaces. Only non-critical interface staying down rule may trigger. Critical interface staying down rule will have no chance to trigger. If this feature is enabled, there are two check boxes - monitor and critical. If critical is checked, monitor will be checked automatically. Monitor controls whether we must generate interface util event. We monitor interface utils events for interface whose monitor check box is selected. Critical controls whether we must generate interface up/down events. FortiSIEM monitors interface up/down events for an interface whose critical check box is selected. If one interface is marked as critical, we set the attribute of `isHostIntfCritical` to true in the generated interface util and up/down events. The Rule “critical interface staying down” will trigger on interfaces whose `isHostIntfCritical` is true. Non-critical interface staying down rule will have no chance to trigger.

Excluded Disks

This setting allows you to exclude disks from disk capacity utilization monitoring. Disk capacity utilization events will not be generated for devices matching device name, access IP and disk name. Incidents will not trigger for these events, and the disks will not show up in summary dashboards. Use this list to exclude read-only disk volumes or partitions that do not grow in size and are close to full.

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Excluded Disks** tab.
2. Click **New**.
3. From the **Choose Disk** dialog box, select the device from the device group.
4. Click **Select**.
5. Select the device from the table and click **Apply**.

Windows WMI Filter

Windows can produce a very high number of system, application, and security logs. The system provides a default filter, **Get All Logs**, which returns all of the Windows logs detected. By defining a filter, you can obtain only the logs you need.

Step 1: Create the Windows WMI Filter

1. Go to **ADMIN** > **Settings** > **Monitoring** > **Windows WMI Filter** tab.
2. Click **New**.
3. Enter a name and an optional description for the filter in the New WMI Filter dialog box.
4. Click **New** to define a filter for the template:
   a. From the **Type** drop-down list, select **Application**, **Security**, or **System**.
   b. In the **Include** and **Exclude** fields, enter a comma-separated list of the event codes which should be included or excluded from the filter.
   c. Click **Save**.
5. Click **Save** again to save the Windows WMI filter.

Step 2: Apply the Filter in a Credential

1. Go to **ADMIN > Setup > Credentials**.
2. Click **New** in **Step 1: Enter Credentials**.
   a. In the Access Method Definition dialog box, select one of the Microsoft devices from the **Device Type** drop-down list.
   b. From the **Access Protocol** drop-down list, select **WMI**.
   c. From the **WMI Filter** drop-down list, select the filter created in Step 1: Create the Windows WMI Filter.
   d. Enter any other required information for the credential. For more information, see Setting Credentials.
   e. Click **Save**.
3. Click **New** in **Step 2: Enter the IP Range for Credential**.
   a. In the Device Credential Mapping Definition dialog box, enter an IP or IP range.
   b. From the **Credentials** drop-down list, select the filter created in Step 1: Create the Windows WMI Filter.
   For more information, see Associating a credential to IP ranges or hosts.
   c. Click **Save**.

Step 3: Discover Using the WMI Credential in Step 2

Any Windows Server discovery that uses that a WMI credential will only pull the logs specified in the Filter in Step 1.

Event Handling Settings

This section provides the procedures to configure Event Handling.

- Event Dropping
- Event Forwarding
- Event Organization Mapping
- Multiline Syslog

Event Dropping

Some devices and applications generate a significant number of logs, which may be very verbose, contain little valuable information, and consume storage resources. You can configure Event Dropping rules that will drop events just after they have been received by FortiSIEM, preventing these event logs from being collected and processed. Implementing these rules may require some thought to accurately set the event type, reporting device, and event regular expression match, for example. However, dropped events do not count towards licensed Events per Second (EPS), and are not stored in the Event database. Dropped events also do not appear in reports, and do not trigger rules. You can also specify that events should be dropped but stored, so event information will be available for searches and reports, but will not trigger rules. An example of an event type that you might want to store but not have trigger any rules would be an IPS event that is a false positive.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Dropping** tab.
2. Click **New**.
3. Deselect **All** and click the drop-down next to **Reporting Device** and browse the folders to select the device group or individual devices for which you must create a rule.
4. Click **Save**.
5. Deselect **All** and click the drop-down next to **Event Type** and browse the folders to find the group of event types, or a specific event type for which you must create a rule.
6. Click **Save**.
7. Enter **Source IP** or **Destination IP** that you want to filter. The value can be IP range.
8. Select the **Action** that should be taken when the event dropping rule is triggered from the available options.
   - Drop event - Event is dropped and not counted towards licensed EPS.
   - Store event - Event is stored and counted towards licensed EPS
     - Do not trigger rules - this means that FortiSIEM will store events, but will not trigger rules. Events are available for reporting.
     - Drop attributes - to select the attributes to drop, click the edit icon. In the **Event Dropping Rule > Drop Attribute** window, from the left pane, select the attribute(s) you want dropped and click the **>** icon. Dropped attributes appear in the **Selected Attributes** column. When done, click **Save**. Only attributes in the left pane are stored. Stored event attributes are available for reporting.

Note: You can move dropped attributes so they are stored attributes by selecting them from the **Selected Attributes** column and clicking the **<** icon. When done, click **Save**.

9. For **Regex Filter**, enter any regular expressions you want to use to filter the log files. If any matches are made against your regular expression, then the event will be dropped.
10. Enter any **Description** for the rule.
11. Click **Save**.

Notes:

- All matching rules are implemented by FortiSIEM, and inter-rule order is not important. If you create a duplicate of an event dropping rule, the first rule is in effect.
- If you leave a rule definition field blank, then that field is not evaluated. For example, leaving **Event Type** blank is the same as selecting **All Event Types**.
- FortiSIEM drops the event at the first entry point. If your deployment uses Collectors, events are dropped by the Collectors. If your deployment doesn't use Collectors, then the event will be dropped by the Worker or Supervisor where the event is received.
- You can use the report System Event Processing Statistics to view the statistics for dropped events. When you run the report, select AVG(Policy Dropped Event Rate (/sec) as one of the dimensions for Chart to see events that have been dropped to this policy.

Event Forwarding

In systems management, many servers may need access to forward logs, traps and Netflows from network devices and servers, but it is often resource intensive for network devices and servers to forward logs, traps and Netflows to multiple destinations. For example, most Cisco routers can forward Netflow to two locations at most. However, FortiSIEM can forward/relay specific logs, traps and Netflows to one or more destinations. A Super, Worker or Collector can forward events - the one which receives and parses the event forwards it. If you want to send a log to multiple destinations, you can send it to FortiSIEM, which will use an event forwarding rule to send it to the desired locations. If you only want the workers (or super) to forward events, after this configuration, see Event Forwarding by Worker.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Forwarding** tab.
2. Click **New**.
3. Select the **Organization** for which the rule will apply.
4. Click the drop-down next to **Reporting Device** and browse the folders to find the group of devices, or a specific device for which you must create a rule.
5. Click the drop-down next to **Event Type** and browse the folders to find the group of event types, or a specific event type for which you must create a rule.
6. Click **Save**.
7. Select the **Traffic Type** to which the rule should apply.
8. For **Source IP**, enter the IP address of the device that will be sending the logs.
9. For **Destination IP**, enter the IP address of the device to which the logs are sent.
10. For **Severity**, select an operator and enter a severity level that must match for the log to be forwarded.

11. For **Regex Filter**, enter any regular expressions you want to use to filter the log files.
    If any matches are made against your regular expression, then the event will be forwarded.
12. Select the forwarding **Protocol** from the drop-down.
    - **UDP** - If you use this protocol, events may be lost.
    - **TCP** - This method ensures reliability.
    - **TCP over SSL** - This method ensures reliability and security. See Note 3 below.
13. Based on your selection of **Traffic Type**, enter the following information:
    a. Enter the **IP** address in **Forward to** > **IP**.
    b. Select the **Port** number in **Forward to** > **Port** field.
    c. Select a **Forward to** > **Protocol** from the drop-down list.
    d. Select the **Forward to** > **Format**:
       - **Incoming** - outgoing format is same as incoming.
       - **CEF** - outgoing events are CEF formatted. See here for details on CEF formatted logs.
14. Click **Save**.

Notes:

1. If you want the same sender IP to forward events to multiple destinations, create a rule for each destination.
2. FortiSIEM will implement all rules that you create and enable, so if you create a duplicate of an event forwarding rule, two copies of the same log will be sent to the destination IP.
3. If you want to use public CA certificates for TCP over SSL communication, then note the following:
   - FortiSIEM's SSL library can validate an external system's certificate if it is signed by a public CA.
   - If the external system wants to verify the FortiSIEM node's certificate, then you need to add the following certificate and key to the `phoenix_config.txt` file of the FortiSIEM nodes forwarding the event.

```
[BEGIN phEventForwarder]
tls_certificate_file= #/opt/phoenix/bin/.ssh/my_cert.crt
…
tls_key_file= #/opt/phoenix/bin/.ssh/my_cert.key
[END]
```

Event Forwarding by Worker

There may be situations where you may not want to forward events from collectors to your target device. Fortinet allows you to forward events when workers (or super) receives collector event information. To configure this, go to **ADMIN** > **Settings** > **Event Handling** > **Forwarding** tab, and add a checkmark to the **Forward From Worker** checkbox. If there is more than one collector per org, this feature will forward events by workers for all collectors.

Event Organization Mapping

FortiSIEM can handle multi-tenant reporting devices that already have Organization names in the events they send, for example, VDOM attribute in FortiGate. This section shows how to map Organization names in external events to those in FortiSIEM. FortiSIEM will create a separate reporting device in each Organization and associate the events to the reporting device in the corresponding FortiSIEM Organization.

This feature requires that:

- One or more (multi-tenant) Collectors are created under Super-Local Organization.
- Multi-tenant devices send logs to the multi-tenant Collectors under Super-Local Organization.

Follow the steps below:

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Event Org Mapping** tab.
2. Click **New**.
3. Select or search the **Device Type** of the sender from the drop-down.
   This has to be a device that FortiSIEM understands and able to parse events.
4. Select or search the **Event Attribute** that contains the external organization name from the drop-down.
   FortiSIEM will map the value in this field to the FortiSIEM Organization.
5. Select or search the multi-tenant **Collectors** under Super-Local Organization that will receive the events from the drop-down.
   To include all Collectors, select **All Collectors**.
6. Specify the **IP/IP Range** of the multi-tenant devices that are sending events.
   Only a single IP or an IP Range is allowed, for example, 10.1.1.1 or 10.1.1.1-10.1.1.2. Comma-separated values, such as 10.1.1.1,10.1.1.2, are not allowed.
7. Click the edit icon next to **Org Mapping** to map an organization to an event.
   - Click on any **Event Organization** cell in the **Event Organization Mapping** dialog box to edit. Click **Save**.
8. Click **Save**.

Note: Do not define overlapping rules - make sure there are no overlaps in (Collector, Reporting IP/Range, Event Attribute) between multiple rules.

Multiline Syslog

Often applications generate a single syslog in multiple lines. For analysis purposes, the multiple lines must be put together into a single log. This feature enables you to do that. User can write multiple multiline syslog combining rules based on reporting IP and begin and ending patterns. All matching syslog within the begin and ending pattern are combined into a single log.

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Multiline Syslog** tab.
2. Click **New**.

3. Enter or select the following information:
   a. **Organization** - syslog from devices belonging to this Organization will be combined to one line.
   b. **Sender IP** - the source of the syslog. Format is a single IP, IP range, CIDR and a combination of the above separated by comma.
   c. **Protocol** - TCP or UDP since syslog can come via either of these protocols.
   d. **Begin Pattern** - combining syslog starts when the regular expression specified here is encountered.
   e. **End Pattern** - combining syslog stops when the regular expression specified here is encountered.
4. Click **Save**.

Note: For all the above configurations, use the **Edit** button to modify any setting or **Delete** to remove any setting.

The current conception is only for UDP, which is different from TCP. If a single event is sent by multiple UDP packets, you need a multiline rule to combine them. Otherwise, FortiSIEM treats them as multiple events. If a continuous TCP stream contains multiple events, you need a multiline rule to separate them. Otherwise, FortiSIEM treats LF (new line character \n) as the separator.

Database Settings

The following sections provide more information about the Database settings:

- Creating Retention Policy
- Viewing Online Event Data Usage
- Viewing Archive Event Data
- Event Log Integrity
- ClickHouse Configuration

Creating Retention Policy

The life cycle of an event in FortiSIEM begins in the *Online* event database, before moving to the *Archive* data store. Online event data resides on faster, but expensive storage. Archive data resides on relatively slower, cheaper and higher capacity storage. You can set up retention policies to specify which events are retained, and for how long, in the online and archive event databases.

- ClickHouse Event Retention
  - How ClickHouse Event Retention Works
  - Creating ClickHouse Time Based Event Retention Policy
  - Creating ClickHouse Archive Event Retention Policy for EventDB on NFS
- FortiSIEM EventDB Event Retention
  - How EventDB Event Retention Works
  - Creating EventDB Online Event Retention Policy
  - Creating EventDB Archive Event Retention Policy
- Elasticsearch Event Retention
  - How Elasticsearch Event Retention Works
  - Configuring Elasticsearch Retention Threshold
  - Configuring HDFS Archive Threshold
  - Creating Elasticsearch Archive Event Retention Policy

ClickHouse Event Retention

This section covers how events retention is managed for ClickHouse based deployments. The deployment possibilities are provided in the following table.

FortiSIEM Deployment	Online Storage	Archive Storage
Non-AWS	Hot and Warm and Cold tiers	Real time archive on NFS. Note that Cold tier with large disks may suffice for Archive.
AWS	Hot and Warm and Cold tiers	AWS S3
GCP	Hot and Warm and Cold tiers	GCS

How ClickHouse Event Retention Works

Case 1: Regular non-AWS/non-GCP Deployments

An example is on-premise ClickHouse deployment, where online data is stored in ClickHouse Hot/Warm/Cold tiers, with multiple disks in each tier. In many cases, Cold tier can serve for archiving old events. If this is not sufficient, then you can add an Archive storage on NFS where events are stored in EventDB format. In this case, events are copied from FortiSIEM to NFS in real time, as events arrive.

Online Storage Management

Online storage includes events stored in ClickHouse Hot/Warm/Cold tiers. For Online storage, event retention is managed using two mechanisms: Space based Retention and Time based Retention.

- **Space based Retention**:
  - If free Hot tier disk utilization is less than 10%:
    - If Warm tier is defined, then events are moved from Hot tier to the Warm tier until free Hot tier disk utilization is more than 20%.
    - If Warm tier is not defined, then those events are purged.
  - If free Warm tier disk utilization is less than 10%:
    - If Cold tier is defined, then events are moved from the Warm tier to the Cold tier until free Warm tier disk utilization is more than 20%.
    - If Cold tier is not defined, then those events are purged.
  - If Cold tier is defined and its disk utilization is less than 10%:
    - Events are purged until free Cold tier disk utilization is more than 20%.

  When events need to be moved to a different tier or purged, FortiSIEM applies a **global oldest first selection policy** and moves or deletes the globally oldest first events across all retention policy buckets. Ties are broken randomly. See the example below.

  Suppose in Hot tier, there are two retention buckets containing events for the following days: Day D1 is the oldest while Day D6 is the latest.

  90 day bucket - days D1, D2, D3, D4, D5, D6

  180 day bucket - days D3, D4, D5, D6

  If the free Hot tier disk utilization goes below 10% on Day D6, then the events (to move or purge) are chosen in the following order, until free Hot tier disk utilization reaches 20%:

  a. 90 day bucket - day D1
  b. 90 day bucket - day D2
  c. 180 day bucket - day D3
  d. 90 day bucket - day D3
  e. 90 day bucket - day D4
  f. 180 day bucket - day D4
  g. 180 day bucket - day D5
  h. 90 day bucket - day D5
- **Time based Retention**: You can specify Online event retention policies to specify the duration for which certain events need to be retained. The policies can take event attributes such as Organization, Reporting Device and Event Type as input. See Creating ClickHouse Time Based Event Retention Policy.

During the retention period, the events can be in Hot or Warm or Cold storage depending on the Space based retention, e.g., if Hot tier becomes full, then the event may move to Warm tier, etc... After the retention period expires, these events are purged from Online storage. If you do not have sufficient disk space for the event retention policies, then Space based retention policies kick in and may purge the data, to make room for FortiSIEM to store new events.
Note: When adding a new retention policy, ensure that there is sufficient disk space to meet the retention policy requirements, or else data may be purged before retention time.

Archive Storage Management

If you define Archive storage, then events are copied in real-time to Archive storage and stored in FortiSIEM EventDB format. This storage is not maintained by ClickHouse. Events can stay in both Online and Archive storage, and their retention is managed independently.

- **Space based Retention**: If free Archive disk utilization is less than 10GB, then *oldest* events are purged until free Archive disk utilization is more than 20GB. These parameters are defined in the `phoenix_config.txt` file.
- **Organization based Retention**: You can write Archive retention policies to specify the duration for which events for each Organization need to be retained. See Creating Archive Event Retention Policy.

Case 2: AWS and GCP Deployments

For AWS deployments, you can define S3 as the Archive storage. For GCP deployments, you can define GCS as the Archive storage. ClickHouse manages both the Online Hot/Warm/Cold disks and Archive S3/Archive GCS storage.

- **Space based Retention**:
  - If free Hot tier disk utilization is less than 10%:
    - If Warm tier is defined, then events are moved from Hot tier to the Warm tier until free Hot tier disk utilization is more than 20%.
    - If Warm tier is not defined, but S3/GCS Archive is defined, then those events are moved from Hot tier to S3/GCS Archive until free Hot tier disk utilization is more than 20%.
    - If neither Warm tier nor S3/GCS Archive is defined, then those events are purged.
  - If free Warm tier disk utilization is less than 10%:
    - If Cold tier is defined, then events are moved from Warm tier to Cold tier until free Warm tier disk utilization is more than 20%.
    - If Cold tier is not defined, but S3/GCS Archive is defined, then those events are moved from Warm tier to S3/GCS Archive until free Warm tier disk utilization is more than 20%.
    - If neither Cold tier nor S3/GCS Archive is defined, then those events are purged.
  - If free Cold tier disk utilization is less than 10%:
    - If S3/GCS Archive is defined, then events are moved to S3/GCS Archive until free Cold tier disk utilization is more than 20%.
    - If S3/GCS Archive is not defined, then events are purged until free Cold tier disk utilization is more than 20%.
  - S3/GCS Archive disk space is considered unlimited. Events are never purged from S3/GCS Archive.

When events need to be moved to a different tier or purged, FortiSIEM applies a **global oldest first selection policy** and moves or deletes the globally oldest first events across all retention policy buckets. Ties are broken randomly. See the example below.

Suppose in Hot tier, there are two retention buckets containing events for the following days where Day D1 is oldest and day D6 is the latest.

90 day bucket - days D1, D2, D3, D4, D5, D6

180 day bucket - days D3, D4, D5, D6

If the free Hot tier disk utilization is less than 10%, then the events to move or purge, are chosen in the following order, until free Hot tier disk utilization reaches 20%:

a. 90 day bucket - day D1
b. 90 day bucket - day D2
c. 180 day bucket - day D3
d. 90 day bucket - day D3
e. 90 day bucket - day D4
f. 180 day bucket - day D4
g. 180 day bucket - day D5
h. 90 day bucket - day D5

- **Time based Retention**: You can specify Online event retention policies to specify the duration for which certain events need to be retained. The policies can take event attributes such as Organization, reporting Device and Event Type as input. See Creating ClickHouse Time Based Event Retention Policy.

  During the retention period, the events can be in Hot or Warm or Cold storage depending on the Space based retention, e.g., if Hot tier becomes full, then the event may move to Warm tier, etc... After the retention period expires, these events are purged from ClickHouse Online storage and S3/GCS Archive.
  Note: When adding a new retention policy, ensure that there is sufficient disk space to meet the retention policy requirements, or else data may be purged before retention time.

Creating ClickHouse Time Based Event Retention Policy

Online event retention policies specify which events are retained, and for how long, in the online event database. Take the following steps to create an Online Event retention policy for ClickHouse.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Online Retention Policy**, click **New**.
3. Select **Enabled** if the policy has to be enforced immediately.
4. Choose the **Organizations** for which the policy must be applied (for service provider installations). Select **All** if it should apply to all organizations.
5. Choose the **Reporting Devices** to apply this policy using the edit icon and click **Save**.
6. Choose the **Event Type** or event type groups to apply this policy and click **Save**.
7. Select the **Retention Period** from the drop-down list (3 Months, 6 Months, 1 Year, 3 Years, 5 Years, 10 Years, Forever (50 Years). Each month is 30 days.

8. Enter any **Description** related to the policy.
9. Click **Save**.
10. When done, click **Apply**.

Implementation Notes:

1. Any time the retention policy on ClickHouse environment is changed, you must click **Apply** to push the retention policy.
2. Retention policies are evaluated based on Rank. A lower rank policy is evaluated first and first match is applied.
3. All events matching a retention policy are retained for the duration specified by the **Retention Period** specified in the policy.
4. For the events that do not match with any existing retention policy, the default value for Retention Days is 18, 250 (50 years)

Creating ClickHouse Archive Event Retention Policy for EventDB on NFS

These policies specify which events are retained, and for how long, when EventDB on NFS is used to archive.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Offline Retention Policy**, click **New** to create a new policy.
3. Select the **Organization** this policy applies to.
4. Enter the **Time Period** in days for archive retention.
5. Click **Save**.

Implementation Notes:

1. Policies are enforced only at the end of the day.
2. FortiSIEM will attempt to retain the events in the archive according to the policies. However, if the low storage threshold is hit (10GB, by default), then the oldest events which occurred in the day are purged.
3. Refer to the ClickHouse Event Retention Table for deployment options.

FortiSIEM EventDB Event Retention

This section covers how events retention is managed for EventDB based deployments.

How EventDB Event Retention Works

For Online storage, event retention is managed using two mechanisms:

- **Space based retention**: If free online disk utilization is less than 10GB, then oldest events are moved to the Archive until free online disk utilization is more than 20GB. If Archive is not defined, then those events are purged.
- **Policy based retention**: You can specify Online event retention policies to specify the duration for which certain events need to be retained in online storage. The policies can take event attributes such as Organization, Reporting Device and Event Type as input. See Creating Online Event Retention Policy. If an event has remained in the online EventDB for the time period in the event retention policy, then the event is moved to the Archive at the end of the day.

For Archive storage, event retention is managed using two mechanisms:

- **Space based retention**: If free archive disk utilization is less than 10GB, then oldest events are purged until free online disk utilization is more than 20GB.
- **Policy based retention**: You can specify Archive event retention policies to specify the duration for specific Organizations. See Creating Archive Event Retention Policy. If an event has remained in the archive EventDB for the time period in the event retention policy, then the event is purged at the end of the day.

Creating EventDB Online Event Retention Policy

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Online Retention Policy**, click **New**.
3. Select **Enabled** if the policy needs to be applied.
4. Choose the **Organizations** for which the policy must be applied (for service provider installations). Select **All** if it should apply to all organizations.
5. Choose the **Reporting Devices** to apply this policy using the edit icon and click **Save**. If all reporting devices should be applied, check the **All** checkbox.
6. Choose the **Event Type** or event type groups to apply this policy and click **Save**. If all event types should be applied, check the **All** checkbox.
7. Enter or select the **Time Period** in days that the event data specified by the conditions (Organizations, Reporting Devices and Event Type) should be held in the online storage before it is moved to archive or purged.
8. Enter any **Description** related to the policy.
9. Click **Save**.

Implementation Notes:

- If an event has remained in the online event database for the time period in the event retention policy, then the event is moved to the archive at the end of the day.
- If an event does not match any online event retention policy, then it remains in the online event database until the low storage threshold (10GB, by default) is reached. The event is then moved to the archive.
- If the archive mount point is defined, then ALL events are moved from online to archive. Nothing is purged.
- If the archive is not reachable after multiple retries, then FortiSIEM is forced to purge the event because there is nowhere to store the event.

- FortiSIEM will attempt to retain the events in the online event database according to the policies. However, if the low storage threshold is hit (10GB, by default), then the events from the oldest day are moved to archive.
- Implementing an online event policy requires selectively deleting specific events from the database and then re-indexing the database for the affected days. This is expensive in terms of time and performance. Therefore, do not define excessively fine-grained retention policies, because this will affect database performance.
- Policies are enforced only at the end of day – this means that events are deleted and re-indexed only at the end of the day. This minimizes the impact on database performance because the database usage should be low at that time.
- Policies are enforced by FortiSIEM only from the date just before the retention period. For example, if the retention period for a policy is 10 days, and today is 12/19/2022, then FortiSIEM will automatically enforce the policy for events with event receive time starting from 12/18/2022. For processing older dates, Fortinet recommends customers to use the `EnforceRetentionPolicy` tool as follows:
  - `EnforceRetentionPolicy <DATES>`, where *DATES* is a comma-separated list of dates or date-range on which to enforce the policy. *DATES* is specified as the number of days since the UNIX epoch began: 1970-01-01. A date-range can specified by two dates inclusively separated by "-". Use the following Linux command to generate a epoch date (**Note**: Replace `MM/DD/YYYY` with actual date):
    ```
    echo $(($(date --utc --date="MM/DD/YYYY" +%s)/86400))
    ```
    For example, run the command `EnforceRetentionPolicy 16230,16233-16235` to enforce retention policies on these dates: 6/8/2014 and from 6/11/2014 to 6/13/2014.
  - Run the tool as admin user.

Creating EventDB Archive Event Retention Policy

These policies specify which events are retained, and for how long, in the archive.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Offline Retention Policy**, click **New** to create a new policy.
3. Select the **Organization** this policy applies to.
4. Enter the **Time Period** in days for archive retention.
5. Click **Save**.

Implementation Notes:

1. Policies are enforced only at the end of the day.
2. If an event has remained in the archive for the duration specified in the event retention policy, then the event is purged at the end of the day.

Elasticsearch Event Retention

This section covers how events retention is managed for Elasticsearch based deployments. The deployment possibilities are:

FortiSIEM Deployment	Online Storage	Archive Storage
On-premises Elasticsearch – Option 1	Hot and Warm tiers	HDFS archive from Elasticsearch
On-premises Elasticsearch – Option 2	Hot and Warm tiers	Real-time HDFS archive from FortiSIEM
On-premises Elasticsearch – Option 3	Hot and Warm tiers	Real-time Archive to NFS
Elastic Cloud and AWS Elasticsearch	Hot and Warm tiers	Not available

How Elasticsearch Event Retention Works

Elasticsearch online events storage is managed by the following thresholds:

- **Hot Node**
  - **Free Space Threshold**: When the Hot node cluster disk free space falls below **Low Threshold**, then events are moved to Warm nodes until the Hot node cluster disk free space reaches **High Threshold**. If Warm node is not defined, then events are Archived. If Archive is not defined or real time archive option is chosen, then events are purged.
  - **Age Limit**: Maximum number of days after which events are moved to Warm nodes. If Warm node is not defined, then events are Archived. If Archive is not defined or real time archive option is chosen, then events are purged.
- **Warm Node**
  - **Free Space Threshold**: When the Warm node cluster disk free space falls below **Low Threshold**, then events are Archived. If Archive is not defined or real time archive option is chosen, then events are purged.
  - **Age Limit**: Maximum number of days after which events are moved to Archive. If Archive is not defined or real time archive option is chosen, then events are purged.

These thresholds are defined in Configuring Elasticsearch Retention Threshold.

For archive you can choose either HDFS or EventDB on NFS.

- **HDFS archive from Elasticsearch**: In this option, FortiSIEM `HDFSMgr` process creates Spark jobs to directly pull events from Elasticsearch and store in HDFS. This option may result in extra load on Elasticsearch as events have to read and then deleted from Elasticsearch while events are getting inserted. In this option, archive disk is managed by threshold, that is when low threshold is reached, then events are purged until the high threshold is reached – see Configuring HDFS Archive Threshold.

- **Real-time HDFS archive from FortiSIEM**: In this option, FortiSIEM `HDFSMgr` process creates Spark jobs to pull events from FortiSIEM Supervisor and Worker nodes. This happens while events are getting inserted into Elasticsearch. This approach has no impact in Elasticsearch performance, but events are stored in both Elasticsearch and HDFS and managed independently. Note that HDFS has better event storage compression properties. In this option, archive disk is managed by threshold, that is when low threshold is reached, then events are purged until the high threshold is reached – see Configuring HDFS Archive Threshold.
- **Real time archive to NFS**: In this option, FortiSIEM Supervisor and Worker nodes store events in NFS managed by FortiSIEM EventDB. This happens while events are getting inserted into Elasticsearch. This approach has no impact in Elasticsearch performance, but events are stored in both Elasticsearch and EventDB and managed independently. Note that EventDB has better event storage compression properties. In this option, archive disk is managed by policies– see Creating Archive Event Retention Policy.

Configuring Elasticsearch Retention Threshold

Complete these steps to configure Native Elasticsearch free space and age retention threshold:

1. Go to **ADMIN > Settings > Database > Online Settings**.
2. Select the low percentage threshold, high percentage threshold, and age under:
   a. Hot Node - Free Space Threshold - Events are moved to Warm nodes based on the first occurrence of one of the following:
      - When the Hot node cluster disk free space falls below Low value, then events are moved to Warm nodes until the Hot node cluster disk free space reaches High value.
      - If the time duration limit set under Hot Age (the Warm age phase) is met, all events under this limit are moved to Warm nodes.
   b. Warm Node - Free Space Threshold - Events are moved to Warm nodes based on the first occurrence of one of the following:
      - When the Warm node cluster disk free space falls below Low value, then events are moved to Cold nodes until the Warm node cluster disk free space reaches High value.
      - If the time duration limit set under Warm Age (the Cold age phase) is met, all events under this limit are moved to Cold nodes.
        Note: In the fsiem_ilm_policy, the cold age phase is reflected as a sum of the warm age phase and cold age phase UI values.

Configuring HDFS Archive Threshold

Complete these steps to configure the HDFS retention threshold:

1. Go to **ADMIN > Settings > Database > Archive Data**.
2. Select the low and high percentage thresholds under **Archive Threshold**. If HDFS disk utilization falls below **Low value**, then events are purged until disk utilization reaches **High value**.

Creating Elasticsearch Archive Event Retention Policy

These policies specify which events are retained, and for how long, in the archive.

1. Go to **ADMIN > Settings > Database > Retention Policy**.
2. Under **Offline Retention Policy**, click **New** to create a new policy.
3. Select the **Organization** this policy applies to.
4. Enter the **Time Period** in days for archive retention.
5. Click **Save**.

Implementation Notes:

1. Policies are enforced only at the end of the day.
2. If an event has remained in the archive for the duration specified in the event retention policy, then the event is purged at the end of the day.

Viewing Online Event Data Usage

Online Event Data Usage enables you to see a summarized view of online event data usage. This view enable you to manage storage more effectively by writing appropriate event dropping policies or online event retention policies.

The Online Event Data Usage is displayed in tree view under **ADMIN** > **Settings** > **Database** > **Online Data** grouped by the year and dates for NFS/Local storage. For Elasticsearch-based deployments, if the storage is set per Organization, the usage is displayed specific to each Organization grouped by year and dates. For Elasticsearch and ClickHouse deployments, you can drill-down from the year to view the usage for any specific date. You can also click on the **Expand All** checkbox to view all the available storage information.

Viewing Archive Event Data

The event database archived data is displayed in tree view grouped by Organization and archive dates.

Note: Events for CustomerId 0 correspond to FortiSIEM internal system events. On the Archive Event Data page, these events are shown under Super/Local.

Complete these steps to view archived data:

1. Go to **ADMIN** > **Settings** > **Database** > **Archive Data**.
2. Search the **Archived Data** by Organization in the search box and drill-down to find the specific data by specific dates from the tree view.

Event Log Integrity

- Validating Event Log Integrity for EventDB
  - Viewing EventDB Event Log Integrity Status
  - Validating EventDB Event Log Integrity
  - Exporting EventDB Event Log Integrity Status
- Validating Event Log Integrity for ClickHouse
  - Viewing ClickHouse Event Log Integrity Status
  - Validating ClickHouse Event Log Integrity
  - Automating ClickHouse Log Integrity

Validating Event Log Integrity for EventDB

Security auditors can validate that archived event data has not been tampered using the **Event Integrity** function of event database management.

Note: This setting is not available for Elasticsearch

Viewing EventDB Event Log Integrity Status

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. Use the following filters to view the event log integrity:
   a. For a specific time using the **From** and **To** fields.
   b. Based on the status of event integrity using the **Status** drop-down:
      - Not Validated - the event integrity has not been validated yet.
      - Successful - the event integrity has been validated and the return was success. This means that the logs in this file were not altered.
      - Failed - the event integrity has been validated and the return was failed. This means that the logs in this file were altered.
      - Archived - the events in this file were archived to offline storage.
      - Purged - the log event is removed from the log.
      - Restored - the event is restored to the log file.

The event log integrity table is automatically updated with the applied filters.

Columns	Description
Start Time	The earliest time of the messages in this file. The file does not contain messages that were received by FortiSIEM before this time.
End Time	The latest time of the messages in this file. The file does not contain messages that were received by FortiSIEM after this time.
Category	• **Internal**: these messages were generated by FortiSIEM for its own use. This includes FortiSIEM system logs and monitoring events such as the ones that begin with `PH_DEV_MON`. • **External**: these messages were received by FortiSIEM from an external system. • **Incident**: these corresponds to incidents generated by FortiSIEM.
File Name	Name of the log file.
Events	Number of events in the file.
Algorithm	Checksum algorithm used for computing message integrity.
Checksum	Value of the checksum.
Status	Event log integrity validation status.
Location	File location: • **Local**: Local to Supervisor node. • **External**: means external to Supervisor node, for example, on NFS storage.

Validating EventDB Event Log Integrity

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. To validate the event log integrity of:
   a. Single event log - select the event log and click **Validate**.
   b. Multiple event logs - use **Ctrl**/**Command** keys to select the event logs and click **Validate**.
   c. All logs at a time - click **Validate All**.

The validation **Status** of the event log(s) will be updated in the list. The Validation History of any selected event log can be viewed under **Action** > **Validation History**.

Exporting EventDB Event Log Integrity Status

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. To generate and download the file in PDF or CSV format, select the event log from the list and click **Export**. Use **Ctrl**/**Command** keys to select multiple event logs.

Validating Event Log Integrity for ClickHouse

Security auditors can validate that archived event data has not been tampered using the **Event Integrity** function of event database management.

Note: This setting is not available for Elasticsearch

Viewing ClickHouse Event Log Integrity Status

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. Use the following filters to view the event log integrity:
   a. For a specific time using the **From** and **To** fields.
   b. Based on the status of event integrity using the **Show** drop-down:
      - All - All events are shown.
      - Not Validated - the event integrity has not been validated yet.
      - Success - the event integrity has been validated and the return was success. This means that the logs in this file were not altered.
      - Failure - the event integrity has been validated and the return was failed. This means that the logs in this file were altered.
      - Not Found - the log event has been removed or detached.

The event log integrity table is automatically updated with the applied filters.

Columns	Description
Start Time	The earliest time of the messages in this file. The file does not contain messages that were received by FortiSIEM before this time.
End Time	The latest time of the messages in this file. The file does not contain messages that were received by FortiSIEM after this time.
Shard	The ID of the shard.
Partition ID	The partition ID of the shard.
Partition Name	The partition or "directory" name for ClickHouse logs. Hover the cursor over the name to display the full directory path and name. **Note**: If ClickHouse is unable to consolidate the event data, such as if there is not enough storage space, the **Partition Name** and **Validation Status** will appear blank.
Validation Status	Event log integrity validation status. The following messages may appear: Success - checksum match verified. Failure - checksum match failure. Not Found - partition issue occurred. System Error - shell command or parsing error.
Checksum	Value of the checksum.

Validating ClickHouse Event Log Integrity

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. To validate the event log integrity of:
   a. Single event log - select the event log and click **Validate**.
   b. Multiple event logs - use **Ctrl**/**Command** keys to select the event logs and click **Validate**.
   c. All logs at a time - click **Validate All**.

The **Validation Status** of the event log(s) will be updated in the list.

Automating ClickHouse Log Integrity

1. Go to **ADMIN** > **Settings** > **Database** > **Event Integrity**.
2. From the **Event Integrity** drop-down list select **On** or **Off**.

When **Event Integrity** is **On**, a ClickHouse log integrity check occurs at the time it consolidates its data. As this is resource intensive, it is off by default.

ClickHouse Configuration

This section covers how to configure a ClickHouse topology of Keeper and Data/Query nodes.

Before beginning, make sure that:

1. You have gone through ClickHouse Operation Overview, FortiSIEM Reference Architecture Using ClickHouse Guide, and the ClickHouse Sizing Guide, with the last two guides located in the FortiSIEM Documentation Library.
2. You have identified the FortiSIEM nodes that are going to be ClickHouse Keeper nodes and ClickHouse Data nodes.
3. You have configured appropriate disks on the FortiSIEM nodes appropriate for their role.
4. It is important to understand that after adding a new shard to an existing cluster, ClickHouse does not automatically rebalance the data among existing shards and new shard. The user must manually rebalance as described in the Scaling FortiSIEM within ClickHouse section of the Reference Architecture, with detailed steps in Rebalancing Shards.

Take the following steps.

1. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
2. Configure **ClickHouse Keeper Cluster**.
   a. Click on **+** and add a Worker.
   b. Click on **-** to remove a Worker.
   c. An operation for a ClickHouse Keeper Cluster node, such as adding or removing a node, MUST be done individually, meaning that after an operation is done, a test and deploy action must be performed. For example, if you add a ClickHouse Keeper Cluster node, you must then perform a test and deploy before doing any other operation for another ClickHouse Keeper Cluster node, such as adding another ClickHouse Keeper Cluster node, or removing a ClickHouse Keeper Cluster node. Do NOT perform more than one operation, such as adding or removing a ClickHouse Keeper Cluster node without testing and deploying it, as doing so may cause stability issues.
3. Configure **ClickHouse Server Cluster**. You need to know the number of shards.
   a. Click on **+** and add a shard.
   b. Add Workers to the shard.
      i. Check **Data** if this Worker is a ClickHouse Data Node. A Data node receives events, processes them and writes to ClickHouse database.
      ii. Check **Query** if this Worker is a ClickHouse Query Node. A Query node stores events replicated from data nodes and participates in Queries. However, it does not process events and triggers incidents.
      iii. Check both **Data** and **Query** if this Worker is both a ClickHouse Data and Query Node. This is the most common setup.
4. Once the shards have been created and workers have been added to the shard, then click **Test**.
5. If **Test** succeeds, then click **Deploy** to push the changes to ClickHouse.

Notes:

1. If you made changes to the ClickHouse Keeper Cluster, then after Deploy succeeds, `phClickHouseMonitor`, `ClickHouseKeeper` and `ClickHouseServer` processes will restart.
2. If you made changes to the ClickHouse Cluster, then after Deploy succeeds, `phClickHouseMonitor`, and `ClickHouseServer` processes will restart.

For Advanced Configuration Operations, see Advanced Operations in the Appendix.

Role Settings

FortiSIEM provides performance, availability, and environmental alerts, as well as change and security monitoring for network devices, servers and applications. It is difficult for one admin to monitor across the entire spectrum of available information. In addition, devices may be in widely distributed geographical and administratively disjointed locations. Role-based access control provides a way to partition the FortiSIEM administrative responsibilities across multiple admins.

A role defines two aspects of a user's interaction with the FortiSIEM platform:

- Which user interface elements a user can see and the ability to use the associated Read/Write/Execute permissions. As an example, the built-in Executive role can see only the dashboard, while the Server Admin role cannot see network devices. Role permissions can be defined to the attribute level in which, for example, a Tier1 Network Admin role can see network devices but not their configurations.
- What data can the user see. For example, consider a Windows Admin role and a Unix Admin role. They both can run the same reports, but the Windows admins sees only logs from Windows devices. This definition can also be fine-grained, for example one Windows admin sub-role can be defined to see Windows performance metrics, while another Windows admin sub-role can see Windows authentication logs. The roles described in the following table are default roles.

Role	Permissions
DB Admin	Full access to the database servers part of the GUI and full access to logs from those devices.
Executive	View access to the Business Service dashboard and personalized My Dashboard tabs, but reports can be populated by logs from any device.
Full Admin	Full access to the GUI and full access to the data. Only this role can define roles, create users and map users to roles.
Help Desk	Access to the Admin, CMDB, and Dashboard tabs, with view and run permissions for the Analytics and Incidents tabs.
Network Admin	Full access to the network device portion of the GUI and full access to logs from network devices.
Read Only Admin	View access to all tabs and permission to run reports.
Security Admin	Full access to Security aspects of all devices.
Server Admin	Full access to the Server part of the GUI and full access to logs from those devices.
Storage Admin	Full access to the Storage device part of the GUI and full access to logs from those devices.
System Admin	Full access to the Server/Workstation/Storage part of the GUI and full access to logs from those devices.
Unix Server Admin	Full access to the Unix Server part of the GUI and full access to logs from those devices.
Windows Server Admin	Full access to the Windows Server part of the GUI and full access to logs from those devices.

The following sections describe the procedures to create custom roles and privileges:

- Adding a New Role
- Modifying a Role
- Example Role Setup
- Viewing User Roles for AD Group Mappings

Adding a New Role

You can create a new role or use an existing role by selecting an existing role and clicking the **Clone** button.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New**.
3. Enter a **Role Name** and **Description**.
4. Enter the **Data Conditions** for this role.
   This restricts access to the event/log data that is available to the user, and will be appended to any query that is submitted by users with this role. This applies to both Real-Time and Historical searches, as well as Report and Dashboard information.
5. Enter the **CMDB Report Conditions** for this role. Choose a type from the drop-down list.
   This restricts access to the reports for devices, users, monitors, rule, report, task, identity, incident, audit that are available to the user with this role.
6. Select the appropriate **Approver** capability:
   - Select **De-Obfuscation** if this role can approve De-Obfuscation requests.
   - Select **Report Schedule** if this role can approve Report Schedule Activation requests.
   - Select **Rule Activation/Deactivation** if this role can approve Rule Activation/Deactivation requests.
   - Select **Remediation** if this role can approve Remediation requests. FortiSIEM recommends creating at least two user accounts with the Remediation approver role. See Adding Users for more information on creating a user account.
7. Select the appropriate **Activation** capability:
   - Select **Report Schedule** if this role does NOT require approval for Report Schedule Activation.
   - Select **Rule Activation/Deactivation** if this role does NOT require approval for Rule Activation/Deactivation.
   - Select **Remediation** if this role does NOT require approval for Remediation Activation.
8. Select the **Data Obfuscation** options for this role:
   - **System Event/CMDB Attribtues** to anonymize IP, User and Email, or Host Name in the events.
   - **Custom Event Attributes** to anonymize custom event attributes. Search or click **+** to include multiple attributes. To create a custom event attribute, see Adding an Event Attribute.

   Note: If Data Obfuscation is turned on for a FortiSIEM user:
   - The value for that object marked for data obfuscation is obfuscated. For example, if IP is marked for data obfuscation, the IP address is obfuscated. In earlier versions of FortiSIEM, raw events were completely obfuscated.
   - CSV Export feature is disabled.

   Note: If Remediation is turned on, the requestor and approver users must have a valid email address, configured in the **Email** field in Contacts, in order for the requestor and approver to receive requests and approval information.
9. Select the **UI Access** conditions for this role.
   This defines the user interface elements that can be accessed by users with this role. By default, the child nodes in the tree inherit the permissions of their immediate parent, however you can

override those default permissions by explicitly editing the permission of the child node. The options for these settings are in the **All Nodes** drop-down list:

- **Full** - No access restrictions.
- **Edit** - The role can make changes to the UI element.
- **Run** - The role can execute processes for the UI element.
- **View** - The role can only view the UI element.
- **Hide** - The UI element is hidden from the role.

10. Click **Save**.

Hiding Network Segments

If a **Network Segment** is marked as hidden for a user role, users with that role will not be able to see any of the devices whose IP addresses fall within that network segment, even if the CMDB folder(s) containing those devices have not been hidden.

Modifying a Role

Complete these steps to modify a cloned or user defined role. (You cannot directly modify a system defined role):

1. Select the role from the table.
2. Click the required option:
   a. **Edit** to modify any role setting.
   b. **Delete** to remove a role.
   c. **Clone** to duplicate a role.
3. Click **Save**.

Example Role Setup

- Setting Up an Incident Remediation Workflow Example

Setting Up an Incident Remediation Workflow Example

You will need at least one user as an incident remediation approver, and one user as a requester that requires approval for incident remediation. This example assumes you have incident remediation configured.

From here, take the following steps as an admin:

1. Create a role for an incident remediation approver by taking the steps in Add a New Role and ensuring in step 6 that the role can approve incident remediation, which we'll call Approver.

2. Create a user with the Approver role by taking the steps in Adding Users, and ensuring that step 4 (**Contacts**) is configured correctly, and that a valid email address is provided.
   Note: A requester can select multiple approvers when making a request. For real world scenarios, Fortinet recommends creating a minimum of two approvers, in case an approver is unavailable.
3. Create a requester user by taking the steps in Adding Users, and ensuring the following:
   - A non-admin role is assigned in step 5dkii (**FortiSIEM Role**).
     Note: By default, a non-admin role requires approval for incident remediation. If you want to create/edit a non-admin role where a user does NOT need to get approval for incident remediation, you would add a checkmark to **Remediation** at **Activation** in step 7 in Add a New Role.
   - A valid email address is provided in step 4 (**Contacts**).
4. Log out of FortiSIEM, and log in as the requester user.
5. Navigate to **INCIDENTS > List by Time >** and select an incident.
6. Click on **Actions**, and select **Remediate Incident**.
7. From the **Remediation** drop-down list, select a remediation script and select **Run**. A **Create New Request** window will appear with the message "No permission to run Remediation. Send a permission request."
8. From the **Approver** drop-down list, select the user with the Approver role that you created.
   Note: The user may select multiple approvers in his/her request, not just one.
9. In the **Justification** field, enter any comments and click **Submit**. This request will appear as "pending" in **TASKS**.
10. Log out of FortiSIEM, and log in as the user with the Approver role. As the "Approver" user, you will see a message stating "You have pending requests. Please check Task > Approval.
11. Navigate to **TASKS** and select **Approval** in the left panel.
12. Select the **Request ID** of the request, and review it. You have the choice to "Approve" or "Reject" the request in the drop-down list, next to the **Status** column. In this situation, select "Approve".
    Note: See Approving a de-anonymization request for more information, including how FortiSIEM handles requests when multiple approvers are involved.
13. An **Approve Request** windows appears, prompting for the expiry timeframe. If we want to make the approval window available for two days, you would select **For**, and input "2" for Days, then click **OK**. The **Status** column is updated with this information.
14. Log out of FortiSIEM, and log in as the requester user.
15. The requester user should have received an email from the user with the approver role, with the title "Remediation Request is approved".
16. Navigate to **TASKS**. In the left panel, select **Request**. In the **Status** column, you will see that the request has been approved.
17. Navigate to **INCIDENTS > List by Time >** and select the incident that was approved for remediation.
18. Click on **Actions**, and select **Remediate Incident**.
19. From the **Remediation** drop-down list, select a remediation script and select **Run**. The remediation script now runs.

Viewing User Roles for AD Group Mappings

To see the AD groups that the user is a member of, go to **CMDB > Users > Member Of**.

The User Roles are explicitly shown in **CMDB > Users > Access Control**.

Mapping AD Groups to Roles

FortiSIEM provides the ability to map Microsoft Active Directory (AD) Groups to Roles. A user mapped to more than one Role has permissions for all roles following the Least Restrictive Role principle described below.

Follow these steps to map an AD Group to a Role:

Step 1: Setup or Edit an Authentication Profile

1. Log in to the FortiSIEM system.
2. Follow the instructions in Adding External Authentication Settings to setup a new profile or edit an existing profile. Currently, only LDAPS and LDAPTLS are supported for mapping AD Groups. The new or edited entry appears in the list of authenticated organizations.

Step 2: Create a Role to be Mapped to the AD Group

Follow the instructions in Adding a New Role to add a role that is to be mapped to an AD Group.

Step 3: Assign an AD Group

1. Click **ADMIN > Settings > Role > AD Group Role**.
2. Click **New** to create a new AD Group mapping or select a row and click **Edit** to edit an existing mapping.
3. Provide the following information in the Add AD Group Role popup:
   - **Organization** - Set to System (all organizations can use the information), Super/Local (only Super/Local can use the information).
   - **AD Group DN** - The AD Group domain name. Currently, the server must be either LDAPS or LDAPTLS.
   - **Mapped Role** - Scroll down the list for the role you want to map to. You can find descriptions of the predefined roles in Role Settings.
   - **Comment** - Enter an optional comment describing the mapping.

Step 4: Test Your Mappings

Test your mappings by logging out of the FortiSIEM session then logging back in as the LDAPS/LDAPTLS user.

You can use either the CN or the SamAccountName as the Username in FortiSIEM.

The following example account illustrates the options:

PS C:\Users\Administrator> Get-ADUser -Identity jdoe

DistinguishedName : CN=J Doe,OU=department1,DC=fortisiem,DC=lab

Enabled : True

GivenName : J

Name : J Doe

ObjectClass : user

ObjectGUID : 2386c3e6-d2c0-47b8-85d0-334585e959f

SamAccountName : jdoe

SID : S-1-5-21-87403157-1919951427-186658781-1620

Surname : Doe

UserPrincipalName : jdoe@fortisiem.lab

- Using the CN as the Username, for example:
  User: J Doe
  Password: ********
  Domain: local
- Using the SamAccountName as the Username, for example:
  User: fortisiem\jdoe
  Password: ********
  Domain: local

Principle of Least Restrictive Role

If a user belongs to two FortiSIEM Roles, then the user will have the rights of BOTH Roles.

- Case 1 - A node is explicitly defined in both role definitions. Then a user belonging to BOTH roles have the union of all permissions for that node. Explicit definitions mean that the node appears in the bottom **Restrictions** area when you view the Role in **Settings > Role > Role Management**. Some examples:

One Role has READ permission on the **RESOURCES** tab, while the other Role has WRITE and EXECUTE permissions on **RESOURCES** tab. Then, a user belonging to BOTH roles has READ, WRITE, EXECUTE on **RESOURCES** tab.

One Role has READ permission on the **RESOURCES** tab, while the **RESOURCES** tab is hidden in the other Role. Then, a user belonging to BOTH roles has READ permission on the **RESOURCES** tab.

- Case 2 - A node is not explicitly defined in one Role but explicitly defined in the other role. Then the user belonging to BOTH roles have the explicit permission defined in the second role. For example, a Full Admin role has nothing explicitly defined, because it has full permission on ALL nodes. If the user belongs to both Full Admin role and another role that can only READ the CMDB tab, then the user has only READ permission on the CMDB tab.
- Case 3 - A node is not explicitly defined in two Roles. Then the user belonging to BOTH roles has full permission on that node.

Compliance Settings

The following sections provide more information about the Compliance settings:

- Compliance PCI Settings

PCI Compliance Policy

This screen allows you to view, create, edit, or delete payment card industry (PCI) logging policies.

- Viewing PCI Policies
- Adding a PCI Logging Policy
- Editing a PCI Logging Policy
- Deleting a PCI Logging Policy

Viewing PCI Policies

The PCI table shows the following PCI attribute information.

PCI Logging Attribute	Description
Device Group Name	The name of the device group with a PCI logging policy.
Authentication	Provides information on last authentication event, if enabled.
FIM	Provides information on last file integrity monitoring (FIM) event, if enabled.
Change	Provides information on when the last change occurred, if enabled.

Adding a PCI Logging Policy

You can create a new PCI logging policy by taking the following steps:

1. From **ADMIN > Settings > Compliance > PCI**, click **New**.
2. From the **Device Group Name** drop-down list, select a device group.
3. Enable your preferred options by checking the appropriate checkboxes. When an option is selected, from the drop-down list, select the report you want the information to be generated from.
   a. Need Authentication
   b. Need FIM
   c. Need Change
4. Click **Save** when done.

Editing a PCI Logging Policy

You can edit a PCI logging policy by taking the following steps:

1. From **ADMIN > Settings > Compliance > PCI**, select an existing policy and click **Edit**.
2. Make any changes to your existing PCI logging policy, and click **Save** when done.

Deleting a PCI Logging Policy

You can delete a PCI logging policy by taking the following steps:

1. From **ADMIN > Settings > Compliance > PCI**, select an existing policy and click **Delete**.
2. Click **Yes** to confirm.

General Settings

- External Authentication Settings
- Automation Policy Settings
- External System Integration Settings
- Case Management Settings
- Configuring SSL Socket Certificates

External Authentication Settings

This section specifies how to configure external authentication for FortiSIEM users. External authentication enables FortiSIEM to offload user authentication to external systems, such as Microsoft Active Directory via (LDAP/LDAPS/LDAPTLS), Azure AD, OKTA, Duo Security and any SAML Provider.

The general configuration steps are described here:

- Configure FortiSIEM Users for non-SAML External Authentication
- Configure FortiSIEM Users for SAML External Authentication

A few concrete examples are provided:

- Example 1: Configure FortiSIEM Users for SAML Authentication with Azure AD
- Example 2: Configuring FortiSIEM Users for RADIUS/LDAP Authentication with FortiAuthenticator (FAC)
- Example 3: Configuring FortiSIEM Users for SAML Authentication with FortiAuthenticator (FAC)
- Example 4: Configuring FortiSIEM Users for SAML Authentication with OKTA
- Example 5: Configuring FortiSIEM Users for 2 Factor Authentication with Duo Security

Some Troubleshooting steps for SAML Configuration are provided here.

Configure FortiSIEM Users for non-SAML External Authentication

Step 1: Create External Authentication Profile

Case 1: LDAP/LDAPS/LDAPTLS Profile

Add LDAP, LDAPS, and LDAPTLS authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**.
5. Set **Protocol** as LDAP or LDAPS or LDAPTLS.
6. Set IP/Host of LDAP server.
7. Change the port if it is different than default port.
8. Check **Check Certificate** if needed.
   This option enables proper X.509 Certificate verification for LDAPS and LDAPTLS. If checked, then

App Server will check if the CN or the subject-alt-name in the Certificate matches the LDAP Server IP address or host name entered in the **External Authentication Profile** dialog. This means that self-signed certificates will fail and a proper certificate needs to be installed on the LDAP Server.

9. Check **Set Base DN** if needed by filling in the DN Pattern field.
   Setting the DN pattern manually is not necessary if the user is discovered via LDAP. However, this feature allows you to manually override the discovered pattern, or enter it for a user that is being manually created. Enter `%s` to represent the user's name (`CN/uid`), for example:
   `CN=%s,CN=Users,DC=accelops,DC=com`
10. Click **Save**.

Case 2: Okta Profile

Add Okta authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**
5. Set **Protocol** as "Okta".
6. Copy and paste the certificate you downloaded during Okta Authentication.
7. Click **Save**.

Case 3: Duo Profile for 2 Factor Authentication

Add a duo (2-factor) external authentication profile as follows:

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter **Name**.
4. Select **Organization**
5. Set **Protocol** as "Duo".
6. In the **IP/Host** field, enter the IP address/host name from the API hostname.
7. In the **Integration Key** field, enter/paste the Integration Key.
8. In the **Secret Key** field, enter/paste the Secret Key.
9. In the Application Key field, enter/paste the Application Key.
10. Click **Save**.

Step 2: Associate User to External Authentication Profile

Case 1: LDAP/LDAPS/LDAPTLS, Okta

To configure a user for all protocols excluding Duo, take the following steps:

1. Log on to FortiSIEM as Admin.
2. Go to **CMDB > Users**.
3. Click **New** to create a new user.
   Note: You may need to navigate to **CMDB > Users > Ungrouped**.
4. Click **System Admin**.
5. From the **Mode** drop-down list, select **External**.
6. From the **Authentication Profiles** drop-down list, select your user profile.
7. Set the user's Role.
8. When done, click **Save**.

Case 2: Duo for 2 Factor Authentication

To configure a user for Duo protocol, take the following steps:

1. Log on to FortiSIEM as Admin.
2. Go to **CMDB > Users**.
3. Click **New** to create a new user.
   Note: You may need to navigate to **CMDB > Users > Ungrouped**.
4. Click **System Admin**.
5. In the **Password** and **Confirm Password** fields, enter the user's password.
6. Select the **Second Factor** checkbox, and select your Duo (2 Factor authentication) profile.
7. Select a **Default Role** from the drop-down list.
8. When done, click **Save**.

Configure FortiSIEM Users for SAML Authentication

- Step 0: Overview
- Step 1 - Preparation
- Step 2 - Create External Authentication Profile in FortiSIEM
- Step 3 - Create SAML Role Mappings in FortiSIEM
- Step 4 - Create the User in CMDB

Step 0: Overview

In SAML authentication, there are 3 entities:

- Identity Provider (IDP) - this is where user authentication happens. There are many examples, OKTA, Entrust, etc...

- IDP Portal - this is where you define users and credentials for your IDP and Service Providers.
- Service Provider (SP) - this is where the user logs on after authentication succeeds, e.g. FortiSIEM in this case.

After configuration, the flow is as follows:

1. The user authenticates on to the IDP Portal.
2. The user clicks a FortiSIEM icon on the IDP Portal.
3. IDP sends a SAML response to FortiSIEM containing the User, Org, and Role. User and Org are required, while Role is optional.
4. FortiSIEM trusts the IDP and logs in the User with the right Org and Role (if applicable).
   Note: You cannot use FortiSIEM default login page with SAML.

To ensure SAML works correctly, the following must be done.

1. Define URLs and credentials in IDP Portal and FortiSIEM so that they can securely communicate with each other.
2. Map the User, Org, and Role in the IDP Portal to the User, Org, and Role in FortiSIEM. The User must be an exact match, including case-sensitivity. For Org and Role, you can define mappings in FortiSIEM for IDP Org to FortiSIEM Org and IDP Role to FortiSIEM Role.

The following is a detailed example showing the steps required for configuration. This example assumes a FortiSIEM user has already been created in an IDP Portal.

Step 1 - Preparation

1. Configure your IDP for the specific User, Organization, and Role. Collect IDP Portal endpoint and certificate.
2. Study the SAML Response from your IDP and determine where to find the User, Org, and Role. Typically, the User is in the NameIdentifier element of the Subject statement. Org is in the Audience element of AudienceRestriction.

This step is different for every IDP vendor. See the representative example below for Okta.com. In OKTA.com, there is no Role information.

Step 2 - Create External Authentication Profile in FortiSIEM

1. Log on to FortiSIEM as Admin.
2. Go to **ADMIN > Settings > General > External Authentication**.
3. Click **New** to create an External Authentication profile.
   a. (Service Provider Case) Set **Organization** to **System** if any User from any Org can use this profile. Otherwise, set it to the specific Org.
   b. In the **Protocol** drop-down list, select **SAML**.
   c. Fill in the **Issuer** and **Certificate** (credentials) fields using the information collected in Step 1 - Preparation.

d. Set **User** to the specific field in the SAML Response containing the User information. (note - match is exact and case-sensitive). This information was gathered in Step 1B. If the User is not in the NameIdentifier element of the Subject Statement, then select **Custom Attribute** and enter the field containing the User information.
e. Set **Org** to the specific field in the SAML Response containing the Org information. This information was gathered in Step 1 - Preparation. If Org is not in the Audience element of AudienceRestriction, then select **Custom Attribute** and enter the field containing the Org information. Matching is determined by the Role mapping rules in Step 3.
f. If Role is present in the SAML Response from the IDP, then select **Custom Attribute** and enter the field containing the Role information. Otherwise, select **None**. In the later case, you must create the User in CMDB for the specific Org, and assign the right Role. Step 3 is not needed.

Step 3 - Create SAML Role Mappings in FortiSIEM

This step is only needed if Role is present in the SAML Response as in Step 2 - 3f. For example, OKTA does not have Role, so this step is not needed.

1. Log on to FortiSIEM as Admin.
2. Go to **ADMIN > Settings > Role > SAML Role**.
3. Click **New**.
4. In the Add SAML Role, enter the following information.
   a. From the **SAML Auth profile**, select the user.
   b. In the **SAML Role** field, enter the SAML Role.
   c. In the **SAML Organization** field, enter the SAML Organization.
   d. From the **Mapped Role** drop-down list, select an existing role.
   e. From the **Mapped Organization** drop-down list, select an organization.
   f. (Optional) In the **Comments** field, enter any information you may wish to reference at a future date.
   g. Click **Save**.

Step 4 - Create the User in CMDB

This step is only needed if Role is not present in the SAML Response, as in Step 2 - 3f. For example, OKTA does not have Role, so this step is needed.

1. Log on to FortiSIEM as Admin.
2. Go to **CMDB > Users**.
3. If the SAML user is not present, then click **New** to create a new user.
   Note: You may need to navigate to **CMDB > Users > Ungrouped**.
4. In the **User Name** field, enter the name exactly as that used in Step 2 -3f. The name must match exactly, including case-sensitivity.
5. Click **System Admin** and set the Role.
6. When done, click **Save**.

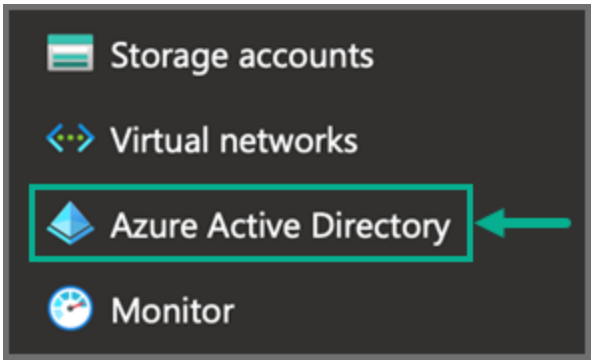
This procedure is described in more details in Adding Users.

Example 1: Configure FortiSIEM Users for SAML Authentication with Azure AD

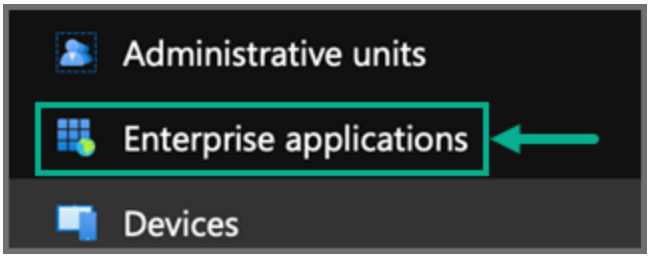
- Step 1: Setup Azure
- Step 2: Setup FortiSIEM
- Step 3: Setup SAML Role Mapping

Step 1: Setup Azure

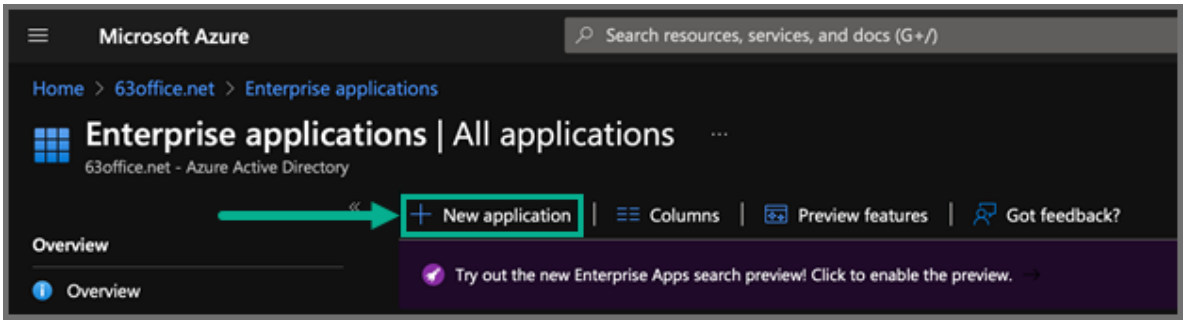
1. In Azure, navigate to **Azure Active Directory**.



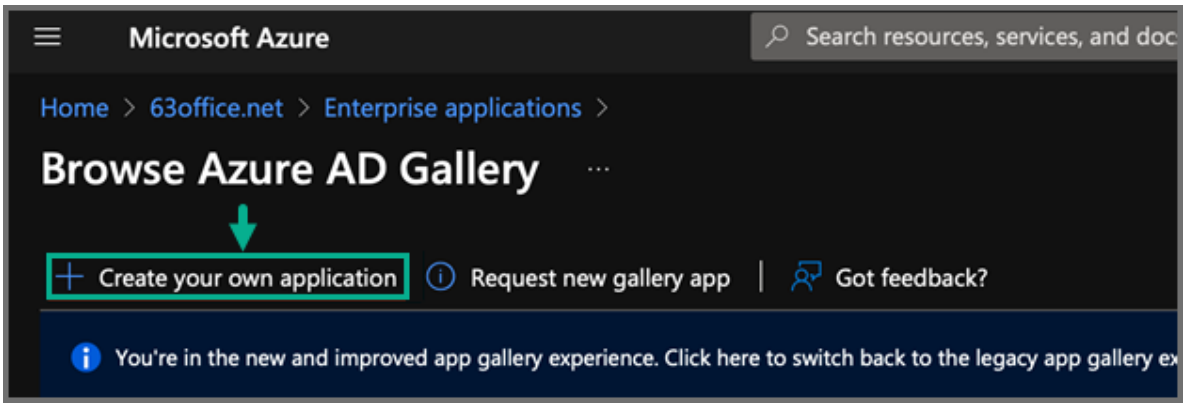
2. Navigate to **Enterprise applications**.



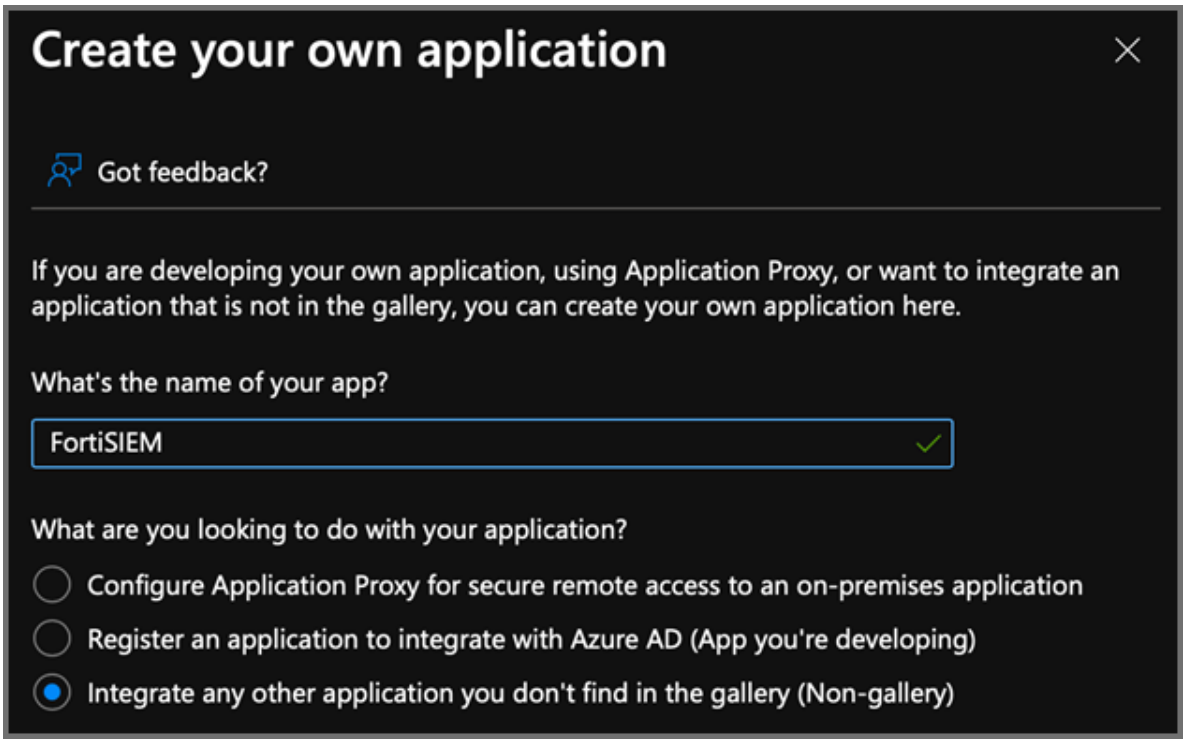
3. Select **New application**.



4. Select **Create your own application**.

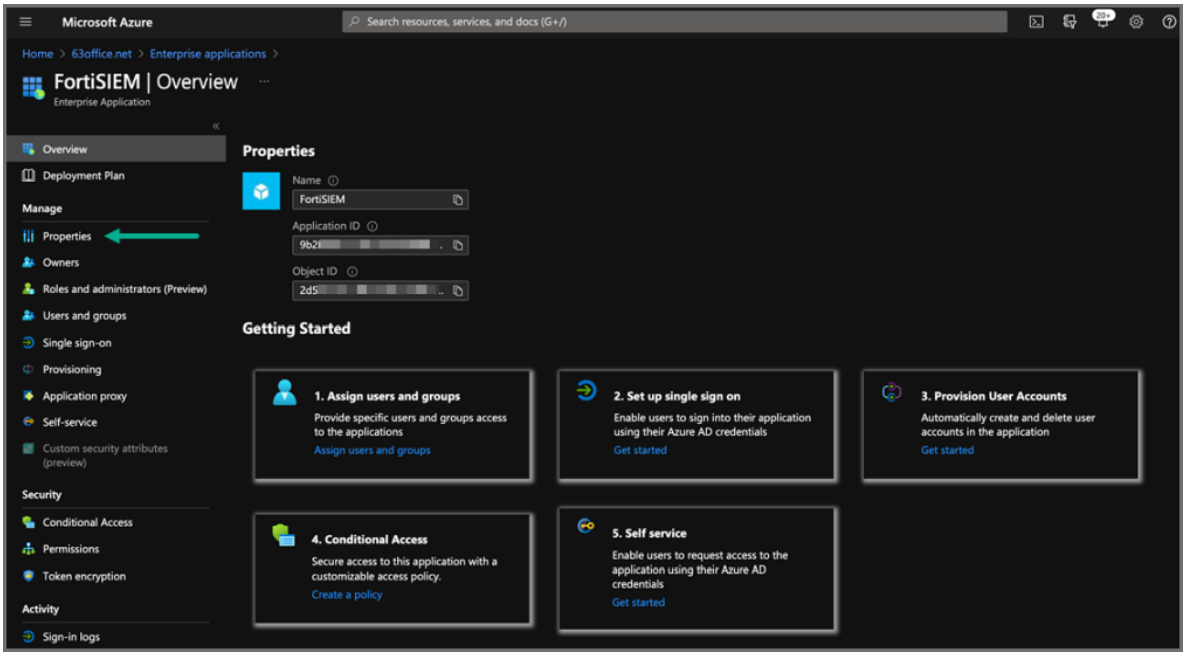


5. For "What's the name of your app?", enter a name, such as FortiSIEM.
6. For "What are you looking to do with your application?", select **Integrate any other application you don't find in the gallery (Non-gallery)**.

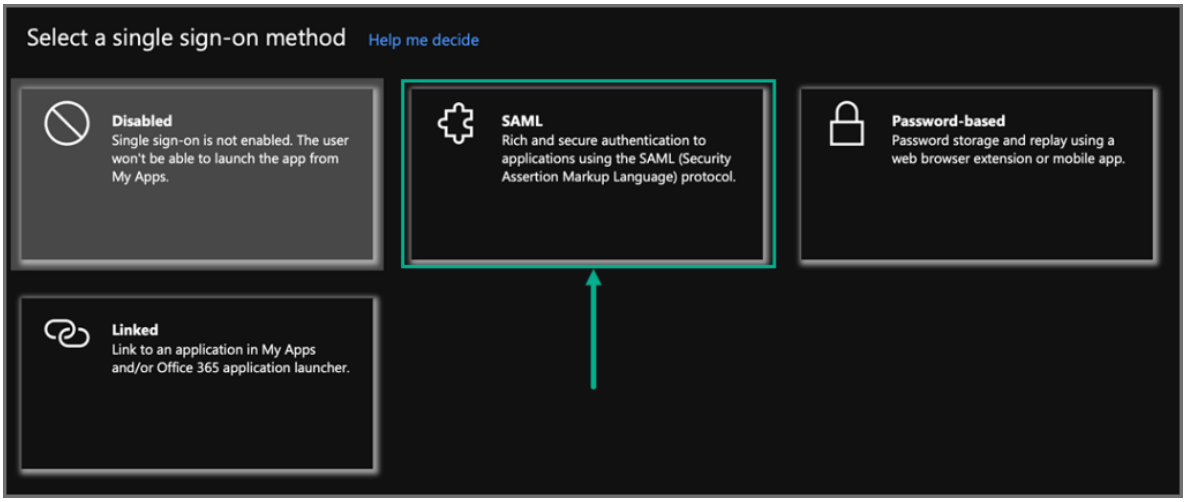


After the application has been created, take the following steps:

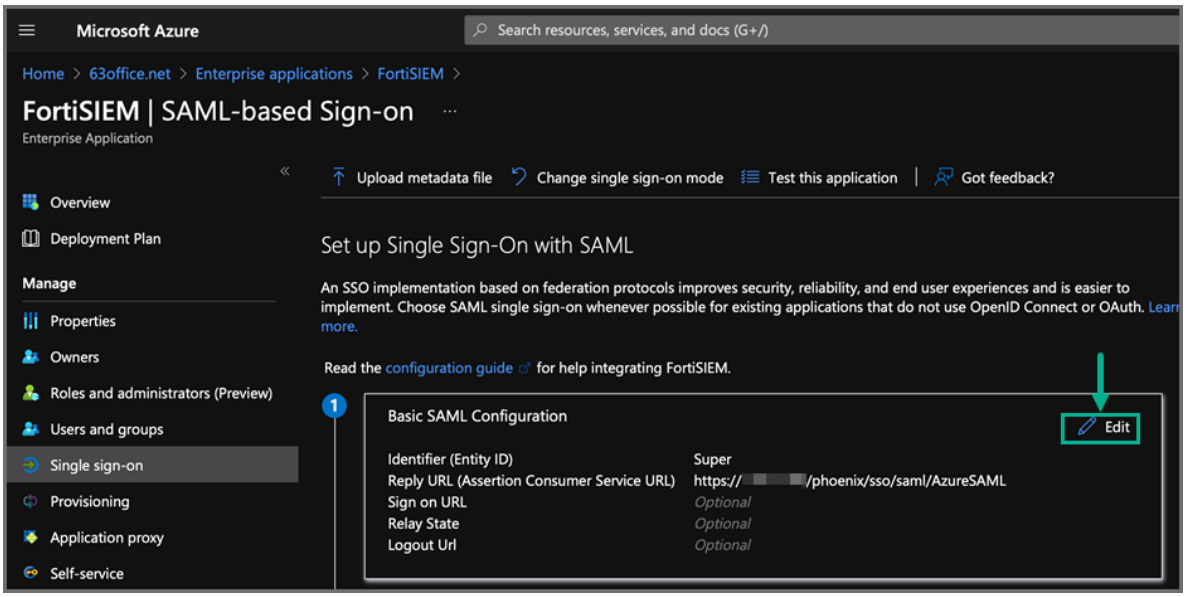
1. From the **Azure Active Directory**, select your new application.
2. Display the **Properties**.



3. Under **Getting Started**, under options **1. Assign users and groups**, select the **Assign users and groups** link and ensure you have some users and groups defined who will be able to access the new application.
4. Under option 2. Set up single sign on, click the **Get started** link, and select **SAML**.



5. Under the **Set up Single Sign-On with SAML** options, click **Edit** for **Step One: Basic SAML Configuration**.



6. For **Identifier (Entity ID)** and **Reply URL**, enter the following information whether you plan to use Option 1 or Option 2.
   Note: The difference between the two options suggested is that for the Option 2 FortiSIEM interface, you need to specify which SAML schema attribute will determine the Organization at login.

Option 1 - Using the Default Org Mapping in FortiSIEM	
Identifier (Entity ID)	*<FortiSIEM Org Name>* For example, enter **Super** for Enterprise installations or the name of your new Organization created in a Multi-Tenant installation.
Reply URL	`https://<fsm ip or fqdn>/phoenix/sso/saml/<external authentication profile name>`

In the FortiSIEM Authentication Profile, the default value of “AudienceRestriction” will be used.

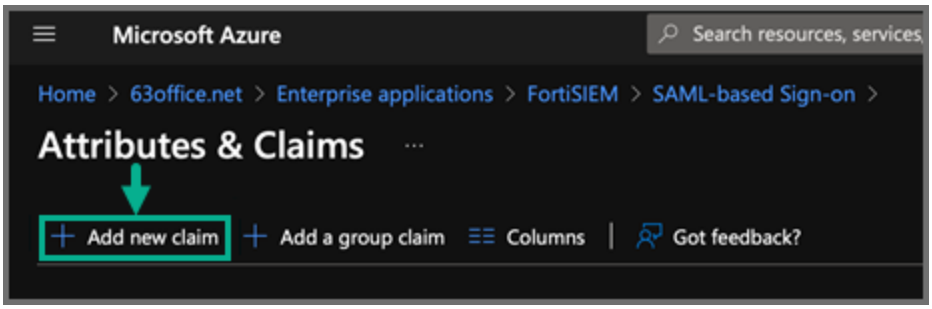
Option 2 - Using a Custom Attribute to Define the Org Mapping in FortiSIEM	
Identifier (Entity ID)	Anything you like.
Reply URL	`https://<fsm ip or fqdn>/phoenix/sso/saml/<external authentication profile name>`

7. Under **Step Two: Attributes & Claims**, click **Edit**.

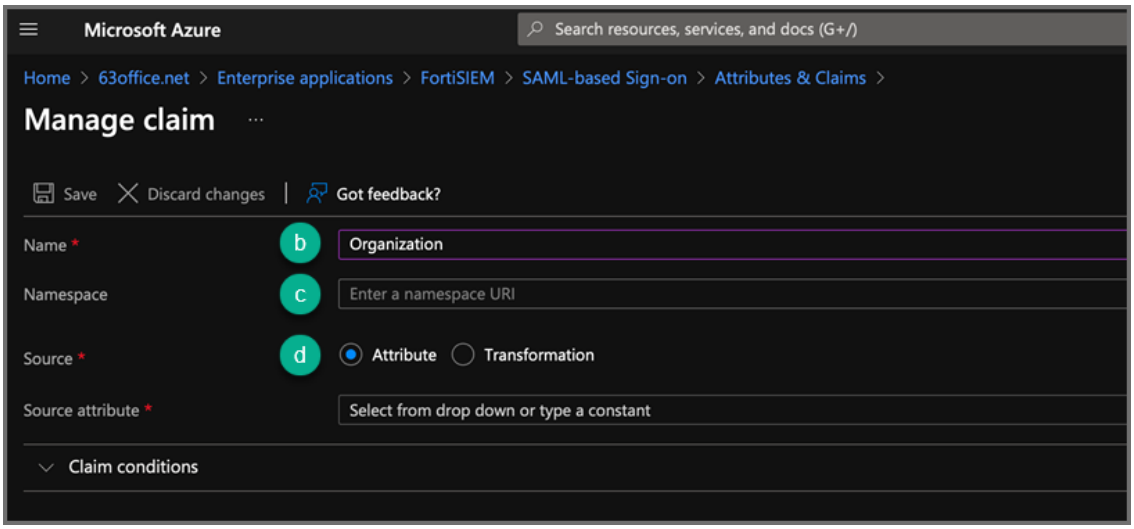
Here is where the SAML response can be manipulated to add extra attributes which can be used to

tell FortiSIEM the Org to use at login (If Option 2 is used above), and also a Role name to be assigned at Login, if the user does not exist already in the FortiSIEM CMDB.
Take the following steps to add an attribute for Organization, if Option 2 is being used above.

a. Click **Add new claim**.

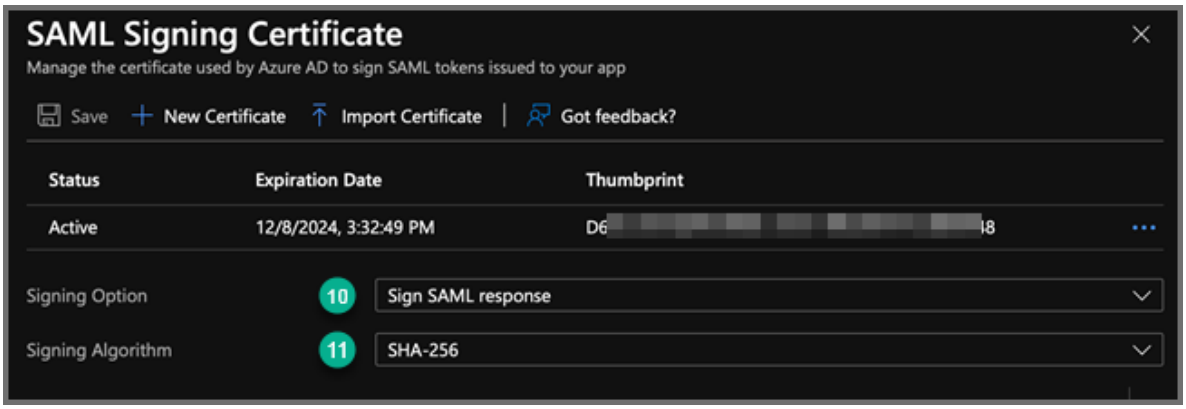


b. In the **Name** field, enter the Custom Attribute to use, for example: Organization.
c. For **Namespace**, leave the field blank.
d. For **Source**, make sure “Attribute” is selected and then under Source attribute select the drop-down and then type a value such as the Organization name or an Identifier you will use in FortiSIEM to map to the correct Org.
Note: Alternatively, one of the predefined Azure Values can be used such as `user.companyname` if those values are populated in the directory. (Just make sure the Name of the attribute does not contain any characters other than letters, underscore or dash.)



8. Take the following steps to add an attribute for Role.
   a. Click **Add new claim**.
   b. In the **Name** field, enter the Custom Attribute to use, for example: **myRole**.
   c. For **Namespace**, leave the field blank.
   d. For **Source Attribute**, set it to be a value for the Role.
9. Under **Step Three: SAML Signing Certificate**, click **Edit**.
10. For the **Signing Option**, select **Sign SAML Response**.

11. For the **Signing Algorithm**, select **SHA-256**.



12. Click **Save**.
13. Exit back to the configuration by clicking the **X** in the top right corner, and then **Download the Certificate in Base64** encoded format. (This will be needed in step 3e. under Step 1: Setup FortiSIEM.)
14. Under **Step Four: Set up FortiSIEM**, copy the **Azure AD Identifier** string. (This will also be needed below to be input into FortiSIEM)

Step 2: Setup FortiSIEM

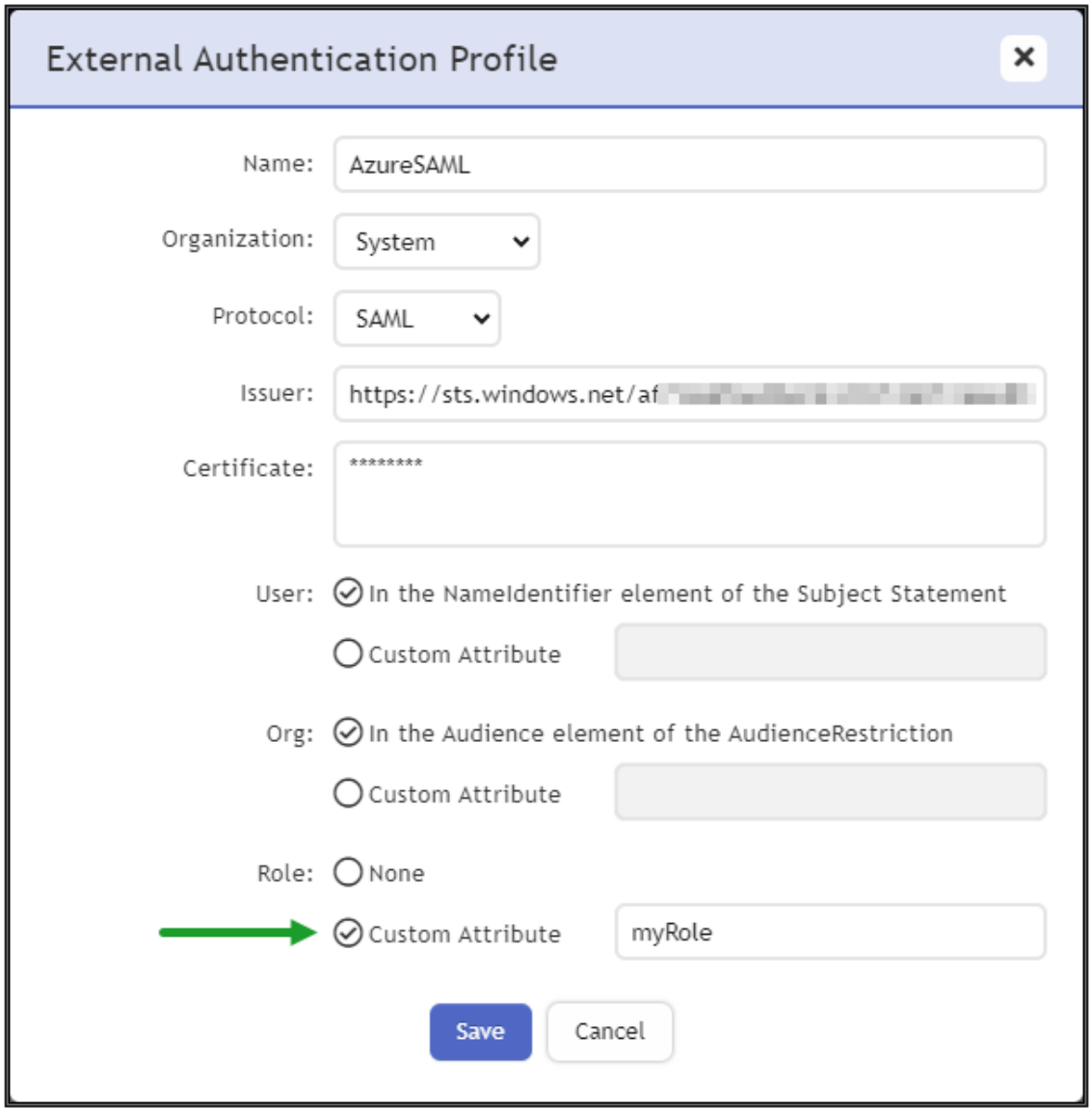
In FortiSIEM, take the following steps:

1. Navigate to **ADMIN > Settings > General > External Authentication**.
2. Click **New**.
3. In the External Authentication Profile window, take the following steps:
   a. In the **Name** field, enter a name, for example, AzureSAML.
   b. In the **Organization** drop-down list, select your Organization.
   c. In the **Protocol** drop-down list, select **SAML**.
   d. In the **Issuer** field, paste the **Azure AD Identifier**.
   e. In the **Certificate** field, paste the certificate information.

   f. In the **User** section, leave the default option “In the NameIdentifier element of the Subject Statement” selected.

g. In the **Org** section, take the following steps:
   i. If Option 1 was used at step (6) in Azure setup, then leave the default option of "In the Audience element of the AudienceRestriction" selected.
   ii. If Option 2 was used, then select **Custom Attribute** and enter the name of the Attribute created at step (7b) in the Azure set up above.

h. In the **Role** section, select **Custom Attribute** and enter the name of the Attribute created at step (8d) in the Azure set up above.



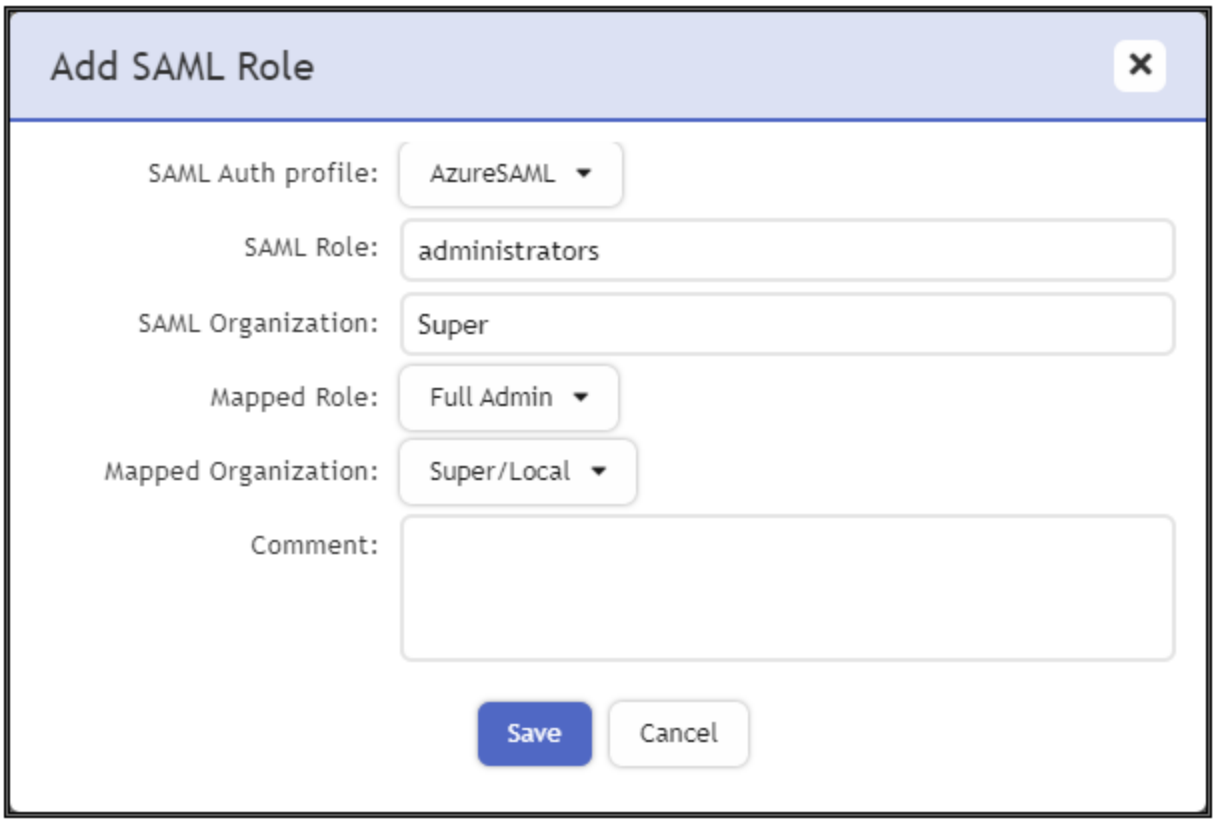
i. Click **Save** when done.

Step 3: Setup SAML Role Mapping

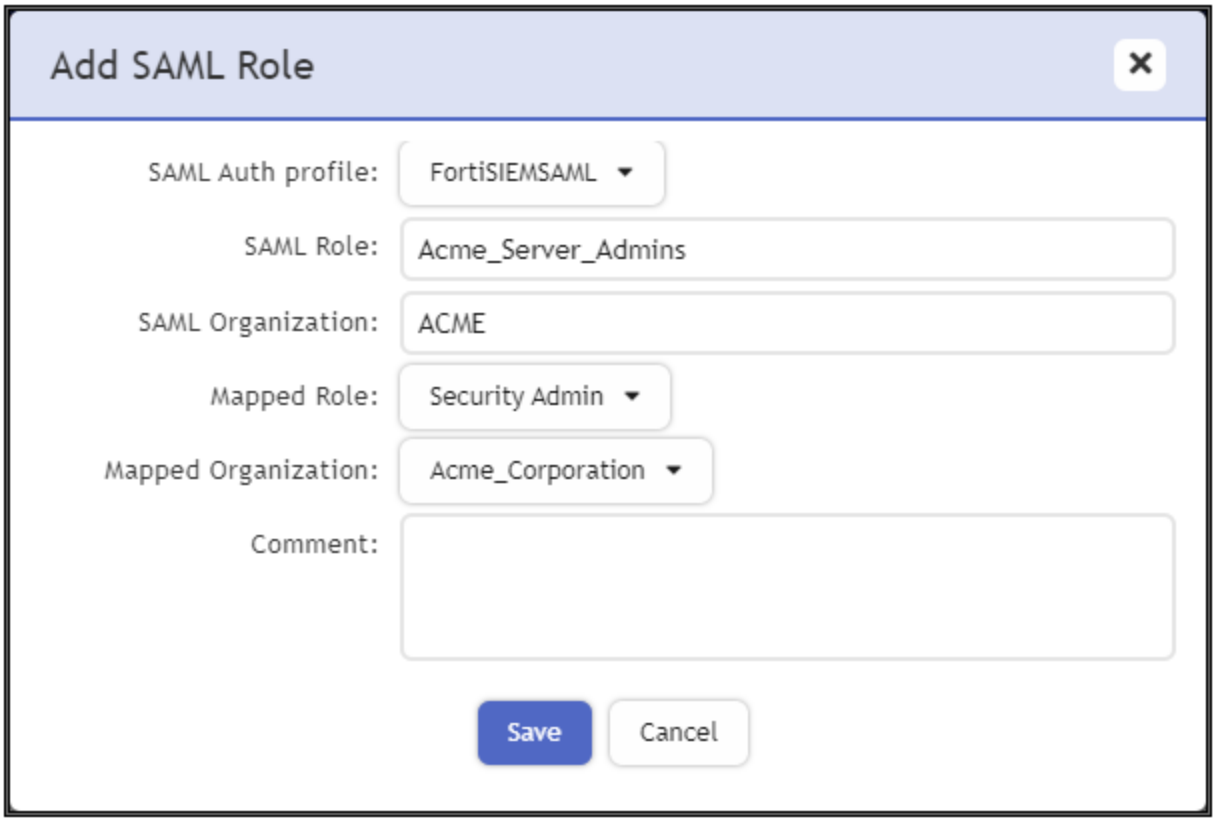
1. Log into the FortiSIEM GUI as a user with Admin rights and navigate to **ADMIN > Settings > Role > SAML Role**.

2. Click **New**.
3. From the Add SAML Role window, take the following steps.
   a. From the **SAML Auth profile** drop-down list, select the External SAML Authentication Profile created above.
   b. For the **SAML Role** field, enter the value being output in the SAML response which should be the Source Attribute value entered at Azure set up step (8d).
   c. For the **SAML Organization** field, enter the value being output in the SAML response which should be the Identifier (Entity ID) at Azure set up step (6) if Option 1 was used, or the Source Attribute value entered at Azure set up step (7c) if Option 2 was used.
   d. For the **Mapped Role** drop-down list, select the FortiSIEM Role to assign based upon a matching value.
   e. For the **Mapped Organization** drop-down list, select the FortiSIEM Organization to assign based upon a matching value.
   f. Click **Save**.

Here is an example of an Enterprise mapping. The SAML Organization for an Enterprise mapping is **Super**.



Here is an example of a Multi-Tenant mapping.



Example 2: Configuring FortiSIEM Users for RADIUS/LDAP Authentication with FortiAuthenticator (FAC)

- Step 1: Configure AD Users
- Step 2: Configure FortiAuthenticator
- Step 3: Configure FortiSIEM

Step 1: Configure AD Users

1. Install AD Domain Services following the steps here.
2. Configure the test domain users:
   a. **Server Manager** > **Tools** > **Active Directory Users and Computers**.
   b. Expand the Domain, right-click **Users**, select **New** > **User**.

Step 2: Configure FortiAuthenticator

1. Perform the basic FAC setup following the steps in the *FortiAuthenticator Administration Guide: Section: FortiAuthenticator-VM image installation and initial setup* here.
   a. Use the default credentials:
      - user name: `admin`
      - password: <blank>
   b. At the CLI prompt enter the following commands:
      - `set port1-ip 192.168.1.99/24`
      - `set default-gw 192.168.1.2`

      Note that the CLI syntax has changed in FAC 5.x. Refer to a 6.x FortiAuthenticator Administration Guide for details.
   c. Log in to the FAC GUI (default credentials user name / password: `admin` / `<blank>`).
   d. Set the time zone under **System** > **Dashboard** > **Status** > **System Information** > **System Time**.
   e. Change the GUI idle timeout for ease of use during configuration, if desired: **System Administration** > **GUI Access** > **Idle Timeout**.
2. Configure the DC as a remote LDAP server under **Authentication** > **Remote Authentication Servers** > **LDAP**.
   Follow the Fortinet Single Sign-On instructions in the appropriate FortiAuthenticator Administration Guide. Note that the user must have appropriate privileges. The Domain Admin account can be used for testing in a lab environment. The 'Remote LDAP Users' section will be blank at this stage, users are imported later.
3. Configure an external Realm to reference the LDAP store:
   a. Select **Authentication** > **User Management** > **Realms** > **Create New**.
   b. Choose the LDAP source from the drop-down and click **OK**.
4. Configure the FortiSIEM as a RADIUS Client:
   a. Select **Authentication** > **RADIUS Service** > **Clients** > **Create New**.
   b. Enter the IP address of FortiSIEM and a shared secret.
   c. Choose the realms as required.
   d. Click 'add a realm' to include multiple realms.
      Note the FAC evaluation license only supports 2 realms.
   e. Click **Save**.
5. Import users from LDAP to FortiSIEM to allow FortiToken to be used:
   a. Select **Authentication** > **User Management** > **Remote Users**.
   b. Select the **Import** button.
   c. Choose and import the test users configured in AD. Note that the FAC Evaluation license is limited to 5 users.
6. (Optional) Configure local users in the FAC database for local authentication under **Authentication** > **User Management** > **Local Users**.
7. Provision the FortiToken:
   a. Select and edit the user in **Authentication** > **User Management** > **Remote Users** (or Local Users as appropriate).
   b. Select the **Token Based Authentication** check box, and assign an available FortiToken Mobile. FAC evaluation includes 2 demo FortiTokens.

c. Choose **Email** delivery method and enter an email address in user information.
The email address doesn't have to be valid for basic testing, the provisioning code is visible in the FAC logs.
d. Click **OK**.

8. Configure the FortiToken iPhone app:
a. Install the FortiToken app from the app store.
b. Open the app and select the **+** icon in the top right corner.
c. Choose **enter manually** from the bottom of the screen.
d. Select and edit the user in **Authentication** > **User Management** > **Remote Users** (or Local Users as appropriate).
e. Select the **Token Based Authentication** check box, and assign an available FortiToken Mobile. FAC eval includes 2 demo FortiTokens.
f. Choose **Email** delivery method and enter an email address in user information. The email address doesn't have to be valid for basic testing, the provisioning code is visible in the FAC logs.
g. Click **OK**.

Step 3: Configure FortiSIEM

Step A: Configure an External Authentication Source

1. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
2. Click **New**.
3. Enter the following settings:
   - **Organization** - System
   - **Protocol** - RADIUS
   - **IP/Host** - IP of FortiAuthenticator
   - **Shared Secret** - Secret configured when setting RADIUS Client in FAC
4. Click **Save**.
5. Click **Test** to test the authentication settings.

Step B: Configure Users in FortiSIEM Database

1. Go to **CMDB** > **Users** and click **New**.
2. Enter the user name to match the user configured in FSM/AD. (Use the format: user@domain.com)
3. Select the **System Admin** checkbox.
4. Select the **Mode** as **External**.
5. Select the RADIUS profile previously configured from **Authentication Profiles**.
6. Select the **Default Role** from the list.
7. Click **Save**.

Logging In

The **User Name** must be entered in the format `user@domain.xyz`. For 2-factor authentication, the password and FortiToken value must be concatenated and entered directly into the **Password** field.

For example:

- Username: `user123@testdomain.local`
- Password : `testpass123456`; where `123456` is the current FortiToken value

Note: FortiAuthenticator logs are accessible by opening the **Logging** tab. Select a log entry to see more details.

Example 3: Configuring FortiSIEM Users for SAML Authentication with FortiAuthenticator (FAC)

FortiSIEM supports integrating with customer SSO (Single Sign On) authentication by supporting the SAML2.0 standard. After configuration is completed, the user login flow experience will be:

1. User logs into Customer controlled SSO portal.
2. FortiSIEM appears as an application in that portal.
3. User selects the FortiSIEM application from the portal.
4. User is authenticated and logged into the FortiSIEM admin interface

This example shows how to integrate FortiSIEM with FortiAuthenticator, with these general steps.

- Set Up FortiAuthenticator as an IdP
- Add FortiSIEM as Service Provider
- Set Up FortiSIEM
- Set Up SAML Role Mapping
- Import Users from FortiAuthenticator

Set Up FortiAuthenticator as an IdP

To set up FortiAuthenticator (FAC) as the identity provider (IdP), take the following steps.

Note: Steps taken from the 6.5.3 FortiAuthenticator Guide. See https://docs.fortinet.com/document/fortiauthenticator/6.5.3/administration-guide/864572.

1. Navigate to **Authentication > SAML IdP > General**.
2. Select **Enable SAML Identity Provider portal**.

3. Configure the following settings:

Setting	Description
Device FQDN	To configure this setting, you must enter a **Device FQDN** in the **System Information** widget in the **Dashboard**.
Server address	Enter the IP address or FQDN of the FortiAuthenticator device.
IdP-initiated login URL	The URL used to access the IdP portal in an IdP-initiated login scenario. Service Providers (SPs) configured in FortiAuthenticator must have the option **Support IdP-initiated assertion response** enabled in order to be listed in the portal.
Username input format	Select one of the following three username input formats: • username@realm • realm\username • realm/username
Captcha	The state of the optional IP lockout CAPTCHA settings. **Note**: The option is read-only. Select the pen icon to edit the IP lockout CAPTCHA settings in Lockouts.
Use default realm when user-provided realm is different from all configured realms	When enabled, FortiAuthenticator selects the default realm for authentication when the user-specified realm is different from all configured realms.
Realms	Realms Select **Add a realm** to add the default local realm to which the users will be associated. Use **Groups** and **Filter** to add specific user groups. **Note**: The maximum number of allowed realms is equal to the maximum number of realms in the legacy self-service portal plus the realms in SAML IdP. A maximum of 100 realms can be added.
Legacy login sequence	When enabled, the legacy sequence requests username and password on the same form. When disabled, only the username is requested on the first form. The option is disabled by default. **Note**: When doing IdP proxy to multiple remote SAML IdP servers, keep this option disabled. IAM login: Enable to allow IAM login. **Note**: The option is now only available when **Legacy login sequence** is enabled.
Trusted endpoint single sign-on	When enabled, SSOMA endpoints can log in without reentering username and password. The username login page includes a **Trusted Endpoint Single Sign-On** button that allows single sign-on for trusted endpoints. The legacy login page does not offer the **Trusted Endpoint Single Sign-On** button. The option is disabled by default.

Setting	Description
	Note: **Trusted endpoint single sign-on** and **Legacy login sequence** options are mutually exclusive. Listening port: Trusted endpoints TLS-connect to this TCP port to present their client certificate to the FortiAuthenticator (default = 8008). Enforce MFA: When enabled, FortiAuthenticator enforces token-based settings configured for the SP during trusted endpoint single sign-on. When disabled, token-based verification is bypassed for trusted endpoints. **Note**: The option is only available when **Trusted endpoint single sign-on** is enabled. Enforce IP matching: When enabled, the source IP address of the endpoint connecting to the listening port must match one of the IP addresses reported by the SSOMA to do a successful trusted endpoint authentication. For example, if the endpoint is on a private network and its connection to the FortiAuthenticator is being NAT'ed, this option should be disabled.
Login session timeout	Set the user's login session timeout limit between 5 - 1440 minutes (one day). The default is 480 minutes (eight hours).
Default IdP certificate	Select a default certificate the IdP uses to sign SAML assertions from the drop down menu.
Automatically switch IdP certificate before its expiry time	Enable and select a **New default IdP certificate** from the drop down menu. Switch at: Enter a date (YYYY-MM-DD) and time when the new default IdP certificate applies. Alternatively: Use the calendar icon to select a date. For changing time, select the clock icon and choose a time from the list. **Note**: Select **Today** to switch to today's date or select **Now** to switch to the time now.
Default signing algorithm	Select a default signing algorithm from the drop down menu.
Get nested groups for user	Enable to get nested groups for Windows AD users.
Use geolocation in FortiToken Mobile push notifications	Enable to use geolocation in FortiToken Mobile push notifications.

4. Select **Save** to apply any changes that you have made.

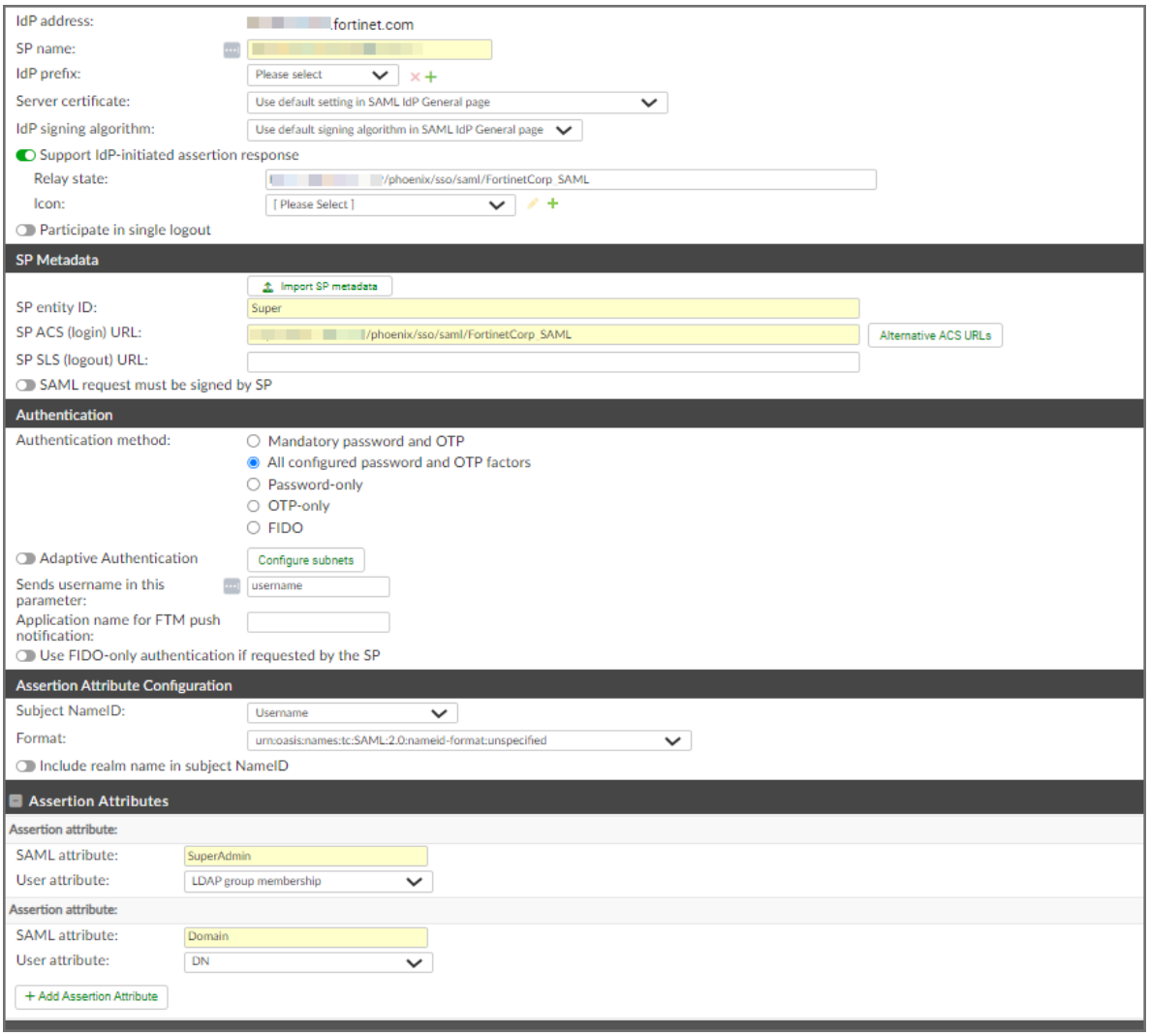
Add FortiSIEM as Service Provider

Once FortiAuthenticator is set up as an IdP, you must add applications or “Service Providers” such as FortiSIEM to the FortiAuthenticator configuration.

Take the following steps:

Note: Steps taken from the 6.5.3 FortiAuthenticator Guide. See https://docs.fortinet.com/document/fortiauthenticator/6.5.3/administration-guide/19212

1. Navigate to **Authentication -> SAML IdP -> Service Providers**.
2. Click **Create New**.
3. Enter the following information:
   a. In the **SP Name** field, enter "FortiSIEM", or any name you prefer. The name entered here is displayed in the SSO portal as an application.
   b. Enable **Support IdP-initiated Assertion response**.
      i. In the **Relay state** field, enter `https://<IP or FQDN of FortiSIEM Supervisor>/phoenix/sso/saml/<profileName>`
      Note: The profile name, such as “FortiSIEM_SAML” will be configured in FortiSIEM later. The name here and in the FortiSIEM configuration must EXACTLY match. E.g. If the following was used for Relay state `https://192.0.2.0/phoenix/sso/saml/Corp_SAML`, in FortiSIEM, the SAML external auth profile MUST be named “Corp_SAML”.
   c. In the **SP entity ID** field, referred to as the Audience, enter <*FortiSIEM organization*>
   Note: This MUST exactly match the FortiSIEM organization the authentication is for. For enterprise customers, this is always “Super”, but for multi-tenant SIEMs it could be “org1” etc...
      i. In the **SP ACS (Login) URL** field, enter `https://<IP or FQDN of FortiSIEM Supervisor>/phoenix/sso/saml/<profileName>`
      Note: The profile name, such as “FortiSIEM_SAML” will be configured in FortiSIEM later. The name here and in the FortiSIEM configuration must EXACTLY match. E.g. If the following was used for Relay state `https://192.0.2.0/phoenix/sso/saml/Corp_SAML`, in FortiSIEM, the SAML external auth profile MUST be named “Corp_SAML”.
   d. From the **Authentication method** selection, choose **All configured password and OTP factors**.
   e. In the **Sends username in this parameter** field, enter "username".
   f. From the **Subject NameID** drop-down list, select **Username**.
   g. In the **Format** field, enter "urn:oasis:names:tc:SAML2.0:nameid-format:unspecified".
   h. Click **Save**.
   FortiAuthenticator is now configured.
4. Download the FAC public certificate to a file as it is needed in the next step for configuring FortiSIEM.

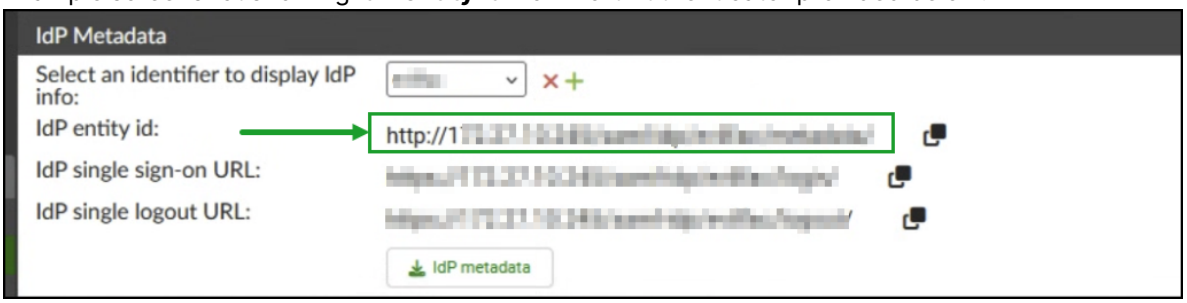


Set Up FortiSIEM

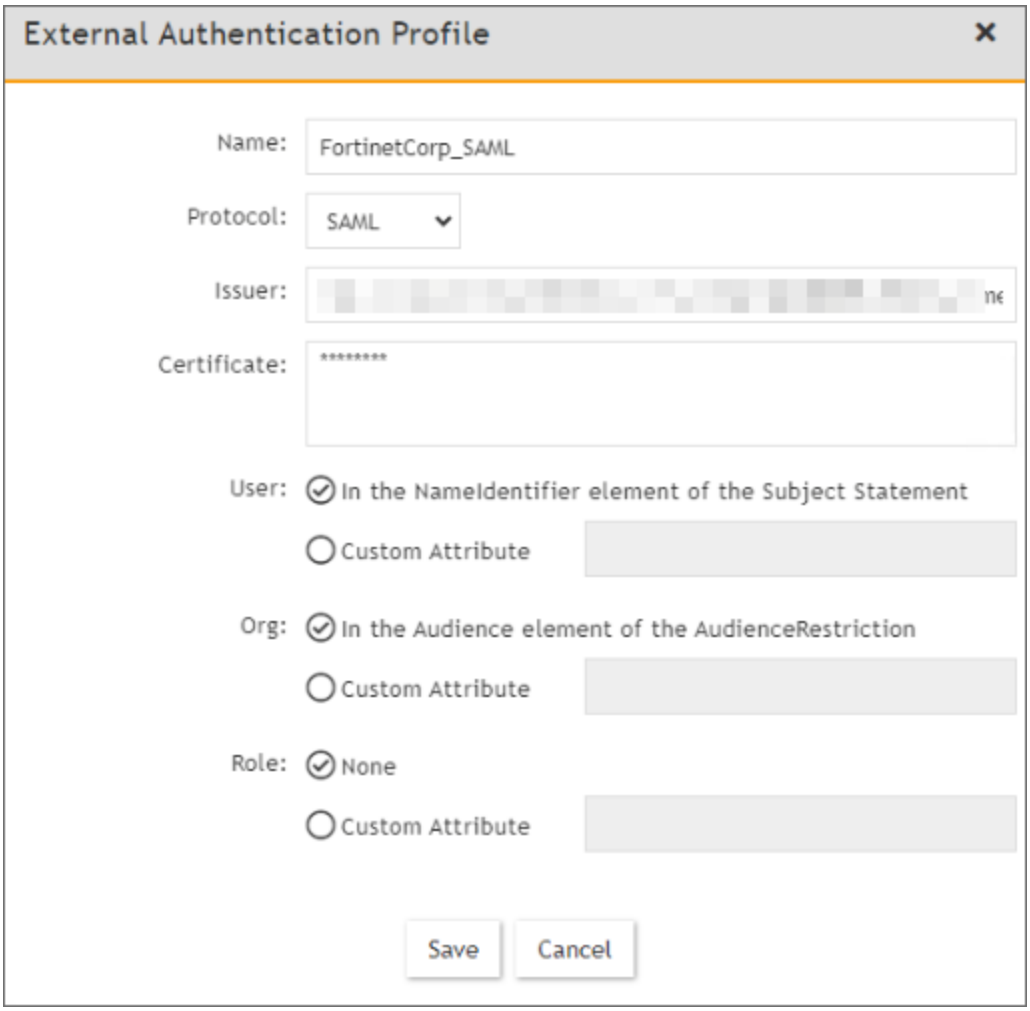
To set up FortiSIEM, take the following steps:

1. Navigate to **Admin > Settings > General > External Authentication**.
2. Click **New**.
3. In the **Name** field, enter the profile name from your FortiAuthenticator configuration.
   Note: This must be an EXACT match of the profile name used in the FortiAuthenticator configuration.
4. From the **Organization** drop-down list, select the organization that this authentication applies for.
   - **System** - For super/global scope. This is the most common option for Enterprise customers.
   - **Super/Local** - Only for super org. It has no access to global admin.
   - <***specific org***> - Select a specific organization.
5. From the **Protocol** drop-down list, select **SAML**.

6. In the **Issuer** field, enter/paste the IP address of the **IdP entity id** to FSM External Auth profile. Example screenshot showing **IdP entity id** from FortiAuthenticator provided below:

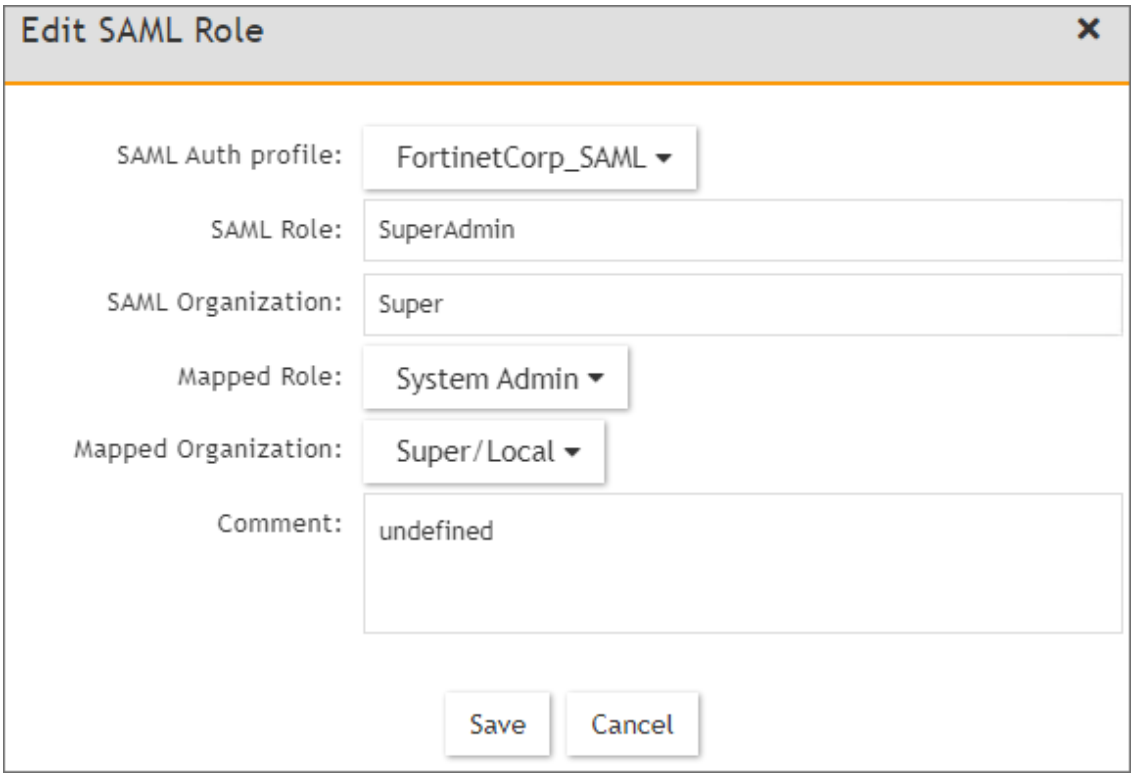


7. In the **Certificate** field, paste the SSL public certificate from the FortiAuthenticator general settings, the specific certificate used for signing assertions to our application/SP.
8. Leave the other options with their default option, and click **Save**.



Set Up SAML Role Mapping

1. Navigate to **Admin > Settings > Role > SAML Role**.
2. Click **New**.
3. From the **SAML Role** window, take the following steps:
   a. From the **SAML Auth profile** drop-down list, select your profile.
   b. In the **SAML Role** field, enter your role, such as "SuperAdmin". This is the SAML attribute representing the provided role. In this example case, “SuperAdmin” is significant only to the FortiAuthenticator configuration.
   c. In the **SAML Organization** field, enter the organization, such as "Super". This is the subject ID configured in the SAML application.
   d. From the **Mapped Role** drop-down list, select the desired FortiSIEM role, such as **System Admin**.
   e. From the **Mapped Organization** drop-down list, select the appropriate FortiSIEM tenant scope, such as **Super/Global** or **Super/Local**.
   f. Click **Save**.



Import Users from FortiAuthenticator

You can either import a set of users, which could be done via LDAP, or manually create users.

Note: The user name in FortiSIEM must exactly match the username as defined in the FortiAuthenticator IdP.

Take the following steps:

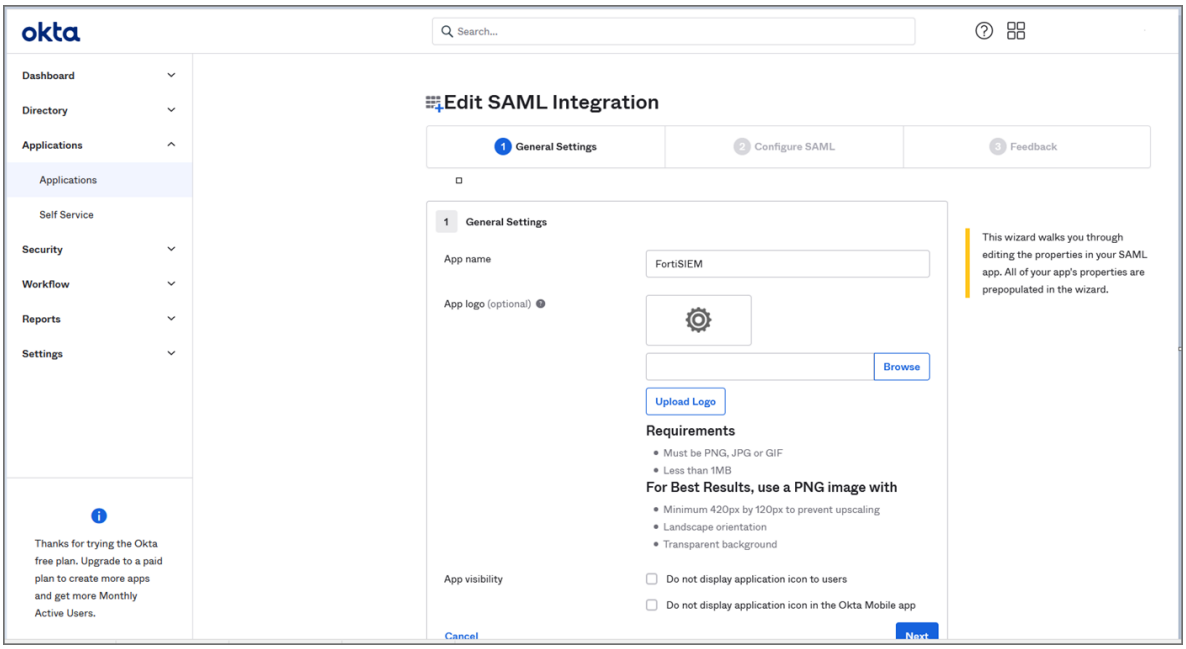
1. Navigate to **CMDB > Users > FortiSIEM Users**.
2. Click **New**.
3. In the **User Name** field. enter "admin1".
   Note: Here, we are assuming FortiAuthenticator has a username called "admin1".
4. Click the **System Admin** checkbox.
5. From the **New User** window, take the following steps:
   a. From the **Mode** drop-down list, select **External**.
   b. From the **Authentication Profiles** drop-down list, select the external authentication profile created earlier.
   c. Define an explicit role for this user instead of relying on SAML role mapping, or select **Default Role**: **Full Admin**.
   d. Click **Back**.
6. Click **Save**.

Note: This user cannot directly login to FortiSIEM. The user must go through the FortiAuthenticator SSO portal.

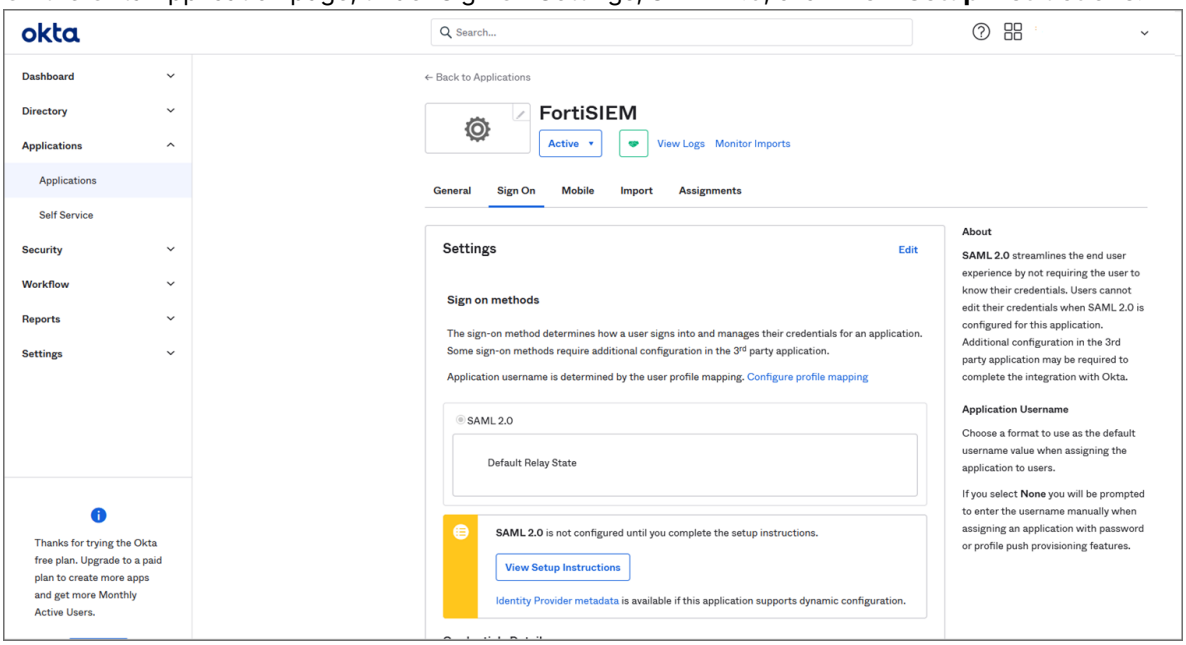
Example 4: Configuring FortiSIEM Users for SAML Authentication with OKTA

7. Using an admin account, log into Okta (https://okta.com/)
8. Click on the **Admin** button.
9. Enter the Okta Verify code.
10. At the **Use single sign on** option, click the **Add App** button.
11. Click on **Create New App**.
12. Select SAML 2.0 and click **Create**.
    In **General Settings**, provide the following:
    - App name - FortiSIEM
    - App logo (optional)

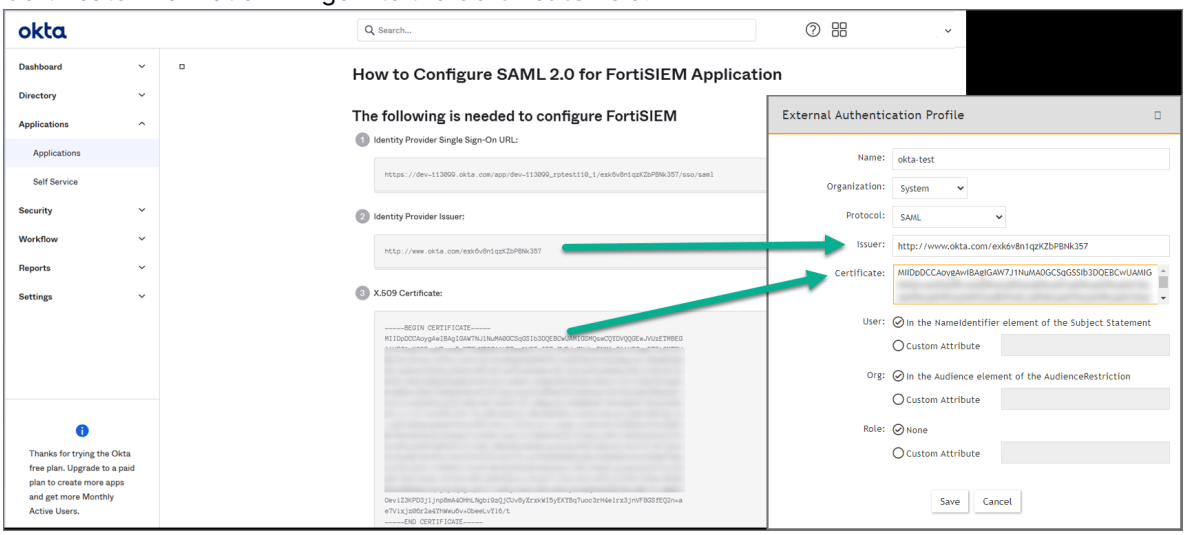
13. Click **Next**.



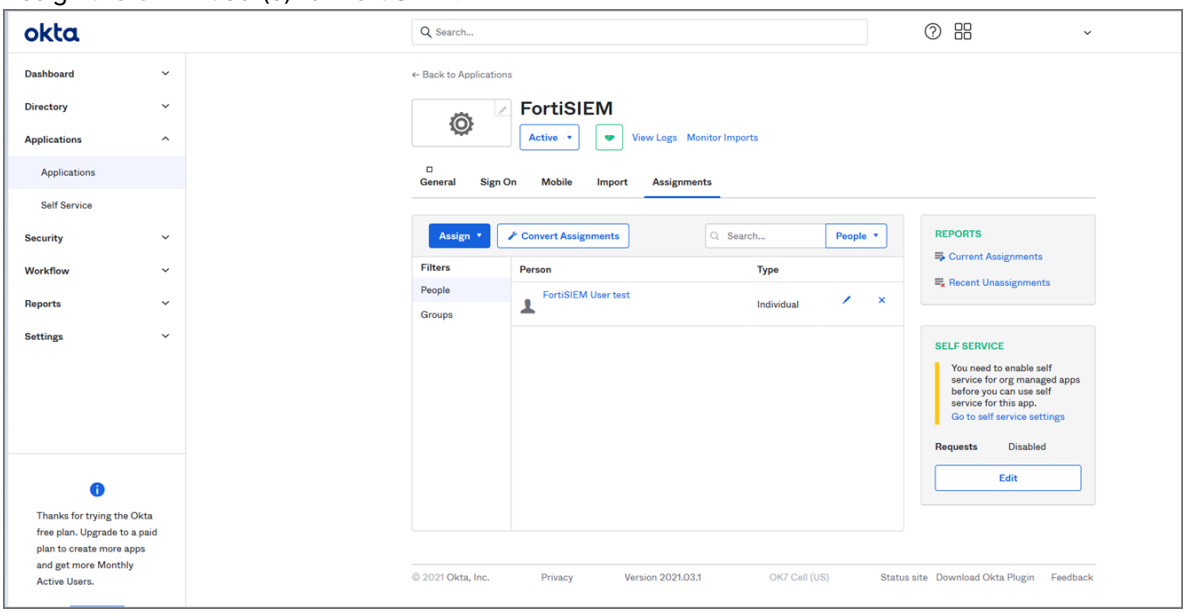
14. In **Configure SAML**, provide the following:
    - In Single sign on URL, enter https://*super_ip*/phoenix/sso/saml/*ExternalAuthenticationProfileName*
      super_ip represents the FortiSIEM IP address you want to log into, and ExternalAuthenticationProfileName will need to be configured in FortiSIEM by a full Admin creating an SAML External Authentication Profile via **ADMIN > Settings > General > External Authentication**.
    - In the **Audience URI (SP Entity ID)**, enter your organization name, for example "Super".
15. Click **Next**, then **Finish**. The FortiSIEM app is now being created.
16. On the Okta Application page, under Sign On Settings, SAML 2.0, click **View Setup Instructions**.



17. Copy the **Identify Provider Issuer** and **Certificate** information. When you create your External Authentication Profile in FortiSIEM, the Identify Provider Issuer will go into the **Issuer** field, and the Certificate information will go into the **Certificate** field.

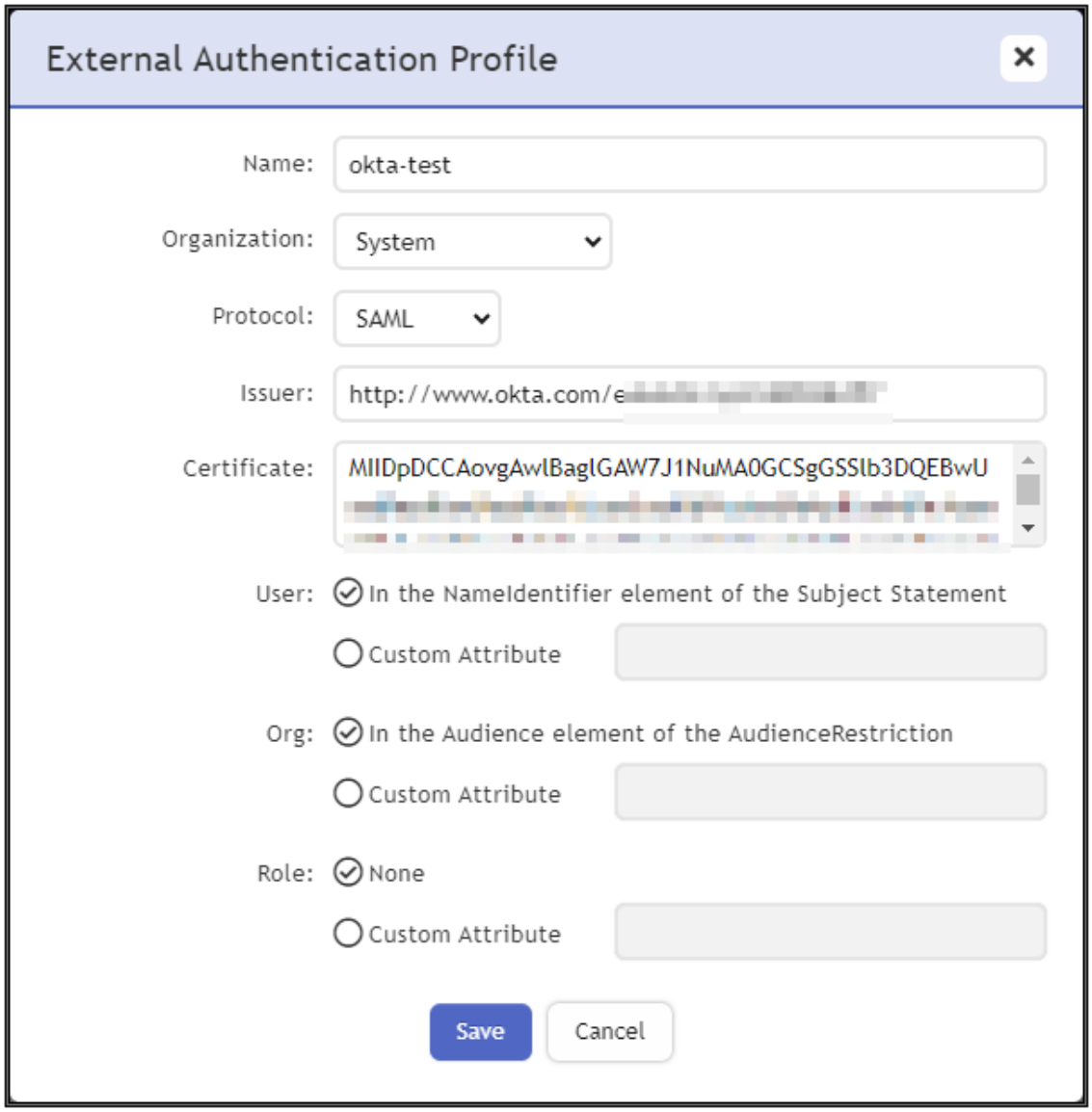


18. Assign the OKTA user(s) for FortiSIEM.



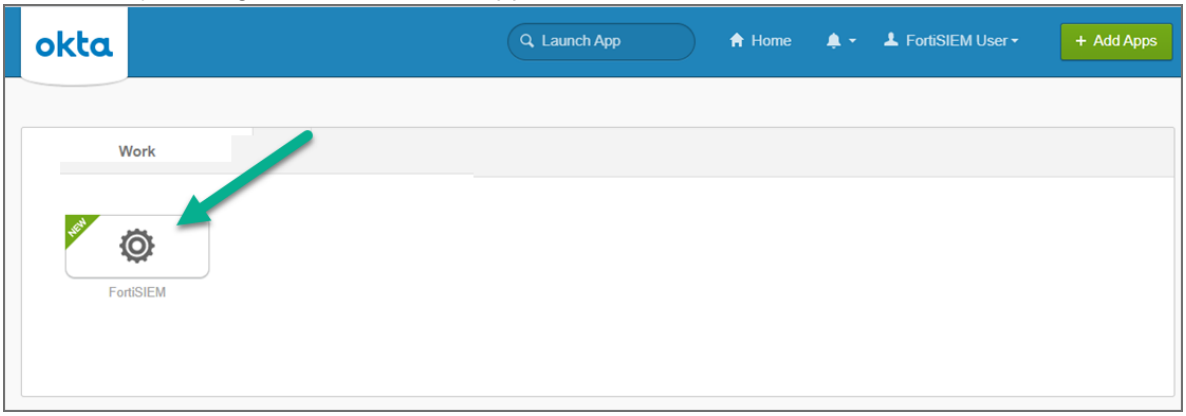
19. Log on to FortiSIEM as a full Admin.
20. Go to **ADMIN > Settings > General > External Authentication**.
21. Click **New** to create an External Authentication Profile.
22. From External Authentication Profile, take the following steps:
    a. In the **Name** field, enter your ExternalAuthenticationProfileName.
    b. From the **Organization** drop-down list, select the org.
    c. From the **Protocol** drop-down list, select **SAML**.
    d. In the **Issuer** field, enter the Identify Provider Issuer from Okta.
    e. In the **Certificate** field, enter/paste the certificate information from Okta.
    f. Configure User, and Org according to your IDP.

g. Click **Save**.



23. Go to **CMDB > Users > Ungrouped**.
24. Click **New** to add the Okta user.
25. In the **User Name** field, enter the user's Okta assigned username.
    Note: You can enter the name by using an email address depending on how the user was configured in Okta.
26. Click the **System Admin** field to open the **New User** window.
27. From the **Mode** drop-down list, select **External**.
28. From the **Authentication Profiles** drop-down list, select your Okta authentication profile that you created under your External Authentication profile.
29. From the **Default Role** drop-down list, select the appropriate user role and check the appropriate organization checkboxes the user is enabled for.
30. Click **Back**.
31. Click **Save**.

32. Log on to Okta as an assigned user for FortiSIEM. The assigned Okta user is now able to log on to FortiSIEM by clicking the FortiSIEM icon/application.



Example 5: Configuring FortiSIEM Users for 2 Factor Authentication with Duo Security

- Step 0: Obtain Keys for FortiSIEM to Communicate with Duo Security
- Step 1: Create and Manage FortiSIEM users in Duo Security
- Step 2: Add 2-Factor Authentication Option for FortiSIEM Users
- Step 3: Log in to FortiSIEM Using 2-Factor Authentication

Step 0: Obtain Keys for FortiSIEM to Communicate with Duo Security

1. Sign up for a Duo Security account: signup.
   This will be admin account for Duo Security.
2. Log in to Duo Security Admin Panel and navigate to **Applications**.
3. Click **Protect an Application.** Locate **Web SDK** in the applications.
4. Get **API Host Name**, **Integration key**, **Secret key** from the page.
   You will need it when you configure FortiSIEM.
5. Generate **Application key** as a long string.
   This is a password that Duo Security will not know. You can choose any 40 character long string or generate it as follows using python

```
import os, hashlib
print hashlib.sha1(os.urandom(32)).hexdigest()
```

Step 1: Create and Manage FortiSIEM users in Duo Security

This determines how the 2-factor authentication response page will look like in FortiSIEM and how the user will respond to the second-factor authentication challenge:

1. Log in to Duo Security as admin user.
2. Choose the **Logo** which will be shown to users as they log on.
3. Choose the super set of 2-factor **Authentication Methods**.
4. **Optional** - you can create the specific users that will logon via FortiSIEM. If the users are not pre-created here, then user accounts will be created automatically when they attempt 2-factor authentication for the first time.

Step 2: Add 2-Factor Authentication Option for FortiSIEM Users

1. Create a 2-factor authentication profile:
   a. Go to **ADMIN** > **Settings** > **General** > **External Authentication**.
   b. Click **New**.
      i. Enter **Name**.
      ii. Select the organization from the **Organization** drop-down.
      iii. Set the **Protocol** as 'Duo'.
      iv. Set the **IP/Host** from API hostname in Step 0: step 4 above.
      v. Set the **Integration key**, **Secret key**from Step 0: step 4 above
      vi. Set the **Application key** from Step 0: step 5 above.
      vii. Click **Save**.
2. Add the 2-factor authentication profile to a user:
   a. Go to **CMDB** > **Users** > **Ungrouped**.
   b. Click **New** to create a new use or **Edit** to modify a selected user.
   c. Select **System Admin** checkbox and click the edit icon.
   d. In the **Edit User** dialog box, enter and confirm a password for a new user.
   e. Select the **Second Factor** check-box.
   f. Select the 2-factor authentication profile created earlier in Step 2: Add 2-Factor Authentication Option for FortiSIEM Users.
   g. Select a **Default Role** from the drop-down list.
   h. Click **Save**.

Step 3: Log in to FortiSIEM Using 2-Factor Authentication

1. Log on to FortiSIEM normally (first factor) using the credential defined in FortiSIEM - local or external in LDAP.
2. If the 2-factor authentication is enabled, the user will now be redirected to the 2-factor step. The user will be able to log in to FortiSIEM.
   a. If the user is not created in the Duo system (by the Duo admin), a setup wizard will let you set some basic information like phone number and ask you to download the Duo app.
   b. If the user already exists in FortiSIEM, then follow the authentication method and click **Log in**.

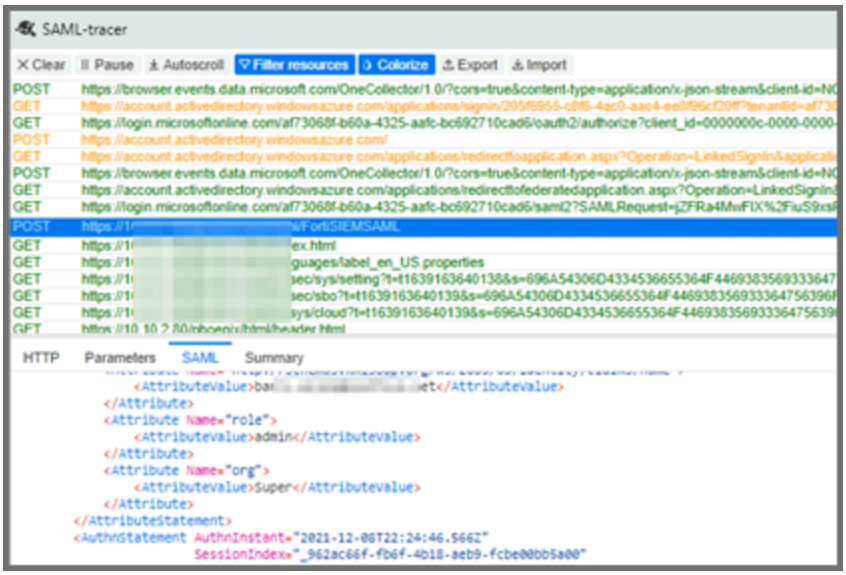
Troubleshooting SAML Operations

- Plugin Tool
- Issues after Successful Authentication
- Common Configuration Errors
- SAML Login Error Codes

Plugin Tool

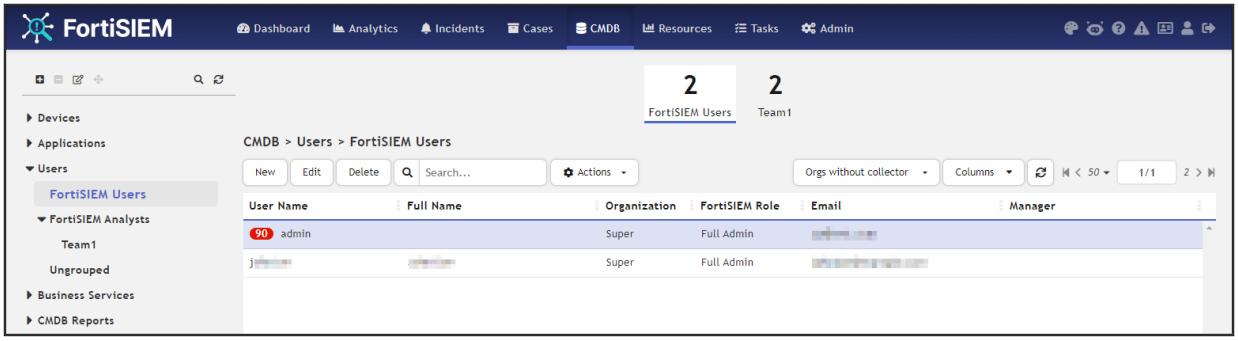
One way to troubleshoot a SAML response is to install the SAML-tracer Google Chrome plugin.

It will display the complete SAML response, with the actual attributes being returned. You can then check what the `AudienceRestriction` or expected Custom Attributes are and whether you have mapped them correctly.



Issues after Successful Authentication

When the logged in user is automatically added to the CMDB.

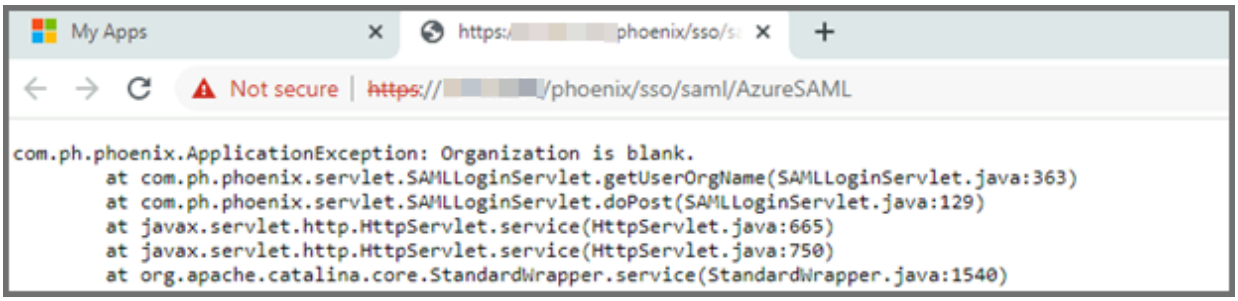


When editing a user, some fields are Read-Only, and can be identified by the inability to select those fields.

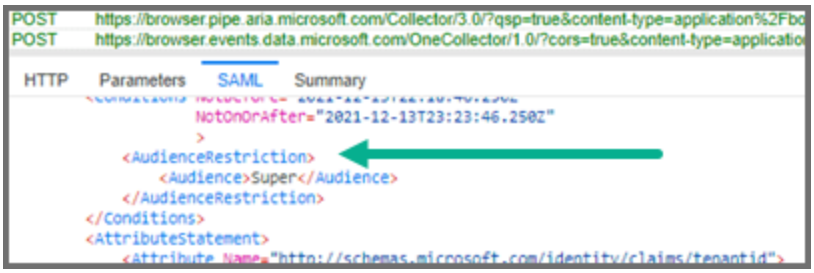
Common Configuration Errors

Organization is Blank

If you get a message saying "Organization is blank", check that the Org definition in the FortiSIEM External Authentication Profile is correct and mapped to the output from the SAML response.

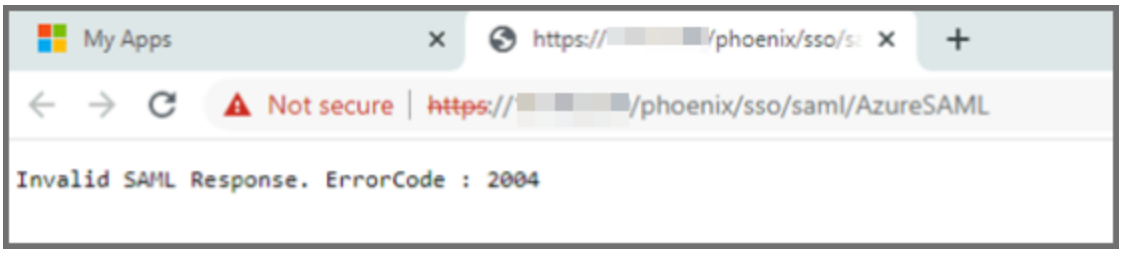


I.e. either `AudienceRestriction` or your Custom Attribute definition:



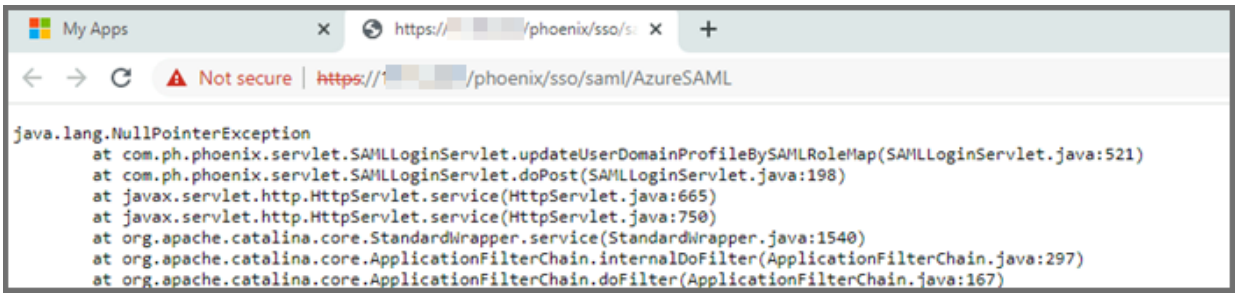
ErrorCode 2004

If you get the message "Invalid SAML Response. ErrorCode : 2004", check that the certificate definition in the FortiSIEM External Authentication Profile is correct.



UpdateUserDomainProfileBySAMLRoleMap Issue

If you run into the following issue, check that the Role definition in the FortiSIEM External Authentication Profile is correct.



SAML Login Error Codes

Error Code 1000-2000: Invalid SAML Configuration

Error Code 2000-3000: Invalid SAML Response

Error Code 3000-4000: Invalid username or password or organization

Error Code	Description
1000	Invalid SAML SSO path.
1001	Invalid SAML SSO path retrieved from SAML Response.
1002	Invalid SAML Config name.
1003	Invalid Issuer.
1004	More than two different Mapped Organizations, but no SAML Role Mapped Organization in \"Super/Global\".
1005	No SAML Role Map List found in DB.
1006	SAML External Profile config issue.
2000	Failed to get success status code.
2001	Missing Assertion.
2002	Failed to get an Issuer element from the assertion.
2003	SAML SSO authentication failed : Invalid X.509.
2004	SAML SSO authentication failed : Untrusted X.509.
2005	Failed to get signature.
3000	The organization doesn't match with the external authentication profile.
3001	Invalid Organization.
3002	No User found in DB.

Automation Policy

Note: Automation Policy replaces Notification Policy.

Automation Policies handles the sending of notifications when an incident occurs. Instead of setting notifications for each rule, you can create a policy and apply it to multiple rules.

The following section describes the procedures to create, modify, and enable Automation Policy settings:

- Adding Automation Policy Settings
- Modifying Automation Policy Settings
- Enabling Automation Policies
- Applying Case Creation to Automation Policy

Adding Automation Policy Settings

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy** tab.
2. Click **New**.
3. Select the **Severity**.
   Note: More than one severity can be selected.
4. For **Rules**, click the drop-down and select the rule or rules you want to trigger this notification from the folders.
5. Set a **Time Range** during which this notification will be in effect.
   Notifications will be sent only if an incident occurs during the time range you set here.
6. For **Affected Items**, click the drop-down and select the devices or applications from the **Select Devices** drop-down list for which this policy should apply.
   Instead of individual devices or groups, you can apply the automation policy to an IP address or range by clicking **Add IP/Range**. You can also select a group, and move to the **(NOT) Selections** column to explicitly exclude that group of applications or devices from the automation policy.
7. For Service Provider deployments, select the **Affected Orgs** to which the automation policy should apply.
   Notifications will be sent only if the triggering incidents affect the selected organization.
8. Select the **Action** to take when the notification is triggered.
   - Send Email/SMS to the target users. See here.
   - Run Remediation/Script. See here.
   - Invoke integration Policy. Click on **Run** to change policy. A drop-down list will appear. Select the policies you wish to invoke. For example, click on **FortiGUARD IOC Lookup** to invoke this integration policy, if it is available for your FortiSIEM environment.
   - Create Case when an incident is created. See here.
     Notes:

    - A group must be created under FortiSIEM Analysts before you are able to access this option.
    - This option is not available at the Org level.
    - This option also requires a Case Management Policy (from **Admin > Settings > General > Case Management**).
  - Send SNMP message to the destination set in **ADMIN > Settings > Analytics > Incident Notification**.
  - Send XML file over HTTP(S) to the destination set in **ADMIN> Settings > Analytics > Incident Notification**.
  - Open Remedy ticket using the configuration set in **ADMIN > Settings > Analytics > Incident Notification**.
  - Invoke FortiAI and update Comments.
9. Select the **Settings** to enable the exceptions for notification trigger.
   - Do not notify when an incident is cleared automatically.
   - Do not notify when an incident is cleared manually.
   - Do not notify when an incident is cleared by system.
10. Enter any **Comments** about the policy.
11. Click **Save**.

You can also create a duplicate notification by selecting a notification from the table and clicking **Clone**.

Remember to enable your automation policy after creating it. See Enabling Automation Policies.

Modifying Automation Policy Settings

Complete these steps to modify an Automation Policy setting.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy** tab.
2. Use the following buttons to modify automation policy settings:
   - **Edit** - To edit an automation policy setting
   - **Delete** - To delete an automation policy setting
3. Click **Save**.

Enabling Automation Policies

Complete these steps to enable or disable an automation policy

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy** tab.
2. In the **Enabled** column, click on an automation policy's checkbox to enable or disable it.

Applying Case Creation to Automation Policy

To associate a Case Management Policy to an Automation Policy, take the following steps.

1. In the **Case Management Policy** drop-down list, select the Case Management Policy you wish to apply.
2. From the **Teams: FIRST** drop-down list, select first team to be used in a case management policy.
3. Click on the **+** icon to add another team to be attached to the case management policy.
   Note: You can click the **-** icon to remove an existing team drop-down list option, but there must be at least one team configured.
4. In the **Teams: THEN** drop-down list, select the next FortiSIEM Analysts team that should be applied in the Case Management Policy.
5. Repeat steps 3-4 until you have configured all the teams that you wish to be part of the case management policy, then click **Save**.You will then be taken back to the **Automation Policy** window, where you can continue to configure your automation policy.

Define Notification Action - Email/SMS/Webhook

- Configuring Notification Action for Email/SMS/Webhook
- Configuring Notification Action for Email via CMDB > Users
- Edit Email Template

Email notifications can be configured in two ways. One way is by adding the email address for notifications. The other is to add via the users from your existing **CMDB > Users**. To configure via email address, see here. To configure via Users, see here.

Configuring Notification Action for Email/SMS/Webhook

To configure an email, SMS, or webhook notification action, take the following steps.

1. Click **Add Addr**.
   Note: To add an email notification via your existing **CMDB > Users**, you can optionally click **Add User**, and select the user(s) to notify by email instead of adding email addresses. See here for steps.
2. From the **Method** drop-down list, select the notification method.
3. For Email, take the following steps:
   a. In the **To:** field, enter the email addresses.
   b. In the **CC:** field, enter any additional email addresses.
   c. From the **Email Template Organization** drop-down list, select the organization.
   d. From the **Email Template** drop-down list, select an email template.
   e. Click **Save**.
4. For SMS, take the following steps.
   a. In the **To:** field, enter the email addresses.
   b. In the **CC:** field, enter any additional email addresses.
   c. Click **Save**.
5. For Webhook, take the following steps.
   a. From the Webhook Notification drop-down list, select a webhook notification configuration.
   Note: To create a webhook notification, see here.
   b. Click **Save**.
6. Click **Save** to return to the Automation Policy.

Configuring Notification Action for Email via CMDB > Users

To configure email notification action via **CMDB > Users** selection, take the following steps.

1. From the organization drop-down list, select the organization.
2. Click **Add User**.
3. From the **Folders** pane, select the appropriate folder to locate the users you wish to notify. These users will appear in the **Items** pane. Select the user(s), and click **>** to move them to the **Selections** pane, or click **>>** to move all users from a selected folder to the **Selections** pane.
4. When done adding users for notification, click **Save**.
5. Click **Save** to return to the Automation Policy.

Edit Email Template

To change the email template being used for email notification, take the following steps.

1. Select an existing Automation Policy Email Notification Action.
2. Click **Edit Email Template**.
3. From the **Email Template** drop-down list, select the email template you wish to apply.
4. Click **Save**, then **Save** again to return to the Automation Policy.

Configuring External Integrations

This section describes how to configure FortiSIEM to integrate with external CMDB and ticket management systems and threat entity reputation systems. Currently out-of-the-box supported external systems include ticket management systems such as ServiceNow, Connectwise, Salesforce and Jira, and reputation systems, such as VirusTotal, RiskIQ and FortiGuard IOC lookup.

- Configuring Ticketing System Integrations
- Configuring Reputation System Integrations
- Configuring Communication through Proxies
- Modifying an External System Integration

Configuring Ticketing System Integrations

FortiSIEM integration helps to create a two-way linkage between external ticketing/work flow systems like ServiceNow, ConnectWise and Salesforce. The integration can be for Incidents and CMDB.

This involves two steps.

1. Create an integration.
2. Attach the integration to an Incident Automation Policy or run the integration on a schedule.

Four types of integrations are supported:

- **Incident Outbound Integration**: This integration creates a ticket in an external ticketing system from FortiSIEM incidents. When an incident triggers in FortiSIEM, a ticket is opened in the external ticketing system. Currently, this out-of-the-box integration is supported for ServiceNow, ConnectWise, Salesforce and Jira.
- **Incident Inbound Integration**: This integration updates FortiSIEM incident ticket state from external system ticket states. Specifically, when a ticket is closed in the external ticketing system, the incident is cleared in FortiSIEM and the ticket status is marked closed to synchronize with the external ticketing system. Currently, this out-of-the-box integration is supported for ServiceNow, ConnectWise, Salesforce and Jira.
- **CMDB Outbound Integration**: This integration populates an external CMDB from FortiSIEM CMDB. When a device is added or updated in FortiSIEM CMDB, a device can be created in the external ticketing system. Currently, this out-of-the-box integration is supported for ServiceNow, ConnectWise and Salesforce.
- **CMDB Inbound Integration**: This integration populates FortiSIEM CMDB from an external CMDB. It works for any external CMDB.

Integration with other systems can be built using the API.

- ServiceNow Integration
- Jira Integration
- ConnectWise Integration

- Salesforce Integration
- CMDB Inbound Integration

ServiceNow Integration

- ServiceNow SOAP Based Integration
- ServiceNow Security Operations (SecOps) Integration

ServiceNow SOAP Based Integration

- Configuring ServiceNow for FortiSIEM Integration
- FortiSIEM Incident Schema
- Incident Outbound Integration (Default)
- Incident Inbound Integration (Default)
- Incident Outbound Integration (Custom)
- Incident Inbound Integration (Custom)
- CMDB Outbound Integration (Default)
- Example Custom Integration

Configuring ServiceNow for FortiSIEM Integration

1. Log in to ServiceNow.
2. For Service Provider Configurations, create Companies by creating Company Name.
3. For the integrations to work, FortiSIEM needs to modify certain ServiceNow database tables.
   - If you are using default integration, make sure that the FortiSIEM user account has the permissions specified, see Required Permissions for ServiceNow SOAP Integration.
   - if you are using custom integration, then make sure that the FortiSIEM user account has the read/write permissions on the specific ServiceNow tables and columns.

FortiSIEM Incident Schema

The following FortiSIEM Incident fields are available for integration.

FortiSIEM Incident Field	Type	Description	Required for Custom Integration
Incident ID	64bit Integer	Incident Id in FortiSIEM database.	Optional for outbound
Incident Title	String	Incident Title is a formatted string to capture Incident details and actors .	Optional for outbound
Rule Name	String	The name of the rule that triggered the Incident.	Optional for outbound
Rule Description	String	The description of the rule that triggered the Incident.	Optional for outbound
First Seen Time	64bit Integer	The first time an incident triggered in FortiSIEM. Format: Unix epoch timestamp (number of seconds that have elapsed since 00:00:00 UTC on 1 January 1970)	Optional for outbound
Last Seen Time	64bit Integer	The last time an incident triggered in FortiSIEM. Format: Unix epoch timestamp (number of seconds that have elapsed since 00:00:00 UTC on 1 January 1970)	Optional for outbound
Incident Severity	32bit integer – values 1-10	Severity of the Incident. Severities are increasing meaning 1 is lowest and 10 is highest.	Optional for outbound
Incident Severity Category	String – takes 3 values: LOW, MEDIUM, HIGH	Incident severity categorized into 3 levels: LOW, MEDIUM, HIGH	Optional for outbound
Incident Source	String	Incident source attributes in comma separated attribute:Value format. Following attributes are included: srcIpAddr	Optional for outbound
Incident Target	String	Incident destination in comma separated attribute:Value format. Following attributes are included: destIpAddr, destName, hostIpAddr, hostname, user, targetUser	Optional for outbound
Incident Detail	String	Incident details in comma separated attribute:Value format. All attributes not included in Incident Source and Incident target are included in this attribute.	Optional for outbound
Triggering Attributes	String	List of attributes present in the incident.	Optional for outbound

FortiSIEM Incident Field	Type	Description	Required for Custom Integration
Incident Count	32bit integer	Number of times the incident triggered.	Optional for outbound
Host Name	String	Host Name in incident. This is also present in Incident Target.	Optional for outbound
Incident Comment	String	Comments added by user or by a notification script.	Optional for outbound
Status	32bit integer	Incident Status: 0 means Active, 1 means System Cleared, 2 means User Cleared.	Optional for outbound
Incident Resolution	String	Four values: Open, InProgress, TruePostive and FalsePositive	Optional for outbound
Rule Remediation Note	String		Optional for outbound
External Ticket Id	String	ServiceNow Ticket Id	Required for both Inbound and Outbound
External Ticket State	String	ServiceNow Ticket State	Required for Inbound and must have a value mapping for “Closed”
External User	String	User who closed the Ticket in ServiceNow.	Optional for outbound
External Cleared Time	String	Time at which Incident cleared in ServiceNow.	Required for Inbound

There are two main requirements for a successful custom integration.

1. Outbound and Inbound – must have a mapping for External Ticket Id.
2. Inbound - External Ticket State must have value “Closed”.
3. Inbound - must have a mapping for External Cleared Time.

Incident Outbound Integration (Default)

In this integration, you can create tickets in ServiceNow when an Incident triggers in FortiSIEM. In the Default integration, FortiSIEM Incidents are written to the ServiceNow **incident** table. FortiSIEM incident attributes are mapped to ServiceNow incident table columns as follows.

FortiSIEM Incident Attribute	ServiceNow Incident Table Column
Incident Status	work_notes
Incident Name	short_description
Incident Comments (generated string containing few Incident attributes – see Step 1.4.k.)	comments
Organization Name	company
Incident Severity	impact
Incident Severity	urgency

Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Outbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.
   d. Set the **Instance** - This is the name of the integration. If you want matching inbound and outbound Incident integration for a specific vendor, then the instance name for the inbound and outbound integration must be the same. For example, ServiceNow Outbound and ServiceNow Inbound should have the same instance name, for example, ServiceNow1.
   e. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements.
   f. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.
   g. In the **User Name** field, enter the ServiceNow username login credential.
   h. In the **Password** field, enter the ServiceNow password login credential.
   i. Leave the **ServiceNow Table Name** attribute alone.
   j. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.
   k. For **Incident Comment**, you can keep the default format shown in Step 1.j.i, or create your own, shown in Step 1.j.ii.
      i. Default format : `[FortiSIEM]Incident Id:<val>;First seen time:<val>;Target IP:<val>;Incident Details:<val>;Mitre TechniqueId:<val>;Mitre Tactics:<val>; Description:<Rule Name>`
      ii. To create your own, click the Edit icon, and form a string by combining your own text and incident attributes by choosing from the Insert Content drop-down list. When done, click **Save**.

l. For **Organization Mapping**, click the Edit icon to create mappings between the Organizations in your FortiSIEM deployment and Company names in ServiceNow (created in Configuring ServiceNow for FortiSIEM Integration, Step 2).
m. For **Run For**, click the Edit icon, and choose the organizations for whom tickets will be created.
n. In the **Max Incidents** field, enter the maximum number of incidents you want to record.
o. Click **Save**.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Settings** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Incident Inbound Integration (Default)

Using this integration, a FortiSIEM Incident can be programmatically cleared when a user closes the corresponding ticket in ServiceNow. In the default integration, the following fields from ServiceNow **incident** table are mapped to FortiSIEM incident fields.

ServiceNow Incident Table Column	FortiSIEM Incident Field
incident_state	Incident Status
Closed_code	Incident Resolution
Closed_by	External User
number	External Ticket Id
incident_state	External Ticket Status

Step 1: Create an Incident Inbound Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Inbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.

d. Set the **Instance** - This is the name of the integration. If you want matching inbound and outbound Incident integration for a specific vendor, then the instance name for the inbound and outbound integration must be the same. For example, ServiceNow Outbound and ServiceNow Inbound should have the same instance name, for example, ServiceNow1.
e. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements.
f. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.
g. In the **User Name** field, enter the ServiceNow username login credential.
h. In the **Password** field, enter the ServiceNow password login credential.
i. Leave the **ServiceNow Table Name** attribute alone.
j. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.
k. For **Content Mapping**, do not make any edits. Keep the system defined one.
l. In the **Time Window** field, enter/select the number of hours for which incident states will be synched from ServiceNow. For example, if time window is set to 10 hours, then the states of incidents that occurred in the last 10 hours will be synched.
m. When done, click **Save**.

Step 2: Create an Incident Inbound Integration Schedule

This determines the schedule on which the inbound integration policy defined in **Step 1: Create an Incident Inbound Integration** will be run.

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **Schedule**.
4. Click **+** to open the **Integration Policy Schedules** window.
   a. From the **Integration Policy** column, select your integration policy and move it to the **Selected** column.
   b. Under **Time Range**, configure your schedule by taking the following steps.
      i. In the **Start Time** field, enter the start time of your schedule.
      ii. From the **Local/UTC Time**and **Region** drop-down lists, configure the start time of the schedule.
   c. Under **Recurrence Pattern**, configure the frequency.
      i. Select **Once**, **Minutely**, **Hourly**, **Daily**, **Weekly**, or **Monthly** for the schedule's recurrence pattern. Depending on what is selected, configure the related date/time schedule attributes.
      ii. In the **Start From** field, enter the date which the schedule starts.
   d. When done, click **Save**.

Incident Outbound Integration (Custom)

In this integration, you can create tickets in ServiceNow when an Incident triggers in FortiSIEM. You can choose your *own ServiceNow table* to map FortiSIEM Incidents to. Take the following steps to create a custom outbound integration.

Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Outbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.
   d. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements. For other vendors, you must create your own plugin and enter the plugin name here.
   e. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.
   f. In the **User Name** field, enter the ServiceNow username login credential.
   g. In the **Password** field, enter the ServiceNow password login credential.
   h. In the **ServiceNow Table Name** field, enter the custom ServiceNow table
   i. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.
   j. For **Incident Comment**, you can keep the default format shown in Step 1.j.i, or create your own, shown in Step 1.j.ii.
      i. Default format : `[FortiSIEM]Incident Id:<val>;First seen time:<val>;Target IP:<val>;Incident Details:<val>;Mitre TechniqueId:<val>;Mitre Tactics:<val>;Description:<Rule Name>`
      ii. To create your own, click the Edit icon, and form a string by combining your own text and incident attributes by choosing from the Insert Content drop-down list. When done, click **Save**.
   k. For **Organization Mapping**, click the Edit icon to create mappings between the Organizations in your FortiSIEM deployment and Company names in ServiceNow (created in Configuring ServiceNow for FortiSIEM Integration, Step 2).
   l. For **Run For**, click the Edit icon, and choose the organizations for whom tickets will be created.
   m. For **Content Mapping**, click the Edit icon to define mappings between FortiSIEM Incident fields and ServiceNow custom table columns.
      i. Select the **Field Mappings** dialog box and click **+**.
      Note: To delete a Field Mapping, select the entry and click **-**. To edit a Field Mapping, click the Edit icon.
      ii. From the **FortiSIEM Incident Field** drop-down list, select a FortiSIEM Incident field.
      iii. From the **ServiceNow Field** drop-down list, select a mapped ServiceNow field. Note that the menu is populated from the table in step 4.i.
      iv. Select the **Value Mappings** dialog box and click **+** to enter Value Mappings if you want the values for a specific field to be transformed. A standard example is Severity, where FortiSIEM Incident Severity 1-> 4 may be mapped to Low, 5-8 as Medium and 9-10 as High.
      v. From **Field**, select the ServiceNow Field whose values need to be transformed.

vi. In the **From** field, select the value that FortiSIEM generates.
vii. In the **To** field, select the value that you want ServiceNow to store.
viii. When done, click **Save**.

n. In the **Max Incidents** field, enter the maximum number of incidents you want to record.
o. Click **Save**.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Note: In the default Outbound integration, Incident updates are recorded in the comments field. However, in the custom integration, Incident updates are not reflected in ServiceNow.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Policy** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Incident Inbound Integration (Custom)

In this integration, you can clear tickets in FortiSIEM when a user closes the corresponding ServiceNow ticket. You can choose your *own ServiceNow table* to update the following FortiSIEM Incident fields:

- External Ticket Id
- Incident Status
- Incident Resolution
- External User
- External Ticket State

Step 1: Create an Incident Inbound Integration

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New**.
4. From the **Integration Policy** window, take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Inbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**. When you select a vendor, an instance is created, with a unique name for the policy. For example, if you had two ServiceNow installations, each would have different instance names.
   d. For **Plugin Name**, a default Plugin Name is populated. Leave it as is. This is the Java code that implements the integration, including connecting to the external help desk systems and synching the CMDB elements.
   e. In the **Host/URL** field, enter the login URL, for example, `https://vendor123.service-now.com`.

f. In the **User Name** field, enter the ServiceNow username login credential.
g. In the **Password** field, enter the ServiceNow password login credential.
h. For the **ServiceNow Table Name**, choose your custom ServiceNow table.
i. In the **Description** field, enter a description as to what the integration does. This is for display purposes only.
j. For **Content Mapping**, click the Edit icon to define mappings between FortiSIEM Incident fields and ServiceNow custom table columns.
    i. Select the **Field Mappings** dialog box and click **+**.
    Note: To delete a Field Mapping, select the entry and click **-**. To edit a Field Mapping, click the Edit icon.
    ii. From the **FortiSIEM Incident Field** drop-down list, select a FortiSIEM Incident field.
    iii. From the **ServiceNow Field** drop-down list, select a mapped ServiceNow field. Note that the menu is populated from the table in step 4.h.
    iv. Select the **Value Mappings** dialog box and click **+** to enter Value Mappings if you want the values for a specific field to be transformed. For the Incident Inbound Integration to function, we need a mapping to the “Closed” value of FortiSIEM Incident Status field. This allows FortiSIEM to close an Incident.
    v. From **Field**, select the ServiceNow Field whose values need to be transformed.
    vi. In the **From** field, select the value that FortiSIEM generates.
    vii. In the **To** field, select the value that you want ServiceNow to store.
    viii. When done, click **Save**.
k. In the **Time Window** field, enter/select the number of hours for which incident states will be synched from ServiceNow. For example, if time window is set to 10 hours, then the states of incidents that occurred in the last 10 hours will be synched.
l. When done, click **Save**.

Step 2: Create an Incident Inbound Integration Schedule

This determines the schedule on which the inbound integration policy defined in **Step 1: Create an Incident Inbound Integration** will be run.

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **Schedule**.
4. Click **+** to open the **Integration Policy Schedules** window.
    a. From the **Integration Policy** column, select your integration policy and move it to the **Selected** column.
    b. Under **Time Range**, configure your schedule by taking the following steps.
        i. In the **Start Time** field, enter the start time of your schedule.
        ii. From the **Local/UTC Time**and **Region** drop-down lists, configure the start time of the schedule.
    c. Under **Recurrence Pattern**, configure the frequency.
        i. Select **Once**, **Minutely**, **Hourly**, **Daily**, **Weekly**, or **Monthly** for the schedule's recurrence pattern. Depending on what is selected, configure the related date/time schedule attributes.
        ii. In the **Start From** field, enter the date which the schedule starts.

d. When done, click **Save**.

CMDB Outbound Integration (Default)

CMDB Outbound Integration populates an external CMDB from FortiSIEM's own CMDB. Built in integrations are available for ServiceNow.

Step 1: Create a CMDB Outbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ServiceNow is supported out of the box.
   When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had 2 ServiceNow installations, each would have different Instance names.
   b. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ServiceNow. For other vendors, you have to create your own plugin and type in the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For ServiceNow, select the login URL
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system. For ServiceNow, select the login credentials.
9. In **Attribute Mapping**, specify the mapping of attributes to resources.
10. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For ServiceNow, select the Company names as in Configuring ServiceNow for FortiSIEM Integration, Step 2.
11. For **Run For**, choose the organizations for whom tickets will be created.
12. For **Groups**, select the FortiSIEM CMDB Groups whose member devices would be synched to external CMDB.
13. Select **Run after Discovery** if you want this export to take place after you have run discovery in your system. This is the only way to push automatic changes from FortiSIEM to the external system.
14. Enter the **Maximum** number of devices to send to the external system.
15. Click **Save**.

Step 2: Create a CMDB Outbound integration schedule

Updating external CMDB automatically after FortiSIEM discovery:

1. Create an integration policy.
2. Make sure **Run after Discovery** is checked.
3. Click **Save**.

Updating external CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policies.
   b. Select a schedule.

Updating external CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

Example Custom Integration

This section provides a sample integration.

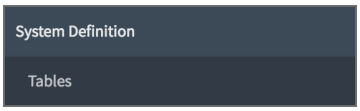
There are a few main requirements for a successful custom integration

1. Outbound and Inbound – must have a mapping for External Ticket Id
2. Inbound - External Ticket State must have value “Closed”
3. Inbound - must have a mapping for External Cleared Time

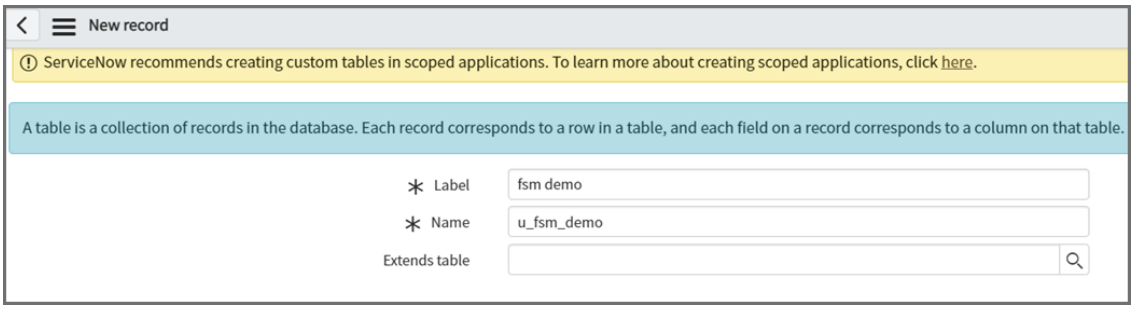
Follow these steps:

Step 1. From ServiceNow, take the following steps to create a ServiceNow Table.

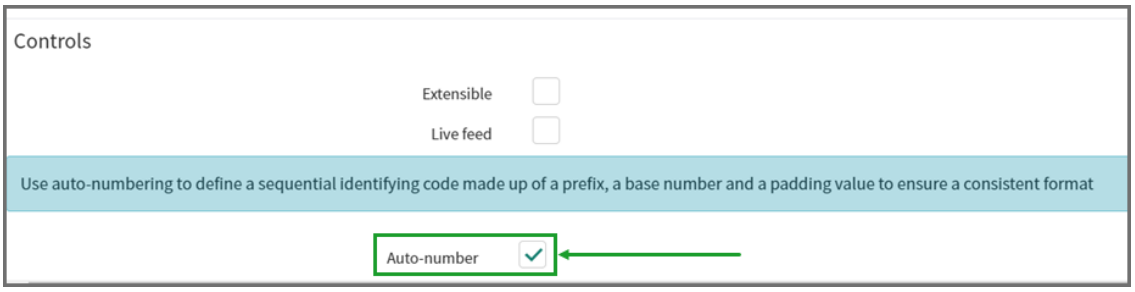
1. Login to ServiceNow.
2. From the left pane, navigate to **System Definitions > Tables**.



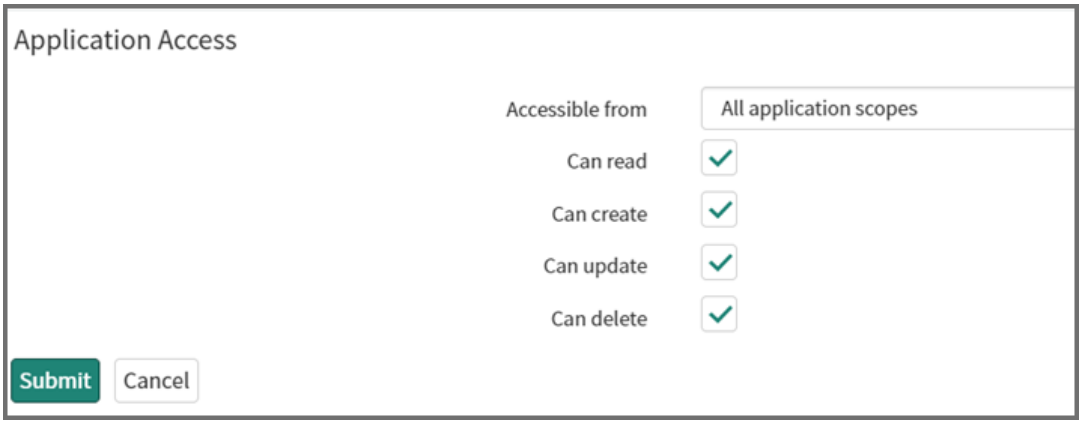
3. Next to the heading **Tables**, click **New** to create a table.
   a. In the **Label** field, enter a label. Here, we can use "fsm demo". The **Name** field will be automatically populated. Keep this name recorded, as it will be needed later.



   b. Under **Controls**, check the **Auto-number** checkbox. This is required to map the External Ticket Id.



c. Under **Application Access**, check the following checkboxes.
   - Can read
   - Can create
   - Can update
   - Can delete



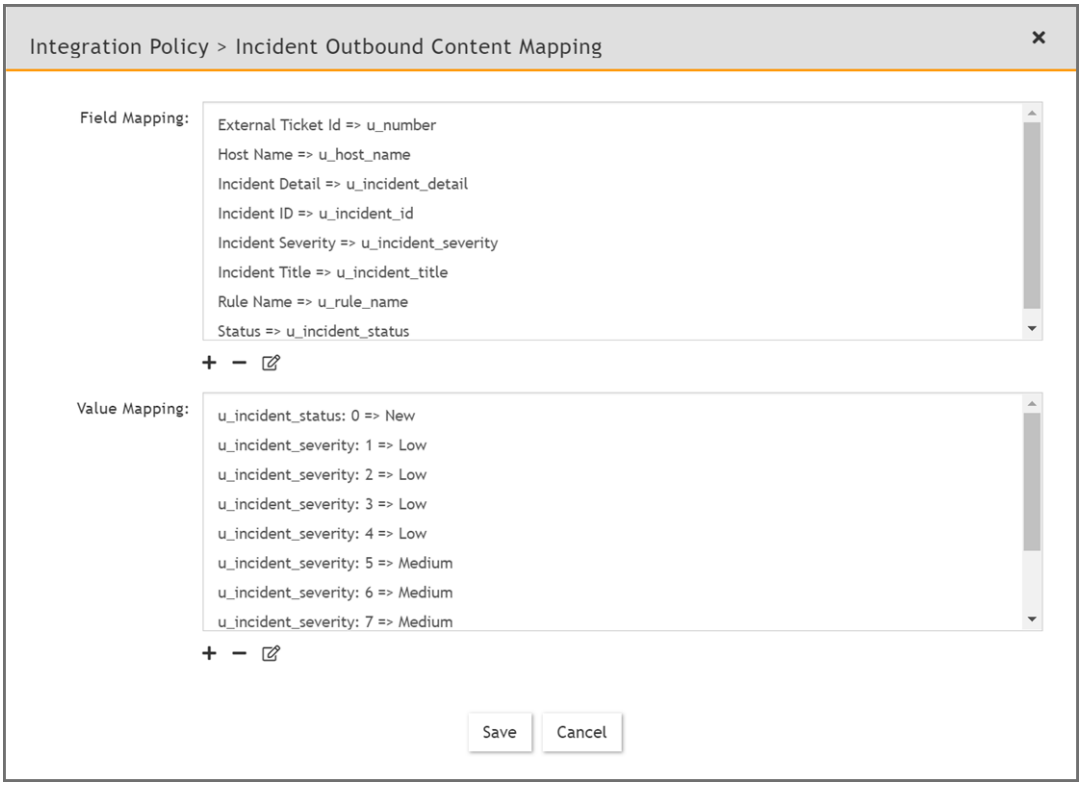
d. Click **Submit**.
   A ServiceNow table has now been created.

4. Next to the heading **Table Columns**, click **New** to create a table column.
   a. Create your column/mappings and ensure that **Type** is set correctly (See FortiSIEM Incident Schema for the correct Types). For this example, we use the following:
   Type: String
   Column label: ticketnumber
   Note: For External Ticket ID
   Max length: 256
   b. **Type**: String
   Column label: externalcleartime
   Note: For External Cleared Time
   Max length: 256
   c. **Type**: String
   Column label: incident_status
   Note: For Ticket Status
   Max length: 256
   d. Configure any additional mappings necessary for your ServiceNow table.
   To create a drop-down list, navigate to **Choice List Specification**, and from the **Choice** drop-down list, make a selection. To configure what will appear in your drop-down list, click the **Advanced view** link, and under **Choices**, click **New** to add items to appear in your drop-down list.

5. When done, click **Submit**.

Step 2. From FortiSIEM, take the following steps to create Incident Outbound Integration Policy.

1. Login to FortiSIEM.
2. Navigate to **ADMIN > Settings > General > External Integration**.
3. Click **New** to create an Integration Policy, and take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Outbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**.
   d. In the **Host/URL** field, enter the ServiceNow URL being used.
   e. In the **User Name** field, enter the ServiceNow username credential.
   f. In the **Password** and **Confirm Password** field, enter the password associated with the ServiceNow User Name account.
   g. In the **ServiceNow Table Name** field, enter the name of the ServiceNow table that was set up during the ServiceNow table creation.
   h. In the **Content Mapping** row, click the Edit icon.
   i. In the **Integration Policy > Incident Outbound Content Mapping** window, take the following steps.
      i. From the **FortiSIEM Incident Field** drop-down list, select **External Ticket Id**.
      ii. From the **ServiceNow Field** drop-down list, select the "ticketnumber" mapping.
      iii. From the **FortiSIEM Incident Field** drop-down list, select **External Ticket State**.
      iv. From the **ServiceNow Field** drop-down list, select the "externalcleartime" mapping.
      A more complicated custom mapping is provided in the following screenshot.

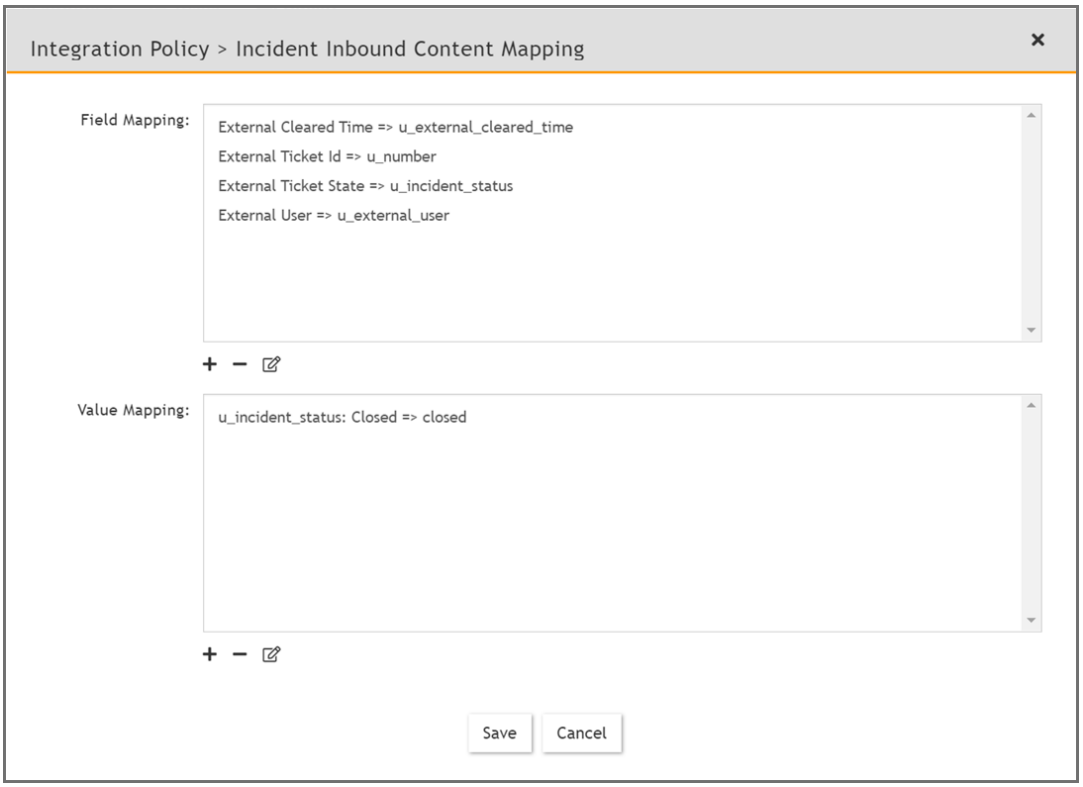


v. **Click Save**.

j. Click **Save**.
Your Outbound Integration Policy has been created.

Step 3. From FortiSIEM, take the following steps to create Incident Inbound Integration Policy.

1. Click **New** to create an Integration Policy, and take the following steps.
   a. From the **Type** drop-down list, select **Incident**.
   b. From the **Direction** drop-down list, select **Inbound**.
   c. From the **Vendor** drop-down list, select **ServiceNow**.
   d. In the **Host/URL** field, enter the ServiceNow URL being used.
   e. In the **User Name** field, enter the ServiceNow username credential.
   f. In the **Password** and **Confirm Password** field, enter the password associated with the ServiceNow User Name account.
   g. In the **ServiceNow Table Name** field, enter the name of the ServiceNow table that was set up during the ServiceNow table creation.
   h. In the **Content Mapping** row, click the Edit icon.
   i. In the **Integration Policy > Incident Outbound Content Mapping** window, take the following steps.
      i. From the **FortiSIEM Incident Field** drop-down list, select from External Cleared Time, External Ticket Id, External Ticket State, External User, or Incident Resolution.
      Note: External Ticket ID and External Ticket State are required.
      ii. From the **ServiceNow Field** drop-down list, select the corresponding column.
      iii. **Click Save**.
      iv. Repeat i.-iii. for any additional mappings. Proceed to v. when done with incident mapping.
      v. In **Value Mapping**, click **+** .
      vi. In the **Field** drop-down list, select the ServiceNow "external ticket state".
      vii. In the **From** field, enter "Closed".
      The value mapping should appear similar to the following example: `u_incident_status: Closed => closed`

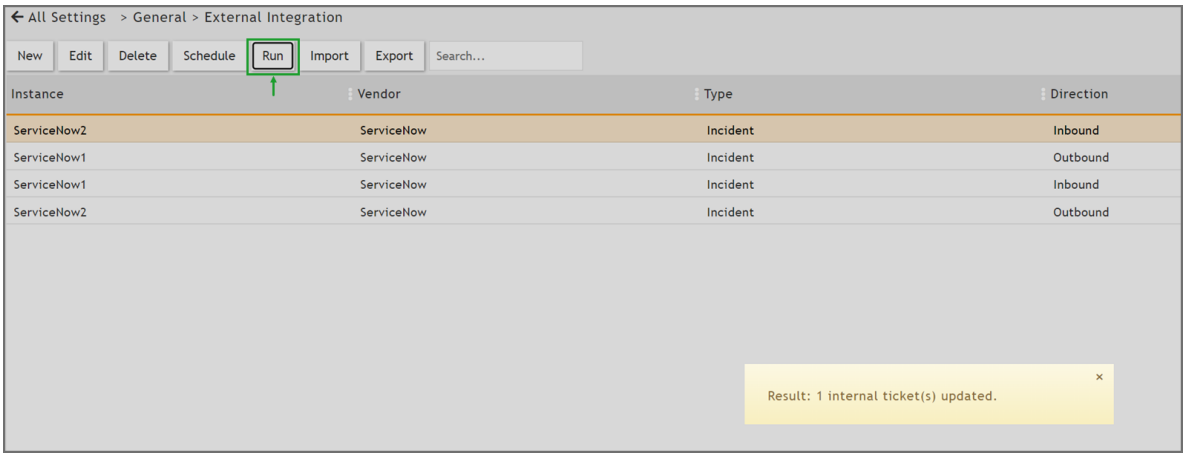


viii. Click **Save**.

j. Click **Save**.
Your Inbound Integration Policy has been created. Now, if you close an incident/ticket in ServiceNow, and run the inbound integration in FortiSIEM, the incident/ticket will also be closed.

Step 4. Run Outbound Integration

1. Confirm you are on the External Integration page. (**ADMIN > Settings > General > External Integration**)
2. Select the Outbound Integration you created.
3. Click **Run**.
Note: The maximum number of incidents can be configured by changing the value of the **Max Incidents** field in your Outbound Integration Automation policy .



4. Click **Yes** to confirm.

Step 5. Run Inbound Integration

1. Confirm you are on the External Integration page. (**ADMIN > Settings > General > External Integration**)
2. Select the Inbound Integration you created.
3. Click **Run**.
   Note: You can verify the closing of an incident/ticket by checking the **External Ticket State** column.

Jira Integration

- Configuring Jira for FortiSIEM Integration
- Jira Incident Outbound Integration
- Jira Incident Inbound Integration

Configuring Jira for FortiSIEM Integration

Before configuring Jira, you must log in to your Jira account and create an API Key. Follow these steps.

1. Log in to your Jira account.
2. Create an API Key.
3. Use the GUI user name and API Key in FortiSIEM.

Jira Incident Outbound Integration

Jira outbound integration allows a user to map FortiSIEM fields to Jira ticket fields and to create incidents in Jira. When the integration runs, FortiSIEM looks for incidents that match the mappings and creates a ticket in the Jira system.

To create an outbound integration, follow these steps.

Step 1: Create an Integration

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.
   - **Vendor**: select **Jira**.
   - **Instance**: enter an instance name or accept the default.
   - **Plugin Name**: is pre-populated with the name of the Jira integration class: `com.accelops.phoenix.jira.JiraTicketIntegration`.
   - **Host/URL**, enter the URL of the Jira provider, for example, `https://<customer>.atlassian.net`.
   - **Username** and **Password**, enter your Jira user name and password.
4. Click the edit icon next to **Field Mapping**.
5. In the **Field Mapping** dialog box, provide the following values:
   - **Project**: enter a name for the project
   - **Issue Type**: select Event.
   - The **Summary**: field is pre-populated with the **Incident Rule Name (**`$ruleName`**)**.
   - For **Description**: click the edit icon to build the expression for the Jira issue description. The drop-down list contains FortiSIEM fields that can be mapped to.
   - The **Priority**: field is pre-populated with **Incident Severity Category (**`$incident_severityCat`**)**.
6. Create mappings between Jira fields and FortiSIEM fields by clicking **New**.
   Select Jira fields from the upper drop-down list and match them with corresponding FortiSIEM fields in the lower drop-down list.
7. Click **Save** when you are finished mapping fileds. The mappings are reflected in the table in the Field Mapping dialog box.
   Note: Click **Cancel** to dismiss the **Mapping Fields** dialog box.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Policy** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Jira Incident Inbound Integration

Jira inbound integration allows a user to close a ticket in FortiSIEM if the ticket is closed in Jira.

To create an inbound integration, follow these steps.

Step 1: Create an Integration

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Inbound**.
   - **Vendor**: select **Jira**.
   - **Instance**: enter an instance name or accept the default.
   - **Plugin Name**: is pre-populated with the name of the Jira integration class: `com.accelops.phoenix.jira.JiraTicketIntegration`.
   - **Host/URL**, enter the URL of the Jira provider, for example, `https://<customer>.atlassian.net`.
   - **Username** and **Password**, enter your Jira user name and password.
   - **Description**: enter an optional description of the integration.
   - **Time Window**: enter the number of hours for which incident states will be synched. For example, if time windows is set to 10 hours, the states of incidents that occurred in the last 10 hours will be synched.
4. Click the edit icon next to **Field Mapping**.
5. In the Field Mapping dialog box, provide the following values:
   - **Project**: enter a name for the project.
   - **Issue Type**: select **Event**.
   - The **Summary**: field is pre-populated with the **Incident Rule Name (**`$ruleName`**)**.
   - For **Description**: click the edit icon to build the expression for the Jira issue description. The drop-down list contains FortiSIEM fields that can be mapped to.
   - The **Priority**: field is pre-populated with **Incident Severity Category (**`$incident_severityCat`**)**.
6. Create mappings between Jira fields and FortiSIEM fields by clicking **New**.
   Select Jira fields from the upper drop-down list and match them with corresponding FortiSIEM fields in the lower drop-down list.
7. Click **Save** when you are finished mapping fileds. The mappings are reflected in the table in the Field Mapping dialog box.
   Note: Click **Cancel** to dismiss the **Mapping Fields** dialog box.

Step 2: Create an Incident Inbound Integration Schedule

This determines the schedule on which the inbound integration policy defined in **Step 1: Create an Incident Inbound Integration** will be run.

1. Log into your Supervisor node with administrator credentials.
2. Navigate to **ADMIN > Settings > General > External Integration**.

3. Click **Schedule**.
4. Click **+** to open the **Integration Policy Schedules** window.
   a. From the **Integration Policy** column, select your integration policy and move it to the **Selected** column.
   b. Under **Time Range**, configure your schedule by taking the following steps.
      i. In the **Start Time** field, enter the start time of your schedule.
      ii. From the **Local/UTC Time**and **Region** drop-down lists, configure the start time of the schedule.
   c. Under **Recurrence Pattern**, configure the frequency.
      i. Select **Once**, **Minutely**, **Hourly**, **Daily**, **Weekly**, or **Monthly** for the schedule's recurrence pattern. Depending on what is selected, configure the related date/time schedule attributes.
      ii. In the **Start From** field, enter the date which the schedule starts.
   d. When done, click **Save**.

ConnectWise Integration

- Adding a Client ID for ConnectWise Integration
- Configuring ConnectWise for FortiSIEM Integration
- ConnectWise Incident Outbound Integration
- ConnectWise Incident Inbound Integration
- ConnectWise CMDB Outbound Integration

Adding a Client ID for ConnectWise Integration

ConnectWise has recently changed their policy and requires that vendors create a client ID in order to integrate with FortiSIEM. Due to this change and restriction from ConnectWise, Fortinet has published a public client ID in order to allow clients to integrate with ConnectWise. This Client ID is `1a7ed749-47a1-4d3e-94b0-696288a1140f`.

Note: A ConnectWise working account is required before integration can occur.

To add this client ID for ConnectWise, take the following steps.

1. Go to **ADMIN > Settings >General > External Integration**.
2. Click **New** to create a new Integration Policy or select an existing Integration Policy and click **Edit**.
3. From the **Vendor** drop-down list, select **ConnectWise**.
4. In the **Client ID** field, paste the following Client ID:
   `1a7ed749-47a1-4d3e-94b0-696288a1140f`
5. Make any necessary configuration changes.
6. Click **Save**.

Configuring ConnectWise for FortiSIEM Integration

1. Log in to ConnectWise MANAGE.
2. Go to **Setup Tables > Integrator Login** List.
3. Create a new **Integrator Login** for FortiSIEM:
   a. Enter **Username**.
   b. Enter **Password**.
   c. Set **Access Level** to **Records created by integrator**.
   d. Enable **Service Ticket API** for Incident Integration.
   e. Enable **Configure API** for CMDB Integration.
4. For Service Provider Configurations, create Companies by creating:
   a. **Company Name**
   b. **Company ID**

ConnectWise Incident Outbound Integration

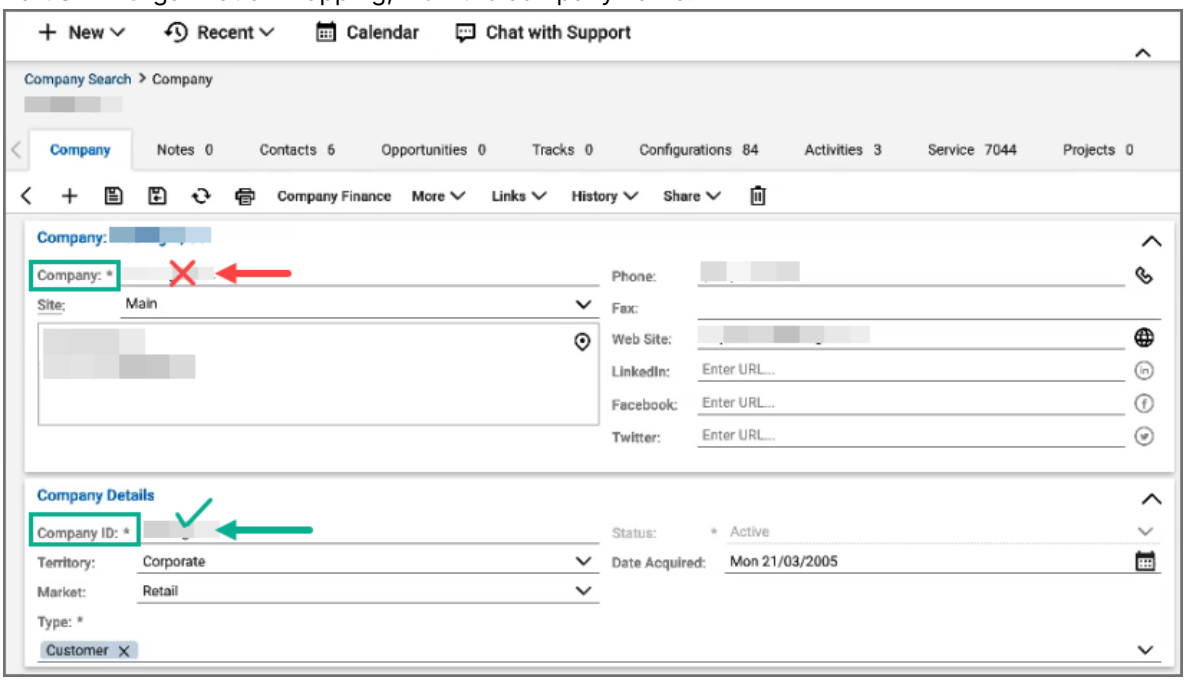
Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ConnectWise is supported out of the box.
   When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had two ConnectWise installations, each would have different Instance names.
   b. Choose whether the **Plugin Type** is **SOAP** or **REST**.
   Note: The SOAP method is deprecated, so you should select REST.
   c. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ConnectWise. For other vendors, you must create your own plugin and enter the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For ConnectWise, enter the login URL of the ConnectWise instance. Make sure to include the https:// prefix.
   Example: `https://my.login.test`

8. For **Company**, enter the company name that you use when logging in to ConnectWise Manage. Do not use the company name from within ConnectWise.

9. If you chose **SOAP** as **Plugin Type**, enter a **User Name**, **Password**, and **Client ID** that the system can use to authenticate with the external system. For ConnectWise, select the credentials created in Configuring ConnectWise for FortiSIEM Integration, Step 3. If you chose REST, enter the **Public Key** and the **Private Key** and **Client ID**.
Note: The Client ID is 1a7ed749-47a1-4d3e-94b0-696288a1140f. See Adding a Client ID for ConnectWise Integration for more information.
To get your **Public Key** and **Private Key** from ConnectWise, login and take the following steps.
   a. In the upper right part of the window, click your account name to open a drop-down list, and select **My Account**.
   b. Click the **API Keys** tab, and create your private and public keys, keeping a record of what they are so you can enter them in the FortiSIEM configuration in the **Private Key** and **Public Key** fields.
10. For **Incidents Comments Template**, specify the formatting using the incident fields.
11. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. In ConnectWise, locate and use the **Company ID** field under Company Details in ConnectWise for the

FortiSIEM Organization Mapping, NOT the company name.



12. For **Run For**, choose the organizations for whom tickets will be created.
13. Enter the **Max Incidents** to be recorded.
    Note: The default number for **Max Incidents** is 50. When running this the first time with the default number, you may encounter a 502 proxy error due to the initial volume of incidents being requested. In this situation, you can change the **Max Incidents** value to 5 or 10 initially, then change it after running the ConnectWise integration once.
14. Click **Save**.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Policy** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

ConnectWise Incident Inbound Integration

This updates the FortiSIEM incident state and clears the incident when the incident is cleared in the external help desk system. Built-in integrations are available for ConnectWise.

The steps are:

1. Create an Incident Inbound integration schedule.
2. Create a schedule for automatically running the Incident Inbound integration.
   This will update the FortiSIEM incident inbound integration schedule and clears the incident when the incident is cleared in the external help desk system.

Step 1: Create an Incident Inbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Inbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ConnectWise is supported out of the box.
   When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had two ConnectWise installations, each would have different Instance names.
   b. Choose whether the **Plugin Type** is **SOAP** or **REST**.
   c. A default **Plugin Name** is populated. This is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ConnectWise. For other vendors, you must create your own plugin and enter the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system (see section Configuring external helpdesk systems). For ConnectWise, select the login URL.
8. If you chose **SOAP** as **Plugin Type**, enter a **User Name**, **Password**, and **Client ID** that the system can use to authenticate with the external system. For ConnectWise, select the credentials created in Configuring ConnectWise for FortiSIEM Integration, Step 3. If you chose REST, enter the **Public Key**, the **Private Key**, and **Client ID**.
9. For **Time Window**, select the number of hours for which incident states will be synched. For example, if time windows is set to 10 hours, the states of incidents that occurred in the last 10 hours will be synched.
10. Click **Save**.

Step 2: Create an Incident Inbound integration schedule

This will update FortiSIEM following incident fields when ticket state is updated in the external ticketing system.

- External Ticket State
- Ticket State
- External Cleared Time
- External Resolve Time

Note: FortiSIEM does not support custom mapping, only "new" and "closed", and the incident resolution is not updated.

Follow these steps.

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.

3. Click **Schedule** and then click **+**.
   a. Select the integration policy.
   b. Select a schedule.

ConnectWise CMDB Outbound Integration

CMDB Outbound Integration populates an external CMDB from FortiSIEM's own CMDB. Built in integrations are available for ServiceNow, ConnectWise and Salesforce.

Step 1: Create a CMDB Outbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. ConnectWise is supported out of the box.
   When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had two ConnectWise installations, each would have different Instance names.
   b. Choose whether the **Plugin Type** is **SOAP** or **REST**.
   c. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for ConnectWise. For other vendors, you have to create your own plugin and type in the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For ConnectWise, select the login URL.
8. If you chose **SOAP** as **Plugin Type**, enter a **User Name**, **Password**, and **Client ID** that the system can use to authenticate with the external system. For ConnectWise, select the credentials created in Configuring ConnectWise for FortiSIEM Integration, Step 3. If you chose REST, enter the **Public Key** and the **Private Key** in addition to the **User Name**, **Password**, and **Client ID**.
9. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For ConnectWise, select the Company name in Configuring ConnectWise for FortiSIEM Integration, Step 4.
10. For **Run For**, choose the organizations for whom tickets will be created.
11. For ConnectWise, it is possible to define a **Content Mapping**.
    a. Enter **Column Mapping** values:
       i. To add a new mapping, click the + button.
       ii. Choose FortiSIEM CMDB attribute as the Source Column.
       iii. Enter external (ConnectWise) attribute as the Destination Column.
       iv. Specify Default Mapped Value as the value assigned to the Destination Column if the Source Column is not found in Data Mapping definitions.
       v. Select Put to a Question is the Destination Column is a custom column in ConnectWise.

b. Enter **Data Mapping** values:
   i. Choose the (Destination) Column Name.
   ii. Enter From as the value in FortiSIEM.
   iii. Enter To as the value in ConnectWise.

12. For **Groups**, select the FortiSIEM CMDB Groups whose member devices would be synched to external CMDB.
13. Select **Run after Discovery** if you want this export to take place after you have run discovery in your system. This is the only way to push automatic changes from FortiSIEM to the external system.
14. Enter the **Max Devices**: the number of devices to send to the external system.
15. Click **Save**.

Step 2: Create a CMDB Outbound integration schedule

Updating external CMDB automatically after FortiSIEM discovery:

1. Create an integration policy.
2. Make sure Run after Discovery is checked.
3. Click **Save**.

Updating external CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policies.
   b. Select a schedule.

Updating external CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

Salesforce Integration

- Configuring Salesforce for FortiSIEM Integration
- Salesforce Incident Outbound Integration
- Salesforce Incident Inbound Integration
- Salesforce CMDB Outbound Integration

Configuring Salesforce for FortiSIEM Integration

1. Log in to Salesforce.
2. Create a **custom domain**.

3. For Service Provider Configurations, create **Service App** > **Accounts**.
   FortiSIEM will use the **Account Name**.

Salesforce Incident Outbound Integration

Step 1: Create an Integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. Salesforce is supported out of the box.
   When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had two Salesforce installations, each would have different Instance names.
   b. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for Salesforce. For other vendors, you must create your own plugin and enter the plugin name here.
7. For **Host/URL**, enter the host name or URL of the external system. For Salesforce:
   a. Log in to Salesforce.
   b. Go to **Setup** > **Settings**.
   c. Use the **Custom URL** under **My Domain**, typically it is `xyz.my.salesforce.com`
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system.
   a. For Salesforce, enter the login credentials.
9. For **Security Token**, enter the security token from Salesforce. If you do not have your security token information, you can get this by taking the following steps.
   a. Log in to Salesforce.
   b. At <*your name*>, click the drop-down list and navigate to **Setup > Personal Setup > My Personal Information**.
   c. Click **Reset My Security Token** to get Salesforce to email your security token.
10. For **Incidents Comments Template**, specify the formatting of the incident fields.
11. For **Organization Mapping**, click the **Edit** icon to take you to the **Integration Policy > Org Mapping** window. Here, you can create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For Salesforce, to get your account name, take the following steps in Salesforce:
    a. Go to **Service App** > **Accounts**.
    b. Use **Account Name**.
    c. In FortiSIEM, at the **Integration Policy > Org Mapping** window, enter the **Account Name** in the **Default** field.
    Note: You can choose to provide an organization name from FortiSIEM in the **Default** field.
12. For **Run For**, choose the organizations for whom tickets will be created.

13. In the **Max Incidents** field, enter the maximum number of incidents you want recorded.
14. Click **Save**.
15. Click **Run** to confirm the integration. If you receive an "...unable to find valid certification path to requested target", you need to upload a certificate to FortiSIEM.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Policy** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Salesforce Incident Inbound Integration

This updates the FortiSIEM incident state and clears the incident when the incident is cleared in the external help desk system. Built-in integrations are available for Salesforce.

The steps are:

1. Create an Incident Inbound integration schedule.
2. Create a schedule for automatically running the Incident Inbound integration.
   This will update the FortiSIEM incident inbound integration schedule and clears the incident when the incident is cleared in the external help desk system.

Step 1: Create an Incident Inbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Incident**.
5. For **Direction**, select **Inbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. Salesforce is supported out of the box.
   When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had two Salesforce installations, each would have different Instance names.
   b. A default **Plugin Name** is populated. This is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The plugin is automatically populated for Salesforce. For other vendors, you must create your own plugin and enter the plugin name here.

7. For **Host/URL**, enter the host name or URL of the external system. For Salesforce:
   a. Log in to Salesforce.
   b. Go to **Setup > Settings**.
   c. Use the **custom URL** under **My Domain** – typically it is `xyz.my.salesforce.com`.
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system. For Salesforce, select the login credentials.
9. For **Time Window**, select the number of hours for which incident states will be synched. For example, if time windows is set to 10 hours, the states of incidents that occurred in the last 10 hours will be synched.
10. Click **Save**.

Step 2: Create an Incident Inbound integration schedule

This will update FortiSIEM following incident fields when ticket state is updated in the external ticketing system.

- External Ticket State
- Ticket State
- External Cleared Time
- External Resolve Time

Follow these steps.

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policy.
   b. Select a schedule.

Salesforce CMDB Outbound Integration

CMDB Outbound Integration populates an external CMDB from FortiSIEM's own CMDB. Built in integrations are available for Salesforce.

Step 1: Create a CMDB Outbound integration

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Outbound**.
6. For **Vendor**, select the vendor of the system you want to connect to. Salesforce is supported out of the box.
   When you select the Vendor:
   a. An **Instance** is created - this is the unique name for this policy. For example if you had 2 Salesforce installations, each would have different Instance names.
   b. A default **Plugin Name** is populated - this is the Java code that implements the integration including connecting to the external help desk systems and synching the CMDB elements. The

plugin is automatically populated for Salesforce . For other vendors, you have to create your own plugin and type in the plugin name here.

7. For **Host/URL**, enter the host name or URL of the external system. For Salesforce:
   a. Log in to Salesforce.
   b. Go to **Setup** > **Settings**.
   c. Use the **Custom URL** under **My Domain**, typically it is `xyz.my.salesforce.com`.
8. For **User Name** and **Password**, enter a user name and password that the system can use to authenticate with the external system. For Salesforce, select the login credentials.
9. Enter the **Maximum** number of devices to send to the external system.
10. For **Organization Mapping**, click **Edit** to create mappings between the organizations in your FortiSIEM deployment and the names of the organization in the external system. For Salesforce:
    a. Go to **Service App** > **Accounts**.
    b. Use **Account Name**.
11. For **Run For**, choose the organizations for whom tickets will be created.
12. For **Groups**, select the FortiSIEM CMDB Groups whose member devices would be synched to external CMDB.
13. Select **Run after Discovery** if you want this export to take place after you have run discovery in your system. This is the only way to push automatic changes from FortiSIEM to the external system.
14. Click **Save**.

Step 2: Create a CMDB Outbound integration schedule

Updating external CMDB automatically after FortiSIEM discovery:

1. Create an integration policy.
2. Make sure Run after Discovery is checked.
3. Click **Save**.

Updating external CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policies.
   b. Select a schedule.

Updating external CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

CMDB Inbound Integration

CMDB Inbound Integration populates FortiSIEM CMDB from an external CMDB.

Step 1: Create a CMDB Inbound integration

You must create a CSV file for mapping the contents of the external database to a location on your FortiSIEM Supervisor, which will be periodically updated based on the schedule you set.

1. Log into your Supervisor node with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New**.
4. For **Type**, select **Device**.
5. For **Direction**, select **Inbound**.
6. Enter the **File Path** to the CSV file.
7. For **Content Mapping**, click the edit icon.
   a. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.
      i. Enter Source CSV column Name for **Source Column**
      ii. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist
         i. Enter a name for the **Destination Column** of the property from the drop-down list.
         ii. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.
      iii. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.
      iv. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.
      v. Click **OK**.
   b. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.
      For example, if you wanted to change all instances of **California** in the entries for the **State** attribute in the external system to **CA** in the destination CMDB, you would select the **State** attribute, enter **California** for **From**. and **CA** for **To**.
8. In **Attribute Mapping**, map attributes to resources.
9. Click **OK**.
10. Click **Save**.

Step 2: Create a CMDB Inbound integration schedule

Updating FortiSIEM CMDB on a schedule:

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **Schedule** and then click **+**.
   a. Select the integration policies.
   b. Select a schedule.

Updating FortiSIEM CMDB on-demand (one-time):

1. Log into your FortiSIEM Supervisor with administrator credentials.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Select a specific integration policy and click **Run**.

Configuring Reputation System Integrations

- VirusTotal Integration
- FortiGuard IOC Lookup Integration
- RiskIQ Integration

VirusTotal Integration

- Configuring VirusTotal for FortiSIEM Integration
- VirusTotal Incident Outbound Integration

Configuring VirusTotal for FortiSIEM Integration

Register at the VirusTotal website to obtain a user name, password, and the API key. For more information, see https://developers.virustotal.com/reference/overview#getting-started.

VirusTotal Incident Outbound Integration

Step 1: Create an Integration

To create an outbound integration, follow these steps.

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.
   - **Vendor**: select **VirusTotal**.
   - **Instance**: enter an instance name or accept the default.
   - **Plugin Name**: is pre-populated with the name of the integration class: `com.accelops.service.integration.impl.VirusTotalIntegrationServiceImpl`.
   - **Password**: enter your API key in the password field.
4. Enter an optional **Description** of the integration.
5. Click the edit icon next to the **Incident Comments template**.
   a. In the **Incident Comments Template** dialog box, select content from the **Insert Content** drop-down list.
   b. Click **Save** when you are finished.

6. Click the edit icon next to the **Organization Mapping**.
   a. In the **Org Mapping** dialog box, click beneath **External Company ID** to enter the ID of the company you want to map to organizations.
   b. Click **Save** when you are finished.
7. Click the edit icon next to the **Run for**.
   a. In the **Run for** dialog box, select the organizations for which the integrations will be run.
   b. Click **Save** when you are finished.
8. Enter the maximum number of incidents you want recorded in the **Max Incidents** field.
9. Click **Save**.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Policy** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

FortiGuard IOC Lookup Integration

- Configuring FortiGuard for FortiSIEM Integration
- FortiGuard Incident Outbound Integration

Configuring FortiGuard for FortiSIEM Integration

No additional license is required to use the FortiGuard feature. Follow the steps in FortiGuard Incident Outbound Integration and Adding Automation Policy Settings to configure this feature.

FortiGuard Incident Outbound Integration

To create an outbound integration, follow these steps.

Step 1: Create an Integration

1. Go to **ADMIN > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.

- **Vendor**: select **FortiGuard IOC Lookup**.
- **Instance**: enter an instance name or accept the default.
- **Plugin Name**: is pre-populated with the name of the integration class: `com.accelops.service.integration.impl.FortiGuardIOCIntegrationServiceImpl`.

4. Enter an optional **Description** of the integration.
5. In the **Max Incidents** field, enter the maximum number of incidents you want recorded.
6. Click **Save**.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Policy** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

RiskIQ Integration

- Configuring RiskIQ for FortiSIEM Integration
- RiskIQ Incident Outbound Integration

Configuring RiskIQ for FortiSIEM Integration

Register at the RiskIQ website to obtain a user name, password, and the API keys. For more information, see https://api.riskiq.net/api/concepts.html.

RiskIQ Incident Outbound Integration

Step 1: Create an Integration

To create an outbound integration, follow these steps.

1. Go to **Admin > Settings > General > External Integration**.
2. Click **New** to create a new integration or **Edit** to modify an existing integration.
3. In the **Integration Policy** dialog box, provide the following values:
   - **Type**: select **Incident**.
   - **Direction**: select **Outbound**.
   - **Vendor**: select **RiskIQ**.
   - **Instance**: enter an instance name or accept the default.

- **Plugin Name**: is pre-populated with the name of the integration class: `com.accelops.phoenix.jira.JiraTicketIntegration`.
- **Username** and **Password**, enter your RiskIQ user name and the API key as the password.

4. Enter an optional **Description** of the integration.
5. Click the edit icon next to **Attribute Mapping**.
   a. In the **Incident Comments Template** dialog box, select content from the **Insert Content** drop-down list.
   b. Click **Save** when you are finished.
6. Click the edit icon next to the **Organization Mapping** to map attributes to resources.
7. Click the edit icon next to the **Run for**.
   a. In the **Run for** dialog box, select the organizations for which the integrations will be run.
   b. Click **Save** when you are finished.
8. Enter the maximum number of incidents you want recorded in the **Max Incidents** field.
9. Click **Save**.

Step 2: Link Integration to an Automation Policy

You need to link the integration to an automation policy, so that the integration runs when the automation policy triggers.

Take the following steps.

1. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**.
2. Click **New** to create a new policy or **Edit** to edit an existing policy.
3. In the **Automation Policy** dialog box, select **Action** > **Invoke an Integration Policy**, then select the edit icon.
4. Choose a specific integration from the drop-down list.
5. Click **Save**.

Configuring Communication through Proxies

If you want the communication between the FortiSIEM Supervisor and the external system to go through a proxy, then complete the following steps

1. Login to Supervisor as `admin`.
2. Go to the glassfish configuration directory: `/opt/glassfish/domains/domain1/config`.
3. Add proxy server information to the `domain.xml` file:
   <jvm-options>-Dhttp.proxyHost=172.30.57.100</jvm-options>
   <jvm-options>-Dhttp.proxyPort=3128</jvm-options>
   <jvm-options>-Dhttp.proxyUser=foo</jvm-options>
   <jvm-options>-Dhttp.proxyPassword=password</jvm-options>
4. Restart glassfish.

Modifying an External System Integration

Complete these steps to modify an External System Integration.

1. Use the below options to modify an External System Integration setting.

Settings	Guidelines
Edit	To edit an External System Integration setting.
Delete	To delete an External System Integration setting.

2. Click **Save**.

ServiceNow Security Operations (SecOps) Integration

- Scope and Purpose
- XML Assets
- Process Overview
- Process Workflow
- ServiceNow FortiSIEM Integration Usage
- ServiceNow FortiSIEM Integration Deletion
- ServiceNow and FortiSIEM Field Mappings
- Known Limitations

Scope and Purpose

ServiceNow FortiSIEM integration is designed to pull FortiSIEM incidents and triggering events from the remote FortiSIEM server every 30 seconds into the desired ServiceNow instance. FortiSIEM incidents pulled into the ServiceNow instance will be automatically mapped to new security incidents. Upon closing the created security incidents, the corresponding FortiSIEM incidents status on the remote FortiSIEM sever will also be updated.

XML Assets

The required XML files for this integration can be downloaded here.

File: FortiSIEM-ServiceNow-Integration-v1_3_6.zip

SHA256 hash: 945214c2128337dc7d8b03f80ebd51e1a07a8c75c855c3ec49583ca61d43e1f5

MD5 hash: d397ad5bf6ba0c0e15942958b95bad4e

Process Overview

1. The ServiceNow system administrator must request a new Paris release ServiceNow instance or login to an existing one to import the provided ServiceNow FortiSIEM integration XML file to ServiceNow.

2. The ServiceNow system administrator configures the REST Message API endpoints and Basic Auth Profile settings on the ServiceNow instance to make API calls to the remote FortiSIEM server.
3. The ServiceNow instance will begin to fetch FortiSIEM incidents and triggering events every 30 seconds.
4. The ServiceNow system administrator or ServiceNow users with security incident roles can view and update security incidents created from FortiSIEM incidents pulled.

Process and Workflow

The following information contains a detailed explanation on how ServiceNow FortiSIEM integration is set up and its usage.

ServiceNow FortiSIEM Integration Prerequisites

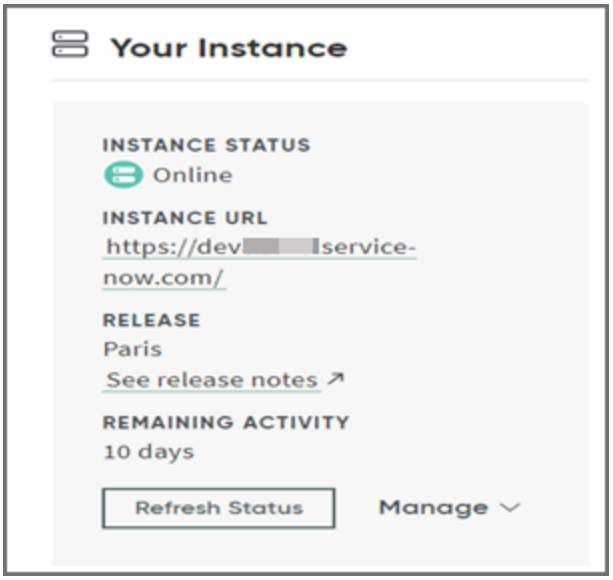
The following is required for ServiceNow FortiSIEM integration.

1. FortiSIEM server.
2. Paris release ServiceNow instance.
3. ServiceNow instance plugin – Security Incident Response Dependencies.
4. ServiceNow instance plugin – Security Incident Response.

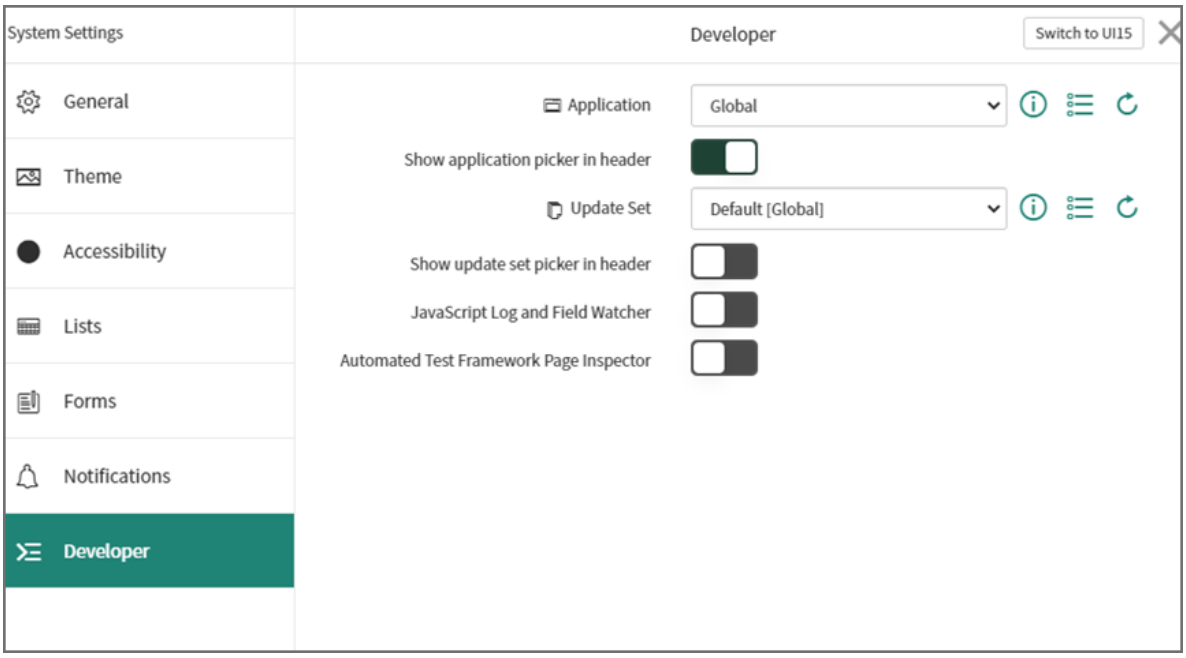
ServiceNow FortiSIEM Integration Installation

A ServiceNow system administrator must take the following steps:

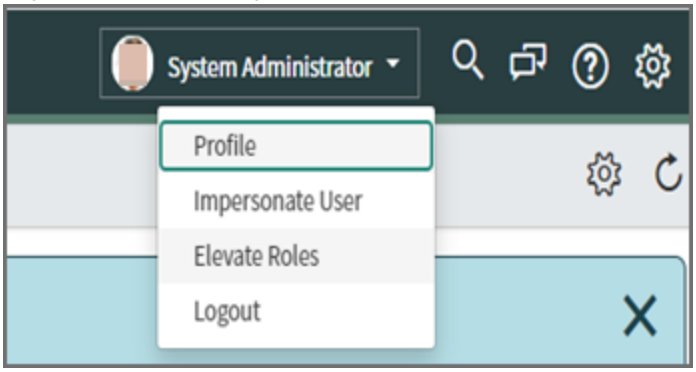
1. Request a new Paris release ServiceNow instance or login to an existing one.

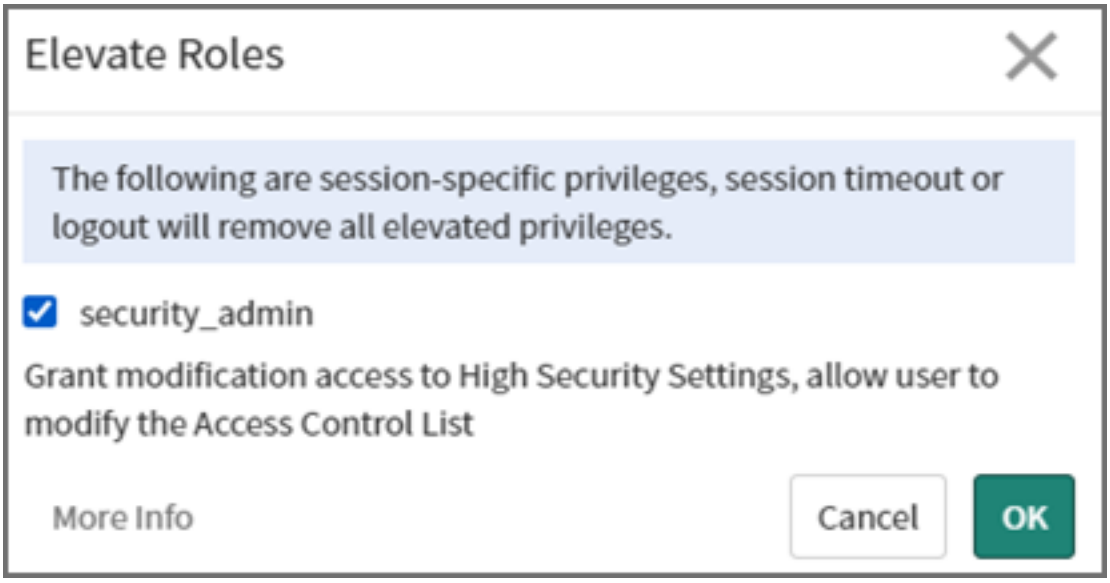


2. In the ServiceNow instance, click the **Application** drop-down list and select **Global**.

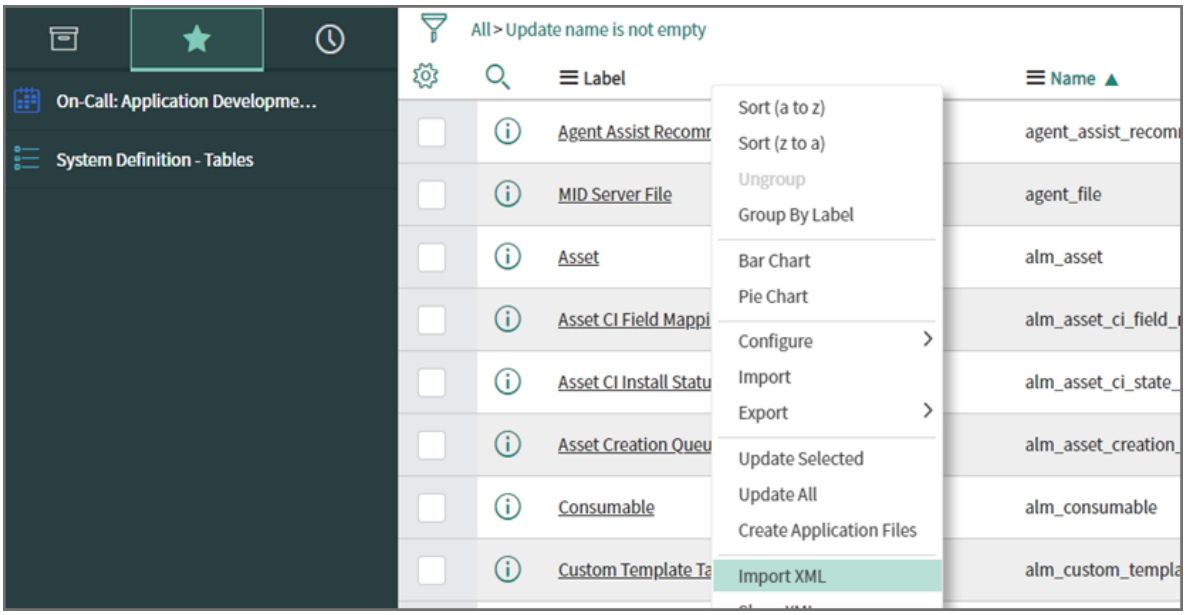


3. Click on the role drop down list and select **Elevate Roles**. Elevate the "System Administrator" role to "Security Admin". This new role ensures the success of the ServiceNow FortiSIEM integration import in the next step.

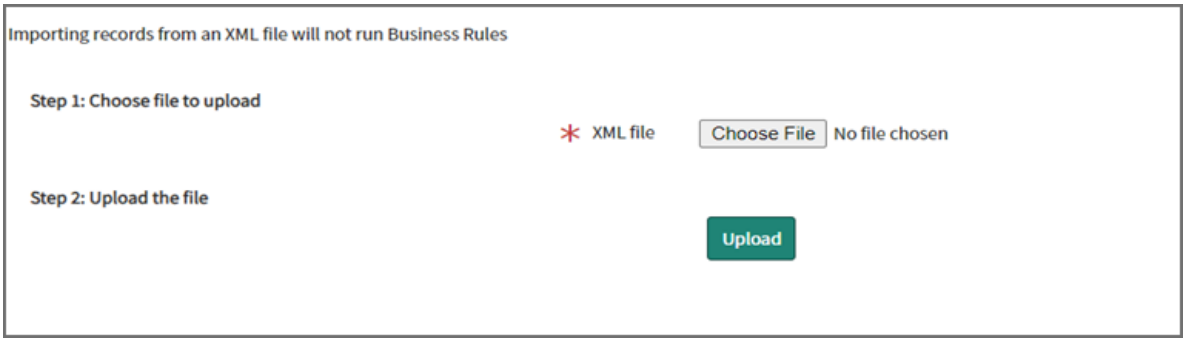




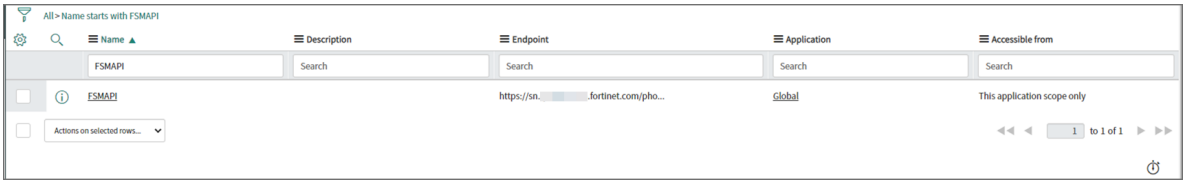
4. Navigate to **System Definition - Tables**, right click on **Table Headers** on the page, and select **Import XML**.



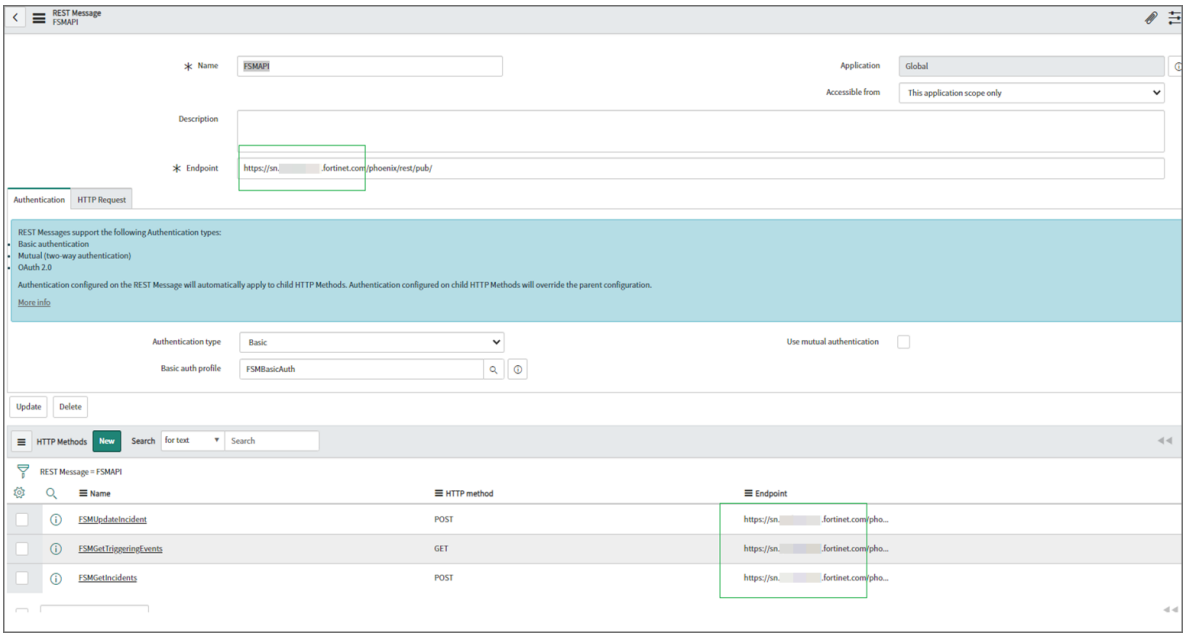
5. In "Import XML", select the provided `FSMSNIntegrationImportData` file (See XML Assets) and click **Upload**.



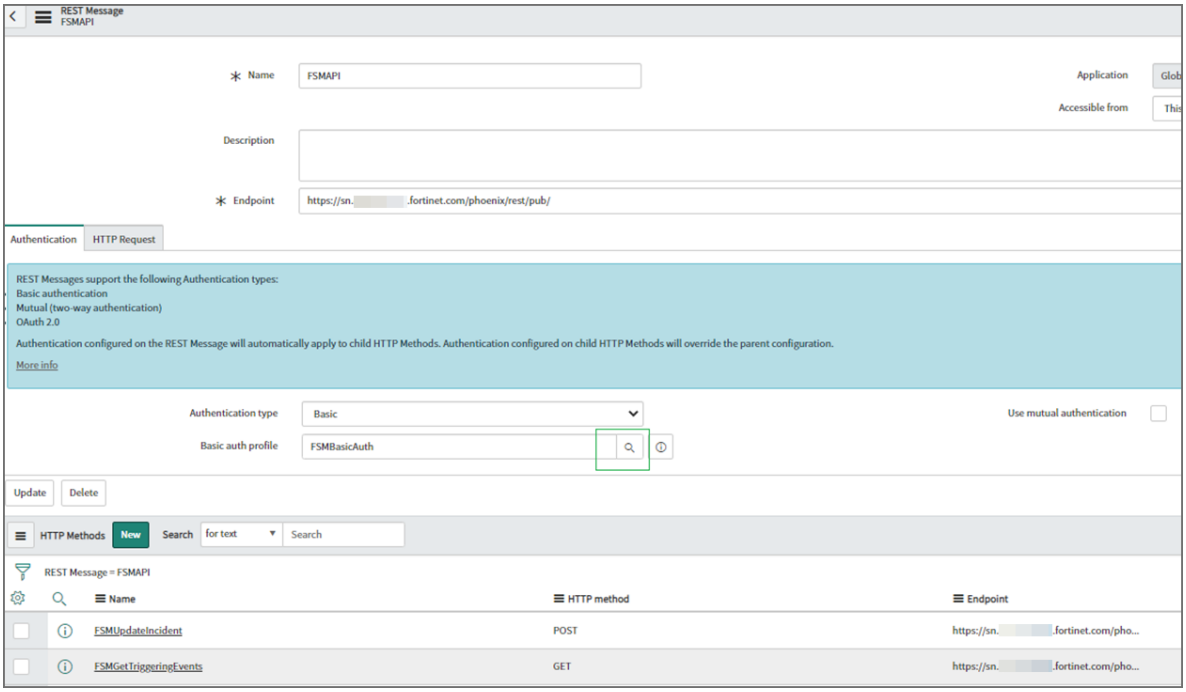
6. After the upload is complete, navigate to **System Web Services/Rest Message**, and click on **FSMAPI** (This was imported in step 5) to change the FortiSIEM remote server API endpoint and basic auth profile.



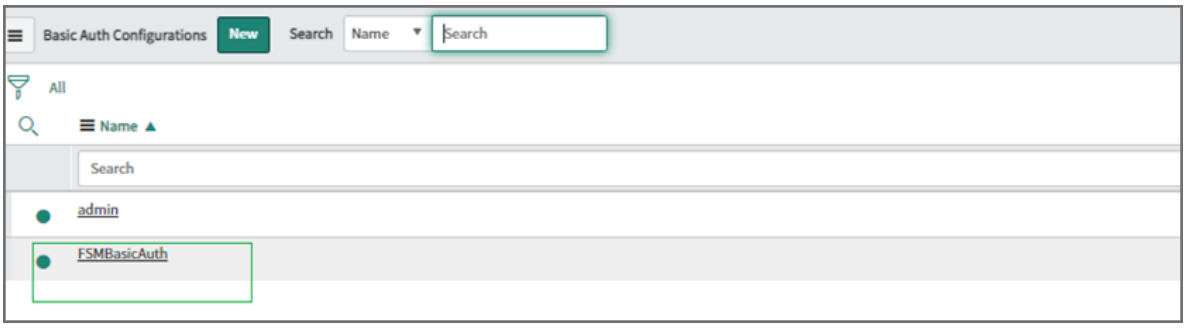
7. In **REST Message/FSMAPI**, if the remote FortiSIEM server host name is different than the ones displayed, please manually change the hostname in “FSMAPI” and all the endpoints in **HTTP Methods**, as shown here. For **HTTP Methods**, please manually click on each record, and change the hostname.
Note: Only change the host name.(I.E. `https://myNewHostName.com`). The slashes or symbols after the host name must be retained.



8. In “REST Message/FSM API”, to change the basic auth profile, first click the search icon.



9. Click **FSMBasicAuth**, and change the user name and password accordingly. You may also create a new Basic auth profile.



10. The integration uses a “HTTPS outbound REST end point”, and requires the FortiSIEM certificate to be added to the ServiceNow Certificate Trust Store. Please follow the sub-steps here before proceeding to step 11.
    a. Retrieve destination server SSL certificates. This can be given by the network administrator of the destination server, or by using the Linux command:
    `openssl s_client -connect <destination_server_name>:443 –showcerts`

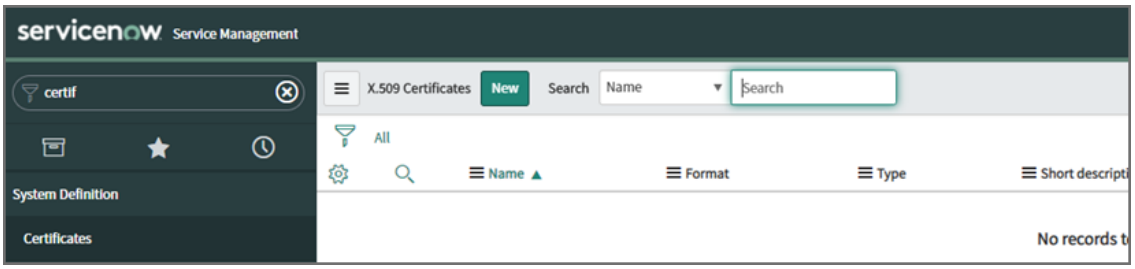
    To gather the specific certificate, run this command from a Linux server:
    `echo | openssl s_client -connect <destination_server_name>:443 2>&1 | sed --quiet '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > <destination_server_name>.pem`

    A sample SSL certificate is shown here.

    b. Validate retrieved SSL certificate in part a to see if it has any issues or errors. It can be done through https://www.digicert.com/help/ or through the Linux command:
    `openssl s_client -connect <destination_server_name>:443 –showcerts`

If the certificate has issues or errors, please contact the destination server administrator for a correct one. For any reason that a correct SSL certificate cannot be obtained, please refer to step 10g for a temporary workaround in a ServiceNow instance. **Note that this workaround is not recommended for ServiceNow production instances**.

c. Now, upload the retrieved SSL certificate in part a to the ServiceNow instance. Navigate to **System Definition/Certificates** and on the right panel, click **New**.



d. On the new dialog box, take the following steps:

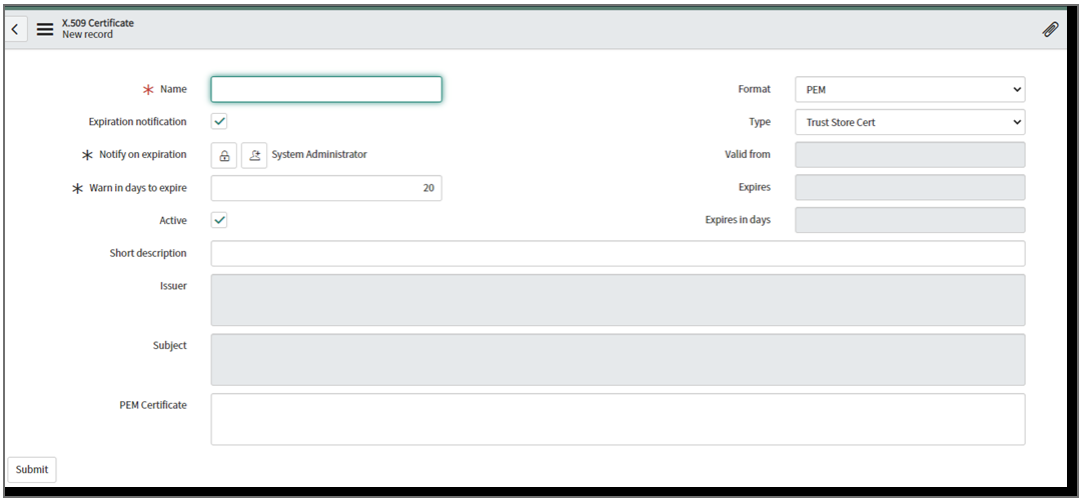
i. In the **Name** field, enter a name for the certificate.

ii. From the **Format** drop-down list, select **PEM**.

iii. From the **Type** drop-down list, select **Trust Store Cert**.

iv. In the **PEM Certificate** field, enter/paste the SSL certificate retrieved in 10a.

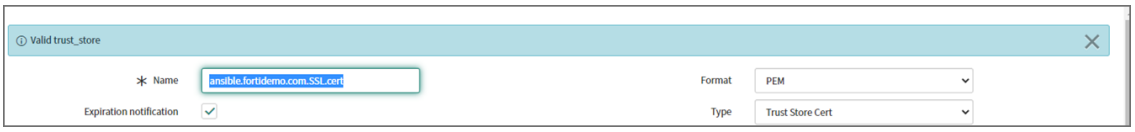
v. When done, click **Submit**.



e. Once the certificate has been created, click on it.

f. Click **Validate Stores/Certificates** to ensure it is valid.

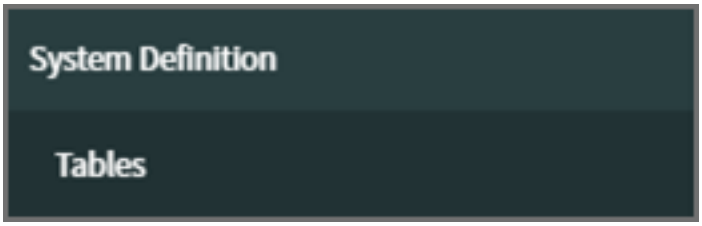
If it is valid, a “Valid trust_store” message will show. If you get an invalid certificate, please contact the destination server administrator.



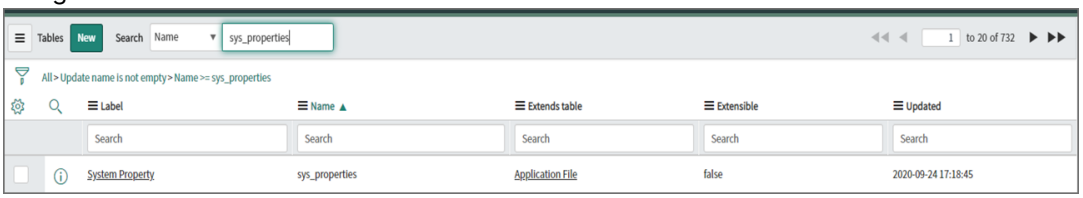
g. **Note**: This is workaround step in ServiceNow instance to solve invalid certification issue encountered in step 10b.
This is only recommended for ServiceNow developer instances.

To proceed, take the following steps:

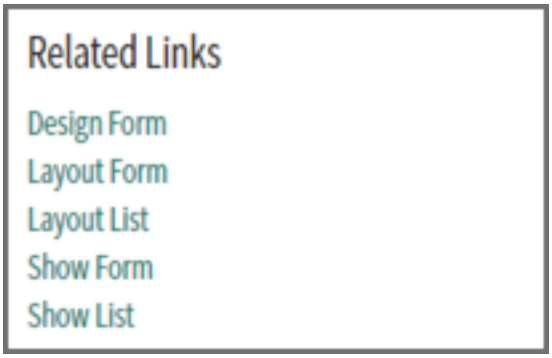
i. Navigate to **System Definition / Tables**.



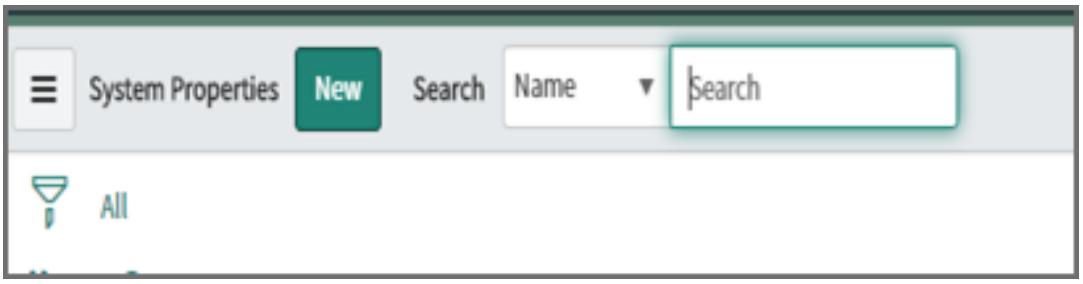
ii. Search for “sys_properties”, click on **System Property** from the displayed records and navigate to **Related Links**.



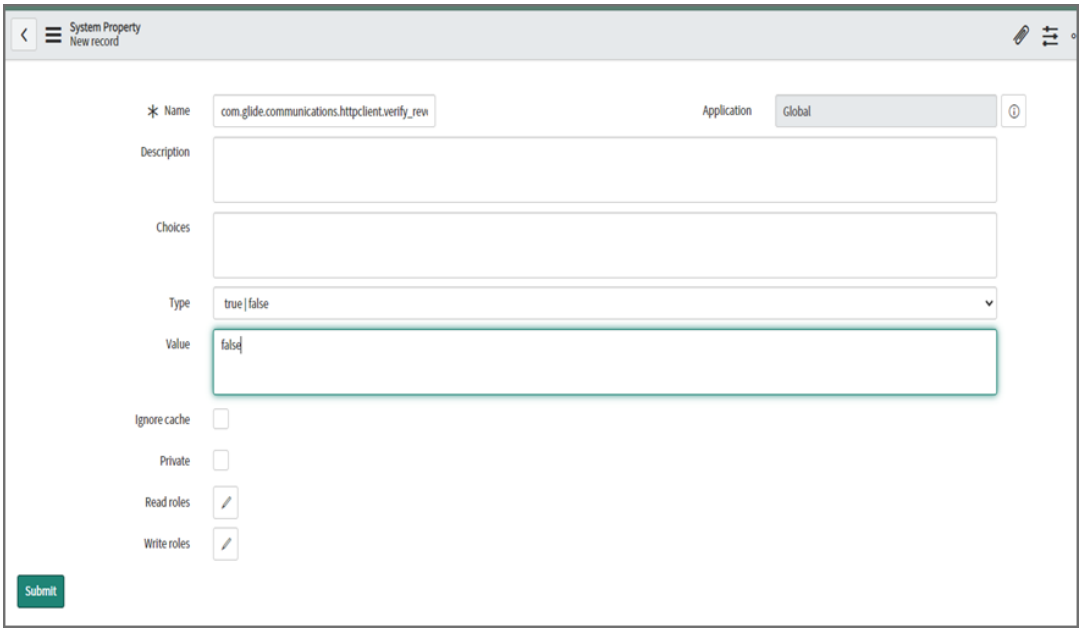
iii. Click **Show List** to open up all system properties entries stored in the current instance.



iv. Next to the System Properties header, click **New**.

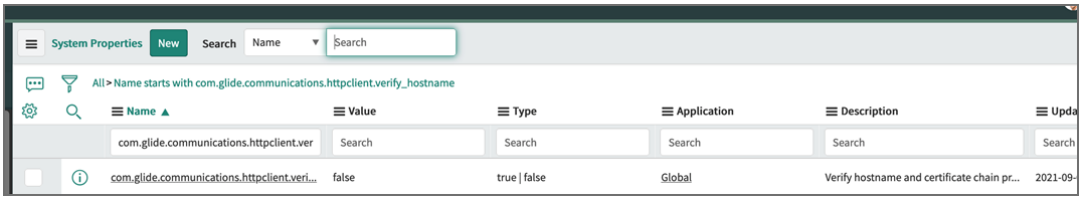


v. Enter the following:
In the **Name** field, enter "com.glide.communications.httpclient.verify_revoked_certificate".
In the **Type** field, enter "true|false".
In the **Value** field, enter "false".



vi. Click **Submit**.

vii. If the certificate in use by FortiSIEM is also Self Signed, then set the following System Property to false . Under the same section, search for *com.glide.communications.httpclient.verify_hostname* and change to false.



Once this record has been created, the ServiceNow instance will ignore any SSL certification validation issues or errors encountered.

The installation is now complete.

ServiceNow FortiSIEM Integration Usage

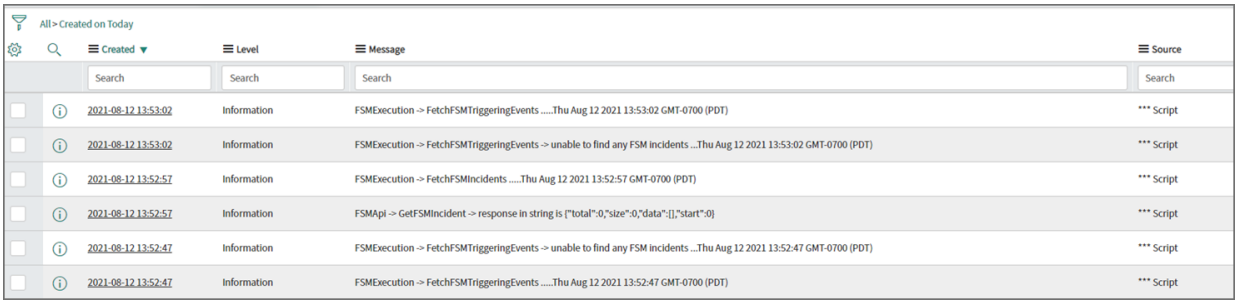
The ServiceNow FortiSIEM Integration can be used in the following ways:

View Scheduled Jobs

The ServiceNow system administrator can view scheduled jobs that are running every 30 seconds to pull FSM incidents and FSM triggering events in “System Definitions/ Scheduled Jobs”.

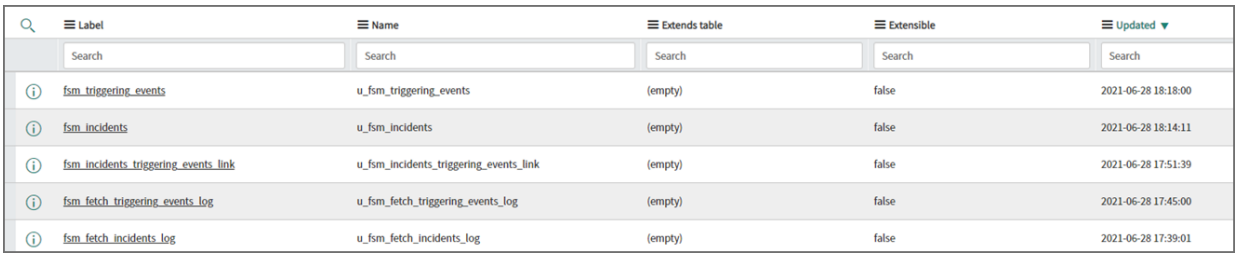
Monitor Scheduled Job Execution Logs

The ServiceNow system administrator can monitor the scheduled job execution logs in **System Log / All**.



Examine FortiSIEM Incidents, Logs, and Triggering Events

Fetched FortiSIEM incidents will be stored in the “fsm_incidents” table, and logs will be stored in “fsm_fetch_incidents_log” table. Fetched FSM triggering events will be stored in “fsm_triggering_events” table, and logs will be stored in the “fsm_riggering_events_log” table. The link between incidents and events will be stored in the “fsm_incidents_triggering_events_link” table.

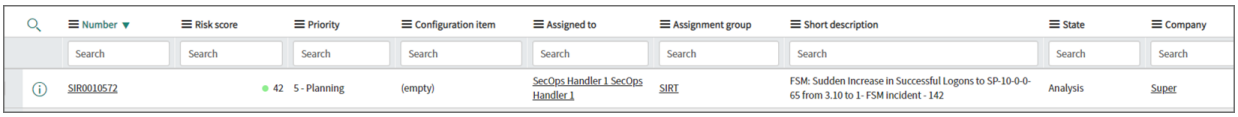


Label	Name	Extends table	Extensible	Updated
fsm_triggering_events	u_fsm_triggering_events	(empty)	false	2021-06-28 18:18:00
fsm_incidents	u_fsm_incidents	(empty)	false	2021-06-28 18:14:11
fsm_incidents_triggering_events_link	u_fsm_incidents_triggering_events_link	(empty)	false	2021-06-28 17:51:39
fsm_fetch_triggering_events_log	u_fsm_fetch_triggering_events_log	(empty)	false	2021-06-28 17:45:00
fsm_fetch_incidents_log	u_fsm_fetch_incidents_log	(empty)	false	2021-06-28 17:39:01

View Corresponding Security Incidents

After a FortiSIEM incident has been fetched, a corresponding security incident will be created with the short description:

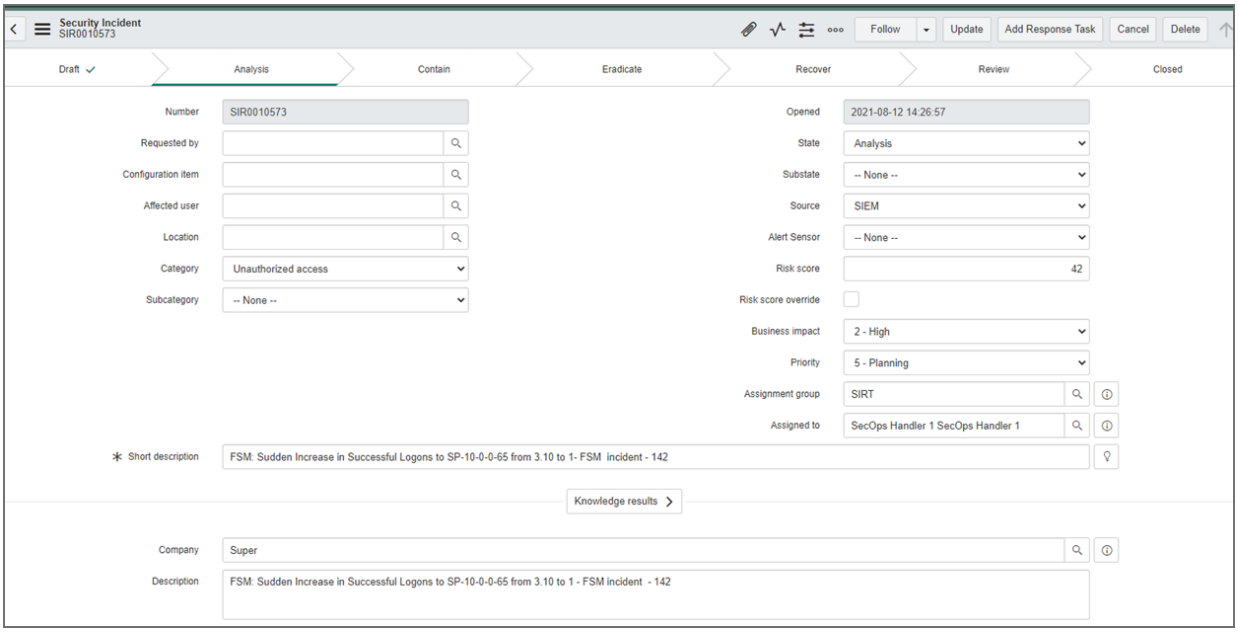
`FSM : <IncidentTitle> - FSM Incident - <IncidentID>`



Number	Risk score	Priority	Configuration item	Assigned to	Assignment group	Short description	State	Company
SIR0010572	42	5 - Planning	(empty)	SecOps Handler 1 SecOps Handler 1	SIRT	FSM: Sudden Increase in Successful Logons to SP-10-0-0-65 from 3.10 to 1- FSM incident - 142	Analysis	Super

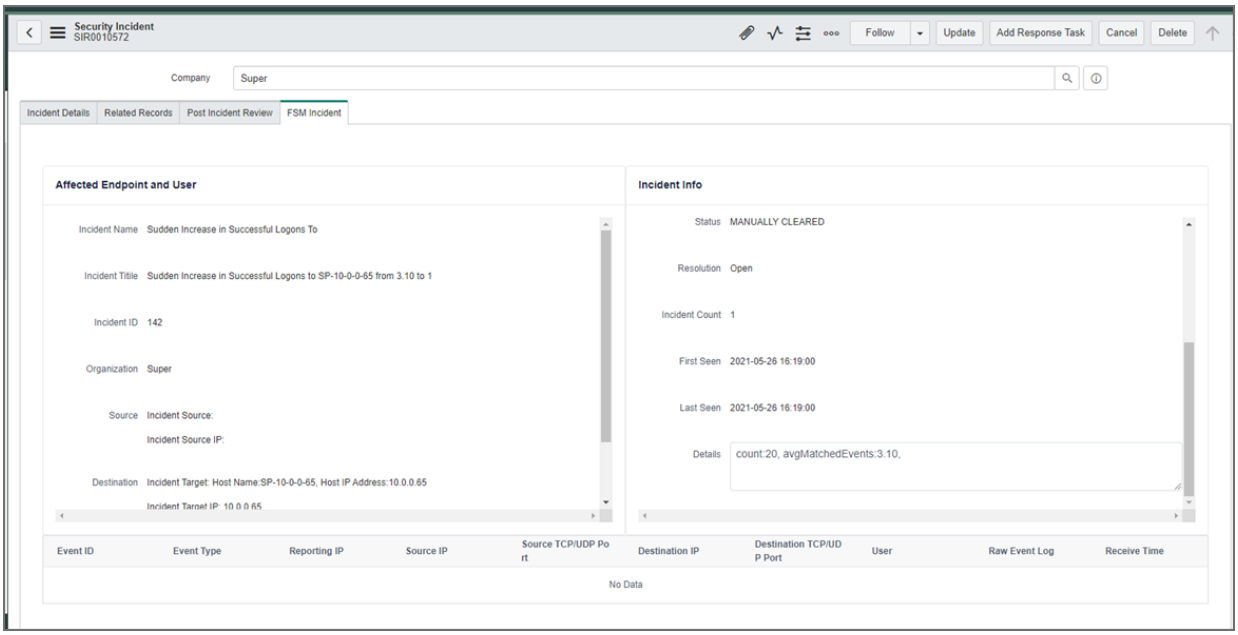
Examine Security Incidents in Detail

Security incidents created by FortiSIEM incident contain the “Category”, “Source”, “Priority”, “Description”, “Short Description”, and “Company” fields, pre-defined based on corresponding FortiSIEM incident fields.



Customized "FortiSIEM Incident" Page

Security incident created by FortiSIEM incidents also have a customized UI section **FSM Incident**, which can be used to view FortiSIEM incident details and triggering events. For the current version V1.3.6, 10 triggering events are fetched per FortiSIEM incident.

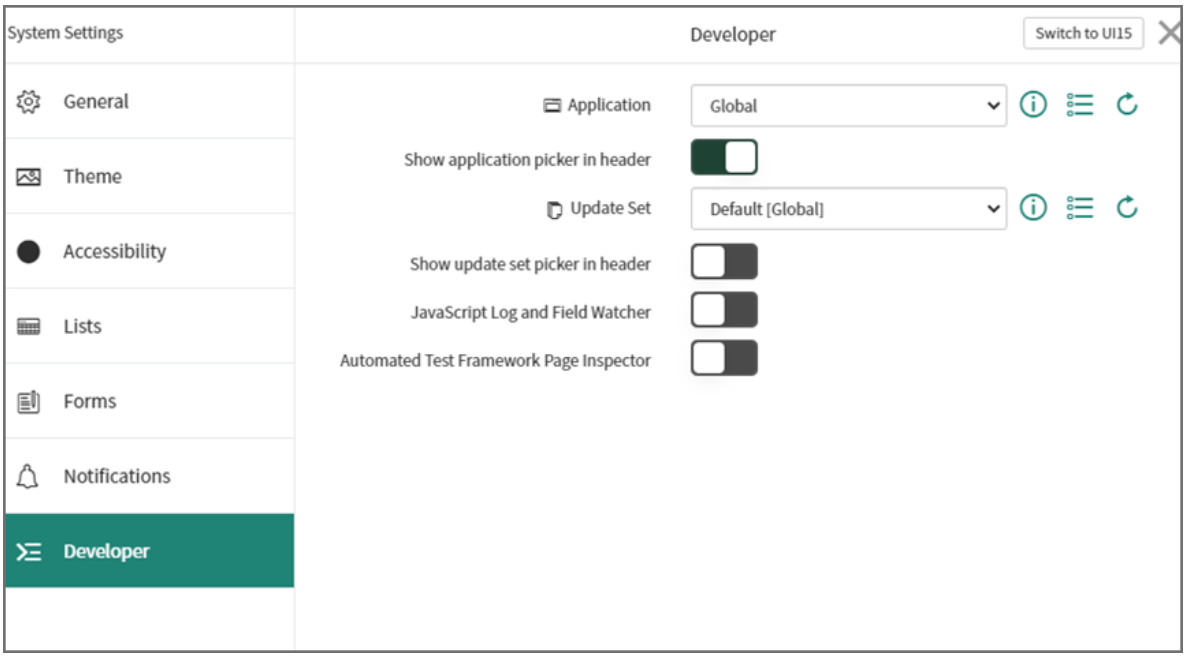


ServiceNow FortiSIEM Integration Deletion

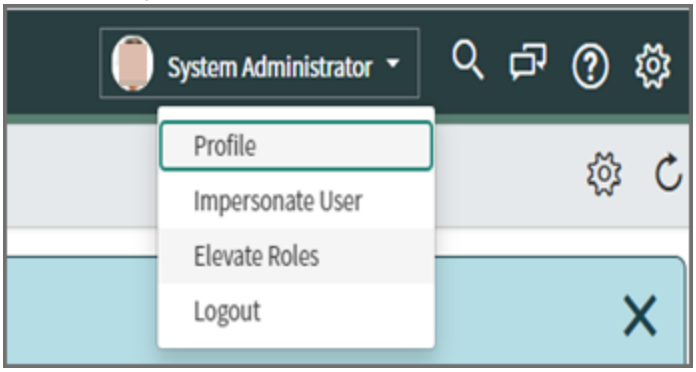
Deleting the Integration will remove the FortiSIEM configuration, scheduled jobs, GUI elements, Incident information from FortiSIEM and Triggering events in ServiceNow. **Do not proceed if these ServiceNow elements and FortiSIEM Incident data is needed in your ServiceNow instance.**

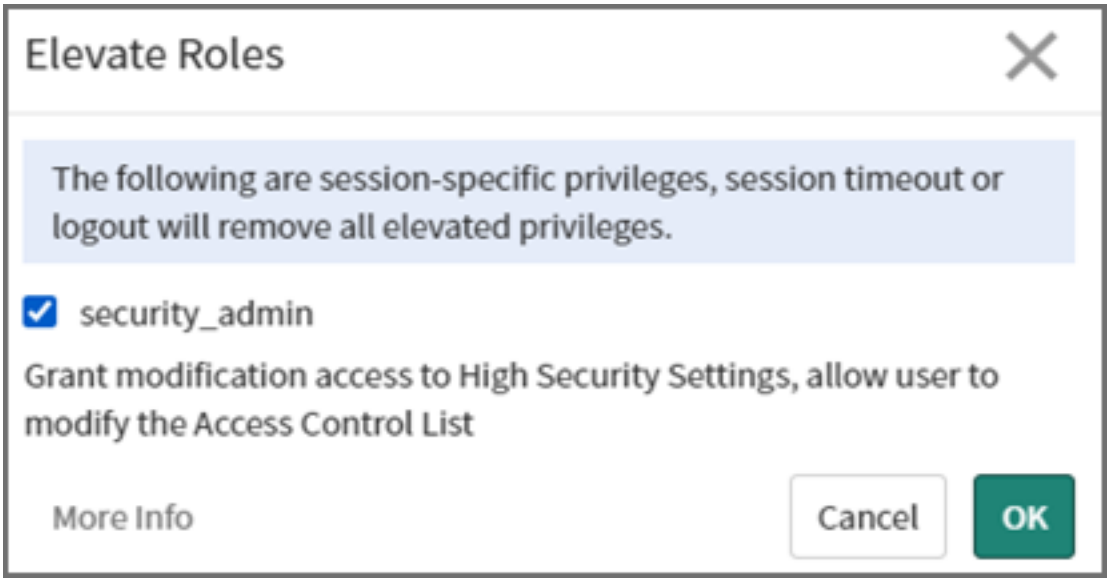
To remove ServiceNow FortiSIEM Integration, take the following steps as a ServiceNow system administrator:

1. Navigate to System Settings, and set Application to **Global**.

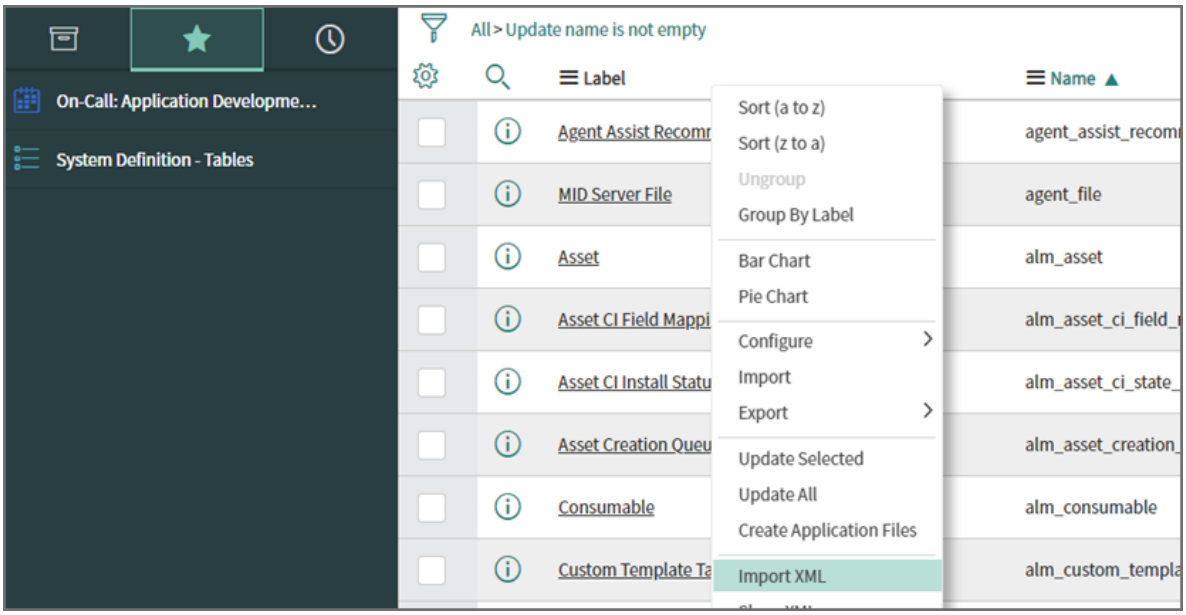


2. Click on the role drop down list and select **Elevate Roles**. Elevate the "System Administrator" role to "Security Admin". This role ensures the success of the ServiceNow FortiSIEM integration import in the next step.

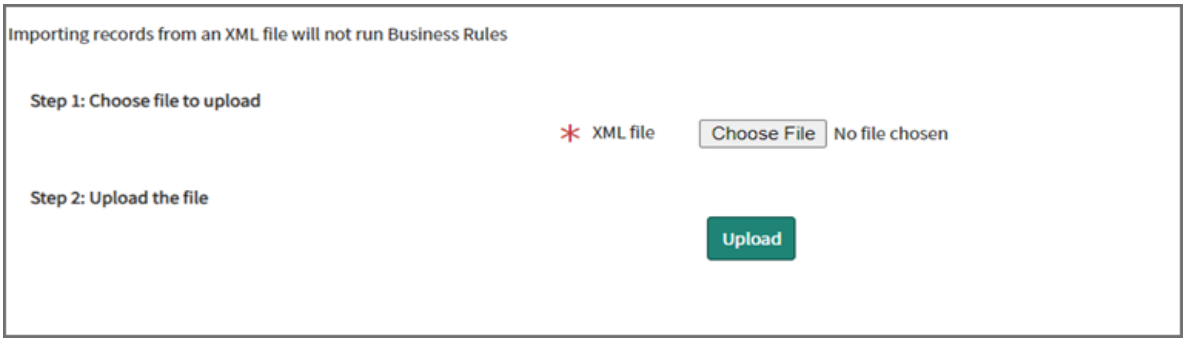




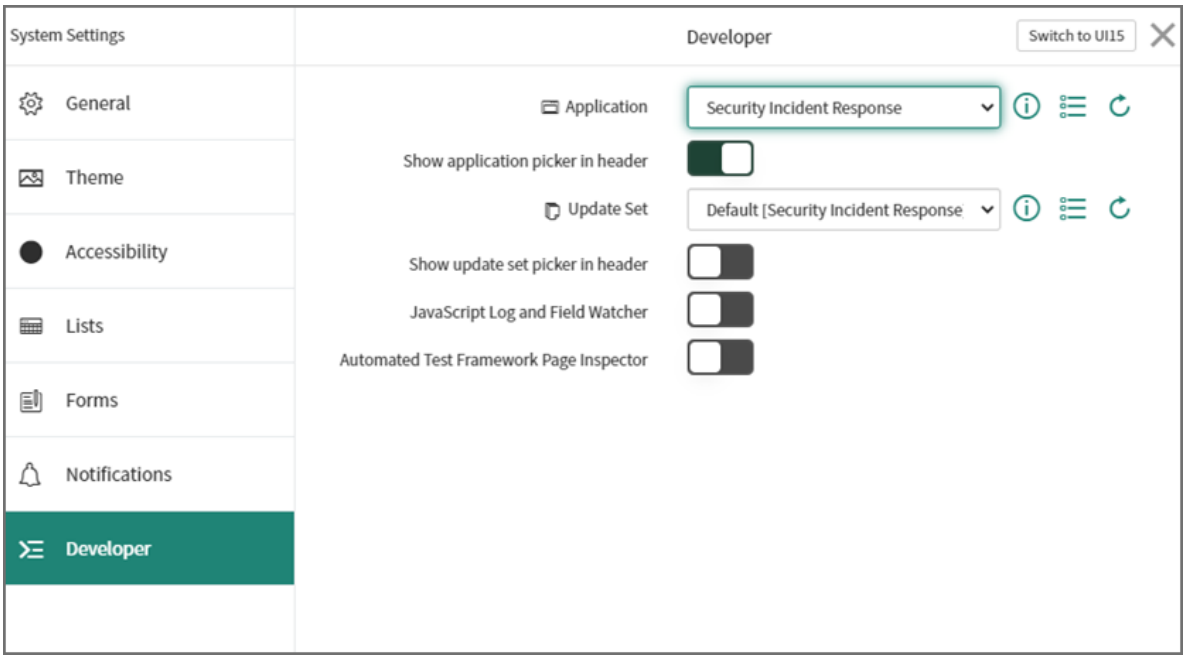
3. With the elevated role, navigate to **System Definition - Tables**. Right click on “table headers” on the page and select **Import XML**.



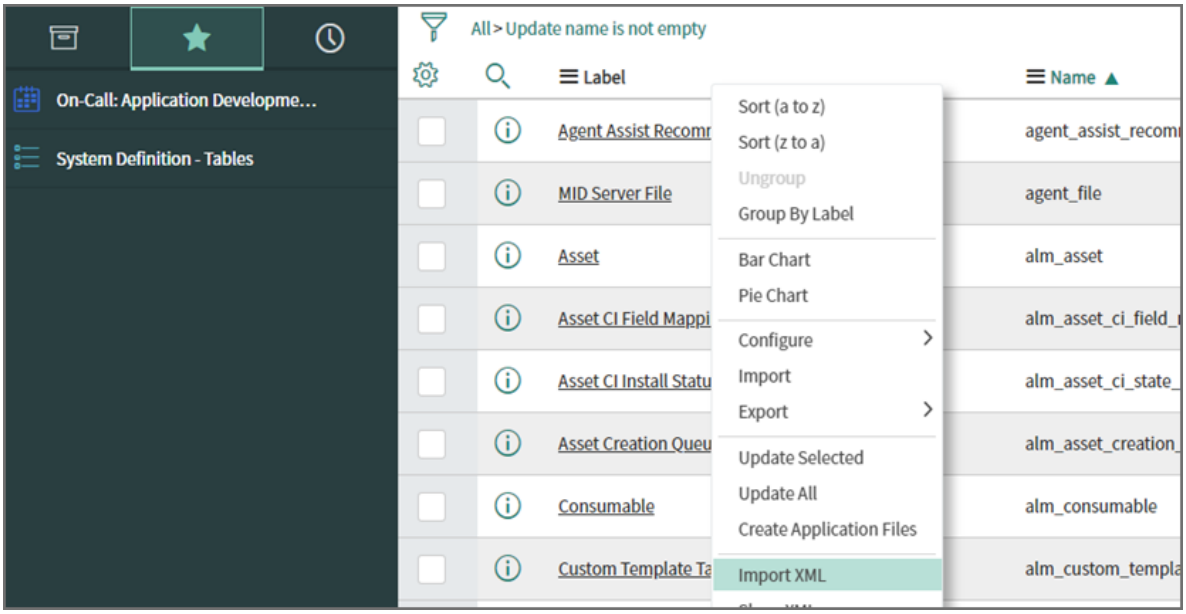
4. In “Import XML”, select the provided `FSMSNIntegrationDeleteData` file (See XML Assets) and click **Upload**.



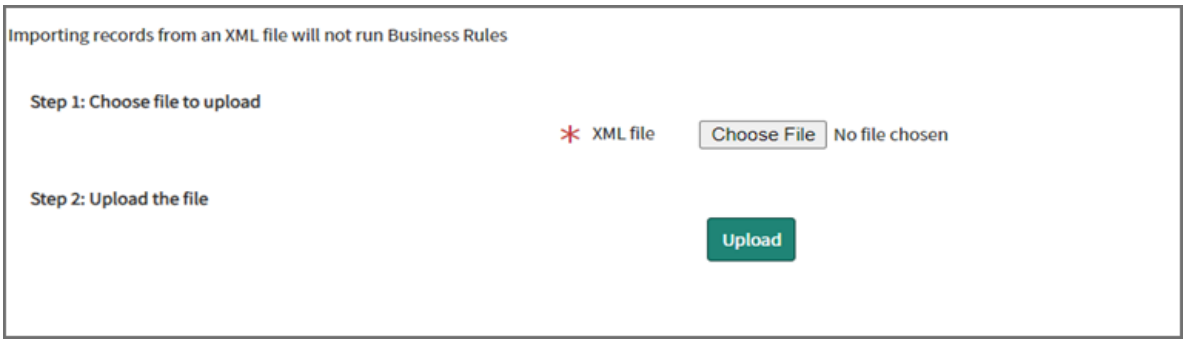
5. To complete the deletion process, you must have the elevated “Security Admin” permission, and change **Application** to “Security Incident Response”.



6. Navigate to **System Definition - Tables**, right click on “table headers” of the page and select **Import XML**.



7. In “Import XML”, select the provided `delete_sys_ui_section` file (See XML Assets) and click **Upload**.



The ServiceNow FortiSIEM Integration deletion is now complete.

ServiceNow and FortiSIEM Field Mappings

FortiSIEM Closed State Mappings

FortiSIEM Incident State	ServiceNow Incident State
MANUALLY CLEARED, 2	Closed

FortiSIEM Incident Category Field: "phSubIncidentCategory" Mappings

FortiSIEM Incident Category	ServiceNow Category	FortiSIEM Major Rule Categories
Audit	Policy violation	Change
Authentication	Failed login	Security
Command and Control	Malware	Security
Command and Control	Malware	Security
Credential Access	Unauthorized access	Security
Defense Evasion	Privilege escalation	Security
Discovery	Reconnaissance activity	Security
Execution	Malicious code activity	Security
Exfiltration	Confidential personal identity data exposure	Security
Exploit	Malware	Security
Initial Access	Unauthorized access	Security
Lateral Movement	Privilege esclation	Security
Mail Server	Spam source	Security
Malware	Malware	Security
Persistence	Malware	Security
Policy Violation	Policy violation	Security
Privilege Escalation	Privilege escalation	Security
Reconnaissance	Reconnaissance activity	Security
Suspicious Activity	Reconnaissance activity	Security
UEBA	Insider Breach	Security

The following FortiSIEM incidents do not have a mapping to ServiceNow SecOps categories.

FortiSIEM	ServiceNow	FortiSIEM Major Rule Categories
Application		Performance
Behavioral Anomaly		Security
Collection		Security
CPU		Performance
Database		Performance
Domain Controller		Performance
Environmental		Performance
FortiSIEM		Performance
Hardware		Performance
HVAC		Performance
Impact		Performance
Interface		Performance
License		Availability
Memory		Performance
Network		Performance
Performance		Performance
SDN		Performance
Server		Performance
Storage		Performance
Storage I/O		Performance
Storage Space		Performance
UPS		Performance
Video Conferencing		Performance
VoIP		Performance
WAN		Performance
Windows Cluster Service		Performance

FortiSIEM	ServiceNow	FortiSIEM Major Rule Categories
Windows File System Replication		Performance

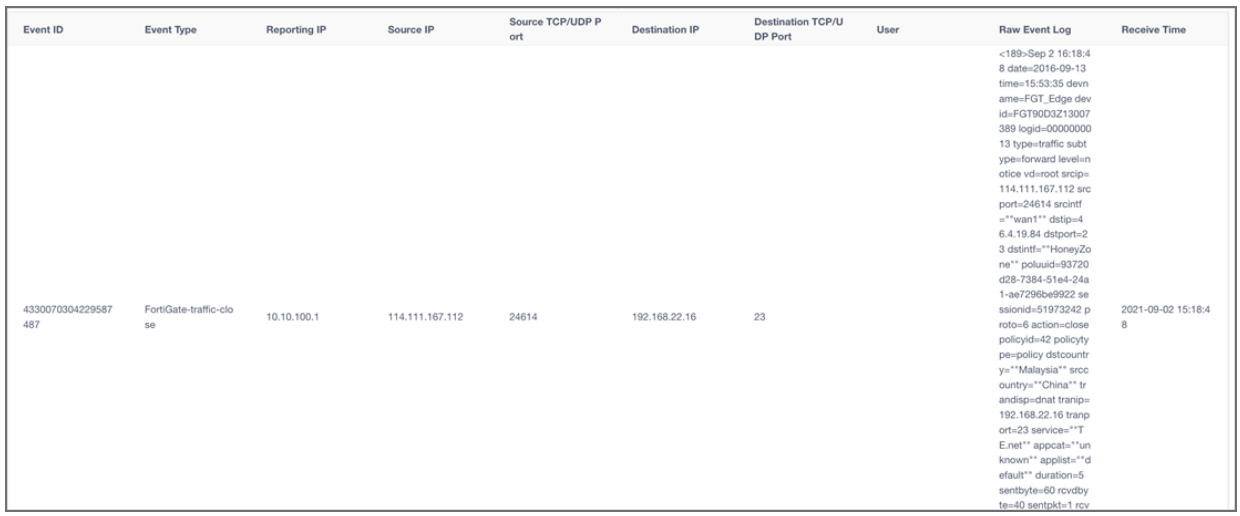
FortiSIEM Incident Severity Field: "eventSeverity" Mappings

FortiSIEM Severities	ServiceNow Severities
10	1 - Critical
9	2 - High
5 to 8	3 - Moderate
1 to 4	4 - Low
N/A	5 - Planning

FortiSIEM Triggering Events Attributes Displayed in ServiceNow

Name	Attribute Name	Type	Always Present in Triggering Events
Event Receive Time	phRecvTime	date	Yes
Event Type	eventType	string	Yes
Reporting IP	reptDevIpAddr	IP	Yes
Source IP	srcIpAddr	IP	No
Source TCP/UDP Port	srcIpPort	uint16	No
Destination IP	destipAddr	IP	No
Destination TCP/UDP Port	destipPort	uint16	No
User	User	string	No
Raw Event Log	rawEventMsg	string	Yes

Here is an example.



Event ID	Event Type	Reporting IP	Source IP	Source TCP/UDP Port	Destination IP	Destination TCP/UDP Port	User	Raw Event Log	Receive Time
4330070304229587487	FortiGate-traffic-close	10.10.100.1	114.111.167.112	24614	192.168.22.16	23		<189>Sep 2 16:18:48 date=2016-09-13 time=15:53:35 devname=FGT_Edge devid=FGT90D3Z13007389 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=114.111.167.112 srcport=24614 srcintf=""wan1"" dstip=46.4.19.84 dstport=23 dstintf=""HoneyZone"" poluuid=93720d28-7384-51e4-24a1-ae7296be9922 sessionid=51973242 proto=6 action=close policyid=42 policytype=policy dstcountry=""Malaysia"" srccountry=""China"" trandisp=dnat tranip=192.168.22.16 tranport=23 service=""TE.net"" appcat=""unknown"" applist=""default"" duration=5 sentbyte=60 rcvdbyte=40 sentpkt=1 rcv	2021-09-02 15:18:48

Known Limitations

The following are known limitation for this integration:

- Incidents are synced by ServiceNow to FortiSIEM every 30 seconds. This is not configurable.
- Incident status changes in FortiSIEM, e.g. are not synced to ServiceNow.
- Incident External ID and External Incident Status is not synced to FortiSIEM from ServiceNow until there is a change to the ServiceNow incident such as the State or assignment to a User.

Required Permissions for ServiceNow SOAP Integration

General Requirements

FortiSIEM uses ServiceNow Direct Web Service for integration. FortiSIEM communicates on SOAP port 80.

The following SOA APIs are used:

- Insert
- Update
- getKeys
- get
- getRecords

The following role types are required:

- soap_create
- soap_query
- soap_query_update
- soap_update

The following Table and Field permissions are provided.

- Required Table and Field Permissions for CMDB Outbound Integration
  - Main Table Permissions
  - Extended Table Permissions
  - Reference Table Permissions
  - Reference Field Permissions
  - Regular Field Permissions
- Required Table and Field Permissions for Incident Outbound Integration
  - Main Table Permissions
  - Reference Table Permissions
  - Reference Field Permissions
  - Regular Field Permissions

Required Table and Field Permissions for CMDB Outbound Integration

Main Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
configuration item [cmdb_ci]	• Query • Insert • Update	• Read • Write • Create
Running Process [cmdb_running_process]	• Query • Insert / Create • Update	• Read • Write • Create
Software Instance [cmdb_software_instance]	• Query • Insert / Create • Update	• Read • Write • Create

Extended Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
cmdb_ci_linux_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_win_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_hpux_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_unix_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_aix_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_solaris_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_esx_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_web_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_java	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_tomcat	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_weblogic	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_ websphere	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_app_server_jboss	• Query • Insert / Create • Update	• Read • Write • Create

ServiceNow Table	FortiSIEM Actions	Required Permissions
cmdb_ci_netware_server	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_database	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_vpn	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_ip_router	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_netgear	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_ups	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_printer	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_network_adapter	• Query • Insert / Create • Update	• Read • Write • Create
cmdb_ci_storage_disk	• Query • Insert / Create • Update	• Read • Write • Create

Reference Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
Company [core_company]	• Query	• Read

Reference Field Permissions

Field	ServiceNow Table	Required Permissions	Need write_role
company	core_company	• Read • Write	Yes. The default role in ServiceNow is : admin

Regular Field Permissions

Need Read/Write and write_role is not required.

Required Table and Field Permissions for Incident Outbound Integration

Main Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
Incident [incident]	• Query • Insert / Create • Update	• Read • Write • Create

Reference Table Permissions

ServiceNow Table	FortiSIEM Actions	Required Permissions
Company [core_company]	• Query	• Read

Reference Field Permissions

Field	ServiceNow Table	Required Permissions	Need write_role
assigned_to	sys_user	• Read	Yes. The default role in ServiceNow is : itil
company	core_company	• Read • Write	Yes. The default role in ServiceNow is: admin

Regular Field Permissions

Field	Required Permissions	Need write_role
state	• Read	Yes. The default role in ServiceNow is : itil
comments	• Read • Write	Yes. The default role in ServiceNow is : itil
closed_by	• Read	Yes. The default role in ServiceNow is : itil
short_description	• Read • Write	Yes. The default role in ServiceNow is : itil
impact	• Read • Write	Yes. The default role in ServiceNow is : itil
urgency	• Read • Write	Yes. The default role in ServiceNow is : itil
closed_at	• Read	Yes. The default role in ServiceNow is : admin
work_notes	• Read • Write	Yes. The default role in ServiceNow is : itil
Active	• Read • Write	No

Case Management

Case Management allows you to define policies for cases and define case close codes for use with the FortiSIEM Case system. To use a case management policy, you must have a group and users created under **FortiSIEM Analysts** in **CMDB > Users**. See Setting Up Manual Case Management or Setting Up Automatic Case Management for general initial configuration steps. A general Case Management demo video is available here.

- Adding/Editing a Case Management Policy
- Adding/Editing Case Close Codes
- Viewing Case Management Policy
- Viewing Case Close Codes
- Applying Case Creation to Automation Policy

Adding/Editing a Case Management Policy

To create/edit a Case Management Policy, take the following steps.

1. From **Admin > Settings > General > Case Management**, click the **Case Management Policy** tab.
2. If creating a new case management policy, click **New**. If editing a case management policy, select the policy you wish to edit, and click **Edit**.
3. Click on each tab to view and configure its settings.
   a. Configure the **General** settings using the table below.

General Settings	Guidelines
Name	Enter the name of the case management policy. This name is used as a reference
Description	Enter a description of the case management policy.

   b. The SLA & Escalation setting allows you to configure how escalations are handled based on their case severity (Critical, High, Medium, and Low). For each case severity type, configure the **SLA & Escalation** settings using the table below.

SLA & Escalation Settings	Guidelines
SET Due Date as:	Configure the due date. The due date can be configured as the period of time "Days" or "Hours". In the first field, enter a numeric value. From the drop-down list, select Days or Hours to configure the period of time as Days or Hours respectively.
WHEN Remaining Time is within: OR Due Date violated	Configure the remaining period of time that must occur from a case, or the due date is violated when an email notification is sent. In the first field, enter a numeric value. From the drop-down list, select Days or Hours to configure the period of time as Days or Hours respectively.
THEN Email To:	Configure for whom an email will be sent to, when a case reaches the remaining time configured, or the due date has been violated, by selecting the Assignee, Team Lead and/or Assignee's Manager checkbox.
If no Case Update in:	Configure when an email is sent if there is no case update. In the first field, enter a numeric value. From the drop-down list, select Days or Hours to configure the period of time as Days or Hours respectively.
THEN Email To:	Configure for whom an email will be sent to, when a case update has not occurred within the configured period of time, by selecting the Assignee, Team Lead and/or Assignee's Manager checkbox.

c. Configure the **Auto-assignment** settings using the table below.

Auto-assignment Settings	Guidelines
Assignment within Team	Configure how cases are automatically assigned. • Always Assign To Team Lead - Select this option to have all cases be automatically assigned to the Team Lead. • Randomly within Team members - Select this option to randomly assign cases to team members. • Team member with least number of Cases - Select this option to automatically assign the newest case to a team member with the least number of cases.
No Assignee found within Team	Configure how cases, based on case severity type, are handled if no assignee can be found. From the drop-down list, configure what case severity types are handled by selecting them from the drop-down list. In the next drop-down list, select whether the configured case severity types will be put in the First or Last Team Queue or to the First or Last Team Lead if no assignee can be located. In the next drop-down list, configure how other case severity types that were not part of the earlier configuration are handled in the Team Queue, by selecting whether to leave the case in the First or Last Team Queue.

d. Configure the **Permissions** settings using the table below.

Permissions Settings	Guidelines
Change Status	Select the personnel allowed to change the status of a case, by selecting the appropriate checkboxes.
Edit Note	Select the personnel allowed to edit cases by selecting the appropriate checkboxes.

e. Configure the **Notifications** settings using the table below.

Notifications Settings	Guidelines
Subject	Select the subjects for which notifications should be sent.
Recipients	Select the recipients whom notifications will be sent to by selecting the appropriate checkboxes.
Method	Select how notifications are sent.

f. Configure the **Auto Close** settings using the table below.

Auto Close Settings	Guidelines
Auto Close	The following options are available. • Do not close - Select this if you do not want any cases to automatically be closed if all related incidents have been cleared from a case. • Close after <#> <period of time> of all Incidents clearing - Select this to configure when a case will be automatically closed. In the first field, enter a number for the period of time required for a case to be closed if all incidents related to that case have been cleared. In the following drop-down list, select Minute(s) or Hour(s) to define the unit of time for automatic closure of a case if all related Incidents have been cleared. This allows you to add any related incidents that may come through to a case that will soon be closed.

g. When done, click **Save**.

Adding/Editing Case Close Codes

To create/edit a Case Close Code, take the following steps.

1. From **Admin > Settings > General > Case Management**, click the **Case Close Codes** tab.
2. If creating a new case close code, click **New**. If editing a case close code, select the case close code you wish to edit, and click **Edit**.

3. If you wish to make the Case Close Code available for use, click the **Enable** checkbox.
4. In the **Name** field, enter the Case Close Code name.
   Note: The **Name** field does not allow the "space" character, or the special characters "!, #, $, %, ^, &, *, (and)".
5. In the **Description** field, enter information about the Case Close Code.
6. Click **Save**.

Viewing Case Management Policy

If you navigate to the **Case Management** page, and click on the **Case Management Policy** tab, the Case Management Policy table appears. Information about the table follows.

Column	Description
Name	Name of the Case Management Policy
SLA & Escalation	The Service Level Agreement and Escalation Case Severity Types configuration
Auto-assignment	How cases are automatically assigned.
Permissions	Permissions in place for changing the state of a case, and who can edit notes.
Notifications	The Subject, Recipients and Method for notifications.
Auto Close	When automatic closure of a case occurs.

Viewing Case Close Codes

If you navigate to the **Case Management** page, and click on the **Case Close Codes** tab, the Case Close Codes table appears. Information about the table follows.

Column	Description
Enabled	If Enabled is checked, it means the Case Close Code is available and can be selected when closing a case.
Name	The Case Close Code name
Description	Information about the Case Close Code, typically describes how a case was closed.
Scope	A Case Close Code can be System or User. If the scope is displayed as System, it is a pre-defined Case Close Code, and cannot be edited. A scope defined as User, is a user created Case Close Code, and can be edited.

Applying Case Creation to Automation Policy

To associate a Case Management Policy to an Automation Policy, take the following steps.

1. In the **Case Management Policy** drop-down list, select the Case Management Policy you wish to apply.
2. From the **Teams: FIRST** drop-down list, select first team to be used in a case management policy.
3. Click on the **+** icon to add another team to be attached to the case management policy.
   Note: You can click the **-** icon to remove an existing team drop-down list option, but there must be at least one team configured.
4. In the **Teams: THEN** drop-down list, select the next FortiSIEM Analysts team that should be applied in the Case Management Policy.
5. Repeat steps 3-4 until you have configured all the teams that you wish to be part of the case management policy, then click **Save**.You will then be taken back to the **Automation Policy** window, where you can continue to configure your automation policy.

Configuring SSL Socket Certificates

Before the 6.0.0 release, the mechanism to communicate notifications between backend processes and the app server was through plain sockets. Beginning with the 6.0.0 release, these communications are performed by the safer SSL sockets.

Before starting to transport data through the SSL tunnel, certificates are used to authenticate endpoints. Certificate verification is important, because “man-in-the-middle” attacks can happen when certificate verification is not enabled.

SSL certificate verification is performed in two directions: the client verifies the server’s certificate and the server verifies the client’s certificate.

By default, certificate verification is disabled in both directions in FortiSIEM. This section describes how to configure certificate verification in FortiSIEM

Running the SSL Configuration Script

The `config-ssl-cert.sh` shell script does the work to configure SSL certificates correctly. This script performs the following tasks:

- Provides values for the SSL configuration attributes in the GLOBAL section of the `/opt/phoenix/config/phoenix_config.txt` file.
- Generates files, such as the certificate chain file, trust store, and key store.
- Restarts backend processes to apply the configuration.

To run the `config-ssl-cert.sh` shell script, follow these steps:

1. Log in to the system as user `root`.
2. Run the `config-ssl-cert.sh` shell script with the appropriate options for your environment. See Script Options and Script Examples.

Note:

- When running the script, use the absolute path for all files and directories.
- The script will back-up the existing `phoenix_config.txt` file and `cert_store`, before modifying it. You can restore the previous version if you need to.

Script Options

The following table describes the options that can be used with the `config-ssl-cert.sh` shell script.

Option	Description
-h	Display the help message of script.
-v <0|1|2|3>	Set certificate verify model. This is a required option, with following possible values. • **0**: Disable certificate verify at both directions • **1**: Enable only the verifying server's certificate. This means that the client will verify the certificate from server, but server will not require or verify the certificate from client. • **2**: Enable only the verifying client's certificate. This means that the server will require and verify certificate from client, but client will not verify the certificate from server • **3**: Enable certificate verification in both directions. This means that the client will verify the certificate from server, and server will require and verify the certificate from client.
-p	This option indicates whether the provided certificate is public. Public certificates are signed by a well-known CA organization. It should not be signed by a private CA, or by itself. This option is useful, because it indicates whether you need a CA for the certificate. As you know, if the certificate is public, then the ROOT CA for that certificate is always installed in the system by default. You do not have to provide one. However, if the certificate is private, then a private CA is required.
-c <Certificate file> -k <Key file>	The **-c** and **-k** options are used together to specify the Certificate File and corresponding Key file.
-a <CA file> -d <CA dir>	The CA is used to verify the certificate. The **-a** and **-d** options are used together to specify the CA file and the directory where it is stored. If the provided certificate is private, then the CA is required. If the provided certificate is public, then the CA is optional (typically, it is not needed).

-i <Intermediate CA chain file>	If the certificate is not signed by the ROOT CA directly (this is typically the case for public certificates), then there is a trust chain:
	`Certificate -> Intermediate CA1 -> Intermediate CA2 ->…-> Root CA`
	Use this option to provide the intermediate CA (`Intermediate CA`) chain. If there is only one intermediate CA, then that intermediate CA certificate can act as the intermediate CA chain file directly. If there is more than one intermediate CA, then you must create a chain file for them by using the `cat` command, for example:
	`cat IntermediateCA1 Intermediate CA2 … IntermediateCAn > IntermediateCAChain`

-s <cert_store>	You might need to generate some useful files, such as the trust store file and key store file. Use this option to specify where you want to store those files. By default, they will be stored in the `/opt/phoenix/config/cert_store` directory.
-r	Typically, you must restart backend processes to apply the configuration changes.

Option	Description

	Use this option, to instruct the script to restart the processes automatically.
	NOTE: because you are configuring the notification communicating mechanism, it might fail if you try to restart the backend processes using tools such as `phtools --stop` all or `monctl stop`.
	If you want to restart the backend processes manually, use following commands:
	`phstatus.py |grep ph |cut -d' ' -f1 |xargs killall -9`
	`monctl start`
	`phtools --start all`

Script Examples

- Disable Certificate Verification in Both Directions
- Enable Verification in Both Directions Using a Public Certificate
- Enable Verification in Both Directions with a Self-Signed Certificate

Disable Certificate Verification in Both Directions

This command disables verification in both directions:

```
config-ssl-cert.sh -v 0 –r
```

where:

- `-v 0` - disables verification in both directions.
- `-r` - restarts backend processes to apply the changes.

Enable Verification in Both Directions Using a Public Certificate

This command enables verification in both directions using a public certificate.

```
config-ssl-cert.sh -v 3 -p -c /opt/star_qa_fortisiem_fortinet_com.crt -k /opt/star_qa_
fortisiem_fortinet_com.key -i /opt/DigiCertCA.crt –r
```

where:

- `-v 3` - enables verification in both directions. You can change to `1` to verify only the server's certificate, or change to `2` to verify only the client's certificate.
- `-p` - specifies that the `-c` and `-k` options identify the <certificate, key> pair of a public certificate.
- `-i` – specifies that there is an intermediate CA for the certificate. This means that there is a trust chain here: `star_qa_fortisiem_fortinet_com.crt -> DigiCertCA.crt -> Root CA`.

Because this is a public certificate, the CA (`-a`) option is not required.

Enable Verification in Both Directions with a Self-Signed Certificate

This command enables verification in both directions using a self-signed certificate.

```
config-ssl-cert.sh -v 3 -c /etc/pki/tls/certs/localhost.crt -k
/etc/pki/tls/private/localhost.key -a /etc/pki/tls/certs/localhost.crt –r
```

where:

- The absence of the `-p` option indicates that the provided `-c` and `-k` options are specifying a private <certificate, key> pair.
- `-a` – specifies the CA file used to verify the certificate. This is the certificate itself, in the self-signed case.

Managing CMDB

FortiSIEM Configuration Management Database (CMDB) contains the following:

- Discovery information about your IT infrastructure such as devices, applications, and users.
- Information derived from your discovered infrastructure, including inter-device relationships such as the relationship of WLAN Access Points to Controller, and Virtual Machines to ESX Hosts.
- Information about system objects such as business services and CMDB reports.

The following topics provide more information about managing CMDB:

- Devices
- Applications
- Users
- Business Services
- CMDB Reports

Devices

You can add devices to the CMDB through the Discovering Infrastructure process. However, there may be situations in which you want to add devices to the CMDB manually. For example, you may not have access credentials for a device but still want to include network information about it so that logs received by FortiSIEM can be parsed properly.

These topics describe those situations and provide instructions for adding a device to the CMDB:

- Viewing Device Information
- Working with Device Groups
- Creating and Editing Devices
- Performing Operations on Devices
- Associating Parsers to a Device
- Searching for Devices

Viewing Device Information

To view device information, open the **CMDB** page and click **Devices** in the left panel. Expand **Devices** to see all of the subgroups belonging to it. Click **Devices**, or on one of its subgroups, to see the devices in the table associated with that group. The icons above the panel allow you to add, edit, and delete subgroups. System-defined subgroups cannot be deleted, but they can be edited. For more information on managing device groups, see Working with Device Groups.

The headings and numbers at the top of the page, such as above **Routers**, **Firewall**, **Windows**, and so on, represent the number of devices of that type that are active in FortiSIEM. Click the heading to see the devices associated with that device type.

The table on the right of the page displays a list of all of the devices known to FortiSIEM. The table contains columns such as Device **Name**, **IP** address, **Device Type**, **Status**, and so on.

On the **CMDB** page you can do the following:

- Choose which columns to display by clicking the **Columns** icon. For more information, see Changing Display Columns.
- Create, edit, and delete devices by clicking the **New**, **Edit**, and **Delete** buttons. See Creating and Editing Devices for more information.
- Filter the list of devices by organization by clicking the Filter ( ) icon, to the right of the **Delete** button.
  - Select from the various parameters, and in the "Search" field, enter a value to filter. When done, click the Apply (✓) icon.
  - To clear any filters, click the Clear (**X**) icon.
- Perform a variety of operations on a selected device by making a selection from the **Actions** drop-down list. For more information on the operations you can perform, see Performing Operations on Devices.
- Get more information about a device by clicking a device name, hovering over the device name, clicking ▼, selecting **Details**, and then clicking one of the buttons in the vertical side panel: **Summary**, **Properties**, **Monitor**, **Software**, **Hardware**, **Configuration**, **Relationships**, **Agent Template**, and **File**. The information returned is described in the following table.

Selection	Description
Summary	Click **Summary** to return general information about the device such as the **Name**, **Device Type**, **Importance**, **IP address**, and so on. It also displays information regarding the device's health, what group it is a member of, and various statistics (such as **Created**, **Last Discovered**, **Last Updated**, and so on.
Properties	Click **Properties** to view general device location information.
Monitor	Click **Monitor** to return tables describing the **Event Received Status** and **Monitor Status**.
Software	Click **Software** and make a selection from the drop-down list: **Installed Software**, **Running Applications**, **Windows Services**, or **Installed Patches** to get more detailed information. For **Installed Software**, you have the following options: • **Diff...** - Click to compare two selected files/revisions. **Note**: Use Ctrl-Click to select a second file. • **Delete** - Click to delete selected file(s). You will be prompted to confirm the deletion. **Note**: You can use Ctrl-Click and Shift-Click to select multiple files. • **Export** - Click to export selected files as a PDF report.
Hardware	Click **Hardware** and make a selection from the drop-down list: **Interfaces**, **Processes**, **Storage**, **SAN Storage**, **System BIOS**, **Components**, or **SAN Ports**.
Configuration	Click **Configuration** to view the existing configuration files for your router device. For **Configuration**, you have the following options: • **Diff...** - Click to compare two selected files/revisions. **Note**: Use Ctrl-Click to select a second file. • **Delete** - Click to delete selected file(s). You will be prompted to confirm the deletion. **Note**: You can use Ctrl-Click and Shift-Click to select multiple files. • **Export** - Click to export selected files as a PDF report.
Relationships	Click **Relationships** to return the device's **Node Name**, **Access IP**, **Version**, **Device Type**, and **Description**.
Agent Template	Click **Agent Template**, then **Apply** to add an existing Agent Template to an appropriate device.
File	Click **File** to view any version or content files from your Windows/Linux agent devices. You have the following options: • **Diff...** - Click to compare two selected files/revisions. **Note**: Use Ctrl-Click to select a second file. • **Delete** - Click to delete selected file(s). You will be prompted to confirm the deletion. **Note**: You can use Ctrl-Click and Shift-Click to select multiple files.

Working with Device Groups

This section provides the procedures to set up Device Groups.

- Adding Device Groups
- Modifying Device Groups
- Performing Operations on Device Groups
- Changing Display Columns

Adding Device Groups

Complete these steps to add device groups:

1. Go to **CMDB** and click **Devices** folder on the left panel.
2. Click **+** above the list of CMDB groups list.
3. In the **Create New Device Group** dialog box, enter/select the information below:

Settings	Guidelines
Scope	Select the organization from the drop-down list.
Group	[Required] Enter a name for the group.
Description	Enter a description of the device group.
Folders	Choose a folder under **Devices** to view items that reside in the selected folder.
Items in Current Folder	Displays the devices in the selected folder. Use the **|<**, **<**, **>** and **>|** buttons to page through the list of devices. Select the device(s) you want to include in the new group, and move to **Items in Group**.
Items in Group	Select devices from **Items in Current Folder** and move them to **Items in Group**. These devices will be the members of the new group.

4. Click **Save**.
   The new device group appears on the left panel.

Modifying Device Groups

Complete these steps to modify a Device Group:

1. Click **Devices** from the left panel and navigate to the device group.
2. Select the required change from the table below:

Settings	Guidelines
Edit	To modify any Device Group.
Delete	To delete any Device Group.

3. Click **Save**.

Performing Operations on Device Groups

You can perform a number of operations on devices or device groups by selecting the **Actions** drop-down list. For more information on these actions, see Performing Operations on Devices and Device Groups.

Changing Display Columns

Complete these steps to choose which columns appear in the device table.

1. Click the **Columns** icon.
2. Select the columns you want to display by adding a checkmark. Likewise, you can remove columns from the display by removing the checkmark from a column heading with a checkmark.

The table will display your chosen columns.

Creating and Editing Devices

Complete these steps to add a new device.

1. Click **CMDB** and select the device group under **Devices** on the left panel.
2. Click **New**.
3. In the **Add New Device** dialog box, enter the information under **Summary**, **Contact**, **Interfaces**, and **Properties** tabs.
4. Click **Save**.
   The new device appears in the list.
5. Hover over a device under the **Name** column, click ▼, and select **Details**. A sidebar appears with information under various tabs.
   Note: If you prefer to have the sidebar appear when a device is selected, select the **Display sidebar when selecting CMDB entry** checkbox option from the sidebar.

Complete these steps to edit a device:

1. Go to **CMDB** tab.
2. From the left panel, select the device type under **Devices** folder.
3. Select the Device from the list displayed on the table and click **Edit**.
4. In the **Edit Device** dialog box, modify the settings under **Summary**, **Contact**, **Interfaces**, **Properties** and **Parser** tabs.
5. Click **Save**.

Performing Operations on Devices and Device Groups

You can perform various operations on individual devices or device groups by selecting the device or device group and clicking the **Actions** drop-down list. The following table describes the operations you can perform.

Action Settings	Function Description
Details	Displays detailed information about the device. Various tabs provide additional information (Summary, Properties, Monitor, Software, Hardware, Advanced).
Quick Info	Displays the a summary of information about the device. The information can include the Device Name, Access IP, Device Type , Version, and so on.
Device Health	Displays Availability Status, Performance Status, and a variety of health reports for the device, such as Monitor Status, Incident Status, and so on. Click the **<** and **>** buttons to move through additional health information.
Vulnerabilities	By default, displays the top 10 vulnerabilities of the past week. You can also choose a time interval of 15 minutes, 1 hour, one day, or 30 days.
Incidents	Displays the summary of incidents associated with the device. Click an incident and open the **Action** drop-down list to drill down on the incident for more information.
Risk	Displays incidents information under **INCIDENTS > Risk** tab.
Real-time Events	Opens a Real Time Search window for events for the selected device. For more information, see Viewing Real-time Search Results.
Historical Events	Displays the historical events under **ANALYTICS** tab. Use **Actions** tab on top-left corner to email, export, copy to a new tab or save results. For more information, see Viewing Historical Search Results.
Real-time Performance	Displays the real-time Performance Metrics of the selected device. You can choose a **Monitor**, and **Collector** from the drop-down lists, and set the polling **Frequency** and the number of **Runs**.
Impacted Business Services	Displays the Business services that contain the selected device.
Change Status	Changes the status of the device to **Approved** or **Unmanaged**. The devices under license are called 'Managed' while the remaining devices are called "Unmanaged".
Edit Location	Changes the device location address: Country, State, City, Latitude, Longitude, Region, Building and Floor.
Change Organization	Changes the organization in the **New Organization** drop-down list.
Impacted Organization	Select the **Impacted Orgs** from the drop-down list.
Decommission	Decommissions the selected device. Enter a reason in the Decommission Device dialog box.
Recommission	Recommissions the selected device.
Connect To	Connects to a specific Protocol or Port. Select a **Protocol** from the drop-down list and enter a **Port** number and **User** name. A Secure Shell plugin is required.

Action Settings	Function Description
	Note:If you have upgraded or performed a fresh install of FortiSIEM 6.3.0 or later, and attempt to connect via a tunnel, it will appear that the tunnel is opened. However, the displayed Supervisor's port on which the tunneled connection is running is actually not open so you will not be able to connect either via plugin or directly. To re-enable open tunnels, follow the steps in Open Tunnel Re-Configuration Required after 6.3.0 or later Upgrade/Fresh Install. Tunnels are closed by default to address bug 602294: CVE-2004-1653 SSH port forwarding exposes unprotected internal services.
Re-Discover	Specify the **Range Definition** information to rediscover the device. For a description of the options in the Discovery Definition dialog box, see the table in Creating a discovery entry.
Add to WatchList	Add the device to Watchlist. In the Add to Watch List dialog, select the **Attribute**, **Organization**, and **Expires** on time. Make selections from the list using the **>** button.
Enable Agent	Enables Agent monitoring for the selected device.
Disable Agent	Disables Agent monitoring for the selected device.
Run Live Osquery	Run an Osquery on device. **Note**: Must have Windows Agent on device.

Associating Parsers to a Device

You can attach a set of parsers to a device in CMDB. This overrides the default parser selection mechanism based on the Event Format Recognizer. When a device with a list of attached parsers sends a log, the specified parsers are attempted first.

1. Go to **CMDB** tab.
2. From the left panel, select the device(s) under **Devices** folder.
3. Click **Edit** and select the **Parsers** tab.
4. Select the parsers from the **Available Parsers** list and move to the **Selected Parsers** list using the right arrow.
   You can use the up and down arrows to re-arrange the order of the parsers. Note that the parsers will be attempted in order.
5. Click **Save** to confirm the parser selection.
   The selected parsers are now associated to the device.

Searching for Devices

FortiSIEM allows you to search for CMDB devices based on system device properties and custom device properties.

Note: For custom properties to appear in the search list, you must first select them in **ADMIN > Device Support > Custom Properties**. To select and define custom properties, see Working with Custom Properties.

1. Go to **CMDB > Devices**.
2. Click the **Search** icon.
3. Select the value(s) you want to search for:
   - In the drop-down list, click a device attribute (for example, **Device Type**). All possible values of the selected attribute (for example, Cent OS, VMware, Cisco, and so on) are displayed with a count next to it. You can select multiple attributes and values in the drop-down list. The results will be ANDed together.
   - If you need to search for a column or an attribute value, enter it in the **Search** field.
4. Click **Apply** at the top of the drop-down list.
   The top 5 items are returned. Click **Show All** to display all of the returned items.
5. The CMDB device list updates based on your search criteria.
6. To refine your search, click the **Search** icon again and select other CMDB device attributes or click **X** to cancel a selection.

Applications

Applications in the CMDB are grouped at the highest level by Infrastructure and User apps, with further sub-categorization in each of those two categories.

- Viewing Application Information
- Editing Applications
- Working with Application Groups

Viewing Application Information

To view application information, open the **CMDB** page and click **Applications** in the left panel. Expand **Applications** to see all of the subgroups belonging to it. Click **Applications**, or on one of its subgroups, to see the applications in the table associated with that group. The icons above the panel allow you to add, edit, and delete subgroups. System-defined subgroups cannot be deleted nor edited. For more information on managing application groups, see Working with Application Groups. To add an application, see Adding an Application.

The headings and numbers at the top of the page represent the number of application processes that are running for a application group/sub-group. Click the heading to see the application/processes associated with the application group.

The table on the right of the page displays a list of all of the applications known to FortiSIEM. The table contains columns such as the **App Group**, **App Name**, **Process**, and so on.

On the **CMDB** page you can do the following:

- Create, edit, and delete applications by clicking the **New**, **Edit**, and **Delete** buttons.
- Get more information about an application by hovering over **App Name**, clicking ▼, and selecting **Details**. A sidebar will appear with the following tabs: **Summary** and **Running On**.

Tab	Description
Summary	The Summary tab provides the name of the application, the number of processes the application is running, and the names of the processes.
Running On	Provides Access IP, Device Name, Process Name, Path, Service, and Status information if available.

Adding an Application

Complete these steps to add an application:

1. Click **CMDB** and select the application group under **Applications** on the left panel.
2. Click **New**.
3. In the **Add New Application** dialog box, enter the information related to the Application.
4. To add an IP to the Application, click the edit icon near **Running on**.
   a. Click **Add by IP** and enter the IP in the search box.
   b. Click the tick mark.
5. Click **Save**.
   The new application appears in the list.

Editing Applications

Complete these steps to edit an application:

1. From the left panel tree, select the application group under **Applications**.
2. Select the Application from the list and click **Edit**.
3. In the **Edit Application** dialog box, modify the settings.
4. To modify an IP, click the edit icon near **Running on** and select the IP.
   - Click **Add by IP** to add a new IP.
   - Click **Delete** to delete the IP.
5. Click **Save**.

Working with Application Groups

This section provides the procedures to set up Application Groups.

- Adding Application Groups
- Modifying Application Groups

Adding Application Groups

Complete these steps to add Application groups:

1. Go to **CMDB** and click Applications folder on the left panel.
2. Click + above the list of CMDB groups list.
3. In the Create New application Group dialog box, enter/select the information below:

Settings	Guidelines
Scope/Organization	Select the Organization.
Group	[Required] Group name.
Description	Description about the application group.
Folders	Select a folder under Applications to see items contained in that folder. The items from that folder appear under the Items in Current Folder. Items can be selected and moved using < and >.
Items	Items to add under the application group.
Selections	Click > to confirm the selections from Folders and Items.

4. Click Save.
   The new application group appears on the left panel.

Modifying Application Groups

Complete these steps to modify an Application Group:

1. Click Applications from the left panel and navigate to the Application group.
2. Use the delete, edit or move icon above the application groups list for the required modification.
3. Click Save.

Users

FortiSIEM CMDB Users page contains information about the users of your system.

In versions earlier than 7.2.0, the default **FortiSIEM Users** group/folder included FortiSIEM Users with the Admin role. Now, all FortiSIEM users with access via the GUI are automatically populated in this folder/group. A new group, **FortiSIEM Analysts**, is a container for all users involved with case management. Add your case management group(s)/folder(s) under **FortiSIEM Analysts**, then create your case management users in these case management groups/folders.

- Viewing User Information
- Adding Users
- Editing User Information
- Performing Operations on Users
- Working with User Groups

Viewing User Information

To view user information, open the **CMDB** page and click **Users** in the left panel. Expand **Users** to see all of the subgroups belonging to it. Click **Users**, or on one of its subgroups, to see the users in the table associated with that group. The icons above the panel allow you to add, edit, and delete subgroups. System-defined subgroups cannot be deleted. Some system-defined subgroups, such as **FortiSIEM Users**, can be edited. For more information on managing device groups, see Working with User Groups.

The headings and numbers at the top of the page, such as above **FortiSIEM Users**, or a manually created user group name, represent the number of existing FortiSIEM users. Click the heading to see the users/groups associated with the user category.

The table on the right of the page displays a list of all of the users known to FortiSIEM. The table contains columns such as the **User Name**, **Full Name**, **Organization**, **FortiSIEM Role**, and so on.

On the **CMDB** page you can do the following:

- Choose which columns to display by clicking the **Columns** icon.
- Create, edit, and delete users by clicking the **New**, **Edit**, and **Delete** buttons.
- Perform a variety of operations on a selected user by making a selection from the **Actions** drop-down list. For more information on the operations you can perform, see Performing Operations on Users.
- Get more information about a user by hovering over a user under the **User Name** column, clicking ▼, and selecting **Details**. A sidebar will appear with the following tabs: **General**, **Contact**, **Member Of**, and **Access Control**. The information returned is described in the following table.

Selection	Description
General	Click **General** to return general information about the user such as the **User Name** and **Last Domain Logon**. It also displays information regarding domain password time, their FortiSIEM role, and existing user configuration policies (password reset, idle timeout, user lockout).
Contact	Click **Contact** to view available user contact information, such as email, phone numbers and physical address.
Member Of	Click **Member Of** to see all the groups that the user is a member of.
Access Control	Click **Access Control** to see what restrictions the user has.

Adding Users

The following section describes how to add users to FortiSIEM CMDB. Once an user is defined, you can do the following functions:

- Allow the user to log in to FortiSIEM GUI
- Allow the user to receive FortiSIEM notification
- Use the users in Analytics (Rules and Reports)

You can add users in one of the following ways:

- Add Users Manually
- Discover Users from Microsoft Active Directory
- Discover Users from OKTA

See Implementation Notes for additional information.

Add Users Manually

Complete these steps to add a user:

1. Navigate to **CMDB > Users**.
2. Select a Users Folder/Group with new user creation permission, such as **FortiSIEM Users**, and click **New** to create a new user.
3. Click on the **General** tab.
   a. Add the user profile information in the **User Name**, **Full Name**, **Job Title** and **Company** fields.
   b. Click the **Importance** drop-down list to select the importance of this user - "Normal", "Important", "Critical", or "Mission Critical".
   c. Enable **Active** if this is an active user.
   d. Enter the user's **Domain**.
   e. Enter the user's Distinguished Name **DN**.
   f. Enter the **Employee ID** of the user.
   g. Select the **Manager** to which this user belongs.
   h. Click **Alias** to enter any alias information for the user.
      i. In the **Alias** field, provide the alias user name.
      ii. From the **Identity Provider** field, enter/select from AWS IAM, DUO, or Microsoft AD.
      iii. In the **Description** field, enter any additional information about the alias.
      iv. If another Alias is needed, in the **Row** column, click **+** to add another row for another alias, and repeat steps i-iii.
      v. Click **Save** when done.
   i. Click the **Team Lead** checkbox to define a user as a Team Lead for Case Management.
   Note: This option is only available for users created under **FortiSIEM Analysts** Group.
   j. Enter any **Description** about the user.

4. Click on the **Contact** tab.
   a. Add user contact information to the appropriate contact information fields - **Work Phone**, **Mobile Phone**, **Home Phone**, **SMS**, **SMS Provider**, **ZIP**, **Email**, **Address**, **City**, **State**, and **Country** field.
   b. If your company uses S/MIME for email, make sure the **Email** field is filled out, and upload the S/MIME certificate in the **Certificate** field by clicking **Upload**, and selecting your certificate.
   c. Click **Save** when done.
5. Click on the **FortiSIEM Attributes** tab.
   a. For **User Unlock**, select **Unlock by Administrator** or **Delay next login for ## minutes**. If **Delay next login for ## minutes** is selected, enter the number of minutes the user will be unable to log into the system after five successive authentication failures.
   b. For **Idle Timeout**, enter the number of minutes after which an inactive user will be logged out.
   c. For **Password Reset**, enter the number of days after which a user's current password for logging in to the system will automatically expire. If left blank, the user's password will never expire.
   d. For **FortiSIEM Role**, enable by selecting the **FortiSIEM Role** checkbox.
      i. For **Mode**, select **Local** or **External**.
      If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
      Notes:
      - If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
      - For local users, passwords must contain between 8 and 64 characters, and must include 1 letter, 1 numeric character and 1 special character.

      ii. Select a **Default Role** for the user.
      See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.

      If this **FortiSIEM Role** user should be allowed to approve de-anonymization requests, ensure the **Deobfuscation Approver** role has been configured in Role Settings and that this configured role is selected here.

      If the **FortiSIEM Role** user should be allowed to approve remediation requests, ensure the **Remediation Approver** role has been configured in Role Settings and that this configured role is selected here.

      For Case Management, FortiSIEM recommends choosing **Full Admin** to get the permissions needed to handle any case.

      iii. Click **Save** when done.
   e. Click on **Work Schedule** to configure the user's work schedule.
   Note: This option is only available for users created under **FortiSIEM Analysts** Group.
      i. Under **Time Range**, enter the **Start Time**, **End Time**, and select the **Time Zone** from the **Time** and **Region** drop-down lists.

ii. Under **Recurrence Pattern**, select **Recurring Days**, then select the **Repeat Days** and **Repeat Months**, or select **Recurring Dates**, followed by selecting the **Repeat Dates**, and **Repeat Months**.

iii. Under **Recurrence Range**, click on the **Start From** field, and select the start date. Next, select **No end date** or **End By**. If **End By** is selected, click on the **End By** field, and select the end date.

iv. Click **Save** when done.

f. Click on **Time Off Schedule** to configure when a user plans to be off work.
Notes:
This option is only available for users created under **FortiSIEM Analysts** Group.
When you configure Time Off, you should only select the period of time that will be taken off from the work schedule, i.e., if a user works from 8:00am-5:00pm, then the time off period should be 8:00am-5:00pm.

i. Under **Time Range**, enter the **Start Time**, **End Time**, and select the **Time Zone** from the **Time** and **Region** drop-down lists.

ii. Under **Recurrence Pattern**, select **Recurring Days**, then select the **Repeat Days** and **Repeat Months**, or select **Recurring Dates**, followed by selecting the **Repeat Dates**, and **Repeat Months**.

iii. Under **Recurrence Range**, click on the **Start From** field, and select the start date. Next, select **No end date** or **End By**. If **End By** is selected, click on the **End By** field, and select the end date.

iv. Click **Save** when done.

g. Click **Save** when done.

Discover Users from Microsoft Active Directory

- Step 1: Create LDAP Login Credentials and Associate with LDAP Server IP Address
- Step 2: Discover Active Directory Server and Users
- Step 3: Set FortiSIEM Attributes for Users

Step 1: Create LDAP Login Credentials and Associate with LDAP Server IP Address

1. Log in to your Supervisor node.
2. Go to **ADMIN** > **Setup** > **Credentials**.
3. Click **New**.
4. Enter a **Name**.
5. For **Device Type**, select **Microsoft Windows**.
6. Select your **Access Protocol.**
FortiSIEM supports these LDAP protocols:

Protocol	Settings
LDAP	[Required] IP Host - Access IP for LDAP Port - Non-secure version on port 389
LDAPS	[Required] IP Host - Access IP for LDAPS Port - Secure version on port 636
LDAP Start TLS	[Required] IP Host - Access IP for LDAP Start TLS Port - Secure version on port 389

7. For **Used For**, select **Microsoft Active Directory**.
8. For **Base DN**, enter the root of the LDAP user tree.
9. Enter the **NetBIOS/Domain** for your LDAP directory.
10. Enter the **User Name** for your LDAP directory.
    For user discovery from OpenLDAP, specify the full DN as the user name. For Active Directory, use your server login name.
11. Enter and confirm the **Password** for your **User Name**.
12. Click **Save**.
    Your LDAP credentials will be added to the list of **Credentials**.
13. Under **Enter IP Range to Credential Associations**, click **Add**.
14. Select your LDAP credentials from the list of **Credentials**. Click **+** to add more.
15. Enter the **IP/IP Range** or host name for your Active Directory server.
16. Click **Save**.
    Your LDAP credentials will appear in the list of credential/IP address associations.
17. Click **Test** > **Test Connectivity** to make sure you can connect to the Active Directory server.

Step 2: Discover Active Directory Server and Users

1. Go to **ADMIN** > **Setup** > **Discovery**.
2. Click **New**.
3. For **Name**, enter **Active Directory**.
4. For **Include Range**, enter the IP address or host name for your Active Directory server.
5. Leave all the default settings, but clear the **Discover Routes** under **Options**.
6. Click **OK**.
   Active Directory will be added to the list of discoverable devices.
7. Select the Active Directory device and click **Discover**.
8. After discovery completes, go to **CMDB > Users** to view the discovered users.
   You may need to click **Refresh** for the user tree hierarchy to load.

Step 3: Set FortiSIEM Attributes for Users

1. From the **CMDB > Users** page, select the user, and click **Edit**.
2. From the **Manager** drop-down list, select the Manager which this user belongs.

3. For **System Admin**, enable by selecting the System Admin checkbox.
   a. For **Mode**, select **Local** or **External**.
   If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
   Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
   b. Select a **Default Role** for the user.
   See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.
4. Click **Save**.

Discover Users from OKTA

- Step 1: Prepare OKTA for Authentication
- Step 2: Create an OKTA API Token
- Step 3: Create OKTA Login Credentials in FortiSIEM and Associate with OKTA Server
- Step 4: Discover OKTA Users
- Step 5: Set FortiSIEM Attributes for Users

Step 1: Prepare OKTA for Authentication

To use Okta authentication for your FortiSIEM deployment, you must set up a SAML 2.0 Application in Okta, and then use the certificate associated with that application when you configure external authentication.

1. Log into Okta.
2. In the **Applications** tab, create a new application using **Template SAML 2.0 App**.

3. Under **Settings**, configure the settings similar to the table below:

Post Back URL	Post Back URL
Application label	FortiSIEM Demo
Force Authentication	Enable
Post Back URL	https://<FortiSIEMIP>/phoenix/okta
Name ID Format	EmailAddress
Recipient	FortiSIEM
Audience Restriction	Super
authnContextClassRef	PasswordProtectedTransport
Response	Signed
Assertion	Signed
Request	Uncompressed
Destination	https://<FortiSIEMIP>/phoenix/okta

4. Click **Save**.
5. In the **Sign On** tab, click **View Setup Instructions**.
6. Click **Download Certificate**.
7. Follow the instructions above and enter the downloaded certificate for Okta authentication.

Step 2: Create an OKTA API Token

1. Log in to Okta using your Okta credentials.
2. Got to **Administration** > **Security** > **API Tokens**.
3. Click **Create Token**.
   You will use this token when you set up the Okta login credentials in the next section. Note that this token will have the same permissions as the person who generated it.

Step 3: Create OKTA Login Credentials in FortiSIEM and Associate with OKTA Server

1. Log in to your Supervisor node.
2. Go to **ADMIN** > **Setup** > **Credentials**.
3. Click **New**.
4. Enter a **Name**.
5. For **Device Type**, select **OKTA.com OKTA**.
6. For **Access Protocol**, select **OKTA API**.
7. Enter the **Pull Interval** in minutes.

8. Enter the **Domain** associated with your Okta account.
   For example, `FortiSIEM.okta.com`.
9. Enter and reconfirm the **Security Token** you created.
10. Enter any related information in **Description**.
11. Click **Save**.
    Your Okta credentials will be added to the list of **Credentials**.
12. Under **Enter IP Range to Credential Associations**, click **New**.
13. Enter the **IP/IP range** or host name for your Okta account.
14. Select your Okta credentials from the list of **Credentials**. Click **+** to add more.
15. Click **Save**.
    Your Okta credentials will appear in the list of credential/IP address associations.
16. Click **Test** > **Test Connectivity** to make sure you can connect to the Okta server.

Step 4: Discover OKTA Users

If the number of users is less than 200, then Test Connectivity will discover all the users. Okta API has some restrictions that do not allow FortiSIEM to pull more than 200 users. In this case, follow these steps:

1. Log in to **Okta**.
2. Download user list CSV file (OktaPasswordHealth.csv) by visiting **Admin** > **Reports** > **Okta Password Health**.
3. Rename the CSV file to `all_user_list_%s.csv`. (`%s` is the placeholder of token obtained in Create an Okta API Token - Step 3, e.g. `all_user_list_00UbCrgrU9b1Uab0cHCuup-5h-6Hi9ItokVDH8nRRT.csv`).
4. Log in to **FortiSIEM Supervisor node**:
   a. Upload CSV file `all_user_list_%s.csv` to this directory `/opt/phoenix/config/okta/`
   b. Make sure the permissions are `admin` and `admin` (Run `chown -R admin:admin /opt/phoenix/config/okta/`)
   c. Go to **ADMIN > Setup > Credentials > Enter IP Range to Credential Associations**.
   d. Select the Okta entry and run **Test** > **Test connectivity** to import all users.

Step 5: Set FortiSIEM Attributes for Users

1. From the **CMDB > Users** page, select the user, and click **Edit**.
2. From the **Manager** drop-down list, select the Manager which this user belongs.
3. For **System Admin**, enable by selecting the System Admin checkbox.
   a. For **Mode**, select **Local** or **External**.
   If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
   Note: If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.

   b. Select a **Default Role** for the user.
      See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.
4. Click **Save**.

Implementation Notes

- For Service Provider deployments:
  - If you add users as a Super/Global admin, then the added users will be in the Super/Global group.
  - If you login to a specific Organization and create users there, then the users will belong to that Organization.
- When viewing this user list as a Super global user, you may see repetitions of a few **User Names**, where those names exist in multiple Organizations. This can be determined by checking the contents of the **Organization** column.
- Repetition of **User Names** may also occur if an LDAP server has moved from one Organization to another and discovery of that LDAP server introduces users from the previous organization who may share the same user name. In this case, the administrator may wish to remove users that are no longer applicable.
- An Agent User can be created by navigating to **ADMIN > Setup > Organization**, and clicking **New** or **Edit**. These types of Admin Users are not allowed to log into the UI. Their primary purpose is for Windows and Linux Agent registration against the FortiSIEM environment. See Setting Organizations and Collectors (Service Provider) for more information.

Editing User Information

Complete these steps to edit a CMDB user:

1. Navigate to **CMDB > Users**.
2. Select a User, and click **Edit**.
3. Click on the **General** tab.
   a. Change the user profile information in the **User Name**, **Full Name**, **Job Title** and **Company** fields, if needed.
   b. Click the **Importance** drop-down list to select the importance of this user - "Normal", "Important", "Critical", or "Mission Critical".
   c. Enable **Active** if this is an active user.
   d. Update the user's **Domain**.
   e. Update the user's Distinguished Name **DN**.
   f. Update the **Employee ID** of the user.
   g. Select the **Manager** to which this user belongs.
   h. Click **Alias** to update any alias information for the user.
      i. In the **Alias** field, provide the alias user name.
      ii. From the **Identity Provider** field, enter/select from AWS IAM, DUO, or Microsoft AD.
      iii. In the **Description** field, enter any additional information about the alias.
      iv. If another Alias is needed, in the **Row** column, click **+** to add another row for another alias, and repeat steps i-iii.
      v. Click **Save** when done.
   i. Click the **Team Lead** checkbox to define a user as a Team Lead for Case Management.
   Note: This option is only available for users created under **FortiSIEM Analysts** Group.
   j. Update any **Description** about the user.
4. Click on the **Contact** tab.
   a. Update user contact information to the appropriate contact information fields - **Work Phone**, **Mobile Phone**, **Home Phone**, **SMS**, **SMS Provider**, **ZIP**, **Email**, **Address**, **City**, **State**, and **Country** field.
   b. If your company uses S/MIME for email, make sure the **Email** field is filled out, and upload the S/MIME certificate in the **Certificate** field by clicking **Upload**, and selecting your certificate.
   c. Click **Save** when done.
5. Click on the **FortiSIEM Attributes** tab.
   a. For **User Unlock**, select **Unlock by Administrator** or **Delay next login for ## minutes**. If **Delay next login for ## minutes** is selected, enter the number of minutes the user will be unable to log into the system after five successive authentication failures.
   b. For **Idle Timeout**, enter the number of minutes after which an inactive user will be logged out.
   Note: By design, this is currently disabled, and cannot be edited.
   c. For **Password Reset**, enter the number of days after which a user's current password for logging in to the system will automatically expire. If left blank, the user's password will never expire.

d. For **FortiSIEM Role**, enable by selecting the **FortiSIEM Role** checkbox.

i. For **Mode**, select **Local** or **External**.
If you select **Local**, enter and then reconfirm the user password. For **External**, see Authentication Settings for more information about using external authentication.
Notes:

- If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
- For local users, passwords must contain between 8 and 64 characters, and must include 1 letter, 1 numeric character and 1 special character.

ii. Select a **Default Role** for the user.
See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.

If this **FortiSIEM Role** user should be allowed to approve de-anonymization requests, ensure the **Deobfuscation Approver** role has been configured in Role Settings and that this configured role is selected here.

If the **FortiSIEM Role** user should be allowed to approve remediation requests, ensure the **Remediation Approver** role has been configured in Role Settings and that this configured role is selected here.

For Case Management, FortiSIEM recommends choosing **Full Admin** to get the permissions needed to handle any case.

iii. Click **Save** when done.

e. Click on **Work Schedule** to configure the user's work schedule.
Note: This option is only available for users created under **FortiSIEM Analysts** Group.

i. Under **Time Range**, enter the **Start Time**, **End Time**, and select the **Time Zone** from the **Time** and **Region** drop-down lists.

ii. Under **Recurrence Pattern**, select **Recurring Days**, then select the **Repeat Days** and **Repeat Months**, or select **Recurring Dates**, followed by selecting the **Repeat Dates**, and **Repeat Months**.

iii. Under **Recurrence Range**, click on the **Start From** field, and select the start date. Next, select **No end date** or **End By**. If **End By** is selected, click on the **End By** field, and select the end date.
Click **Save** when done.

f. Click on **Time Off Schedule** to configure when a user plans to be off work.
Notes:
This option is only available for users created under **FortiSIEM Analysts** Group.
When you configure Time Off, you should only select the period of time that will be taken off from the work schedule, i.e., if a user works from 8:00am-5:00pm, then the time off period should be 8:00am-5:00pm.

i. Under **Time Range**, enter the **Start Time**, **End Time**, and select the **Time Zone** from the **Time** and **Region** drop-down lists.

ii. Under **Recurrence Pattern**, select **Recurring Days**, then select the **Repeat Days** and **Repeat Months**, or select **Recurring Dates**, followed by selecting the **Repeat Dates**, and **Repeat Months**.

iii. Under **Recurrence Range**, click on the **Start From** field, and select the start date. Next, select **No end date** or **End By**. If **End By** is selected, click on the **End By** field, and select the end date.

iv. Click **Save** when done.

g. Click **Save** when done.

Performing Operations on Users

You can perform various operations on an individual user by selecting the user and clicking the **Actions** drop-down list. The following table describes the operations you can perform.

Action Settings	Function Description
Details	Opens a vertical side pane with access to **General**, **Contact**, **Member Of**, and **Access Control** tabs for the selected user. • **General** - Provides general user information, including last domain logon, last time domain password ws set, domain password age, whether use is system administrator, the user's FortiSIEM role, password reset information, idle timeout information, and user lockout time. • **Contact** - User contact information, such as email and phone number. • **Member Of** - Lists all groups that the user is a member of. • **Access Control** - Lists all user restrictions. **Note**: Vertical side pane is also available by clicking ▼then clicking **Details** while hovering over a user name.
Unlock	To unlock a user, select the user from the list and click **Actions** >**Unlock**.
Add to WatchList	Select the user from the list and click **Actions** > **Add to WatchList**. In the **Add to Watch List** dialog, select the **Organization** and **Expires on** time. Make the selections from the list using the **>** button and click **Save** to save.
Risk	To view a risk summary of a user, click **Actions > Risk**.

Working with User Groups

This section provides the procedures to set up User Groups.

- Adding User Groups
  - Adding a FortiSIEM Analyst Team
- Modifying User Groups

Adding User Groups

Complete these steps to add User groups:

1. Go to **CMDB** and click the **Users** folder on the left panel.
2. Click **+** above the list of CMDB groups.
3. In the **Create New User Group** dialog box, provide the following information:

Settings	Guidelines
Scope	Select the Organization.
Group	[Required] Group name.
Description	Description about the User group.
Folders	Select a Folder to view the **Users** that are under that folder/group. The users that are part of the selected folder appear under **Items in Current Folder**.
Items in Current Folder	Items from the selected Folder can be moved to **Items in Group** by selecting an items and clicking **>**.
Items in Group	Items that appear under Items in Group will be part of the new folder/group when you click **Save**.

4. Click **Save**.
   The new User group appears on the left panel.

Adding a FortiSIEM Analyst Team

To add a FortiSIEM Analyst Team, add this user group under **FortiSIEM Analysts** by taking the following steps.

1. Navigate to **CMDB**.
2. From the left pane, click **Users**, and select **FortiSIEM Analysts**.

3. Click **+** from the left pane.
4. From the **Create New User Group** dialog box, in the **Group** field, enter the FortiSIEM Analyst Team name and add any additional information (See Adding User Groups for details).
5. Click **Save**.

After your FortiSIEM Analyst Team has been created, you can add FortiSIEM Analyst users, including a Team Lead to the team. For more information on adding users, see here.

Modifying User Groups

Complete these steps to modify a User Group:

1. Click **Users** from the left panel and navigate to the User group.
2. Use the delete, edit or move icon above the User groups list for the required modification.
3. Click **Save**.

Business Services

A business service lets you view FortiSIEM metrics and prioritize alerts from a business service perspective. A business service is defined within FortiSIEM as a smart container of relevant devices and applications serving a business purpose. Once defined, all monitoring and analysis can be presented from a business service perspective. It is possible to track service level metrics, efficiently respond to incidents on a prioritized basis, record business impact, and provide business intelligence on IT best practices, compliance reporting, and IT service improvement. What is also novel about FortiSIEM is how easily a business service can be defined and maintained. Because FortiSIEM automatically discovers the applications running on the servers as well as the network connectivity and the traffic flow, you can simply choose the applications and respective servers and be intelligently guided to choose the rest of components of the business service. This business service discovery and definition capability in FortiSIEM completely automates a process that would normally take many people and considerable effort to complete and maintain.

Defining an IT or Business Service can create a logical grouping of devices and IT components which can be monitored together.

- Viewing Business Services
- Creating Business Services
- Working with Business Service Groups

Viewing Business Services

Complete these steps to view Business Services:

1. Go to **CMDB** and select a service under Business Services in the left panel.
   The services are: IT Srvc, Biz Srvc, Compliance, or Ungrouped.
2. Select the service from the list.
   The lower panel displays the information about the service including the following details: Type, Name, Running on, Access IP, Details, and Maintenance.

Creating Business Services

Complete these steps to create a Business Service:

1. Go to **CMDB** and select a service under Business Services in the left panel.
2. Click **New**.

3. In the New Business Service dialog box, enter the following information.

Settings	Guidelines
Name	Name of the Business Service group.
Description	Description about the Business Service group.
Filter	Use this function to filter out devices from the existing Selected Devices list of the given Business Service. This filter is applied to inline reports.
Devices	Browse this folder to select or search the devices and also the adjacent network devices. Click > to move the device selections to the Selected Devices/Apps table.
Applications	Browse this folder to select or search the applications, instance running on and adjacent network devices. Click > to move the application selections to the Selected Devices/Apps table.

4. Click Save to save the selections or Apply Filter and Save to proceed with adding the service.

You can use the links in the drilldown menu on the Business Services Summary Dashboard to find out more information about incidents, device availability, device and application performance, interface and event status, and real-time and historical search for a selected business service.

Working with Business Service Groups

This section provides the procedures to set up Business Service Groups.

- Adding Business Service Groups
- Modifying Business Service Groups

Adding Business Service Groups

Complete these steps to add Business Service groups:

1. Go to **CMDB** and click Business Services folder on the left panel.
2. Click + above the list of CMDB groups list.
3. In the Create New Business Service Group dialog box, enter/select the information below:

Settings	Guidelines
Organization	Select the Organization.
Group	[Required] Group name.
Description	Description about the Business Service group.
Folders	Folder under Business Service where the group has to be created.
Items	Items to add under the Business Service group.
Selections	Click > to confirm the selections from Folders and Items.

4. Click Save.
   The new Business Service group appears on the left panel.

Modifying Business Service Groups

Complete these steps to modify a Business Service Group:

1. Click Business Services from the left panel and select a Business Service group.
2. Click the required option:
   - Edit to modify the settings of a Business Service.
   - Delete to remove a Business Service.

3. Click Save.

CMDB Reports

You can find all system-defined reports under **CMDB** > **CMDB Reports**. The reports are organized into folders as shown on the left tree. Click a report to view Summary and Schedule information. the report conditions, and the columns included in the report.

CMDB Report Folder	Object to Report On	Report Name
Overall	Device Approval Status	• Approved Devices • Not Approved Devices
	Users	• Discovered Users • Externally Authenticated FortiSIEM Users • Locally Authenticated FortiSIEM Users • Manually Defined Users
	Rules	• Active Rules • Rules with Exceptions
	Reports	• Scheduled Reports
	Performance Monitors	• Active Performance Monitors
	Task	• All Existing Tasks
	Business Service	• Business Service Membership
Network	Inventory	• Network Device Components with Serial Number • Network Interface Report • Router/Switch Inventory • Router/Switch Image Distribution
	Ports	• Network Open Ports
	Relationship	• WLAN-AP Relationship
Server	Inventory	• Server Inventory • Server OS Distribution • Server Hardware: Processor • Server Hardware: Memory and Storage
	Ports	• Server Open Ports
	Running Services	• Windows Auto Running Services • Windows Auto Stopped Services • Windows Exchange Running Services • Windows IIS Running Services • Windows Manual Running Services • Windows Manual Stopped Services • Windows SNMP Running Services • Windows VNC Running Services • Windows WMI Running Services

CMDB Report Folder	Object to Report On	Report Name
	Installed Software / Patches	• Windows Installed Software • Windows Installed Patches • Windows Installed Software Distribution
Virtualization	Relationship	• VM-ESX Relationship
Beaconing		• CMDB Device Types • CMDB Network Device Count • CMDB Server Count • CMDB Storage Device Count • PING Monitored Device Count • Performance Monitor Status
FortiCare		• FortiCare 360 Device Inventory Report • FortiCare 360 Software License Report • FortiCare 360 Software Update Report • Top FortiCare 360 Customers By Devices Monitored • Top FortiCare 360 Customers and Hardware Models By Count • Top FortiCare 360 Customers and OS Versions By Count
Ungrouped	user-defined	user-defined

The following topics provides information about using CMDB reports.

- Creating a new CMDB Report
- Scheduling a CMDB Report
- Running a CMDB Report
- Adding CMDB Report to Dashboard

Creating CMDB Reports

There are two ways you can create new CMDB reports:

- Create a new report from scratch.
- Clone and modify an existing system or user-defined report by selecting a report and clicking Clone.

Follow these procedures to create or modify a CMDB Report.

- Creating a CMDB Report
- Cloning and Modifying a CMDB Report
- Exporting a CMDB Report
- Importing and Exporting CMDB Report Definitions

Creating a CMDB Report

1. Go to **CMDB** and select the CMDB report folder where you want to create the report.
2. Click **New**.
3. In the New CMDB Report dialog box, enter the following information.

Settings	Guidelines
Report Name	Name of the CMDB report.
Description	Any information related to the new report.
Target	Select the target type.
Conditions	Set the filter conditions by selecting (Attributes, Operator and Value) together with Next Operators. Parenthesis can be added by clicking + to give higher precedence to any evaluation conditions.
Display Columns	The columns in the report result. The order can be changed by selecting a column and clicking the Up or Down icons. You can specify the Order as ASC or DESC.

4. Click Save.

You can also import a report under CMDB by clicking Import to browse and choose.

Cloning and Modifying a CMDB Report

You can modify user-defined reports by selecting the report and clicking **Edit**. However, you cannot directly edit a system-defined report. Instead, you have to clone it, then save it as a new report and modify.

1. Go to **CMDB** > **CMDB Reports**.
2. Select the system-defined report you want to modify, and click **Clone**.
3. Enter a name for the new report, and click **Save**.
   The cloned report will be added to the folder of the original report.
4. Select the new report, and then click Edit.
5. Modify the report, and click **Save**.

Exporting a CMDB Report

1. Go to **CMDB** > **CMDB Reports**.
2. Select the CMDB Report folder from where the report will be exported.
3. Click Export to download and save the report.

Importing and Exporting CMDB Report Definitions

Instead of using the user interface to define a report, you can import report definitions, or you can export a definition, modify it, and import it back into your FortiSIEM virtual appliance. Report definitions follow an XML schema.

Importing a CMDB Report Definition

1. Go to **CMDB** > **CMDB Reports**.
2. Select the CMDB Report folder to where the report will be imported.
3. Click Import. The report will appear in the selected folder.

Exporting a Report Definition

1. Go to **CMDB** > **CMDB Reports**.
2. Select the CMDB report to be imported.
3. Click Export. The report will appear in the selected folder.

4. Paste the report definition into a text editor, modify it, and then follow the instructions for importing it back into your virtual appliance.

XML Schema for Report Definitions

The XML schema for the report definition is:

```
<cmdbReports>
<cmdbReport>
<name></name>
<naturalid></naturalid>
<description></description>
<selectClause></selectClause>
<orderByClause></orderByClause>
<whereClause></whereClause>
</cmdbReport>
</cmdbReports>
```

This is an example for the **Active Rules** report:

```
<cmdbReports>
<cmdbReport>
<name>Active Rules</name>
<naturalId>PH_CMDB_Report_Overall_8</naturalId>
<target>com.ph.phoenix.model.query.Rule</target>
<description>This report captures active rules on a per organization
basis</description>
<selectClause>ph_drq_rule.ph_incident_category,ph_drq_rule.name,ph_sys_d
omain.name</selectClause>
<orderByClause>ph_drq_rule.ph_incident_category ASC</orderByClause>
<whereClause>ph_drq_rule.active = true</whereClause>
</cmdbReport>
</cmdbReports>
```

Scheduling a CMDB Report

Complete these steps to schedule a CMDB report to run at a later time:

1. Go to **CMDB** and browse to select the report under CMDB Reports on the left tree.
2. Select the report from the list.
3. Click **Schedule**.
4. In the Schedule dialog box, select the required information.

Settings	Guidelines
Organization	Organization type. Select whether to Run this report for or Schedule this report for the remaining settings. • Choose Run this report for if you would like to run the report for only Global administrators. This choice will combine event data from all selected Organizations within one PDF, RTF, or CSV report and sent to the Global Administrators added in the notification settings while scheduling report alerts. • Choose Schedule this report for if you would like to run this report for each selected Organization seperately same as your login to each of these Organizations and schedule this report there. In this case, each selected Organization will receive its own copy of PDF, RTF, or CSV report containing the event data for its own Organization based on the notification settings added while scheduling report alerts.
Schedule Time Range	Enter the Time range to run the report.
Schedule Recurrence Pattern	Recurrence pattern: once, hourly, daily, weekly or monthly. Enter the start date in the Start From field.
Notification	Use the options as required: • Default Notification - to send notification to new recipients by adding them using the + icon. • Custom Notification - to send the notification to the specific email addresses added under ADMIN > Settings > System. • Copy to a remote location - To copy the report to a remote directory, first define the remote location in ADMIN > Settings > Analytics > Scheduled Report to be copied to this remote location when scheduler runs any report and then select this option.

5. Click OK.

You can also schedule a CMDB report by selecting the report from the list and clicking +under Schedule tab in the lower pane.

Running a CMDB Report

Complete these steps to run a CMDB Report.

1. Go to **CMDB > CMDB Reports** and select the report you want to run from the folder.
2. Click **Run**.
3. In the Run CMDB for dialog box, select the Organization and click Run.

Reports are saved only for the duration of your login session. You can view saved reports by clicking Results. You can use the Export button to export any report in PDF or CSV format.

Adding CMDB Report to Dashboard

Complete these steps to add CMDB reports to Dashboard:

1. Select the dashboard to which you want to add a CMDB report.
2. Click **+** to the right of the dashboard.
3. In the **Create New Dashboard** dialog box, enter a name for the Dashboard and select the Widget Dashboard from the drop-down list. For more information, refer to Dashboard.
4. Click **+** below the Dashboard drop-down list.
5. Select a report from the **CMDB Reports** folder, then click **>**. The report will be added to the dashboard.

Managing Resources

The following sections provide the procedures for managing Resources:

- Reports
- Rules
- Network
- Watch List
- Protocols
- Event Types
- Working with AlienVault OTX
- Working with Dragos IOCs
- Working with FortiGuard IOCs
- Working with Malware Patrol
- Working with MISP Threatfeeds
- Working with OpenCTI Threatfeeds
- Working with ThreatConnect
- Malware Domains
- Malware IPs
- Malware URLs
- Malware Processes
- Country Groups
- Malware Hash
- Default Password
- Anonymity Network
- User Agents
- Remediations
- Lookup Tables
- Playbooks
- Connectors
- Machine Learning Jobs
- Osquery

Reports

Reports as similar to pre-defined versions of searches that you can load and run at any time. FortiSIEM includes over 2000 pre-defined reports that you can access in **RESOURCES > Reports**.

- Viewing System Reports
- Working with Report Design Templates
- Creating Reports
- Running System Reports
- Scheduling Reports
- Importing and Exporting Reports
- Importing and Exporting Report Definitions

Viewing System Reports

Complete these steps to view system-defined Reports:

1. Go to **RESOURCES** > **Reports**.
2. Select the **Organization** for which you want to view the available reports.
3. Expand the **Reports** folder on the left panel and select the sub-category of report to view.
4. Select the report you want to view information about.
   The reports display the information below under various tabs in the lower pane:
   - **Summary** - Includes the **Condition** and **Group By** conditions for the report, and the report's **Display** attributes.
   - **Schedule** - Information about when the report is scheduled to run. See Scheduling a Report for more information. Click the **+** icon to set a schedule for the report to run.
   - **Results** - The results from any scheduled runs of the report, or results you have saved by running the report.

Note: If Data Obfuscation is turned on for a FortiSIEM user:

- The value for that object marked for data obfuscation is obfuscated. For example, if IP is marked for data obfuscation, the IP address is obfuscated. In earlier versions of FortiSIEM, raw events were completely obfuscated.
- CSV Export feature is disabled.

Running System Reports

FortiSIEM includes a number of baseline reports for common data center analytics, as well as over 300 reports relating to IT infrastructure. You can also create your own reports.

Complete these steps to run a system-generated or user-defined baseline report:

1. Go to **RESOURCES** tab and select the desired report group from the **Reports** folder.
2. Select the report(s) from the table.
3. Click **Run** to run the report(s) immediately, or select **More** and click **Schedule** to schedule the report.
4. If you have a multi-tenant deployment, select the **Organization** for which you want to run the report.
5. Select one of the **Report Time Range** options:
   - **Relative**: Select the last number of hours from which report has to be generated.
   - **Absolute**: Select the range of start and end date and time.
6. Click **OK**.
   The report will run and the results will be displayed.

Starting in 6.1.1, adhoc reports run from GUI and scheduled reports may time out after running for a long time. In a cluster environment with Worker nodes, the user may see partial results (indicated in the PDF), if some workers are able to finish their queries within the timeout. The default timeouts are specified (in seconds) in the `phoenix_config.txt` file on the Supervisor node.

[BEGIN phQueryMaster]

...

interactive_query_timeout=1800 # 30 mins

...

scheduled_query_timeout=3600 # 60mins

...

[END]

To change the default timeout values, SSH to the Supervisor node, change the values, save the file, and restart the Query Master process.

Creating New Reports

- Creating a Report
- Creating a Report Bundle
- Editing a Report Bundle

Creating a Report

Creating a report or baseline report is like creating a structured historical search, because you set the **Conditions** and **Group By** attributes that will be used to process the report data, and specify **Display Columns** to use in the report summary. You can clone an existing report to use as the basis for a new report by selecting the existing report, clicking the **More** drop-down list and selecting **Clone**.

Complete these steps to create a report:

1. Go to **RESOURCES** > **Reports**.
2. Select the report type from the **Reports** folder on the left panel.
3. Click **New**.
4. Enter a **Report Name** and **Description**.
5. For baseline reports, select **Anomaly Detection Baseline**.
6. Enter the **Conditions** to use in your report.
7. Set the **Display Columns** to use in your search results.
8. Click **Save**.
9. Optional - If you want to create a new PDF report template for this report, follow the steps in Working With Report Templates or else the system-defined template will be used.

Your report will be saved into the selected category, and you can run it or schedule it to run later.

Creating a Report Bundle

Complete these steps to create a report bundle:

1. Go to the **RESOURCES** tab and select a **Report Bundle** from the left panel.
2. Click **New**.
3. Enter a **Report Name** and **Description**.
4. For baseline reports, select **Anomaly Detection Baseline**.
5. Enter the **Conditions** to use in your report.
6. Set the **Display Columns** to use in your search results.
7. Click **Save**.

8. Optional - If you want to create a new PDF report template for this report, follow the steps here or else the system-defined template will be used.

Your report will be saved into the selected category, and you can run it or schedule it to run later.

Editing a Report Bundle

Complete these steps to edit a user-defined resource bundle:

1. Go to the **RESOURCES** tab and select a **Report Bundle** from the left panel.
2. Click the Edit icon ( ) above the left panel. The Edit Report Group dialog box opens.
3. Edit the Report Group **Name** and **Description**, if needed.
4. From the **Folders** column select the report subcategory.
5. In the **Items** column, select the desired report(s) to add to the report bundle.
6. Select **Update Template** if you want to add the selected reports to the previously defined Report Bundle template. See Creating a PDF Report Template.
7. Click **Save**.

Working with Report Design Templates

FortiSIEM gives you the flexibility of designing custom templates for each of your reports. When you select **RESOURCES > Reports**, notice that the table of reports includes a **Report Design Template** column. This column identifies the template to be used when generating and exporting a report. By default, all reports are assigned the same template. The default template name has the format *organization_name scope* **Reports Template**. For example, Global System Reports Template would be a report for the Global organization with System scope.

The Global System Reports Template can be edited when you log in as Super/Global. In this case, an Edit icon will appear next to Global System Reports Template after you modify the report design template.

A Template can be created at various levels:

- For each Report in **RESOURCES > Reports**
- For each Report folder in **RESOURCES > Reports**
- For each Report Bundle defined in **RESOURCES > Reports > Report Bundles**

When you run a report under **RESOURCES > Reports**, FortiSIEM will choose the appropriate Report Template in the following order:

1. If a specific template is defined for the selected report, then that template will be chosen.
2. If a template in the previous step is not found, then the template for the folder to which the Report belongs will be chosen.
3. If no matching template is found in Steps 1 and 2, then the system-defined template for the root folder **RESOURCES > Reports** will be chosen. System-defined templates cannot be edited.

If you load and run a report in **RESOURCES > Reports** from the **ANALYTICS** page and then manually export the Report in PDF format:

- If you choose the **Defined** option, then FortiSIEM will use the rules above to find the matching template.
- If you choose the **New** option, then you can define a new Report format for this report instance only.

Note:

- For Service Provider deployments, the Report templates can only be defined at the Super/Global level and applies for all customers.
- If a report is part of two folders and each folder has its own template defined, then the template of the current folder being viewed will be used.

The following sections provide information about:

- Creating a Report Template
- Designing a Report Template

Creating a Report Template

A Report template for PDF can be created as follows:

1. Go to **RESOURCES > Reports** and select one of the subcategories from the left pane.
2. Select the desired row from the table.
3. (Optional) Select the **Sync** checkbox in the row to synchronize the report with the Report Server.
4. Open the **More** drop-down list and select **Report Design**. The Report Design page opens.
5. Notice that the **Name** given to the report template is in the form *organization_name scope report_name* **Template**. You can edit this name if you want.
6. Follow the instructions in Designing a Report Template to design the cover page and add sections, objects, attachments, and so on, to the report.
7. Click **Save**.
   The name of the new template will be displayed in the **Report Design Template** column of the table. Notice that an edit icon appears next to the name of the template.

Creating Report Templates for a Report Folder or Resource Bundle

To create a report template for a Resource folder, choose any Report folder from the left pane. The steps to create the template are similar to Creating a Report Template.

To create a report template for a Report Bundle, complete these steps:

1. Select any system-defined or user-defined report bundle in this group.
2. Select all of the reports in the table.
3. Click **More** > **Report Design**.

Notice that the **Name** of the template for a Report Bundle cannot be edited.

Modifying an Existing Report Template

1. Click the edit icon next to the name of the existing report design template. The Report Design page opens.
2. Make the desired changes to the template design.
3. Click **Save**.

Designing a Report Template

You can design or modify the following template sections using the settings under Report Design for PDF reports:

- Overview
- Cover Page
- Report - Sections and Objects

Overview

Report Designer allows you to build a report out the following objects, the Cover Page, Table of Contents, Pages (Sections), and Objects.

- Visual PDF Report Designer Interface
- Adding an Object
- Deleting an Object
- Orientation
- Using the Text Editor when Adding Text to an Object

Visual PDF Report Designer Interface

The main interface consists of the **Template Name** field, that allows you to rename your report template, an **Organization** drop-down list to select the organization that the report template belongs to, an **Orientation** drop-down list to choose a Portrait or Landscape generated PDF report, and a horizontal control bar that has the following buttons.

- New Page - Clicking this adds a new page (Section) to your report template structure. A page can contain any number of elements, which include text, images, charts, and report tables.
- Discard Changes - Clicking this removes all prior work done before you saved (Save appears at the bottom of the interface).
- Layout - Allows you to make size and positional adjustments to an element as well as being able to adjust the margins of an element that is selected. To make a positional adjustment, select the Section or Object, and click an arrow (up, down, left, right) to change its position to where you want to move it. To adjust a margin, select the appropriate margin box and enter the new pixel value. **Note**: Only valid position options will be displayed, for example a Page/Section can only be moved up or down, and cannot be positioned left or right, so lef t and right options will not appear if a Page/Section is selected.
- Cover - When selected, a cover will be included with your PDF report. If unselected, no cover page is included with the report.
- TOC - When selected, a table of contents (TOC) will be included with your PDF report. If unselected, no TOC is included with the report.

The buttons that are available depend on how you entered the Visual PDF Report Designer.

If you entered the Visual PDF Report Designer via **Resources**, the following options are available:

At the upper right of the page:

- **Organization**: Select the organization the report is for.
- **Orientation**: Select between Portrait or Landscape.

At the bottom of the page:

- **Save** - Click to save your changes.
  Note: This will overwrite the default template stored for a Report or Report Bundle.
- **Cancel** - Click to cancel out of the Visual PDF Report Designer.
- **Preview** - Click to see a preview of the how the exported data will appear in PDF.
- **Restore to Default** - Removes custom templates that have been created, leaving only the default templates available.

If you entered the Visual PDF Report Designer via **Analytics**, the following options are available:

At the upper right of the page:

- **Orientation**: Select between Portrait or Landscape.
- **Window Size icon**: Toggle between full window or default window.

At the bottom of the page:

- **Generate** - Click to export the report.
- **Cancel** - Click to abandon the report.

Adding an Object

When you create a new Report Design, a default Cover Page and Table of Contents is automatically created.

To add a page, also known as a section, select an existing page and click the **+** icon, and select **Add page above** or **Add page below**. You can also click on the **New Page** button to add a new page/section.

To add an Object, select an existing Object where you wish to add an Object to, then click the **+** icon, and select the Object that you wish to add (Image, Text, Chart, Report Table, Legend, PDF).

Note: Only allowable objects will be available from the drop-down list. For example, a PDF are only available to create from the last page.

Deleting an Object

A report can have a maximum of one Cover Page and one Table of Contents. The Table of Contents is based off the section(s) that you create, or that already exist. To delete any existing object, select the object and then click the trash icon that appears in the upper right corner for that object.

Orientation

You can choose the page orientation that your report appears in by clicking on the **Orientation** drop-down list button and selecting **Portrait** or **Landscape**.

Using the Text Editor when Adding Text to an Object

When you choose to add text to a cover page, section, a text Object will appear. Click on the edit icon to open the text editor. Use the editor to add any text you wish to display with your report in the **Text** window. When done, click **Save**.The text editor also provides the following tools:

Icon	Description
Undo	Click to undo the last typing action.
Redo	Click to re-apply the last undo action.
Size	Click the drop-down list, and select a font size. To apply to existing text, select the text first, then click the icon and select a size.
Font Color	Click the icon and select a color. To apply to existing text, select the text first, then click the icon and select a color.
Bold	Click the icon to begin bolding text. To apply to existing text, select the text first, then click the icon.
Underline	Click the icon to begin underling text. To apply to existing text, select the text first, then click the icon.
Italic	Click the icon to begin italicizing text. To apply to

Icon	Description
	existing text, select the text first, then click the icon.
Strikethrough	Click the icon to begin strikethrough text. To apply to existing text, select the text first, then click the icon.
Remove Format	Click the icon to remove any existing formatting information that is currently being applied. To apply to existing text, select the text first, then click the icon.
Align	Click the Align icon and select one of the following alignments: • Align left - Aligns the text to start at the left side of the window. • Align center - Aligns the text to appear in the center of the window.

Icon	Description
	• Align right - Aligns the text to end at the right side of the window. • Align justify - Aligns text so it is both left and right aligned by inserting spaces between words.
Full Screen/Text Editor	Click to toggle between expanding to full screen and the standard text editor window.
Code view	Click to toggle between normal and code view.

Cover Page

The default Cover Page template includes the Report title, current Organization, Start Time, End Time, Generated Time, and Device Time Zone as Default Text. These sections can be deleted, rearranged, or have text content and images added to them. To modify an existing section, select it, then select the type from the **Cover Type** drop-down list.

- Adding Text to Cover Page
- Adding Images to Cover Page

Adding Text to Cover Page

1. Click the **Cover Page** bar to expand the section.
2. Click on any Object in the Cover page, click the **+** icon, and select **Text** from the drop-down list to add text content to the cover page.

3. Add the text in the **Text** window. For information on text tools, see Using the Text Editor when Adding Text to an Object.
4. Click **Save** to apply the changes.

Adding Images to Cover Page

1. Click the **Cover Page** bar to expand the section.
2. Click on any Object in the Cover page, click the **+** icon, and select **Image** from the drop-down list to add any JPG, PNG, or SVG image in the cover page.
3. Click **Select File** to add the image.
4. From the **Scale** drop-down list, select one of the following:
   - **Not Scale** - The image will not be resized.
   - **Fit Width** - The image will be resized to fit width.
   - **Fit Height** - The image will be resized to fit height.
   - **Fill all** - The image will be resized to fill the entire space available for it.
5. Click on the Left, Center, or Right Alignment icon to adjust the image alignment.

Note:

1. To fill the width of a page, the image size must be set to 5000 x 5000.
2. Even when enlarged, the JPG, PNG, or SVG image will appear pixelated (it does not use vector graphics). the more you zoom the page, the worse the image will look.

Report - Sections and Objects

This section allows you to add new **Sections (Pages)** and **Objects** to your Report. You can also add text content, images, charts, report tables, or a PDF attachment here.

- Adding Sections
- Adding Objects
- Adding Text to a Section or Object
- Adding an Image to a Section or Object
- Adding a PDF to a Custom Report
- Adding a Chart
- Adding a Report Table
- Adding a Legend to a Section
- Adding a CMDB Report to a Section or Object

Adding Sections

Click the **New Page** button to add a section, or from an existing section, take the following step.

1. Select the Section, and click on the **+** icon at the top or bottom of the Section to respectively add a page above the Section, or below it. After clicking the + icon, select **Add page above**, or **Add page below** to add a new Section.

Adding Objects

To add an Object to a Section, select a Section or Object, and click on the **+** icon. From the drop-down list, select an object (Text, Image, Chart, Report Table, Legend).

Note: Only allowable objects will be available from the drop-down list. For example, a Report Table and Legend are only available from a Section, and are not available when selecting **+** from an Object.

Adding Text to a Section or Object

1. Click the required Section or Object.
2. Click on a **+** icon, and select **Text** from the drop-down list to add text information.
3. Click the Text Edit icon and add the text in the **Text** window. For information on text tools, see Using the Text Editor when Adding Text to an Object.
4. Click **Save** to apply the changes.

Adding an Image to a Section or Object

1. Click on the required Section or Object.
2. Click on a **+** icon, and select **Image** from the drop-down list to add any JPG, PNG, or SVG image.
3. Click **Select File** to add the image.
4. From the **Scale** drop-down list, select one of the following:
   - **Not Scale** - The image will not be resized.
   - **Fit Width** - The image will be resized to fit width.
   - **Fit Height** - The image will be resized to fit height.
   - **Fill all** - The image will be resized to fill the entire space available for it.
5. Click on the Left, Center, or Right Alignment icon to adjust the image alignment.

Note:

1. To fill the width of a page, the image size must be set to 5000 x 5000.
2. Even when enlarged, the JPG, PNG, or SVG image will appear pixelated (it does not use vector graphics). the more you zoom the page, the worse the image will look.

Adding a PDF to a Custom Report

A PDF attachment can only be added to the last page (Section) of a Custom report. To add a PDF attachment, click on the bottom **+** icon from the bottom most Page (Section), and select **PDF**. Click **Select File**, and select the PDF file to attach.

Adding a Chart

1. Click on the required section or object bar to expand the section.
2. To add a **Chart**, select a section or object.

3. Click the **+** icon, and select **Chart** from the drop-down list.
4. In the Report Section window, take the following steps.
   a. In the **Chart Name** field, enter the name of the chart.
   Note: The chart name will named as the Display Attribute unless a Chart Name is provided.
   b. From the **Format** drop-down list, select the chart type. The list displays the available charts.
   c. From the **Items** field, enter the number of items to display.
   Note: If the item number is changed for one chart, all charts and Legend within that page will be also be updated with that change.
   d. From the **Report** drop-down list, select the report to use.
   e. From the **Attribute** drop-down list, select an attribute.

Adding a Report Table

1. Click on the required section or object bar to expand the section.
2. To add a **Report Table**, select a section or object.
   Note: The Report Table option is only available if no Report Table exists on the page.
3. Click the **+** icon, and select **Report Table** from the drop-down list.
4. Select the Report from the **Report** drop-down.
5. To display the event type, add a check to the **Event Type** checkbox.
6. To display a summary, add a check to the **Summary** checkbox.
7. When you define a custom template for **Report Bundles** (excluding the root group), you can select any Event Reports from the **Report** drop-down list.
   Note the following:
   - For Report folders (including the root group), the **Report** setting is not available.
   - For a single Report, the Event Report is automatically selected under the **Report** setting and you cannot modify this.

Adding a Legend to a Section

1. Click on the required section to expand the section.
2. Click on the **+** icon, and select **Legend**.
   Note: The Legend option is only available if no Legend exists on the current section.

Adding a CMDB Report to a Section or Object

Note: You can add **CMDB Reports** only to a **Report Bundle** template.

1. Navigate to **Resources > Reports > Report Bundles > <*Report Bundle*>**.
   For <*Report Bundle*>, select a specific Report Bundle, for example Important PCI, Firewall Health, or Router Health.
2. In the left pane, click the Report Design icon.
3. Click on the required section or object bar to expand the section.
4. Click the **+** icon and select **CMDB Report** from the drop-down list.

5. Click the **Edit** icon, then from the Select CMDB Report window, select the **CMDB Report** from the drop-down list. You can also use the search bar to find a specific CMDB report.
6. Click **Save** to confirm the selection.
7. Select the number of **Items** to display.
8. Click **Save** to apply the changes.

Scheduling Reports

You can schedule reports/report bundles to run once or for recurring periods in the future. When you schedule a reports/report bundle, you can specify notifications that can be sent for the report. In addition, you should make sure that the default settings for notifications for all scheduled reports/report bundles have been set up.

- Scheduling a Report
- Scheduling a Report Bundle
- Scheduling Reports Using a Workflow

Starting in 6.1.1, adhoc reports run from GUI and scheduled reports may time out after running for a long time. In a cluster environment with Worker nodes, the user may see partial results (indicated in the PDF, in PDF or RTF starting in 6.3.0), if some workers are able to finish their queries within the timeout. The default timeouts are specified (in seconds) in the `phoenix_config.txt` file on the Supervisor node.

[BEGIN phQueryMaster]

...

interactive_query_timeout=1800 # 30 mins

...

scheduled_query_timeout=3600 # 60mins

...

[END]

To change the default timeout values, SSH to the Supervisor node, change the values, save the file, and restart the Query Master process.

Scheduling a Report

Complete these steps to schedule a report:

1. Go to **RESOURCES** tab and select the report under **Reports** folder from the left pane.
2. Select the report(s) to schedule from the list on the right pane.
3. Click **More** > **Schedule**.
   Note: You can also schedule a report from the lower pane - select the **Schedule** tab after selecting the report. Use the **+** icon to enter the **Schedule** settings.
4. In Super/Global scope, under **Organization** section, for **Report Data**, you can choose either **Combine all selected Organizations into one Report** or **Generate separate Report for each selected Organization** with selected organizations:
   - Choose **Combine all selected Organizations into one Report** if you would like to run the report for only Global administrators. This choice will combine event data from all selected Organizations within one PDF or RTF report and sent to the Global Administrators added in the

Notification settings while scheduling reports.

- Choose **Generate separate Report for each selected Organization** if you would like to run this report for each selected Organization separately same as your login to each of these Organizations and schedule this report there. In this case, each selected organization will receive its own copy of the CSV, PDF or RTF report containing the event data for its own Organization based on the Notification settings added while scheduling reports.

5. In Report Time Range, configure the range of time that the report should provide. See Specifying Search Time Window.
6. In Trend Interval, configure appropriately if your report uses trend event attributes, otherwise, leave as **Auto**. See Specifying Trend Interval.
7. Click **Next**.
8. Use the **Schedule Time Range** option if the run time has to be scheduled for a later period and a specific place.
9. Schedule the **Schedule Recurrence Pattern** for the report to run once, hourly, daily, weekly, or monthly or set the range under **Schedule Recurrence Range**.
10. Click **Next**.
11. Select the **Output Format** as **PDF**, **CSV**, or **RTF**.
    For PDF and RTF output, the default template configured under **RESOURCES** > **Reports** is used. You can customize the report templates following the steps under Designing a Report Template.
12. Specify the **Notification** that should be sent when the report runs from the available options:
    - **Default Notifications** - to send default notifications. Click the edit icon to add more **Recipients**.
    - **Custom Notifications** - to send notifications to specific email addresses. Use the edit icon to add more **Recipients**
    - **Copy to a remote directory** - to copy the report to a remote directory.
13. Specify the time that the report should be retained after it has run using the **Retention** setting in hours or number of days.
14. Click **OK**.
    The report will run at the time you scheduled.

Scheduling a Report Bundle

Complete these steps to schedule a report bundle:

1. Go to **RESOURCES > Reports** tab and select a report bundle under **Report Bundles** folder from the left pane.
2. Select the clock icon ( ) above the left panel folders to open the scheduler settings.
3. In the **Schedule Report Bundle** window, click **+**.
4. In Super/Global scope, under **Organization** section, for **Report Data**, you can choose either **Combine all selected Organizations into one Report** or **Generate separate Report for each selected Organization** with selected organizations:

- Choose **Combine all selected Organizations into one Report** if you would like to run the report for only Global administrators. This choice will combine event data from all selected Organizations within one PDF or RTF report and sent to the Global Administrators added in the Notification settings while scheduling reports.
- Choose **Generate separate Report for each selected Organization** if you would like to run this report for each selected Organization separately same as your login to each of these Organizations and schedule this report there. In this case, each selected Organization will receive its own copy of the PDF or RTF report containing the event data for its own Organization based on the Notification settings added while scheduling reports.

5. Select the **Report Time Range**:
   - Select the **Time Zone**.
   - Select **Relative** to enter the last number of hours from which report has to be generated or **Absolute** to enter the range of start and end date and time.
6. Select the Trend Interval for **Trend**. See Specifying Trend Interval.
7. Click **Next**.
8. Use the **Schedule Time Range** if the run time has to be scheduled for a later period and a specific place.
9. Click **Next**.
10. Select the **Output Format** as **PDF** or **RTF**.
    For PDF or RTF output, the default template configured under **RESOURCES** > **Reports** is used. You can customize the report templates following the steps under Designing a Report Template.
11. Schedule the **Schedule Recurrence Pattern** for the report bundle to run once, hourly, daily, weekly, or monthly or set the range under **Schedule Recurrence Range**.
12. Specify the **Notification** that should be sent when the report bundle runs from the available options:
    - **Default Notifications** - to send default notifications. Click **+** to add more **Recipients**.
    - **Custom Notifications** - to send notifications to specific email addresses. Use the edit icon to add more **Recipients**.
    - **Copy to a remote directory** - to copy the report bundle to a remote directory.
13. Specify the Event/CMDB **Attribute**, **Operator**, and **Value**. Click **+** to add more, if required.
14. Click **OK**.
    The report bundle will run at the time you scheduled.

Scheduling Reports Using a Workflow

Follow these steps to schedule a report by using a workflow.

- Step 1 - Create Appropriate Roles for Users
- Step 2 - Map Users to Appropriate Roles
- Step 3 - Request the Report to be Scheduled
- Step 4 - Approve the Report Scheduling Request
- Step 5 - View the Report Scheduling Request Status

Step 1 - Create Appropriate Roles for Users

Complete these steps to create a role that will require report scheduling approval.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.
3. Make sure the **Approver > Report Schedule** option is not checked.
4. Make sure the **Activation > Report Schedule** option is not checked.
5. Save the role definition.

Complete these steps to create a role that can approve report scheduling requests.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.
3. Make sure the **Approver > Report Schedule** option is checked.
4. Make sure the **Activation > Report Schedule** option is not checked.
5. Save the role definition.

Step 2 - Map Users to Appropriate Roles

1. Go to **CMDB > Users**.
2. Select a user from the table and click **Edit**.
3. In the Edit User dialog box, select the **System Admin** option, and click the **Edit** icon.
4. Select the **Requestor** or **Approver** role as appropriate.

Step 3 - Request Report to be Scheduled

1. Go to **RESOURCES > Reports**.
2. Select a report, then select **More > Schedule**. The Create New Request dialog box opens.
3. If the role requires approval, select an approver from the **Approver** drop-down list.
4. Click **Submit**.
5. The approver will receive an email with a link to log back in to FortiSIEM and approve the request.

Step 4 - Approve the Report Scheduling Request

1. Login to FortiSIEM using a role that can approve a report being scheduled .
2. Click **Approval**. The table in the **TASKS** page lists pending requests.
3. To process the requests, scroll to the right-hand end of the row.

4. From the drop-down list, select **Approve** or **Reject**.
   - If you select **Approve**, the Approve Request dialog box opens. You can choose whether the request is valid **Until** or **For the date and time listed in the time stamp field**. You can click the time stamp field to choose a different date and time.
   - If you choose **Reject**, the Reject Request dialog box opens where you can enter a reason for the rejection.
5. If you choose **Approve**, the report will now be scheduled.

Step 5 - View Report Scheduling Request Status

Complete this step to see the status of your report schedule activation requests.

1. Login to FortiSIEM using the same account as in Step 3.
2. Click **Request**. The table in the **TASKS** page shows the status of requests.

Importing and Exporting Reports

Importing a Report

1. Go to **RESOURCES > Reports** and select the folder where you want to import the report.
2. Open the **More** drop-down list and select **Import**.
3. Click **Choose File** and browse to the report file to import.
4. Click **Import**.

Exporting a Report Definition

1. Go to **RESOURCES > Reports** and select the folder where you want to export a report definition.
2. Select a report definition in the main panel.
3. Open the **More** drop-down list and select **Export**.

Exporting Report Results

Complete these steps to export Reports in PDF, RTF, or CSV format:

1. Go to **RESOURCES** tab and select the report under **Reports** folder from the left panel.
2. Select the reports and click **Run** to view the results under **ANALYTICS** tab.
3. Go to **Actions** and select **Export Result**.
4. Optional - Enter any **User Notes** about this report.
5. Select the **Output Format** for the report as CSV, RTF or PDF.
6. Select the **Time Zone** for which the report is to be generated. If the devices are in a different Timezone from the Supervisor, then you can choose the time zone of the devices while configuring the PDF or RTF report.
7. Select the **Template** if PDF or RTF format is selected:
   - **Defined** - to use the default template defined for this report defined under **RESOURCES** > **Reports**.
   - **New** - to create a new custom report template for one-time use. The **Report Design** settings appear on choosing this option. Note that this template will not replace the template defined under **RESOURCES** > **Reports**. See Designing a Report Template for the steps to customize the report template.
8. Click **Generate** to create the report.
9. Click **View** to open and save the report.

Note: If Data Obfuscation is turned on for a FortiSIEM user:

- The value for that object marked for data obfuscation is obfuscated. For example, if IP is marked for data obfuscation, the IP address is obfuscated. In earlier versions of FortiSIEM, raw events were completely obfuscated.
- CSV Export feature is disabled.

Importing and Exporting Report Definitions

Instead of using the user interface to define a report, you can import report definitions, or you can export a definition, modify it, and import it back into your FortiSIEM virtual appliance. Report definitions follow an XML schema.

- Importing a Report Definition
- Exporting a Report Definition

Importing a Report Definition

Complete these steps to import a Report Definition:

1. Go to **RESOURCES** tab and select the report under **Reports** folder from the left panel.
2. Select **More** > **Import**.
3. Click **Browse** to select the Report Definition in XML format.
4. Click **Import** to import the Report Definition.

Exporting a Report Definition

Complete these steps to export a Report:

1. Go to **RESOURCES** tab and select **Reports** folder from the left panel.
2. Select the report to export.
3. Select **More** > **Export**.
4. Save the exported Report Definition in XML format.

Rules

FortiSIEM continuously monitors your IT infrastructure and provides information to analyze performance, availability, and security. There may also be situations in which you want to receive alerts when exceptional, suspicious, or potential failure conditions arise. You can accomplish this using rules that define the conditions to watch out for, and which trigger an incident when those conditions arise. You can configure an automation policy that will send email and SNMP alerts that the incident has occurred. FortiSIEM includes over 500 system-defined rules, which you can see in **RESOURCES > Rules**, but you can also create your own rules as described in the topics in this section.

- Viewing Rules
- Creating a Rule
- Activating and Deactivating a Rule
- Testing a Rule
- Importing and Exporting Rule Definitions
- Importing Sigma Rules

Viewing Rules

FortiSIEM includes a large set of rules for Availability, Performance, Change, Security, and Beaconing groups in addition to the rules that you can define for your system.

Complete these steps to view all system and user-defined rules:

1. Go to **RESOURCES** > **Rules**.
2. Use the **System** drop-down menu of the Rules list pane to filter rules by Organization.
3. Select any rule in the Rules list to view related information in the lower pane.

   All rules have two information tabs:

Tabs	Description
Summary	This tab provides an overview of the rule logic, its status, and notification settings.
Test Results	If you are testing a rule, you can view the results here. **Note**: Active rules cannot be tested. You must deactivate a rule before testing.

Creating Rules

Creating a new rule involves defining the attributes of the incident that is triggered by the rule, as well as the triggering conditions and any exceptions or clear conditions. You can also create a rule by cloning an existing rule using the **Clone** button and editing it.

Note: Do not use certain keywords in sub-pattern names - `regexp`.

- Creating a Rule
- Defining Rule Conditions
- Defining the Incident Generated by a Rule
- Defining Rule Exceptions
- Defining Clear Conditions
- Defining an Incident Title

Creating a Rule

Complete these steps to create a rule:

1. Go to **RESOURCES** > **Rules**.
2. Select the group where you want to add the new rule.

3. Click **New** to create a new rule.

Settings	Guidelines
Step 1: General	
Group	From the drop-down list, select the group the rule will belong to.
Rule Name	Enter a name for the new Rule.
Description	Enter a description of the new Rule.
Data Source	Select or enter the source where the data comes from for the rule to define its data source.
Detection Technology	Provide the detection technology method used by the rule by selecting from the drop-down list. The choices are: • Correlation - Uses an association between variables for discovery. • Correlation Using Lookup Table - Uses lookup table for discovery. • Machine Learning - Uses machine learning models for discovery. • Profiling - Collects specific data for discovery.
Event Type	The name you enter in the Rule Type field is replicated in the Event Type field.
Evaluation Mode	Select **Streaming** or **Scheduled**. Streaming rules are rules that are run in real-time. Scheduled rules are rules that run on a defined schedule. Rules in scheduled mode requires configuration of Query Time Window and Schedule. **Note**: This option is only made available with a ClickHouse database. In contrast to Streaming, Scheduled rules require disk access and does not scale comparably. In-memory Streaming option is faster and a large number of rules can be evaluated concurrently. However, Scheduled reports have the following advantages: • Rules can be written using the complex analytic functions introduced in 7.0. • Rules can be evaluated over larger time intervals. • Once the scheduled rule conditions are met, Incidents are created the same way as Streaming rules.
Remediation Note	Enter the **Remediation** script. Make sure that the Remediation script for your scenario is defined. Check the existing Remediation scripts under **ADMIN** > **Settings** > **General** > **Notification Policy** > **Action** column. If your device is not in the list, add the needed Remediation script.
Query Time Window	For Scheduled Mode, the following configuration is required. Time Zone - Configure the Time Zone by selecting from the drop-down list (s), and configure the frequency that the rule will be run in the following row.
Schedule Time Window	For Scheduled Mode, the following configuration is required. Schedule Time Range - In the **Start Time** field, enter/select the time to start the scheduled rule.

Settings	Guidelines
	Schedule Recurrence Range - In the **Start From** field, enter the time when the scheduled rule should run. Next, configure when the scheduled rule should end from the following choices: **No end date**, **End after**, or **End by**. For End after, enter the number of occurrence(s) needed to stop the scheduled rule. For End by, enter the date when the scheduled rule will stop running.
Step 2: Define Conditions	
Conditions	Click **Condition** to create the rule conditions. See Defining Rule Conditions.
Step 3: Define Actions	
Severity	Select a **Severity** to associate with the incident triggered by the rule.
Category	Select the **Category** of incidents to be triggered by the rule.
Subcategory	Select the **Subcategory** from the available list based on the selected incident **Category**. To add custom subcategories, follow the steps under Setting Rule Subcategory.
Technique	Select any techniques from the available **Technique** list. You can choose to select zero, one, or multiple techniques. The Tactics row will update itself based on the techniques selected.
Action	Click the edit icon to define the incident (Incident Attributes and Triggered Attributes) that will be generated by this rule. You must have at least one incident defined before you can save your rule.
Exception	Click the edit icon to define any **Exceptions** for the rule. See Defining Rule Exceptions.
Tag	Click the drop-down list icon to view the tag list. If no tags appear, it means no tags have been created. From the drop-down list, select any tags you wish to associate with the rule. From Incidents View (by Time, by Device, by Incident), tags are displayed in the **Tag** column. See Tags for more information.
Update Status on Summary Dashboard	Add a check mark to the **Update Status on Summary Dashboard** checkbox to add this rule update in the Summary Dashboard, under the **DASHBOARD** tab.
Notification	Enter a **Notification** frequency for how often you want notifications to be sent when an incident is triggered by this rule.
Impacts	Select the **Impacts** of the incident triggered by this rule from the drop-down.
Watch List	Click the edit icon to add the rule you want to add to the watch list. **Note:** The Type that you set for the watch list must match the Incident Attribute Types for the rule. For example, if your watch list Type is IP, and the Incident Attribute Type for the rule is string, you will not be able to associate

Settings	Guidelines
	the watch list to the rule.
Clear	Click the edit icon to define any **Clear** conditions for the rule. See Defining Clear Conditions.

4. Click **Save**.
   Your new rule will be saved to the group you selected in an inactive state. Before you activate the rule, you should test it.

Defining Rule Conditions

Rule conditions define the event attributes and thresholds that will trigger an incident. Rule conditions are built from sub-patterns of event attribute filters and aggregation functions. You can specify more than one subpattern and the relationships and constraints between them.

Specifying a Subpattern

A subpattern defines the characteristics of events that will cause a rule to trigger an incident. A subpattern involves defining event attributes that will be monitored, and then defining the threshold values for aggregations of event attributes that will trigger an incident.

Note: Only one subpattern is allowed for Scheduled Rules.

Event Filters

Event filter criteria determine which event attributes and values will be monitored by the rule, and are set in a way that is similar to the way you set event attributes for structured historical searches and real time searches.

Event Aggregation

While you could have a rule that triggers an incident on a single instance of a particular event, it is more likely that you will want your rule to trigger an incident when some number of events have been found that meet your event filter criteria.

Group By Attributes

This determines which event attributes will be used to group the events before the group constraints are applied, in a way that is similar to the way the Group By attribute is used to aggregate the results of structured searches.

Aggregate Conditions

The group aggregation conditions set the threshold at which some aggregation of events will trigger a rule to create an incident. You create an aggregation condition by using the **Expression Builder** to set a function, and then enter the **Operator** and **Value** for the aggregation condition. Examples of Group By and Aggregate Conditions Settings are shown below:

Scenario	Group By Attributes	Aggregate Conditions
10 or more events	none	**COUNT(Matched events) >= 10**
Connections to 100 or more distinct destination IPs from the same source IP	**Source IP**	**COUNT (DISTINCT Destination IP) >= 100**
Connections to 100 or more distinct destination IPs from the same source IP on the same destination port	**Source IP,Destination Port**	**COUNT (DISTINCT destination IP) >= 100**
Average CPU Utilization on the same server > 95% over 3 samples	**Host IP**	**COUNT (Matched Events) >= 3 AND AVG(CPU Util) > 95**
Logins from the same source workstation to 5 or more accounts on the same target server	**Source IP**, **Destination IP**	**COUNT(DISTINCT user) >= 5**

Setting the Relationship between Subpatterns

If you have more than one sub-pattern, you must specify the relationship between them with these operators.

Operator	Meaning
AND	**Sub-pattern P1 AND Sub-pattern P2** means both sub-patterns P1 and P2 have to occur
OR	**Sub-pattern P1 OR Sub-pattern P2** means either P1 or P2 have to occur
FOLLOWED-BY	**Sub-pattern P1 FOLLOWED-BY Sub-pattern P2** means P1 has to be followed by P2 in time
AND-NOT	**Sub-pattern P1 AND-NOT Sub-pattern P2** means P1 must occur while P2 must not; the time order between P1 and P2 is not important
NOT-FOLLOWED-BY	**Sub-pattern P1 NOT-FOLLOWED-BY P2** means P1 must occur and P2 must not occur after P1

Setting Inter-subpattern Constraints

You may want to relate attributes of a sub-pattern to the corresponding attributes of another sub-pattern, in a way that is similar to a JOIN operation in an SQL, by using the relationship operators **<**, **>**, **<=**, **>=**, **=**, **!=**.

Examples of inter-subpattern relationships and constraints

Scenario	Sub-pattern P1 - filter	P1 - Group-by attribute set	P1 Group constraint	Sub-pattern P2 filter	P2-group-by attribute	P2 group constraint	Inter-P1-P2 relationships	Inter-P1-P2 constraints
5 login failures from the same source to a server not followed by a successful logon from the same source to the same server	Event type = Login Success	Source IP, Destination IP	COUNT (Matched Event) >= 5	Event type = Login failure	Source IP, Destination IP	COUNT (Matched Event) > 0	P1 NOT_FOLLOWED_BY P2	P1's Source IP = P2's Source IP
An security attack to a server followed by the server scanning the network, that is, attempting to commun	Event type = Attack	Destination IP	COUNT (Matched Event) > 0	Event Type = Connection Attempted	Source IP	COUNT (DISTINCT Destination IP) > 100	P1 FOLLOWED_BY P2	P1's Destination IP = P2's Source IP

Scenario	Sub-pattern P1 - filter	P1 - Group-by attribute set	P1 Group constraint	Sub-pattern P2 filter	P2-group-by attribute	P2 group constraint	Inter-P1-P2 relationships	Inter-P1-P2 constraints
icate to 100 distinct destination IP addresses in 5 minute time windows								
Average CPU > 95% over 3 sample on a server AND Ping loss > 75%	Event Type = CPU_Stat	Host IP	COUNT (Matched Event) >= 3 AND AVG (cpuUtil) > 95	Event Type = PING Stat	Host IP	pingLossPct > 75	P1 AND P2	P1's Host IP = P2's Host IP

Defining the Incident Generated by a Rule

Defining an incident involves setting attributes for the incident based on the subpatterns you created as conditions for the rule, and then setting attributes for the incident that will be used in analytics and reports.

Note: You must have at least one incident defined before you can save your rule.

1. Select the rule you want to define an incident for.
2. Click **Edit** and go to **Step 2: Define Condition**.
3. Select a **Subpattern** from the drop-down list and click the edit icon to define the conditions for the rule. See Defining Rule Conditions.
   Define attributes for the incident based on the **Filter**, **Aggregate**, and **Group By** attributes you set for your subpatterns. Typically, you will set the Incident attributes to be the same as the Group By attributes in the subpattern:
   a. Select the **Attribute** you want to add to Incident.
   b. Select a **Subpattern**.
   c. This will populate values from the **Group By** attributes in the subpattern to the **Filter** menu.
   d. In the **Filter** menu, select the attribute you want to set as equivalent to the **Event Attribute**.

4. In **Step 3: Define Action**, provide values for the **Severity**, **Category**, **Subcategory**, **Dashboard**, **Notification**, **Impacts**, and **Watch List** fields as described in Creating a Rule. For information on exceptions, see Defining Rule Exceptions.
5. Click the **Action** edit icon to define the incident events and triggered attributes in the **Generate Incident for** dialog box. This dialog box is is pre-populated with typical attributes you would want included in an incident report.
6. Under **Triggered Attributes**, select the attributes from the triggering events that you want to include in Dashboards and Analytics for this event.
7. Click **Save**.

Defining Rule Exceptions

Once you activate a rule, it continuously monitors your IT infrastructure for conditions that would trigger an event. However, you may also want to define exceptions to those conditions. For example, you may know that a server will be going down for maintenance during a specific time period and you don't want your **Server Down - No Ping Response** rule to trigger an incident for it.

1. In **RESOURCES** > **Rules**, select the rule you want to add the exception to, and click **Edit**.
2. Select **Step 3: Define Action**.
3. Next to **Exceptions**, click **Edit**.
4. Select an **Attribute** and **Operator**, and enter a **Value**, for the conditions that will prevent an incident from being generated.
   The values in the Attribute menu are from the **Event Attributes** associated with the incident definition.
5. Click the **+** icon to set an effective time period for the exception.
   You can set effective time periods for single and recurring events, and for durations of time from hours to days.
6. Enter any **Notes** about the exception.
7. Click **Save**.

Defining Clear Conditions

Clear conditions specify conditions in which incidents will have their status changed from **Active** to **Cleared**. You can set the time period that must elapse for the clear condition to occur, and then set the conditions based on the triggering of the original rule, or on a sub pattern based on the Incident Attributes.

1. In **RESOURCES** > **Rules**, select the rule you want to add the clear condition to, and click **Edit**.
2. Select **Step 3: Define Action**.
3. Next to **Clear Condition**, click **Edit**.
4. Set the **Time Period** that should elapse for the clear condition to go into effect.

5. If you want the clear condition to go into effect based on the firing of the original rule, select **the Original Rule Does Not Trigger**.
   Note: For Scheduled Rules, this is not selectable.
   For example, if you wanted the clear condition to change the status of **Active** incidents to **Cleared** after the original rule had not been triggered for ten minutes, you would set **Cleared Within** to **10 Minutes** and select this option.
6. If you want to base the clear condition on a sub-pattern of the incident attributes, select **the following conditions are met**.
   The incident attributes from your rule will load and the clear condition attributes will be set to match.
7. Define the pattern to use by clicking the **Edit** icon next to the clear sub pattern.
8. Click **Save**.

Defining an Incident Title

Defining an incident title makes it convenient to identify an incident without having to search on incident source, target, and details. You can define titles for both user-defined rules and system rules.

These steps assume you have already created a rule or are editing a system rule.

1. In **RESOURCES** > **Rules**, select the rule you want to add a title to, and click **Edit**.
2. Select **Step 3: Define Action**.
3. You can either enter text for the title or build the title using incident attributes defined for the rule.
   To use the incident attributes to build the title, follow these steps:
   a. Open the drop-down list next to **Insert Attribute**.
      Notice that the list contains all of the attributes defined in the **Incident Attributes** field.
   b. Select an attribute and click the **+** symbol to the right of the **Insert Attribute** list.
      The attribute appears in the **Incident Title** field prefixed by a "$" symbol, for example, `$user`.
   c. Repeat the previous step for all of the attributes you want to appear in the title.
   d. You can add text to the **Incident Title** field to make it more meaningful to you, for example: `$user` *created* `$fileName` *on* `$hostName`.
4. Click **Save** when you have finished your edits.

Once the title is defined in a rule definition, FortiSIEM will populate Incident **Title** field for all new instances of the Incidents.

To Display the Incident Title Field

Follow these steps to display the **Incident Title** column in the list of incidents table.

1. Go to **INCIDENTS > List by Time** view.
2. Open the **Actions** drop-down list and select **Change Display Columns**.
3. Select **Incident Title** from the list.
4. Click **Close**.

The **Incident Title** column appears in the incidents table.

Activating and Deactivating a Rule

- Activating a Rule Without a Workflow
- Activating a Rule Using a Workflow
- Activating/Deactivating Multiple Rules

Activating a Rule Without a Workflow

If you have permission to activate a rule, follow these steps: You may also want to deactivate a rule, for example to test it, instead of deleting it from the system.

1. Go to **RESOURCES** > **Rules**.
2. Browse or search to find the rule that you want to activate or deactivate.
3. Select **Active** in the Active column to activate the rule, or clear the **Active** option to deactivate the rule.

Activating a Rule Using a Workflow

Follow these steps to activate a rule by using a workflow.

- Step 1 - Create Appropriate Roles for Users
- Step 2 - Map Users to Appropriate Roles
- Step 3 - Rule to be Activated/Deactivated
- Step 4 - Approve the Rule Activation/Deactivation Request
- Step 5 - View the Rule Activation/Deactivation Request Status

Step 1 - Create Appropriate Roles for Users

Complete these steps to create a role that will require approval for rule activation/deactivation requests.

1. Go to **ADMIN > Settings > Role > Role Management**.
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.
3. Make sure the **Approver > Rule Activation/Deactivation** option is not checked.
4. Save the role definition.

Complete these steps to create a role that can approve rule activation/deactivation requests.

1. Go to **ADMIN > Settings > Role > Role Management**
2. Click **New** to create a new role or edit an existing role by selecting a role from the table and clicking **Edit**.
3. Make sure the **Approver > Rule Activation/Deactivation** option is checked.
4. Save the role definition.

Step 2 - Map Users to Appropriate Roles

1. Go to **CMDB > Users**.
2. Select a user from the table and click **Edit**.
3. In the Edit User dialog box, select the **System Admin** option, and click the **Edit** icon.
4. Select the **Requestor** or **Approver** role as appropriate.

Step 3 - Request Rule to be Activated/Deactivated

1. Go to **RESOURCES > Rules**.
2. Select a rule, then check or uncheck the active column status as needed. The Create New Request dialog box opens.
3. If the role requires approval, select an approver from the **Approver** drop-down list.
4. Click **Submit**.
5. The approver will receive an email with a link to log back in to FortiSIEM and approve the request.

Step 4 - Approve the Rule Activation/Deactivation Requests

1. Login to FortiSIEM using a role that can approve rule activation/deactivation requests.
2. Click **Approval**. The table in the **TASKS** page lists pending requests.
3. To process the requests, scroll to the right-hand end of the row.
4. From the drop-down list, select **Approve** or **Reject**.
   - If you select **Approve**, the Approve Request dialog box opens. You can choose whether the request is valid **Until** or **For the date and time listed in the time stamp field**. You can click the time stamp field to choose a different date and time.
   - If you choose **Reject**, the Reject Request dialog box opens where you can enter a reason for the rejection.
5. If you choose **Approve**, the rule will be enabled or disabled.

Step 5 - View the Rule Activation/Deactivation Request Status

Complete this step to see the status of your rule activation/deactivation requests.

1. Login to FortiSIEM using the same account as in Step 3.
2. Click **Request**. The table in the **TASKS** page shows the status of requests.

Activating/Deactivating Multiple Rules

If you have permission to activate a rule, follow these steps to activate/deactivate multiple rules with a single click.

1. Go to **RESOURCES** > **Rules**.
2. Click the Edit icon ( ) and select **Multiple Rules**.
3. From the Edit Multiple Rules window, take the following steps:
   a. In the leftmost panel, expand Rules, and rule categories/sub-categories (Availability, Network, etc...) to locate your rule(s) in the middle panel.
   b. In the middle panel, select your rule(s) you wish to make activation/deactivation changes to. You can use Shift-Click to select a group of ascending or descending rules from your first selection. You can also use Ctrl-Click to individually select a group of rules.
   c. Click **>** to add the selected rule(s) for activation/deactivation.
   Note: You can also select a rule in the rightmost panel and click **<** to remove it from the group selection.
   d. When you are done selecting all the rules you wish to make an activation/deactivation change to, in the **Select Actions** panel, take any of the following actions:
      - Select a Severity from the **Severity** drop-down list to change for your selected rules.
      - Select/deselect Active Status for New Org, to make the selected rules active or inactive for new organizations by default.
      - From the **All Status for Existing Orgs** and specific org checkboxes, add a check to the checkbox to make the selected rules for that organization active, or remove the checkmark from a checkbox to make the selected rules inactive for that particular organization.
4. When done, click **Save**.

Testing a Rule

After creating or editing a rule, you should test it to see if it works as expected, before activating.

Note: You can perform rule testing only on the super global organization and not within the local organization.

Complete these steps to test a rule:

1. Go to **RESOURCES** > **Rules**, and deactivate the rule to test.
   Note: If you cannot deactivate a rule for testing, you can clone an inactive version of it.
2. In the **Set Activation Scope** dialog box, deselect the **Activation Status for New Org** and all of the organizations under **Activation Status for This Rule**.
3. Click **Save** to close the **Set Activation Scope** dialog box.
4. Select the rule, and click **Test**.
   This opens the **Rule Debug Events** dialog box.
5. Enter a **Reporting IP** where the synthetic event should originate from.
   If the rule you're testing specifies that the **Reporting IP** should be a member of a group, you should make sure that the Reporting IP you enter here is in that group.
6. Under **Raw Event**, enter the raw event log text that contains the triggering conditions for the rule.
7. Under **Pause**, enter the number of seconds before the next test event will be sent, and click **+** under **Action** to enter additional test events.
   Create as many events as necessary to trigger the rule conditions.
8. Click **Test Rule**.
   If the test succeeds you are now ready to activate the rule.

Exporting and Importing Rule Definitions

Instead of using the user interface to define a rule, you can import rule definitions, or you can export a definition, modify it, and import it back into your FortiSIEM virtual appliance. Rule definitions follow an XML schema.

- Exporting a Rule Definition
- Importing a Rule Definition

Exporting a Rule Definition

Complete these steps to export a Rule Definition:

1. Go to **RESOURCES** > **Rule**.
2. Select the Rule Definition(s) to export from the table.
3. Click **Export** to download and save the Rule Definition.

Importing a Rule Definition

Complete these steps to import a Rule Definition:

1. Go to **RESOURCES** > **Rule**.
2. Select the Rule Definition(s) to import in XML format.
3. Click **Import** to import the Rule Definition.

Importing Sigma Rules

This section shows how you can import a new SIGMA rule into FortiSIEM. FortiSIEM will automatically convert the SIGMA rule format to FortiSIEM Rule format. Currently, this works for Windows rules. Other rules may work partially - you can download them and make modifications.

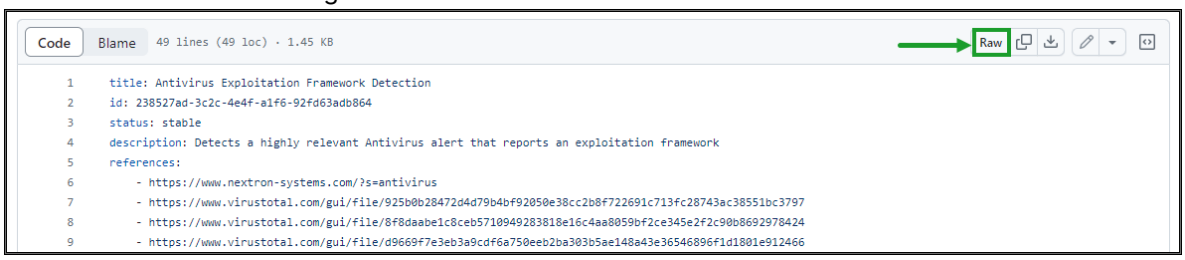
You can import in one of 3 ways:

- By providing the URL for the SIGMA Rule
- By uploading a SIGMA Rule File
- Custom Input

Importing via URL

For this method, you will provide the URL of the SIGMA Rule.

1. Go to the GitHub SIGMA rule repository and click on the SIGMA rule you want to import, e.g. https://github.com/SigmaHQ/sigma/blob/master/rules/windows/create_remote_thread/create_remote_thread_win_hktl_cactustorch.yml
2. Click the **Raw** icon on the right.



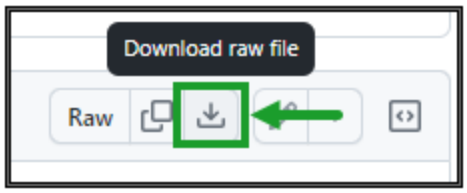
   This will take you to a web page that provides a link to the raw rule, e.g. https://raw.githubusercontent.com/SigmaHQ/sigma/master/rules/windows/create_remote_thread/create_remote_thread_win_hktl_cactustorch.yml
3. Copy the link to your clipboard.
4. Login to the FortiSIEM GUI.
5. Navigate to **Resources > Rules**.
6. From the **More** drop-down list, select **Import Sigma Rule**.
7. Choose the **URL** option.
8. Paste the link from your clipboard into the **URL** field.
9. Click **Import**.
10. If import succeeds, then you will see a message like "Import Rule <*Rule XYZ*> successful, view the rule?" Click **Yes** to save the file and be taken to Edit Rule page.
    Note: You can click **No** to save the rule without reviewing the rule conditions, but you should make sure to check the rule conditions at some point.

11. Go through the 3 tabs and make sure the import captured all aspects of the SIGMA rule. Special importance should be given to **Step 2: Define Condition > Filter**. See Defining Rule Conditions for more information.
12. Click **Save**.
13. A "The Rule has been changed" window will appear. You can click **OK** to overwrite the existing imported rule, or you can modify the rule name, then click **OK** to save as a new rule.

Importing via File

For this method, you will provide the SIGMA Rule file. This may be useful if your Supervisor does not have access to the GitHub SIGMA Rule Repository.

1. Go to the GitHub SIGMA rule repository and click on the SIGMA rule you want to import, e.g. https://github.com/SigmaHQ/sigma/blob/master/rules/windows/create_remote_thread/create_remote_thread_win_hktl_cactustorch.yml
2. Click the Download raw file icon on the right.



   This will download the file onto your workstation.
3. Login to the FortiSIEM GUI.
4. Navigate to **Resources > Rules**.
5. From the **More** drop-down list, select **Import Sigma Rule**.
6. Choose the **File** option and select the file you downloaded in Step 2.
7. Click **Import**.
8. If import succeeds, then you will see a message like "Import Rule <*Rule XYZ*> successful, view the rule?" Click **Yes** to save the file and be taken to Edit Rule page.
   Note: You can click **No** to save the rule without reviewing the rule conditions, but you should make sure to check the rule conditions at some point.
9. Go through the 3 tabs and make sure the import captured all aspects of the SIGMA rule. Special importance should be given to **Step 2: Define Condition > Filter**. See Defining Rule Conditions for more information.
10. Click **Save**.
11. A "The Rule has been changed" window will appear. You can click **OK** to overwrite the existing imported rule, or you can modify the rule name, then click **OK** to save as a new rule.

Importing via Custom Input

For this method, you will enter a SIGMA rule in YAML format in the **Custom Input** edit box.

1. Login to the FortiSIEM GUI.
2. Navigate to **Resources > Rules**.
3. From the **More** drop-down list, select **Custom Input**.
4. Enter in the rule in SIGMA YAML file format as specified here (https://sigmahq.io/docs/basics/rules.html).
5. Click **Import**.
6. If import succeeds, then you will see a message like "Import Rule <*Rule XYZ*> successful, view the rule?" Click **Yes** to save the file and be taken to Edit Rule page.
   Note: You can click **No** to save the rule without reviewing the rule conditions, but you should make sure to check the rule conditions at some point.
7. Go through the 3 tabs and make sure the import captured all aspects of the SIGMA rule. Special importance should be given to **Step 2: Define Condition > Filter**. See Defining Rule Conditions for more information.
8. Click **Save**.
9. A "The Rule has been changed" window will appear. You can click **OK** to overwrite the existing imported rule, or you can modify the rule name, then click **OK** to save as a new rule.

Networks

The Networks page lists the defined networks in your IT infrastructure.

- Adding a Network
- Modifying a Network
- Deleting a Network

Adding a Network

Complete these steps to add a network:

1. Go to **RESOURCES** > **Networks**.
2. Select a group where you want to add the Network group, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the following information:
   - **Name** - name of the network
   - **Low** - lower IP address of the network IP range
   - **High** - higher IP address of the network IP range
   - **Mask** - Subnet mask
5. Click **Save**.

Modifying a Network

Complete these steps to modify a network:

1. Go to **RESOURCES** > **Networks**.
2. Select the network to modify from the table.
3. Click **Edit**.
4. Modify the required information:
   - **Name** - name of the network
   - **Low** - lower IP address of the network IP range
   - **High** - higher IP address of the network IP range
   - **Mask** - Subnet mask
5. Click **Save**.

Deleting a Network

Complete these steps to delete a network:

1. Go to **RESOURCES** > **Networks**.
2. Select the network to modify from the table.
3. Click **Delete**.
4. Click **Yes** to delete the network or **Remove only from group** to just remove the network from the group.

Watch Lists

A Watch List is a smart container of similar items such as host names, IP addresses, or user names, that are of significant interest to an administrator and must be watched. Examples of watch lists that are already set up in FortiSIEM are:

- **Frequent Account Lockouts** - users who are frequently locked out
- **Host Scanners** - IP addresses that scan other devices
- **Disk space issues** - hosts with disks that are running out of capacity
- **Denied countries** - countries with an excessive number of access denials at the firewall
- **Blacklisted WLAN endpoints** - Endpoints that have been blacklisted by Wireless IPS systems

Items are added to a watch list dynamically when a rule is triggered, but you can also add items to a watch list manually. When you define a rule, you can also choose a watch list that will be populated with a specific incident attribute, and you can use watch lists as conditions while creating reports, as described in Using a Watch List. You can also define when an entry leaves a watch list - this is time based. For example, if the rule does not trigger for that attribute for defined time-period, then the entry is removed from the watch list. Watch lists are also multi-tenant aware, with organization IDs tracked in relation to watch list items.

The following section provides the procedures to use Watch Lists:

- System-defined Watch List
- Creating a Watch List
- Modifying a Watch List
- Using a Watch List
- Exporting and Importing Watch List

System-defined Watch List

FortiSIEM includes several pre-defined watch lists that are populated by system-defined rules.

Watch list	Description	Attribute Type	Triggering Rules
Accounts Locked	Domain accounts that are locked out frequently	User (STRING)	Account Locked: Domain
Application Issues	Applications exhibiting issues	Host Name (STRING)	IIS Virtual Memory Critical SQL Server Low Buffer Cache Hit Ratio SQL Server Low Log Cache Hit Ratio SQL Server Excessive Deadlock SQL Server Excessive Page Read/Write SQL Server Low Free Pages In Buffer Pool SQL Server Excessive Blocking Database Server Disk Latency Critical SQL Server Excessive Full Scan SQL Server scheduled job failed High Oracle Table Scan Usage High Oracle Non-System Table Space Usage Oracle database not backed up for 1 day Exchange Server SMTP Queue High Exchange Server Mailbox Queue High Exchange Server RPC Request High Exchange Server RPC Latency High Oracle DB Low Buffer Cache Hit Ratio Oracle DB Low Library Cache Hit Ratio Oracle DB Low Row Cache Hit Ratio Oracle DB Low Memory Sorts Ratio Oracle DB Alert Log Error Excessively Slow Oracle DB Query Excessively Slow SQL Server DB Query Excessively Slow MySQL DB Query
Availability Issues	Servers, networks or storage devices or Applications that are exhibiting availability issues	Host Name (STRING)	Network Device Degraded - Lossy Ping Response Network Device Down - No Ping Response Server Degraded - Lossy Ping Response Server Down - No Ping Response Server Network Interface Staying Down Network Device Interface Flapping Server Network Interface Flapping Important Process Staying Down Important Process Down Auto Service Stopped Critical network Interface Staying Down EC2 Instance Down Storage Port Down Oracle Database Instance Down

Watch list	Description	Attribute Type	Triggering Rules
			Oracle Listener Port Down MySQL Database Instance Down SQL Server Instance Down Service Staying Down - Slow Response To STM Service Down - No Response to STM Service Staying Down - No Response to STM
DNS Violators	Sources that send excessive DNS traffic or send traffic to unauthorized DNS gateways	Source IP	Excessive End User DNS Queries to Unauthorized DNS servers Excessive End User DNS Queries Excessive Denied End User DNS Queries Excessive Malware Domain Name Queries Excessive uncommon DNS Queries Excessive Repeated DNS Queries To The Same Domain
Denied Countries	Countries that are seeing a high volume of denials on the firewall	Destination Country (STRING)	Excessive Denied Connections From An External Country
Denied Ports	Ports that are seeing a high volume of denies on the firewall	Destination Port (INT)	Excessive Denied Connection To A Port
Environmental Issues	Environmental Devices that are exhibiting issues	Host name (String)	UPS Battery Metrics Critical UPS Battery Status Critical HVAC Temp High HVAC Temp Low HVAC Humidity High HVAC Humidity Low FPC Voltage THD High FPC Voltage THD Low FPC Current THD High FPC ground current high NetBoz Module Door Open NetBotz Camera Motion Detected Warning APC Trap Critical APC Trap
Hardware Issues	Servers, networks or storage devices	Host Name (String)	Network Device Hardware Warning Network Device Hardware Critical Server Hardware Warning

Watch list	Description	Attribute Type	Triggering Rules
	that are exhibiting hardware issues		Server Hardware Critical Storage Hardware Warning Storage Hardware Critical Warning NetApp Trap Critical Network Trap
Host Scanners	Hosts that scan other hosts	Source IP	Heavy Half-open TCP Host Scan Heavy Half-open TCP Host Scan On Fixed Port Heavy TCP Host Scan Heavy TCP Host Scan On Fixed Port Heavy UDP Host Scan Heavy UDP Host Scan On Fixed Port Heavy ICMP Ping Sweep Multiple IPS Scans From The Same Src
Mail Violators	End nodes that send too much mail or send mail to unauthorized gateways		Excessive End User Mail to Unauthorized Gateways Excessive End User Mail
Malware Found	Hosts where malware found by Host IPS /AV based systems and the malware is not remediated	Host Name (String)	Virus found but not remediated Malware found but not remediated Phishing attack found but not remediated Rootkit found Adware process found
Malware Likely	Hosts that are likely to have malware - detected by network devices and the determination is not as certain as host based detection	Source IP or Destination IP	Excessive Denied Connections From Same Src Suspicious BotNet Like End host DNS Behavior Permitted Blacklisted Source Denied Blacklisted Source Permitted Blacklisted Destination Denied Blacklisted Destination Spam/malicious Mail Attachment found but not remediated Spyware found but not remediated DNS Traffic to Malware Domains Traffic to Emerging Threat Shadow server list Traffic to Emerging Threat RBN list Traffic to Emerging Threat Spamhaus list Traffic to Emerging Threat Dshield list Permitted traffic from Emerging Threat Shadow server list

Watch list	Description	Attribute Type	Triggering Rules
			Permitted traffic from Emerging Threat RBN list Permitted traffic from Emerging Threat Spamhaus list Permitted traffic from Emerging Threat Dshield list
Port Scanners	Hosts that scan ports on a machine	Source IP	Heavy Half-open TCP Port Scan: Single Destination Heavy Half-open TCP Port Scan: Multiple Destinations Heavy TCP Port Scan: Single Destination Heavy TCP Port Scan: Multiple Destinations Heavy UDP Port Scan: Single Destination Heavy UDP Port Scan: Multiple Destinations
Policy Violators	End nodes exhibiting behavior that is not acceptable in typical Corporate networks	Source IP	P2P Traffic detected IRC Traffic detected P2P Traffic consuming high network bandwidth Tunneled Traffic detected Inappropriate website access Inappropriate website access - multiple categories Inappropriate website access - high volume Inbound clear text password usage Outbound clear text password usage Remote desktop from Internet VNC From Internet Long lasting VPN session High throughput VPN session Outbound Traffic to Public DNS Servers
Resource Issues	Servers, networks or storage devices that are exhibiting resource issues: CPU, memory, disk space, disk I/O, network I/O, virtualization resources - either at the system level or	Host Name (STRING)	High Process CPU: Server High Process CPU: Network High Process Memory: Server High Process Memory: Network Server CPU Warning Server CPU Critical Network CPU Warning Network CPU Critical Server Memory Warning Server Memory Critical Network Memory Warning Network Memory Critical

Watch list	Description	Attribute Type	Triggering Rules
	application level		Server Swap Memory Critical Server Disk space Warning Server Disk space Critical Server Disk Latency Warning Server Disk Latency Critical Server Intf Util Warning Server Intf Util Critical Network Intf Util Warning Network Intf Util Critical Network IPS Intf Util Warning Network IPS Intf Util Critical Network Intf Error Warning Network Intf Error Critical Server Intf Error Warning Server Intf Error Critical
			Virtual Machine CPU Warning Virtual Machine CPU Critical Virtual Machine Memory Swapping Warning Virtual Machine Memory Swapping Critical ESX CPU Warning ESX CPU Critical ESX Memory Warning ESX Memory Critical ESX Disk I/O Warning ESX Disk I/O Critical ESX Network I/O Warning ESX Network I/O Critical Storage CPU Warning Storage CPU Critical NFS Disk space Warning NFS Disk space Critical
			NetApp NFS Read/Write Latency Warning NetApp NFS Read/Write Latency Critical NetApp CIFS Read/Write Latency Warning NetApp CIFS Read/Write Latency Critical NetApp ISCSI Read/Write Latency Warning NetApp ISCSI Read/Write Latency Critical NetApp FCP Read/Write Latency Warning NetApp FCP Read/Write Latency Critical NetApp Volume Read/Write Latency Warning
			NetApp Volume Read/Write Latency Critical EqualLogic Connection Read/Write Latency Warning

Watch list	Description	Attribute Type	Triggering Rules
			EqualLogic Connection Read/Write Latency Critical Isilon Protocol Latency Warning
Routing Issues	Network devices exhibiting routing related issues	Host Name (STRING)	OSPF Neighbor Down EIGRP Neighbor down OSPF Neighbor Down
Scanned Hosts	Hosts that are scanned	Destination IP	Half-open TCP DDOS Attack TCP DDOS Attack Excessive Denied Connections to Same Destination
Vulnerable Systems	Systems that have high severity vulnerabilities from scanners	Host Name (STRING)	Scanner found severe vulnerability
Wireless LAN Issues	Wireless nodes triggering violations	MAC Address (String)	Rogue or Unsecure AP detected Wireless Host Blacklisted Excessive WLAN Exploits Excessive WLAN Exploits: Same Source

Creating a Watch List

Complete these steps to create a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select an existing group under **Watch Lists** folder or create a new Watch List group.

To create a new Watch List group:

1. Select **Watch Lists** folder from the left panel and click **+** above the **RESOURCES** groups.
2. In the **Create New Watch List** dialog box, select the **Organization** type.
3. Enter the information below:
   - **Group** - name of the Watch List group
   - **Description** - description about the Watch List group
   - **Type** - Watch List type - String, Number, IP, or Date
   - **Case Sensitive** - Select if the group name is case-sensitive
   - **Expired in** - time period in which the items will expire from the watch if there is no activity for that time

To create a new Watch List:

1. Select a Watch List and click **New**.
   In the **Add New Entry** dialog box, the **Watch List** and **Type** values are pre-populated based on the Watch List selection.
2. Enter the information below:
   - **Active** - select whether the Watch List will be active when it is created
   - **Value** - a value for the Watch List
   - **Description** - a description of the Watch List
   - **Expires** - time period in which the items will expire from the watch if there is no activity for that time
3. Click **Save**.

Modifying a Watch List

Complete these steps to modify a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select the Watch List to modify from the table.
3. Click **Edit** and make the required changes.
4. Click **Save**.

Use the **Delete** button to select and delete any Watch List(s) from the table.

Using a Watch List

- Adding Watch List to a Rule
- Using Watch Lists as Conditions in Rules and Reports

Adding Watch List to a Rule

You can now add your new watch list to a rule, so that when the rule is triggered, items will be added to the watch list.

1. Go to **RESOURCES** > **Rules**.
2. Select the rule where you want to add the watch list, and click **Edit**.
3. Go to the **Step 3: Define Action** page.
4. Click the edit icon for the **Watch List**.
5. For **Incident Attribute**, select the incident information you want to add to the watch list.
   Note: **Watch List Attribute Type Must Match Incident Attribute**- The Type that you set for the watch list must match the Incident Attribute Types for the rule. For example, if your watch list Type is IP, and the Incident Attribute Type for the rule is string, you will not be able to associate the watch list to the rule.
6. Move the watch list you want to add from **Available** to **Selected** list using the right arrow.
7. Click **Save**.
   The **Watch Lists** field value displays "Defined".

Using Watch Lists as Conditions in Rules and Reports

If you want to create a rule that refers to the attributes in a watch list, for example if you want to create a condition in which a **Source IP** listed in your **DNS Violators** watch list will trigger an incident.

1. Go to **RESOURCES** > **Reports** or **Rules** and select the rule or report where you want to use the watch list.
2. Click **Edit**.
3. Go to the **Step 2: Define Condition** page.
4. Under **Conditions** for the report in your rule sub-pattern, enter the watch list attribute you want to filter for in the **Attribute** field.
   For example, **Source IP**.
5. For **Operator**, select **IN**.

6. Click **... Select from CMDB** under **Value**, and browse the folders to select the watch list using the right arrow.
   For example, **DNS Violators**.
7. Click **OK** and continue creating your search criteria or rule sub pattern.

Exporting and Importing Watch Lists

- Exporting Watch Lists
- Importing Watch Lists

Exporting a Watch List

Complete these steps to export a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select the Watch List(s) to export from the table.
3. Click **Export**.
4. Select the file format as **PDF**, **RTF** or **CSV** and click **Generate**.
   "Export successful" message is displayed.
5. Click **Open Report File** to save the file.

Importing a Watch List

Complete these steps to import a Watch List:

1. Go to **RESOURCES** > **Watch Lists**.
2. Select the Watch List to modify from the table.
3. Click **Import**.
4. Select the file to import in CSV format and click **Import**.

Protocols

The Protocols page lists the protocols used by applications and devices to communicate with the FortiSIEM virtual appliance.

- Adding a Protocol
- Modifying a Protocol
- Deleting a Protocol

Adding a Protocol

Complete these steps to add a Protocol:

1. Go to **RESOURCES** > **Protocols**.
2. Select a group where you want to add the Network group, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the following information:
   a. **Name** - name of the protocol.
   b. **Description** - description about the protocol.
   c. **Protocol/Port(s)** - select the Protocol and Port from the drop-down.
   d. **Apps Group** - enter the group to associate with the Protocol.
5. Click **Save**.

Modifying a Protocol

Complete these steps to modify a Protocol:

1. Go to **RESOURCES** > **Protocols**.
2. Select the protocol to modify from the table.
3. Click **Edit**.
4. Modify the required information:
   - **Name** - name of the protocol.
   - **Description** - description about the protocol.
   - **Protocol/Port(s)** - protocol and port from the drop-down.
   - **Apps Group** - group to associate with the protocol.
5. Click **Save**.

Deleting a Protocol

Complete these steps to delete a Protocol:

1. Go to **RESOURCES** > **Protocols**.
2. Select the Protocol to delete from the table.
3. Click **Delete**.
4. Click **Yes** to confirm.

Event Types

The Event Types page lists the types of events that are collected for supported devices.

- Adding an Event Type
- Modifying an Event Type
- Deleting an Event Type

Adding an Event Type

Complete these steps to add an event type:

1. Go to **RESOURCES** > **Event Types**.
2. Select a group to add the new event to, or create a new one.
3. Click **New**.
4. Enter a **Name**, and **Description** for the event type.
5. Select the **Device Type** from the drop-down list to associate with this event type.
6. Select the level of **Severity** associated with this event type.
7. For **CVE IDs**, enter links to any vulnerabilities associated with this event type as cataloged by the National Vulnerability Database.
8. Click **Save**.

Modifying an Event Type

Complete these steps to modify an Event Type:

1. Go to **RESOURCES** > **Event Types**.
2. Select the Event Type to modify from the table.
3. Click **Edit** to modify any settings.
4. Click **Save**.

Deleting an Event Type

Complete these steps to delete an Event Type:

1. Go to **RESOURCES** > **Event Types**.
2. Select the Event Type group from the folder structure on the left panel.
3. Select the Event Type from the table and click **Delete** to delete.
4. Confirm whether to **Remove only from group** or to remove completely by clicking **Yes**.

Working with AlienVault OTX

This section describes how to configure FortiSIEM to work with AlienVault OTX malware domains, IPs, URLs, and hashes with Taxii 2.1 integration.

- Working with AlienVault OTX Malware Domains
- Working with AlienVault OTX Malware IPs
- Working with AlienVault OTX Malware URLs
- Working with AlienVault OTX Malware Hash

Working with AlienVault OTX Malware Domains

- Enabling the AlienVault OTX Service
- Disabling the AlienVault OTX Service
- AlienVault OTX Malware Domain Values

Enabling the AlienVault OTX Service

To start the AlienVault OTX service, follow these steps once you have defined the feeds:

1. Go to **RESOURCES > Malware Domains>** select the OTX service you defined.
2. Click **More > Update**. In the **Update Malware Domain** dialog box, click **+** to schedule the starting of the service. See Specifying a schedule.
3. Click **Save**.

Disabling the AlienVault OTX Service

To stop the AlienVault OTX service, follow these steps:

1. Go to **RESOURCES > Malware Domains** and select the **Malware Domain** folder with your AlienVault OTX service.
2. Click **More > Update**.
3. Select an existing schedule.
4. Delete the existing schedule.
5. Repeat steps 3 through 4 until all schedules have been removed.
6. Click **Save**.

AlienVault OTX Malware Domain Values

After creating a group/folder for AlienVault, select the group/folder, click **More > Update**, select **Update via API**, click the edit icon next to **URL**, and use the following values to configure AlienVault OTX Malware Domains for FortiSIEM, then click **Save**.

Parameter	Value
URL	https://otx.alienvault.com/taxii/root
User Name	<user> (Your API key)
Password	Not required. (Not necessary to put anything here, password is ignored)
Plugin Class	com.accelops.service.threatfeed.impl.Stix2MalwareDomainUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with AlienVault OTX Malware IPs

For AlienVault OTX Malware IPs, go to **RESOURCES > Malware IPs,** and repeat the same steps as for **AlienVault OTX Malware Domains**.

Use the following values to configure AlienVault OTX Malware IPs for FortiSIEM.

Parameter	Value
URL	https://otx.alienvault.com/taxii/root
User Name	<user> (Your API key)
Password	Not required. (Not necessary to put anything here, password is ignored)
Plugin Class	com.accelops.service.threatfeed.impl.Stix2MalwareIPUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with AlienVault OTX Malware URLs

For AlienVault OTX Malware URLs, go to **RESOURCES > Malware URLs,** and repeat the same steps as for **AlienVault OTX Malware Domains**.

Use the following values to configure AlienVault OTX Malware URLs for FortiSIEM.

Parameter	Value
URL	https://otx.alienvault.com/taxii/root
User Name	<user> (Your API key)
Password	Not required. (Not necessary to put anything here, password is ignored)
Plugin Class	com.accelops.service.threatfeed.impl.Stix2MalwareUrlUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with AlienVault OTX Malware Hash

For AlienVault OTX Malware Hash, go to **RESOURCES > Malware Hash,** and repeat the same steps as for **AlienVault OTX Malware Domains**.

Use the following values to configure AlienVault OTX Malware Hash for FortiSIEM.

Parameter	Value
URL	https://otx.alienvault.com/taxii/root
User Name	<user> (Your API key)
Password	Not required. (Not necessary to put anything here, password is ignored)
Plugin Class	com.accelops.service.threatfeed.impl.Stix2MalwareHashUpdateService
Data Format	Select STIX/TAXII Format
Collection	user_AlienVault
Data Update	Select Full

Working with Custom Threat Feeds that use HTTPS Connectivity

When integrating with a Custom Threat Feed that provides IoC over an HTTPS connection, for example a STIX/TAXII feed, or connecting to a web server hosting a CSV file, the web server Certificate must be imported into FortiSIEM key store. Please follow the steps here from the Configuring CA Certificates Guide to import the certificate into the key store.

Working with Dragos IOCs

The following sections describe how to work with Dragos Worldview malware malware domains, IPs, and hashes.

- Download Dragos Worldview Malware Domains
- Download Dragos Worldview Malware IPs
- Download Dragos Worldview Malware Hashes

Download Dragos Worldview Malware Domains

1. Go to **RESOURCES > Malware Domains** and select the **Dragos Worldview Malware Domain** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your Dragos credentials to complete the **URL**, **API Token**, and **API Secret** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **Custom** is supported.
6. Select a **Data Update** process. Selecting Full means FortiSIEM will download all data. If Incremental is selected, FortiSIEM will download from the latest recorded update date.
7. Click **Save**.
8. Schedule the download. See Specifying a Schedule.
9. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Download Dragos Worldview Malware IPs

1. Go to **RESOURCES > Malware IPs**, select the **Dragos Worldview Malware IP** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your Dragos credentials to complete the **URL**, **API Token**, and **API Secret** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **Custom** is supported.
6. Select a **Data Update** process. Selecting Full means FortiSIEM will download all data. If Incremental is selected, FortiSIEM will download from the latest recorded update date.
7. Click **Save**.
8. Schedule the download. See Specifying a Schedule.
9. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Download Dragos Worldview Malware Hashes

1. For Dragos Worldview hash, go to **RESOURCES > Malware Hash** , select the **Dragos Worldview Malware Hash** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your Dragos credentials to complete the **URL**, **API Token**, and **API Secret** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **Custom** is supported.
6. Select a **Data Update** process. Selecting Full means FortiSIEM will download all data. If Incremental is selected, FortiSIEM will download from the latest recorded update date.
7. Click **Save**.
8. Schedule the download. See Specifying a Schedule.
9. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Specifying a Schedule

1. Click the **+** icon next to **Schedule**.
2. Enter values for the following options:
   - **Time Range** specifies start time (within the day) and the duration of the scheduling window. Select a UTC time and a corresponding location from the drop-down lists.
   - **Recurrence Pattern** specifies if and how the window will repeat.
     - If you are scheduling for one time only:
       a. Select **Once** for **Recurrence Pattern**.
       b. Select the specific date in **Start From**.
     - If you are scheduling for hourly:
       a. Enter the hourly interval.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Daily**:
       a. Select the interval of days or **Every weekday**.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Weekly**:
       a. Select the interval of weeks or select particular days of the week.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Monthly**:
       a. Select the days and months from the drop-down lists.
       b. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.

3. Click **Save** to apply the changes.

Working with FortiGuard IOCs

The following sections describe how to work with FortiGuard malware domains, IPs, and URLs.

- Working with FortiGuard Malware Domains
- Working with FortiGuard Malware IPs
- Working with FortiGuard Malware URLs
- Internet Connectivity Requirements

Working with FortiGuard Malware Domains

The following sections describe how to enable, disable, and setup a proxy for the FortiGuard Malware domain.

- Enabling the FortiGuard IOC Service
- Disabling the FortiGuard IOC Service
- Using a Proxy for the FortiGuard IOC Service

Enabling the FortiGuard IOC Service

To start the FortiGuard IOC service, follow these steps:

1. Go to **RESOURCES > Malware Domains** and select the **FortiGuard Malware Domain** folder.
2. Select an inactive domain from the table.
3. Click **More > Update**. In the **Update FortiGuard IOC Service** dialog box, select **Enable IOC Service**.
4. (Optional) Schedule the starting of the service. See Specifying a schedule.
5. Click **Save**.

Disabling the FortiGuard IOC Service

To stop the FortiGuard IOC service, follow these steps:

1. Go to **RESOURCES > Malware Domains** and select the **FortiGuard Malware Domain** folder.
2. Select an active domain from the table.
3. Click **More > Update**. In the **Update FortiGuard IOC Service** dialog box, select **Disable IOC Service**.
4. Click **Save**.

Using a Proxy for the FortiGuard IOC Service

Follow these steps to use a proxy for the FortiGuard IOC service:

1. Go to **RESOURCES > Malware Domains** and select the **FortiGuard Malware Domain** folder.
2. Select a domain from the table.
3. Click **More > Update**. In the **Update FortiGuard IOC Service** dialog box, select **Use Proxy**.
4. The **Mode** will be **Proxy**. Provide the following information:
   a. **IP/Host**
   b. **Port**
   c. **User Name**
   d. **Password**
5. Click **Save**.

Working with FortiGuard Malware IPs

For FortiGuard Malware IPs, go to **RESOURCES > Malware IPs**, select the **FortiGuard Malware IP** folder, and repeat the same steps as for **FortiGuard Malware Domains**.

Working with FortiGuard Malware URLs

For FortiGuard Malware URLs, go to **RESOURCES > Malware URLs**, select the **FortiGuard Malware URL** folder, and repeat the same steps as for **FortiGuard Malware Domains**.

Working with Malware Patrol

The following section describes how to configure Malware Patrol with FortiSIEM for Malware Domains, Malware IPs, Malware Hashes, and Malware URLs. Additional information is available on the Malware Patrol website https://www.malwarepatrol.net/tech-support/.

- Configuring Malware Patrol Malware Domains
- Configuring Malware Patrol Malware IPs
- Configuring Malware Patrol Malware Hashes
- Configuring Malware Patrol Malware URLs

Configuring Malware Patrol Malware Domains

To configure Malware Patrol Malware Domains, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware Domains**.
3. In the left pane, click the **+** icon and create a group named “Malware Patrol”.
4. Select the **Malware Patrol** folder you just created.
5. Click **More > Update**. In the **Update Malware** dialog box, select **Update via API**.
6. In the **URL** row, click the Edit icon.
7. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.
8. In the **Username** field, enter your Malware Patrol username.
9. In the **Password** field, enter the password associated with your Malware Patrol username.
10. In the **Plugin Class** field, enter:
    `com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService`
11. For **Field Separator**, enter a comma, by inputting the "," character.
12. For **Data Format**, select **CSV**.
    Note: Currently, only CSV is supported.
13. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
14. For **Data Mapping**, add your Mapped fields. The following is an example.
    - Domain Name, set to Position 1.
    - Malware Type, set to Position 2.
    - Description, set to Position 3.
    - Date Found, set to Position 4.
    - Last Seen, set to Position 5.
15. Click **Save**.
16. Schedule the download. See Specifying a Schedule.
17. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Configuring Malware Patrol Malware IPs

To configure Malware Patrol Malware IPs, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware IPs**.
3. In the left pane, click the **+** icon and create a group name “Malware Patrol”.
4. Click **Save**.
5. Select the **Malware Patrol** folder you just created.
6. Click **More > Update**. In the **Update Malware IP** dialog box, select **Update via API**.
7. In the **URL** row, click the Edit icon.
8. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.
9. In the **Username** field, enter your Malware Patrol username.
10. In the **Password** field, enter the password associated with your Malware Patrol username.
11. In the **Plugin Class** field, enter:
    `com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService`
12. For **Field Separator**, enter a comma, by inputting the "," character.
13. For **Data Format**, select **CSV**.
    Note: Currently, only CSV is supported.
14. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
15. For **Data Mapping**, add your Mapped fields. The following is an example.
    - Name, set to Position 1.
    - Low IP , set to Position 2.
    - High IP, set to Position 3.
    - Malware Type, set to Position 4.
    - Description, set to Position 5.
    - Date Found, set to Position 6.
    - Last Seen, set to Position 7.
16. Click **Save**.
17. Schedule the download. See Specifying a Schedule.
18. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Configuring Malware Patrol Malware Hashes

To configure Malware Patrol Malware Hashes, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware Hash**.
3. In the left pane, click the **+** icon and create a group name “Malware Patrol”.
4. Click **Save**.

5. Select the **Malware Patrol** folder you just created.
6. Click **More > Update**. In the **Update Malware Hash** dialog box, select **Update via API**.
7. In the **URL** row, click the Edit icon.
8. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.
9. In the **Username** field, enter your Malware Patrol username.
10. In the **Password** field, enter the password associated with your Malware Patrol username.
11. In the **Plugin Class** field, enter:
`com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService`
12. For **Field Separator**, enter a comma, by inputting the "," character.
13. For **Data Format**, select **CSV**.
Note: Currently, only CSV is supported.
14. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
15. For **Data Mapping**, add your Mapped fields. The following is an example.
    - Description, set to Position 1.
    - Algorithm, set to Position 2.
    - HashCode, set to Position 3.
    - Malware Type, set to Position 4.
    - Date Found, set to Position 5.
    - Last Seen, set to Position 6.
16. Click **Save**.
17. Schedule the download. See Specifying a Schedule.
18. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Configuring Malware Patrol Malware URLs

To configure Malware Patrol Malware URLs, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **RESOURCES > Malware URLs**.
3. In the left pane, click the **+** icon and create a group name “Malware Patrol”.
4. Click **Save**.
5. Select the **Malware Patrol** folder you just created.
6. Click **More > Update**. In the **Update Malware Url** dialog box, select **Update via API**.
7. In the **URL** row, click the Edit icon.
8. In the **URL** field, enter the URL of the threat feed as provided via the Malware Patrol portal.
9. In the **Username** field, enter your Malware Patrol username.
10. In the **Password** field, enter the password associated with your Malware Patrol username.
11. In the **Plugin Class** field, enter:
`com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService`
12. For **Field Separator**, enter a comma, by inputting the "," character.
13. For **Data Format**, select **CSV**.
Note: Currently, only CSV is supported.

14. Select a **Data Update** process. Selecting **Full** means FortiSIEM will download all data. If **Incremental** is selected, FortiSIEM will download from the latest recorded update date.
15. For **Data Mapping**, add your Mapped fields. The following is an example.
    - URL, set to Position 1.
    - Malware Type, set to Position 2.
    - Last Seen, set to Position 3.
16. Click **Save**.
17. Schedule the download. See Specifying a Schedule.
18. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed.

Working with MISP Threatfeeds

MISP is an open source threat sharing web application to facilitate automated centralization of threats. MISP also hosts an API where you can export threats to products such as FortiSIEM.

- MISP Server Setup
- FortiSIEM Setup

MISP Server Setup

- Prerequisites
- Limitations
- Create API Key

Prerequisites

Your MISP server must have configured data ingestion that includes attributes (ip-src, url, domain, or sha256).

FortiSIEM uses the following API to query the MISP server for threatfeed indicators:

- /attributes/restSearch

The following attributes are searchable to ingest as indicators depending on if you configured a malware IP, domain, URL, or hash ingestion in FortiSIEM:

- ip-src
- domain
- url
- sha256

The following categories of attributes are checked during the threatfeed ingest:

- Network activity
- Payload activity

To view available attributes in your MISP server, click the Home button -> List Attributes.

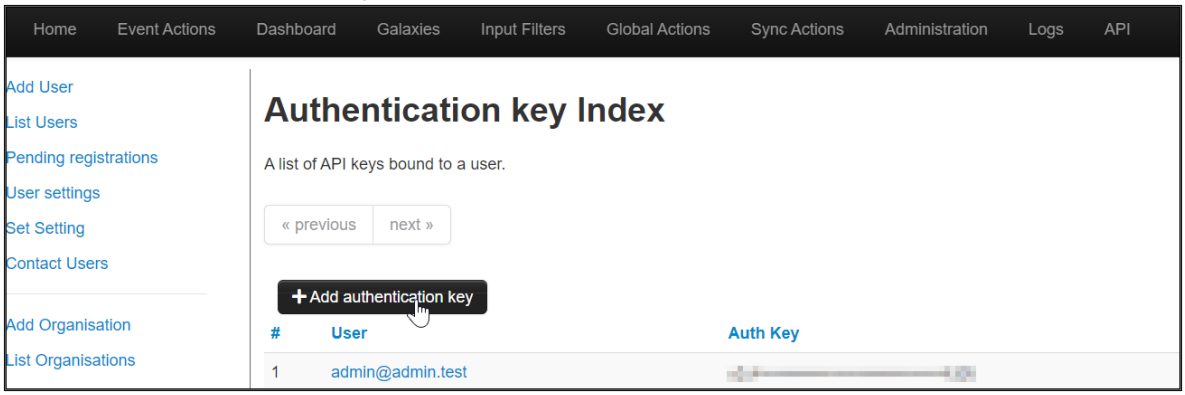
Limitation

FortiSIEM only queries new attributes seen in the last 7 days.

Create API Key

To create an API Key, take the following steps.

1. Login to the MISP server.
2. Go to **Administration > List Auth Keys**.
3. Click **+Add authentication key**.



4. Save the authentication key as it will be needed later in the FortiSIEM configuration.

FortiSIEM Setup

After the MISP Server Setup, take the following steps to configure FortiSIEM.

- Malware IP Setup
- Malware URL Setup
- Malware Domain Setup
- Malware Hash Setup

Malware IP Setup

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware IPs > MISP IP**.
3. Select **More** and click **Update**.
   a. Select the Edit Icon next to URL.
   b. On the Update Malware IP window, take the following steps.
      i. Click the **Update via API** radio button.
      ii. In the **Plugin Type** row, click the **Python** radio button.
      iii. In the **URL** field, enter the base URL of your MISP server.
      iv. Leave the **User Name** field blank.
      v. In the **Password** field, enter/paste the authentication key you created earlier.

vi. (Optional) Enable (default) SSL Verify, or disable SSL verification for your MISP server.
vii. From the **Plugin Name** drop-down list, select **misp_threatfeed.py**.
viii. Click **Full** for the **Data Update** radio button.
ix. Click **Save**.

c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.
d. Confirm after the schedule has run (after a few minutes), that data is ingested.

Malware URL Setup

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware URLs > MISP IP**.
3. Select **More** and click **Update**.
   a. Select the Edit Icon next to URL.
   b. On the Update Malware URL window, take the following steps.
      i. Click the **Update via API** radio button.
      ii. In the **Plugin Type** row, click the **Python** radio button.
      iii. In the **URL** field, enter the base URL of your MISP server.
      iv. Leave the **User Name** field blank.
      v. In the **Password** field, enter/paste the authentication key you created earlier.
      vi. (Optional) Enable (default) SSL Verify, or disable SSL verification for your MISP server.
      vii. From the **Plugin Name** drop-down list, select **misp_threatfeed.py**.
      viii. Click **Full** for the **Data Update** radio button.
      ix. Click **Save**.
   c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.
   d. Confirm after the schedule has run (after a few minutes), that data is ingested.

Malware Domain Setup

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware Domains > MISP Domain**.
3. Select **More** and click **Update**.
   a. Select the Edit Icon next to URL.
   b. On the Update Malware Domain window, take the following steps.
      i. Click the **Update via API** radio button.
      ii. In the **Plugin Type** row, click the **Python** radio button.
      iii. In the **URL** field, enter the base URL of your MISP server.
      iv. Leave the **User Name** field blank.

v. In the **Password** field, enter/paste the authentication key you created earlier.
vi. (Optional) Enable (default) SSL Verify, or disable SSL verification for your MISP server.
vii. From the **Plugin Name** drop-down list, select **misp_threatfeed.py**.
viii. Click **Full** for the **Data Update** radio button.
ix. Click **Save**.

c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.
d. Confirm after the schedule has run (after a few minutes), that data is ingested.

Malware Hash Setup

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware Hash > Malware Hash > MISP Malware Hash**.
3. Select **More** and click **Update**.
   a. Select the Edit Icon next to URL.
   b. On the Update Malware Hash window, take the following steps.
      i. Click the **Update via API** radio button.
      ii. In the **Plugin Type** row, click the **Python** radio button.
      iii. In the **URL** field, enter the base URL of your MISP server.
      iv. Leave the **User Name** field blank.
      v. In the **Password** field, enter/paste the authentication key you created earlier.
      vi. (Optional) Enable (default) SSL Verify, or disable SSL verification for your MISP server.
      vii. From the **Plugin Name** drop-down list, select **misp_threatfeed.py**.
      viii. Click **Full** for the **Data Update** radio button.
      ix. Click **Save**.
   c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.
   d. Confirm after the schedule has run (after a few minutes), that data is ingested.

Working with OpenCTI Threatfeeds

OpenCTI is an opensource threat intel platform that facilitates centralized data sharing and information. One primary item of interest is the IP, Domain, URL, and Hash Indicators. If you have a list of any such indicators in your own OpenCTI server, it supports exporting these to other appliances such as FortiSIEM via TAXII2.1 threatfeeds.

Terminology Notes:

Indicator: These are IP, domain, URL, or hash objects that indicate the presence of a threat. Observables are typically promoted to indicator status if there is a high likelihood that observable is a threat.

Observable: An object of interest observed in your or others environment, but may not necessarily indicate a threat, such as network addresses, domains, URLs, or hashes.

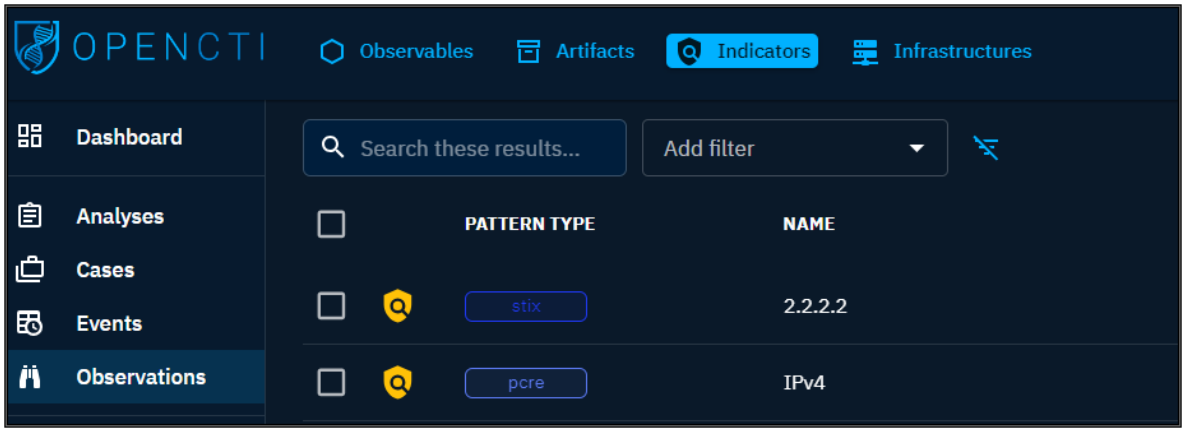
FortiSIEM supports ingesting indicators only from OpenCTI.

- OpenCTI Threatfeeds Setup
- FortiSIEM Setup
- Troubleshooting

OpenCTI Threatfeeds Setup

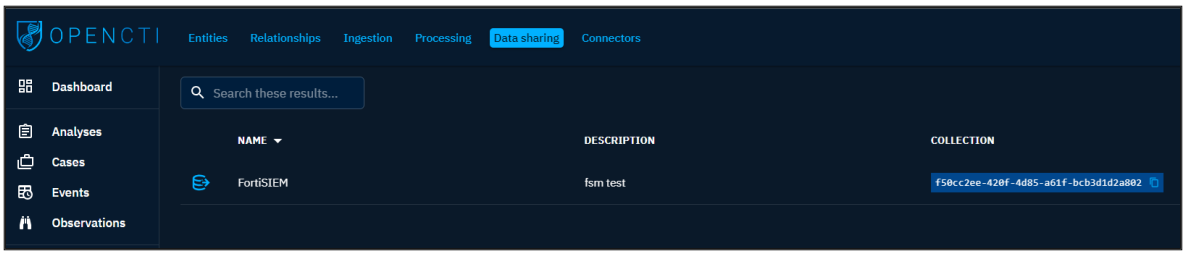
From an OpenCTI server, take the following steps.

1. Ensure you have at least one observable.

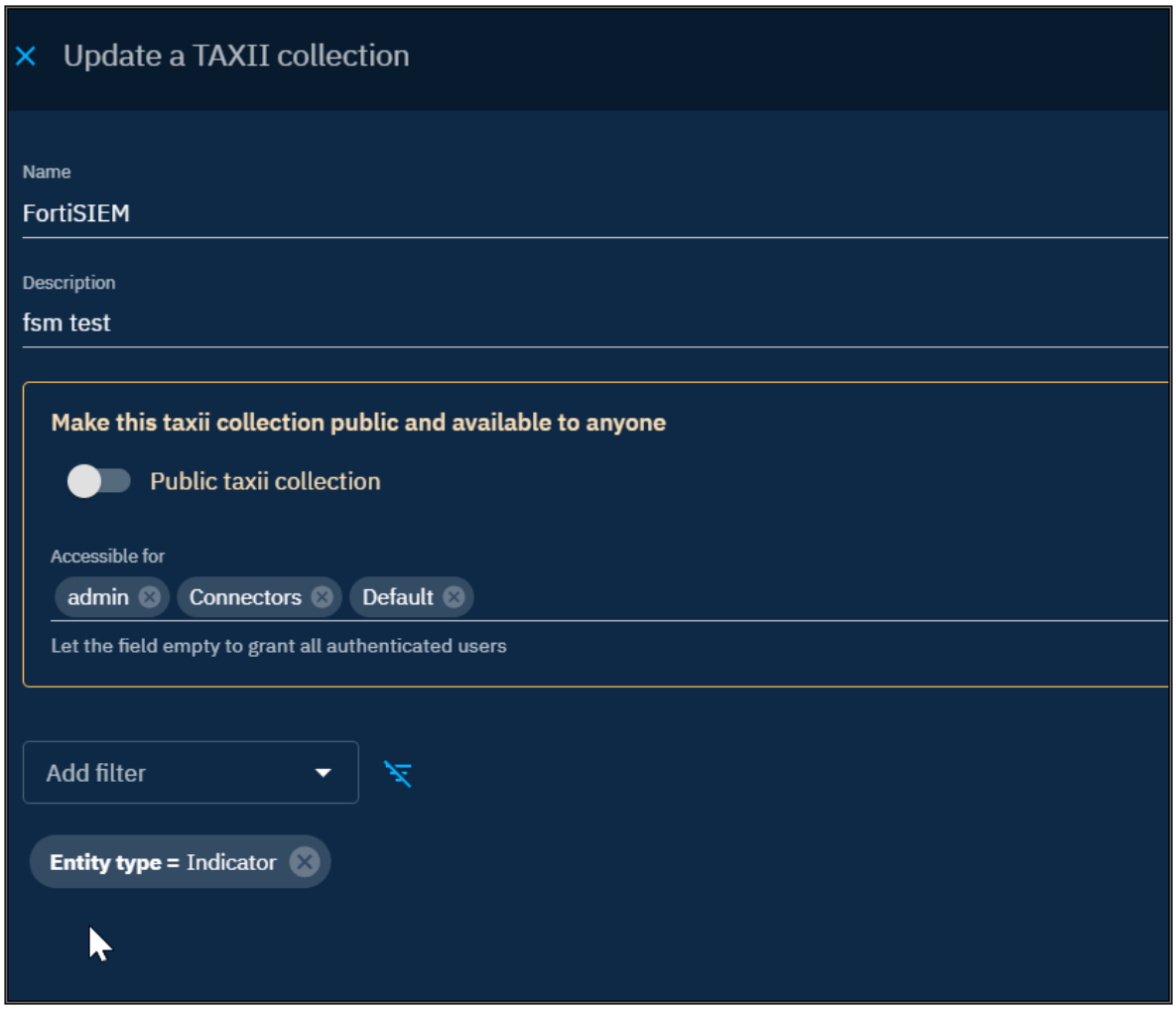


2. Login to OpenCTI Server.

3. Navigate to **Data > Data Sharing > TAXII collections**.



4. At the bottom right, click **+** to add a new entry.
5. In the **Name** field, enter a name, for example, "FortiSIEM".
6. In the **Add filter** field, enter "Entity type = Indicator".



7. Click **Create**.

8. Note the COLLECTION ID.

The TAXII Feed you will input into FortiSIEM will be in the format:
`https://<ip or fqdn>:<port>/taxii2/root/collections/<collectionId>/objects`
Replace each <*field*> with the appropriate value based on your OpenCTI Server.

FortiSIEM Setup

After the OpenCTI Threatfeeds Setup, take the following steps to configure FortiSIEM.

- Malware IP Setup
- Malware URL Setup
- Malware Domain Setup
- Malware Hash Setup

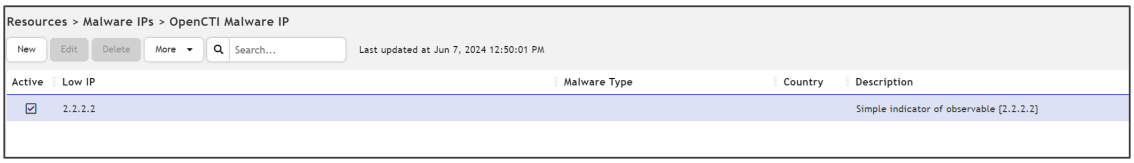
Malware IP Setup

Note: You will repeat this step for each type of indicator you want to receive. The `taxii2` feed example from OpenCTI Threatfeeds Setup will export all feed types, so the same URL is used for Malware IP, Malware URL, Malware Domains, and Malware Hash.

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware IPs > OpenCTI Malware IP**.
3. Select **More** and click **Update**.
   a. Select the Edit Icon next to the sample URL.
   b. On the Update Malware IP window, take the following steps.
      i. In the **URL** field, update the URL with your URL for your TAXII2.1 feed on your OpenCTI server.
      Sample URL:
      `https://<YourOpenCTIURL>/taxii2/root/collections/<collectionID>/objects`
      Note: The URL path may not be exactly the same, but should end with a `collectionID/objects`.
      ii. In the **User Name** field, enter the username used to access the OpenCTI server.
      iii. In the **Password** field, enter the password associated with the username.
      Note: Optionally, check if you'd like to enable SSL Certificate validation (Recommended, but requires your OpenCTI server use a public CA signed SSL/TLS certificate.
      iv. Click **Save**.

c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.

d. Confirm after the schedule has run (after a few minutes), that data is ingested.



Malware URL Setup

Note: You will repeat this step for each type of indicator you want to receive. The `taxii2` feed example from OpenCTI Threatfeeds Setup will export all feed types, so the same URL is used for Malware IP, Malware URL, Malware Domains, Malware Hash.

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware URLs > OpenCTI Malware URL**.
3. Select **More** and click **Update**.
   a. Select the Edit Icon next to the sample URL.
   b. On the Update Malware URL window, take the following steps.
      i. In the **URL** field, update the URL with your URL for your TAXII2.1 feed on your OpenCTI server.
      Sample URL:
      `https://<YourOpenCTIURL>/taxii2/root/collections/<collectionID>/objects`
      Note: The URL path may not be exactly the same, but should end with a `collectionID/objects`.
      ii. In the **User Name** field, enter the username used to access the OpenCTI server.
      iii. In the **Password** field, enter the password associated with the username.
      Note: Optionally, check if you'd like to enable SSL Certificate validation (Recommended, but requires your OpenCTI server use a public CA signed SSL/TLS certificate.
      iv. Click **Save**.
   c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.
   d. Confirm after the schedule has run (after a few minutes), that data is ingested.

Malware Domain Setup

Note: You will repeat this step for each type of indicator you want to receive. The `taxii2` feed example from OpenCTI Threatfeeds Setup will export all feed types, so the same URL is used for Malware IP, Malware URL, Malware Domains, Malware Hash.

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware Domains > OpenCTI Malware Domain**.

3. Select **More** and click **Update**.
   a. Select the Edit Icon next to the sample URL.
   b. On the Update Malware Domain window, take the following steps.
      i. In the **URL** field, update the URL with your URL for your TAXII2.1 feed on your OpenCTI server.
      Sample URL:
      `https://<YourOpenCTIURL>/taxii2/root/collections/<collectionID>/objects`
      Note: The URL path may not be exactly the same, but should end with a `collectionID/objects`.
      ii. In the **User Name** field, enter the username used to access the OpenCTI server.
      iii. In the **Password** field, enter the password associated with the username.
      Note: Optionally, check if you'd like to enable SSL Certificate validation (Recommended, but requires your OpenCTI server use a public CA signed SSL/TLS certificate.
      iv. Click **Save**.
   c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.
   d. Confirm after the schedule has run (after a few minutes), that data is ingested.

Malware Hash Setup

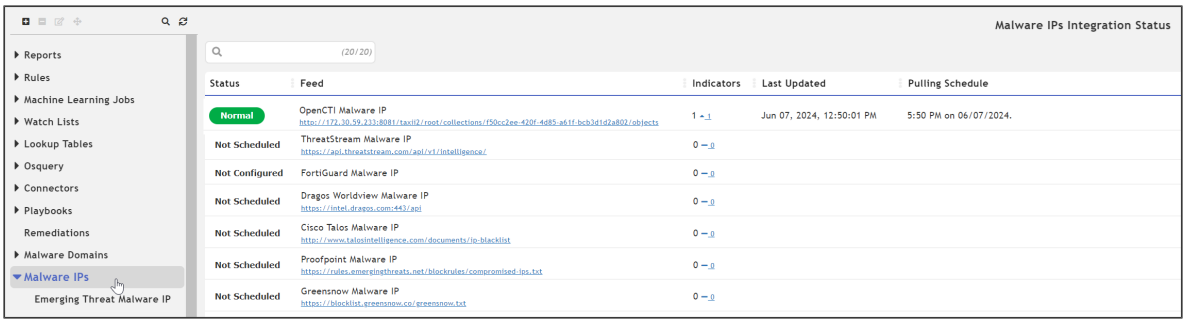
Note: You will repeat this step for each type of indicator you want to receive. The `taxii2` feed example from OpenCTI Threatfeeds Setup will export all feed types, so the same URL is used for Malware IP, Malware URL, Malware Domains, Malware Hash.

1. Login to FortiSIEM.
2. Navigate to **Resources > Malware Hash > Malware Hash > OpenCTI Malware Hash**.
3. Select **More** and click **Update**.
   a. Select the Edit Icon next to the sample URL.
   b. On the Update Malware Hash window, take the following steps.
      i. In the **URL** field, update the URL with your URL for your TAXII2.1 feed on your OpenCTI server.
      Sample URL:
      `https://<YourOpenCTIURL>/taxii2/root/collections/<collectionID>/objects`
      Note: The URL path may not be exactly the same, but should end with a `collectionID/objects`.
      ii. In the **User Name** field, enter the username used to access the OpenCTI server.
      iii. In the **Password** field, enter the password associated with the username.
      Note: Optionally, check if you'd like to enable SSL Certificate validation (Recommended, but requires your OpenCTI server use a public CA signed SSL/TLS certificate.
      iv. Click **Save**.
   c. At the **Schedule** row, click **+** to add a schedule. Fortinet recommends a Daily schedule for the **Recurrence Pattern**, but for an initial test, you can create a **Once** time schedule. After configuring your schedule, click **Save**.
   d. Confirm after the schedule has run (after a few minutes), that data is ingested.

Troubleshooting

The vast majority of the time with OpenCTI, if the threatfeed pull succeeded without errors, likely no indicators exist of that type in OpenCTI. Check your OpenCTI server for applicable indicators.

1. To view Threatfeed execution history, click the top level folder for that threatfeed type, in this case **Malware IPs**.



2. See that OpenCTI **Status** is “Normal”, indicating the last event pull was successful, if you see this but no data, likely the OpenCTI does not have any indicators of type IPv4 or IPv6.

Working with ThreatConnect IOCs

ThreatConnect can provide malware IPs, domains, hashes, or URLs which FortiSIEM can use to match in log data The steps are as follows: for each IOC (IP, domain, hash, URL).

1. Discover Collections
2. Create Collection Policy
3. Schedule IOC Download

Since an Organization may subscribe to many Collections (an intelligence source), downloading every IOC for all Collections may result in too much data. Therefore, specifying a Collection Policy is essential.

Download ThreatConnect Malware Domains

1. Go to **RESOURCES > Malware Domains** and select the **ThreatConnect Malware Domain** folder.
2. Click **More > Update**. In the **Update Malware** dialog box, then select **Update via API**.
3. Use your ThreatConnect credentials to complete the **URL**, **User name**, and **Password** fields.
4. **Plugin Class** is provided by default.
5. Select a **Data Format**. In this release, only **STIX-TAXII** is supported.
6. Enter an **Organization** name that is defined in your ThreatConnect account.
7. Define a **Collection**.
8. Click **Discover Collections** to expose all of the collections you are eligible to use.
9. Select a collection policy in the table and click **Edit**.
10. Edit any of the following values in the **Edit Collection Policy** dialog box:
    - **Enabled**: select whether the collection policy is enabled
    - **Collection**: edit the collection name
    - **Tag**: enter an optional user-defined tag for the collection
    - **Max False Positive Count**: enter a number where the frequency of an attack produces a false positive on your network.
    - **Min Rating**: enter a value between 0 and 5.
    - **Confidence**: enter a value between 1 and 100.
11. Click **Save**.
12. Schedule the download. See Specifying a Schedule.
13. Check the folder 5 minutes after the scheduled time. Downloaded results should be displayed – organized by each collection.

Note that FortiSIEM does not provide system rules and reports because ThreatConnect folders are dynamic. The user must create them using the Collection folders.

Download Other ThreatConnect IOCs

For ThreatConnect Malware IP, go to **RESOURCES > Malware IPs**, select the **ThreatConnect Malware IP** folder, and repeat the same steps as for **Malware Domains**.

For ThreatConnect Malware URL, go to **RESOURCES > Malware URLs**, select the **ThreatConnect Malware URL** folder, and repeat the same steps as for **Malware Domains**.

For ThreatConnect Malware hash, go to **RESOURCES > Malware Hash** , select the **ThreatConnect Malware Hash** folder and repeat the same steps as for **Malware Domains**.

Specifying a Schedule

1. Click the **+** icon next to **Schedule**.
2. Enter values for the following options:
   - **Time Range** specifies start time (within the day) and the duration of the scheduling window. Select a Start time, a UTC (or Local) and a corresponding location from the drop-down lists.
   - **Recurrence Pattern** specifies if and how the window will repeat.
     - If you are scheduling for one time only:
       i. Select **Once** for **Recurrence Pattern**.
       ii. Select the specific date in **Start From**.
     - If you are scheduling for hourly:
       i. Enter the hourly interval.
       ii. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Daily**:
       i. Select the interval of days or **Every weekday**.
       ii. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Weekly**:
       i. Select the interval of weeks or select particular days of the week.
       ii. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
     - If you are scheduling for **Monthly**:
       i. Select the days and months from the drop-down lists.
       ii. Select the **Start From** date for **Recurrence Range**, then either **End after** the number of occurrences, and **End by** date, or **No end date** to continue the recurrence forever.
3. Click **Save** to apply the changes.

Malware Domains

The Malware Domains page lists domains that are known to generate spam, host botnets, create DDoS attacks, and generally contain malware. Since Malware Domains are constantly changing, FortiSIEM recommends maintaining a dynamically generated list of IP addresses provided by services that are updated on a regular schedule, but you can also add or remove blocked IP addresses from these system-defined groups, and create your own groups based on manual entry of IP addresses or file upload. A Python Threat Feed Framework is also available, see here.

The following sections describe Malware Domains:

- Adding a Malware Domain
- Modifying a Malware Domain
- Deleting a Malware Domain
- Importing Malware Domains
- Viewing Malware Domains

Adding a Malware Domain

Complete these steps to add a Malware domain:

1. Go to **RESOURCES** > **Malware Domains**.
2. Select a group where you want to add the Malware Domains, or create a new one by clicking **+** above the **RESOURCES** groups. To create a new Malware Domain group:
   a. Select Malware Domain folder and click **+** above the **RESOURCES** groups.
   b. Enter the **Group** name and **Description** of the Malware Domain.
3. Select the Malware Domain group (existing or new) and click **New**.
4. Select the **Domain Name** and **Description** of the Malware domain.
5. Click **Save**.

To configure a ThreatConnect Malware Domain, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware Domain, see Working with FortiGuard Malware Domains.

Modifying a Malware Domain

Complete these steps to edit a Malware Domain:

1. Go to **RESOURCES** > **Malware Domains**.
2. Select the Malware Domain group on the left panel.
3. Select the Malware Domain from the table and click **Edit** to modify the settings.
4. Click **Save**.

To configure a ThreatConnect Malware Domain, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware Domain, see Working with FortiGuard Malware Domains.

Deleting a Malware Domain

Complete these steps to delete a Malware Domain:

1. Go to **RESOURCES** > **Malware Domains**.
2. Select the Malware Domain on the left panel.
3. Select the Malware Domain from the table and click **Delete**.
4. Click **Yes**.

Importing Malware Domains

You can import Malware Domain information into FortiSIEM from external threat feed websites.

- Custom Threat Feed Websites - CSV Data - One-time Manual Import
- Custom Threat Feed Websites - CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python
- Working with Custom Threat Feeds that use HTTPS Connectivity

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   ```
   Name, IP Address, Reverse Lookup, Malware  Type, Confidence, Severity, ASN, Origin,
   Country, Description, Date Found (MM/DD/YYYY), Last Seen(MM/DD/YYYY)
   ```

   If the fields are not in this order, then the whole file will not be imported.
2. The `Name` field is required and must be unique. If two or more `Name` fields are identical, the latter ones will not be imported.
   Example Name Field: mydomain.local

1. Select **RESOURCES > Malware Domains**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Domain Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a description.
5. Click **Save** to create the folder under **Malware Domains**.
6. Select the folder just created.
7. Select **More > Update**.
8. Click **Choose File**.
9. Browse to the CSV file you want to import and select it.
10. Leave **Data Update** as **Full** (Completely replace all data) or **Incremental** (add on to existing data).
11. Click **Import**.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:
   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
   b. An individual entry is in one line.
2. The `Name` field is required and must be unique. The Malware domain import will fill this group with only unique values within the name field.
   Example Name Field: mydomain.local

Follow these steps:

1. Select **RESOURCES > Malware Domains**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Domain Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a Description.
5. Click **Save** to create the folder under **Malware Domains**.
6. Select the folder just created.
7. Select **More > Update**.
8. From the Update Malware Domain dialog box, select **Update via API**.
9. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
   Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Java**.
   e. For **Plugin Class**, the default class **com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService** is displayed.
   Note: Do not modify this in any case.
   f. Enter the correct **Field Separator** (by default, it is a comma).
   g. Select **CSV** as the **Data Format**.
   h. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the Domain Name is in third position, then choose 3 in the **Position** column.
   i. Enter the **Data Update** as **Full** (Completely replace all data) or **Incremental** (add on to existing data).
10. Click **Save**.
11. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
    The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Programmatic Import via Python

Follow these steps:

1. Select **RESOURCES > Malware Domains**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Domain Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a Description.
5. Click **Save** to create the folder under **Malware Domains**.
6. Select the folder just created.
7. Select **More > Update**.
8. From the Update Malware Domain dialog box, select **Update via API**.
9. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
   Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Python**.
   e. Check the **SSL Verify** checkbox to include a check to the authenticity and validity of an SSL certificate.
   f. From the **Plugin Name** drop-down list, select the python script to use. Python scripts located under
   `/opt/phoenix/data-definition/threatfeedIntegrations/`
   will be available.
   Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.
   g. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).
10. Click **Save**.
11. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
    The imported data will show on the right pane after some time.

Viewing Malware Domains

The Malware Domains Integration Status page shows all your existing Malware Domain feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware Domains** to view the Malware Domains Integration Status page.

Column	Description
Status	Displays the current status of the Malware Domain listed in the Feed column.
Feed	Displays Malware Domain group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware Domain group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware Domain threat feed objects. • **Update** - Click to update the Malware Domain threat feed.

Malware IPs

The Malware IP Addresses page lists IP addresses that are known to generate spam, host botnets, create DDoS attacks, and generally contain malware. The default group included in your FortiSIEM deployment, Emerging Threat, contains IP addresses that are derived from the website rules.emergingthreats.net. Because malware IP addresses are constantly changing, FortiSIEM recommends maintaining a dynamically generated list of IP addresses provided by services such as Emerging Threat that are updated on a regular schedule, but you can also add or remove blocked IP addresses from these system-defined groups, and create your own groups based on manual entry of IP addresses or file upload. A Python Threat Feed Framework is also available, see here.

The following sections describe Malware IPs:

- Adding a Malware IP
- Modifying a Malware IP
- Deleting a Malware IP
- Importing Malware IPs
- Viewing Malware IPs

Adding a Malware IP

Complete these steps to add a Malware IPs:

1. Go to **RESOURCES** > **Malware IPs**.
2. Select a group where you want to add the Malware IPs, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the details of the Malware IP.
5. Click **Save**.

To configure a ThreatConnect Malware IP, see Working with ThreatConnect.

To configure a FortiGuard Malware IP, see Working with FortiGuard Malware IPs.

Modifying a Malware IP

Complete these steps to edit a Malware IP:

1. Go to **RESOURCES** > **Malware IPs**.
2. Select the Malware IP group in the left panel.
3. Select the Malware IP from the table and click **Edit** to modify the settings.
4. Click **Save**.

To configure a ThreatConnect Malware IP, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware IP, see Working with FortiGuard Malware IPs.

You can use the **Delete** button to select and remove any Malware IP from the list.

Deleting a Malware IP

Complete these steps to delete a Malware IP:

1. Go to **RESOURCES** > **Malware IPs**.
2. Select the Malware IP group from the folder structure on the left panel.
3. Select the Malware IP from the table and click **Delete** to delete.
4. Click **Yes** to confirm.

Importing Malware IPs

You can import Malware IP information into FortiSIEM from external threat feed websites.

- Prerequisites
- Websites with Built-in Support
- Custom Threat Feed Websites - CSV Data - One-time Manual Import
- Custom Threat Feed Websites - CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python
- Working with Custom Threat Feeds that use HTTPS Connectivity

Prerequisites

Before proceeding, gather the following information about a threat feed web site:

- Website URL
- Credentials required to access the website (optional).
- If the website is not supported by FortiSIEM, you may need to understand the format of the data returned by the URL.
  - If the data is in the comma-separated value format (the separator need not be a comma but could be any separator), then a simple integration is possible.
  - If the data is any other format, for example, XML, then some code must be written for integration using the framework provided by FortiSIEM.

Websites with Built-in Support

The following websites are supported:

- Emerging threat (http://rules.emergingthreats.net)
- Threat Stream Malware IP (https://api.threatstream.com)
- Hail-A-TAXII Malware IP (http://hailataxii.com/)

For Threat Stream Malware IP, the following Malware types are imported:

- Bot IP
- Actor IP
- APT Email
- APT IP

- Bruteforce IP
- Compromised IP
- Malware IP
- DDoS IP
- Phishing email IP
- Phish URL IP
- Scan IP
- Spam IP

To import data from these websites, follow these steps:

1. In the **RESOURCES** > **Malware IPs**, find the website you must import data from.
2. Select the folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will show in the edit box.
5. Enter a **Schedule** by clicking the **+** icon.
6. Enter the schedule parameters - when to start and how often to import. FortiSIEM recommends no more frequent than hourly.
7. Select the type of template you want to create.

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value format.

Requirements for Importing

1. The CSV file columns must be in the following order:

```
Name, Low IP, High IP, Malware Type, Confidence, Severity, ASN, Org, Country
,Description, Date Found(MM/DD/YYYY), Last Seen(MM/DD/YYYY)
```

   If the fields are not in this order, then the whole file will not be imported.
2. `Name`, `Low IP`, and `High IP` are required fields. All `Name` fields must be unique. If `High IP` is not available, then the `High IP` field should be set to the `Low IP`.Example: BadMalware,1.2.3.4,1.2.3.10

1. Select **RESOURCES** > **Malware IPs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware IP Group** dialog box.
3. Enter a **Group** name and add a **Description**.
4. Click **Save** to create the folder under **Malware IPs**.
5. Select the folder just created.
6. Select **More > Update**.
7. Click **Choose File**.
8. Browse to the file you want to import and select it.
9. Leave **Data Update** as **Full** (Completely replace) or **Incremental** (add on to existing data).

10. Click **Import**.
    The imported data will appear in the right pane.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:
   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
   b. An individual entry is in one line.
2. The `Low IP` field is required and must be unique.
   Example: 1.2.3.4

Follow these steps:

1. Select **RESOURCES** > **Malware IPs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware IPs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon next to **URL** and provide the following information:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, the default class **com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService** is displayed.
   Note: Do not modify this in any case.
   e. Enter the correct **Field Separator** (by default, it is a comma).
   f. Select **CSV** as the **Data Format**.
   g. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the IP is in third position, then choose 3 in the **Position** column.
7. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
   The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java

This is the most general case where the website data format does not satisfy the previous conditions. In this case, write a Java plugin class by modifying the default system provided one.

After the class has been written and fully tested for correctness, follow these steps.

1. Select **RESOURCES** > **Malware IPs**.
2. Click on the "**+**" button on the left navigation tree to bring up the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**.
4. Click **Save** to create the folder under **Malware IPs**.
5. Select the folder just created.
6. Select **More** > **Update** > **Update via API**.
7. Click the edit icon and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, the custom Java class for this case.
   e. Select 'Custom' as the **Data Format**.
   f. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
   The imported data will display on the right pane after some time.

Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java

In this case, the threat feed data is available formatted as STIX and follows the TAXII protocol.

1. Select **RESOURCES** > **Malware IPs**.
2. Click on the "**+**" button on the left navigation tree to bring up the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware IPs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).

c. For **Plugin Type**, select **Java**.
d. Select 'STIX-TAXII' as the **Data Format**.
e. For **Plugin Class**, choose **com.accelops.service.threatfeed.impl.StixMalwareIPUpdateService** and **Full**.
f. Click **Save**.

7. Select a import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Programmatic Import via Python

In this case, the threat feed data is available via python integration.

1. Select **RESOURCES**>**Malware IPs**.
2. Click on the "**+**" button on the left navigation tree to bring up the **Create New Malware IP Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware IPs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
   Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Python**.
   e. Check the **SSL Verify** checkbox to include a check to the authenticity and validity of an SSL certificate.
   f. From the **Plugin Name** drop-down list, select the python script to use. Python scripts located under
   `/opt/phoenix/data-definition/threatfeedIntegrations/`
   will be available.
   Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.
   g. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).
7. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
The imported data will show on the right pane after some time.

Viewing Malware IPs

The Malware IPs Integration Status page shows all your existing Malware IP feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware IPs** to view the Malware IPs Integration Status page.

Column	Description
Status	Displays the current status of the Malware IPs listed in the Feed column.
Feed	Displays Malware IP group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware IP group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware IP threat feed objects. • **Update** - Click to update the Malware IP threat feed.

Malware URLs

The Malware URLs page lists URLs that are known to host malware. The Threat Stream Blocked URL group is included in your FortiSIEM deployment. A Python Threat Feed Framework is also available, see here.

The following sections describe Malware URLs:

- Adding a Malware URL
- Modifying a Malware URL
- Deleting a Malware URL
- Importing Malware URLs
- Viewing Malware URLs

Adding a Malware URL

Complete these steps to add a Malware URL:

1. Go to **RESOURCES** > **Malware URLs**.
2. Select a group where you want to add the Malware URL, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the following information about the Malware URL:
   - URL
   - Malware Type
   - Confidence
   - Description
   - Last Seen
5. Click **Save**.

To configure a ThreatConnect Malware Domain, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware URL, see Working with FortiGuard Malware URLs.

Modifying a Malware URL

Complete these steps to edit a Malware URL:

1. Go to **RESOURCES** > **Malware URLs**.
2. Select the Malware URL group from the folder structure on the left panel.
3. Select the Malware URL from the table and click **Edit** to modify the settings.
4. Click **Save**.

To configure a ThreatConnect Malware URL, see Working with ThreatConnect IOCs.

To configure a FortiGuard Malware URL, see Working with FortiGuard Malware URLs.

You can use the **Delete** button to select and remove any Malware URL from the list.

Deleting a Malware URL

Complete these steps to delete a Malware URL:

1. Go to **RESOURCES** > **Malware URLs**.
2. Select the Malware URL group from the folder structure on the left panel.
3. Select the Malware URL from the table and click **Delete** to delete.
4. Click **Yes** to confirm.

Importing Malware URLs

This section describes how to import Malware URL information into FortiSIEM from external threat feed websites.

- Prerequisites
- Threat Feed Websites with Built-in Support
- Custom Threat Feed Websites - CSV Data - One-time Manual Import
- Custom Threat Feed Websites - CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python
- Working with Custom Threat Feeds that use HTTPS Connectivity

Prerequisites

Before proceeding, gather the following information about a threat feed web site:

- Website URL.
- Credentials required to access the website (optional).
- If the website is not supported by FortiSIEM, you may need to understand the format of the data returned by the URL.
  - If the data is in comma-separated value (CSV) format, then a simple integration is possible. Note that the separator need not be a comma but could be any separator.
  - If the data is any other format, for example, XML, then some code must be written for integration using the framework provided by FortiSIEM.

Threat Feed Websites with Built-in Support

The following websites are supported:

- Threat Stream Malware URL (https://api.threatstream.com)
- FortiSandbox Malware URL
- Hail-A-TAXII Malware IP (http://hailataxii.com/)

To import data from these websites, follow these steps:

1. In the **RESOURCES** > **Malware URLs**, find the website you must import data from.
2. Select the folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will show in the edit box.
5. Enter a **Schedule** by clicking the **+** icon.

6. Enter the schedule parameters: when to start and how often to import. FortiSIEM recommends no more frequent than hourly.

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   ```
   URL, Malware Type, Confidence, Description, Last Seen (MM/DD/YYYY)
   ```

   If the fields are not in this order, then the whole file will not be imported.
2. The `URL` field is required and must be unique.
   Example: www.0800thissite.ru/zone/freebee.php
1. Select **RESOURCES** > **Malware URLs**.
2. Click the + button on the left navigation tree to open the **Create New Malware URL Group** dialog.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **Import from a CSV file**.
6. Click **Choose File**; enter the file name and click **Upload**.
   The imported data will show on the right pane.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:
   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
   b. An individual entry is in one line.
2. The `URL` field is required and must be unique.
   Example: www.0800thissite.ru/zone/freebee.php

Follow these steps:

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog box.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.

6. Click the edit icon next to **URL** and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, the default class **com.accelops.service.threatfeed.impl.ThreatstreamMalwareUrlUpdateService** is shown. Do not modify this value for this case.
   e. Enter the correct **Field Separator** (by default it is a comma).
   f. Set **Data Format** to **CSV**.
   g. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
   h. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example if the URL is in third position, then choose 3 in the **Position** column.
   i. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will show on the right pane.

Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java

This is the most general case where the website data format is not CSV. In this case, write a Java plugin by modifying the default class provided by the system.

After the class has been written and fully tested for correctness, follow these steps:

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog.
3. Enter the **Group** name and add a **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Type**, select **Java**.
   d. For **Plugin Class**, enter the name of the custom Java plugin class.
   e. Select **Custom** as the **Data Format**.
   f. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
   g. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will show on the right pane.

Custom Threat Feed Websites - STIX Formatted Data and TAXII Import via Java

In this case, the threat feed data is available formatted as STIX and follows the TAXII protocol.

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog box.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon and:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. Do not edit the name of the **Plugin Class**.
   d. For **Plugin Type**, select **Java**.
   e. Select **STIX-TAXII** as the **Data Format**.
   f. Enter the name of the STIX-TAXII **Collection**.
   g. Select **Full** as the **Data Update** value. Existing data will be overwritten.
   h. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will display on the right pane.

Custom Threat Feed Websites - Programmatic Import via Python

In this case, the threat feed data is available through Python integration.

1. Select **RESOURCES** > **Malware URLs**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware URL Group** dialog box.
3. Enter **Group** and add **Description**. Click **Save** to create the folder under **Malware URLs**.
4. Select the folder just created.
5. Select **More** > **Update** > **Update via API**.
6. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
      Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Python**.

e. Check the **SSL Verify** checkbox to include a check to the authenticity and validity of an SSL certificate.

f. From the **Plugin Name** drop-down list, select the python script to use. Python scripts located under
`/opt/phoenix/data-definition/threatfeedIntegrations/`
will be available.
Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.

g. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).

7. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
The imported data will show on the right pane after some time.

Viewing Malware URLs

The Malware URLs Integration Status page shows all your existing Malware URL feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware URLs** to view the Malware URLs Integration Status page.

Column	Description
Status	Displays the current status of the Malware URLs listed in the Feed column.
Feed	Displays Malware URLs group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware URL group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware URL threat feed objects. • **Update** - Click to update the Malware URL threat feed.

Malware Processes

The following sections describe Malware Processes:

- Creating Malware Process Groups
- Adding Malware Processes
- Modifying Malware Processes
- Deleting a Malware Processes
- Importing Malware Processes
- Viewing Malware Processes

Creating a Malware Process Group

Complete these steps to add a Malware Process group:

1. Go to **RESOURCES** and select **Malware Processes**.
2. Click **+** above the **RESOURCES** groups.
3. Enter a group **Name** and **Description** in the **Create New Malware Process Group** dialog box.
4. Choose processes to include by expanding the tree in the **Folders** panel.
5. Select processes from the **Items** panel and move them to the **Selections** panel.
6. Click **Save**.

Adding a Malware Process

Complete these steps to add a Malware Processes:

1. Go to **RESOURCES** > **Malware Processes**.
2. Select a group where you want to add the Malware Processes.
3. Click **New**.
4. Enter the **Process Name** and **Description** of the Malware Process.
5. Click **Save**.

Complete these steps to import Malware processes from a CSV file:

1. Go to **RESOURCES** > **Malware Processes**.
2. Click **More** > **Update** > **Import from a CSV file**.
3. Click **Choose File** to select the CSV file.
4. Click **Import**.

Modifying a Malware Process

Complete these steps to edit a Malware Process:

1. Go to **RESOURCES** > **Malware Processes**.
2. Select the Malware Process group from the folder structure on the left panel.
3. Select the Malware Process from the table and click **Edit** to modify the settings.
4. Click **Save**.

Deleting a Malware Process

Complete these steps to delete a Malware Process:

1. Go to **RESOURCES** > **Malware Processes**.
2. Select the Malware Process group from the folder structure on the left panel.
3. Select the Malware Process from the table and click **Delete** to delete.
4. Confirm whether to **Remove only from group** by clicking **Yes** or **No**.

Importing Malware Processes

- Custom Threat Feed Websites - CSV Data - One-time Manual Import

Custom Threat Feed Websites - CSV Data - One-time Manual Import

This requires that the data to be imported is already in a file in comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

   ```
   Process Name, Description
   ```

   If the fields are not in this order, then the whole file will not be imported.
2. The `Process Name` field is required and must be unique.
   Example: mscd.exe

1. Select **RESOURCES > Malware Processes**.
2. Click the **+** button on the left navigation tree to open the **Create New Malware Process Group** dialog box.
3. In the **Group** field, enter a Group name.
4. In the **Description** field, enter a description.
5. Click **Save** to create the folder under **Malware Processes**.
6. Select the folder just created.
7. Select **More > Update**.
8. Click **Choose File**.
9. Browse to the CSV file you want to import and select it.
10. Leave **Data Update** as **Full** (Completely replace) or **Incremental** (add on to existing data)
11. Click **Import**.

Viewing Malware Processes

The Malware Processes Integration Status page shows all your existing Malware Process feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware Processes** to view the Malware Processes Integration Status page.

Column	Description
Status	Displays the current status of the Malware Processes listed in the Feed column.
Feed	Displays Malware Processes group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware Processes group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware Processes threat feed objects. • **Update** - Click to update the Malware Processes threat feed.

Country Groups

The Country Groups page contains a list of all of the country names in the FortiSIEM geolocation database. You can also create folders that represent different organizations of countries for use in analytics.

- Creating a Country Group
- Adding a Country Group
- Modifying Country Groups
- Deleting a Country Group
- Changing the Home Country

Creating a Country Group

Complete these steps to add a Country Group:

1. Go to **RESOURCES** > **Country Group**.
2. Click **+** above the **RESOURCES** groups.
3. Enter a group **Name** and **Description** in the **Create New Country Group** dialog box.
4. Choose countries to include by expanding the tree in the **Folders** panel, selecting countries from the **Items** panel, and moving them to the **Selections** panel.
5. Click **Save**.

Adding a Country Group

Complete these steps to add a Country Group:

1. Go to **RESOURCES** > **Country Group**.
2. Select a group where you want to add the Country Group, or create a new one by clicking **+** above the **RESOURCES** groups.
3. Click **New**.
4. Enter the **Country Name** and **Description** of the Country Group.
5. Click **Save**.

Modifying a Country Group

Complete these steps to edit a Country Group:

1. Go to **RESOURCES** > **Country Groups**.
2. Select a Country Group from the left panel.
3. Select the Country Group from the table and click **Edit** to modify the settings.
4. Click **Save**.

Deleting a Country Group

Complete these steps to delete a Country Group:

1. Go to **RESOURCES** > **Country Groups**.
2. Select a Country Group from the left panel.
3. Select **-** above the Resource groups.
4. Confirm whether to **Remove only from group** or to remove the group completely by clicking **Yes**.

Changing the Home Country

Many rules and reports use the My Home CMDB Object as defined in **Resources** > **Country Groups** > **My Home**.

By default, this is set to **United States of America**.

Complete these steps to change your home country:

1. Go to **RESOURCES** > **Country Groups**.
2. Select **My Home** from the left panel.
3. Click the Edit icon ( ) at the top left panel.
4. From the **Edit Country Group : My Home** window, take the following steps:
   a. In the leftmost panel, expand **Country Groups** and select a country group folder.
   b. In the middle panel, select a country.
   c. Click **>** to add the selected country to your My Home.
   Note: You can also select a country in the rightmost panel and click **<** to remove it from My Home.
5. Click **Save**.

Malware Hash

Use the **Malware Hash** page to define a list of malware files and their hash functions. When FortiSIEM monitors a directory, it generates these directory events:

Directory Event	Generated by This Action
PH_DEV_MON_CUST_FILE_CREATE	New file creation
PH_DEV_MON_CUST_FILE_SCAN	Directory is scanned
PH_DEV_MON_CUST_FILE_CHANGE_CONTENT	Changes in file content

When FortiSIEM scans a file and collects its hash, it uses the system rule `Malware Hash Check` to check the list of malware hashes. FortiSIEM will then trigger an alert if a match is found. A Python Threat Feed Framework is also available, see here.

The following sections describe Malware Hashes:

- Adding a Malware Hash
- Modifying a Malware Hash
- Importing/Updating User-defined Malware Hash
- Viewing Malware Hash

Adding a Malware Hash

Complete these steps to add a Malware Hash:

1. Go to **RESOURCES** > **Malware Hash**.
2. Select a group where you want to add the Malware Hash, or create a new group by clicking **+** above the **RESOURCES** groups.
3. Click **New** and add the information related to the Malware Hash.
4. Click **Save**.

To add a ThreatConnect Malware Hash, see Working with ThreatConnect.

Modifying a Malware Hash

Complete these steps to edit a Malware Hash:

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the Malware Hash group from the folder structure on the left panel.
3. Select the Malware Hash from the table and click **Edit** to modify the settings.
4. Click **Save**.

To modify a ThreatConnect Malware Hash, see Working with ThreatConnect.

You can use the **Delete** button to select and remove any Malware Hash from the list.

Importing/Updating User-defined Malware Hash

System defined groups are updated by its own service:

- Threat Stream Malware Hash
- FortiSandbox Malware Hash

You can update the Malware Hash using the following options:

- Import from a CSV File
- Update via API

Prerequisites:

Before proceeding, gather the following information about a threat feed web site.

- Website URL.
- Credentials required to access the website (optional).
- If the website is not supported by FortiSIEM, you must understand the format of the data returned by the URL.
  - If the data is in the comma-separated value format (the separator need not be a comma but could be any separator, then a simple integration is possible.)
  - If the data is any other format, for example, XML, then some code must be written for integration using the framework provided by FortiSIEM.

Import from a CSV File

Custom Websites - CSV Data - One-time Manual Import

Instead of manually adding Malware Hashes to a group individually, you can upload a CSV file with multiple entries. This requires that the data to be imported is already in a file in a comma-separated value (CSV) format.

Requirements for Importing

1. The CSV file columns must be in the following order:

```
Botnet Name, Algorithm, Hash Code, Controller IP, Malware Type, Confidence,
Severity, Asn, Origin, Country, Description, Date Found(MM/DD/YYYY), Last Seen
(MM/DD/YYYY)
```

   If the fields are not in this order, then the whole file will not be imported.

2. `Botnet Name`, `Algorithm`, and `Hash Code` are required fields. The 3 required fields are linked, so any changes to the fields within each row will produce a unique entry.

   Examples:

   newbotnet, md5, 4da0bb01a96e70ce43ece0147f8438d1

   newbotnet1,sha256,8e53e4d236c99ba4dcf7c4cbf1cea93d023391ea

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the group from the left panel or create a new group by clicking the **+** icon above the list of RESOURCES groups.
3. Select **More** > **Update**.
4. Select **Import from a CSV file** and choose the file to import.
5. Click **Import**.

Update via API

This section describes how to import Malware Hash information into FortiSIEM from external threat feed websites. Malware Hashes are used by malware to hide their own identity.

- Updating System Defined Malware Hash Group
- Custom Threat Feed Websites - CSV Data - Programmatic Import
- Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java
- Custom Threat Feed Websites - Non-CSV Data -STIX Formatted Data and TAXII Import via Java
- Custom Threat Feed Websites - Programmatic Import via Python

Updating System Defined Malware Hash Group

The following websites are supported:

- Threat Stream Open Proxy (https://api.threatstream.com)
- Threat Stream TOR Node (https://api.threatstream.com)

Complete these steps to import data from these websites:

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder and find the website you want to import data from.
3. Click **More** > **Update**.
4. Select **Update via API**.
   The link will be displayed in the URL field or else manually enter the URL and details.
5. Enter a **Schedule** by clicking the **+** icon.
6. Enter the schedule parameters - **Start Time** and **Recurrence Pattern**. FortiSIEM recommends no more frequent than hourly.
7. Click **Save**.
   You can use the edit icon to modify or delete icon to remove a **Schedule**.

Custom Threat Feed Websites - CSV Data - Programmatic Import via Java

Requirements for Importing

1. The Web Site Data requires the following:
   a. A file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
   b. An individual entry is in one line.
2. The CSV file columns must be in the following order:

```
Botnet Name, Algorithm, Hash Code, Controller IP, Malware Type, Confidence, Severity,
Asn, Origin, Country, Description, Date Found (MM/DD/YYYY), Last Seen (MM/DD/YYYY)
```

   If the fields are not in this order, then the whole file will not be imported.
3. The `Botnet Name` field is required and must be unique.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will be displayed in the URL field or else manually enter the URL and details.
5. Click the edit icon near **URL**.
6. Enter the following information:
   a. In the **URL** field, enter the URL of the website.
   Note: Ensure you have an "http://" or "https://" prefix.
   b. (Optional) In the **User Name** field, enter the username associated with the API.
   c. (Optional) In the **Password** field, enter the password associated with the username.
   d. For **Plugin Type**, select **Java**.
   e. For **Plugin Class**, the default class '**com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService**' is shown. Do not modify this in any case.
   f. Enter the correct **Field Separator** (by default it is a comma).
   g. Select **CSV** as the **Data Format**.
   h. Select **Data Update** as **Full**.
   i. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the Botnet Name is in third position, choose 3 in the **Position** column. Click **+** if you must add more rows.
   j. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will show on the right pane after some time.

Custom Threat Feed Websites - Non-CSV Data - Programmatic Import via Java

This is the most general case where the website data format does not satisfy the previous conditions. In this case, write a Java plugin class by modifying the default system provided one.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon near **URL**.
6. Enter the following information:
7. Enter the **URL** of the website.
   a. Enter **User Name** and **Password** (optional).
   b. For **Plugin Type**, select **Java**.
   c. For **Plugin Class**, the custom Java class in this case.
   d. Select **Custom** as the **Data Format**.
      - Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the IP is in third position, choose 3 in the **Position** column. Click **+** if you must add more rows.
      - Select **Full** as the **Data Update** value. Existing data will be overwritten. Select **Incremental** to preserve the existing data.

      For **STIX-TAXII**:
      - Enter the name of the STIX-TAXII **Collection**.
      - Select **Full** as the **Data Update** value. Existing data will be overwritten.
   e. Click **Save**.
8. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
   The imported data will display in the table after some time.

Custom Threat Feed Websites - Non-CSV Data -STIX Formatted Data and TAXII Import via Java

In this case, the threat feed data is available formatted as STIX and follows the TAXII protocol.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon near **URL**.
6. Enter the following information:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).

c. For **Plugin Type**, select **Java**.
d. For **Plugin Class**, the custom Java class in this case.
e. Enter the name of the STIX-TAXII **Collection**.
f. Select **STIX-TAXII** as the **Data Format**.
g. Select **Data Update** as **Full**.
h. Click **Save**.

7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import new data from the website.
The imported data will display in the table after some time.

Custom Threat Feed Websites - Programmatic Import via Python

In this case, the threat feed data is available via Python integration.

1. Go to **RESOURCES** > **Malware Hash**.
2. Select the folder or click **+** to add a new group under **Malware Hash** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon next to **URL** and provide the following information:
   a. In the **URL** field, enter the URL of the website.
   Note: Include the "http://" or "https://" prefix.
   b. (optional) In the **User Name** field, enter the username used by the API.
   c. (optional) In the **Password** field, enter the password related to the username.
   d. For **Plugin Type**, select **Python**.
   e. Check the **SSL Verify** checkbox to include a check to the authenticity and validity of an SSL certificate.
   f. From the **Plugin Name** drop-down list, select the python script to use. Python scripts located under
   `/opt/phoenix/data-definition/threatfeedIntegrations/`
   will be available.
   Note: For more information on creating/using a Python script, see Appendix: Python Threat Feed Framework.
   g. For **Data Update**, select **Full** (Completely replace all data) or **Incremental** (add on to existing data).
6. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule**. Select when to start the import and how often to import to get new data from the website.
The imported data will show on the right pane after some time.

Viewing Malware Hash

The Malware Hash Integration Status page shows all your existing Malware Hash feeds. See the following table for more information.

Navigate to **RESOURCES**, and select **Malware Hash** to view the Malware Hash Integration Status page.

Column	Description
Status	Displays the current status of the Malware Hash listed in the Feed column.
Feed	Displays Malware Hash group and its threat feed URL, if the information is available.
Indicators	Shows the current and prior threat feed objects for the Malware Hash group to easier identify the change that occurred.
Last Updated	Displays the last time the threat feed was updated.
Pulling Schedule	Displays the scheduled time, when the threat feed update occurs.
Integration Type	Displays how the threat feed information is gathered, MANUAL or API.
Action	The Action columns allows you to perform one of three actions: • **View Content** - Click to view the existing Malware Hash threat feed objects. • **Update** - Click to update the Malware Hash threat feed.

Default Password

The Default Password page contains a list of default vendor credentials. These well-known credentials should never be used in production. During device discovery FortiSIEM checks if the device credentials are still set to default, The system rule `Default Password Detected by System` triggers an incident if they are.

This is a sample raw event log for a default password incident:

```
<174>Oct 20   22:50:03   [PH_AUDIT_DEFAULT_PWD_MATCH]:[phEventCategory]=2,
[appTransportProto]=SNMP,[reptModel]=Firewall-1   SPLAT,[srcIpAddr]=192.168.19.195,
[phCustId]=1,[sessionId]=0f8bdee2b6a265c4bd075fc777ed,[procName]=AppServer,
[reptVendor]=Checkpoint,[hostIpAddr]=172.16.0.1,[hostName]=SJ-QA-F-Lnx-CHK,
[eventSeverity]=PHL_INFO,[user]=,[phLogDetail]=Default password matches for   the same
composite key (Vendor, Model, Access method, User Name, Password)
```

The following sections describe Default Passwords:

- Adding a Default Password
- Modifying Default Password
- Importing and Exporting Default Password

Adding a Default Password

Complete these steps to add a default password:

1. Go to **RESOURCES** > **Default Password**.
2. Select a group where you want to add the default password, or create a new group by clicking **+** above the **RESOURCE** groups.
3. Click **New**.
4. Select the **Vendor** and **Model** of the device for which you want to enter a default password.
5. Select the **Access Protocol** that is used to connect to the device from the drop-down.
6. Enter the default **User Name** and **Password** for the device.
7. Click **Save**.

Modifying a Default Password

Complete these steps to edit a default password:

1. Go to **RESOURCES** > **Default Password**.
2. Select the default password group from the folder structure on the left panel.
3. Select the default password from the table and click **Edit** to modify the settings.
4. Click **Save**.

Use the **Delete** button to select and remove any default password(s) from the list.

Importing and Exporting a Default Password

The procedures below describe how to import and export a Default Password.

Importing Default Password

Instead of manually adding default passwords to a user-defined or system group individually, you can upload a CSV file with multiple entries into a group.

You must format the file with these fields: `Vendor,Model,Access Protocol,User Name,Password`

For example: `Microsoft,Windows,WMI,Administrator,Administrator`

1. Go to **RESOURCES** > **Default Password**.
2. Select the Default Password group where you want to import the new password from the folder structure.
3. Click **Import** and select the CSV file.
4. Click **Import**.

Exporting Default Password

Complete these steps to export a default password from a Group to a CSV File.

1. Go to **RESOURCES** > **Default Password**.
2. Select the Default Password group from where you want to export the Default Password from the folder structure.
3. Select the Default Password from the table and click **Export**.
4. Click **Generate**.
   'Export successful' message is displayed.
5. Click **Open Report File** and save the report.

Anonymity Network

An anonymity network is used to hide one's network identity, and is typically used by malware to hide its originating IP address. Enterprise network traffic should not be originating from or destined to Anonymity network.

When FortiSIEM discovers traffic destined to or originating from anonymity networks, it triggers these rules:

- Inbound Traffic from Tor Network
- Outbound Traffic to Tor Network
- Inbound Traffic from Open Proxies
- Outbound Traffic to Open Proxies

The following topics are available:

- Adding Anonymity Networks
- Modifying Anonymity Networks
- Updating Anonymity Networks

Adding Anonymity Networks

FortiSIEM provides two default (system-defined) groups for Anonymity Networks:

- **Open Proxies**: A set of open proxies in the internet. This is a static group.
- **Tor Nodes**: This group is dynamically updated from https://check.torproject.org/exit-addresses. To schedule regular updates for this group, click the group name, then click **Update** and provide updated scheduling information.

Complete these steps to add Anonymity Networks:

1. Go to **RESOURCES**> **Anonymity Network** folder on the left panel.
2. Select **Open Proxies** or **Tor Nodes** folder or click **+** to add a new group.
3. Click **New**.
4. Enter **IP**, **Port**, and **Country** information about the anonymity network.
5. Click the **Calendar** icon to select the **Date Found** and **Last Seen**.
6. Click **Save**.

Adding Anonymity Networks to Watch Lists

You can easily add an anonymity network IP address to your watch lists. Hover your mouse cursor over the anonymity network IP address until the icon for the **Options** menu appears, and then select **Add to Watchlist**.

Modifying Anonymity Networks

Complete these steps to edit an Anonymity Network:

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the Anonymity Network group from the folder structure on the left panel.
3. Select the Anonymity Network from the table and click **Edit** to modify the settings.
4. Click **Save**.

You can use the **Delete** button to select and remove any Anonymity Network from the list.

Updating Anonymity Networks

This section describes how to update Anonymity Network information in FortiSIEM from external threat feed websites.

You can update the Anonymity Network information in the following ways:

- Import from a CSV File
- Update via API

Prerequisites:

Before proceeding, gather the following information about a threat feed web site.

- Website URL.
- Credentials required to access the website (optional).
- If the website is not supported by FortiSIEM, you must understand the format of the data returned by the URL.
  - If the data is in the comma-separated value format (the separator need not be a comma but could be any separator, then a simple integration is possible.)
  - If the data is any other format, for example, XML, then some code needs to be written for integration using the FortiSIEM provided framework.

Import from a CSV File

Custom Websites - CSV Data - One-time Manual Import

Instead of manually adding anonymity networks to a group individually, you can upload a CSV file with multiple entries. This requires that the data to be imported is already in a file in comma-separated value format.

```
IP, Port, Malware Type, Confidence, Severity, Asn, Org, Country, Description, Data Found (MM/DD/YYYY), Last Seen(MM/DD/YYYY)
```

Note: Although many fields are possible, only the IP is required.

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the group from the left panel or create a new group by clicking the **+** icon above the list of RESOURCES groups.
3. Select **More** > **Update**.
4. Select **Import from a CSV file** and choose the file to import.
5. Click **Import**.

Update via API

This section describes how to import anonymity networks information into FortiSIEM from external threat feed websites. Anonymity networks are used by malware to hide their own identity.

Websites with Built-in Support

The following websites are supported:

- Threat Stream Open Proxy (https://api.threatstream.com)
- Threat Stream TOR Node (https://api.threatstream.com)

Complete these steps to import data from these websites:

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the folder and find the website you must import data from.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will be displayed in the URL field or else manually enter the URL and details.
5. Enter a **Schedule** by clicking the **+** icon.
6. Enter the schedule parameters - **Start Time** and **Recurrence Pattern**. FortiSIEM recommends no more frequent than hourly.
7. Click **Save**.
   You can use the edit icon to modify or delete icon to remove a **Schedule**.

Custom Websites - CSV Data - Programmatic Import

This requires that the web site data is:

- a file in comma-separated value format (separator can be any special character such as space, tab, hash, dollar etc.).
- one entry is in a single line.

Note: Although many fields are possible, only the IP is required.

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the folder or click **+** to add a new group under **Anonymity Network** folder.
3. Click **More** > **Update**.
4. Select **Update via API**. The link will be displayed in the URL field or else manually enter the URL and details.
5. Click the edit icon near **URL**.
6. Enter the following information:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).

c. For **Plugin Class**, the default class `com.accelops.service.threatfeed.impl.ThreatFeedWithMappingPolicyService` is shown. **Do not modify this in this case.**
d. Enter the correct **Field Separator** (by default it is a comma).
e. Select **CSV** as the **Data Format**.
f. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
g. Enter the **Data Mapping** by choosing the mapped field and the corresponding position in the website data. For example, if the IP is in third position, choose 3 in the **Position** column. Click **+** if you must add more rows.
   a. Click **Save**.

7. Select an import schedule by clicking **+** on the **Schedule Summary**. Select when to start the import and how often to import new data from the website.
The imported data will show on the right pane after some time.

New Websites - Non-CSV Data - Programmatic Import

This is the most general case where the website data format does not satisfy the previous conditions. In this case, you have to write a Java plugin class by modifying the default system provided one. After the class has been written and fully tested for correctness, follow these steps.

1. Go to **RESOURCES** > **Anonymity Network**.
2. Select the folder or click **+** to add a new group under **Anonymity Network** folder.
3. Click **More** > **Update**.
4. Select **Update via API**.
5. Click the edit icon near **URL**.
6. Enter the following information:
   a. Enter the **URL** of the website.
   b. Enter **User Name** and **Password** (optional).
   c. For **Plugin Class**, the custom Java class in this case.
   d. Enter the correct **Field Separator** (by default it is a comma).
   e. Select **Custom** or **STIX-TAXII** as the **Data Format**.
      - **STIX-TAXII** - provide the name of the **Collection**. Select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
      - **Custom** - select **Data Update** as **Full** to overwrite the existing data or **Incremental** to retain the existing data.
   f. Click **Save**.
7. Select an import schedule by clicking **+** on the **Schedule Summary**. Select when to start the import and how often to import new data from the website.
The imported data will display in the table after some time.

User Agents

The User Agent page lists common and uncommon user agents in HTTP communications. The traditional use case for a user agent is to detect browser types so the server can return an optimized page. However, user agents are often misused by malware, and are used to communicate the identity of the client to the BotNet controller over HTTP(S). FortiSIEM monitors HTTP(S) logs and the system rule Blacklist User Agent Match uses regular expression matching to detect blacklisted user agents.

- Adding User Agents
- Modifying User Agents
- Importing and Exporting User Agents

Adding User Agents

Complete these steps to add a User Agent:

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group where you want to add the new user agent from the folder structure on the left panel. To create a new User Agent group, click **+** above the **Resources** tree.
3. Click **New**.
4. Enter the **User Agent** using regular expression notation.
5. Click **Save**.

Modifying User Agents

Complete these steps to edit a User Agent:

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group from the folder structure on the left panel.
3. Select the User Agent from the table and click **Edit** to modify the settings.
4. Click **Save**.

You can use the **Delete** button to select and remove any User Agent from the list.

Importing and Exporting User Agents

The procedures below describe how to import and export User Agents.

Importing User Agents

Instead of manually adding User Agents to a user-defined or system group individually, you can upload a CSV file with multiple entries into a group.

Note: You must format the User Agent password with regular expression notation: *User Agent (regular expression)*

Complete these steps to import User Agents to a Group from a CSV File.

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group where you want to import the new User Agents from the folder structure.
3. Click **Import** and select the CSV file.
4. Click **Import**.

Exporting User Agents

Complete these steps to export User Agents from a Group to a CSV File.

1. Go to **RESOURCES** > **User Agents**.
2. Select the **User Agent** group from where you want to export the User Agents from the folder structure.
3. Select the User Agent from the table and click **Export**.
4. Click **Generate**.
   If the export is successful, an "Export successful" message is displayed.
5. Click **Open Report File** and save the report.

Remediations

Remediation can be performed either on an ad hoc basis or by using an Automation Policy. An Automation Policy directs the system to take a Remediation action when an Incident occurs. To invoke a Remediation, do the following:

- Make sure the Remediation script for your scenario is defined.
- Check the existing Remediation scripts. Go to **ADMIN** > **Settings** > **General** > **Automation Policy**, then choose **Run Remediation/Script** in the **Action** section of the Automation Policy dialog box. See Adding Automation Policy Settings.
- If your device is not in the list, add the needed Remediation script.

The system-defined and custom Remediations are listed under **RESOURCES** > **Remediations**. The following sections describe how to create and manage custom Remediations.

- Adding Remediations
- Modifying Remediations
- Deleting Remediations

Adding Remediations

Complete these steps to create a new custom Remediation. You can also select any existing Remediation to **Clone** and customize.

1. Go to **RESOURCES** > **Remediations**.
2. Click **New**.
3. Enter the **Name** of the Remediation.
4. Select the **Device Type** to which this Remediation will be applied.
5. Select the **Protocol** as SSH, HTTP, HTTPS or MS_WMI for the device type.
6. Enter the Remediation **Script Name**.
7. Enter the Remediation **Script Content**.
8. Add any **Description** related to this Remediation.
9. Click **Save**.
   The Remediation will be available in the list along with the system-defined Remediations.

Modifying Remediations

Note that you cannot modify any system-defined Remediations.

Complete these steps to modify a custom Remediation:

1. Go to **RESOURCES** > **Remediations**.
2. Select a custom Remediation from the list.
3. Click **Edit** and modify the remediation settings.
4. Click **Save**.
   The updated Remediation will be available in the list along with the system-defined Remediations.

Deleting Remediations

Note that you cannot remove any system-defined Remediations.

Complete these steps to delete a custom Remediation(s).

1. Go to **RESOURCES** > **Remediations**.
2. Select the custom Remediation to delete from the list.
3. Click **Delete**.
4. Click **Yes** to confirm.
   These Remediation(s) will be deleted from the list.

Lookup Tables

The Lookup Tables page lists existing lookup tables. Lookup table schemas can be added, and Lookup table data can be added or imported on this page.

The Lookup Table page is comprised of the following fields:

Column	Description
Table Name	The name of the table is displayed.
Organization	The organization(s) which the table belongs to is displayed.
Description	Any additional information from the Description field when creating the table is displayed here.
Action	**View** - Click to open a table. From here, you can add data, edit existing data, or import data. **Delete** - Click to delete the table. **Schema** - Click to view the Lookup table's schema.

The following topics are available:

- Adding a Lookup Table
- Deleting a Lookup Table
- Working with Lookup Table Data

Adding a Lookup Table

Complete these steps to add a Lookup table:

Note: Once a table is created, the schema cannot be modified.

1. Go to **RESOURCES > Lookup Table**.
2. In the left panel, click on **+**.
3. In the **Create a New Lookup Table** window, from the **Organization** drop-down list, select the Organization that the Lookup table belongs to.
4. In the **Table Name** field, enter the name of the Lookup table.
5. (Optional) In the **Description** field, enter any additional information about the Lookup table.
6. In the **Schema** section, take the following actions.
   a. If adding a key to your Lookup table, select the **Key** checkbox, otherwise, if unselected, it becomes a column.
   b. In the **Name** field, enter a name for the key or the column.
   c. In the **Type** drop-down list, select the value type from LONG (for integers), STRING (character strings), or DOUBLE (for real numbers).
   d. Click **+** to add another Key value, and repeat steps a-c.
   Note: A maximum of 5 Key values may be created for a Lookup table.
   e. When done, click **Save**.

Deleting a Lookup Table

Complete these steps to remove an existing Lookup table:

1. Go to **RESOURCES > Lookup Table**.
2. Select the Lookup Table you wish to delete.
3. In the left panel, click on **-**.
4. Click **Yes** to confirm.

Working with Lookup Table Data

The following sections are available. For information on importing Lookup Table Data APIs, refer to the latest information here.

Usage Notes: Lookup table data may not be immediately available for Rules and Reports. Supervisor pushes the Lookup table changes to the Supervisor Redis database once every 5 minutes. Supervisor Master Redis immediately pushes the data to the Worker Slave Redis databases. Rule, Report and Query modules on Supervisor and Worker nodes re-read the Lookup tables from local Redis database, once every 5 minutes. Therefore in the worst case, it may take 10 minutes for data to be propagated to the analytics modules. Rules and Reports using Lookup tables should show the correct results after 10 minutes (worst case). In practice, FortiSIEM will have the results show up between 5 and 10 minutes.

- Adding Lookup Table Data
- Deleting Lookup Table Data
- Editing Lookup Table Data
- Importing Lookup Table Data

Note: A maximum of 10 million entries is allowed before the rest of the data is truncated.

Adding Lookup Table Data

To add Lookup table data to your Lookup table, take the following steps:

1. From the **RESOURCES > Lookup Tables** page, select your Lookup table.
2. Click **View**.
3. Click **New**.
4. Enter the Key or Column data.
5. Click **Save**.

Deleting Lookup Table Data

1. From the **RESOURCES > Lookup Tables** page, select your Lookup table.
2. Click **View**.
3. Select the row of data you wish to delete.
4. Click **Delete**.
5. Click **Yes** to confirm.

Editing Lookup Table Data

To edit Lookup table data in your Lookup table, take the following steps:

1. From the **RESOURCES > Lookup Tables** page, select your Lookup table.
2. Click **View**.
3. Select the row you wish to edit.
4. Click **Edit**.
5. Enter the new Key or Column data.
6. Click **Save**.

Importing Lookup Table Data

You can import lookup table data from user-defined lookup tables or from a system-defined lookup table.

Note: System-defined lookup table data can only be imported via Report.

To import Lookup table data from a Lookup table, take the following steps:

1. From the **RESOURCES > Lookup Tables** page, select the Lookup table you wish to import.
2. Click **Import**.

From the Import window, select one of the following depending on the Lookup table type (user or system defined) and continue with the instructions that follow.

User-defined Lookup Table Data

- Import from a CSV file
- Update via API
- Import via Report

System-defined Lookup Table Data

- Import System Defined Lookup Table Data via Report

Importing from a CSV File

If **Import from a CSV file** is selected, take the following steps:

1. Click **Choose File**, and select your CSV file.
2. In the **Field Separator** field, select the character that represents your separator for data.
3. In the **Field Quote Char** field, select the character that represents the beginning and end quotation used for strings.
4. Select **Ignore Header** to ignore the header from your CSV file.

5. Click the **Mapping** edit icon to define your data with your schema.
   a. From the **Mapped Field** drop-down list, select the key or column.
   b. From the **Position** drop-down list, select the position of the data from the csv file that should map to the key or column.
   c. Click **+** to create a new row.
   d. Click **Save** when done mapping your data.
6. Click **Save**.

Update via API

If **Update via API** is selected, take the following steps:

1. In the **URL** field, enter the API URL endpoint.
2. In the **User** field, enter the user name to access the API endpoint.
3. In the **Password** field, enter the password to access the API endpoint.
4. In the **Field** Separator, enter the character that represents your separator for data.
5. In the **Mapping** field, click the edit icon and take the following steps:
   a. From the **Mapped Field** drop-down list, select an existing mapping to set its position.
   b. From the **Position** drop-down list, select the position of the data from the csv file that should map to the key or column.
   c. Click **+** to add a new row for any additional mapping that is needed.
   d. Click **Save** when done mapping your data.
6. In the **Schedule** field, set the time which the update should occur by doing the following:
   a. In the **Start Time** field, set the time.
   b. In the **Schedule Recurrence Pattern**, set the period.
   c. Click **OK** when done.
7. Click **Save**.

Import via Report

If Import via Report is selected, take the following steps:

1. Click the **Report** edit icon.
2. Select a Report or CMDB Report, and click **OK**.
3. Click the **Mapping** edit icon.
4. From the Mapping dialog box, take the following steps:
   a. From the **Mapped** drop-down list, select an existing mapping to set its position.
   b. In the **Attribute** field, select or type the associated attribute to use.
   c. Click **+** to add a new row for any additional mapping that is needed.
   d. Click **Save** when done mapping your data.
5. Click the **Enabled** checkbox to configure a schedule.
6. Click the **Schedule** edit icon.

7. In the **Schedule Report Time Range** dialog box, do the following:
   a. In the **Time Zone** row, select the appropriate time from the drop-down lists.
   b. Select **Relative** or **Absolute** time, and then enter the information for period of time for recurrence.
   c. From the **Trend Interval** drop-down list, select the period of recurrence.
   d. Click **Next**.
8. In the **Schedule Time Range** dialog box, do the following:
   a. Enter the scheduling information using the **Start Time** fields/drop-down list.
   b. Under **Schedule Recurrence Pattern**, enter/select when the schedeul repeats.
   c. Under **Schedule Recurrence Range**, enter the Start date.
   d. Under **Schedule Recurrence Range**, choose/enter the time that the schedule ends.
   e. Click **Next**.
9. In the **Schedule Retention** dialog box, do the following:
   a. Under **Retention**, enter/choose the period of time for retaining reports.
   b. Click **OK**.
10. Click **Save** to save the Schedule configuration.
11. Click **Run now** to import the data.

Import System Defined Lookup Table Data via Report

If **Import via Report** is selected for a system-defined Lookup table, take the following steps:

1. Click the **Enabled** checkbox to configure a schedule.
2. Click the **Schedule** edit icon.
3. In the **Schedule Report Time Range** dialog box, do the following:
   a. In the **Time Zone** row, select the appropriate time from the drop-down lists.
   b. Select **Relative** or **Absolute** time, and then enter the information for period of time for recurrence.
   c. From the **Trend Interval** drop-down list, select the period of recurrence.
   d. Click **Next**.
4. In the **Schedule Time Range** dialog box, do the following:
   a. Enter the scheduling information using the **Start Time** fields/drop-down list.
   b. Under **Schedule Recurrence Pattern**, enter/select when the schedeul repeats.
   c. Under **Schedule Recurrence Range**, enter the Start date.
   d. Under **Schedule Recurrence Range**, choose/enter the time that the schedule ends.
   e. Click **Next**.
5. In the **Schedule Retention** dialog box, do the following:
   a. Under **Retention**, enter/choose the period of time for retaining reports.
   b. Click **OK**.
6. Click **Save** to save the Schedule configuration.
7. Click **Run now** to import the data.

Playbooks

A Playbook is a chain of actions that are taken based on logic programmed by a user. A Playbook can only be added, modified, or deleted through FortiSOAR. Playbooks can be executed on an incident. After creating a FortiSIEM user in FortiSOAR and configuring Playbook on FortiSIEM, playbooks can be executed through FortiSIEM. Additional information can also be found in Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

The following sections provide information on Playbooks:

- Viewing Playbooks
- Updating Playbooks

Viewing Playbooks

FortiSIEM can sync with FortiSOAR to pull the latest FortiSOAR Playbooks. These Playbooks are available on the **RESOURCES > Playbooks** page.

Column	Description
Name	The Playbook name is displayed.
Description	A description of what the Playbook does is displayed.

Updating Playbooks

To update your FortiSOAR playbooks, take the following steps.

Note: You must create a FortiSIEM user in FortiSOAR before proceeding with these steps. For more information, see here.

1. From **RESOURCES > Playbooks > FortiSOAR Playbooks**, click **Update**.
2. From the Update Playbook window, in the **URL** row, click the pencil icon to configure how FortiSIEM will connect with FortiSOAR. If there is an existing configuration, click the Edit icon to modify it.
   a. In the **Host Name** field, enter the IP address of the FortiSOAR application.
   b. In the User Name field, enter the username to access the FortiSOAR application.
   c. In the **Password** field, enter the password associated with the username for FortiSOAR application access.
   d. When done, click **Save**.
3. From the Update Playbook window, in the **Schedule** row, click **+** to create a new schedule, or the Edit icon to modify an existing one.
   a. In the **Start Time** field, enter the time when FortiSIEM will connect to FortiSOAR to retrieve any updated Playbooks.
   b. In the next two drop-down lists, define the time by selecting the appropriate time zone and region.
   c. Under **Recurrence Pattern** , select how frequently FortiSIEM will connect to FortiSOAR to check FortiSOAR Playbooks. Choices are: **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.
   d. Click on the **Start Now** field, and enter or select the Month, Day, and Year when update(s) should occur. The format is `mm/dd/yyyy`.
   e. When done, click **Save**.

Connectors

A connector is a solitary action that can be run by a user. Connectors can only be added, modified, or deleted through FortiSOAR. A connector can be run on an incident. After creating a FortiSIEM user in FortiSOAR and configuring Connector on FortiSIEM, connectors can be run through FortiSIEM. Additional information can also be found in Playbooks and Connectors under Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

The following sections provide information on Connectors:

- Viewing Connectors
- Updating Connectors

Viewing Connectors

FortiSIEM can sync with FortiSOAR to pull the latest FortiSOAR Connectors. These Connectors are available on the **RESOURCES > Connectors** page.

Column	Description
Name	The Connector name is displayed.
Description	A description of what the Connector does is displayed.

Updating Connectors

To update your FortiSOAR connectors, take the following steps.

Note: You must create a FortiSIEM user in FortiSOAR before proceeding with these steps. For more information, see here.

1. From **RESOURCES > Connectors > FortiSOAR Connectors**, click **Update**.
2. From the Update Connectors window, in the **URL** row, click **+** to configure how FortiSIEM will connect with FortiSOAR. If there is an existing configuration, click the Edit icon to modify it.
   a. In the **Host Name** field, enter the IP address of the FortiSOAR application.
   b. In the User Name field, enter the username to access the FortiSOAR application.
   c. In the **Password** field, enter the password associated with the username for FortiSOAR application access.
   d. When done, click **Save**.
3. From the Update Connectors window, in the **Schedule** row, click **+** to create a new schedule, or the Edit icon to modify an existing one.
   a. In the **Start Time** field, enter the time when FortiSIEM will connect to FortiSOAR to retrieve any updated Playbooks.
   b. In the next two drop-down lists, define the time by selecting the appropriate time zone and region.
   c. Under **Recurrence Pattern** , select how frequently FortiSIEM will connect to FortiSOAR to check FortiSOAR Playbooks. Choices are: **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.
   d. Click on the **Start Now** field, and enter or select the Month, Day, and Year when update(s) should occur. The format is `mm/dd/yyyy`.
   e. When done, click **Save**.

Machine Learning Jobs

Machine Learning Jobs are available through **ANALYTICS > Machine Learning**. You can access Machine Learning Jobs in **RESOURCES > Machine Learning Jobs**.

- Viewing Machine Learning Jobs
- Editing a Machine Learning Job
- Deleting a Machine Learning Job

Viewing Machine Learning Jobs

Complete these steps to view existing Machine Learning (ML) Jobs.

1. Go to **RESOURCES** > **Machine Learning Jobs**.
2. Expand the **Machine Learning Jobs** folder on the left panel. If needed, select a category sub-folder under the Machine Learning Jobs folder to view other ML jobs.
3. To view a specific Machine Learning Job, select it and click **View**.

The following information is available for each Machine Learning Job from the main pane.

Column	Description
Enabled	If checked, the job is enabled to execute per its configured schedule.
Job ID	The Job ID
Name	The name of the job
Description	A description of the job
Algorithm	The algorithm used to create the model.
Parameters	The parameters used for the ML algorithm.
For Org	The organization(s) that the ML job belongs to.
Schedule	The schedule when the inference is run.
Action	Displays the actions taken when job is executed.
Scope	The organizational scope that the ML job belongs to.

If a Machine Learning Job is selected, there are two tabs available in the lower part of the main pane to provide more information on the selected Machine Learning Job.

Summary tab - Displays the Machine Learning Job information in a dedicated pane, with additional information.

Schedule Result tab - Displays the schedule history of the selected Machine Learning Job.

Editing a Machine Learning Job

To edit a Machine Learning (ML) Job, take the following steps.

1. Navigate to **RESOURCES > Machine Learning Jobs**.
2. Select the Machine Learning Job you wish to modify and click **Edit**.
   Note: You can select a Machine Learning Job category sub-folder (Anomaly Detection, Classification, Clustering, Forecasting, Regression) or Ungrouped sub-folder to locate other Machine Learning jobs.
3. Make any necessary changes to the available fields (**Job Name**, **Job Description**, **Inference Schedule**, **Re-training Schedule**, **Action**).
4. Click **Save**.

Deleting a Machine Learning Job

To delete an existing Machine Learning (ML) Job, take the following steps.

1. Navigate to **RESOURCES > Machine Learning Jobs**.
2. Select the Machine Learning Job you wish to delete and click **Delete**.
3. Click **Yes** to confirm.

Osquery

Note: FortiSIEM 7.1.0 and Windows Agent 5.1 or later is required to utilize this feature.

osquery is an open-source simple instrumentation tool that can be used across the following operating systems, Windows, OS X (macOS), and Linux. It provides a simplified interface to query information held within an operating system itself, using an SQL based language.

In FortiSIEM, the user can create high level queries that will be pushed to Windows Agent, which will schedule, run and return data from the queries.

For more information on osquery, see osquery.

For more information on osquery schema, see osquery Schema.

Note: Don't forget to select **Windows** from the "Show only Tables compatible with" drop-down list when reviewing the osquery schema page to see the applicable schema.

FortiSIEM includes over 25 default system defined osquery templates, which you can see in **Resources > Osquery**, under **Agent**.

- Viewing osquery Templates
- Creating osquery Templates

Viewing osquery Templates

FortiSIEM comes with default system defined osquery templates. These templates are available on the **Resources > Osquery** page. These templates, and any newly created osquery templates appear on this page.

Column	Description
Name	The name of the osquery template.
Description	A description of what the osquery template does.
osquery	The actual osquery.
Severity	The configured severity for the osquery template, ranging from 1 to 10, with 10 being the highest severity.
Frequency	The frequency that the osquery template is run.
Event Type	The event type name associated with any events that occur under the executed osquery.
Scope	An osquery template is either a **System** template (a default osquery template), or a **User** template (created by the user).

Creating Osquery Templates

Creating an osquery template involves creating the osquery itself, and defining the event type attributes for events triggered by the osquery, which includes severity, frequency and event type name. You can also create an osquery template by cloning an existing osquery template using the **Clone** button and editing it.

- Creating an osquery Template
- Applying Changes to an osquery Template

Creating an osquery Template

Complete these steps to create an osquery template:

1. Navigate to **Resources > Osquery**.
2. Select the group where you want to add the new template.
3. Click **New** to create a new osquery template.
   a. In the **Name** field, enter the name of the osquery template.
   b. In the **Description** field, enter a description for the osquery template.
   c. In the **osquery** field, enter the osquery.
   Notes:
      - osquery involving EVENTED TABLE do NOT work with this feature. Example: process_etw_events
      - osquery must be mapped to an event attribute.
   d. In the **Event Type** field, enter the event type name for events that trigger from this osquery.
   Note: All osquery event types start with the following prefix: `PH_OSQUERY_WIN_`
   e. From the **Severity** drop-down list, select the severity associated with this event type.
   f. From the **Frequency** field and **Frequency** drop-down list, enter the length of time and select the unit of time (**Minute(s)**, **Hour(s)**, **Day(s)**) for how often Windows Agent runs the osquery template.
   g. Click **Test** to validate the osquery template.
   h. From the **Select Agent** drop-down list, select a Windows Agent and click **Test**.
   i. If Test succeeds, click **Save** to save the osquery template.

Applying Changes to an osquery Template

After a change has been made to an osquery template, you can click **Apply** to push the osquery template change to all Windows Agent Monitor Templates that have this existing osquery template.

Working with Cases

A Case is a collection of *related Incidents* that can be assigned to a FortiSIEM analyst for resolving the underlying issues detected by the Incidents. A Case can be created manually by an analyst or automatically by FortiSIEM according to an Automation Policy (previously called Notification Policy).

The following Case topics are available:

- Creating a Case Manually
- Creating a Case Automatically
- Viewing All Cases
- Searching Cases
- Viewing a Case in Depth
- Acting on a Case
- Case Dashboard
- Case Report
- Steps to Update Case Escalation from 6.x-7.1.x to 7.2.x

Creating a Case Manually

A Case can be manually created from Incidents or Events. The following steps need to be performed.

- Step 1 - Configure an Email Server for Notifications
- Step 2 - Create one or more FortiSIEM Analyst Teams
- Step 3 - Create a Case Management Policy
- Step 4 - Create a Case

Step 1 - Configure an Email Server for Notifications

FortiSIEM will notify Case Owners, Managers and Team Leads as a Case progresses through various stages and changes are made to the Case. For this reason, an email server must be set up first. If you have done this step for Incident notification or other purposes, then you can skip this step. The steps are:

1. Go to **Admin > Settings > System > Email**.
2. Under Email Settings, enter your Email server account information.
3. Click **Test Email**, and if it succeeds, click **Save**.

Detailed email server configuration steps are here.

Two points to be noted:

1. Case Management Policy controls email recipients and notification triggers. See Step 3 - Create a Case Management Policy for details.
2. The content of the email is fixed and cannot be customized.

Step 2 - Create one or more FortiSIEM Analyst Teams

FortiSIEM users assigned to a Case need some special attributes for proper enforcement of Case Management policies. For this reason, two special groups are created under **CMDB > Users**.

1. **FortiSIEM Users**: This includes all users that have login access to FortiSIEM. These users can be populated in one of the following ways:
   a. Manually define a user under **CMDB > Users > FortiSIEM Users**.
   b. Discovered users via LDAP and then assign a FortiSIEM Role.

2. **FortiSIEM Analysts**: This includes the subset of **FortiSIEM Users** that can be assigned to work on a Case.

FortiSIEM Analysts need to be organized into Teams. The organization of Teams can be arbitrary, but important use cases are

- *Based on Geography and Time zones* - e.g. US Team, Europe Team and APAC Team that have minimally overlapping work hours.
- *Based on skill set* – e.g. Windows Team, Firewall Team, Cloud Team, etc.
- *Based on Case Severities* – e.g. Critical Team, Medium Severity Team, Low Severity Team, etc.

You can configure FortiSIEM to attempt multiple Teams for finding an Assignee during Case Assignment. This can be specified during Automation Policy. See Step 4 - Create Automation Policy in Creating a Case Automatically.

Each Team needs:

- A **Team Lead** that can perform various roles such as (a)Manual Case Assignment, (b) Handling Case escalations that have violated Service Level Agreements (SLA).
- A **Team Queue** to hold Cases that cannot be assigned to any one. These Cases have to be manually assigned to Analysts.

Each Team Member needs:

- **Work schedule**: This information is used to automatically assign Tickets to users who are working when the Case is Created.
- **Time off schedule**: This information is used to automatically assign Tickets to users who are working when the Case is Created.
- A **Manager** for Case escalations and notifications.
- **Email** for notifications.

Follow these steps to create a FortiSIEM Analyst Team.

1. Go to **CMDB**.
2. From the left pane, click **Users**, and select **FortiSIEM Analysts**.
3. Click **+** from the left pane.
4. From the **Create New User Group** dialog box:
   a. In the **Group** field, enter the Team Name.
   b. In the **Description** field, enter a Description for the Team, such as brief geographical, time zone, or team intent focus.
   c. Under **Folders**, click **Users** to expand, and select the Team users from the **FortiSIEM Users >** folder and move them to **Items in Group** to place them in the group.
5. Click **Save**.
6. To make a user a Team Lead:
7. Select the user and click **Edit**.
   a. Under the **General** tab, select the **Team Lead** checkbox.
   b. Click **Save**.
8. To specify Work and Time off schedules:
   a. Select the user and click **Edit**.

b. To change the Work schedule: Under **FortiSIEM Attributes**, click on ✎ next to **Work Schedule**. By default, a Monday-Friday 8AM to 5PM local time schedule is chosen. To change this, use the GUI to create a new schedule after clicking on ✎. When done, click **Save**.

c. The Time Off schedule is similar to Work schedule and can be defined under **FortiSIEM Attributes**, by clicking on ✎ next to **Time Off Schedule**. When done, click **Save**.

d. Click **Save**.

See detailed Team Creation Steps in Working with User Groups and detailed User Creation steps in Adding Users.

Step 3 - Create a Case Management Policy

Case Management Policy Templates dictate how a Case is assigned to an Analyst and how the Case progresses from New state to Closed state. A Case Management Policy Template can be created under **Admin > Settings > General > Case Management**. This involves specifying the following:

1. **SLA (Violation) & Escalation**
   - Setting Case Due Date.
   - Whom to notify when Remaining Time is close to Due Date, or Due Date is violated.
   - Whom to notify when there is no Case Update within a defined period.
2. **(Case Change) Notifications**: The users that will receive notification when a Case Attribute changes (e.g. if Case Severity, Status are manually modified).
3. **(Case Change) Permission**: This specifies the Analysts that are permitted to change Case Status and edit Case Notes.
   - **Case Status Change**: Possibilities for **Change Status** are Anyone, Anyone within Team, Current Asignee, and/or Team Lead.
   - **Case Notes Edit**: Possibilities for **Edit Note** are Current Assignee and/or Team Lead.
4. **(Case) Auto Close**: This specifies whether to close a Case immediately if all Incidents in the Case are cleared, or keep the Case open for a specific duration before closing. Keeping the Case open enables newer Incidents with matching host name or IP addresses to be included in the Case.

To create a Case Management Policy:

1. Go to **Admin > Settings > General > Case Management**.
2. Go to **Case Management Policy** tab and click **New**.
3. Go through the SLA & Escalation, Permissions, Notifications and Auto Close sections and choose the settings for your case environment, based on the information above. The Auto-assignment section is for Automatic case Creation section, see Creating a Case Automatically for more information.
4. Click **Save**.

Details for creating Case Management Policies can be found in Adding/Editing a Case Management Policy.

Step 4 - Create a Case

- Create a Case from an Incident
- Add an Incident to an Existing Case
- Create a Case from an Event
- Add an Event to an Existing Case

Create a Case from an Incident

To manually create a **new Case from an Incident**:

1. Go to **Incidents > List View**.
2. From the **Columns** drop-down list, select **Case ID** if it is not a display column. Now **Case ID** shows as an Incidents display column.
3. Select an Incident. If no Case ID appears, then a new Case can be created for this Incident.
4. Make sure Incident is selected and from the **Actions** drop-down list, select **Create Case**.
5. From the **General** tab:
   a. In the **Summary** field, enter a Case Summary.
   b. Next to **Assignee**, click **Select** and select the user who is going to work on the Case.
   c. Click **Due Date** and set the due date (if you want to override the settings from Case Management Policy).
   d. (Optional) Click **Case Management Policy**, and select a Case Management Policy to apply a Case Management Policy to set the Due Date.
   Note: If no Case Management Policy is selected, the Assignee will only receive an email notification for the assignment. Afterward, regardless of any case changes, the Assignee will not receive any email notification.
   e. From the **Severity** drop-down list, choose the severity of the Case.
6. If you want to add other related Incidents to the Case, then from **Incidents** tab, select other related Incidents from the provided list. *The list is created automatically by including Incidents with the same IP address or host name in Incident Source and Incident Target fields. Only past Incidents are included here. Future Incidents with the same IP address or host name will not be included since the Case is created manually.*
7. Click **Save**. In the dialog box, choose **Jump to Cases** if you want to go to the specific Case just created, or click **Close** if you want to stay on the current page.

Add an Incident to an Existing Case

To manually **add an Incident to an Existing Case**:

1. Go to **Incidents > List View**.
2. From the **Columns** drop-down list, select **Case ID** if it is not a display column. Now **Case ID** shows as an Incidents display column.
3. Select an Incident. If no Case ID appears, then the incident can be added to an existing Case.

4. Make sure Incident is selected and from the **Actions** drop-down list, select **Add to Case...**.
5. Select the Case from the list provided.
6. Click **OK**. In the dialog box, choose **Jump to Cases** if you want to go to the specific Case you added the incident to, or click **Close** if you want to stay on the current page.

Note that if you create a Case automatically using Automation Policy, then related Incidents (*same IP address or host name in Incident Source and Incident Target fields*) will be automatically added to the Case.

Sometimes, an Incident may not have triggered and you may want to create a new Case from an event.

Create a Case from an Event

To manually create a **new Case from an Event**:

1. Go to **Analytics**.
2. Run a Report to capture the event raw message.
3. Hover over an event under the **Raw Event Log** column, click ▼, and select **Create Case**.
   a. In the **Summary** field, enter a Case Summary.
   b. Next to **Assignee**, click **Select** and select the user who is going to work on the Case.
   c. Click **Due Date** and set the due date (if you want to override the settings from Case Management Policy).
   d. (Optional) Click **Case Management Policy**, and select a Case Management Policy to apply a Case Management Policy to set the Due Date.
   Note: If no Case Management Policy is selected, the Assignee will only receive an email notification for the assignment. Afterward, regardless of any case changes, the Assignee will not receive any email notification.
   e. From the **Severity** drop-down list, choose the severity of the Case.
   f. Click **Save**. In the dialog box, Choose Jump to Cases if you want to go the specific Case just created, or click Close if you want to stay on this page.

Add an Event to an Existing Case

To **Add an Event to an Existing Case**:

1. Go to **Analytics**.
2. Run a Report to capture the event raw message.
3. Hover over an event under the **Raw Event Log** column, click ▼, and select **Add to Case...**.
   a. Select the Case from the list provided.
   b. Click **OK**. In the dialog box, choose **Jump to Cases** if you want to go to the specific Case you added the incident to, or click **Close** if you want to stay on the current page.

Creating a Case Automatically

FortiSIEM can automatically create a Case when an Incident triggers. The advantages of automatic case creation are

- Case is automatically assigned using the Automation Policy.
- Related Incidents (specifically Incidents with same IP address or host name in Incident Source and Incident Target fields) will be automatically added to the Case.

The following steps need to be performed to set up automatic Case creation.

- Step 1 - Configure an Email Server for Notifications
- Step 2 - Create one or more FortiSIEM Analyst Teams
- Step 3 - Create a Case Management Policy
- Step 4 - Create Automation Policy

Step 1 - Configure an Email Server for Notifications

FortiSIEM will notify Case Owners, Managers and Team Leads as a Case progresses through various stages and changes are made to the Case. For this reason, an email server must be set up first. If you have done this step for Incident notification or other purposes, then you can skip this step. The steps are:

1. Go to **Admin > Settings > System > Email**.
2. Under Email Settings, enter your Email server account information.
3. Click **Test Email**, and if it succeeds, click **Save**.

Detailed email server configuration steps are here.

Two points to be noted:

1. Case Management Policy controls email recipients and notification triggers. See Step 3 - Create a Case Management Policy for details.
2. The content of the email is fixed and cannot be customized.

Step 2 - Create one or more FortiSIEM Analyst Teams

FortiSIEM users assigned to a Case need some special attributes for proper enforcement of Case Management policies. For this reason, two special groups are created under **CMDB > Users**.

1. **FortiSIEM Users**: This includes all users that have login access to FortiSIEM. These users can be populated in one of the following ways:
   a. Manually define a user under **CMDB > Users > FortiSIEM Users**.
   b. Discovered users via LDAP and then assign a FortiSIEM Role.
2. **FortiSIEM Analysts**: This includes the subset of **FortiSIEM Users** that can be assigned to work on a Case.

FortiSIEM Analysts need to be organized into Teams. The organization of Teams can be arbitrary, but important use cases are

- *Based on Geography and Time zones* - e.g. US Team, Europe Team and APAC Team that have minimally overlapping work hours.
- *Based on skill set* – e.g. Windows Team, Firewall Team, Cloud Team, etc.
- *Based on Case Severities* – e.g. Critical Team, Medium Severity Team, Low Severity Team, etc.

You can configure FortiSIEM to attempt multiple Teams for finding an Assignee during Case Assignment. This can be specified during Automation Policy. See Step 4 - Create Automation Policy for details.

Each Team needs:

- A **Team Lead** that can perform various roles such as (a)Manual Case Assignment, (b) Handling Case escalations that have violated Service Level Agreements (SLA).
- A **Team Queue** to hold Cases that cannot be assigned to any one. These Cases have to be manually assigned to Analysts.

Each Team Member needs:

- **Work schedule**: This information is used to automatically assign Tickets to users who are working when the Case is Created.
- **Time off schedule**: This information is used to automatically assign Tickets to users who are working when the Case is Created.
- A **Manager** for Case escalations and notifications.
- **Email** for notifications.

Follow these steps to create a FortiSIEM Analyst Team.

1. Go to **CMDB**.
2. From the left pane, click **Users**, and select **FortiSIEM Analysts**.
3. Click **+** from the left pane.
4. From the **Create New User Group** dialog box:
   a. In the **Group** field, enter the Team Name.
   b. In the **Description** field, enter a Description for the Team, such as brief geographical, time zone, or team intent focus.

   c. Under **Folders**, click **Users** to expand, and select the Team users from the **FortiSIEM Users >** folder and move them to **Items in Group** to place them in the group.
5. Click **Save**.
6. To make a user a Team Lead:
   a. Select the user and click **Edit**.
   b. Under the **General** tab, select the **Team Lead** checkbox.
   c. Click **Save**.
7. To specify Work and Time off schedules:
   a. Select the user and click **Edit**.
   b. To change the Work schedule: Under **FortiSIEM Attributes**, click on ✎ next to **Work Schedule**. By default, a Monday-Friday 8AM to 5PM local time schedule is chosen. To change this, use the GUI to create a new schedule after clicking on ✎. When done, click **Save**.
   c. The Time Off schedule is similar to Work schedule and can be defined under **FortiSIEM Attributes**, by clicking on ✎ next to **Time Off Schedule**. When done, click **Save**.
   d. Click **Save**.

See detailed Team Creation Steps in Working with User Groups and detailed User Creation steps in Adding Users.

Step 3 - Create a Case Management Policy

Case Management Policy Templates can be created under **Admin > Settings > General > Case Management**. This involves specifying the following:

1. **SLA (Violation) & Escalation**
   - Setting Case Due Date.
   - Whom to notify when Remaining Time is close to Due Date, or Due Date is violated.
   - Whom to notify when there is no Case Update within a defined period.
2. **Automatic Case Assignment**: Auto-assignment specifies the rules to find a Case Assignee. In general, the Automation Policy may specify more than one Team in a specific order.
   - Finding an Assignee within a Team – 3 options are provided.
     - Always Assign to Team Lead, if available.
     - Assign Randomly within Available Team members.
     - Assign to Available Team member with least number of Cases.
   - FortiSIEM may fail to find an available Team member within the first Team. When this occurs, then the following logic is applied:
   - No Assignee found within Team
     - For Important (e.g. Critical and High Severity by default) Cases, find next Assignee within the next Team. If Assignee still can not be found, then 4 choices are provided:
       - Assign to First Team Lead
       - Leave in First Team Queue
       - Assign to Last Team Lead

        - Leave in Last Team Queue
    - For not so important (e.g. Medium and Low Severity by default) Cases, 2 choices are provided:
        - Leave in First Team Queue
        - Leave in Last Team Queue
    - User can configure Important categories by selecting their choices (Critical, High, Medium, Low) from the drop-down list.
3. **(Case Change) Notifications**: Select the users that will receive notification when a Case Attribute changes (e.g. if Case Severity, Status are manually modified).
4. **(Case Change) Permissions**: Specify the Analysts that are permitted to change Case Status and edit Case Notes.
    - **Case Status Change**: Possibilities for **Change Status** are Anyone, Anyone within Team, Current Asignee and/or Team Lead.
    - **Case Notes Edit**: Possibilities for **Edit Note** are Current Assignee and/or Team Lead.
5. **(Case) Auto Close**: Auto Close specifies whether to close a Close immediately if all Incidents in the Case are cleared, or keep the Case open for a specific duration before closing. Keeping the Case open enables newer Incidents with matching host name or IP addresses to be included in the Case.

To create a Case Management Policy:

1. Go to **Admin > Settings > General > Case Management**.
2. Go to **Case Management Policy** tab and click **New**.
3. Go through the SLA & Escalation, Permissions, Notifications and Auto Close sections and choose the settings for your case environment, based on the information above.
4. Click **Save**.

Details for creating Case Management Policies can be found in Adding/Editing a Case Management Policy.

Step 4 - Create Automation Policy

Automation policy provides fine grained control over the set of Incidents for which Cases will be created.

The following Incident attributes can be chosen to determine if a Case needs to be created:

- Incident Severity
- Specific Rules or Rule Groups
- Time Range
- Affected Items in Incident Source And Target
- Affected Orgs (Service Provider Case)

For FortiSIEM to automatically find an Assignee and then manage the Case, you need to specify:

1. A Case Management Policy
2. An ordered list of FortiSIEM Analyst Teams to work on the Case. FortiSIEM will try to find users within the Teams in the specified order.

You can create multiple policies and arrange them using Policy Rank. Lower Ranks appear first in the list and are evaluated first. **The First matched Policy is chosen to create and manage the Case for that Incident.**

To create an **Automation Policy**:

1. Go to **Admin > Settings > General > Automation Policy**.
2. Click **New**.
3. Enter the following Incident attributes:
   a. In the **Name** field, enter the name of the policy.
   b. From the **Severity** checkboxes, select the Incident Severities.
   c. From **Rules**, click ▼, then use the arrow buttons and select the Rule Groups or individual rules. When done, click **Save**. If you do not choose anything, then the default choice is ANY (meaning ALL Rules).
   d. From **Time Range**, click ▼, select **Define Time Range**, then use the GUI to configure your time range. When done, click **Save**. If you do not choose anything, then the default choice is ANY (meaning ALL Time Ranges).
   e. From **Affected Items**, click ▼to specify specific devices and/or IP ranges. Click **Select Device** to configure specific devices using the GUI. Click **Add IP/Range** to configure an IP address or IP Range. When done, click **Save**. If you do not choose anything then the default choice is ANY (meaning ALL Affected Items).
   f. From **Affected Orgs**, click ▼and use the GUI to select the Affected Organizations for your Service Provider deployment. When done, click **Save**. If you do not choose anything then the default choice is ANY (meaning ALL Organizations).
   g. For **Action**: check the **Create Case when an incident is created** checkbox and click on ✎.

      Then
      i. From the **Case Management Policy** drop-down list, select a Case Management Policy.
      ii. From the **Teams FIRST** drop-down list, select the FortiSIEM Analyst Team that will first handle the case. Then select **+** and choose the next FortiSIEM Analyst Team from the **THEN** drop-down list that will handle the Case if no one from the first Team is found. Click **+** and select another FortiSIEM Analyst Team as needed.
      iii. Click **Save** when finished with selecting Teams.
   h. Click **Save**.
4. You can change the order of evaluation by selecting a Policy and clicking the **Up** or **Down** buttons.
5. Click a policy's **Enabled** checkbox to enable that policy and its rules.

Detailed steps for creating an Automation Policy can be found here.

Viewing All Cases

To have tabular view of all Cases, go to **Cases > List**.

- Case Summary
- Case Attributes
- Viewing Specific Case Attributes

Case Summary

A summary is provided at the top. It also functions as a filter appear at the top of the Cases List View page. To use the filter view, click the Case Category "button" you wish to get a filtered view of. For example, click "New" to display only new cases. For more information on the Case Categories, see the following table.

Case Category	Description
New	The number of new cases. A case is classified as new if it has been created, but has not yet been assigned to a user. Hence, a case labeled as "New" can only come from an automation policy.
Open	The number of open cases. Cases considered Open are under the Status of Assigned, In Progress, Pending Customer Feedback, or Received Customer Feedback.
Open For Me	The number of open cases that are assigned to the user currently logged into FortiSIEM.
Critical	The number of cases with critical severity that are also open.
High	The number of cases with high severity that are also open.
Escalated	The number of cases that are open and have also met the case management policy's escalation requirements.
Overdue	The number of cases that are open and have gone past the due date.
Closed	The number of cases that are closed.

Case Attributes

A Case has the following attributes. By default, only a specific set of attributes are displayed. You can click **Columns** and choose the attributes you want to display in the **Cases > List View**.

Case ID: Unique ID of the Case.

Case Summary: Case Title describing the Case.

Assets: Assets include the Host name and IP in Incident Source and Target for all for all Incidents in the Case.

Assigned: The time when the Case was assigned to a user.

Assignee: The person currently assigned to handle the case. The Assignee can change while a case is being worked on.

Case Management Policy: Name of the Case Management Policy governing the Case.

Closed: The time when the Case was closed.

Close Code: A Code that indicates how the Case was resolved. There are several system defined ones in **Admin > Settings > General > Case Management > Case Close Codes**.

- Manual-Analyst-Disable: Manually by Analyst by Disabling Rule
- Manual-Analyst-Exception: Manually by Analyst by Rule Exception
- Automatic-FSM-FP: Automatically by FortiSIEM as False Positive
- Manual-Analyst-FP: Manually by Analyst as False Positive
- Manual-Analyst-Testing: Manually by Analyst as Security Testing
- Manual-Analyst-Known: Manually by Analyst as Known Problem
- Automatic-FSM-TP: Automatically by FortiSIEM as True Positive
- Manual-Analyst-Modification: Manually by Analyst by Rule Modification
- Manual-Analyst-TP: Manually by Analyst as True Positive

You can add your own by clicking **New** from **Admin > Settings > General > Case Management > Case Close Codes**.

Close Code Description: Provides a description of the Case Close Code.

Created: The time when the Case was created.

Creator: The person or entity (system) that created the case. For manually created Cases, it specifies the user that created the Case. For automatically created cases, Creator is system.

Due: The time by which the Case is expected to be resolved. A Case is escalated according to Case Management Policy, when Due Date is approaching.

Elapsed: The percentage of time that has occurred before a case has reached its due date, or "Overdue", if the case due date has been reached.

Incident ID: IDs of Incidents included in the Case.

Interested: Users interested in the Case. This value can be set from the Cases Page by selecting a Case, then selecting **Actions > Set Interested**.

Organization: The FortiSIEM Organization to which this Case belongs. A Case can only include Incidents or events belonging to one Organization.

Resolution Time: The time duration it took to resolve the Case:

Risk: Case Risk is computed from entity (Host or User) Risk using a proprietary algorithm.

- **Entity Risk** captures Asset Importance along with Incident Severity, Incident Resolution and Incident Rarity of all Incidents that the entity is involved in.

- **Case Risk** captures Entity Risk of all entities involved in the Case.

Case Risk is a number between 0-100, with a higher number indicating higher risk.

Risk Explanation: An explanation of Case Risk showing the Entity Risk for all entities involved in the Case. An explanation of Entity Risk is provided including Asset Importance and Incident Severities and Rarities for all Incidents in the Case.

Severity: Case Severity indicates relative Case prioritization. For Automatically created Cases, the Case Severity is derived from the Incident Severities of all Incidents included in the Case. For Manually created cases, the Case Severity is set by the user. Severity is also color coded.

- **Critical**: A Case that requires the highest prioritization. An automation policy assigns Critical severity if the Case contains two or more high severity Incidents.
- **High**: A Case that requires high prioritization. An automation policy considers a case with one high severity incident to be a high severity case.
- **Medium**: A Case with medium prioritization.
- **Low**: A Case with low prioritization.

Stage: Case Stage specifies Incident Response stage. It can be one of the following:

- **Detection**: A case automatically defaults to "Detection", where a potential threat has been detected. The user can manually update to the next stage to indicate where they are with the case.
- **Analysis**: Inspection of potential threat.
- **Containment**: Threat isolation.
- **Eradication**: Removal of threat.
- **Recovery**: Restoration of system and relevant updates.
- **Lesson Learned**: Postmortem.

Status: Case Status indicates the current progress on the Case. It can be one of the following:

- **New**: Case created by the system through an automation policy that is currently in a Team Queue and is unassigned to a user.
- **Assigned**: Case that is assigned to a user.
- **In Progress**: Case where a user has manually acknowledged to be working on the case.
- **Pending Customer Feedback**: Case where the user is waiting for customer feedback to proceed.
- **Received Customer Feedback**: Case where the user has received customer feedback and is able to proceed with the case.
- **Closed**: Case that has been resolved and marked as closed. A closed case is also associated with a close code that provides information on the "how and why" the case was closed.

Viewing Specific Case Attributes

If you select a Case, a vertical slide in display shows the Case Attributes. You can choose to display specific case attributes from **Cases > List > Columns**.

Searching Cases

By default, only New and Open Cases for the last 10 days are shown in the Cases List View. If you want to search a specific Case or list all Cases with specific filtering criteria, then click on the icon and a

Search filter pane opens on the left. You can select Case Attributes and the results are displayed on the table on the right.

Viewing a Case in Depth

You can drill down on a Case from Cases > List View, select a Case, then click Action> Drill Down.

- Overview
- Explore View
- MITRE ATT&CK View
- Investigate View
- Case Notes
- Case Evidence
- Action History

Overview

The Overview page provides the following case information:

- **Case Overview** - The following Case attributes are shown in this section: Organization, Severity, Risk and Risk Explanation. For details on case attributes, see Case Attributes.
- **Case Progress** - The following Case attributes related to the Case's progress are shown in this section: Status, Stage, Assignee, Created, Assigned, Interested, Due, Elapsed, Close Code, Close Code Description and Case Management Policy. For details on case attributes, see Case Attributes.
- **Incidents** - All incidents related to a case are listed here. Clicking on an incident's ID link will take you to that incident on the **Incidents List View** page.
- **Hosts** - The assets involved with the case are listed, for example IP addresses.
- **Observables** - Events, non-threatening or malicious, on a network or system.
- **Techniques** - Any relevant MITRE ATT&CK Tactics and Techniques are listed.

Explore View

Case Explore View provides the same view as **Incidents > Explorer**, but *only for the Incidents included in a Case*.

See here for details.

MITRE ATT&CK View

Case MITRE ATT&CK View provides the same view as **Incidents > MITRE ATT&CK**, but *only for the Incidents included in a Case*.

See here for details.

Investigate View

Case Investigate View provides the same view as **Incidents > Investigate**, but *only for the Incidents included in a Case*. The entire Incident Attack Graph is shown at once for all Incidents included in the Case.

See here for details.

Case Notes

The Notes section displays all existing notes for a case, and allows you to Add, Edit and/or Delete a note, assuming you have permission to do so. Click on the refresh icon to update the notes section. The options to **Edit** or **Delete** a note appear in the right upper corner of each note. To add a new note, enter the note in the **Add New Note** section, and click the **Save** icon when done. For more information on the tools available when creating a note, see the following table.

Icon	Description
Undo	Click to undo the latest change.
Redo	Click to re-apply the last undo change.
Text Size	Increase/decrease text size. Click the Text Size icon, and select a text size to apply to selected text, or for the text to be entered.
Font Color	Set the color of your font. Click the Font Color icon, and select a color to apply to selected text, or for the text to be entered. You can also enter a hex color code and click the Submit icon instead of selecting a pre-defined color. If you click the Remove Format icon from the color selection, only the color format will be changed.
Align	Configure the alignment of your text. Click the Align icon, and select one of the following options: • Align left - Click to align text to the left. • Align center - Click to center text. • Align right - Click to align text to the right. • Align Justify - Click to apply justification alignment to the text.
Bold	Click the Bold icon to toggle the Bold format on or off. You can enter text with Bold formatting, or select text and apply the Bold format.
Underline	Click the Underline icon to toggle the Underline format on or off. You can enter text with the Underline format, or select text and apply the Underline format.
Italic	Click the Italic icon to toggle the Italic format on or off. You can enter text that is Italicized, or select text and apply the Italic format.
Strike	Click the Strike icon to toggle Strikethrough format on or off. You can enter text with the strikethrough format, or select text and apply the Strikethrough format.
Remove Format	Select the text you wish to remove existing text formatting from, then click the Remove Format button. This remove all formatting from the selected text. For example, if the size of your text is 72 pixels, with a red font, clicking remove format will change the text size to the default size, and color.
Full screen	Click to toggle between full screen and window view.
Save	Click to save the note content.

Case Evidence

The Evidence page provides the trigger events for the Incidents in the case, and any events that have also been linked to the case. Any attachments that have been uploaded to the case can be found in the right pane.

The main pane is comprised of two sections. The left column displays the incidents and events associated with the case. You can select an incident under **Incidents in Case**, or select **Events** to see its raw event data. Click on **Detail >** to display the Event Details sidebar. This sidebar provides the raw message and a list of the event's attributes for examination.

The right pane displays all files attached to the case. Next to each file is a Download icon and Trash icon. Click the Download icon to download an attachment. Click the Trash icon to remove the attachment from a case.

Action History

The Action History page provides the following:

Case Action History - Timeline of all case actions that have been taken.

Incidents Action History - Timeline of all the actions taken to incidents related to the case.

Acting on a Case

You can take an Action on a Case from either the **Cases > List View** or single Case Drill Down View.

- From **Cases > List View**, select a Case, then click **Actions** and select an **Action**.
- From the same View, you can choose **Actions > Drill Down** and then choose an Action from that page.

Various Actions are enumerated below.

FortiAI: Click to send Case information to FortiAI for analysis. FortiAI must be configured for this feature to work.

Case Details: Open the Case Details sidebar to view case details. The default selection is **Details**.

- **Details** - Displays information about a case - Case ID, Severity, Risk, Risk Explanation, Organization, Summary, Incident ID, Assets, Status, Stage, Assignee, Created, Due, Elapsed. See Case Attributes for more information.
  Note: If a certain detail does not exist, the attribute is not presented. For example, if a case was created with an event, and there is no incident, no Incident ID appears in the Case Details sidebar under Details.
- **Action History** - Displays Case Action History, and Incidents Action History.
- **Actions** - Click to access drop-down list of actions that can be taken.
- **Drill Down** - Click Drill Down to access the Overview, Explore, MITRE ATT&CK®, Investigate, Notes, Evidence, and Action History tabs for enhanced analysis. See Viewing a Case in Depth for more information.
- **Display sidebar when selecting a case** - Select if you wish for the Case Details sidebar to appear when a case is selected.

Drill Down: Click **Drill Down** to access the Overview, Explore, MITRE ATT&CK®, Investigate, Notes, Evidence, and Action History tabs for enhanced analysis. See Viewing a Case in Depth for more information.

Assign to...: Click to change the user assigned to the case by clicking **Select**, then selecting the user to assign the case to. You can use the GUI to select a group, then the user under **FortiSIEM Analysts** as well. The case due date can also be changed by clicking on the Due Date widget. When done, click **Save**.

Set Interested (Users): Click to configure users as Interested. If a user is set as Interested, and the Case Management Policy associated with the case includes notification for Interested Recipient(s), the Interested user(s) will receive notifications. To use, take the following steps:

1. Click **Select**.
2. Click on the user you wish to add as Interested, then click **OK**.
   To add another user, click **+** and repeat steps 1 and 2.
3. When done, click **Save**.

Set Due Date:Set the case due date by taking the following steps.

1. Click on the **Due Date** field.
2. From the year and month drop-down lists, select the year and month.

3. Select the day of the month.
4. Select the Hour, minute, second, and AM/PM from the respective drop-down lists.
5. Click on the Due Date field when done, and click **Save**.

Set Status: Choose one of the available options to set the Case status. For more information, see Status in Case Attributes.

- New
- Assigned
- In Progress
- Pending Customer Feedback
- Received Customer Feedback
- Closed

Set Stage: Choose one of the available options to set the Case stage. For more information, see Stage in Case Attributes.

- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Lesson Learned

Set Severity: Choose one of the available options to set the Case severity. For more information, see Severity in Case Attributes.

- **Critical**
- **High**
- **Medium**
- **Low**

Set Case Management: Choose a case management policy to apply to the case using the **Case Management Policy** drop-down list and then click **Save**.

Add Note: Click to add a selected note to the case. In the Add New Note section, enter any text you wish to include about the case. When done, click **Save**.

For more information on features in Add Note, see here.

Add Attachment: To add an attachment to a note, click **Choose Files**, select your file(s) and click **Upload**.

- To select multiple files, hold down the Ctrl key while selecting files.
- The maximum size of a file attachment is 20MB.
- Existing attachments to a case can be found from the Drill Down **Evidence** tab.

Edit Summary: Click on the **Summary** field, and make any changes you need. When done, click **Save**.

Export Case: If you have any notes, add them to the **User Notes** field. To export the case as a PDF file, click **Generate**. After the report has been generated, click **View** to examine the case file.

Case Dashboard

Clicking **Cases > Overview** brings you to the Case Dashboard. It consists of 3 sub-dashboards.

- Case Health Dashboard
- Case KPI Dashboard
- Case Handling Dashboard

Case Health Dashboard

Case Health Dashboard provides an easily accessible summary of currently active cases.

- The first row shows the total number of **New**, **Open**, **Escalated** and **Overdue** cases. A Case is considered Escalated if it is close to violating the Due date and the exact criteria is specified in the associated Case management Policy.
- Second and Third row charts show the details of these Case types.
- For **New Cases**, the specific cases and their severity is shown along with a count by Severity.
- For **Open Cases**, the number of Open cases by Severity and by Analyst are provided.
- For **Escalated Cases**, the listing of cases is provided.
- For **Overdue Cases**, the listing of cases is provided.
- A Case Inflow (New) and Case Outflow (Closed) Trend is provided.

See diagram below for information that each Case Health Dashboard panel provides.

New - Number of New Cases	**Open** - Number of Open Cases	**Escalated** - Number of Escalated Cases	**Overdue** - Number of Overdue Cases
New Cases - List of New Cases	**Open by Severity** - Chart shows Open Cases by their severity (Critical, High, Medium, Low).	**Escalated Cases** - List of Escalated Cases	**OverDue Cases** - List of OverDue Cases
New by Severity - Chart shows New Cases by their severity (Critical, High, Medium, Low).	**Open Cases by Analysts** - Chart shows number of open cases associated with assignees.	**Case Trend** - A Case Inflow (New) and Case Outflow (Closed) Trend chart	

Case KPI Dashboard

Case KPI Dashboard shows the following information:

- **Event to Case Conversion** chart shows the relative proportions of Events, Incidents and Cases in a time window. This demonstrates that FortiSIEM only requires users to deal with a small number of cases instead of much larger number of Incidents and Events.
- **Data Source** chart shows:
  - Which Data Sources lead to Incidents by Severity.
  - Which Incidents lead to Cases by Severity.
- **Case Status** charts the number of cases currently in each Case Status category along with the average time spent in each category.
- **Case Stage** charts the number of cases currently in each Case Stage category along with the average time spent in each category.

Case Handling Dashboard

Case Handling Dashboard shows the following information:

- **Closed Cases By Code** shows the proportion of Case Close Codes among Closed Cases.
- **Assigned Case Trend By User** chart shows the number of Cases that top users are working on a day by day basis.
- **Resolution Time By User** chart shows the top analysts taking the most time to resolve cases.
- **Resolution Time By Case** chart shows the top Cases taking the most time to resolve.

Case Report

To run a report involving Cases, take the following steps:

1. Go to **CMDB > CMDB Reports**.
2. Select a folder and click **New**.
3. In **Step 1: General**, take the following steps:
   a. In the **Report Name** field, enter the name of the report.
   b. In the **Description** field, enter a description, such as the purpose of the report, or what it provides.
   c. From the **Target** drop-down list, select **CASE**.
4. Click **Step 2: Define Condition**, and take the following steps:
   a. Under **Attribute**, select a case attribute.
   b. Under **Operator**, select an operator.
   c. Under **Value**, select/enter a value.
   d. Click **+** to add a new row for additional conditions, and repeat 4a.-4c..
5. Click **Step 3: Define Display Column**, and select the Case Attributes to display.
6. Click **Save**.
7. With the case report selected, click **Run**.

The following Case Attributes are available. For more information, see Case Attributes.

- **Age**: This new attribute specifies the difference between Current Time and Case Assignment Time.
- **Assigned**: The time when the Case was assigned to a user.
- **Assignee**: The person currently assigned to handle the case.
- **Case Entity**: Same as Case Assets.
- **Case ID**: Unique ID of the Case.
- **Case Title**: Case Title describing the Case.
- **Close Code**: A Code that indicates how the Case was resolved.
- **Closed**: The time when the Case was closed.
- **Created**: The time when the Case was created.
- **Creator**: The person or entity (system) that created the case.
- **Customer ID**: FortiSIEM Organization ID (for Service Provider deployments).
- **Customer Name**: FortiSIEM Organization name (for Service Provider deployments).
- **Due**: The time by which the Case is expected to be resolved.
- **Incident IDs**: Comma separate list of IDs of Incidents included in the Case.
- **Resolution Time**: The time duration it took to resolve the Case
- **Rule Name**: List of rule names associated with Incidents included in the Case
- **Severity**: Case Severity indicates relative Case prioritization.
- **Stage**: Case Stage specifies Incident Response stage.
- **State**: Same as Case Status, indicates the current progress on the Case.

For the following Case Attributes, you need to use the numerical values in **Step 2: Define Condition:**, e.g. Severity = 0 to get Critical Cases, Case State = 5 to get OverDue Cases, etc.

Case Attribute	String Value	Numerical value
Case Stage	Detection	0
	Analysis	1
	Containment	2
	Eradication	3
	Recovery	4
	LessonLearned	5
Case State	New	0
	Assigned	1
	Closed	2
	In Progress	3
	OverDue	5
	Unassigned	6
	Pending Customer Feedback	7
	Received Customer Feedback	8
Close Code	Automatic-FSM-TP	0
	Automatic-FSM-FP	1
	Manual-Analyst-TP	2
	Manual-Analyst-FP	3
Severity	Critical	0
	High	1
	Medium	2
	Low	3

Steps to Update Case Escalation from 6.x-7.1.x to 7.2.x

If you had an existing case escalation policy prior to FortiSIEM 7.2.0 or later, you must take the following steps for these old cases/case users to work with FortiSIEM 7.2.0 or later.

- Step 1 - Move or Create Prior Case Users to FortiAnalysts Groups
- Step 2 - Update your Escalation Policy (now called a Case Management Policy)
- Step 3 - Associate Case Management Policy with an Automation Policy

Step 1 - Move or Create Prior Case Users to FortiAnalysts Groups

If you have any users involved with cases prior to FortiSIEM 7.2.0 or later that you wish to use, you will need to move these users so they are in a group under **FortiSIEM Analysts** in **CMDB**. The general steps to create a group and move users are provided:

1. Navigate to **CMDB > Users**.
2. Expand **Users**.
3. Select **FortiSIEM Analysts**.
4. In the left upper pane, click**+** to create a folder/group.
5. In the **Group** field, enter a name.
6. Use the GUI to move prior case user(s) to a FortiSIEM Analysts group.
   Note: Remember to update these users so they have a Work Schedule, and if you wish to designate a user as a Team Lead, to select the **Team Lead** checkbox during your update for that user. For more information, see here.
7. Click **Save**.

Step 2 - Update your Escalation Policy (now called a Case Management Policy)

1. Navigate to **Admin > Settings > General > Case Management**.
2. Select your Case Management Policy and click **Edit**.
3. Update your settings appropriately depending on whether to plan to handle cases manually or through an automation policy.

- For manual case management, configure everything except the Auto-assignment section. More information about configuration is available here.
- For automation, configure the entire case management policy. More information about configuration is available here.

4. Click **Save**.

Step 3 - Associate Case Management Policy with an Automation Policy

Automation policy provides fine grained control over the set of Incidents for which Cases will be created.

The following Incident attributes can be chosen to determine if a Case needs to be created:

- Incident Severity
- Specific Rules or Rule Groups
- Time Range
- Affected Items in Incident Source And Target
- Affected Orgs (Service Provider Case)

For FortiSIEM to automatically find an Assignee and then manage the Case, you need to specify:

1. A Case Management Policy
2. An ordered list of FortiSIEM Analyst Teams to work on the Case. FortiSIEM will try to find users within the Teams in the specified order.

You can create multiple policies and arrange them using Policy Rank. Lower Ranks appear first in the list and are evaluated first. **The First matched Policy is chosen to create and manage the Case for that Incident.**

To create an **Automation Policy**:

1. Go to **Admin > Settings > General > Automation Policy**.
2. Click **New**.
3. Enter the following Incident attributes:
   a. In the **Name** field, enter the name of the policy.
   b. From the **Severity** checkboxes, select the Incident Severities.
   c. From **Rules**, click ▼, then use the arrow buttons and select the Rule Groups or individual rules. When done, click **Save**. If you do not choose anything, then the default choice is ANY (meaning ALL Rules).
   d. From **Time Range**, click ▼, select **Define Time Range**, then use the GUI to configure your time range. When done, click **Save**. If you do not choose anything, then the default choice is ANY (meaning ALL Time Ranges).
   e. From **Affected Items**, click ▼to specify specific devices and/or IP ranges. Click **Select Device** to configure specific devices using the GUI. Click **Add IP/Range** to configure an IP address or IP Range. When done, click **Save**. If you do not choose anything then the default choice is ANY (meaning ALL Affected Items).

f. From **Affected Orgs**, click ▼and use the GUI to select the Affected Organizations for your Service Provider deployment. When done, click **Save**. If you do not choose anything then the default choice is ANY (meaning ALL Organizations).

g. For **Action**: check the **Create Case when an incident is created** checkbox and click on .

Then

i. From the **Case Management Policy** drop-down list, select a Case Management Policy.

ii. From the **Teams FIRST** drop-down list, select the FortiSIEM Analyst Team that will first handle the case. Then select **+** and choose the next FortiSIEM Analyst Team from the **THEN** drop-down list that will handle the Case if no one from the first Team is found. Click **+** and select another FortiSIEM Analyst Team as needed.

iii. Click **Save** when finished with selecting Teams.

h. Click **Save**.

4. You can change the order of evaluation by selecting a Policy and clicking the **Up** or **Down** buttons.
5. Click a policy's **Enabled** checkbox to enable that policy and its rules.

Detailed steps for creating an Automation Policy can be found here.

Working with Incidents

When a correlation rule triggers, an incident is created in FortiSIEM. This section describes how to view and manage Incidents in FortiSIEM. There are six views:

- **Overview**: This view provides a "top down" view of the various types of Incidents and impacted hosts.
- **List View**: This tabular view enables the user to search incidents and take actions.
- **Risk View**: This view organizes impacted entities (Devices, Users) by Risk based on the triggered incidents.
- **Incident Explorer View**: This view helps users to correlate Actors (IP, Host, User) across multiple incidents, without creating multiple reports in separate tabs.
- **MITRE ATT&CK View**This view classifies security events detected by FortiSIEM into MITRE ATT&CK categories. You can select Information Technology (**IT**) or Industrial Control Systems (**ICS**) MITRE ATT&CK view.
  Note: Previously this was Attack View.
- **UEBA View**: This view monitors the AI alerts obtained from FortiInsight.

To interact with an incident, see Acting on Incidents.

FortiSIEM can cross-correlate incident data and perform lookups on selected external ticketing/work flow systems. See Filtering in the Incident Explorer View and Lookups Via External Websites.

FortiSIEM can also be configured to collect this host vulnerability data to preform CVE-Based IPS False Positive Analysis.

Overview View

The Overview view provides a "top down" view of various types of Incidents and impacted hosts. Go to **INCIDENTS** > **Overview** to see this view. Overview can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Overview** from the **Incident Home** drop-down list.

The panel is divided into three sections:

- **Incidents by Category** – displays Incident Counts By Function and Severity.
- **Top Incidents** – displays the Top Incidents sorted first by Severity and then Count.
- **Top Impacted Hosts** – displays Top impacted hosts by Severity or Risk Score. Click **Severity** or **Risk Score** to display this section by Severity or Risk Score respectively.

To change the incident time range, choose the **Time Range** option on the top right. For Service provider installations, choose the appropriate Organizations on top right. By default, the data combined for all Organizations and the Organization is shown next to each host. This view will automatically refresh every minute by default. The refresh menu on top bar allows the user to disable the automatic refresh or choose a different refresh interval.

Incidents by Category

This pane shows the number of unique Security, Performance, Availability, and Change incidents that have triggered in the specified time range.

To drill into a specific category, click the number and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Incidents

This pane shows the Top Incidents, first by Severity and then by Count.

- Each box represents an Incident.
- The color of the box title reflects the Incident Severity.
- The number reflects the unique incidents that has triggered in the chosen time window.
- The entries inside the box represent the IP address and host names appearing in either the Incident Source or Incident Target.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each host and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Severity

This pane shows the Top Impacted Hosts, first by Severity and then by Count.

- Each box represents an impacted host (where an Incident has occurred during the specified time window).

- The color of the box title reflects the maximum of Severity over all Incidents.
- The number on the left of the box reflects the unique incidents that have triggered on the host in the chosen time window.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that the Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Risk Score

This pane shows the Top Impacted Hosts, first by Risk Score.

- Each Box represents an impacted host (where an Incident has occurred during the specified time window).
- The color of the box title reflects the Risk Score (80 and above is Red, 50-79 is Yellow, and less than 50 is Green).
- The number on the left of the box reflects the risk score.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Risk Score. That means that Red colored boxes (High Risk) appear first, then Yellow colored boxes (Medium Risk), and Green colored boxes (Low Risk).
- You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

List View

This tabular view enables the user to search incidents and take actions.

- Viewing Incidents
- Acting on Incidents
- Searching Incidents

Additional Incident related information: Automated Incident Resolution Recommendation

Viewing Incidents

To see this view, click **INCIDENTS** in the FortiSIEM header. By default, an Incidents Overview dashboard appears, that displays the following information: Incidents by Category, Top Incidents, and Top Impacted Hosts - by Severity/Risk Score. To access List View, which offers Listing by Time, Device, and Incident, click the **List** drop-down button, and select a list view.

The **INCIDENTS** "List by" views allow you to filter data by device and by incident.

You can set any of the **INCIDENTS** views as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list. You can filter the **INCIDENTS** view further by choosing **Overview**, **List – by Time**, **List – by Device**, or **List – by Incident** from the **Incident Home** drop-down list.

An incident's status can be one of the following:

- **Active**: An ongoing incident.
- **Manually Cleared**: Cleared manually by a user - the incident is no longer active.
- **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition.
- **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of **System Cleared**.
- **Externally Cleared**: Cleared in the external ticketing system.

The resolution for an incident can be:

- **Open**
- **In-progress**
- **True Positive**, or
- **False Positive**

When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **False Positive**, then you must **Clear** the Incident.

The following sections describe the three views that are available through the **INCIDENTS** view:

- List by Time View
- List by Device View
- List by Incident View

List by Time View

The **List by Time** view displays a table of the incidents which have been active in the last 2 hours. Additionally, above the table, "buttons" for the number of incidents, number of new incidents that have occurred, number of assigned incidents, and number of incident notifications that have occurred in the last 2 hours appears, and any of these "buttons" can be clicked to display a filtered incident table. The **Last Occurred** column contains the incidents sorted by time, with the most recent first. By default, the view refreshes automatically every minute. The refresh menu on the top bar allows the user to disable automatic refresh or choose a different refresh interval.

Unique to the **List by Time** view is a list of five time range buttons (`15m 1h 1d 7d 30d`) which appear above the paginator. They allow you to filter data by the last 15 minutes, 1 hour, 1 day, 7 days, or 30 days.

See the following table for information on the attributes shown for each incident. A caret will appear when you hover the cursor over some attributes for additional actions:

Attribute	Description
Severity	High (Red), MEDIUM (Orange), or LOW (Green).
ID	Incident's identification number.
Last Occurred	Last time this incident occurred.
Incident	Name of the incident. Click the caret icon for the following options: • Incident Details - Click to get more details on the incident. • Add to Filter - Click to add to filtered list.
Tactics	Name of the tactic involved with the incident.
Technique	Name of the technique involved with the incident. Click the caret icon for the following option: • Details - Click to get more Tactics and Technique information.
Reporting	Set of devices that is reporting the incident. Click the caret icon for the following options: • Quick info - Click to get information on the reporting device. • Device Health - Click to get more device health information. • Vulnerabilities - Click to view device vulnerability timeline. • Related Real-time Events - Click to check real-time events for the device. • Related Historical Events - Click to get older events for the device. • Real-time Performance - Click to get performance metrics. • Add to Filter - Click to add to filtered list. • Add to WatchList - Add IP address/host name to Watch List(s).
Source	Source of the incident (host name or IP address). Click the caret icon for the following options: • Quick info - Click to get information on the reporting device. • Device Health - Click to get more device health information. • Vulnerabilities - Click to view device vulnerability timeline. • Check Reputation - Click to check the source's reputation. • Related Real-time Events - Click to check real-time events for the device. • Related Historical Events - Click to get older events for the device. • Real-time Performance - Click to get performance metrics. • Add to Filter - Click to add to filtered list. • Add to WatchList - Add IP address/host name to Watch List(s). • Add to Application Group - Associate IP address with application group. See Working with Application Groups for more information.
Target	Target of the incident (host name or IP address or user). Click the caret icon for the following options: • Quick info - Click to get information on the reporting device. • Device Health - Click to get more device health information.

Attribute	Description
	• Vulnerabilities - Click to view device vulnerability timeline. • Check Reputation - Click to check the target's reputation. • Related Real-time Events - Click to check real-time events for the device. • Related Historical Events - Click to get older events for the device. • Real-time Performance - Click to get performance metrics. • Add to Filter - Click to add to filtered list. • Add to WatchList - Add IP address/host name/user to Watch List (s). • Add to Application Group - Associate IP address with application group. See Working with Application Groups for more information.
Detail	Other incident details, for example, Counts, Average CPU utilization, file name, and so on. Click the caret icon for the following option: • Check Reputation - Click to check the reputation based of the detail information.
Status	An incident's status can be one of the following: • **Active**: An ongoing incident. • **Manually Cleared**: Cleared manually by a user - the incident is no longer active. • **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition. • **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of System Cleared. • **Externally Cleared**: Cleared in the external ticketing system.
Resolution	Current state of the incident. Click the caret icon for the following options: • Set Resolution to In Progress - Change the incident resolution to "In Progress". • Set Resolution to True Positive - Change the incident resolution to "True Positive". • Clear and set Resolution to False Positive - Change the incident to "False Positive".
Biz Service	Name of the business services affected by this incident
Case ID	The case ID associated with the incident. Click the ID to go to the Cases page.
Category	Category of incidents triggered (Availability, Change, Performance, Security and Other).
Cleared Reason	Reason for clearing the incident if it was cleared.

Attribute	Description
Cleared Time	Time at which the incident was cleared.
Cleared User	User who cleared the incident.
Confidence	The confidence level of a threat.
Count	Number of times the incident triggered between the first and last seen times
Event Type	Event type associated with this incident. All incidents with the same name have the same Incident Type.
External Cleared Time	Time when the incident was resolved in an external ticketing system.
External Ticket ID	ID of a ticket in an external ticketing system such as ServiceNow, ConnectWise, etc.
External Ticket State	State of a ticket in an external ticketing system.
External Ticket Type	Type of the external ticketing system (ServiceNow, ConnectWise, Salesforce, Remedy).
External User	External user assigned to a ticket in an external ticketing system.
First Occurred	The first time that the incident was triggered.
Incident Comments	Comments made on an incident.

Incident Title	The incident title - This typically displays more information than the "Incident" attribute.
	• Click the caret icon for the following options:
	  • Incident Details - Click to get more details on the incident.
	  • Add to Filter - Click to add to filtered list.

Notification Recipients	Incident Notification recipients
Notification Status	Incident Notification Status
Organization	Organization of the reporting device (for Service Provider installations).
Reporting Device Status	Status of the device: Approved or Pending. You must approve devices for the incidents to trigger, but they will still be monitored.
Reporting IP	IP addresses of the devices reporting the incident.
Subcategory	Subcategory of the triggered incident. To add custom subcategories to an incident category, see here.
Tag	Name of the tag involved with the rule that triggered the incident.
View Status	Whether the Incident has been Read or Not.

To see the incident details, click the incident. Next, hover your cursor over the incident name, click the caret icon, and select **Incident Details**:

- **Incident Details** - Includes the full list of incident attributes in a separate pane. A search field to locate incident attributes is available. You can toggle whether to hide empty incident attributes from being displayed by clicking on the icon.

Column	Description
Incident ID	Unique ID of the incident in the Incident database.
Incident Title	A system default title or a user-defined title for an incident.
Rule Name	Rule involved with Incident.
Event Type	Event type associated with this incident. All incidents with the same name have the same Incident Type.
Severity Category	Incident Severity Category: High, Medium or Low.
First Occurred	The first time that the incident was triggered.
Last Occurred	The last time when the incident was triggered.
Category	Category of incidents triggered.
Subcategory	Subcategory of the triggered incident. To add custom subcategories to an incident category, see here.
Tactics	Name of the tactics involved with the incident.
Technique	Name of the technique involved with the incident.
Organization	Organization of the reporting device (for Service Provider installations).
Reporting	Reporting device.
Reporting IP	IP addresses of the devices reporting the incident.
Reporting Device Status	Status of the device: Approved or Pending. You must approve devices for the incidents to trigger, but they will still be monitored.
Target	Target of the incident (host name or IP address or user).
Detail	Event attributes that triggered the incident.
Count	Number of times this incident has occurred with the same incident source and target criteria.
Resolution	The resolution for an incident can be: • **Open** (not defined or not known whether the incident is True Positive or False Positive) • **True Positive**, or • **False Positive** When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.
Case ID	The Case ID for the case associated with the incident. Click the Case ID link to go to the Cases page for the selected case.
View Status	Whether the Incident has been Read or Not.

- **Threat** - This displays threat related information, which includes FortiGuard IP Geolocation, Whois, and Watchlists information. It also provides FortiGuard and Virus Total analysis, if configured.
- **Triggering Events** - This displays the set of events that triggered the incident. If an incident involves multiple sub-patterns, select the sub-pattern to see the events belonging to that sub-pattern. When an event is selected, raw message and parsed fields for that event is displayed. A "Copy to clipboard" icon is available to copy the raw message, and the FortiAI icon can be clicked to provide an analysis and recommended action.
- **Rule Summary** - This displays the **Definition of Rule that Triggered the Incident** and the **Triggered Event Attributes**.
- **Comments** - Information about the incident is provided.
- **Context** - Displays contextual incident information.
- **Action History** - Displays the action history for the incident.

To close the incident details pane, click the highlighted incident, or click **X** in the upper right corner of the pane itself.

List by Device View

The upper pane of the **List by Device** view lists the devices that are experiencing incidents. In the list, the device can be identified by either an IP or a host name. The name of the device is followed by the organization name and the number of incidents. Click the device name to see the incidents associated with the device. This view contains the same features and functionality as the **List by Time** view.

List by Incident View

The upper pane of the **List by Incident** view lists the incidents detected by FortiSIEM. The name of the incident is followed by the number of incidents. Click the incident name to see the incidents associated with the device. This view contains the same features and functionality as the **List by Time** view.

Acting on Incidents

The **Actions** menu provides a list of actions that can be taken on incidents.

To change the incident attribute display columns in the List View, select the **Columns** drop-down list and check/uncheck the desired attributes to display. When done, click the **Columns** drop-down button again.

Location View

To see a Location View of the incidents, select the **Show locations** (Pin) icon, located in the Incident Title row. From the **Select Column to Plot** drop-down list, select **Incident Source** or **Incident Target** to

plot the appropriate geographical location. FortiSIEM has a built in database of locations of public IP addresses. Private IP address locations can be defined in **ADMIN** > **Settings** > **Discovery** > **Location**.

Note: This feature requires Google Maps API Key to be configured, under **Admin > Settings > System > UI**.

Clearing Incidents

To clear one or more incidents, select the incidents you wish to clear, or do not select any incidents if you wish to clear them all, select **Clear Incident** or **Clear All Incidents in View** from the **Actions** menu. In the **Resolution** field, you will be prompted to select **True Positive** or **False Positive** for the affected incidents, and a **Reason** field is available to provide an explanation for clearing the incidents chosen.

Note:

- To select a range of incidents, hold down the Shift key, select an incident, then select the last incident you wish to include in the range as part of your selected incidents.
- To select specific incidents, hold down the Ctrl key, and click each incident that you wish to include.

Actions

You can perform the following operations using the **Actions** menu:

- FortiAI
- Check Reputation
- Investigate
- Changing the Severity of an Incident
- Clearing One or More Incidents
- Create Case
  - From Incident
  - From Event
- Add to Case
  - Add Incident
  - Add Event
- Creating Event Dropping Rules
- Disabling One or More Rules
- Fine Tuning a Rule Triggering an Incident
- Creating an Exception for the Rule
- Executing a Playbook
- Creating a Remediation Action
- Resolve Incident
- Running a Connector
- Exporting One or More Incidents into a PDF or CSV File
- Emailing Incidents
- Show Case History

Changing the Severity of an Incident

1. Select the incident.
2. Select **Change Severity** from the **Actions** menu.
3. Select **Change to HIGH**, **MEDIUM**, or **LOW**.

Clearing One or More Incidents

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Clear Incident** from the **Actions** menu.
5. Select whether the **Resolution** is **True Positive** or **False Positive**.
6. Enter a **Reason** for clearing.
7. Click **OK**.

Disabling One or More Rules

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Disable Rule** from the **Actions** menu.
5. For Service Provider installations, select the Organizations for which to disable the rule.
6. Click **Save**.

Exporting One or More Incidents into a PDF or CSV File

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Export** from the **Actions** menu.
5. Enter or edit the comment in the edit box.
6. Select the **Output Format** and **Maximum Rows**.
7. Click **Generate**.
   A file will be downloaded in your browser.

Fine Tuning a Rule Triggering an Incident

1. Select an incident.
2. Select **Edit Rule** from the **Actions** menu.
3. In the **Edit Rule** dialog box, make the required changes.
4. Click **OK**.

Creating an Exception for the Rule

1. Select an incident.
2. Select **Edit Rule Exception** from the **Actions** menu.
3. In the **Edit Rule Exception** dialog box, make the required changes:
   a. For Service provider deployments, select the Organizations for which the exception will apply.
   b. Select the exception criteria:
      i. For incident attribute based exceptions, select the incident attributes for which rule will not trigger.
      ii. For time based exceptions, select the time for which rule will not trigger.
      iii. Select AND/OR between the two criteria.
      iv. Add Notes.
   c. Click **Save**.

Creating Event Dropping Rules

Event Dropping Rules may need to be created to prevent an incident from triggering. To create such a rule:

1. Select an incident.
2. Select **Event Dropping Rule** from the **Actions** menu.
3. In the **Event Dropping Rule** dialog box, enter the event dropping criteria:
   a. **Organization** - For Service provider deployments, select the organizations for which the exception will apply.
   b. **Reporting Device** - Select the device whose reported events will be dropped.
   c. **Event Type** - Select the matching event types.
   d. **Source IP** - Select the matching source IP address in the event.
   e. **Destination IP** - Select the matching destination IP address in the event.
   f. **Action** - Choose to drop the events completely or store them in the event database. If you store events, you can select the following actions:
      - Do not trigger rules
      - Drop attributes (Click the edit icon to open the selection window and select the attributes to drop)
   g. **Regex filter** - Select a regex filter to match the raw event log.
   h. **Description** - Add a description for the drop rule.
4. Click **Save**.
   The Rule will be appear in **ADMIN** > **Settings** > **Event Handling** > **Dropping**.

Creating a Case

See Creating a Case from the INCIDENTS tab.

Emailing Incidents

Incidents can be emailed to one or more recipients. Make sure that Email settings are defined in **ADMIN** > **Settings** > **System** > **Email**. Note that email notification from the Incident page is somewhat ad hoc and must be manually setup by the user after the incident has triggered. To define an automatic notification, create an Incident Automation Policy in **ADMIN** > **Settings** > **Automation Policy**. To email one or more incidents on demand:

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Notify via Email** from the **Actions** menu and enter the following information:
   a. Send To – a list of receiver email addresses, separated by commas.
   b. Email template – Choose an email template. You can use the default email template, or create your own in **ADMIN** > **Settings** > **System** > **Email** > **Incident Email Template**.

Creating a Remediation Action

Incidents can be mitigated by deploying a mitigation script, for example, blocking an IP in a firewall or disabling a user in Active Directory. Note that this type of incident mitigation from the Incident page is somewhat ad hoc and must be manually setup by the user after the incident has triggered.

To define an automatic remediation, create an Incident Automation Policy in **ADMIN > Settings > General > Automation Policy**. Click **New**, and in the Automation Policy dialog box, select **Run Remediation/Script** in the **Action** section. To create a remediation action:

1. Select an incident.
2. Select **Remediate Incident** from the **Actions** menu.
3. Choose the **Enforce On** devices – the script will run on those devices. Make sure that FortiSIEM has working credentials for these devices defined in **ADMIN** > **Setup** > **Credentials**.
4. Choose the **Remediation** script from the drop-down menu.
   Note: Some Remediation scripts, such as FortiGate/Forti iOS version 7.0 and higher require a **VDOM**. Enter a Virtual Domain (VDOM) in the **VDOM** field for these particular scripts. Be aware that this field is case sensitive, so the VDOM must be entered exactly as it is named.
5. Choose the node on which the remediation will **Run On** from the drop-down list.
6. Click **Run**. If the user does not have permission to run remediation, a Create New Request window will appear. Take the following actions:
7. In the **Approver** drop-down list, select an approver. Fortinet recommends selecting all approvers to better ensure a response.
8. In the **Type** drop-down list, ensure Remediation Request is selected.
9. In the **Justification** field, enter an explanation why you want to run a remediation.

10. Click **Submit**. An email with the your request will be sent to all selected approvers. Approvers will receive a pending task notification in the FortiSIEM console, where they can resolve the request.
11. If you receive an email with an approval, repeat steps 1 through 6 before the expiration. If you received a rejection or received approval that has expired, repeat steps 1-10 if you wish to try again.

Resolve Incident

You can directly resolve an incident by taking the following actions.

1. Select the incident.
2. From the **Actions** drop-down list, select **Resolve Incident**.
3. Select the resolution (Open, In Progress, True Positive, False Positive).
4. Click **OK**.

Check Reputation

FortiSIEM utilizes an external integration policy to perform a reputation check on incidents.

To create an external integration policy, navigate to **ADMIN > Settings > General > External Integration**. Click **New** to begin creating an external integration. For more information, see Configuring External Integration.

To perform a reputation check, take the following steps:

1. Select an incident (or event from Analytics).
2. Select **Check Reputation** from the **Actions**/▼menu.

A **Check Reputation** sidebar will appear with reputation related information.

Note: For incidents, you can add comments by selecting **Add Results to Comment** from the **Actions** drop-down list.

Show Case History

Note: Prior to FortiSIEM 7.0.0, this was **Show Ticket History**.

1. Select an incident.
2. Select **Show Case History** from the **Actions** menu.

3. The Ticket History dialog box opens and displays the following information:

Field	Description
Detail:	
Incident ID	The unique ID of the incident in the incident database.
Due Date	The date by which the ticket should be resolved.
Escalation Policy	The escalation policy defined for the incident.
Attachment	The list of files related to the incident.
Action History:	
Created at	The time when the incident was created.
Incident Name	The name of the rule that triggered the incident.
Incident Target	The IP or host name where the incident occurred.
Incident Detail	The event attributes that triggered the incident.
Incident ID	The unique ID of the incident in the incident database.

Investigate

1. Select an incident.
2. Select **Investigate** from the **Actions** menu.

You will be taken the **Analytics > Investigation** page. See Investigating Incidents.

Searching Incidents

- Searching Incidents
- Searching for MITRE ATT&CK Incidents

Searching Incidents

1. Select **Search** by clicking the Search icon.
2. In the left pane, click an Incident attribute (for example, Category). All possible values of the selected attribute with a count next to it is shown (for example, Security, Availability and Performance for Function).
3. Select any value (for example, Performance) and the right pane updates with the relevant incidents.
4. Click and select other Incident Attributes to refine the Search or click the Trash icon to cancel the selection.

Changing the Time Range for the Search

1. Select **Search** by clicking the **Search** icon.
2. Near the top of the left panel, click the time value.
3. Click **Relative** or **Absolute**:
   - If you click **Relative**, adjust the time value in the **Last** field.
   - If you click **Absolute** enter a time range. If you select **Always Prior**, enter a time period prior to the current time.

Saving the Search Criteria

Once you have performed your search, follow these steps to save the search criteria:

1. Click the **Save** icon ( ) which appears above the list of incident attributes, and to the right of **Search**.
2. In the **Save Search Filter under by Time as** dialog box, enter a name for the filter or accept the default. The default will be a time stamp value such as `Search Filters - 12/17/2019 17:04:59`.

The filter will appear in the **Search** (Search) drop-down list, for example:

- When saving a filter based on the List by Time View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Device View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Incident View, it displays in the **Search** drop-down list.

Searching for MITRE ATT&CK Incidents

To find incidents that fall into any of the MITRE ATT&CK categories, follow these steps:

1. Select **Search** by clicking the Search icon.
2. Click **Tactics** or **Technique** in the left pane.
   The total number of security incidents will appear under the selected MITRE ATT&CK category.
3. Select one or more checkboxes next to the categories of interest.
   The incidents associated with the category are displayed.

For more information on MITRE ATT&CK views and MITRE ATT&CK categories, see MITRE ATT&CK View.

Risk View

Risk view displays the Entities (Devices and Users) ordered by Risk. Risk is calculated based on the triggering incidents using a proprietary algorithm that incorporates asset criticality, incident severity, frequency of incident occurrence, and vulnerabilities found. Risk is only computed for devices in CMDB, private IP addresses, and users found in logs or discovered via LDAP.

Go to **INCIDENTS** > **Risk** to see this view. Risk can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Risk** from the **Incident Home** drop-down list.

Devices and Users are categorized by Risk as follows:

- Devices - number of devices with Risk
- Users - number of users with Risk
- High Risk - number of devices and users with high risk
- Medium Risk - number of devices and users with medium risk
- Low Risk - number of devices and users with low risk

To see only the above categories of devices and users in the Risk View, click any of the five categories above.

The Risk View displays the following:

- Entity (Device or User name)
- Entity Detail Options (For devices, drop-down actions available)
- Current Risk - Current value, up or down versus the same period
- 24 Hour Risk Trend (1 day trend)
- Incidents in Last 24 hours (1 day)

To drill down, click one row and the incidents that led to this risk are shown in a time line format. You can select an incident, and select any action from the **Actions** menu. The actions are similar to those described for the List View.

An Entity (Device or User) can be selected. When selected, the Risk View page expands to three panes that provide more information on the selected object. To go back to the main Risk View, click on **<** in the left pane.

Pane Information

- Left Pane for Device
- Left Pane for User
- Middle Pane for Device and User
- Right Pane for Device
- Right Pane for User

Left Pane for Device

If a device is selected, in the left pane, the following tabs are available:

- General - The name of the device, its access IP, device type, version, importance, and additional description are displayed if available.
- Discovery Status - Discovery information for the device is displayed, which includes its creation date, last discovered date, and last update.
- Collection Status - Information collected from the device is displayed, which includes uptime.
- Member of # Group - Any groups that the device is a member of is displayed.
- Properties - Any custom defined properties are listed here.
- Software - Installed Software, Running Applications, Windows Services, Installed Patches. Click on a specific property for more information.
- Hardware - Interfaces, Processors, Storage, Components. Click on a specific property for more information.

Left Pane for User

If a user is selected, in the left pane, the following tabs are available:

- General - User information, such as user name, full name, job title, company, domain, and last domain where the user was logged on is displayed.
- Advanced - Information such as when the domain password was last set, the age of the domain password, system role, and user lockout time is displayed.
  Note: The information that appears here is also provided under **CMDB > Users > Summary > Advanced**.
- Contact - User contact information is displayed, which can include work phone number, mobile phone number, email address, and physical address.
- Member of # Groups - Any groups that the user is a member of is displayed.

Middle Pane For Device and User

In the middle pane, information on incidents and activities is displayed for the device or user.

A Time Range drop-down selector is available to adjust the time range. Additionally, a Refresh button is available to update information from the middle pane.

- Current Risk Score
- Risk Score and Incident Trend graph - The color of a circle represents its event severity (Red: High Severity, Yellow: Medium Severity, Green: Low Severity). The size of the circle represents the incident count.
  Note: In the case of incident overlap, the color will blend, i.e. a high severity and medium severity incident that occurred at the same time would appear as dark orange.
- Incident Timeline
- Overview by Incident Category - Information from triggered incidents are shown by category and severity. Categories are Security, Performance, Availability, Change, and Other.
  Note: This information is the same as that provided by the incident trend report.
- Incidents and Activity Timeline - Incidents are shown by timeline by default. Click the **Show Activities** checkbox to load activities. Once the data is loaded, this section will show a combination of occurred incidents and activities ordered by the occurred time. Incidents are color coded, and also have a notification (bell) icon next to them.

Timeline	Description
Incident	In the timeline, incident status, its name, and number of occurrences including date and time are shown. Click on **Details** for a slide-in panel that provides **Details** (default), **Triggering Events**, **Rule Summary**, **Comments**, (Incident) **Context** and **Action History** information available by clicking on the respective icon. Click **Actions** to act on the incident (for more information on Actions, see Acting on Incidents).
Activity	In the timeline, the activity name, occurrences, and the user who did the activity are displayed. An **Event Details** link provides the raw messages related to the activity when clicked.

Right Pane for Device

The right pane contains a few pre-defined report widgets to provide an overview for the device.

Device Dashboards

- Successful and Failed Logins - Displays the number of successful and failed logins as a graph.
- Top Users by Failed Login - Displays the most frequent users with failed logins as a graph.
- Top Users by Successful Login Type and Count - Displays the most frequent users with successful logins as a graph.
- Top Security Event Types - Displays the most frequent security event types as a graph.
- System CPU and Memory - Displays the system CPU and memory usage as a graph.
- Top Processes by CPU - Displays the most used processes used by the CPU as a graph.
- Top Processes by Memory - Displays the most used processes using memory as a graph.

Right Pane for User

The right pane contains a few pre-defined report widgets to provide an overview for the user.

User Dashboards

- Top User Actions - Displays the top user's actions taken for the time range configured as a graph.
- Top Actions on User Account - Displays the top actions for the user account as a graph.
- Host Logon Activity - Displays the user's logon activities as a graph.
- Successful and Failed Logins - Displays the user's number of successful and failed logins as a graph.

Explorer View

The Incident Explorer view allows you to correlate Actors (IP, Host, User) across multiple incidents, without creating multiple reports in separate tabs. Incident trends, Actor and Incident detail are displayed on the same page. You can choose an actor and see all the incidents that actor is part of. You can then choose a time range and narrow down the incidents. Time ranges, Actors, and Incidents can be chosen in any order. Each time a selection is made, the rest of the dashboard updates to reflect that selection.

To open the Incident Explorer view, click **INCIDENTS**, then click the Explorer icon ( ).

Explorer can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Explorer** from the **Incident Home** drop-down list.

The Incident Explorer view is divided into three layers:

- The top layer displays the Incident Trend graph. The graph displays the incident counts over time, organized by severity, then by count.

  Each bar in the graph represents the number of incidents at a given time. The colors used in the bars reflects the Incident Severity. Red colored boxes (High Severity) appear first then Yellow (Medium Severity), and finally Green (Low Severity). The numbers in the bars reflect the number of unique incidents that triggered in the chosen time window.
- The middle layer displays panels for Incidents, Hosts, IPs, and Users. You can filter the items in the panels by Category, Status, and Time Range. See “Filtering in the Incident Explorer” for more information.
- The bottom layer displays the Incidents Table with these headings: Severity, Last Occurred, Incident, Source, Target, Detail, Subcategory, Incident Status, and Resolution. Select **Incident Details** from the caret drop-down next to **Incident** to get more details.

  Drill down is available from the Incident, Target, Detail, and Resolution columns.

The following tables describe the drill down options available for each column.

Incident Options

Option	Description
Incident Details	A window with more details about the incident is accessible to review.
Investigate	Go to the **Analytics > Investigation** page for the selected incident.

Source/Target Options

Option	Description
Quick Info	Displays the quick information about the device.
Device Health	Availability, Performance, and Security health reports for the device.
Vulnerabilities	Displays the top 10 vulnerabilities for a selected time period (15 minutes, 1 hour, 1 day, 7 days, 30 days).
Check Reputation	Looks up external threat intelligence websites about likely malicious Indicators of Compromise (IOCs).
Related Real-time Events	Switches to the **ANALYTICS** tab and displays related real time events.
Related Historical Events	Switches to the **ANALYTICS** tab and displays related historical events.
Add to Filter	Switches to List view. Open the drop-down list next to the **Reporting** column for the desired incident and select **Add to Filter**. **Add to Filter** modifies the search on the current tab by including this constraint.
Add to Application Group	Opens the IP Application Group Mapping Definition dialog box where you can choose the group where you want to add the incident.

Detail Options

Select **Check Reputation** to do a look up via external threat intelligence websites about likely malicious Indicators of Compromise (IOCs).

Resolution Options

Option	Description
Set Resolution to Open	Sets the resolution status to Open (not defined or not known whether the incident is True Positive or False Positive).
Set Resolution to In Progress	Sets the incident resolution status to In Progress.
Set Resolution to True Positive	Sets the incident resolution status to True Positive.
Set Resolution to False Positive	Sets the incident resolution status to False Positive. If you are changing the Resolution to False Positive, you must clear the incident at the same time.

To leave the Incident Explorer View, click the **List** icon.

Using the Incident Explorer View

Click any of the bars in the **Incident Trend** graph. The corresponding Incidents, IP addresses, Hosts and Users are displayed in the panels. The corresponding incidents are also displayed in the **Incident Table**.

Click any of the items in the Incident, IP, Host, or User panels. The corresponding bar is displayed in the **Incident Trend** graph and corresponding incidents are displayed in the **Incident Table**.

Click multiple items in the **Incident Trend** graph and in the panels. Your selections will be ANDed together and the results displayed in the **Incident Table**.

Select **Incident Details** from the drop-down caret next to **Incident** column to show Incident details, Trigger events, Rule summary, Comments, Incident context and Action history.

Filtering in the Incident Explorer View

You can filter the incident data by incident category, whether the incident is active or cleared, and the time range when the incident occurred.

- The **Category** drop–down list allows you to filter on unique **Security**, **Performance**, **Availability**, and **Change** incidents that have triggered in the specified time range.

  In order for any Incident to show up on this list, the rule must be configured to be one of the 4 unique categories above (Security, Performance, Availability, Change). Incidents that trigger outside of the above 4 Categories will not show up (eg. Other).

- The **Status** drop-down list allows you to filter on **Active** and/or **Cleared** incidents.
- The **Time Range** dialog box allows you to choose a relative or absolute time range. For **Relative**, enter a numerical value and then either **Minutes**, **Hours**, or **Days** from the drop-down list. For **Absolute**, use the calendar dialog to specify **From** and **To** dates.

MITRE ATT&CK® View

MITRE ATT&CK view provides Information Technology (**IT**) and Industrial Control Systems (**ICS** view summaries by selecting **IT** or **ICS** prior to the following available types of views.

- Rule Coverage View
- Incident Coverage View
- MITRE ATT&CK Incident Explorer View

Rule Coverage View

The Rule Coverage View provides an overview of the tactics and techniques that FortiSIEM covers as defined by MITRE Corporation. Go to **INCIDENTS** > **MITRE ATT&CK®** > **[IT** or **ICS]** > **Rule Coverage** to see this view. Rule Coverage can be set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **MITRE ATT&CK - Rule Coverage** from the **Incident Home** drop-down list.

The ICS and IT Attack (Tactic Categories) are available.

- ICS Attack (Tactic Categories) Table
- IT Attack (Tactic Categories) Table

ICS Attack (Tactic Categories) Table

The following table briefly describes the ICS attack (tactic) categories. See https://attack.mitre.org/tactics/ics/ for more detailed information.

Category (Tactic)	Description
Initial Access ICS	The adversary is trying to get into your network.
Execution ICS	The adversary is trying to run malicious code.
Persistence ICS	The adversary is trying to maintain their foothold.
Privilege Escalation ICS	The adversary is trying to gain higher-level permissions.
Evasion ICS	The adversary is trying to avoid security defenses.
Discovery ICS	The adversary is trying to figure out your environment.
Lateral Movement ICS	The adversary is trying to move through your environment.
Collection ICS	The adversary is trying to gather data of interest to their goal.
Command and Control ICS	The adversary is trying to communicate with compromised systems to control them.
Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
Impact ICS	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

IT Attack (Tactic Categories) Table

The following table briefly describes the IT attack (tactic) categories. See https://attack.mitre.org/matrices/enterprise/ for more detailed information.

Category (Tactic)	Description
Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
Resource Development	The adversary is trying to establish resources they can use to support operations.
Initial Access	The adversary is trying to get into your network.
Execution	The adversary is trying to run malicious code.
Persistence	The adversary is trying to maintain their foothold.
Privilege Escalation	The adversary is trying to gain higher-level permissions.
Defense Evasion	The adversary is trying to avoid being detected.
Credential Access	The adversary is trying to steal account names and passwords.
Discovery	The adversary is trying to figure out your environment.
Lateral Movement	The adversary is trying to move through your environment.
Collection	The adversary is trying to gather data of interest to their goal.
Command and Control	The adversary is trying to communicate with compromised systems to control them.
Exfiltration	The adversary is trying to steal data.
Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Using the Rule Coverage View

To open the Rule Coverage View, go to **INCIDENTS** > **MITRE ATT&CK®** >**[IT** or **ICS]** > **Rule Coverage View**. The top row displays the number of rules and the percentage of MITRE techniques that FortiSIEM covers. In the main row header, the bolded number that appears under each tactic indicates the number of rules that are covered under it. Clicking a tactic here will show all the rules that belong to it. Each tactic cell also lists the number of major techniques (Tech) and sub-techniques (Sub-Tech) related to the involved tactic. All major techniques related to a tactic are listed underneath their respective tactic column. Tactics and techniques covered/not covered by FortiSIEM rules can be selected from the "**Show All**" drop-down list. You can hover your mouse cursor over any major technique to view the following information:

- Total number of rules covered by the technique (security category)
- The number of rules covered by each sub-technique (if applicable)

Left clicking on any technique will bring up a small menu, allowing you to select **Detail** or **Show Rules**.

Clicking on **Detail** will provide you with details about the major techniques and sub-techniques.

Clicking on **Show Rules** will display all the rules associated with the specific technique as provided in the following table:

Note: Clicking a tactic displays the rules information for all related techniques.

Note 2: Click the Columns drop-down list to select which headings you want to display.

Heading	Description
Status	Provides information on whether a rule is enabled (checkmark), or is disabled ("X").
Name	The name of the rule is listed. You can left click on a rule to bring up the following selectable options: • **Show in Resources > Rule** - view/edit the selected rule on the Rules page. • **Rule Summary** - view the rule summary description.
Tactics	The tactic involved with the rule is listed here.
Techniques	The involved technique is listed here. You can click on the technique link to get detailed information from the attack.mitre.org site.
Description	Detailed information about the Rule is provided here.
Exceptions	Any rule exceptions are listed here.

Searching Techniques in Rule Coverage View

A technique search field is available in the upper left corner. You can enter your query in the **Search technique...** field. Results are shown in real-time as you enter your query. A drop-down filter next to the **Search technique...** field is available. Your choices are:

- Show All - all techniques are highlighted. The "Show All" text appears when Show Covered and Show Not Covered are both selected.
- Show Covered - only techniques covered by FortiSIEM are displayed.
- Show Not Covered - only techniques not covered by FortiSIEM are displayed.

Incident Coverage View

The Incident Coverage View provides an overview of the security incidents detected by FortiSIEM that fall under the tactics and techniques as defined by MITRE Corporation. Go to **INCIDENTS** > **MITRE ATT&CK®** >**[IT** or **ICS]** > **Incident Coverage** to see this view. Incident Coverage can be set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **MITRE ATT&CK - Incident Coverage** from the **Incident Home** drop-down list.

The table in Rule Coverage View briefly describes the attack (tactic) categories also shown in Incident Coverage View.

Using the Incident Coverage View

To open the Incident Coverage View, go to **INCIDENTS** > **MITRE ATT&CK®** > **[IT** or **ICS]** > **Incident Coverage View**.The top row displays the number of incidents detected by FortiSIEM in the time range specified. In the main row header, the bolded number that appears under each tactic indicates the number of incidents associated with a specific tactic. Clicking a tactic will show all related detected incidents. Each tactic cell also lists the number of major techniques (Tech) and sub-techniques (Sub-Tech) related to the involved tactic/incidents. All major techniques related to a tactic are listed underneath their respective tactic column. Tactics and techniques covered/not covered by FortiSIEM rules can be selected from the "**Show All**" drop-down list.. You can hover your mouse cursor over any major technique to view the following information:

- Total number of incidents triggered by this technique
- The number of incidents triggered by each sub-technique (if applicable)

Left clicking on any technique will bring up a small menu, allowing you to select **Detail** or **Show Incidents**.

Clicking on **Detail** will provide you with details about the major technique and sub-techniques.

Clicking on **Show Incidents** will display all the incidents associated with the specific technique. It also provides the following Incident information:

Note: Click the Columns drop-down list to select which headings you want to display.

Heading	Description
Severity Category	The severity/category of the incident is listed.
Last Occurred	The date and time when the incident last occurred is listed.
Incident	The event name of the incident is displayed. Clicking on it will bring up a drop-down list with the following options: • Add to Filter - Click to add to filtered list. • Create Case - Create a case with the incident. See here for more information. • Add to Case... - Add incident to an existing case. See here for more information. • Remediate Incident - Run a remediation on the incident. See here for more information. • Rule Summary - displays the **Rule Pattern Definitions** that triggered the incident. • Triggering Events - displays the **Event Details** that triggered the event, including triggered event attributes. • Investigate - takes you to **Analytics > Investigation** with the incident.
Tactics	The tactic involved with the rule is listed here.
Technique	The involved technique is listed here. You can click on the technique link to get detailed information from the attack.mitre.org site.
Target	The object targeted in the incident is listed. For example, the target user in a steal or forge kerberos tickets incident is listed.
Detail	Additional information about the incident is provided here. For example, the command involved, service involved, or registry key is listed, if relevant.
Incident ID	The incident ID is listed.
Reporting	The device that reported the incident is listed.
Source	Source information from the triggered incident is listed. For example, the TCP/UDP Port involved with a protocol tunneling technique is provided.
Incident Status	An incident's status can be one of the following: • **Active**: An ongoing incident. • **Manually Cleared**: Cleared manually by a user - the incident is no longer active. • **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition. • **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of System Cleared. • **Externally Cleared**: Cleared in the external ticketing system.
Resolution	The resolution for an incident can be:

Heading	Description
	• **Open** (not defined or not known whether the incident is True Positive or False Positive) • **True Positive**, or • **False Positive** When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.
First Occurred	The first time that the incident was triggered.
Event Type	The event type triggering the incident is displayed.
Reporting IP	IP addresses of the devices reporting the incident.
Case Status	Current status of the case associated with the incident.
Case User	The user assigned to a case related to the incident.
Case ID	The Case ID for the case associated with the incident. Click the Case ID link to go to the Cases page for the selected case.
Incident Comments	Comments from Incidents Comments/Root Incident Comments.
Organization	The organization where case was created.
Biz Service	Name of the business services affected by this incident
Notification Status	Incident Notification Status
Notification Recipients	Incident Notification recipients
Cleared Reason	Reason for clearing the incident if it was cleared.
Cleared Time	Time at which the incident was cleared.
Cleared User	User who cleared the incident.
Count	Number of times the incident triggered between the first and last seen times
External User	External user assigned to a ticket in an external ticketing system.
External Cleared Time	Time when the incident was resolved in an external ticketing system.
External Ticket ID	ID of a ticket in an external ticketing system such as ServiceNow, ConnectWise, etc.
External Ticket State	State of a ticket in an external ticketing system.
View Status	Whether the Incident has been Read or Not.

Heading	Description
Reporting Device Status	Status of the device: Approved or Pending. You must approve devices for the incidents to trigger, but they will still be monitored.
Category	The category of the triggered incident. Categories are Availability, Performance, Change, Security and Other.
Subcategory	Subcategory of the triggered incident. To add custom subcategories to an incident category, see here.
Incident Title	A system default title or a user-defined title for an incident.
Tag	Name of the tag involved with the rule that triggered the incident.
Instance Org	Name of instance organization.
Confidence	The confidence level of a threat.

Searching Techniques in Incident Coverage View

A technique search field is available in the upper left corner. You can enter your query in the **Search technique...** field. Results are shown in real-time as you enter your query. A drop-down filter next to the **Search technique...** field is available. Your choices are:

- Show All - all techniques are displayed. The "Show All" text appears when Show Triggered and Show Not Triggered are both selected.
- Show Triggered - only techniques with triggered incidents are displayed.
- Show Not Triggered - only techniques with no triggered incidents are displayed.

Filtering in Incident Coverage View

You can filter the incident data, whether the incident is active or cleared, and the time range when the incident occurred.

- The **Status** drop-down list allows you to filter on **Active** and/or **Cleared** incidents.
- The **Time Range** dialog box allows you to choose a relative or absolute time range. For relative times, enter a numerical value and then either **Minutes**, **Hours**, or **Days** from the drop-down list. For absolute times, use the calendar dialog to specify **From** and **To** dates.
- For MSP deployments, the drop-down list allows you to filter incidents based on organizations.

MITRE ATT&CK Incident Explorer View

The MITRE ATT&CK Incident Explorer View maps security incidents detected by FortiSIEM into attack categories defined by MITRE Corporation (MITRE ATT&CK). Go to **INCIDENTS** > **MITRE ATT&CK®** >

[IT or **ICS]** > **Incident Explorer** to see this view. The MITRE ATT&CK Incident Explorer can be set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **MITRE ATT&CK - Incident Explorer** from the **Incident Home** drop-down list.

The table in Rule Coverage View briefly describes the attack (tactic) categories shown in MITRE ATT&CK Incident Explorer View.

Using the MITRE ATT&CK Incident Explorer View

To open the MITRE ATT&CK Incident Explorer View, go to **INCIDENTS** > **MITRE ATT&CK®** >**[IT** or **ICS]** > **Incident Explorer**. The table at the top of the MITRE ATT&CK Incident Explorer View displays the devices experiencing the security incidents and the MITRE ATT&CK categories into which the incidents fall. The circles in the table indicate:

- Number - The number in the middle of the circle indicates the number of incidents in that category. Click the number to get more detail on the incidents. See Getting Detailed Information on an Incident.
- Size - The size of the circle is relative to the number of incidents.
- Color - The color of the circle indicates the severity of the incident: Red=HIGH severity, Orange=MEDIUM severity, and Green=LOW severity.

Filtering in the MITRE ATT&CK Incident Explorer View

You can filter the incident data, whether the incident is active or cleared, and the time range when the incident occurred.

- The **Tactics** drop–down list allows you to filter on one or more of the attack categories. You can also display **All** of the categories.
- The **Status** drop-down list allows you to filter on **Active** and/or **Cleared** incidents.
- The **Time Range** dialog box allows you to choose a relative or absolute time range. For relative times, enter a numerical value and then either **Minutes**, **Hours**, or **Days** from the drop-down list. For absolute times, use the calendar dialog to specify **From** and **To** dates.
- For MSP deployments, the drop-down list allows you to filter incidents based on organizations.

Getting Detailed Information on an Incident

The lower pane of the MITRE ATT&CK Incident Explorer View provides a table with more detailed information about a security incident. You can populate the table in any of these ways:

- Click a device to see all of the incidents associated with the device.
- Open the **Tactics** drop-down list and choose one of the attack categories. All of the incidents associated with the selected category or categories are displayed. You can also choose to display **All** of the categories.
- Click the number in the middle of the circle. All of the incidents associated with the selected device and category are displayed.

For more information on the column headings that appear in the lower pane of the Incident Explorer View, see Viewing Incidents.

Displaying Triggering Events for an Incident

Select **Incident Details** from the caret drop-down next to **Event Name** and select **Trigger Events** icon to display information related to the event that triggered the incident, such as **Host Name**, **Host IP**, and so on.

UEBA View

The UEBA view monitors AI alerts obtained from FortiInsight. To configure what data appears in the UEBA view, see UEBA Settings. The UEBA view is divided into these layers:

- Incident Trend Chart
- Attribute List
- Related Incidents

The **Actions** drop-down list displays the operations you can perform on selected incidents. For descriptions of the operations, see Acting on Incidents.

Incidents in the UEBA View can be filtered by activity status or time range. See Filtering in the UEBA View.

Incident Trend Chart

The Incident Trend Chart displays frequency of incidents over time. You can click the bars in the chart to filter both the chart and the attribute list. The attribute lists will update based on the time and severity category of the bar.

Attribute List

The Attribute List table provides the following information about the AI alerts received from FortiInsight:

Attribute	Description
Incident	The name of the incident that was detected. The incident name is defined in Setting Tags.
Host	The host name or IP address where the alert originated.
Application	The name of the application that is the source of the incident.
User	The Windows Agent user. This user is specified in Setting UEBA Higher Risk Entities.
Tag	The tag used to categorize the alert. The tag is defined in Setting Tags.
Activity	The description of the activity which raised the alert.

Related Incidents

The Related Incidents table provides additional information on the incidents selected in the Attribute List table.

Attribute	Description
Severity Category	The severity of the incident: **HIGH**, **MEDIUM**, or **LOW**. You can change the severity value in the **Actions** drop-down list.
Last Occurred	The date and time when the incident was last detected.
Incident	The name of the incident.
Tag	The tag used to categorize the alert.
Host Name	The host name or IP address of the host where the alert originated.
User	The Windows Agent user.
Application	The name of the application that is the source of the incident.
Resource	A resource name, typically a file path.
Activity	The description of the activity which raised the alert.

Triggering Events

Click the caret icon next to an incident in the **Related Incidents** table to display its triggering events.

These display options are available above the table:

- **Subpattern: FIN** - Indicates that only FIN events are displayed.
- **Wrap Raw Events** - Select to display the full log event in the table.
- **Show Event Type** - Select to display the event type only.
- **Show Raw Event Only** - Select to display the full log event only.

The following table describes incidents in the Triggering Events table.

Attribute	Description
Event Receive Time	The date and time when the event was received.
Host Name	The IP address or host name that was the source of the event.
Domain	The Windows domain that was the source of the event.
User	The Windows Agent user.
Tag Name	The tag used to categorize the alert.
Process Name	The name of the process producing the event.
Activity Name	The description of the activity which raised the alert.
Resource Name	A resource name, typically a file path.

Filtering in the UEBA View

Use the **Status** button in the upper right corner of the UEBA View to filter the display for active or cleared incidents, or both. Use the **Time Range** button to filter the display for incidents within a specific time range:

- **Status** - Use the drop-down list to display **Active** incidents, **Cleared** incidents, or both.
- **Time Range** - Filter the incidents according to a time range:
  - If you click **Relative**, adjust the time value in the **Last** field.
  - If you click **Absolute** enter a time range.

Investigating Incidents

You can examine an incident in-depth through the following methods.

1. From the **Incidents** page, select an incident and choose **Investigate** from the **Action** drop-down list.

   or

2. On the **Analytics > Investigation** page, enter the Incident ID number of the incident you wish to examine, or select it from the top 10 incidents that appear initially on a new tab, and click **Load**.

When an incident number has been provided, the Analytics Investigation page will show an undirected graph of the incident and involved entities (host/ip, user, process, file) as nodes. The latest top 10 incidents appear initially on a new tab on the **Analytics > Investigation** page.

A **Time From** and **To** field are available to set the time span you wish to investigate for the selected incident. A **Layout** drop-down option is also available. You can choose **Force** or **Bipartite** layout.

A left vertical bar offers the following functions.

Icon	Description
Investigation History	Click to view investigation actions that have taken place for the incident.
Timeline	Click to view information on when the incident occurred. Incidents are ordered by when they occurred in the timeline. Hover your mouse cursor over an incident in the Timeline panel to see the incident and its affected entities in the undirected graph. A Play icon can be clicked to illustrate when the incident occurred for the selected time span. The information icon can be clicked to get more detailed information. Check the **Auto** checkbox to play the next node automatically without having to click it. Check the **Recenter** checkbox to position the current incident in the timeline sequence to the center. Select an incident in the Timeline panel to identify its place in the Timeline graph.
Root Incident Comments	Click to view any comments made related to the incident.

Examining an Incident and Related Entities

After an incident has been loaded into Analytics, you can take the following actions. A node will either be an incident or an entity (host/ip, user, process, file). An incident can be recognized by a colored

border that also indicates the severity of the incident.

- Hover over a node to bring up a quick overview on the incident/entity object.
- Click on a incident node to access a left pane that provides detailed information on the incident and various actions that you can take.

Button	Description
Details	Click to view detailed information on the incident.
Events	Click to view the triggering events that led to the incident. Click > to go to the next triggering event, if applicable.
Context	Click to get information about all the IPs and hosts in the incident. Device type, presence in Malware lists and watch lists is also provided.
Comments	Click to view and add/edit comments related to the incident.
...	Click to view additional actions available to take on the incident. See Acting on Incidents for more information. In addition to the actions that can be taken listed in Acting on Incidents, the user also has access to **Action History**. Clicking on **Action History** displays all the actions that the user has taken on the incident in the current session, including the date/time each action was taken. The user can expand and get more details on a particular action by clicking on the caret icon.

- Click on a node that is an entity to access a left pane that shows entity information. See Pane Information on the Risk Page for more information.

Button	Description
Details	Click to view detailed information on the entity.
Check Reputation	Click **Check Reputation** to view available Check Reputation options. Click **Check Reputation** to run an threat integration lookup (VirusTotal, RiskIQ, and/or FortiGuard) for the entity. First, select the IP address from the **Select Target** drop-down list, select the threat integrations from the **Check from** drop-down list, then click **Check**. Then click **View Result**.
Run Report	If the entity is a host or IP node, **Run Report** is available. Click the **Select report...** drop-down to see a list of available report categories located in the left column of the left pane. Select a report category to view a list of available reports for the selected report category in the right column of the left pane. Some report categories have sub-categories, viewable by clicking the caret icon. Click on a caret icon to view a report's sub-category reports. For example, under **Threat Hunting**, you can select **Discovery** to see all Discovery reports that exist under **Threat Hunting** instead of scrolling through all the reports under **Threat Hunting**. Select a report. You can select multiple reports by taking these actions: • To select a range of items, hold down the Shift key, select a report, then select the last report you wish to include in the range as part of your selected reports. • To select specific reports, hold down the Ctrl key, and click each report that you wish to include. After selecting your report(s), hover your cursor over a selected report to view a caret icon. Click it, and the following options appear: • **Report Summary** - Click to view general information on the selected report(s). For multiple reports, you can click **Previous**/**Next** to view each selected report summary. Click **Close** when done reviewing the Report Summary. **Note**: With only one report selected, the option to run the report is available from the Report Summary window, by clicking **Run**. • **Add Report** - Click to add the selected report(s) to be run. When report(s) have been added, you can click **Edit additional filters** to include any additional filters. When you are ready to run your report(s), click the **Run**/**Run # Reports** button. From the **Result Summary**, if there are successful results, click **Show Result** to view the actual results. To view results from the Analytics Search page, click **Run In Search**.
Context	Click to get IP and host information.

- Additionally, when a node is selected from the undirected graph, related objects can be added to the undirected graph. See the following table for further information on the actions you can take.
  Note: Actions that are available are determined by the object you selected.

Action	Description
Related Entities	Click to view additional identified related entities for the incident you selected. Select an entity, and a checkmark appears next to it. Click **Add** to add all selected entities, or click **Add All** to display all related entities.
Related Incidents	Click to view additional identified related incidents for the entity you selected. Select an incident, and a checkmark appears next to it. Click **Add** to add all selected incidents, or click **Add All** to display all related incidents.
Related Incidents and Entities	Click to view additional identified related incidents and entities for the entity you selected. Select an incident or entity, and a checkmark appears next to it. Click **Add** to add all selected incidents and entities, or click **Add All** to display all related incidents and entities.
Remove Node	Click to remove the selected node.

Working with the Undirected Graph

- Adding an Undirected Graph
- Clearing an Undirected Graph
- Fitting the Undirected Graph in Panel
- Repositioning a Node
- Repositioning the Undirected Graph
- Zooming In/Out of the Undirected Graph

Adding an Undirected Graph

Click on **+**, enter the Incident ID that you wish to view an undirected graph of, and click **Load**.

Clearing an Undirected Graph

To clear an undirected graph, click the trash icon in the lower right corner.

Fitting the Undirected Graph in Panel

To fit the undirected graph in the existing panel, click the "fit in frame" icon.

Note: While in Bipartite layout, this function is unavailable.

Repositioning a Node

To reposition a node, click and hold the left mouse button over a node. Next, move the mouse to reposition the node, and release the mouse button when done.

Repositioning the Undirected Graph

To reposition the undirected graph, click and hold the left mouse button over a location that isn't a node. Next, move the mouse to reposition the undirected graph, and release the mouse button when done.

To recenter the undirected graph around a selected node, select a node, then click the Center icon, located in the lower right corner.

Zooming In/Out of the Undirected Graph

To zoom in or out of a graph, click the **+** or **-** icons.

Note: While in Bipartite layout, this function is unavailable.

Automated Incident Resolution Recommendation

FortiSIEM provides 2 attributes to record Incident status:

1. **Incident Resolution**: None, True Positive, False Positive
2. **Incident Status**: Active, System Clear and Manually Cleared

When an Incident triggers, Incident Status is set to Active and Incident Resolution is set to None. There are 3 ways an Incident can get resolved:

1. If the Incident turns out to be a false positive, then the user can set Incident Resolution to False Positive and Incident Status to Manually Cleared.
2. The Incident may clear itself because of a clearing condition in the rule. In that case, Incident Resolution is set to True Positive and Incident Status is set to System Cleared.
3. The Incident may be a real issue. In that case, after working through the Issue, the user can set Incident Resolution to True Positive and Incident Status to Manually Cleared.

FortiSIEM uses a Machine Learning Classification algorithm to recommend Incident Resolution. First, it learns the Incident Resolution set by the user for Incidents over the previous 2 days. Then it recommends Incident Resolution for new Incidents as they occur. The algorithm runs daily at midnight (12AM) to cover Incidents over the last 2 days. Recommendation is done as follows:

1. Incident Resolution is set to True Positive or False Positive.
2. A new Incident attribute called Confidence (between 0 and 100) is set. A high confidence number implying high confidence on the result.
3. Incident Comment is updated with the comment "Resolution set by Machine Learning".

Notes:

1. Only Incident Resolution is set. Incident Status is not modified.
2. The Machine Learning algorithm always runs in the background and cannot be disabled. The algorithm uses a set of Incident attributes as features (including Event Receive Time, Event Type, Reporting Device, Source, Target, Category and MITRE Attack Technique) to make its recommendation.

Lookups Via External Websites (e.g. VirusTotal)

Indicators of Compromise (IOC) can be transmitted via external IPs, domain names, URLs, and file hashes.

When a security incident is triggered due to a potentially malicious IOC, you may want to consult an external threat intelligence website to get more information about the IOC. If the website can confidently say that the IOC is malware, then you can take corrective action, such as blocking the IOC. On the other hand, if the website says that the IOC is safe, then you can mark the IOC as a false positive.

There are two types of external lookups:

- Some websites accept an IOC as a parameter in the URL and the website will respond with information about the IOC. In many of these cases, the IOC information in the web page cannot be parsed programmatically, and user must manually determine whether the IOC is malware. For example, see https://www.talosintelligence.com/reputation_center/lookup?search=8.8.8.8.
- Other websites, such as VirusTotal and FortiGuard have APIs. FortiSIEM can analyze the data from these websites and present the results in an easily understandable format for user. **Note:** VirusTotal supports domain, URL, and file hash lookups. FortiGuard supports IP, domain, URL and file hash lookups.

FortiSIEM supports all three types of lookups. External Website lookups can be performed only from the **Incident List View**.

Prerequisites

Complete these steps before performing external lookups:

1. External lookups that accept an IOC in the URL must be defined in **ADMIN > Settings > System > Lookup**. See Lookup Settings for more information.
2. VirusTotal, RiskIQ, and FortiGuard integrations must be defined in **ADMIN > Settings > General > External Integration**. This involves setting credentials.
   See VirusTotal Integration, RiskIQ Integration, and FortiGuard Integration for more information.

Performing an External Lookup on VirusTotal, RiskIQ, and/or FortiGuard

Follow these steps to perform an external lookup on VirusTotal, RiskIQ, and/or FortiGuard.

1. Go to **INCIDENTS** and click the **List** view.
2. Select an incident from the table.
3. Drill down on either the **Source**, **Target**, **Detail** or **Reporting IP** columns and choose **Check Reputation**. FortiSIEM will identify IP, Domain, URL and file hash fields for lookup.
4. Choose one of the following and click **Lookup**.
   a. An External website that accepts IP in the URL
   b. **VirusTotal**, **RiskIQ**, and/or **FortiGuard**
5. For the first case (4a), the page opens in a different tab in the browser.
6. For the second case (4b), FortiSIEM collects information about the IOC from the websites using the API, makes a conclusion as to whether it is Safe/Malware/Not Sure, and presents the data in the **Result** tab.
7. If a FortiGuard result is determined to possibly be malicious, you can click on **Malicious** to get more details as to why FortiGuard flagged the incident as malicious.
8. Based on the information about the IOC, you can click on the **Action** tab and take any of the following actions.
   a. Update **Comments**: You can update Incident comment based on the website findings. Enter an optional comment about the incident and click the **Save** icon. You can also move the information from **Result Summary** to **Comments** by clicking the **Append Summary to Comments** button. Comments will appear in the **Incident Comment** panel in the **Details** tab when you select the incident in the **List** view.
   b. **Resolve Incident**: You can resolve the incident. Choose **Open**, **True Positive**, **False Positive**, or In **Progress**. Click **Apply**, and the selection will appear in the Resolution column for that incident.
      - If you choose **False Positive**, you have the option of providing a reason for your choice. You also have the option to **Create a False Positive in ThreatConnect**. Clicking this option will respond with a message describing whether the creation was successful. This option assumes that you have created a malware configuration for ThreatConnect. You can configure IPs, domains, hash, or URLs for ThreatConnect. See Working with ThreatConnect IOCs.
   c. **Create Rule Exception**: If it is a false positive, then you can create a rule exception. Click the edit icon to create an exception to the rule. For more information on using the **Edit Rule Exception** dialog box, see Creating an exception for the rule.
   d. **Set Incident Severity**: You can change the incident severity. Open the drop-down list and choose **Change to LOW**, **Change to MEDIUM**, or **Change to HIGH**.
   e. **Remediate Incident**: You can remediate the Incident, e.g. block the malware domain. Click the edit icon to remediate the incident. For more information on using the **Run Remediation** feature, see Creating a Remediation action.
   f. **Run External Integration**: You can create a ticket in an external ticketing system. Click the edit icon to choose an integration policy from the drop-down list. Click **OK**.
9. Click **Close**.

CVE-Based IPS False Positive Analysis

Network Intrusion Prevention Sensors (IPS) trigger alerts based on network traffic. When an IPS sees traffic matching an attack signature, it generates an alert. Some of these attacks correspond to host vulnerabilities and have an associated CVE number. Most organizations run vulnerability scanning tools to scan their servers for vulnerabilities. If FortiSIEM is configured to collect this host vulnerability data, it can combine the IPS signature to CVE mapping, and Host to CVE mapping to detect if an IPS Alert is false positive.

- Requirements
- False Positive Detection Logic
- Running an IPS False Positive Test
- Consequences of Running the IPS False Positive Test

Requirements

- Currently, FortiSIEM applies this logic on Incidents but not events. All important IPS events trigger some rule in FortiSIEM.
- FortiSIEM IPS rules must be written with a **Signature Id** and **Event Type** in the group by conditions. All built-in rules have been enhanced with this requirement starting with release 5.3.0.
- The primary source of IPS Signature to CVE mapping is FortiSIEM CMDB. These mappings are part of the FortiSIEM knowledge base and upgraded with every release. For FortiGate IPS signatures, FortiSIEM can also pull this information from FortiGuard Services via an API. The FortiGuard IOC license must be enabled in FortiSIEM.
- The source of Host to CVE mapping is Vulnerability scanners. FortiSIEM currently supports Qualys, Rapid7, Nessus and Tenable scanners. Make sure FortiSIEM is configured to collect this data at least once a day.

False Positive Detection Logic

Recall that for this detection logic to work, IPS-related incidents must have **Signature Id** and **Component Event Type** configured (for example, see the built-in **High Severity Outbound Permitted IPS Exploit** rule). The test is performed separately for both internal (for example, RFC-1918 address space) **Incident Source** and **Incident Target IPs**, as it does not make sense to perform tests for Internet addresses.

After the incident triggers, the associated CVEs for the Incident Event Type are first looked up. The primary source is the CMDB. If the CMDB does not have this information, then external websites are looked up. In the current release, only Fortinet IPS signatures are looked up using **Signature Id** in the FortiGuard database.

If associated CVEs are found, then another CMDB lookup is performed to see if the Host (in **Incident Source** or **Target**) is vulnerable to the CVEs. CMDB collects Host Vulnerability information from vulnerability scan data.

There are four detection outcomes:

- **Vulnerable** - this can result if ALL the following are true:
  a. IP is internal and,
  b. Event type to CVE mapping is found and,
  c. Host has been scanned for vulnerabilities in the last 2 weeks and,
  d. At least one CVE in (b) is found in the list of current vulnerabilities in (c).
- **Not Vulnerable** - this can result if ALL the following are true:
  a. IP is internal and,
  b. Event type to CVE mapping is found and,
  c. Host has been scanned for vulnerabilities in the last 2 weeks and,
  d. None of the CVEs in (b) are found in the list of current vulnerabilities in (c).
- **Insufficient Information** - this can result any of these cases:
  a. Even type to CVE mapping is not found or,
  b. Host has not been scanned in the last 2 weeks.
- **Not Needed** - this case is true if the IP is external.

An Incident is False positive if either of the following cases is true

- **Source Detection Status** is not **Not Needed** and Destination is **Not Vulnerable** or vice-versa
- Both **Source** and **Target** are **Not Vulnerable**

An Incident is True positive when either **Source** or **Destination** is **Vulnerable**.

Running an IPS False Positive Test

This test can be run on-demand or automatically when an Incident triggers. First you need to set up an Integration.

1. Go to **ADMIN > Settings > General > External Integration**.
2. Click **New**.
3. Set **Type = Incident**, **Direction = Outbound**, **Vendor = "FortiSIEM Attack CVE Check"**.
4. Click **Save**.

To Run the IPS False Positive Test On-Demand on an IPS Incident

1. Go to **INCIDENTS > List By Time**.
2. Select one incident. Make sure that the **Signature Id** and **Component Event Type** are configured in the **Incident Detail**.
3. Click **Action** and select **Run External Integration**.
4. Select the specific integration and click **OK**.

The IPS False positive test can be automated so that it runs automatically when the Incident triggers for the first time. To do this, create an **Incident Automation Policy**. The IPS Attack CVE Check will run as an **Incident Action**.

1. Go to **ADMIN > Settings > General > Automation Policy**.
2. Select an existing automation policy to edit, or click **New** to create one.
3. In the **Action** section, select **Invoke an Integration Policy**, then select the policy.
4. Save the policy.

Consequences of Running the IPS False Positive Test

When you run the integration policy, the following results can occur:

- The **Incident Comment** is updated with the detection status.
- The **Incident Status** is determined based on the following cases:
  a. False Positive Case: the **Incident Severity** is set to **Low** and the Incident is cleared.
  b. True Positive Case: the **Incident Severity** is set to **High** and a Case is opened.
  c. In all other cases, the **Incident Status** remains unchanged.

Remediating an Incident using a Script

- Overview
- Requirements
- How App Server Determines Enforce On and Run On Devices
- Structure of a Remediation Script

Overview

FortiSIEM provides a framework to remediate an Incident by running a script. As an example, when an Incident triggers that detects that a host is communicating to a Malware website found in FortiGuard IOC database, the host (IP) can be blocked on a FortiGate firewall. The remediation can be done in one of two ways:

- In an ad hoc manner from **Incidents > List View** page by selecting an Incident, then selecting **Actions > Remediate Incident**.
- In an automated way by defining a Remediation Action in an *Automation Policy* from **Admin > Settings > Automation Policy > Run Remediation Script**. This option does not require user action when an Incident triggers.

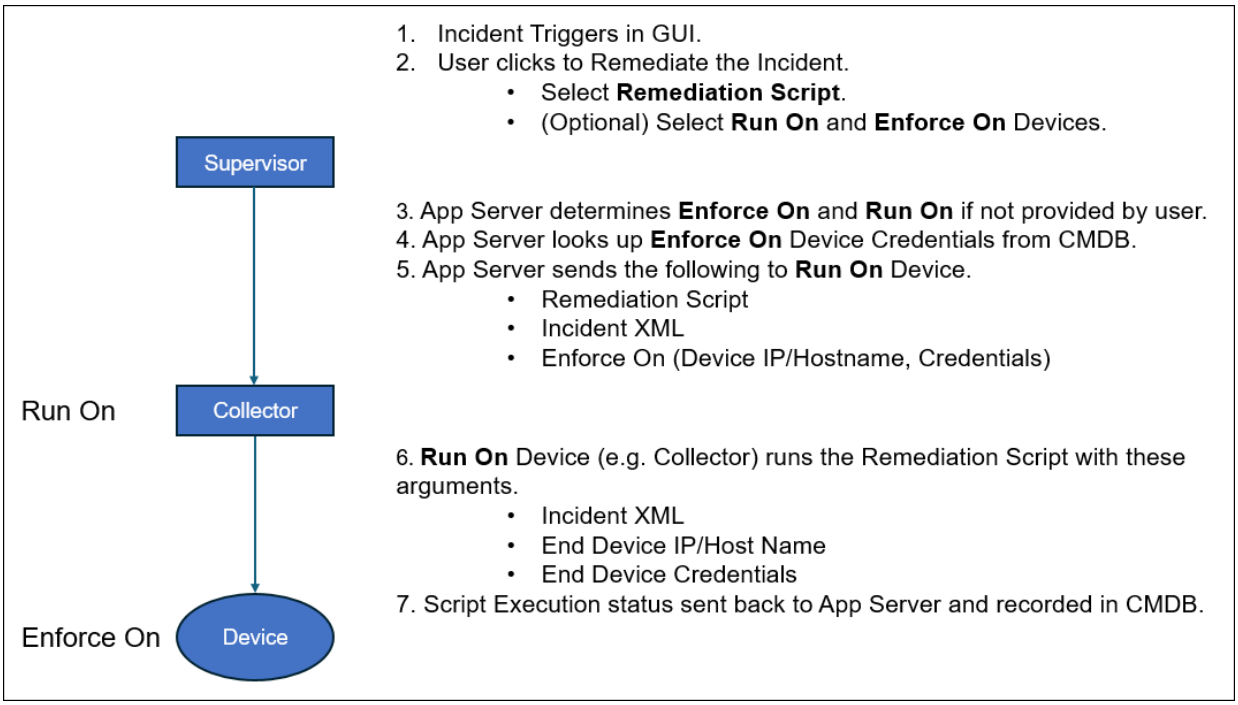
Many built-in automation scripts are provided in **Resources > Remediations**. The user also can create their own remediations by clicking **Resources > Remediations > New**.

The following figure illustrates how the Remediation scripts work within the FortiSIEM framework. There are two key concepts.

- **Run On Device**: This is the FortiSIEM node from where the Remediation script is launched, e.g. a FortiSIEM Collector.
- **Enforce On Device**: This is the end device where the remediation script runs and the remediation is enforced, e.g. a Firewall, a Server, Windows Active Directory, etc...

FortiSIEM can automatically choose Run On and Enforce On Devices, but user can also override these choices.

App Server sends the remediation script and the Enforce On Device Credentials to the Run On Device, which then invokes the script. The Run On Device needs the specified Access Protocol connectivity to the Device.



Requirements

The following are required for a Remediation framework to function.

1. The **Enforce On** Device must be defined in CMDB.
2. The **Enforce On** Device Access Credential must be defined in **Admin > Setup > Credentials**. This credential will be used to run the remediation script.
3. Currently, the following **Device Type** and **Credential** combinations are supported for remediation. Several remediation scripts that use these credentials are provided in **Resources > Remediations**.

Device Type	Access Protocol
Fortinet FortiOS (FortiGate firewalls)	SSH, HTTPS, FORTIOS_REST_API
Fortinet FortiEDR	FortiEDR_API
Fortinet FortiClient FortiEMS	FortiEMS_API
Fortinet FortiMail	HTTPS
Fortinet FortiWeb	HTTPS
Fortinet FortiAuthenticator	HTTPS
Fortinet FortiADC	SSH
Microsoft Windows	MS_OMI, MS_WMI
Generic Linux	SSH
Any Device Type that has SSH credential defined in FortiSIEM	SSH
Any Device Type that has HTTPS credential defined in FortiSIEM	HTTPS

4. The **Run On** Device needs specified Access Protocol connectivity to the **Enforce On** Device.

How App Server Determines Enforce On and Run On Devices

The **Enforce On** device is selected from the **Incident Reporting Device** field in an Incident. The **Incident Reporting Device** field is set from the **Reporting Device** field in the events that trigger the Incident. If there are multiple Incident Reporting Devices, then the first one is chosen.

The **Run On** device is selected from the FortiSIEM node that received the events that trigger the Incident. If there are multiple Incident Reporting Devices, then the first one is chosen.

The user can always choose *specific* **Enforce On** and **Run On** devices to override the auto-selection.

Structure of a Remediation Script

A Remediation script is passed the following arguments.

1. A FortiSIEM Incident in XML format
2. Enforce On Device IP or Host name
3. Enforce On Device Credentials

For **HTTP/HTTPS/FortiEMS/FortiEDR API Credentials**, the remediation script is invoked as follows:

`python3.9 <script.py> <incidentXml> <user> <password> <accessIp> <hostname> <port>`

For **SSH**, the remediation script is invoked as follows:

`python3.9 <script.py> <incidentXml> <user> <password> <enable> <password> <accessIp> <port>`

For **other Access protocols**, the remediation script is invoked as follows:

`python3.9 <script.py> <incidentXml> <user> <password> <accessIp>`

Often, remediation needs some fields (e.g. VDOM) that are not present in an Incident. The user can provide this information via the GUI when setting the Remediation, and these fields are passed to the remediation script via the `<override>` xml tag in the incidentXML.

Step 1: The script must parse the Incident XML and locate the entity (e.g. `IP/ user/ domain`) that needs to be remediated. There are a few inbuilt helper functions that extract a set of common entities from the Incident XML.

Entity	Helper Function	Sample Script with Helper Function
Source IP	`get_incident_attribute(<incidentXML>, 'incidentSource', 'srcIpAddr')`	Block IP Cisco ASA
Source MAC	`get_incident_attribute(<incidentXML>, 'incidentSource', 'srcMACAddr')`	Deauth User ArubaOS
Destination IP	`get_incident_attribute(<incidentXML>, 'incidentTarget', 'destIpAddr')`	
User	`get_incident_attribute(<incidentXML>, 'incidentTarget', 'user')`	Disable User Account Windows DC
File	`get_incident_attribute(<incidentXML>, 'incidentDetails, 'fileName')`	Delete File By Checksum Linux
File Checksum	`get_incident_attribute(<incidentXML>, 'incidentDetails, 'hashCode')`	Delete File By Checksum Linux
Host Interface	`get_incident_attribute(<incidentXML>, 'incidentTarget', 'intfName')`	Disable Port Cisco IOS

The user can also write code to parse the Incident XML and derive any entity.

Step 2: Next, the script needs to extract the device IP and credentials from the parsed arguments and execute the remediation.

Code snippets can be found in the built-in remediation scripts in **Resources > Remediations**.

Executing a Playbook on an Incident

To execute a Playbook on an incident, take the following steps.

1. From the **INCIDENTS** page, select an incident.
   Note: You must be on the List by Time, List by Device, or List by Incident View.
2. Select **Execute Playbook** from the **Actions** menu.
3. From the **Execute Playbook** window, take the following steps.
   a. From the **Folders** column, expand any Playbook folder to view its content.
   b. From the **Items** column, select the Playbook you wish to execute and click **>**. The Playbook will appear in the **Selections** column. You may also search for Playbooks by using the Items **Search...** field.
      If you wish to remove a Playbook from the **Selections** column, select the Playbook you wish to remove and click **<**.
   c. When ready to execute your Playbook, click **Execute**. The **Playbook Execution Result** window appears, in the **Result** tab. This window provides a summary of result. Clicking **Details** will display additional information. Click on **View Output** to view any information related on a specific Playbook topic (Summary, Details, a specific attribute if applicable).
   d. Click on the **Actions** tab to perform any of the following actions.
      Note: All actions are optional.
      i. In the **Update Comment** field, enter any comments related to the Incident.
      ii. Click on **Add Summary** to add the Summary and Details from the Result tab into the **Update Comment** field.
      iii. To save the information added to the Update Comment field, click **Save**.
      iv. For **Resolve Incident**, select the one of the following resolutions: **Open**, **True Positive**, **False Positive**, or In **Progress**. When done, click **Apply**.
      v. Click on **Create Rule Exception** create icon to create a rule exception.
      vi. Click on the **Remediate Incident** create icon to run a remediation on the incident.
      vii. Click on **Set Incident Severity** drop-down list and select a severity level.
      viii. Click on the **Run External Integration** create icon to run an external integration.
   e. When done, click **Close**.

Under **Details**, the **Action History** column provides a log of all the actions taken, including comments from the **Update Comment** field.

Running a Connector on an Incident

To run a Connector on an incident, take the following steps.

1. From the **INCIDENTS** page, select an incident.
   Note: You must be on the List by Time, List by Device, or List by Incident View.
2. Select **Run Connector** from the **Actions** menu.
3. From the **Run Connector** window, take the following steps.
   Under **Details**, the **Action History** column provides a log of all the actions taken, including comments from the **Update Comment** field.
   a. From the **Folders** column, select the Connector you want to run. When a Connector is selected, a list of actions for that Connector will populate under the **Items** column.
   b. From the **Items** column, select the Connector action you wish to run and click **>**. The Connector action will appear in the **Selections** column. You may also search for a Connector by using the Items **Search...** field.
   If you wish to remove a Connector from the **Selections** column, select the Connector you wish to remove and click **<**.
   c. Depending on the Connector action selected, a **Select Connector Parameters** section may appear. Enter and/or select the information necessary in the additional fields to continue.
   d. When ready to run your Connector, click **Execute**. The **Run Connector** window appears, in the **Result** tab. This window provides a summary of result. Clicking **Details** will display additional information. Click on **View Output** to view any information related on a specific Connector topic (Summary, Details, a specific attribute if applicable).
   e. Click on the **Actions** tab to perform any of the following actions.
   Note: All actions are optional.
      i. In the **Update Comment** field, enter any comments related to the Incident.
      ii. Click on **Add Summary** to add the Summary and Details from the Result tab into the **Update Comment** field.
      iii. To save the information added to the Update Comment field, click **Save**.
      iv. For **Resolve Incident**, select the one of the following resolutions: **Open**, **True Positive**, **False Positive**, or In **Progress**. When done, click **Apply**.
      v. Click on **Create Rule Exception** create icon to create a rule exception.
      vi. Click on the **Remediate Incident** create icon to run a remediation on the incident.
      vii. Click on **Set Incident Severity** drop-down list and select a severity level.
      viii. Click on the **Run External Integration** create icon to run an external integration.
   f. When done, click **Close**.

Troubleshooting Incident Trigger

An Incident may not trigger for one or more of the following reasons:

1. Rule filter conditions may not be satisfied, or events may be present. In this case, Fortinet recommends the following:
   - Test the rule with real events. If the rule does not trigger, then there may be some event attributes that are not parsed, or the rule is not written correctly.
   - View the rule and from the Filter condition page, and run the Rule as a Query for a previous time-period to see if there are matches.
2. The reporting device may be in maintenance mode, in which case, its events are ignored.
3. The Rule exception condition may be satisfied – this is expected behavior.
4. Events from Collector are delayed more than `dropping_time_threshold` when received by Worker. In this case, the log PH_DROP_EVENT_FROM_SHARED_BUFFER will be generated by the Rule Worker.
5. Rule Worker failed to upload packed aggregated result to Rule Master. This could be a networking issue. In this case, the log PH_RULEMOD_SUMMARY_UPLOAD_FAILED will be generated by the Rule Worker.
6. Rule Worker failed to pack summary events, before sending to Rule Master because of send buffer limit exceeded. This can happen if a rule is loosely written and the group by table size is very large at Rule Worker level. In this case, the log PH_REPORT_PACK_FAILED will be generated by the Rule Worker.
7. Rule Master failed to upload Incident to App Server. In this case, the log PH_UTIL_NOTIFICATION_UPLOAD_FAILURE will be generated by the Rule Master.
8. Incident dropped because of too many incidents from the same rule, or too many incidents in general. In this case, the log PH_DROP_INCIDENT will be generated by the Rule Master. This is done to protect the system from getting flooded with Incidents. There are 6 parameters (in phoenix_config.txt) to control the incident rate:

   Short term Incident generation thresholds:
   - incident_rate_short_term_time_gap = 1 #unit: minute
   - incident_rate_short_term_per_rule_limit = 20
   - incident_rate_short_term_all_rules_limit = 200;

   Long term Incident generation thresholds:
   - incident_rate_long_term_time_gap = 60 #uint: minute
   - incident_rate_long_term_per_rule_limit = 300;
   - incident_rate_long_term_all_rules_limit = 3000;

   For the above parameters, if the following "too many incidents" condition is met, then incident generation pauses until the next hour boundary. For example, if this happens at 12:35PM, then Incident generation pauses from 12:35PM to 1:00PM.

   Excessive Incident Generation Condition:

   In 1 minute

- For one rule, more than 20 incidents fired OR
- For all rules, more than 200 incidents fired

OR in 60 minutes

- For one rule, more than 300 incidents fired OR
- For all rules, more than 3000 incidents fired

Working with Analytics Search

- Overview
- Running a Built-in Historical Search
- Creating a New Search
- Creating a Nested Search
- Viewing Real-time Search Results
- Viewing Historical Search Results
- Searches Using Pre-computed Results
- Working with Search Results

Overview

FortiSIEM allows two types of searches:

- **Real time search**: This enables you to search the events in real time as they are being ingested and before they are stored in the event database. You cannot do Group By operations in Real time Search.
- **Historical search**: This enables you to search events that are already stored in event database.

You can create the following types of searches:

- **Pure Event Search**: Searches on Events, e.g. Top Destination IP addresses in Inbound Firewall Denies.
- **Pure CMDB Search**: Searches on CMDB data stored in PostGreSQL, e.g. All Windows Servers where MS SQL Server process is running.
- **Lookup Table Searches**: Searches by combining Events and Lookup Tables.
- **Combined Event and CMDB Searches**
  - Nested Searches by combining Event Searches with CMDB Reports, e.g. All Windows Servers in CMDB that did not report in last 1 hour.
  - Event Searches using *DeviceToCMDBAttr* Function that can refer to CMDB Device Properties, e.g. All Critical Windows Servers in CMDB that did not report in last 1 hour, or All Windows Servers located in San Jose that did not report in last 1 hour.

Running a Built-in Historical Search

A historical search enables you to search events that are already stored in event database.

You can run a search from the Analytics tab.

1. Go to **Analytics > Search**.
2. From the folder drop-down list on the left, select **Shortcuts** or the **Reports** folder. The Shortcuts folder contains a few quick reports. The Reports folder contains the entire collection of built-in reports.
3. To run a Search from the **Shortcuts folder**, select a Report, click ▼, then click **Run** and choose the tab where Results will be displayed: **New Tab** or **Current Tab**. The Search will run and results would be displayed in the chosen tab.
4. To run any other Search, look for a report in the **Reports** folder. You can open the **Reports** folder and look through the reports one by one, or enter keywords in the Search box. Select a specific report and click ▼, and then **Run**. The Search will run and results will be displayed.

You can modify the Search and make this your own Search. The details are explained in Creating a New Search.

Creating a New Search

To create a search, the following steps are needed:

- Step 1 - Specify Search Filter
- Step 2 - Specify Time Range
- Step 3 - Specify Trend Interval
- (Optional) Step 4 - Specify Event Source
- (Optional) Step 5 - Specify Organization in a Service Provider Deployment
- Step 6 - Specify **Group By**, **Display Fields** and **Display Conditions**

Other Search Topics:

- Specify Maximum Number of Rows in the Result
- Saving Filter Conditions

Step 1 - Specify Search Filter

This step is similar to specifying the WHERE clause in SQL Query Language.

Follow these steps:

1. Go to **Analytics > Search** tab.
2. Click the **Edit Filters and Time Range...** field.
3. In **Filter By** Section, you can specify a filter condition in one of the following ways:
   a. **Event Keyword** - Enter any related keyword for search. See below for details.
   b. **Event Attribute** – Enter one more (Attributes, Operator, Value) tuples. See below for details.
   c. **CMDB Attribute** – Enter the attributes for CMDB Reports

Specifying Event Keyword Based Filters

Event Keyword based Filter is specified as a Boolean expression containing AND, OR, e.g. “(TCP OR UDP) AND 514”. When you enter this expression, then the search condition becomes

```
Raw Event Log CONTAINS “(TCP OR UDP) AND 514”
```

Specifying Event Attribute Based Filters

Event Attribute based Filter is specified as a Boolean expression of (Attribute Operator Value) tuples. Allowed Boolean Operators are AND, OR

- **Attribute** can be event attribute such as Source IP or an expression consisting of *non-aggregating* functions of event attributes. Examples are
  - LEN(Raw Event Log)
  - TO_LOWER(User)
- **Operator** can be of the following types
  - Arithmetic Operators: +, -, *, /
  - Comparison Operators: =, !=, <, <=, >, >=
  - Range Operators: BETWEEN, NOT_BETWEEN
  - Pattern matching Operators: CONTAIN, NOT_CONTAIN, REGEXP, NOT_REGEXP
  - List Filtering Operators: IN, NOT IN
  - NULL Testing Operators: IS (NULL), IS NOT (NULL)
- **Value** can be
  - An Event Attribute or
  - A CMDB Object
  - An expression consisting of *non-aggregating* functions of event attributes.

The full list of Event Attributes and their Data Types can be found in **Admin > Device Support > Event Types**. Note that you can create your Event Attribute to parse new event fields. Note that IP type is an Integer attribute in FortiSIEM. So regular expression is not allowed on IP types.

The following table shows the applicability of Operators to the various data types.

Operator Type	Operators	Operand Type	Example
Arithmetic Operators	+, -, *, /	IP, STRING, Integer, Double	
Comparison Operators	<, <=, >, >=, =, !=	IP, STRING, Integer, Double	Source IP = 10.1.1.1
Range Operators	BETWEEN, NOT_ BETWEEN	IP, Integer, Double	Source IP BETWEEN (10.1.1.1, 10.1.1.3)
Pattern matching Operators	CONTAIN, NOT_ CONTAIN, REGEXP, NOT_ REGEXP	STRING	Event Type CONTAIN PH_ DEV_MON
List Filtering Operators	IN, NOT IN	IP, STRING, Integer	Source IP IN CMDB > Network Device > Firewall Source IP IN (20.1.1.1, 10.1.1.3)
NULL Testing Operators	IS (NULL), IS NOT (NULL)	IP, STRING, Integer, Double	Source IP IS NULL User IS NOT NULL
Logical Operators	AND, OR, AND_NOT	Any expression that can be evaluated to true or false	(Source IP = 10.1.1.1) AND (Destination IP = 20.1.1.2)

The following CMDB Objects can be used in Queries.

- Any folder under **CMDB > Devices**
- Any folder under **CMDB > Applications**
- Any folder under **CMDB > Users**
- Any folder under **CMDB > Business Services**
- Any folder under **Resources > Watch Lists**
- Any folder under **Resources > Malware IPs**
- Any folder under **Resources > Malware Domains**
- Any folder under **Resources > Malware Hash**
- Any folder under **Resources > Malware Processes**
- Any folder under **Resources > Malware URLs**
- Any folder under **Resources > Watch Lists**
- Any folder under **Resources > Anonymity Network**
- Any folder under **Resources > Country Groups**
- Any folder under **Resources > Default Password**
- Any folder under **Resources > Event Types**
- Any folder under **Resources > Networks**
- Any folder under **Resources > Protocols**
- Any folder under **Resources > User Agents**

GUI enforces the correct CMDB Object usage, e.g.

- Source IP IN **CMDB > Network Device > Firewall** is allowed
- User IN **CMDB > Network Device > Firewall** is not allowed
- User IN **CMDB > Users** is allowed

The following list of functions are supported. For details see Appendix: Functions in Analytics.

Type	Functions
Aggregation Functions	AVG, COUNT, COUNT DISTINCT, FIRST, LAST, MAX, MEDIAN, MIN, MODE, PctChange, PCTILE, Pctile95, STDDEV, SUM, VARIANCE
CMDB Lookup Function	DeviceToCMDBAttr
Conversion Functions	LOG, TO_DOUBLE, TO_INTEGER, TO_STRING
Date Conversion Functions	DayOfWeek, HourOfDay
Evaluate and Set Function	IF
Extraction Function	EXTRACT
LookupTable Functions	LookuptableGet, LookupTableHas
String Manipulation Functions	LEN, LTRIM, REPLACE, RTRIM, SUB_STR, TO_LOWER, TO_UPPER, TRIM
Time Window Functions	EMA, SMA

Nesting of functions is allowed: e.g.

- AVG(LEN(Raw Event Log)),
- COUNT DISTINCT (TO_LOWER(User))

Specifying CMDB Attribute Based Filters from CMDB Reports

CMDB Attribute is for writing CMDB Queries. This enables you to write CMDB Queries in the same way as in CMDB Reports.

CMDB has various kinds of data, so you need to select the Target which specifies the data type. Possibilities are

- DEVICE – Device related information e.g. Device Vendor, Model, Operating System, etc.
- USER – User related information e.g. User Employee ID, User Name, User Login Time, etc.
- RULE – Rule related information e.g. Rule name, Severity, Active Flag, etc.
- REPORT - Report related information e.g. Report name, Report Filter, etc.
- MONITOR – Performance Monitoring related information such as Device Name, Job name, Job Status, etc

- TASK - Task related information Task Description, Task Progress, etc.
- IDENTITY – Identity and Location related information such Host Name, IP, User, Last Seen, First Seen, etc
- INCIDENT – Incident related information such as Incident Name, Incident Source, Incident target, First Seen, Last Seen, Count, etc
- EVENT_PULLING – Event Pulling Status such as Host Name, IP, Access Protocol, Status.
- CASE – Case Status such as Case ID, Case Title, Case Status, Assignee, etc.

After selecting Target, the Attributes will only show the ones relevant for the selected Target.

Step 2 - Specify Time Range

You need to specify whether you want to run a *real time search* or a *historical search* with time window.

- A *real time search* enables you to search events in real time in a streaming mode as events are being ingested.
- A *historical search* enables you to search events that are already stored in the event database. For a historical search, you need to specify the time window over which the query will run.

Follow these steps:

1. Click the **Edit Filters and Time Range...** field.
2. Go to **Time Range** section.
3. Click **Real-time** if you want to run a Real time Search. Specify **Display Time Range**, which is the time range for which the results are displayed in the chart window.
4. To run a **Historical search**, specify the Time window in one of two ways:
   a. **Relative** option: Events will be searched for the last N (Minutes/Hours/Days) starting from the current time. Choose the time scale and the quantity.
   b. **Absolute** option: The query will run for a specific time window in the past. There are two ways to specify this:
      i. Using two explicitly defined time epochs: **From** and **To**. Specify the **From** and **To** time ranges.
      ii. Using **Always prior** option to define time-periods such as the previous week or the previous two months. This option is helpful if you are interested in re-running the same report periodically, as you do not have to change the time period.

Step 3- Specify Trend Interval

When a Search is run, the result is shown in two parts. The top part shows the result trend chart, while the bottom part shows the results in a tabular form.

1. Click the **Edit Filters and Time Range...** field.
2. Specify the **Trend Interval** to determine the granularity of the time axis for the Trend chart.

Step 4 - Specify Event Source

If you have separate Online and Archive databases, then you can use **Event Source** field to specify whether Online or Archive events will be searched.

1. If you are running FortiSIEM EventDB as the Online database and have Archive Configured, then you can specify whether to direct the search to the Online database or Archive database.
2. If you are running Elasticsearch as the Online database and have Archive Configured, then you can specify whether to direct the search to the Online database or Archive database.
3. If you are running ClickHouse and have setup real time archive using NFS, then you can specify whether to direct the search to the Online or Archive database. If you have chosen AWS S3 or GCP GCS as Archive destination, then Event Source does not need to be specified, since ClickHouse manages the Hot/Warm/Cold Tiers and AWS S3/FCP GCS in a unofmr way – no matter where the data resides, ClickHouse will find it.

Specify Maximum Number of Rows in the Result

This enables you to limit the number of rows returned in an unaggregated search. For EventDB and Elasticsearch based deployments, the limit is 100K rows. For ClickHouse based deployments, the limit is 1 Million rows. It is recommended to have at least 32vCPU and 32GB memory on Supervisor and Worker nodes to achieve 1 Million rows.

1. Click the **Edit Filters and Time Range...** field.
2. Specify **Result Limit**.

Note that for aggregated search, you can limit the number of rows returned using **Display Conditions**.

Saving Filter Conditions

You can save this Filter by clicking the **Save** button and providing a name for this Filter condition. Next time, you can click **Load** to load this Filter into the GUI.

Click **Apply** to save the Filters as part of the current Search. You can also click **Apply and Run** to save and run the search with the currently configured Organization, Group By and Display Fields and Display Conditions. If you want to modify them, then follow the steps below.

Step 5 - Specify Organizations for Service Provider Deployments

In a Service Provider deployment, you can choose to Search over any subset of Organizations. Select the organizations from the **Select Organizations** drop-down icon ( ).

Step 6 - Specify Group By, Display Fields and Display Conditions

This enables you to select how the events that match the Filter Criteria will be displayed. You can choose one of the following views:

- Un-aggregated view consisting of a subset of parsed event attributes
- Aggregated view consisting of a set of event attributes and aggregated values such as COUNT, COUNT DISTINCT, AVG etc.

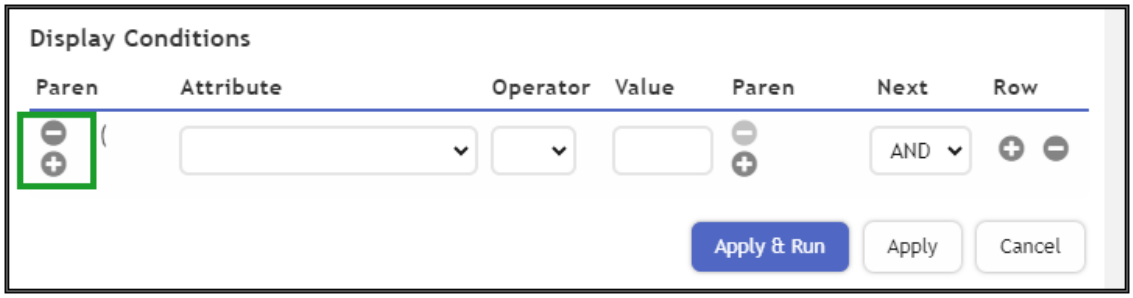
This step is similar to specifying the SELECT, GROUP BY and HAVING clauses in SQL Query Language.

Follow these steps:

1. Click on the Change Display Fields ( ) icon
2. You can select multiple rows, each row consisting of the fields: **Attribute**, **Order** and **Display As**. You can add or delete a row using the icons. You can move each row up or down using the icons.
3. For **Attribute**: you can specify an Event Attribute or the built-in expression COUNT (Matched Events) or build you own custom expression.
   a. To specify an **Event Attribute**, simply type the attribute name and select the exact match from the drop-down list.
   b. To specify the built-in expression COUNT (Matched Events), simply select it from the drop-down list.
   c. To build a custom expression, click **Expression Builder** and follow these steps:
      i. Click **Select function** and type in the function name in Search window and select the exact match from the drop-down list.
      ii. Click the **Functions** and pick either another **function** for nested function or an **event attribute** from the drop-down list. If you picked a function, then click **Functions** again and pick either another **function** or an **event attribute**. You can continue until the function definition is complete. By default, the function shows horizontally but you can select the **Vertical** option to display it vertically.
      iii. After completing the function definition, click **Add to** and the function shows in the **Expression** edit box.
      iv. You can click **Validate** to make sure FortiSIEM accepts this definition. You can click **Clear** to start over.

v. If you want an expression such as X + Y, then you can enter + in the **Expression** edit box after the function you just entered (X) and start defining the second function (Y) by clicking **Functions**, completing the function definition, and then clicking **Add to**. The entire function will appear in the **Expression** box. You can click **Validate** to make sure FortiSIEM accepts this definition. Some examples of expressions are:
   i. SUM(Sent Bytes)
   ii. SUM(Sent Bytes) + SUM(Received Bytes)
   iii. (SUM(Sent Bytes) + SUM(Received Bytes))/2
   iv. AVG(LEN(Raw events))
vi. Click **OK** to add this expression as an Attribute.

4. For **Order**, you can choose ASC (respectively DESC) to display the values in ascending (respectively descending order
5. For **Display As**, you can enter a display name for the attribute to show up in the query result table.
6. If you entered an aggregation function (such as COUNT (Matched Events) or SUM (Sent Bytes)) as an attribute, then you can use the **Display Conditions** to truncate the query result table.
   a. You can select multiple rows, each row consisting of the fields: **Attribute**, **Operator** and **Value**. You can add or delete a row using the ⊕ ⊖ icons. Multiple rows are connected with AND/OR operator. You can add parenthesis using + and - to control the order of operations.



   b. Select an **Attribute** from the drop-down list. This list auto populated with the aggregate functions in the **Group By** and **Display Fields**.
   c. Select an **Operator** from the drop-down list.
   d. Type in a **Value**.
   e. If multiple rows are needed, then add a row and enter **Attribute**, **Operator** and **Value** for that row. Some examples of expressions are:
      i. COUNT(Matched Events) > 20
      ii. AVG(CPU Util) >= 90
      iii. AVG(CPU Util) >= 90 AND AVG(Memory Util) >= 95
7. You can save this **Group By** and **Display Fields** by clicking the **Save** button and providing a name for this definition set. Next time, you can click **Load** to load this definition into the GUI.
8. Click **Apply** to save the **Group By** and **Display Fields**. You can also click **Apply and Run** to save and run the search with the currently configured Filters, Time range and Organizations.

Creating a Nested Search

Nested Query functionality enables one query to refer to results from another query. This section describes how to set up and use nested queries for the three supported scenarios:

- Outer CMDB Query, Inner Event Query
- Outer Event Query, Inner Event Query
- Outer Event Query, Inner CMDB Query

Outer CMDB Query, Inner Event Query

The following generalized steps describe how to create a nested query where the outer query targets CMDB and the inner event query targets events.

If you want to reuse an existing query, then skip Step 1 and go to Step 2. Note that for a nested query to work correctly, the data type of the filter attribute in the outer query must "match up" with the data type of one certain display column in the inner query.

Step 1: Construct the Inner Event Query

1. Go to the **ANALYTICS** page.
2. Construct the query and make sure it produces the desired results.
   a. Click the **Edit Filter and Time Range** field and select **Event Attribute** in the query tab.
   b. Set the **Time Range**. For example, you can set it to the last 1 hour. This time period is not important if you use this query as an inner query.
   c. If it has the **Event Source**, then you can set it as Online.
   d. Click **Apply** to save your changes.
   e. Click the **Change Display Fields** icon and enter the attributes you want to display.
   f. Click **Apply & Run**.
3. Click **Action > Save as Report**.
4. Ensure **Save Definition** is checked.

Step 2: Construct the Outer CMDB Query by Referring to the Query in Step 1

1. Go to the **ANALYTICS** page.
2. Click in the Search bar--it will open the **Filter** dialog box.
3. Select **CMDB Attribute**.

4. Select the appropriate target from the drop-down list.
5. Set the query condition.
   a. Select the **Attribute**.
   b. Select the **Operator**--the most common operators are IN and NOT IN.
   c. Click in the **Value** field and select **Select from Report.**
   d. Select the **Report** name, saved in Step 1, Substep 4.
   e. Open the **Attribute** drop-down list and choose the attribute that matches the attribute in Step 2, Substep 5a.
   f. Click **OK**.
6. Choose the **Nested Time Range**: the inner report will be run for this time range.
7. Click the **Change Display Fields** icon and choose the attributes you want to display.
8. Click **Apply & Run**.
9. To save the report, click **Actions > Save as Report**. Enter the name of the nested query.

Outer Event Query, Inner Event Query

The following generalized steps describe how to set up and use nested queries for an outer event query and an inner event query.

Step 1: Construct the Inner Event Query

1. Go to the **ANALYTICS** page.
2. Click the **Edit Filter and Time Range** field.
   a. Select **Event Attribute** and create the **Filter Condition**.
   b. Set the **Time Range**.
   For example, you can set it to the last 1 hour. This time period is only useful to check if this query produces the desired results. If used as an inner query, time range would be set separately in Step 2 below.
   c. If it has the **Event Source**, then you can set it as Online.
   d. Click **Apply** to save your changes.
   e. Click the **Change Display Fields** icon and enter the attributes you want to display. This query needs to be an aggregate query to be used as an inner query. One of the Group By attributes must match (meaning compatible value sets) an attribute chosen in the outer query in Step 2, Substep 2.d.ii
   f. Click **Apply & Run**.
3. If you are happy with the result, then click **Actions > Save as Report**. Ensure **Save Definition** is checked.

Step 2: Construct the Outer Event Query

1. Go to the **ANALYTICS** page.
2. Click the Edit Filter and Time Range field.
   a. Select **Event Attribute** in the query tab.
   b. Choose an **Attribute**.
   c. Choose an **Operator**. The most common operators are IN and NOT IN.
   d. Click the **Value** field and select **Select from Reports**.
      i. Select the **Report** name, saved in Step 1, Substep 3.
      ii. Open the **Attribute** drop-down list and choose the attribute that matches the attribute in Step 1, Substep 2e.
      iii. Click **OK**.
3. Choose the time ranges.
   a. Choose the time range for outer query.
   b. Choose **Nested Time Range** for the inner query.
   c. If it has the **Event Source**, then you can set it as Online.
4. Click **Apply** to save your changes.
5. Click the **Change Display Fields** icon and enter the attributes you want to display.
6. Click **Apply & Run**.
7. You can save the results by clicking **Actions > Save as Report**. Ensure **Save Definition** is checked.

Outer Event Query, Inner CMDB Event Query

The following generalized steps describe how to set up and use nested queries for an outer event query and an inner CMDB query.

Step 1: Construct the Inner CMDB Query

1. Go to the **ANALYTICS** page.
2. Click the **Edit Filter and Time Range** field and select **CMDB Attribute** in the query tab.
   a. Select the appropriate **Target** from the drop-down list.
   b. Set the query condition.
      i. Select the **Attribute**.
      ii. Select the **Operator**
      iii. Click in the **Value** field. Do not select **Select from Report**.
   c. Click **Apply** to save your changes.
3. Click the **Change Display Fields** icon and enter the attributes you want to display.
4. Click **Apply & Run**.

5. If you are happy with the result, then click **Actions > Save as Report**. Ensure **Save Definition** is checked.

Step 2: Construct the Outer Event Query

1. Go to the **ANALYTICS** page.
2. Click the **Edit Filter and Time Range** field and select **Event Attribute** in the query tab.
   a. Choose an **Attribute**.
   b. Choose an **Operator** - the most common operators are IN and NOT IN.
   c. Click in the **Value** field and select **Select from Report**.
      i. Select the **Report** name, saved in Step 1 Substep 5.
      ii. Open the **Attribute** drop-down list and choose the attribute that matches the attribute in Step 1 Substep3.
      iii. Click **OK**.
3. Choose the **Time Range** for outer query.
4. If it has the **Event Source**, then you can set it as Online.
5. Click **Apply** to save your changes.
6. Click the **Change Display Fields** icon and enter the attributes you want to display.
7. Click **Apply & Run**.
8. You can save the results by clicking **Actions > Save as Report**. Ensure **Save Definition** is checked.

Viewing Real-time Search Results

Real time search enables you to search the events in real time as they are being ingested and before they are stored in the event database. Events matching filter conditions are shown from current time onwards. Note that aggregations are not permitted in real-time search.

The search results are displayed in two panes:

- Top pane displays the counts of matched events over time.
- Bottom pane displays the results in tabular form following the definitions in the **Display Fields**.
- Since results are coming in continuously, the results scroll and the latest events are displayed at the top.

The following topics are available:

- Display Controls
- Viewing Parsed Raw Events
- Modifying Search Filter Criteria
- Modifying Search Display Fields
- Zooming-in on a Specific Time Window

Display Controls

The following actions are possible while viewing Real-time Search results:

- To pause the search, click **Pause**.
- To restart the real-time search from the point you left off, click **Resume** after **Pause**.
- To fast forward to the current time, click **Fast forward**.
- To clear the result table, click **Clear**.
- To restart the search all over again from the current time, click **Stop** and then **Run**.

Viewing Parsed Raw Events

If Raw Event Log is displayed, then hover over a **Raw Event Log** cell, click ▼, and click **Show Details**. The display shows how FortiSIEM parses the event. Note that from this view, you can choose a parsed attribute to be displayed or added to the Filter condition.

Modifying Search Filter Criteria

This can be done in three ways:

1. You can edit **Filters and Time Range** and then click **Apply and Run**.
2. You can Select a column in the bottom pane and choose **Add to Filter** and the operator. Then **Stop** the query and click **Run**.
3. If Raw Event Log is displayed, then hover over a **Raw Event Log** cell, click ▼, click **Show Details** and then select **Filter** next to the Item that you want to Filter on. Then **Stop** the query and click **Run**.

Modifying Search Display Fields

This can be done in two ways:

1. You can edit **Group By** and **Display Fields** and then click **Apply and Run**.
2. If Raw Event Log is displayed, then hover over a **Raw Event Log** cell, click ▼, click **Show Details** and then select **Display** next to the Item that you want to Filter on. Then **Stop** the query and click **Run**.

Zooming-in on a Specific Time Window

If you see an unusual pattern (for example, a spike) in the trend chart and want to drill down without entering the exact time range, do one of the following:

- Click the bar – a new search tab is created by duplicating the original search and adding the right time window as seen by hovering on the bar.
- Press and hold **Shift** key and drag the mouse over a time window – this modifies the time window in the current tab.
  Click **Apply & Run** to see the results.
- When you run the Real-time search, a pop-up will appear asking if you want to stop the Real-time search before proceeding to the Historical Search.
- If Raw events are displayed, then you can hover over a **Raw Event Log** cell, click ▼, and click **Show Details** to see how FortiSIEM parses the event.

Viewing Historical Search Results

Historical search enables you to search events that are already stored in event database.

The following topics are available:

- Understanding Default Result Display
- Choosing other Chart Displays
- Viewing Parsed Raw Events
- Modifying Search Filter Criteria
- Modifying Search Display Fields
- Zooming in on a Specific Time Window
- Copying the Search to a Separate tab

Understanding Default Result Display

Historical search results are displayed in two panes:

- Bottom pane displays the results in tabular view following the definitions in the Display Fields. For ClickHouse based deployments, there is an additional Result Filter pane on the left, that shows the distribution of the result columns (other than Date fields and Raw Event Log).
- Top pane displays how the results in the bottom pane trend over time:
  - For **non-aggregated searches**, the trend is for event occurrence and is displayed in a trending bar graph. Each bar captures the number of entries in the table during a particular time window.
  - For **aggregated searches**, the trend is for any of the (numerical) columns with aggregations. Trends are displayed for the Top 5 entries in the table. For integer values, such as COUNT (Matched Events), you will see a trend Stacked Bar Chart, while for continuous values such as AVG(CPU Utilization), you will see a Stacked Line Chart.

The **Result Filter** display enables you to see the distinct values in each column in the search result and their frequencies. Top 100 results are shown and by default, they are shown in Descending order. You can change the order by clicking the icon.

1. If you select one or more values for a field, then
   a. Other columns on the left changes to reflect the selection
   b. Trend and the Result table on the right pane changes to reflect the change
2. You can click the button to minimize the Result Filter display, then the trend chart and the result table takes over the whole horizontal width. This may be useful for analyzing unaggregated raw message queries. Subsequent searches will not show the result Filter by default. You can restore the Result Filter by clicking on the button
3. You can add the Result Filter choices to the Query condition by clicking the icon.

   Note: Some event attributes, functions and queries are not supported:

- Date Fields (Examples: Event Receive time, Event Receive Hour, Event Receive Date...)
- Raw event log, Binary Raw event log
- Some functions:
  - Aggregate functions – COUNT, MEDIAN, MODE, STDDEV, VARIANCE, SUMSQ, PCTILE, COUNT DISTINCT, MAX, MIN, AVG, SUM, FIRST, LAST, Pctile95
  - Time window functions – SMA, EMA
- Some queries
  - Baseline reports
  - Incidents reports
  - Real-time query

For displaying trends in aggregated searches, you can change the default chart choice and opt for one of the following charts:

1. Stacked Bar Chart
2. Stacked Line Chart
3. Line Chart

To show the trend for only one row in an aggregated search, uncheck all the checkboxes under **Chart** column other than the oneyou want to keep. To add the trend chart for a new row, check the checkbox under **Chart** column for that row. The trend will show automatically.

When an aggregated search has multiple aggregated fields:

- To display trend for another aggregated field, choose that field in the drop down in right hand side. The chart will automatically refresh.
- To show trends of both aggregated fields on two sides of the same graph, choose the other field in the Lower chart drop down. The chart will automatically refresh.

A few shortcuts are available to run the search for different relative time windows: 15 mins, 1 hour, 1 days, 7 days, 30 days. You can select these values from the top right (15m 1h 1d 7d 30d) and the search will automatically re-run.

To hide the trend chart, click the icon on the top right. To bring back the trend chart, click the icon on the top right.

Choosing other Chart Displays

FortiSIEM provides a variety of charts and maps to better help you understand and analyze your incident data. You can access these charts and views from the widget dashboard settings (see Modifying widget information display) or by clicking the **TABLE** or drop-down icon in the Analytics page (see Viewing Historical Search Results).

Chart/View	Description	Display Settings	Requirements
Table	Displays data in a tabular format.	You can choose to display the bar chart (**Show Bar**), the event type (**Show Event Type**), and the count (**Count**). Set the colors for the bar chart or reverse the color map.	None
Link Graph	Displays source, event, and destination relationships. Source nodes appear in light blue, Event nodes are color coded by their severity if event attribute "Event Severity Category" exists in the Display Fields on Table view. A node can be clicked and dragged to be repositioned. If a node can be represented by a recognizable device type from FortiSIEM, the appropriate icon will be displayed, otherwise a default monitor icon will appear. The Rows and Total number represent the number of data items in the table view, not the number of nodes. For example, one representation will consist of 3 nodes (source, event, destination), but if all the data items share the same source, event, and destination, only three nodes will appear. Click on any node and the following options appear: • Quick Info - Select to show more information about the selected node. • Add <*object*> to Filter - Adds the data from the selected node to a filter.	Select the **Source**, **Event**, and **Destination** from the drop - down lists. Auto Layout attempts to show all nodes in an optimal manner. To disable, deselect the **Auto Layout** checkbox.	A source and destination are required.

Chart/View	Description	Display Settings	Requirements
Bar Chart	Displays data similar to a bar chart.	Select the Aggregate Field (**Column**) to display and their colors. You can also reverse the color map.	At least one numeric column is required.
Chord Chart	A graphical method of displaying the inter-relationships between data in a matrix. The data is arranged radially around a circle with the relationships between the data points typically drawn as arcs connecting the data.	Select the incident **Source**, **Target**, and **Value** from the drop-down lists.	At least two key columns and one numeric column are required.
Choropleth Chart	A thematic map in which areas are shaded or patterned in proportion to the measurement of the statistical variable being displayed on the map.	Select the **Location** and **Value** from the drop-down lists.	At least one numeric column is required. Configure **Google Maps API Key** in **ADMIN > Settings > System > UI** See UI Settings.
Cluster Bubble Chart	You can use a bubble chart instead of a scatter chart if your data has three data series that each contain a set of values. The sizes of the bubbles are determined by the values in the third data series.	Select the **Column** from the drop-down list.	At least one numeric column is required.
Donut Chart	Displays data similar to a pie chart.	Select the Aggregate Field (**Column**) to display since the report may have multiple Aggregate Fields.	At least one numeric column is required.

Chart/View	Description	Display Settings	Requirements
GEO Map Chart	Displays the IP addresses in a geographic map.	Public or private IP addresses with location defined in **ADMIN > Settings > Discovery > Location**. See Setting Location.	At least one numeric column is required.
Heat Map Chart	Displays two event attributes and a numerical aggregate value.	Select the Heat map coordinates **X** and **Y**, and an associated **Value**.	At least two key columns and one numeric column are required.
Sankey Chart	A specific type of flow diagram, in which the width of the arrows is shown proportionally to the flow quantity.	Select the **Source**, **Target**, and **Value** from the drop-down lists.	At least two key columns and one numeric column are required.
Scatter Plot Chart	Plots two aggregate fields.	Select two aggregate fields, **X** and **Y**. Select the **Size** of the sample.	At least two numeric columns are required.
Sunburst Chart	Visualizes hierarchical data, depicted by concentric circles. The circle in the center represents the root node, with the hierarchy moving outward from the center.	Select the **Rank1**, **Rank2**, **Rank3** and **Count** from the drop-down lists.	Only one column can be used in one rank.
Tree Map Chart	Displays columns in a Tree Map.	Select the Tree Map **Ranks** and the **Count** attributes from the drop-down lists.	Only one column can be used in one rank.
Trend Line Chart	A "trend" line is superimposed on a chart that reveals the overall direction of the data.		
Trend Area Chart	A graph that shows trend changes over time, by displaying a series of data as different colored lines.		

Chart/View	Description	Display Settings	Requirements
Trend Bar Chart	Uses bars to track trends over time.		

Viewing Parsed Raw Events

If Raw Event Log is displayed as a column, then hover over a **Raw Event Log** cell, click ▼, and click **Show Details**. The display shows how FortiSIEM parses the event. Note that from this view, you can choose a new parsed event attribute to be displayed or added to the Filter condition.

Modifying Search Filter Criteria

This can be done in three ways:

1. You can edit using **Edit Filters and Time Range...** and then click **Apply and Run**.
2. You can select a column in the bottom pane and choose **Add to Filter** and the operator. Then **Stop** the query and click **Run**.
3. If Raw Event Log is displayed, then hover over a **Raw Event Log** cell, click ▼, click **Show Details**, and then select **Filter** next to the Item that you want to Filter on. Then **Stop** the query and click **Run**.

Modifying Search Display Fields

This can be done in two ways:

1. You can edit **Group By and Display Fields** and then click **Apply and Run**.
2. If Raw Event Log is displayed, then hover over a **Raw Event Log cell**, click ▼, click **Show Details**, and then select **Display** next to the Item that you want to Filter on. Then **Stop** the query and click **Run**.

Zooming in on a Specific Time Window

If you see an unusual pattern (for example, a spike) in the Trend Chart and want to drill down without providing an exact time range, do one of the following:

- Click the bar – a new search tab is created by duplicating the original search and adding the right time window as seen by hovering on the bar.
- Press and hold the **Shift** key and drag the mouse over a time window. This modifies the time window in the current tab. Click **Apply & Run** to see the results.

Copying the Search to a Separate tab

At some point, you may want to copy the search results to a new tab for further modifications. To do this, click **Actions** and select **Copy to New Tab**.

Searches Using Pre-computed Results

If you want to run the same search again and again, or you want to run certain pre-defined searches over a large time window, then the search time can be reduced by setting up pre-computation. See Known Issues in the latest What's New for any limitations with pre-computed results.

It is important that search filters, group by, and display parameters and display filters do not change. Otherwise, the pre-computation results will be invalid.

To use this feature, you must complete these steps:

1. Select a Report and turn on pre-computation.
2. Select the Pre-computed result option when running the search.

The following sections provide more information about the pre-computation feature and how to use it.

- Usage Notes
- Setting Up Pre-computation
- Impact of Organization and Roles
- Viewing Pre-computed Results
- Running a GUI Search on Pre-computed Results
- Scheduling a Report Based on Pre-computed Results
- Running a Report Bundle Based on Pre-computed Results
- Scheduling a Report Bundle Based on Pre-computed Results

Usage Notes

1. Currently, pre-computation only works with
   - FortiSIEM EventDB
   - Elasticsearch
1. Pre-computation is currently supported for Aggregated queries with COUNT, SUM, AVG, MAX, and MIN operators. Raw event queries and nested searches are not supported.
2. If you run a query with pre-computed results, but the search interval is wider than the available pre-computed results, then the results are returned for the pre-computed time interval only. Currently, FortiSIEM does not run a separate search for the missing time window and stitch together the two search results.
3. Pre-computation begins at hourly/daily boundaries. For example, if you set up hourly pre-computation at 2:34 PM, then the first pre-computation will begin at 3:10 PM for the time interval 2:00 PM – 3:00 PM.
4. FortiSIEM does not semantically compare search filters, group by, and display parameters and display filters for two searches. Thus, pre-computed results cannot be used for a cloned search.

5. Pre-computation is set up at a report level and not a report bundle level.
6. For the Service provider case, you must effectively have the same role in all Organizations to be able to use pre-computed results. Examples are
   a. Full Admin for all Organizations.
   b. Help desk user for one Organization and Read only user for another Organization. Note that both of these roles have empty data conditions and hence are effectively the same role from a pre-computation perspective.

Setting Up Pre-computation

Only a Super Global user having the Full Admin role can set up pre-computation. This is because only such a user can see all the roles. A Full Admin user for a specific organization cannot set up pre-computation. Follow these steps to set up pre-computation.

1. Log in to FortiSIEM as a Super Global Full Admin user.
2. Go to **RESOURCES > Reports**.
3. Select a **Report**, Click **More** and Select **Pre-compute**.
4. Enter the pre-compute options:
   a. Select the **Enable** option to enable pre-computation. If you do not select **Enable**, then the definition will be there, but pre-computation will stop and all older results will be deleted.
   b. Carefully select the **Organization** and the **Roles** for whom queries will be pre-computed. These selections determine when a user query can use pre-computed results. See Impact of Organization and Roles for more detail.
   Note: If duplicate roles with different names exist, only one role will appear for selection. For example, if you have "Full Admin" and "Full Admin2" with the same permissions, only "Full Admin" would appear for the pre-compute role selection.
   c. Select Pre-computation **Frequency**. A lower frequency provides more accuracy at the expense of more system load and storage. Choose the lowest frequency you can accept.
   d. Select the **Age** in number of days. Pre-computed results older than this age will be deleted.
   e. Check the **Pre-compute history** option if you want the system to automatically run and fill up data from earlier time intervals.
5. Click **OK**.

The system will begin pre-computation on the hour or day boundary. For example, if you set up hourly pre-computation at 2:34 PM, then the first pre-computation will begin at 3:10 PM for the time interval 2:00 PM – 3:00 PM. As another example, if you set up daily pre-computation at 10:00 PM, then the first pre-computation will begin slightly after 12:00 AM midnight for the previous day.

Impact of Organization and Roles

A query definition does not enforce Organization and Role restrictions. When you run a query, you are forced to choose one or more Organizations. The data conditions for your role definition are

automatically applied. For example, if you run a Top Event Type query as a Full Admin user for Org1 and Org2, then you get All Event Types for Org1 and Org2. However if you run as a Network Admin for Org2 then you only get Network Event Types for Org2. Your Organization and Role assignments have an effect on the query results as they change the query filters.

If you set up pre-computation for an Organization and a set of Roles, then only the users belonging to the same Organization and having exactly the same Role can use pre-computed results. The only exception is for a Full Admin user who can use any pre-computed result in a query. The examples in the following table illustrate this point.

Pre-computation Definition			
Organization	**Role**	**Who can use pre-computed results**	**Who cannot use pre-computed results**
All Orgs Combined	Full Admin	Super-global users that are Full Admin for all Organizations or have roles without data conditions in some organizations.	Other users, for example, Super Global Network Admins for Org1 and Full Admin for Org2
All Orgs Combined	Network Admin	Super-global users that have the Network Admin role in All Organizations.	
All Orgs Combined	Network Admin, Server Admin	Super-global users that are both Network Admin and Server Admin in All Organizations.	If the user is a Network Admin for Org1 and Server Admin for Org2.
Org1	Full Admin	Full Admin or users with no data constraints belonging to Org1 can use pre-compute results.	Other users, for example, Org1 Network Admins cannot use these pre-computed results.
Org1	Network Admin	Network Admin users belonging to Org1 can use pre-compute results.	
Org1	Network Admin, Server Admin	Users belonging to BOTH Network Admin and Server Admin and belonging to Org1.	If the user belongs to only one role, for example Network Admin only, then the user cannot use pre-computed results.

Viewing Pre-computed Results

Once pre-computation is defined, FortiSIEM will pre-compute on the hour or day boundary.

To see the time slots of pre-computed results:

1. Select a Report.
2. Click **Pre-compute > Results**.
3. Click **Refresh** to get the latest results.
   a. **Time Range From** and **Time Range To** represent the Query Time Window.
   b. **Organization** and **Roles** relate to the query conditions.
   c. **Finish Time** specifies when the pre-computed query finished.

To see the content of a pre-computed result:

1. Select one row and click **View Results**.
2. You will be taken to the **ANALYTICS** tab with the query conditions already provided. You can see the results. The query name will display **(Pre-computed)** appended to the end of the name.
3. Note that because you are running a pre-computed query, you are allowed to perform only these two operations:

   All of the other possible choices, such as Query Filters, Organization Drip down, and Query Group By and Display Fields, are grayed out and unavailable.

   a. Change the time range by clicking the **Query Filter** search bar and selecting a different **Time range**.
   b. Load another pre-computed (Organization, Role) combination for the same query by going to the **Query Filter** search bar and selecting a different (Organization, Role) from the **Pre-compute Settings** menu.
4. If you want to stay in this page and change other conditions, click **Query Filter** search bar and deselect **Pre-compute Settings**.

Running a GUI Search on Pre-computed Results

You can run a search from the GUI on pre-computed results from the **ANALYTICS** page or the **RESOURCES** page.

- From the ANALYTICS Page
- From the RESOURCES Page

From the ANALYTICS Page

1. Load a **Report** and click **>**.
2. If the Report has been pre-computed, then the system will ask you to choose whether you want to use pre-computed results.
   a. If you do not want to use pre-computed results, then remove the check from **Use pre-compute for** and click **OK**. The query will run by searching the database.
   b. If you want to use pre-computed results, then check **Use pre-compute for** and select the Organization/Role combination from the drop-down list and click **OK**. The query will run based on pre-computed results.

3. Note that because you are running a pre-computed query, you are allowed to perform only these two operations:.
   All of the other possible choices, such as Query Filters, Organization Drip down, and Query Group By and Display Fields, are grayed out and unavailable.
   a. Change the time range by clicking the **Query Filter** search bar and selecting a different **Time range**.
   b. Load another pre-computed (Organization, Role) combination for the same query by going to the **Query Filter** search bar and selecting a different (Organization, Role) from the **Pre-compute Settings** menu.
4. If you want to stay in this page and change other conditions, click the **Query Filter** search bar and deselect **Pre-compute Settings**.

From the RESOURCES Page

1. Select a **Report** and click **Run**. A dialog box will open.
2. Select the **Organization** for which you want to run the report. The query result will contain the selected organizations. Note that based on the selected organizations, the pre-compute options below will change.
3. Select **Report Time Range**.
4. Select the pre-compute option if available from the menu.
5. Click **Run**.
6. You will be taken to the **ANALYTICS** tab with the query conditions already provided. You can see the results. The Query name will display **(Pre-computed)** appended at the end of the name.
7. Note that because you are running a pre-computed query, you are allowed to perform only these two operations:.
   All of the other possible choices, such as Query Filters, Organization Drip down, and Query Group By and Display Fields, are grayed out and unavailable.
   a. Change the time range by clicking the **Query Filter** search bar and selecting a different **Time range**.
   b. Load another pre-computed (Organization, Role) combination for the same query by going to the **Query Filter** search bar and selecting a different (Organization, Role) from the **Pre-compute Settings** menu.
8. If you want to stay in this page and change other conditions, click the **Query Filter** search bar and deselect **Pre-compute Settings**.

Scheduling a Report Based on Pre-computed Results

1. Go to the **RESOURCES** page.
2. Select a **Report** and click **More > Schedule**. A dialog box will open.
3. Select the **Organization** for which you want to run the report. Note that based on the selected organizations, the pre-compute options below will change.

   a. If you select **Combine all selected Organizations into one Report**, then the report will contain data from all organizations. You also have the option to select the organizations that you want to include. For pre-compute to work, you must select **All Organizations**.
   b. If you select **Generate separate Report for each selected Organization**, then a separate report will be sent out for each selected organization, Data between organizations will not be mixed in the same report. For pre-compute to work, you must select these Organizations to be pre-computed.
4. Select **Report Time Range**.
5. If you want data to be pre-computed, then select **Pre-compute settings** from the menu. You can select multiple entries for step 3b above.
6. Click **Next** and enter values for the rest of the options in the dialog box.
7. Click **OK**.

The system will run the report based on a schedule. If pre-compute settings are specified then the report results will be based on pre-computed data.

Running a Report Bundle Based on Pre-computed Results

A Report Bundle consists of one or more reports. One or more reports may be set to be pre-computed. If you run the Report Bundle, then the reports set up for pre-computation will have pre-computed results, while other reports will run normally (without pre-computation).

1. Go to **RESOURCES > Reports > Report Bundle**.
2. Select a **Report Bundle**.
3. On top left, select **Export Report Bundle**.
4. In **Pre-compute Settings**, select the Organization and Role combination. Each Report can be pre-computed for multiple Organization and Role combinations. When scheduling a report bundle, a common Organization and Role combination must be chosen that is applicable for ALL pre-computed reports. When Pre-Computation is defined, Filters cannot be selected.
5. Select other setting as usual.
6. Click **OK** to run the Report Bundle.

Scheduling a Report Bundle Based on Pre-computed Results

A **Report Bundle** consists of one or more reports. One or more reports may be set to be pre-computed. If you schedule the Report Bundle, then the reports set up for pre-computation will have pre-computed results, while other reports will run normally (without pre-computation).

1. Go to **RESOURCES > Reports > Report Bundle**.
2. Select a **Report Bundle**.
3. On top left, select **Schedule Report Bundle**.
4. Click **+** to create a schedule.
5. In **Pre-compute Settings**, select the Organization and Role combination. Each Report can be pre-computed for multiple Organization and Role combinations. When scheduling a report bundle, a common Organization and Role combination must be chosen that is applicable for ALL pre-computed reports. When Pre-Computation is defined, Filters cannot be selected.
6. Select other setting as usual.
7. Click **OK** to schedule the Report Bundle.

Working with Search Results

After receiving your search results, there are a number of actions you can take.

- Saving Search Definition and Results
- Viewing / Deleting Saved Search Results
- Exporting Search Results
- Emailing Search Results
- Creating a Rule
- Saving Search Filter and Display Conditions
- Executing a FortiSOAR Playbook
- Running a FortiSOAR Connector
- Invoking FortiAI
- Creating a New Case
- Adding to an Existing Case

Saving Search Definition and Results

Follow these steps to save the Search definition and Results.

1. From the **Actions** drop-down list, select **Save as Report**.
2. Specify the **Report Name**.
3. If the **Search Definition** needs to be saved, then follow these steps:
   a. Check **Save Definition** to specify that the Search Definition must be saved.
   b. In **Save To**, select the folder in **Resources > Reports** where the Search Definition will be saved.
4. If the **Search Result** needs to be saved, then follow these steps:
   a. Check **Save Results** and choose the duration for which the result needs to be saved.
   b. Since the results will be saved as PDF, you can select a Report Design template by checking the **Save Report Design Template** option and modifying the template inline.
5. Click **OK**.

Viewing / Deleting Saved Search Results

Follow these steps:

1. Go to the **Load Report/Saved Results** folder by clicking .
2. Click **Saved Results**.

3. Select the Saved Result, Click **>**, select **View Result**.
4. The result will be displayed.

To delete a Saved Result, choose **Delete** in Step 2 above.

Exporting Search Results

Follow these steps to export Search Results to a PDF or CSV file and save it on you local workstation.

1. From the **Actions** drop-down list, select **Export Result**.
2. Enter the **User Notes** (optional).
3. Specify the **Output Format** as **PDF**, **RTF**, or **CSV**.
   Files with a large number of rows should be exported in CSV format.
4. Select the **Time Zone** of the data from the drop-down list.
5. Select the **Report Template** if you select **PDF** or **RTF** format:
   - **Defined**: To use the template defined for this report defined under **Resources > Reports**, or use the system default template for Analytics export
   - **New**: To create a new custom report template for one-time use. The **Report Design** settings appear when you choose this option. Note that this template will not replace the template defined under **Resources > Reports**.
     Refer to Designing a Report Template for the steps to design the **Cover Page** and **Table of Contents**.
6. Click **Generate** to generate the report.
7. Click **View** to download the report to the local disk.

Emailing Search Results

You must first configure email settings under **Admin > Settings > System > Email**.

With the search result displayed in **Analytics** tab, complete these steps to email search results:

1. Go to the **Actions** drop-down list and select **Email Result**.
2. Enter the receiver email address in the To field.
3. Enter the **Subject** of the email.
4. Enter any **Description** about the email.
5. Enter any **User Notes** about the search results (optional).
6. Choose the **Output Format** as **PDF**, **RTF**, or **CSV**.
7. Select the **Time Zone** of the data from the drop-down list.
8. Select the **Report Template** if you select **PDF** or **RTF** format:
   - **Defined**: To use the template defined for this report defined under **Resources > Reports** or use the system default template for Analytics export.

- **New**: To create a new custom report template for one-time use. The **Report Design** settings appear when you choose this option. Note that this template will not replace the template defined under **Resources > Reports**.
  Refer to Designing a Report Template for the steps to design the **Cover Page** and **Table of Contents**.

9. Click **Send**.

Creating a Rule

With the search result displayed in Analytics, follow the steps below to create a rule based on this Search. *Note that your Search condition must contain at least one Filter condition and at at least one Filter condition containing Event Type, else Rule creation will fail.* A Rule requires these restrictions for efficient evaluation in the streaming mode.

1. From the **Actions** drop-down list, select **Create Rule**.
2. A rule template is automatically created by copying over important Search parameters:
   a. Rule Sub-pattern Filters contain Search Filter conditions
   b. Rule Sub-pattern Group By contain Search Display conditions
   c. Rule Aggregate Conditions are set to COUNT(Matched Events) >= 1. **You may want to modify this threshold.**
3. To complete the rule creation, set the following Rule attributes as appropriate:
   a. In **Step 1 > General**, specify
      i. Rule Name
      ii. Rule Description
      iii. Data Source
      iv. Detection technology
      v. Remediation Note
   b. In **Step 2 > Define Conditions** – Check the threshold specified by Aggregate Condition Value
   c. In **Step 3 > Define Action**, specify
      i. Severity
      ii. Category
      iii. MITRE Technique
      iv. Exception
      v. Watch List
      vi. Click **Save**.
4. Click **Save**. Your new rule will be saved to **Resources > Rules > Ungrouped** folder as a User defined rule and will be in an **Inactive state**. Before you activate the rule, you should test it. You can also move this rule to any folder of your choice.

Saving Search Filter and Display Conditions

You can save the Filter Conditions and Display Conditions and re-use them in another search.

To save a Search Filter:

1. Click the **Edit Filters and Time Range...** edit box.
2. Click **Save**.
3. Enter the name of current Filter Condition.
4. Click **Save** again.

To load a previously saved Search Filter:

1. Click the **Edit Filters and Time Range...** edit box.
2. Click **Load** and choose a Filter Condition from the list.
3. Click **Load**.

To save a Display Condition:

1. Click the **Group By and Display Fields** edit box.
2. Click **Save**.
3. Enter the name of current Display Field.
4. Click **Save** again.

To load a previously saved Search Filter:

1. Click the **Group By and Display Fields** edit box.
2. Click **Load** and choose a Display Field from the list.
3. Click **Load**.

Executing a FortiSOAR Playbook

FortiSIEM allows you to execute existing FortiSOAR Playbooks on an Search Result. To execute a Playbook on an event, take the following steps.

1. From the Analytics page, run an *unaggregated Search with Raw Message as a Column*.
2. Select a row and then click **Execute Playbook**.
3. From the **Execute Playbook** window, take the following steps.
   a. From the **Folders** column, expand any Playbook folder to view its content.
   b. From the **Items** column, select the Playbook you wish to execute and click **>**. The Playbook will appear in the **Selections** column. You may also search for Playbooks by using the Items **Search...** field.
   If you wish to remove a Playbook from the **Selections** column, select the Playbook you wish to remove and click **<**.
   c. When ready to execute your Playbook, click **Execute**. The **Playbook Execution Result** window appears. This window provides a summary of result. Clicking **Details** will display additional

information. Click on **View Output** to view any information related on a specific Playbook topic (Summary, Details, a specific attribute if applicable).

d. When done, click **Close**.

Running a FortiSOAR Connector

FortiSIEM allows you to execute existing FortiSOAR Connectors on an Search Result. To execute a Playbook on an event, take the following steps.

1. From the **Analytics** page, run a Search.
2. Click **Run Connector**.
3. From the **Run Connector** window, take the following steps.
   a. From the **Folders** column, select the Connector you want to run. When a Connector is selected, a list of available actions for that Connector will auto-populate under the **Items** column.
   b. From the **Items** column, select the desired Connector action and click **>** to add it to the **Selections** column. A **Select Connector Parameters** section may appear that is specific to the FortiSOAR Connector, if additional parameter information is needed. The parameters that appear will vary per Connector and specification type.
   Note: If you wish to remove a Connector action from the **Selections** column, select the Connector action you wish to remove and click **<**.
   c. If the **Select Connector Parameters** section appears based on the Connector action selected, populate the Connector parameters required to run the Connector action. Refer to FortiSOAR documentation for a given Connector for information regarding requirements.
   Note: The first parameter on nearly all Connectors is the Connector Config, which is essentially a descriptive name for a credential set for a given application, service, or device on FortiSOAR for that Connector type.
   An example is the Fortinet FortiGate Connector. Each Connector configuration is an binding of credential (API key) to a particular firewall. When you select this Connector configuration, the action will be executed on that firewall.
   d. When done, click **Execute**. FortiSIEM will call the given Connector using the parameters specified. The **Connector Result** window appears. This window provides a summary of result. Clicking **Details** will display additional information. Click on **View Output** to view any information related on a specific Connector topic (Summary, Details, a specific attribute if applicable).
   e. When done, click **Close**.

Invoking FortiAI

If you see a suspicious Event during Analytics Search, you can ask FortiAI to analyze this log and suggest remediation action. To do this, take the following steps.

1. Create a Search with **Raw Event Log** as a field.
2. Select the row column; hover over the **Raw Event Log** column and select **FortiAI** from the ▼drop-down.
3. In the FortiAI popup dialog, you will see that FortiSIEM is about to send this question to OpenAI – *"Can you analyze this log and tell me what action should I take? <Raw Message>"*
4. Before sending, you can click the View Anonymized Question (👁) button to see anonymized version that FortiSIEM is going to send to OpenAI.
5. Click the Send ( ) icon to send this question.
6. The response from OpenAI will be displayed in FortiAI popup.

Example of Anonymization

Original Raw Event

```
"Mon May 14 14:52:53 2012 172.16.10.9 AccelOps-WinLog-WMI [Category]="12810"
[CategoryString]="Filtering Platform Connection" [ComputerName]="WIN-RAQBSNW8OVY"
[Data]="NULL" [EventCode]="5156" [EventIdentifier]="5156" [EventType]="4"
[Logfile]="Security" [RecordNumber]="117554246" [SourceName]="Microsoft-Windows-Security-
Auditing" [TimeGenerated]="20120514215141.987139-000" [TimeWritten]="20120514215141.987139-
000" [Type]="Audit Success" [User]="" [Message]="The Windows Filtering Platform has allowed
a connection." [[Application Information]] [Process ID]="888" [Application
Name]="\device\harddiskvolume1\windows\system32\svchost.exe" [[Network Information]]
[Direction]="Inbound" [Source Address]="172.16.10.9" [Source Port]="135" [Destination
Address]="192.168.1.69" [Destination Port]="57654" [Protocol]="6" [[Filter Information]]
[Filter Run-Time ID]="0" [Layer Name]="Receive/Accept" [Layer Run-Time ID]="44""
```

Anonymized Raw Event

```
"Mon May 14 14:52:53 2012 FSM_5141732762 AccelOps-WinLog-WMI [Category]="12810"
[CategoryString]="Filtering Platform Connection" [ComputerName]="FSM_7667192459"
[Data]="NULL" [EventCode]="5156" [EventIdentifier]="5156" [EventType]="4"
[Logfile]="Security" [RecordNumber]="117554246" [SourceName]="Microsoft-Windows-Security-
Auditing" [TimeGenerated]="20120514215141.987139-000" [TimeWritten]="20120514215141.987139-
000" [Type]="Audit Success" [User]="" [Message]="FSM_3977836670" [[Application
Information]] [Process ID]="888" [Application Name]="FSM_8309774165" [[Network
Information]] [Direction]="Inbound" [Source Address]="FSM_5141732762" [Source Port]="135"
[Destination Address]="FSM_3787666401" [Destination Port]="57654" [Protocol]="6" [[Filter
Information]] [Filter Run-Time ID]="0" [Layer Name]="FSM_1396980488" [Layer Run-Time
ID]="44""
```

Note: Only certain parsed fields are anonymized.

Creating a New Case

You can create a Case in FortiSIEM if you see a suspicious Event during Analytics Search. To do this, take the following steps.

1. Create a Search with **Raw Event Log** as a field.
2. Select an event log, hover over the **Raw Event Log** column, click the ▼drop-down and select **Create Case**.
3. In the **Create Case** dialog, take the following steps.
   a. In the **Summary** field, enter a case summary.
   b. Click the **Due Date** field and use the GUI to make any changes to the Case due date.
   c. For **Assignee**, click **Select** and select the assignee for the Case, and click **OK**.
   d. From the **Case Management Policy** drop-down list, select a Case Management Policy.
   e. From the **Severity** drop-down list, choose the Case Severity.
   f. Click **Save**.
   g. Click **Close** to stay in Search page or **Jump to Cases** to go to the Case just created. Since this Case is created from an Event and does not have associated Incidents, the associated Event will show in **Evidence > Events**.

Adding to an Existing Case

If you see a suspicious Event during Analytics Search, you can add this event to an existing Case. To do this, take the following steps.

1. Create a Search with **Raw Event Log** as a field.
2. Select an event log, hover over the **Raw Event Log** column, click the ▼drop-down and select **Add to Case**.
3. In the **Add to Case** dialog, the open Cases belonging to the same Organization as the event will be presented. Choose one case and click **OK**. The raw event will be added to the selected Case.

Advanced Search

For ClickHouse based deployments, FortiSIEM allows you to perform an SQL Query from **Analytics** by clicking the **Advanced Search** tab.

A view of the Database Schema table and its attributes can be toggled on/off by clicking the Database ( ) icon.

Click the Filter Panel icon ( ) to toggle the Result Filter.

Click / to expand / reduce the **Query Results** pane.

Actions Drop-Down List options:

- **Export Results** - Export Search Results to a PDF or CSV file. See Exporting Search Resultsfor details.
- **Copy to a New Tab** - Click to copy the search results to a new tab for further modifications.
- **Save as Report** - Save results as a report. See Saving Search Results for details. **Note**: The option **Save Report Design Template** is not available for **Advanced Search**.

(Load Report/ Saved Results) options:

- To save results - See Viewing / Deleting Saved Search Results.
- To load a report - See Running a Built-in Historical Search.
  Note: **Shortcuts** is not available for **Advanced Search**.

SQL queries can be entered in the **Query Console** pane. This page also has the following functions.

- Attributes drop-down list -
- **CMDB Group Converter** - Click to create a CMDB group filter. When one is created, click **Convert & Copy** to be able to paste it in your SQL query.
- **Format** - Click to format the SQL query into a more legible and standardized ClickHouse SQL format.
- **Run** - Click to run the SQL query in the Query Console. Your result will appear in the **Query Results** pane.

Overview

Advanced Search enables users to use the full power of SQL to search FortiSIEM Event Database stored in ClickHouse. Currently only the SELECT SQL statement is available.

For full details on ClickHouse supported SQL, go here.

A video demonstration of Advanced Search is available here.

Running a Built-in Advanced Search

30+ built-in searches are provided in **Resources > Reports > Advanced Search**.

There are two ways to run an advanced search report, from the **Resources** page or from the **Analytics > Advanced Search** page.

- Running Advanced Search from Resources
- Running Advanced Search from Analytics

Running Advanced Search from Resources

From the **Resources** page.

1. From the left pane, expand **Reports > Advanced Search**.
2. Select a report, then click **Run**.
3. The **Query Console** panel displays the Search SQL. The search should be automatically running. Results appear in the **Query Results** panel.
4. To maximize the **Query Results** panel, click . To revert to the original size, click . The horizontal separation bar that appears between the **Query Console** and **Query Results** panels can be adjusted to give more space to the **Query Console** or **Query Results** panel. To manipulate the horizontal separation bar, click and hold it, then move up or down.
5. The that appears after an advanced report's name can be clicked on to display a report summary.

Running Advanced Search from Analytics

From the **Analytics > Advanced Search** page.

1. Click and the full list of available reports appears under **Reports > Advanced Search**.
2. Select a report, select , and click **Run**.
3. The **Query Console** panel displays the Search SQL. The search should be automatically running. Results appear in the **Query Results** panel.
4. To maximize the **Query Results** panel, click . To revert to the original size, click . The horizontal separation bar can be adjusted to give more space to the **Query Console** or **Query Results** panel. To manipulate the horizontal separation bar, click and hold it, then move up or down.
5. The that appears after an advanced report's name can be clicked on to display a report summary.

Creating a New Advanced Search

FortiSIEM events have the following table schema.

- Events are stored in table **fsiem.events**.
- Some frequently appearing attributes can be used *directly* in a Query. These appear in the **Database Schema** panel on the left. The schema can be toggled on/off by clicking the Database button on the left. Examples are `phRecvTime`, `phRecvHour`, etc...
- To use any of the remaining attributes in a Query, you need to choose them from the **Attributes used** drop-down.
  Note: Hover your cursor over the **Attributes used** drop-down to see currently selected attributes.
- Event attribute details is available at **Admin > Device Support > Event Attributes**. You can also add your own custom event attribute types here for use with Advanced Search. See Adding an Event Attribute for more information.

To create a Query, take the following steps.

Use an existing SQL from an Advanced Search report to help construct your query. To do so, click **> Reports > Advanced Reports**, select an Advanced Search report, select , then **Report Summary**. In the **Report Summary** windows, the SQL Query will appear under **SQL Query**, which you can select and copy, then paste in the **Query Console** panel.

1. Navigate to **Analytics > Advanced Search > Query Console**.
2. Write your query in the **Query Console** panel. You can also paste a query into this area from another editor. While writing your Query, contextual help is provided.
   A sample query is:
   `SELECT eventType, COUNT(*) FROM fsiem.events GROUP BY eventType ORDER BY COUNT(*) desc LIMIT 10`
3. Click **Format** to make the query more readable and also to catch any SQL syntax errors. If there are no errors then from the earlier example, the formatted query would appear as:

```
SELECT
    eventType,
    COUNT(*)
FROM fsiem.events
GROUP BY eventType
ORDER BY COUNT(*) DESC
LIMIT 10
```

4. Click **Run** to execute the query. The results will appear in the bottom **Query Results** pane. To view additional results, use the >, >|, <, and |< buttons.
5. You can see the distribution of the column values by clicking the Result Filter button. This works in the same way as Regular Search.
6. You can create a new Query in a different tab by clicking .
   Note: A maximum of ten tabs is allowed.

7. You can clear the Query area by clicking . You can copy the Query to a Clipboard by clicking .
8. To add an event attribute not explicitly present in the **Database Schema** panel (e.g. `destProto`), select the attribute from the **Attributes used** drop down and then use it in the query, e.g.

```
SELECT
    eventType,
    destProto,
    COUNT(*)
FROM fsiem.events
GROUP BY
    eventType,
    destProto
ORDER BY COUNT(*) DESC
LIMIT 10
```

If you see "Missing Exception: Missing columns: <*attribute*>..." in **Query Results** after running a query, it's likely you missed selecting that attribute from the **Attributes used** list.

9. To add a CMDB Group in the Query (e.g. `reptDevIpAddr IN Firewall group`):
   a. Point the cursor to where the condition is to be added. This is typically inside a `WHERE` clause.
   b. Click **CMDB Group Converter**.
   c. In the CMDB Group Converter window, take the following steps.
      i. For **Attribute**, select **Reporting IP**.
      ii. For **Operator**, select **IN**.
      iii. For **Value**, select **Devices > Network Device > Firewall** by clicking on **Select from CMDB**, then from **Folders**, navigate to **Devices > Network Device > Firewall**, click **>>**, then click **OK**.
      iv. Click **Convert & Copy**. The expression will be copied to Clipboard.
   d. Return to where the cursor was pointing in the **Query Console** panel. Paste the Clipboard entry. Using our earlier example, we would insert a line and enter `WHERE` after `FROM fsiem.events` before pasting the Clipboard entry. This will add the equivalent of "reptDevIpAddr IN Firewall group" using ClickHouse dictionary functions. See https://clickhouse.com/docs/en/sql-reference/functions/ext-dict-functions for details. The query will look like the following.
   e.

```
SELECT eventType,destProto,COUNT(*)
FROM fsiem.events
WHERE (dictHas('fsiem.dict_cmdb_group', (phCustId, toString
(fsiem.events.reptDevIpAddr),'PH_SYS_DEVICE_FIREWALL')) OR dictHas('fsiem.dict_
cmdb_group', (toUInt32(0), toString(fsiem.events.reptDevIpAddr),'PH_SYS_DEVICE_
FIREWALL')) OR dictHas('fsiem.dict_cmdb_group', (phCustId, toString
(fsiem.events.reptDevIpAddr),'PH_SYS_DEVICE_FIREWALL:IntfIP')) OR dictHas
('fsiem.dict_cmdb_group', (toUInt32(0), toString(fsiem.events.reptDevIpAddr),'PH_
SYS_DEVICE_FIREWALL:IntfIP')))
GROUP BY eventType,destProto
ORDER BY COUNT(*) DESC
```

General Usability Notes

- Use single quote only for string value comparisons, e.g. reptDevName = 'WIN-ABC'
- Use backtick ` for Alias, e.g. reptDevName AS `Reporting Device` or double quote ", e.g. reptDevName AS "Reporting Device"

Query Performance Considerations

Follow the guidelines in ClickHouse Query Optimization Guidelines.

Specifically:

1. Always add time constraints in the WHERE clause, e.g. last 1 hour amounts to phRecvTime > (now() - 3600).
2. Always run with a LIMIT to see if the query is working as expected.
3. Use the narrowest possible Filter Condition by always including ClickHouse Primary and Data skipping indices.

Fixing Query Errors

If you hit an error while formatting or running a SQL search, then you can either manually fix the query or use FortiAI to fix it.

Fixing SQL Query Syntax Errors with FortiAI

Suppose you created a SQL search but there are some errors while you **Format** or **Run** it. You can use the power of Generative AI to fix the errors. This requires that you have ChatGPT API Key configured in **Admin > Settings > Analytics > ML/AI**.

Once the ClickHouse Query Engine returns an error from either a **Format** or **Run** operation, the **Fix with FortiAI** button will be clickable. When clicked, the following occurs.

1. A new **Ask FortiAI** window opens next to **Query Console**. FortiAI interaction with ChatGPT will appear in this window.
2. FortiSIEM will send a request to ChatGPT to fix the SQL Query error.
3. ChatGPT will first respond with "I am trying to fix the Query". Then it may provide an explanation of the error and a fixed SQL Query.
4. If you want to directly run the fixed query returned by ChatGPT, then go to the **Action** drop-down on the top right corner of the ChatGPT response and choose **Replace Original Query**. The query will replace your query. Check the fix for accuracy and then click **Run**.
5. You also have the option to Copy the fixed query to Clipboard by choosing this option **Copy Query to Clipboard** under the **Action** drop-down. Then you can open a new tab and paste the query from your Clipboard and click **Run**.
6. The result will show in the **Query Results** pane below.

Miscellaneous Advanced Search Operations

- Saving Advanced Search Definition and/or Results
- Viewing Saved Advanced Search Results
- Exporting Search Results
- Importing and Exporting Advanced Search Definition

Saving Advanced Search Definition and/or Results

To save a Search definition or results, take the following steps.

1. Click the **Actions** drop-down list, and click **Save**.
   - To Save a Search definition:
     1. Under the **Report Name** field, edit the report name and description if needed.
     2. Check the **Save Definition** checkbox.
     3. Under **Save To**, choose the folder where the definition is to be saved.
     4. Click **OK**.
   - To Save Search results:
     1. Under the **Report Name** field, edit the report name and description if needed.
     2. Check the **Save Results** checkbox, and make any changes to the number of hours/days if needed.
     3. Click **OK**.

Viewing Saved Advanced Search Results

To view previously saved Advanced Search results, take the following steps.

1. Click .
2. Click **Saved Results**.
3. Click the saved result, click , then click **View Results**.
4. The **Query Console** panel shows the Search SQL. The results appear in the **Query Results** panel.

Exporting Search Results

To export search results, take the following steps.

1. Click the **Actions** drop-down list, and click **Export Results**.
2. In the Export Report window, take the following steps.
   a. (Optional) In the **User Notes** field, enter any information you wish to include about the search results.
   b. From the **Output Format** selection, choose **PDF** or **CSV**.
   c. Use the **Time Zone** drop-down options to configure the time and date format when the exported results were generated.
   d. Click **Generate**.
   e. Click **View** and your results will be downloaded.

Importing and Exporting Advanced Search Definition

Importing and exporting search definitions can be done from **Resources > Reports > Advanced Search**.

1. Navigate to **Resources > Reports > Advanced Search**.
   - To export:
     1. Select the report you want to export the definition of.
     2. Click the **More** drop-down list and select **Export**.
     3. An XML file will be generated and downloaded to your local workstation.

   - To import, you must have saved the report in an XML file in your local workstation.
     1. Click the **More** drop-down list and select **Import**.
     2. Click **Choose File**, and select the XML file.
     3. Click **Import** and the report will appear in the **Reports > Advanced Search** folder.

Advanced Search Examples

This section offers some simple examples to demonstrate the basic SQL building blocks. These examples are intended to be followed in sequential order.

- Example 1 - Query Top 10 Reporting Devices by Event Count in Last 1 Hour
- Example 2 - Add the Reporting Vendor and Model of the Reporting Devices and the Last Time that They Reported an Event
- Example 3 - Show the Reporting IP and the Top Event Types for these Devices and only Include External Events
- Example 4 - Show the External Events from a Specific Reporting Device with a Specific IP
- Example 5 - Show Information from a Specific CMBD Group
- Example 6 - Show Reporting Devices Reporting External Events Today that were not Reporting External Events Yesterday
- Example 7 - Only Return Top 5 Event Types for Each Reporting Device

Example 1 - Query Top 10 Reporting Devices by Event Count in Last 1 Hour

Lets start with this query: *Top 10 Reporting Devices by Event Count in last 1 hour*.

```
SELECT
    reptDevName AS `Reporting Device`,
    COUNT(*) AS `Total Events`
FROM fsiem.events
WHERE phRecvTime > (now() - 3600) AND eventParsedOk=1
GROUP BY reptDevName
ORDER BY COUNT(*) DESC
LIMIT 10
```

Example 2 - Add the Reporting Vendor and Model of the Reporting Devices and the Last Time that They Reported an Event

Suppose you want to see *the reporting vendor and model of the reporting devices and the last time that they reported an event*. Then run the following query:

```
SELECT
    reptDevName AS `Reporting Device`,
    reptVendor AS Vendor,
    reptModel AS Model,
    COUNT(*) AS `Total Events`,
    MAX(phRecvTime) AS `Last Reporting Time`
FROM fsiem.events
WHERE phRecvTime > (now() - 3600) AND eventParsedOk=1
GROUP BY
    reptDevName,
    reptVendor,
    reptModel
ORDER BY COUNT(*) DESC
LIMIT 10
```

Example 3 - Show the Reporting IP and the Top Event Types for these Devices and only Include External Events

Suppose you want to see *the Reporting IP and the Top Event Types for these devices and only include external events*. Then run the following query:

```
SELECT
    reptDevName AS `Reporting Device`,
    reptDevIpAddrV4 AS `Reporting IP`,
    eventType AS `Event Type`,
    reptVendor AS Vendor,
    reptModel AS Model,
    COUNT(*) AS `Total Events`,
    MAX(phRecvTime) AS `Last Reporting Time`
FROM fsiem.events
WHERE (phRecvTime > (now() - 3600)) AND eventParsedOk=1  AND (phEventCategory IN (0, 4))
GROUP BY
    reptDevName,
    reptDevIpAddrV4,
    eventType,
    reptVendor,
    reptModel
ORDER BY COUNT(*) DESC
LIMIT 10
```

Example 4 - Show the External Events from a Specific Reporting Device with a Specific IP

Suppose you want to *choose a specific reporting device named WIN-ABC with Reporting IP as 10.1.1.1*. Then run the following query:

```
SELECT
    reptDevName AS `Reporting Device`,
    reptDevIpAddrV4 AS `Reporting IP`,
    eventType AS `Event Type`,
    reptVendor AS Vendor,
    reptModel AS Model,
    COUNT(*) AS `Total Events`,
    MAX(phRecvTime) AS `Last Reporting Time`
FROM fsiem.events
WHERE (phRecvTime > (now() - 3600)) AND eventParsedOk=1 AND (phEventCategory IN (0, 4)) AND
((reptDevName = 'WIN-ABC') OR (reptDevIpAddrV4 = '10.1.1.1'))
GROUP BY
    reptDevName,
    reptDevIpAddrV4,
    eventType,
    reptVendor,
    reptModel,
ORDER BY COUNT(*) DESC
LIMIT 10
```

Example 5 - Show Information from a Specific CMBD Group

Instead of focusing on a single device, suppose you want to focus on *devices in CMDB Group: Devices > Server > Windows*. Then use the **CMDB Group Converter** to generate the query.

To create this CMDB group, click on **CMDB Group Converter**, and in the CMDB Group Converter window, take the following steps.

1. Set **Attribute** as **Reporting IP**.
2. Set **Operator** as **IN**.
3. Set **Value** as **Group: Windows** by taking the following steps.
   a. Click **Value** and click **Select from CMDB**.
   b. From **Folders**, navigate to **Devices > Server > Windows**, and ensure **Windows** is selected.
   c. Click **>>** to create group, then **OK**.
   d. Click **Convert & Copy**.

```
SELECT
    reptDevName AS `Reporting Device`,
    reptDevIpAddrV4 AS `Reporting IP`,
    eventType AS `Event Type`,
    reptVendor AS Vendor,
    reptModel AS Model,
    COUNT(*) AS `Total Events`,
    MAX(phRecvTime) AS `Last Reporting Time`
FROM fsiem.events
WHERE (phRecvTime > (now() - 3600)) AND eventParsedOk=1 AND (phEventCategory IN (0, 4)) AND
(dictHas('fsiem.dict_cmdb_group', (phCustId, toString(fsiem.events.reptDevIpAddr), 'PH_SYS_
DEVICE_WINDOWS_SERVER')) OR dictHas('fsiem.dict_cmdb_group', (toUInt32(0), toString
(fsiem.events.reptDevIpAddr), 'PH_SYS_DEVICE_WINDOWS_SERVER')) OR dictHas('fsiem.dict_cmdb_
group', (phCustId, toString(fsiem.events.reptDevIpAddr), 'PH_SYS_DEVICE_WINDOWS_
SERVER:IntfIP')) OR dictHas('fsiem.dict_cmdb_group', (toUInt32(0), toString
(fsiem.events.reptDevIpAddr), 'PH_SYS_DEVICE_WINDOWS_SERVER:IntfIP')))
GROUP BY
    reptDevName,
    reptDevIpAddrV4,
    eventType,
    reptVendor,
    reptModel
ORDER BY COUNT(*) DESC
LIMIT 10
```

Example 6 - Show Reporting Devices Reporting External Events Today that were not Reporting External Events Yesterday

Suppose you want to see *the reporting devices that are reporting external events today but were not reporting yesterday*. This uses the SQL SubQuery capability. Then run the following query:

```
WITH reporting_devices_last_1_day AS
    (
        SELECT DISTINCT reptDevName
        FROM fsiem.events
        WHERE (phRecvTime >= toStartOfDay(now() - (1 * 86400))) AND eventParsedOk=1 AND
(phRecvTime < toStartOfDay(now())) AND (phEventCategory IN (0, 4))
    )
SELECT DISTINCT
    reptDevName AS `Reporting Device`,
    reptDevIpAddrV4 AS `Reporting IP`,
    reptVendor AS Vendor,
    reptModel AS Model
FROM fsiem.events
WHERE (phRecvTime >= toStartOfDay(now())) AND eventParsedOk=1 AND (phEventCategory IN (0,
```

```
4)) AND (reptDevName NOT IN (
    SELECT reptDevName
    FROM reporting_devices_last_1_day
))
ORDER BY reptDevName ASC
```

Example 7 - Only Return Top 5 Event Types for Each Reporting Device

Lets go back to Example 3, but *only return Top 5 event types for each reporting device*. This is achieved via the SQL Window function (For more information, see https://clickhouse.com/docs/en/sql-reference/window-functions and https://www.postgresql.org/docs/current/tutorial-window.html).

```
WITH subquery AS
    (
        SELECT
            reptDevName,
            eventType,
            count() AS count,
            rank() OVER (PARTITION BY reptDevName ORDER BY count DESC) AS rank
        FROM fsiem.events
        WHERE phRecvTime > (now() - 3600) AND eventParsedOk=1
        GROUP BY ALL
    )
SELECT
    reptDevName AS `Reporting Device`,
    eventType AS `Event Type`,
    count
FROM subquery
WHERE rank <= 5
```

Machine Learning

The following sections provide information and procedures for Machine Learning:

- Overview
- Anomaly Detection
- Classification
- Clustering
- Forecasting
- Regression

Overview

FortiSIEM 7.0.0 introduces Machine Learning, which allows you to run various Machine Learning tasks on data collected by FortiSIEM.

Machine Learning Job Types

The following Machine Learning Tasks are supported:

- **Anomaly Detection** - The objective of an Anomaly Detection task is to learn what is normal in a dataset, and create an alert if the new values deviate from the normal dataset, by user specified threshold. Learning is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Classification** – The objective of a Classification task to learn how to assign labels to items based on various fields in a dataset and then assign a label to a new item based on current values. This requires labels to be present in the dataset. Labels can be binary e.g. malware/not malware, spam/not-spam, or can belong to more than 2 classes as well. Learning the label assignment is done during the Training phase and assigning labels to new data is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Clustering** - The objective of a Clustering task is to group similar items based on a set of fields in a dataset, and then create an alert if an item belongs to a different group based on current values. Learning the groups is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Forecasting** – The objective of a Forecasting task is to learn a time based trend of a field in a dataset and then predict future values of that field. Learning the time based trend is done during the Training phase and future prediction is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.
- **Regression** - The objective of a Regression task is to build a model for predicting a Target field based on other fields in a dataset, and then create an alert if the new values of the Target field exceeds the predicted value, by user specified threshold. Building the prediction model is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

Running Modes and Algorithms

The following Machine Learning running modes are supported:

- **Local** – In this mode, both Training and Inference phases run on the Supervisor and Worker cluster. During the Training phase, the user has to choose the Machine Learning Algorithm and its optimal parameters.
- **Local Auto** – In this mode, both Training and Inference phases run on the Supervisor and Worker cluster. FortiSIEM picks the best Machine Learning Algorithm with a tuned parameter set. In contrast to Local mode, the Training phase in Local Auto mode takes a significantly longer time to complete, since many algorithms are evaluated and the performance of each algorithm is optimized by tuning the parameter set.

- **AWS** - In this mode, both the Training and Inference stages take place on AWS. It is important to note that for regression, BinaryClassification, and MulticlassClassification, the algorithm parameters can be auto-tuned on AWS and the user can also define the Object Metric for Hyperparameter Tuning Job. However, for Anomaly Detection and Clustering, the user is required to configure the algorithm parameters themselves.
- **AWS Auto** - In this mode, Amazon SageMaker Autopilot helps you automatically build, train, and tune the best machine learning models without manual model selection and tuning. Although the training time might be longer (2 – 3 hours), using Autopilot can still be suitable when facing a dataset with a large number of features and complexity, Autopilot can automatically perform feature engineering and select the best model, helping you achieve good results in a short amount of time.

The following table shows the supported Machine Learning algorithms for each Task type and running mode.

Task	Running Mode	Supported Machine Learning Algorithms
Anomaly Detection	Local	Local Outlier Factor, Elliptic Envelope, Isolation Forest, Statistical Deviation, Bipartite Edge Anomaly Detection (Proprietary)
	AWS	Random Cut Forest
Classification	Local	Logistic Regression, Decision Tree Classifier, Random Forest Classifier, SGDClassifier, Support Vector Classifier (SVC)
	Local Auto	Decision Tree Classifier, Random Forest Classifier, SGDClassifier, Support Vector Classifier (SVC)
Binary Classification	AWS	Linear Learner
	AWS Auto	See https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html
Multiclass Classification	AWS	Linear Learner
	AWS Auto	See https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html
Clustering	Local	KMeans, GMeans, DBScan, BIRCH, Spectral Clustering
	Local Auto	BIRCH, DBSscan, KMeans
	AWS	KMeans
Forecasting	Local	ARIMA, State Space Dynamic factor MQ
Regression	Local	Linear Regression, Decision Tree Regressor, Random Forest Regressor, SGDRegressor, Support Vector Regression (SVR)
	Local Auto	Decision Tree Regressor, Random Forest Regressor, SGDRegressor, Support Vector Regression (SVR)
	AWS	Linear Learner
	AWS Auto	See https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html

A Machine Learning Job

The concept of a Machine Learning Job is introduced. It consists of the following attributes:

- **Job Id** – The unique ID for this job, assigned by FortiSIEM.
- **Scope** – System defined or User defined. System defined Jobs are provided by FortiSIEM. User defined jobs are created by the user. Note that System defined jobs are simply templates and must be trained.
- **Name** – Name of the job.
- **Description** – Description of the job.
- **Task** – One of the following Machine Learning Task Categories: Anomaly Detection, Regression, Clustering, Forecasting, Classification.
- **Machine Learning Algorithm** – A relevant algorithm for the Machine Learning Task.
- **Report** – The FortiSIEM Report that provides the data for training and inference.
- **Report Time Window** – The time window for which the report must be run. In other words, the fataset contains data during this Report Time Window.
- **Target** – The fields in the FortiSIEM Report that should be used as the target for the Machine Learning Task.
- **Features** – The fields in the FortiSIEM Report that should be used as the features for the Machine Learning Task.
- **Organization** (For FortiSIEM Service Provider deployments only) – The Organization for which the Report must be run. Currently the supported values are – All Organization data combined or a specific Organization at a time. In other words, if you want to run the machine learning task for 2 Organizations, then 2 separate Machine Learning jobs must be created.
- **Inference Schedule** – The frequency at which inference must be done. The purpose of Inference is to detect deviations from the model built during Training phase or to create future data for Forecasting.
- **Re-training Schedule** – The frequency at which training must be repeated. The purpose of retraining is to capture new patterns in the data.
- **Action** – Specifies the action to be taken after Inference is completed: whether to create an Alert or send an email containing the anomalies found.

System defined Machine Learning Job templates are provided in **Resources > Machine Learning Jobs**. Note that these are templates and cannot be run like Rules and Reports, since they are missing the Machine Learning model. A System defined Machine Learning Job does not set the following attributes:

1. Report Time Window
2. Organization
3. Inference Schedule
4. Re-training schedule
5. Action

These attributes must be provided by the user while training and scheduling a machine learning job.

Running a System Defined Machine Learning Job

To build a model and schedule a System defined job, the user must take the following steps:

1. Go to **Analytics > Machine Learning** and select the job.
2. Create an input dataset by running the report
   a. Choose Report Time Window
   b. Chose Organization for FortiSIEM Service Provider deployments
3. Train the dataset from **Analytics >Train**. A model will be built. You can tune the tune the algorithm parameters and Train again.
4. Once the model is ready, you can schedule the job to run for Inference from **Analytics >Schedule**.
5. A new job id will be assigned and will show in **Resources > Machine Learning Jobs** as an User defined job.
6. As part of Inference action, the alert will show up in Incidents or email will be sent.
7. You can edit the Inference and Re-training schedules by editing a job in **Resources > Machine Learning Jobs**.

Creating a Machine Learning Job From Scratch

A Machine Learning job can also be created from scratch. To do this, the user must take the following steps:

1. Navigate to **Analytics > Machine Learning** and Select a Report from the **Reports > Machine Learning Reports** folder. If the report is not present in that folder, then you can pre-built a report from **Analytics > Search** and save it in **Reports > Machine Learning Reports** before proceeding.
2. Create an input dataset by running the report
   a. Choose Report Time Window
   b. Chose Organization for FortiSIEM Service Provider deployments
3. Train the dataset from **Analytics >Train**.
   a. Choose **Run Mode**.
   b. Choose **Task**.
   c. Choose **Algorithm** and tune the parameters if needed.
   d. Choose **Training factor**.
   e. Click **Train**. You can tune the tune the algorithm parameters and Train again.
4. Once the model is ready, you can schedule the job to run for Inference from **Analytics >Schedule**.
5. A new job id will be assigned and will show in **Resources > Machine Learning Jobs** as an User defined job.
6. As part of Inference action, the alert will show up in Incidents or email will be sent.
7. You can edit the Inference and Re-training schedules by editing a job in **Resources > Machine Learning Jobs**.

Preparing Data with ClickHouse

For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Anomaly Detection

The objective of an Anomaly Detection Task is to learn what is normal in a dataset, and create an alert if the new values deviate from the normal dataset, by user specified threshold. Learning is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

- Anomaly Detection Algorithms for Local Mode
- Running Anomaly Detection Local Mode
- Anomaly Detection Algorithms for AWS Mode
- Running Anomaly Detection AWS Mode

Anomaly Detection Algorithms for Local Mode

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

Bipartite Graph Edge Anomaly Detection Algorithm

This is a proprietary machine learning algorithm that tries to detection login anomalies by learning the login patterns and forming dynamic user peer groups. A bipartite graph is a graph where the sets of nodes can be split into two disjoint sets such that there are no edges between the nodes within the same set. An example is Users and Workstations where the edge between a user and a Workstation represents a login, and the edge weight can be the number of logins. The anomaly detection algorithm works as follows. During the training phase, a similarity score between a user/workstation and another user/workstation is calculated. The principle behind similarity score calculation is as follows:

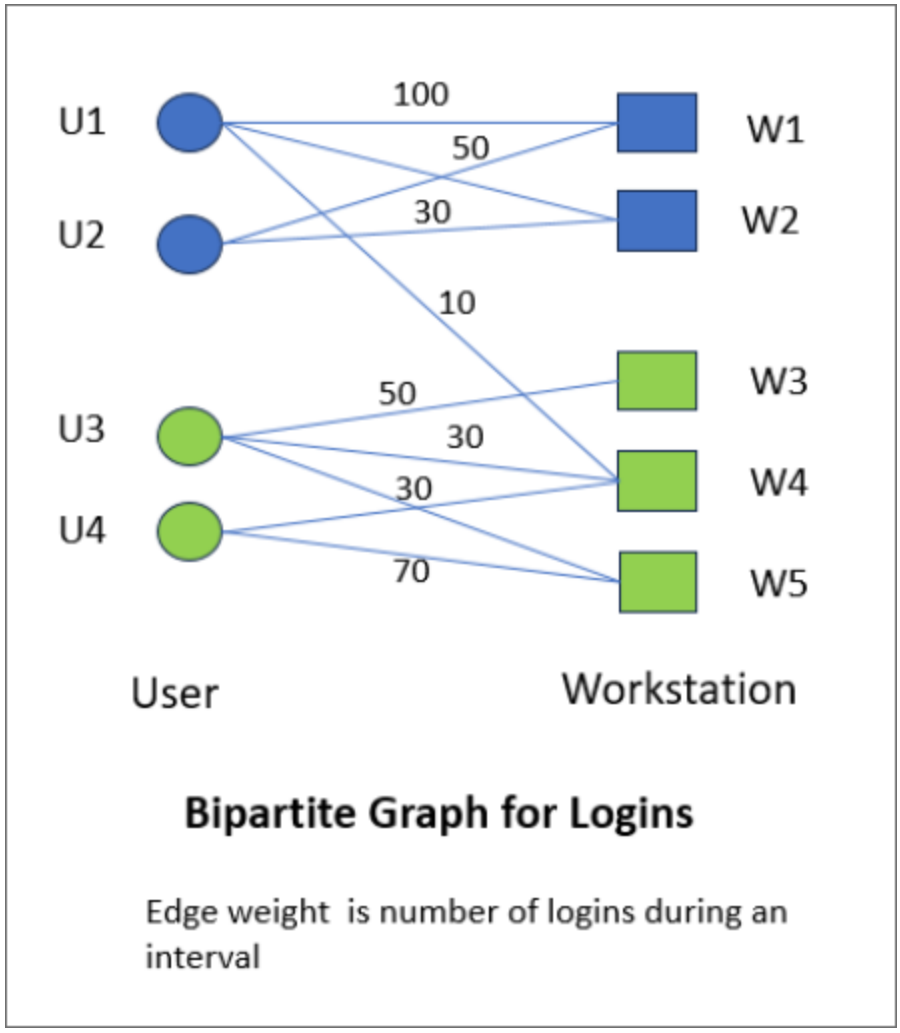
- The similarity score between a user and a workstation is high if the user accesses that workstation.
- The similarity score between two users is high if they access similar workstations.
- The similarity score between two workstations is high if they are accessed by a common set of users.

During testing and inference phases, a login from user (A) to a workstation (B) is considered anomalous if the similarity score between user A and the other users that typically access workstation B is lower than a user defined threshold. More specifically:

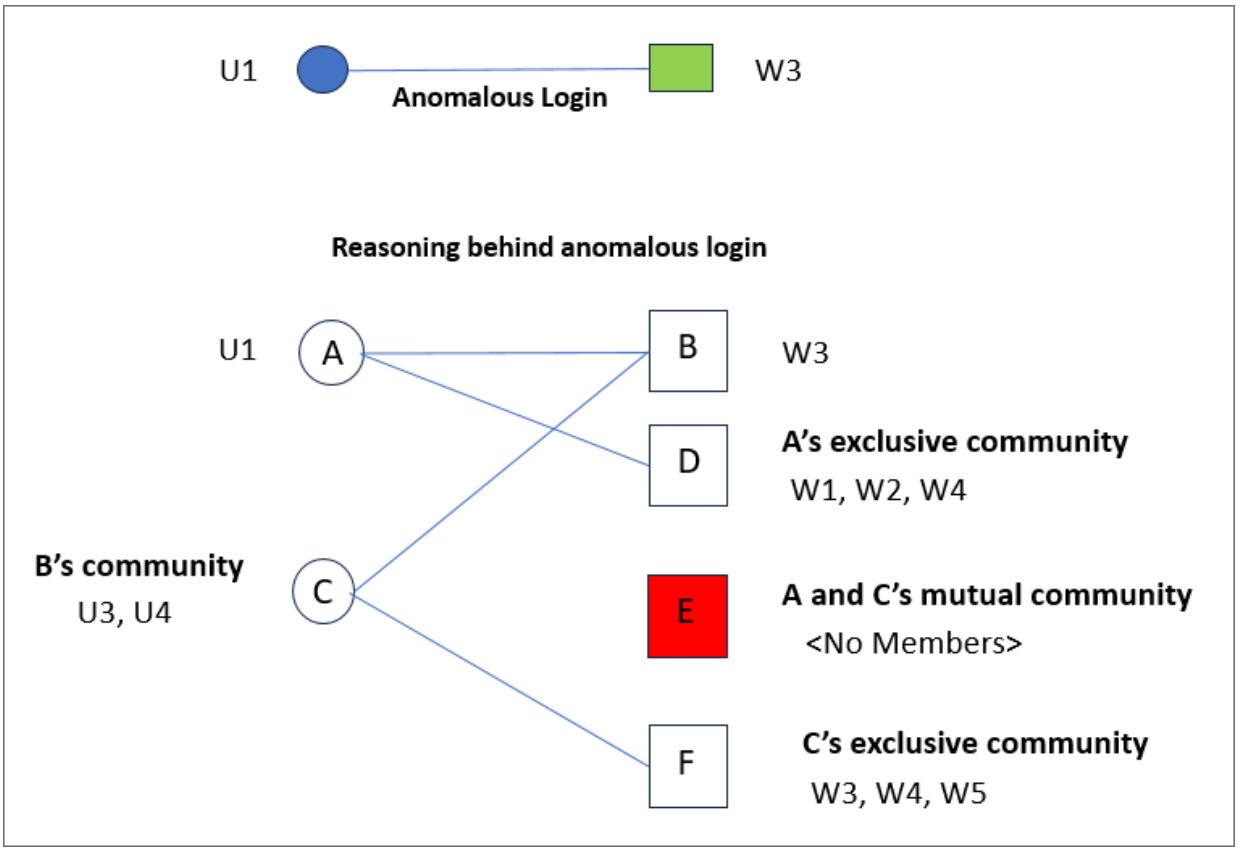
- C: The set of users that access workstation B during training phase. This is B's community.
- E: The set of workstations that are accessed by both A and C during training phase. This is A and C's mutual community.
- D: The set of workstations that are accessed by only A during training phase. This is A's exclusive community.
- F: The set of workstations that are accessed by only C during training phase. This is C's exclusive community.

For an anomaly to occur, the set of workstations E should be far fewer compared to set of Workstations D (A's exclusive community) and F (C's exclusive community). If this is not the case, then consider reducing the anomaly threshold.

As an example, consider the following login scenario between users U1, U2, U3, U4 and Workstations W1, W2, W3, W4. The login is modeled as a weighted Bipartite graph as shown below.



A login from user U1 to Workstation W3 is considered an anomaly because user U1 and W3's user community (namely U3 and U4) do not access common workstations.



There are 3 parameters for this algorithm:

- **Threshold** : Scores lower than this threshold is considered anomalous.
- **Max node degree**: Nodes with degree higher than this value will be ignored. In the User and Workstation case.
  - Users that access more than max node degree workstations will be ignored.
  - Workstations that are accessed by more than max node degree users will be ignored.
- **Convergence bound**: Bipartite Edge Anomaly Algorithm stops if the change in reward matrix is lower than this value. This is an internal parameter.

The following groups of users/workstations are eliminated during testing and inference phases, and they do not raise incidents:

1. Users that access many workstations (e.g., Domain Admins in Microsoft Active Directory environments).
2. Workstations that are accessed by many users (e.g., Microsoft Active Directory)
3. Users or Workstations that were never seen during the training phase and hence not part of the model. A periodic retraining would resolve this issue.

Elliptic Envelope Algorithm

An *unsupervised* anomaly detection algorithm which constructs an ellipsoid around the center of the data points. If a data point falls outside the Ellipsoid, then it is considered as an anomaly. This is suitable

for Gaussian distributed data. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.covariance.EllipticEnvelope.html

Isolation Forest Algorithm

An *unsupervised* anomaly detection algorithm that builds a random tree by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of that feature. If a data point has a small path from the root of the tree, then it is considered as an anomaly. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.IsolationForest.html

Local Outlier Factor Algorithm

An *unsupervised* anomaly detection algorithm which computes the local density deviation of a data point with respect to its neighbors. If a data point has substantially lower density than their neighbors, then it is considered as an anomaly. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.LocalOutlierFactor.html

Statistical Deviation Algorithm

An *unsupervised* anomaly detection algorithm based on mean, median, standard deviation and absolute median deviation. A data point is considered an anomaly if the difference between current value and sample mean (or sample median) in a Window is more than a user specified multiplier times the standard deviation (respectively absolute median deviation) over the same window. This is a generalization of the Z-score based methods. The parameters for this algorithm are:

- *Mode*: Std (meaning Standard Deviation) or Median Absolute (meaning MedAbs)
- *Multiplier*: It will be used to calculate the lower/upper bound
- *Window*: Length of sliding window for calculating mean, median and standard deviation

Specially,

- For **Mode=Std**: a data point is anomalous if the absolute difference between current value and sample mean in the Window is more than Multiplier times the Standard Deviation over the same Window
- For **Mode= MedAbs**: a data point is anomalous if the absolute difference between current value and sample median in the Window is more than Multiplier times the Median Deviation over the same Window

Gaussian Model

This unsupervised machine learning model approximates the probability distribution of an event attribute as a Gaussian distribution. A data point is considered anomalous if its occurrence probability is lower than the provided threshold. The parameters for this algorithm are:

- *prob_threshold*: A data point is anomalous if its probability density function value is less than this threshold. To reduce the number of anomalies, lower this threshold.

Gaussian Mixture Model

As a generalization of the Gaussian model, this unsupervised machine learning model approximates the probability distribution of an event attribute as N Gaussian distributions. This is useful for modeling

event attributes which has multiple peaks and valleys. A data point is considered anomalous if its occurrence probability is lower than the provided threshold. The parameters for this algorithm are:

- *prob_threshold*: A data point is anomalous if its probability density function value is less than this threshold. To reduce the number of anomalies, lower this threshold.
- *eval_method*: The evaluation method for finding the best Gaussian Mixture model approximation - AIC (Akaike Information Criterion) or BIC (Bayesian Information Criterion).

Running Anomaly Detection Local Mode

Step 1: Design

First identify the following items:

- Fields to Analyze – these fields will be considered for anomaly detection. Currently each field must be a numerical field.
- Time field – this field is required for Statistical Deviation algorithms. It is optional for other algorithms.
- A FortiSIEM Report to get this data.

Requirements

1. Report must contain one or more numerical fields to use for anomaly detection. To provide several samples, you can provide a time field. This is optional.
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be columns other than the Fields to Analyze in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Jobs** folder

c. To prepare data from a CSV file, choose **Import via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.

3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Anomaly Detection task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import Via Jobs**, then make sure the Fields to Analyze are populated correctly.
3. If you chose **Import Via Report** or **Import Via CSV File**, then
   a. Set **Run Mode** to Local
   b. Set **Task** to Anomaly Detection
   c. Choose the **Algorithm**
   d. Choose the **Fields to Analyze** from the report fields.
4. Specify a *threshold* for detecting anomalies.
   - For **Local Outlier Factor**, **Elliptic Envelope**, **Isolation Forest** algorithms, the threshold is the **Contamination** parameter. Contamination is between 0 and 1 and specifies the proportion of the data that can be considered anomalous. If Contamination is 0.1, then roughly 10% of the data will be detected as anomalous during the training phase.
   - For **Statistical Deviation** algorithm, the threshold is the Multiplier parameter:
     - For **Statistical Deviation and Mode=Std**: a data point is anomalous if the absolute difference between current value and *sample mean* in the Window is more than *Multiplier* times the *Standard Deviation* over the same *Window*.
     - For **Statistical Deviation and Mode= MedAbs**: a data point is anomalous if the absolute difference between current value and *sample median* in the Window is more than *Multiplier* times the *Median Deviation* over the same *Window*.
   - For **Bipartite Graph Edge Anomaly Detection**, scores lower than the **threshold** is considered anomalous.
   - For **Gaussian Model** and **Gaussian Mixture Model**, a data point is anomalous if its probability density function value is less than *prob_threshold* parameter.
5. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
6. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab. For Anomaly detection, results includes **Model Quality** and **Anomalies found**.

Model Quality:

The following metrics show the quality of the anomaly detection algorithm.

- **Anomalies Found**: This shows the number of anomalies in the data.
- **Normal Results**: This shows the number of normal (or non-anomalous) results.

Anomaly Detection Results:

The Anomaly Detection Results table shows which results are anomalous (*isAnomaly* = 1).

- For **Statistical Deviation**: The columns avg, stddev, lower_bound, upper_bound are added to the table.
- For **Regression Deviation**: The columns avg, stddev, lower_bound, upper_bound are added to the table
- **Anomaly Details > Trend View**: For **Statistical Deviation**, this area shows a time trend and shows where anomaly occurs.
- For **Gaussian Model** and **Gaussian Mixture Model**: The data points are plotted on the probability density function. The anomalous data points are marked red.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**. Note the important tuning parameters are

- For **Local Outlier Factor**, **Elliptic Envelope**, **Isolation Forest** algorithms, the threshold is the **Contamination** parameter.
- For **Statistical Deviation** algorithm, the threshold is the **Multiplier** parameter.
- For **Gaussian Model** and **Gaussian Mixture Model**, tune the **prob_threshold** parameter.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.

- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Anomaly Detection Algorithms for AWS Mode

In this mode, the following algorithm runs in AWS. The following algorithm is supported.

Random Cut Forest

Random Cut Forest is an *unsupervised* anomaly detection algorithm that builds a random tree by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of that feature. If a new data point changes the tree structure, then it is considered as an anomaly. The parameters for this algorithm are described here:

Running Anomaly Detection AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- Fields to Analyze – these fields will be considered for anomaly detection. Currently each field must be a numerical field.
- Time field – this field is required for Statistical Deviation algorithms. It is optional for other algorithms.
- A FortiSIEM Report to get this data.

Requirements

1. Report must contain one or more numerical fields to use for anomaly detection. To provide several samples, you can provide a time field. This is optional.

2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be columns other than the Fields to Analyze in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Jobs** folder
   c. To prepare data from a CSV file, choose **Import via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report Time Interval and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Anomaly Detection task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the Fields to Analyze are populated correctly.
3. If you chose **Import via Report** or **Import Via CSV File**, then
   a. Set **Run Mode** to AWS
   b. Set **Task** to Anomaly Detection
   c. Choose the **Algorithm**
   d. Choose the **Fields to Analyze** from the report fields.
4. Specify the parameters for Random Cut Forest.

5. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
6. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Classification

The objective of a Classification Task to learn how to assign labels to items based on various fields in the dataset and then assign a label to new item based on current values. This requires labels to be present in the dataset. Labels can be binary e.g. malware/not malware, spam/not-spam or can belong to more than 2 classes as well. Learning the label assignment is done during the Training phase and assigning labels to new data is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

- Classification Algorithms for Local Mode
- Running Classification Local Mode
- Classification Algorithms for Local Auto Mode
- Running Classification Local Auto Mode
- Classification Algorithms for AWS Mode
- Running Classification AWS Mode
- Classification Algorithms for AWS Auto Mode
- Running Classification AWS Auto Mode

Classification Algorithms for Local Mode

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

- **Decision Tree Classifier**: A *supervised* classification algorithm that uses a Decision Tree constructed using the feature variables to classify new data points. It requires a set of pre-labelled data points during the training process to construct the tree.
- **Logistic Regression**: A *supervised binary* classification algorithm that can classify data points into two classes based on sigmoid function using a set of features. It requires a set of pre-labelled data points during the training process.
- **Random Forest Classifier**: A *supervised* classification algorithm that uses Ensemble learning and Bootstrapping techniques to improve the accuracy of Decision Tree based classification algorithms. Ensemble learning uses multiple models and Bootstrapping randomly samples datasets and then averages the results of each model to improve accuracy. It requires a set of pre-labelled data points during the training process to construct the trees.
- **SGDClassifier**: A *supervised* classification algorithm that uses Stochastic Gradient Descent (SGD) update techniques for existing classifiers and is computationally efficient for large datasets. It requires a set of pre-labelled data points during the training process.
- **Support Vector Classifier**: Support Vector Classifier (SVC), also called Linear Support Vector Machine (SVM), is a *supervised* classification algorithm that separates data points using a hyperplane with specified margins (support vector). It requires a set of pre-labelled data points during the training process.

Running Classification Local Mode

Step 1: Design

First identify the following items:

- **Fields to use for Classification**: Each field must be a numerical field.
- **Class Label**: The class to which the data corresponds to.
- A **FortiSIEM Report** to get this data.

To provide several samples of the data, you can choose one of the following time attributes as a report column

- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - A Class Label
   - One or more numerical fields to use for classification

   To provide several samples, you can provide a time field. This is optional.
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.

3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Classification task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Class Label** and **Fields to use for Classification** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to Local
   b. Set **Task** to Classification
   c. Choose the **Algorithm**
   d. Choose the **Class Label** and **Fields to use for Classification** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

- **True Positives (TP)**: Correct classification for label = 0, i.e. actual = 0 and predicted = 0
- **True Negative (TN)**: Correct classification for label = 1, i.e. actual = 1 and predicted = 1
- **False Positive (FP)**: Incorrect classification for label = 0, i.e. actual = 0 and predicted = 1
- **False Negative (FN)**: Incorrect classification for label = 1, i.e. actual = 1 and predicted = 0
- **Accuracy**: Accuracy is the total number of correct classification divided by the total number of attempted classification, i.e. ((TP+TN)/(TP+TN+FP+FN)). It is between 0 and 1. A score close to 1 means accurate classification.
- **Recall**: Recall is calculated by dividing the True Positives by anything that should have been predicted as Positive. So Recall is FP/(FP+TN).
- **Precision**: Precision is calculated by dividing the True Positives by anything that was classified as a Positive. So Precision is TP/(TP+FP).
- **F1 Score**: F1 Score combines Precision and Recall into a single metric by taking their harmonic mean. F1 Score = 2 / ((1/Precision)+(1/Recall)). It ranges from 0-1, and a higher F1 score denotes a better quality classifier.
- **ROC AUC**: It measures the entire two-dimensional area underneath the entire ROC curve (think integral calculus) from (0,0) to (1,1). It tells how much the model is capable of distinguishing

between classes. Higher ROC AUC values indicate that the model is better at predicting 0 classes as 0 and 1 classes as 1.

- **Confusion Matrix**: presents TP, TN, FP and FN in a matrix

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Classification Algorithms for Local Auto Mode

In this mode, FortiSIEM picks the best algorithm from the following:

- Decision Tree Classifier
- Random Forest Classifier
- SGDClassifier
- Support Vector Classifier (SVC)

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 5 minutes. The longer this job runs, potentially better result can be generated.

Running Classification Local Auto Mode

To run, follow the Classification steps in Algorithms for Local Mode, but in Step 3, 3a, select **Run Mode** as **Local Auto**.

Classification Algorithms for AWS Mode

In this mode, the following algorithms runs in AWS. The following algorithms are supported.

- **Linear Learner Algorithms**: Linear models are supervised learning algorithms used for solving either classification or regression problems. For more information, see https://docs.aws.amazon.com/sagemaker/latest/dg/linear-learner.html

Running Classification AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- **Fields to use for Classification**: Each field must be a numerical field.
- **Class Label**: The class to which the data corresponds to.
- A **FortiSIEM Report** to get this data.

To provide several samples of the data, you can choose one of the following time attributes as a report column

- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - A Class Label
   - One or more numerical fields to use for classification

   To provide several samples, you can provide a time field. This is optional.
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Classification task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Class Label** and **Fields to use for Classification** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to AWS
   b. Set **Task** to Classification
   c. Choose the **Algorithm**
   d. Choose the **Class Label** and **Fields to use for Classification** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

Binary Classification

- **True Positives (TP)**: Correct classification for label = 0, i.e. actual = 0 and predicted = 0
- **True Negative (TN)**: Correct classification for label = 1, i.e. actual = 1 and predicted = 1
- **False Positive (FP)**: Incorrect classification for label = 0, i.e. actual = 0 and predicted = 1
- **False Negative (FN)**: Incorrect classification for label = 1, i.e. actual = 1 and predicted = 0
- **Precision**: The precision of the final model on the validation dataset. If you choose this metric as the objective, we recommend setting a target recall by setting the binary_classifier_model_ selection hyperparameter to precision_at_target_recall and setting the value for the target_recall hyperparameter. This objective metric is only valid for binary classification.
- **Recall**: The recall of the final model on the validation dataset. If you choose this metric as the objective, we recommend setting a target precision by setting the binary_classifier_model_ selection hyperparameter to recall_at_target_precision and setting the value for the target_ precision hyperparameter. This objective metric is only valid for binary classification.
- **roc_auc_score**: The area under receiving operating characteristic curve (ROC curve) of the final model on the validation dataset. This objective metric is only valid for binary classification.
- **binary_classification_accuracy**: The accuracy of the final model on the validation dataset. This objective metric is only valid for binary classification.
- **binary_f_beta**: The F-beta score of the final model on the validation dataset. By default, the F-beta score is the F1 score, which is the harmonic mean of the validation:precision and validation:recall metrics. This objective metric is only valid for binary classification.
- **Confusion Matrix**: Presents TP, TN, FP and FN in a matrix

Multiclass Classification

- **Dcg**: The discounted cumulative gain of the final model on the validation dataset. This objective metric is only valid for multiclass classification.
- **multiclass_accuracy**: The accuracy of the final model on the validation dataset. This objective metric is only valid for multiclass classification.
- **multiclass_top_k_accuracy**: The accuracy among the top k labels predicted on the validation dataset. If you choose this metric as the objective, we recommend setting the value of k using the accuracy_top_k hyperparameter. This objective metric is only valid for multiclass classification.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Classification Algorithms for AWS Auto Mode

In this mode, FortiSIEM automatically chooses the best algorithm with the optimal parameters. Depending on the size of your dataset (whether is it greater or smaller than 100MB), algorithms from HPO mode or from ensembling mode will be considered. For more information, see https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html. Definitions below taken from Amazon SageMaker Developer Guide.

HPO mode (Dataset > 100MB)

- **Linear learner**: A supervised learning algorithm that can solve either classification or regression problems.
- **XGBoost**: A supervised learning algorithm that attempts to accurately predict a target variable by combining an ensemble of estimates from a set of simpler and weaker models.
- **Deep learning algorithm**: A multilayer perceptron (MLP) and feedforward artificial neural network. This algorithm can handle data that is not linearly separable.

Ensembling mode (Dataset <=100MB)

- **LightGBM**: An optimized framework that uses tree-based algorithms with gradient boosting. This algorithm uses trees that grow in breadth, rather than depth, and is highly optimized for speed.
- **CatBoost**: A framework that uses tree-based algorithms with gradient boosting. Optimized for handling categorical variables.
- **XGBoost**: A framework that uses tree-based algorithms with gradient boosting that grows in depth, rather than breadth.
- **Random Forest**: A tree-based algorithm that uses several decision trees on random sub-samples of the data with replacement. The trees are split into optimal nodes at each level. The decisions of each tree are averaged together to prevent overfitting and improve predictions.
- **Extra Trees**: A tree-based algorithm that uses several decision trees on the entire dataset. The trees are split randomly at each level. The decisions of each tree are averaged to prevent overfitting and to improve predictions. Extra trees add a degree of randomization in comparison to the random forest algorithm.
- **Linear Models**: A framework that uses a linear equation to model the relationship between two variables in observed data.
- **Neural network torch**: A neural network model that is implemented using Pytorch.
- **Neural network fast.ai**: A neural network model that is implemented using fast.ai.

Note: The Max Run Time parameter is used to limit the amount of time this job runs. By default it is set to 225 minutes.

The longer this job runs, potentially better results can be generated.

Running Classification AWS Auto Mode

To run, follow the Regression steps in Algorithm for AWS Mode, but in Step 3, 3a, select **Run Mode** as **AWS Auto**.

For Step 3, the following model quality information pertains.

Model Quality:

The following metrics show the quality of the clusters found.

Binary Classification

- **True Positives (TP)**: Correct classification for label = 0, i.e. actual = 0 and predicted = 0
- **True Negative (TN)**: Correct classification for label = 1, i.e. actual = 1 and predicted = 1
- **False Positive (FP)**: Incorrect classification for label = 0, i.e. actual = 0 and predicted = 1

- **False Negative (FN)**: Incorrect classification for label = 1, i.e. actual = 1 and predicted = 0
- **F1**: The F1 score is the harmonic mean of the *precision* and *recall*, defined as follows: F1 = 2 * (*precision* * *recall*) / (*precision* + *recall*). It is used for binary classification into classes traditionally referred to as positive and negative. Predictions are said to be true when they match their actual (correct) class, and false when they do not.*Precision* is the ratio of the true positive predictions to all positive predictions, and it includes the false positives in a dataset. *Precision* measures the quality of the prediction when it predicts the positive class.*Recall* (or sensitivity) is the ratio of the true positive predictions to all actual positive instances. *Recall* measures how completely a model predicts the actual class members in a dataset.F1 scores vary between 0 and 1. A score of 1 indicates the best possible performance, and 0 indicates the worst.
- **LogLoss**: Log loss, also known as cross-entropy loss, is a metric used to evaluate the quality of the probability outputs, rather than the outputs themselves. It is used in both binary and multiclass classification and in neural nets. It is also the cost function for logistic regression. Log loss is an important metric to indicate when a model makes incorrect predictions with high probabilities. Values range from 0 to infinity. A value of 0 represents a model that perfectly predicts the data.
- **Recall**: Recall measures how well an algorithm correctly predicts all of the true positives (TP) in a dataset. A true positive is a positive prediction that is also an actual positive value in the data. Recall is defined as follows: Recall = TP/(TP+FN), with values ranging from 0 to 1. Higher scores reflect a better ability of the model to predict true positives (TP) in the data. It is used in binary classification.

  Recall is important when testing for cancer because it's used to find all of the true positives. A false positive (FP) reflects a positive prediction that is actually negative in the data. It is often insufficient to measure only recall, because predicting every output as a true positive yields a perfect recall score.
- **Precision**: Precision measures how well an algorithm predicts the true positives (TP) out of all of the positives that it identifies. It is defined as follows: Precision = TP/(TP+FP), with values ranging from zero (0) to one (1), and is used in binary classification. Precision is an important metric when the cost of a false positive is high. For example, the cost of a false positive is very high if an airplane safety system is falsely deemed safe to fly. A false positive (FP) reflects a positive prediction that is actually negative in the data.
- **AUC**: The area under the curve (AUC) metric is used to compare and evaluate binary classification by algorithms that return probabilities, such as logistic regression. To map the probabilities into classifications, these are compared against a threshold value.
  The relevant curve is the receiver operating characteristic curve (ROC curve). The ROC curve plots the true positive rate (TPR) of predictions (or recall) against the false positive rate (FPR) as a function of the threshold value, above which a prediction is considered positive. Increasing the threshold results in fewer false positives, but more false negatives.
  AUC is the area under this ROC curve. Therefore, AUC provides an aggregated measure of the model performance across all possible classification thresholds. AUC scores vary between 0 and 1. A score of 1 indicates perfect accuracy, and a score of one half (0.5) indicates that the prediction is not better than a random classifier.
- **Accuracy**: The ratio of the number of correctly classified items to the total number of (correctly and incorrectly) classified items. It is used for both binary and multiclass classification. Accuracy measures how close the predicted class values are to the actual values. Values for accuracy metrics vary between zero (0) and one (1). A value of 1 indicates perfect accuracy, and 0 indicates perfect inaccuracy.
- **BalancedAccuracy**: BalancedAccuracy is a metric that measures the ratio of accurate predictions to all predictions. This ratio is calculated after normalizing true positives (TP) and true negatives (TN) by the total number of positive (P) and negative (N) values. It is used in both binary and

multiclass classification and is defined as follows: 0.5*((TP/P)+(TN/N)), with values ranging from 0 to 1. BalancedAccuracy gives a better measure of accuracy when the number of positives or negatives differ greatly from each other in an imbalanced dataset, such as when only 1% of email is spam.

Multiclass Classification:

- **F1macro**: The F1macro score applies F1 scoring to multiclass classification problems. It does this by calculating the precision and recall, and then taking their harmonic mean to calculate the F1 score for each class. Lastly, the F1macro averages the individual scores to obtain the F1macro score. F1macroscores vary between 0 and 1. A score of 1 indicates the best possible performance, and 0 indicates the worst.
- **PrecisionMacro**: The precision macro computes precision for multiclass classification problems. It does this by calculating precision for each class and averaging scores to obtain precision for several classes. PrecisionMacro scores range from zero (0) to one (1). Higher scores reflect the model's ability to predict true positives (TP) out of all of the positives that it identifies, averaged across multiple classes.
- **Accuracy**: The ratio of the number of correctly classified items to the total number of (correctly and incorrectly) classified items. It is used for both binary and multiclass classification. Accuracy measures how close the predicted class values are to the actual values. Values for accuracy metrics vary between zero (0) and one (1). A value of 1 indicates perfect accuracy, and 0 indicates perfect inaccuracy.
- **BalancedAccuracy**: BalancedAccuracy is a metric that measures the ratio of accurate predictions to all predictions. This ratio is calculated after normalizing true positives (TP) and true negatives (TN) by the total number of positive (P) and negative (N) values. It is used in both binary and multiclass classification and is defined as follows: 0.5*((TP/P)+(TN/N)), with values ranging from 0 to 1. BalancedAccuracy gives a better measure of accuracy when the number of positives or negatives differ greatly from each other in an imbalanced dataset, such as when only 1% of email is spam.
- **LogLoss**: Log loss, also known as cross-entropy loss, is a metric used to evaluate the quality of the probability outputs, rather than the outputs themselves. It is used in both binary and multiclass classification and in neural nets. It is also the cost function for logistic regression. Log loss is an important metric to indicate when a model makes incorrect predictions with high probabilities. Values range from 0 to infinity. A value of 0 represents a model that perfectly predicts the data.
- **RecallMacro**: The RecallMacro computes recall for multiclass classification problems by calculating recall for each class and averaging scores to obtain recall for several classes. RecallMacro scores range from 0 to 1. Higher scores reflect the model's ability to predict true positives (TP) in a dataset, whereas a true positive reflects a positive prediction that is also an actual positive value in the data. It is often insufficient to measure only recall, because predicting every output as a true positive will yield a perfect recall score.

Clustering

The objective of a Clustering Task is to group similar items based on a set of fields in a dataset, and then create an alert if an item belongs to a different group based on current values. Learning the groups is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

- Clustering Algorithm for Local Mode
- Running Clustering Local Mode
- Clustering Algorithms for Local Auto Mode
- Running Clustering Local Auto Mode
- Clustering Algorithm for AWS Mode
- Running Clustering AWS Mode

Clustering Algorithm for Local Mode

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

- **BIRCH**: Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH) is an *unsupervised* clustering algorithm for grouping particularly large data-sets. It takes a hierarchical approach by first summarizing large datasets into smaller, dense regions called Clustering Feature (CF) entries and then clustering the smaller data set. It only works for numerical entries. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.Birch.html
- **DBScan**: Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is an *unsupervised* clustering algorithm that groups together points that are closely packed together (points with many nearby neighbors) and discarding data points that lie alone in low-density regions (whose nearest neighbors are too far away). The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.DBSCAN.html
- **GMeans**: An *unsupervised* clustering algorithm for grouping data points. It extends K-means by trying to *automatically determine the number of clusters* by Gaussian normality test. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.KMeans.html
- **KMeans**: An *unsupervised* clustering algorithm that groups data points into user specified K groups so that each data point belongs to one group. It tries to iteratively minimize intra-cluster distance and maximize inter-cluster distance. Note that user needs to specify the number of clusters based on user's knowledge of data. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.KMeans.html
- **Spectral Clustering**: An *unsupervised* graph-based clustering algorithm for grouping data points. It first constructs a similarity graph, then embeds the data points in a lower dimensional space and then applying classical algorithms like KMeans to partition the data points. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.SpectralClustering.html

Running Clustering Local Mode

Step 1: Design

First identify the following items:

- **Fields to use for Clustering**: Each field must be a numerical field.
- **Id field**: The identity of a row of data, typically the host name or host IP.
- A **FortiSIEM Report** to get this data.

The Time field is not recommended for a Clustering task since an item may belong to different clusters at different point in time.

Requirements

1. Report must contain
   - an Id field
   - One or more numerical fields to use for clustering
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are

part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Clustering task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Id Field** and **Fields to use for Clustering** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to Local
   b. Set **Task** to Clustering
   c. Choose the **Algorithm**
   d. Check the algorithm parameters, e.g. for KMeans choose the cluster size as a guess.
   e. Choose the **Id Field** and **Fields to use for Clustering** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

- **Calinski Marabasz Score**: Calinski Marabasz Score (also known as the Variance Ratio Criterion) is calculated as a ratio of the sum of inter-cluster dispersion and the sum of intra-cluster dispersion for all clusters (where the dispersion is the sum of squared distances). *A high Calinski-Harabasz Score means better clustering* since observations in each cluster are closer together (more dense), while clusters themselves are further away from each other (well separated).
- **Davies Bouldin Score**: This is calculated as the average similarity of each cluster with a cluster most similar to it. *Low Davies Bouldin Score means clusters are well separated*.
- **Silhouette Score**: This is calculated using the mean intra-cluster distance and the mean nearest-cluster distance for each sample. *Silhouette Score of 1 means clusters are well apart from each other and clearly distinguished*. Silhouette Score of 0 means that clusters are indifferent, or we can say that the distance between clusters is not significant. Silhouette Score of -1 means clusters are assigned in the wrong way.

The actual and predicted values and the errors are shown in 3 ways:

- **Clustering Result table**: this shows which entity is in which cluster
- **Clustering Membership > Heatmap View**: this shows entity-cluster membership along with the values. Entities in the same cluster should have the same color.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when cluster changes during the Inference process.
  - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Clustering Algorithms for Local Auto Mode

In this mode, FortiSIEM picks the best algorithm from the following:

- BIRCH
- DBSCAN
- KMeans

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 10 minutes. The longer this job runs, potentially better result can be generated.

Running Clustering Local Auto Mode

To run, follow the Clustering steps in Algorithms for Local Mode, but in Step 3, 3a, select **Run Mode** as **Local Auto**.

Clustering Algorithm for AWS Mode

In this mode, the following algorithm runs in AWS.

- KMeans

Running Clustering AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- **Fields to use for Clustering**: Each field must be a numerical field.
- **Id field**: The identity of a row of data, typically the host name or host IP.
- A **FortiSIEM Report** to get this data.

The Time field is not recommended for a Clustering task since an item may belong to different clusters at different point in time.

Requirements

1. Report must contain
   - an Id field
   - One or more numerical fields to use for clustering
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Clustering task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Id Field** and **Fields to use for Clustering** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to AWS
   b. Set **Task** to Clustering
   c. Choose the **Algorithm**
   d. Check the algorithm parameters, e.g. for KMeans choose the cluster size as a guess.
   e. Choose the **Id Field** and **Fields to use for Clustering** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

The following metrics show the quality of the clusters found.

- **Calinski Marabasz Score**: Calinski Marabasz Score (also known as the Variance Ratio Criterion) is calculated as a ratio of the sum of inter-cluster dispersion and the sum of intra-cluster dispersion for all clusters (where the dispersion is the sum of squared distances). *A high Calinski-Harabasz Score means better clustering* since observations in each cluster are closer together (more dense), while clusters themselves are further away from each other (well separated).
- **Davies Bouldin Score**: This is calculated as the average similarity of each cluster with a cluster most similar to it. *Low Davies Bouldin Score means clusters are well separated*.
- **Silhouette Score**: This is calculated using the mean intra-cluster distance and the mean nearest-cluster distance for each sample. *Silhouette Score of 1 means clusters are well apart from each other and clearly distinguished*. Silhouette Score of 0 means that clusters are indifferent, or we can say that the distance between clusters is not significant. Silhouette Score of -1 means clusters are assigned in the wrong way.
- **'msd' (Mean Squared Distance)**: This metric is the average of the squared distances between each data point and its assigned cluster center. The mean squared distance is used to assess the overall quality of the clustering, where lower values indicate better clustering performance.
- **'ssd' (Sum of Squared Distances)**: This metric is the sum of the squared distances between each data point and its assigned cluster center. It is also known as the within-cluster sum of squares (WCSS) and is commonly used to evaluate the compactness of the clusters.

The actual and predicted values and the errors are shown in the following ways:

- **Clustering Result table**: this shows which entity is in which cluster
- **Clustering Membership > Heatmap View**: this shows entity-cluster membership along with the values. Entities in the same cluster should have the same color.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.

    - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
    - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when cluster changes during the Inference process.
    - Two choices are available – creating a FortiSIEM Incident or sending an email. Specify the emails if you want emails to be sent. Make sure that email server is specified in **Admin > Settings > Email**.
    - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Forecasting

- Forecasting Algorithms for Local Mode
- Running Forecasting Local Mode

The objective of a Forecasting Task is to learn a time based trend of a field in a dataset and then predict future values of that field. Learning the time based trend is done during the Training phase and future prediction is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

Forecasting Algorithms for Local Mode

In this mode, the following algorithms can run locally within the FortiSIEM Super/Worker cluster.

- **ARIMA (AutoRegressive Integrated Moving Average)**: A statistical analysis model that uses time series data to predict future values. Descriptions of the parameters are here: https://analyticsindiamag.com/quick-way-to-find-p-d-and-q-values-for-arima/ and https://www.sciencedirect.com/topics/mathematics/arima
- **State Space Dynamic MQ**: A forecasting method that can be used to predict future values. Descriptions of the parameters are here: https://www.statsmodels.org/devel/generated/statsmodels.tsa.statespace.dynamic_factor_mq.DynamicFactorMQ.html#statsmodels.tsa.statespace.dynamic_factor_mq.DynamicFactorMQ

Running Forecasting Local Mode

Step 1: Design

First identify the following items:

- **Field to Forecast**: Each field must be a numerical field.
- **Fields to use for Forecasting**: Each field must be a numerical field. Field to forecast could be the same as field to use for forecasting; meaning that previous values of a field is used to forecast future values of the same field.
- **Id Field**: Identifies who the data is for.
  Note: The Id Field is optional.
- **Date Field**: Can be hourly or daily.
- A **FortiSIEM Report** to get this data.

To provide several samples of the data, you can choose one of the following time attributes as a report column

- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - Date Field - Event Receive Hour or Event Receive Date
   - One numerical field to forecast
   - (Optional) Other fields to use for forecasting
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**, and click the Import Machine Learning Jobs (open folder) icon.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Forecasting task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Date Field**, **Field(s) to use for Forecasting**, and **Id Field** are populated correctly.
3. If you chose **Import via Report** or **Import via CSV File**, then
   a. Set **Run Mode** to Local
   b. Set **Task** to Forecasting
   c. Choose the **Algorithm**
   d. Choose **Id Field**
   e. If the **Algorithm** is ARIMA:
      i. Choose the **Field to Forecast** from the report fields. Current ARIMA implementation uses previous values of a field to forecast the future values of the same field.
      ii. Choose the **Steps** parameter to specify how many time steps to be forecasted. The default value is 5 and can be found by clicking the Settings icon next to the Algorithm.
   f. If the Algorithm is **State Space Dynamic Factor MQ**:
      i. Choose the **Field to Forecast** and **Fields to use for Forecasting** from the report fields.
      ii. Choose the **Steps** parameter to specify how many time steps to be forecasted. The default value is 5 and can be found by clicking the Settings icon next to the Algorithm.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **Max Error**: Mmaximum of the error between predicted value and actual value over all data points. *Lower value means that regression is a better fit.*
- **Mean Absolute Error**: Average of Absolute difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Mean Squared Error**: Average of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **R2 score**: a statistical measure of how well the regression predictions approximate the real data points. *An R2 of 1 indicates that the regression predictions perfectly fit the data.* R-square value of 0.8 means that 80% of the variation in the predicted attribute is explained by the feature attributes.
- **Root Mean Squared Error (RMSE)**: Square root of the average of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.* RMSE is affected by the scale of the data. RMSE can be heavily affected by a few predictions which are much worse than the rest.

Forecasting Result is shown in two ways

- **Tabular form**: The predicted values are shown in the first few rows.
- **Trend form**: Shows how the algorithm learns the values over time and is able to forecast future values

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - One choice is available – Send email(s) by entering the email address(es) in the **Send email to** field. Make sure that the email server is specified in **Admin > Settings > Email**.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Regression

The objective for Regression Task is to build a model for predicting a Target field based on other fields in a dataset, and then create an alert if the new values of the Target field exceeds the predicted value, by user specified threshold. Building the prediction model is done during the Training phase and alert creation is done during the Inference phase. The dataset for both Training and Inference phases is provided by running FortiSIEM reports.

- Regression Algorithms for Local Mode
- Running Regression Local Mode
- Regression Algorithms for Local Auto Mode
- Running Regression Local Auto Mode
- Regression Algorithms for AWS Mode
- Running Regression AWS Mode
- Regression Algorithms for AWS Auto Mode
- Running Regression AWS Auto Mode

Regression Algorithms for Local Mode

The following Machine Learning Algorithms are available:

In this mode, the following algorithms can run *locally* within the FortiSIEM Supervisor/Worker cluster.

- **Decision Tree Regressor**: A supervised regression algorithm that uses a Decision Tree to predict a Target variable based on Feature variables. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.tree.DecisionTreeRegressor.html
- **Linear Regression**: A supervised regression algorithm that predicts a Target variable based on a linear combination of Feature variables. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.LinearRegression.html
- **Random Forest Regressor**: A supervised regression algorithm that uses Ensemble learning and Bootstrapping techniques to improve the accuracy of Decision Tree based prediction algorithms. Ensemble learning uses multiple models and Bootstrapping randomly samples datasets and then averages the results of each model to improve accuracy. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestRegressor.html
- **SGDRegressor**: A supervised regression algorithm that uses Stochastic Gradient Descent (SGD) method to minimize a user specified loss function for the Linear Regression algorithm. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.linear_model.SGDRegressor.html
- **SVR**: A supervised regression algorithm that finds a linear function representing the data within a margin of error Support Vector Regression (SVR) error function for prediction. SVR is more robust to outliers than most other regression methods, since it does not care much about the data outside

the margin. The parameters for this algorithm are described here: https://scikit-learn.org/stable/modules/generated/sklearn.svm.SVR.html

Running Regression Local Mode

Step 1: Design

First identify the following items:

- **Field to Predict**: Must be a numerical field.
- **Fields to use for Prediction**: Each field must be a numerical field.
- A **FortiSIEM Report** to get this data.

There must be several samples of the data. This can be accomplished by choosing one of the following time attributes as a report column

- Event Receive Time
- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - A time attribute
   - One numerical **Field to Predict**
   - One or more numerical **Fields to use for Prediction**
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.

   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Regression task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Fields to use for Prediction** and **Fields to Predict** are populated correctly.
3. If you chose **Import via Report** or **Import Via CSV File**, then
   a. Set **Run Mode** to Local
   b. Set **Task** to Regression
   c. Choose the **Algorithm**
   d. Choose the **Fields to use for Prediction** and **Fields to Predict** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **Max Error**: Maximum of the error between predicted value and actual value over all data points. *Lower value means that regression is a better fit.*
- **R2 score**: A statistical measure of how well the regression predictions approximate the real data points. *An R2 of 1 indicates that the regression predictions perfectly fit the data.* R-square value of 0.8 means that 80% of the variation in the predicted attribute is explained by the feature attributes.
- **Mean Absolute Error**: Average of Absolute difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Mean Squared Error**: Average of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Root Mean Squared Error (RMSE)**: Square root of the verage of Square of difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*

RMSE is affected by the scale of the data. RMSE can be heavily affected by a few predictions which are much worse than the rest.

The actual and predicted values and the errors are shown in 3 ways:

- **Regression Result table**: If the model did well, then the error column should have small values.
- **Scatter plot**: If the model did well, then this chart must be centered along the y=x line.
- **Error histogram**: If the model did well, then the chart should be clustered around the x=0 line.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.
- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Only one choice is available – Creating an incident when Error is #. Enter a number in the **Create an Incident when Error is great than** field.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Regression Algorithms for Local Auto Mode

In this mode, FortiSIEM automatically chooses the best algorithm with the optimal parameters. The following algorithms are considered:

- **Decision Tree Regressor**
- **Random Forest Regressor**
- **SGDRegressor**
- **SVR**

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 5 minutes. The longer this job runs, potentially better results can be generated.

Running Regression Local Auto Mode

To run, follow the Regression steps in Algorithms for Local Mode, but in Step 3, 3a, select **Run Mode** as **Local Auto**.

Regression Algorithms for AWS Mode

The following algorithm runs in AWS mode.

- **Linear- Learner Algorithem-for-Regression**: Linear models are supervised learning algorithms used for solving either classification or regression problems. See https://docs.aws.amazon.com/sagemaker/latest/dg/linear-learner.html for more information.

Running Regression AWS Mode

Step 0: Set Up AWS

Set up AWS SageMaker by following the instructions in Set Up AWS SageMaker.

Configure AWS in FortiSIEM by following the instructions in Configure FortiSIEM to use AWS SageMaker.

Step 1: Design

First identify the following items:

- **Field to Predict**: Must be a numerical field.
- **Fields to use for Prediction**: Each field must be a numerical field.
- A **FortiSIEM Report** to get this data.

There must be several samples of the data. This can be accomplished by choosing one of the following time attributes as a report column

- Event Receive Time
- Event Receive Hour
- Event Receive Date

Requirements

1. Report must contain
   - A time attribute
   - One numerical **Field to Predict**
   - One or more numerical **Fields to use for Prediction**
2. Each field must be present in the report result; else the whole row will be ignored by the Machine Learning algorithm.
3. There can be additional columns in the report and they will be ignored by the machine learning algorithm. However, it is recommended to remove unnecessary columns from the dataset to reduce the size of the dataset exchanged between App Server and phAnomaly modules, during Training and Inference.

Go to **Analytics > Search** and run various reports. Once you have the right report, save it in **Resources > Machine Learning Jobs**.

Step 2: Prepare Data

Prepare the data for training.

1. Go to **Analytics > Machine Learning**.
2. Select the data source in one of three ways:
   a. To prepare data from a Machine Learning Job, choose **Import via Jobs** and select the Job which has associated Report and algorithm.
   b. To prepare data from the Report folder, choose **Import via Report** and select the report from the **Resources > Machine Learning Job** folder
   c. To prepare data from a CSV file, choose **Import Via CSV File** and upload the file. In this mode, you can see how the Training algorithm performs, but you cannot schedule for inference, since the data may not be present in FortiSIEM.
3. For Case 2a and 2b, select the Report **Time Range** and the Organization for Service Provider Deployments.
4. Click **Run**. The results are displayed in **Machine Learning > Prepare** tab.
   Note: For FortiSIEM with ClickHouse deployments, **Historical mode** searches include a **Result Filter** panel that provides a top and bottom 100 list (click / to toggle) for the attributes that are part of your Display Field ( ) search. An Add to Main Filter icon ( ) is available to hone search results and identify trends related to the selected attributes with other attributes.

Step 3: Train

Train the Regression task using the dataset in Step 2.

1. Go to **Analytics > Machine Learning > Train**.
2. If you chose **Import via Jobs**, then make sure the **Fields to use for Prediction** and **Fields to Predict** are populated correctly.
3. If you chose **Import via Report** or **Import Via CSV File**, then
   a. Set **Run Mode** to AWS
   b. Set **Task** to Regression
   c. Choose the **Algorithm**
   d. Choose the **Fields to use for Prediction** and **Fields to Predict** from the report fields.
4. Choose the **Train factor** which should be greater than 70%. This means that 70% of the data will be used for Training and 30% used for Testing.
5. Click **Train**.

After you have completed the Training, the results are shown in the **Train > Output** tab.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **Mean Absolute Error (MAE)**: Average of Absolute difference between predicted and actual values over all data points. *Lower value means that regression is a better fit.*
- **Mean Squared Error (MSE)**: The mean square error of the final model on the validation dataset. This objective metric is only valid for regression.
- **R2 score**: A statistical measure of how well the regression predictions approximate the real data points. *An R2 of 1 indicates that the regression predictions perfectly fit the data.* R-square value of 0.8 means that 80% of the variation in the predicted attribute is explained by the feature attributes.
- **Root Mean Squared Error (RMSE)**: The root mean square error of the final model on the validation dataset. This objective metric is only valid for regression.

The actual and predicted values and the errors are shown in 3 ways:

- **Regression Result table**: If the model did well, then the error column should have small values.
- **Scatter plot**: If the model did well, then this chart must be centered along the y=x line.
- **Error histogram**: If the model did well, then the chart should be clustered around the x=0 line.

If you want to change the algorithm parameters and re-train, then click **Tune & Train**, change the parameters and click **Save & Train**.

Step 4: Schedule

Once the training is complete, you can schedule the job for Inference.

- **Input Details** section shows the Report and the Org chosen for the report. These were already chosen during **Prepare** phase and will be used during **Inference**.
- **Algorithm Setup** shows the Machine Learning Algorithm and its parameters. These were already chosen during **Train** phase and will be used during **Inference**.

- **Schedule Setup** shows the Job details and schedules
  - **Job Id**: Specifies the unique Job Id. If it is a system job, it will be overwritten with a new job id when it is saved as a User job. If it is a User job, then user has option to Save as a new user job with different job id or keeping the same job Id.
  - **Job Name**: Name of the job. You can overwrite this one. When a job with the same name exists then a data stamp will be appended.
  - **Job Description**: Description of the job.
  - **Inference schedule**: The frequency at which Inference job will be run
  - **Retraining schedule**: The frequency at which the model would be retrained. Retraining is expensive and it should be carefully considered. Recommended retraining is at least 7 days.
  - **(Retraining) Report Window**: The Report time window during retraining process. Long time window may cause the report to run slowly and this should be carefully considered as well. It is recommended to choose the same time window chosen during the Prepare process.
  - **Job Group**: Shows the folder under **Resources > Machine Learning Jobs** where this job will be saved.
- **Action on Inference**: Specifies the action to be taken when an anomaly is found during the Inference process.
  - Only one choice is available – Creating an incident when Error is #. Enter a number in the **Create an Incident when Error is great than** field.
  - Check **Enabled** to ensure that Inference is enabled.

Finally click **Save** to save this to database. If it is a system job, then a new User job will be created. If it is a User job, then user has option to Save as a new user job with different job id or overwriting the current job.

Regression Algorithms for AWS Auto Mode

In this mode, FortiSIEM automatically chooses the best algorithm with the optimal parameters. Depending on the size of your dataset (whether is it greater or smaller than 100MB), algorithms from HPO mode or from ensembling mode will be considered. For more information, see https://docs.aws.amazon.com/sagemaker/latest/dg/autopilot-model-support-validation.html. Definitions below taken from Amazon SageMaker Developer Guide.

HPO mode (Dataset > 100MB)

- **Linear learner**: A supervised learning algorithm that can solve either classification or regression problems.
- **XGBoost**: A supervised learning algorithm that attempts to accurately predict a target variable by combining an ensemble of estimates from a set of simpler and weaker models.
- **Deep learning algorithm**: A multilayer perceptron (MLP) and feedforward artificial neural network. This algorithm can handle data that is not linearly separable.

Ensembling mode (Dataset <=100MB)

- **LightGBM**: An optimized framework that uses tree-based algorithms with gradient boosting. This algorithm uses trees that grow in breadth, rather than depth, and is highly optimized for speed.

- **CatBoost**: A framework that uses tree-based algorithms with gradient boosting. Optimized for handling categorical variables.
- **XGBoost**: A framework that uses tree-based algorithms with gradient boosting that grows in depth, rather than breadth.
- **Random Forest**: A tree-based algorithm that uses several decision trees on random sub-samples of the data with replacement. The trees are split into optimal nodes at each level. The decisions of each tree are averaged together to prevent overfitting and improve predictions.
- **Extra Trees**: A tree-based algorithm that uses several decision trees on the entire dataset. The trees are split randomly at each level. The decisions of each tree are averaged to prevent overfitting and to improve predictions. Extra trees add a degree of randomization in comparison to the random forest algorithm.
- **Linear Models**: A framework that uses a linear equation to model the relationship between two variables in observed data.
- **Neural network torch**: A neural network model that is implemented using Pytorch.
- **Neural network fast.ai**: A neural network model that is implemented using fast.ai.

Note: The **Max Run Time** parameter is used to limit the amount of time this job runs. By default it is set to 225 minutes. The longer this job runs, potentially better results can be generated.

Running Regression AWS Auto Mode

To run, follow the Regression steps in Algorithms for AWS Mode, but in Step 3, 3a, select **Run Mode** as **AWS Auto**.

For Step 3, the following model quality information pertains.

Model Quality:

This shows how accurately the algorithm is able to predict the field. The following metrics are calculated:

- **MAE**: The mean absolute error (MAE) is a measure of how different the predicted and actual values are, when they're averaged over all values. MAE is commonly used in regression analysis to understand model prediction error. If there is linear regression, MAE represents the average distance from a predicted line to the actual value. MAE is defined as the sum of absolute errors divided by the number of observations. Values range from 0 to infinity, with smaller numbers indicating a better model fit to the data.
- **RMSE**: Root mean squared error (RMSE) measures the square root of the squared difference between predicted and actual values, and is averaged over all values. It is used in regression analysis to understand model prediction error. It's an important metric to indicate the presence of large model errors and outliers. Values range from zero (0) to infinity, with smaller numbers indicating a better model fit to the data. RMSE is dependent on scale, and should not be used to compare datasets of different sizes.**MSE**: The mean squared error (MSE) is the average of the squared differences between the predicted and actual values. It is used for regression. MSE values are always positive. The better a model is at predicting the actual values, the smaller the MSE value is.
- **R2**: R2, also known as the coefficient of determination, is used in regression to quantify how much a model can explain the variance of a dependent variable. Values range from one (1) to negative one

(-1). Higher numbers indicate a higher fraction of explained variability. R2 values close to zero (0) indicate that very little of the dependent variable can be explained by the model. Negative values indicate a poor fit and that the model is outperformed by a constant function. For linear regression, this is a horizontal line.

Working with Dashboards

FortiSIEM collects logs and performance metrics and create Incidents by event correlation and other means. This data can be summarized in Reports. A Dashboard provides a graphical view of these reports. FortiSIEM Dashboards are organized into a two-level hierarchy: Dashboard folders with each folder containing multiple Dashboards.

You can perform various operations from FortiSIEM Dashboards:

- General Operations

A Dashboard can be one of the following six built-in dashboard types:

- Widget Dashboard
- Summary Dashboard
- Business Service Dashboard
- Identity and Location Dashboard
- Interface Usage Dashboard
- PCI Logging Status Dashboard

General Operations

FortiSIEM Dashboard can be used to perform various operations:

- Viewing Built-in Dashboard Folders
- Displaying Only Dashboard Folders of Interest
- Setting a Home Dashboard Folder
- Creating a New Dashboard Folder
- Creating a New Dashboard Under a Folder
- Sharing Dashboard Folders
- Deleting a Dashboard
- Deleting a Dashboard Folder
- Starting Dashboard Slideshow

Viewing Built-in Dashboard Folders

FortiSIEM provides several built-in dashboard folders:

Folder	Dashboard	Type	Description
Application Server Dashboard	JBoss	Widget Dashboard	
	WebSphere	Widget Dashboard	
	WebLogic	Widget Dashboard	
	Tomcat	Widget Dashboard	
	GlassFish	Widget Dashboard	
Amazon Web Services Dashboard	Summary	Summary Dashboard	
	Performance	Widget Dashboard	
	Login	Widget Dashboard	
	Cloud Trail	Widget Dashboard	
	Elastic Load Balancer	Widget Dashboard	
Database Dashboard	Logon	Widget Dashboard	
	System Perf	Widget Dashboard	
	Oracle Performance	Widget Dashboard	
	SQL Server Performance	Widget Dashboard	
	MySQL Performance	Widget Dashboard	
Fortinet Security Fabric	Security Posture	Widget Dashboard	
	FortiGate Threat	Widget Dashboard	
	FortiGate Traffic	Widget Dashboard	
	FortiMail	Widget Dashboard	
	FortiSandbox	Widget Dashboard	
	FortiDeceptor	Widget Dashboard	
	FortiEDR	Widget Dashboard	
	FortiClient	Widget Dashboard	
	FortiADC	Widget Dashboard	
	FortiNDR On-Premise	Widget Dashboard	
	FortiNDR Cloud	Widget Dashboard	
	FortiProxy	Widget Dashboard	
	FortiWeb	Widget Dashboard	

Folder	Dashboard	Type	Description
	FortiRecon	Widget Dashboard	
FortiSIEM Dashboard	Event	Widget Dashboard	
	Audit	Widget Dashboard	
	Incidents	Widget Dashboard	
	Cases	Widget Dashboard	
GCP Dashboard	Google Cloud Audit	Widget Dashboard	
Global FortiSIEM Dashboard	Event	Widget Dashboard	After upgrading, super users in global mode can access the Global FortiSIEM Dashboard. **Note**: This is the same as the FortiSIEM Dashboard.
	Audit	Widget Dashboard	
	Incidents	Widget Dashboard	
	Cases	Widget Dashboard	
Google Apps Dashboard	Summary	Widget Dashboard	
	Audit	Widget Dashboard	
Identity and Location Dashboard	Identity and Location	Summary Dashboard	
Mimecast	Overview	Widget Dashboard	
	Threats	Widget Dashboard	
NetApp Dashboard	Overall	Widget Dashboard	
	NFS Perf	Widget Dashboard	
	CISF Perf	Widget Dashboard	
	ISCSI Perf	Widget Dashboard	
Network Dashboard	Summary	Summary Dashboard	
	Hardware	Summary Dashboard	
	Availability	Widget Dashboard	
	Performance	Widget Dashboard	
	Login/Change	Widget Dashboard	
	Netflow	Widget Dashboard	
	IPSLA	Widget Dashboard	

Folder	Dashboard	Type	Description
	VoIP	Widget Dashboard	
	CBQoS	Widget Dashboard	
Nutanix Dashboard	Nutanix Audit	Widget Dashboard	
Office365 Dashboard	Logon Audit	Widget Dashboard	
	Sharepoint Audit	Widget Dashboard	
	Sensitivity Label Audit	Widget Dashboard	
	Mail Statistics	Widget Dashboard	
Oracle Cloud Dashboard	Oracle Cloud Audit	Widget Dashboard	
Salesforce Dashboard	Login	Widget Dashboard	
	Activity	Widget Dashboard	
	Performance	Widget Dashboard	
Security Dashboard	Perimeter	Widget Dashboard	
	Access	Widget Dashboard	
	Malware	Widget Dashboard	
	Vulnerability	Widget Dashboard	
	Exploits	Widget Dashboard	
	Policy Violation	Widget Dashboard	
	UEBA AI Alerts	Widget Dashboard	
	UEBA Events	Widget Dashboard	
	OT/IoT	Widget Dashboard	
Server Dashboard	Summary	Summary Dashboard	
	Hardware	Summary Dashboard	
	Availability	Widget Dashboard	
	Performance	Widget Dashboard	
	Login	Widget Dashboard	
Trend Vision One	Alerts	Widget Dashboard	
	Audit	Widget Dashboard	
VMWare Dashboard	VM	Widget Dashboard	
	ESX	Widget Dashboard	
	Cluster	Widget Dashboard	

Folder	Dashboard	Type	Description
	Resource Pool	Widget Dashboard	
	Datastore	Widget Dashboard	
	Environment	Widget Dashboard	
	Events	Widget Dashboard	
VNX Dashboard	Processor	Widget Dashboard	
	Ports	Widget Dashboard	
	LUNs	Widget Dashboard	
	Storage Pool	Widget Dashboard	
Web Server Dashboard	System Performance	Widget Dashboard	
	IIS Performance	Widget Dashboard	
	Apache Performance	Widget Dashboard	
	Access	Widget Dashboard	

Displaying Only Dashboard Folders of Interest

Complete these steps to see only the dashboards folders that are of interest to you:

1. Click the **User Profile** icon ( ) in the upper right corner of the UI.
2. Click the **UI Settings** tab.
3. Click the Edit icon for **Dashboard Settings**.
4. Select the currently **Visible Dashboards** that you want to hide and click **<**.
5. Click **Save**.

The dashboard folder drop-down list under the **DASHBOARD** tab will display only the selected dashboard folders.

Setting a Home Dashboard Folder

Complete these steps to see a specific dashboard folder when you navigate to the **DASHBOARD** tab:

1. Click the **User Profile** icon ( ) in the upper right corner of the UI.
2. Click the **UI Settings** tab.
3. Select a **Dashboard Home** from the drop-down list.
4. Click **Save**. Refresh the Web page if it doesn't reload automatically.

Creating a New Dashboard Folder

Complete these steps to create a new dashboard folder:

1. Go to **DASHBOARD** and select **New** from the Dashboard drop-down list.
2. Enter a dashboard **Name**.
3. Select whether you want to share the dashboard.
4. Click **Save**.

Creating a New Dashboard Under a Folder

Note: You can add a dashboard to a built-in dashboard folder.

To create a new dashboard under a dashboard folder:

1. Go to **DASHBOARD** tab.
2. Select the dashboard from the folder drop-down list. The dashboards belonging to the folder will display on the top menu.
3. Click **+** to the right.
4. Enter a dashboard **Name**, select a dashboard **Type**, and add any related **Description** about this dashboard.
5. Click **Save**.

Sharing Dashboard Folders

When you create a new dashboard folder, FortiSIEM gives you the option of sharing the folder, and all of the dashboards in it, with other users.

Note the following rules and restrictions on shared dashboards:

Rules for creating and using shared dashboard folders:

- A user can share only with other users in the same organization.
  - A Super user can share only with other Super users, even if that Super user is in Global mode.
  - Org users can share only with (the same) Org users.
- If a Global/Super user shares a dashboard with another user, the other user can see only this dashboard in Global/Super mode.
- If a Local/Super user shares a dashboard with another user, the other user can see only this dashboard in Local/Super mode.
- If you share with all users in the current Org, then above rules also apply.

Restrictions on shared dashboards:

- Only the user who created the dashboard has Write permission to it, including setting the list of shareable users. The users with whom the dashboards are shared have only Read permission.
- Shared users can view the reports and perform Search and drill down operations on them. If shared users try to change the dashboard in any way, they will be asked to clone the dashboard with a new name. Cloning the dashboard breaks the link with the original dashboard. If the user wants access to the original dashboard, then the user who created the dashboard must share it again.
- For shared dashboards, run the report once, so that all users see the same data.
- A shared dashboard cannot be hidden from view.

Advantages of a shared dashboard folder:

- The dashboard owner can seamlessly propagate changes to the users with whom the dashboard is shared.
- An organization can quickly standardize on a set of dashboards created by experts.
- The report to populate the dashboard is run once if the report is run in inline mode. This uses less system resources

Creating a Shared Dashboard

Complete these steps to create a shared dashboard folder:

1. Go to **DASHBOARD** and click **New** to create a dashboard folder.
2. In the **Create Dashboard Folder** dialog box, enter a **Name** for the dashboard folder.
3. Select the **Everyone in current org** checkbox to share the dashboard folder with everyone in the current organization.
   a. To share with selected users/groups, click the edit icon. Select **Users** (CMDB Users) and/or **AD Groups** from the left column, then select individual users from the middle column and shuttle them to the **Selections** column.
   b. Click **Continue**. The selected users and groups will be able to access the shared dashboard and its contents.
4. Click the edit icon next to **Exclude** to exclude sharing with selected users.
   a. Select **Users** (CMDB Users) and/or **AD Groups** from the left column, then select individual users from the middle column and shuttle them to the **Selections** column.
   b. Click **Continue**. The excluded users will not be able to see or access the shared dashboard folder.
5. Click **Save**. The dashboard folder will have a icon – this indicates that it is a shared folder. At this point, you can create dashboards for the shared dashboard folder. See Creating a new dashboard under a folder.

Cloning a Shared Dashboard Folder

In shared dashboard, you can perform the refresh, drill down, and search operations. If you want to make any other changes, such as add a dashboard, change display settings, or delete the dashboard, then you must clone the shared dashboard folder. Once cloned, the link between the original shared

dashboard and the cloned dashboard will be broken. This means that changes to the original shared dashboard will not be reflected in the cloned dashboard.

Complete these steps to clone a dashboard folder.

1. Log in to FortiSIEM.
2. Go to **Dashboard** and select the dashboard folder that has been shared with you from the drop-down list.
3. Any changes you attempt to make, such as add a dashboard, change display settings, or delete the dashboard, will open the **Clone Dashboard Folder** dialog box.
4. Enter a new **Folder Name** in the **Clone Dashboard Folder** dialog box.
5. Click **Save**.

You can now make your own changes to the dashboards in the cloned dashboard folder.

Deleting a Dashboard

Note: Built-in dashboards cannot be deleted.

Complete these steps to delete a user-created dashboard:

1. Go to **DASHBOARD** tab.
2. Select the dashboard folder drop-down list. The dashboards belonging to that folder will display.
3. Select the dashboard to delete from the top menu and click the **x**.

Deleting a Dashboard Folder

Note: Built-in dashboard folders cannot be deleted.

Complete these steps to delete a user-created dashboard folder:

1. Go to **DASHBOARD** tab.
2. Select the dashboard folder from the folder drop-down list and click the **x**.

Starting Dashboard Slideshow

Make sure that you have created the slideshow templates before starting a slideshow. See Dashboard Slideshow Settings.

Complete these steps to start a dashboard slideshow:

1. Go to **DASHBOARD** tab.
2. Click the dashboard folder drop-down list and click **Start Slideshow** to select the configured slideshow.

The slideshow starts in full screen mode. To exit full screen mode, click the **Exit Full Screen (Esc)** button.

3. To return to the dashboard page, click button on the top-right.

Widget Dashboard

A Widget Dashboard displays a graphical view of FortiSIEM reports. The reports can be from CMDB data or Event data. The reports can be Top N type aggregated reports or non-aggregated reports, likely displaying raw messages. Aggregated reports can be displayed in various forms: gadgets, bar, donuts, tables, line, stacked line, scatter plot, heat maps, tree maps, and geo-maps.

- Creating a Widget Dashboard
- Data Source
- Populating a Widget Dashboard
- Modifying Widget Dashboard Layout
- Modifying Widget Information Display
- Searching in a Widget Dashboard
- Drill-down into a Widget
- Exporting Widget Dashboard Definition
- Importing Widget Dashboard
- Forcing a Refresh

Creating a Widget Dashboard

When you create a new dashboard, choose Widget Dashboard as the **Type**.

Data Source

All Event data and CMDB Data can be used to populate a Widget Dashboard.

Populating a Widget Dashboard

You can add up to a maximum of 20 event reports or CMDB reports to a Widget Dashboard. Complete these steps to add a report to a Widget Dashboard:

1. Make sure the report of your choice exists. CMDB Reports can be found in **CMDB** > **CMDB Reports**. Event Reports can be found in **RESOURCES** > **Reports**.
   - If the report exists, then run the report to make sure that data is accurate and the fields you want to see are present. Do not choose too many columns in a dashboard view, as may clutter the dashboard.
   - If the report does not exist, then create the report and **Save** it. You can save it in a folder for easy navigation.
2. Go to **DASHBOARD** tab. Select the dashboard folder from the drop-down list.
3. Click **+** below the dashboard folder drop-down list. Select the report from the menu and click **>** to display it on the dashboard.
   The report will run and the results will be displayed in the Widget Dashboard.

Modifying Widget Dashboard Layout

You can select one of two Widget Dashboard layouts from the **Layout** drop-down list on top-right menu of dashboard:

- **Tile view** - widgets can be of non-uniform size and can be dragged around the dashboard space.
- **Column view** - widgets are arranged in a fixed number of columns (1 or 3) in the dashboard space.

Modifying Widget Information Display

1. Click the tools icon on the top-right of the widget to open the **Settings** page.
   a. To change the title, enter a new **Title**.
   b. To change the chart format, choose a new **Display** from the available choices, only if it is relevant for the report. FortiSIEM Charts and Views describes the available charts.
   c. To change the time duration of the report, choose a different **Time**.
   d. To modify the size of the widget, choose a different **Width** and **Height**. Widgets displayed in tabular formats typically take more width and height compared to Single Line view.
   e. To display more or fewer entries, choose the appropriate **Result Limit**. Note that a larger result limit may require more width and height.
   f. For a Service Provider installed in a Super/Global view, choose the **Organizations** to run the report for. This option is available if you run reports from the Super/Global view.
   g. To change the chart refresh interval, select the appropriate **Refresh Interval**. Reports will be re-run periodically at specified refresh intervals.
   h. To change the **Trend Interval**, select one of the following from the drop-down list:
   Auto - (Default) Query is handled normally.
   Hourly - Select this configuration for proper chart display if you want to check the data hourly.
   Daily - Select this configuration for proper chart display if you want to check the data daily.
   Weekly - Select this configuration for proper chart display if you want to check the data weekly.
   i. Select **Display Settings** for the specific **Display** chosen before. FortiSIEM Charts and Views describes the required settings for each of the charts.
   j. If the report contains nested query report, select a time range from “Nested Time” drop-down list for the inner query.
2. Click **Save**.

Searching in a Widget Dashboard

You can search data for specific event attributes simultaneously in all the widgets in a dashboard. To do this, click the Filter button on left and select the values. You can search on any field that appears in at least one widget on a dashboard.

For example, if you choose to Filter on IP = 10.1.1.1, then only the entries for Source IP or Destination IP or Host IP = 10.1.1.1 are shown on all the widgets.

Note the following:

- The values you can search are pre-populated by searching through the data in various widgets. You can only search for a value if it is present in any widget on the dashboard.
- Without filters, a dashboard shows pre-computed results – so they load quickly. However, when you search, all the reports in the Widget Dashboard are run in an ad hoc mode. Subsequently, search results may return relatively slowly.

Drill-down into a Widget

To analyze the results shown in a widget further, click the magnifying glass icon on the top-right of the widget. This will take you to the **ANALYTICS** tab. The same query will be re-run slightly differently:

- Time conditions are maintained
- Filter conditions are maintained
- Aggregation conditions are removed and the field values and the raw messages are shown directly

This enables users to better understand the widget results. For example, if a column like AVG(CPU) is high over a time duration, then drill down shows all the individual CPU values over the time duration so that you can quickly go to the time when CPU spiked.

Exporting Widget Dashboard Definition

If you want to create the same dashboard in another FortiSIEM, or share with another user, or create the same dashboard for another Organization in a Service Provider FortiSIEM instance, use the export/import feature.

To export the dashboard definition, click the export button on top-right. The definition will be saved in a file, which then can be imported into another FortiSIEM Widget Dashboard.

Importing a Widget Dashboard

To import a dashboard widget, click the import button on top-right and select the file. The imported file must be exported from another FortiSIEM Widget Dashboard.

Forcing a Refresh

To update the whole dashboard, click the refresh icon on the top-right menu.

Summary Dashboard

A Summary Dashboard displays the metrics for many devices in a spreadsheet format. Unlike the widget dashboard that shows a few metrics in one widget, a Summary Dashboard can simultaneously show many more metrics. This often allows rapid diagnostics. FortiSIEM calculates and maintains these metrics in an in-memory database inside Query Master module.

Note: RBAC for Summary dashboard is controlled by hiding by Device Group and not by Data Condition. If you want to hide a group of devices in Summary dashboard for a role, hide the Device Group in the role. The user should not be able to choose the devices from the Device Group.

- Creating a Summary Dashboard
- Data Source
- Managing Devices in a Summary Dashboard
- Changing Display Columns
- Changing Refresh Interval
- Forcing a Refresh
- Searching a Summary Dashboard

Creating a Summary Dashboard

When you create a new dashboard, choose Summary Dashboard as **Type**.

Data Source

The source of data in a Summary Dashboard is the performance and availability monitoring metrics and incidents. To see the metrics that can be displayed, click the column icon. The left table shows the event types and the middle table shows the available metrics for the selected event type. These metrics can be displayed in a Summary Dashboard. Custom attributes from custom monitoring may also be displayed after they are defined.

In addition to metrics, the following are shown:

- Performance, Availability and Security incident counts
- Performance, Availability and Security Status each derived from respective incident severities

Managing Devices in a Summary Dashboard

When you create a Summary Dashboard for the first time, no devices are displayed.

Complete these steps to add devices to the dashboard:

1. Click the device icon.
2. Choose devices to display from the **Available Devices** list and click the right arrow button.
3. Click **OK**.

If the devices do not display in the dashboard, check the pre-defined filters for **Severity**. You may want to set Severity to **All Severities** to see the device recently added. When there are a large number of devices being monitored, you may want to show only the devices with **Critical + Warning** severity, as they would need attention.

Complete these steps to remove a device from the dashboard:

1. Click the device icon.
2. Choose devices to display from the **Selected Devices** list and click the left arrow button.
3. Click **OK**.

Changing Display Columns

Complete these steps to change the pre-defined set of display columns in the Summary Dashboard:

1. Click the columns icon.
2. To remove a column, choose the column from the **Selected Columns** list and click the left arrow button.
3. To add a new column:
   a. Select an **Event Types** on the left-most tab
   b. Choose the **Columns** from the middle tab corresponding to the selected **Event Types**.
   c. Click right arrow.
4. Click **OK**.

Changing Refresh Interval

Select the refresh interval from the drop-down menu on the top-right menu.

Forcing a Refresh

To update the whole dashboard click the refresh icon on top-right menu.

Searching a Summary Dashboard

You can search for specific devices by entering values in the search field.

1. Select the fields to search by clicking the search icon.
2. Enter the search string in the search field.

You can also filter from the three pre-defined drop-down lists:

- Severity
- Organizations
- Locations

You can set the location property for devices from **ADMIN** > **Settings** > **Discovery** > **Location**.

Business Service Dashboard

In FortiSIEM, you can define a Business Service as a container of Devices (Go to **CMDB** > **Business Services**, then click **New**). A Business Service Dashboard provides an overview of the health of the business service by showing the related Incidents and impacted devices.

- Creating a Business Service Dashboard
- Data Source
- Adding/Removing Business Service to the Dashboard
- Summary View
- Drilldown View
- Filtering Summary View
- Filtering Drilldown View
- Changing Refresh Interval
- Forcing a Refresh

Creating a Business Service Dashboard

When you create a new dashboard, choose Business Service Dashboard as **Type**.

Data Source

The only source of data for this dashboard is incidents triggering for the devices belonging to a Business Service.

Adding/Removing Business Services to the Dashboard

When you create a Business Service Dashboard for the first time, no Business Services are shown.

Complete these steps to add a Business Service to the dashboard:

1. Click the devices icon.
2. Select the Business Services from the **Available Services** Business Service list.
3. Click right arrow to move them to the **Selected Services** list.
4. Click **Save**.

Complete these steps to remove a Business Service from the dashboard:

1. Click the devices icon.
2. Select the Business Services to remove from the **Selected Services** list.
3. Click left arrow to move them back to the **Available Services** list.
4. Click **Save**.

Summary View

Business Service Dashboard has two views: Summary view and Drilldown view. The Summary view is the default view when you access the Dashboard.

The first level Summary view displays:

- Incident Counts By Severity and Top Impacted Devices across all Business Services.
- High and Medium Severity Incident Counts for each Business Service.

Click a specific Business Service in the first level to see the second level Summary view. This displays:

- Devices belonging to the Business Service that has triggered incidents.
- For each device:
  - Device Name
  - Device Type
  - Availability Status
  - Incidents and counts – you can click an Incident to see more details in a pop up. From there, you can take action on an incident (for example, drill down the incident on Incident page).

Drilldown View

Click the **Drilldown** button to display the Drilldown view of Business Services.

The first level Drilldown view displays the Incidents of each Business Service.

Click a specific Business Service in the first level to display the second level Drilldown view. It displays the Summary dashboard view of each device belonging to the selected Business Service.

Click the **Overview** button to get back to the Summary view.

Filtering Summary View

In the first level Summary view, you can filter the information displayed by Incident Severity and Organizations (for Service Provider deployments). Choose the values from the respective drop-down lists.

In the second level Summary view, you can filter the information by Device name and type.

Filtering Drilldown View

In the first level Drilldown view, you can filter the information by Organizations (for Service Provider deployments). Simply choose the values from the drop-down list.

In the second level Drilldown view, you can filter the information by Device name and type.

Changing Refresh Interval

Select the refresh interval from the drop-down menu on top-right.

Forcing a Refresh

To update the whole dashboard, select **Refresh Now** on top-right.

Identity and Location Dashboard

In many situations, you would like to know which user is using an IP address and where the user connected from. The Identity and Location Dashboard provides you an audit trail of this information by providing the linkage between:

- Network Identity - IP address, or MAC address
- User identity - user name, host name, or domain
- Location - a wired switch port, a wireless LAN controller, or VPN gateway

The following sections provide more information about Identity and Location Dashboard:

- Data Source
- Adding to the Data Source
- Viewing Identity and Location Dashboard
- Searching for Specific Information

Data Source

This association is built over time by combining information from the following events:

- **Active Directory logon events** – such as Win-Security-540 and Win-Security-4624 that provide IP Address, User, and Domain information
- **DHCP events** – these provide IP, MAC address, and sometimes host name information. Events include:
  - WIN-DHCP-IP-LEASE-RENEW
  - WIN-DHCP-IP-ASSIGN
  - FortiGate-event-DHCP-response-Request
  - FortiGate-event-DHCP-response-Ack
  - AO-WUA-DHCP-IP-LEASE-RENEW
  - AO-WUA-DHCP-IP-ASSIGN
  - Linux_DHCPACK
  - Generic_DHCPACK
  - Cradlepoint-dhcp-updated
- **VPN logon events** – these provide IP and user information. Events include:
  - ASA-713228
  - Juniper-SecureAccess-Session-Start
  - Cisco-VPN3K-IKE/25
  - ASA-722022
  - ASA-713049-Client-VPN-Logon-success
  - FortiGate-ssl-vpn-session-tunnel-up
  - ASA-113019

- **WLAN logon events** – these provide IP and user information. Events include:
  - Aruba-1014-wlsxNUserEntryCreated,
  - FortiGate-Wireless-Client-IP-Assigned
  - Cisco-WLC-53-bsnDot11StationAssociate
- **Cloud Service logon events** – these provide IP and user information. Events include:
  - AWS-CloudTrail-SIGNIN-ConsoleLogin-Success
  - Google_Apps_login_login_success
  - Salesforce_Login_Success
  - OKTA-USER-AUTH-LOGIN-SUCCESS
  - MS_OFFICE365_UserLoggedIn_Succeeded
- **AAA Authentication events** - these provide IP and user information. Events include:
  - Win-IAS-PassedAuth
  - CisACS_01_PassedAuth
- **FortiSIEM Discovery events** – these provide IP, user, and location information. Events include:
  - PH_DISCOV_HOST_LOCATION
  - PH_DISCOV_CISCO_WLAN_HOST_LOCATION
  - PH_DISCOV_ARUBA_WLAN_HOST_LOCATION
  - PH_DISCOV_GEN_WLAN_HOST_LOCATION

Adding to the Data Source

You can modify the file `/opt/phoenix/config/identityDef.xml` file to add new events. Remember to restart the `phIdentityMaster` and `phIdentityWorker` modules on all nodes after the changes are done.

Viewing Identity and Location Dashboard

Identity and Location Dashboard is a spreadsheed style tabular dashboard that displays the following information:

- **IP Address** - IP address of a host whose identity and location is recorded in this result. You can view IP addresses with country flags in a map by clicking **Locations**.
- **MAC Address** - MAC address of the host
- **User Name** - User associated with this IP Address. Obtained from one of these event types in the Data Source section.
- **Host Name** - Host Name from which IP Address was used. Obtained from one of these event types in the Data Source section.
- **Domain** - Provides context for the User. The Information displayed here depends on the logon event type it was obtained from:
  - Windows Domain Logon: Domain name
  - VPN Logon: reporting IP address of the VPN gateway
  - WLAN Logon: reporting IP address of the WLAN controller
  - AAA Logon: reporting IP of the AAA server
- **VLAN ID** - For hosts directly attached to a switch, this is the VLAN ID of the switch port,

- **Connected to** - For hosts attached to a switch port, this is the switch name, reporting IP address, and interface name,
- **First Seen** - The time at which this entry was first created in the FortiSIEM Identity and Location database,
- **Last Seen** - The time at which some attribute of this entry was last updated. If there is a conflict, for example, a host acquiring a new IP address because of DHCP, then the original entry is closed and a new entry is created. A closed entry will never be updated.
- **Organization** - Displays the Organization to which the IP address belongs for Service Provider installations in a Super/Global View.

Searching for Specific Information

You can search in two ways:

- **Search single field** - use the search box.
  - For Time Range, choose the time ranges in the time range field on the top right
  - For other fields, select the fields in the Search area and enter the value to be searched
- **Search multiple fields at the same time** – use the Filter area
  - Select the field, enter the searched value and click **OK**. The condition will diaplay on the top
  - Select another field and so on.
  - You can clear a condition by clicking the **x** button.

Interface Usage Dashboard

This dashboard provides an overview of the usage of individual interfaces of Router and Firewall devices. The dashboard has three levels:

- The Top view displays device level metrics in a tabular form.
- Once you select a device in the Top view, the middle table shows the basic interface level metrics such as received and sent bytes.
- You can drill-down and get Application level usage and QoS metrics for a specific device interface. To do this, select a device in the Top view and a specific interface in the middle view.

The following sections provide more information about the Interface Usage Dashboard:

- Data Source
- Adding/Removing Devices and Interfaces to the Dashboard
- Viewing Device Level Metrics
- Viewing Interface Level Metrics
- Viewing Application Usage
- Viewing QoS Statistics
- Drill-down from Widgets
- Modifying Widget Information Display
- Changing Refresh Interval
- Forcing a Refresh

Data Source

This dashboard applies to network devices: Routers/Switches and Firewalls.

- Top View - Device level metrics are sourced from Ping monitoring and SNMP.
- Middle View – Basic interface level metrics are also sourced from SNMP.
  - The sent and receive metrics are available for all network devices implementing MIB2 (RFC 1213).
  - Latency, Jitter, and Loss are available for FortiGate Firewalls/UTM devices via SNMP – see FORTINET-FORTIGATE-MIB: `fgSystem.fgLinkMonitor` (see note below on configuration restriction).
- Bottom View
  - Application Usage is available from Netflow
  - QoS values are available for FortiGate Firewalls/UTM devices via SNMP – see FORTINET-FORTIGATE-MIB: `fgIntf.fgIntfBcs.fgIntfBcInTable.fgIntfBcInEntry` for ingress and `fgIntf.fgIntfBcs.fgIntfBcTable.fgIntfBcEntry` for egress.

Configuring Latency, Jitter and Loss

FortiGate SNMP metrics report Latency, Jitter. and Loss by link ID, which is different from SNMP interface ID. FortiSIEM requires that the user configures the link ID to be identical to SNMP interface ID.

SNMP interface IDs are available by running the SNMP walk command: `snmpwalk -v2c -c<cred> <ip> ifName`. In the output, the integer after `ifName` is the interface ID.

```
#snmpwalk -v2c -cpwd 10.1.1.1 ifName
IF-MIB::ifName.1 = STRING: port1
IF-MIB::ifName.2 = STRING: port2
IF-MIB::ifName.3 = STRING: port3
```

Here the SNMP interface ID of port1 is 1, SNMP interface ID of port2 is 2 and so on.

Use the SNMP interface ID in the `config system virtual-wan-link` command – see the examples below:

This is a basic example where the port, health check members and SNMP index can align naturally, however this is not likely to be the case with all configurations.

```
#config system virtual-wan-link
  set status enable
  config members
    edit 1
      set interface port1
    next
    edit 2
      set interface port2
    next
  end

#config health-check
    edit "HC_Backoffice"
                set server "8.8.8.8"
                set update-static-route disable
                set members 1 2
     next
```

As mentioned, to ensure that the Interface SNMP Index ID corresponds to that of the virtual WAN link and the health check, it is required that SNMP index must align. This example and description shows how to configure a FortiGate for SDWAN monitoring with FortiSIEM.

1. The interface should specify the SNMP index, for example, `105 (set snmp-index 105)` :

   config system interface

   edit "port4"

   set vdom "root"

   set ip 10.1.31.10 255.255.255.240

   set allowaccess ping https ssh

   set type physical

   set netflow-sampler both

   set inbandwidth 50192

   set outbandwidth 50192

   set ingress-shaping-profile "test_Internal"

set egress-shaping-profile "test_Internal"
set alias "MPLS"
set snmp-index 105
set preserve-session-route enable
next
end

2. The member ID in the virtual WAN link must be same as the SNMP index associated with the Interface, for example, `105`.

config system virtual-wan-link
set status enable
config members
edit **105**
set interface "ha"
set gateway 10.1.31.1
set comment "MPLS"
next
.....
.....
end
end

3. The member ID should be added to a health check, again in this example it is `105`.

config health-check
edit "TEST_Backoffice"
set server "10.10.33.240" "10.10.1.240"
set interval 5
set update-cascade-interface disable
set update-static-route disable
set members 1 2 **105**
next
end

4. When monitoring Latency, Jitter and Loss via SNMP it is now possible to identify the Interface it is associated with the health check.

[snmpwalk -v2c -c **{password} {HostIp}** 1.3.6.1.4.1.12356.101.4.9.2.1
SNMPv2-SMI::enterprises.12356.101.4.9.2.1.3.7 = Gauge32: **105**
SNMPv2-SMI::enterprises.12356.101.4.9.2.1.5.7 = STRING: "20.078" (latency)
SNMPv2-SMI::enterprises.12356.101.4.9.2.1.6.7 = STRING: "0.736" (Jitter)
SNMPv2-SMI::enterprises.12356.101.4.9.2.1.9.7 = STRING: "0.000" (Loss)

Adding/Removing Devices and Interfaces to the Dashboard

When you create an Interface Usage Dashboard for the first time, no devices are displayed.

Complete these steps to add a device to the dashboard:

1. Click the devices icon.
2. Select the Organization and then click the **Firewall** or **Router Switch** folder.
3. Select a device and its interface of interest.
4. Click the right arrow.
5. Click **Save**.

Complete these steps to remove a device from the dashboard:

1. Click the devices icon.
2. Select the **Device**/**Interface** pair from the selected list.
3. Click the left arrow.
4. Click **Save**.

This dashboard is data driven. That means the dashboard will be populated only if the metrics are present. First, create a Summary dashboard and see if the devices are present in that dashboard and display values. Then, you will see them in this dashboard.

Viewing Device Level Metrics

The Top view displays Device level metrics. The metrics are averaged over three minute intervals. To see the trend, click the trend icon next to the numbers.

Viewing Interface Level Metrics

Once you select a device in the Top view, the middle table displays the interface level metrics for that device. The metrics are averaged over three minute intervals. To see the trend, click the trend icon next to the numbers.

Viewing Application Usage

Complete these steps to see the Application Usage for an interface:

1. Select a device in the Top view.
2. Select an interface in the Middle view.
3. Click the **Application Usage** tab.

Viewing QoS Statistics

Complete these steps to see the QoS Statistics for an interface:

1. Select a device in the Top view.
2. Select an interface for the selected device in the Middle view.
3. Click the **QoS Statistics** tab.

Drill-down from Widgets

Click the magnifying glass icon on a widget. This will take you to the **ANALYTICS** tab with the values populated. From there, you can analyze the data in more depth.

Modifying Widget Information Display

Follow the steps in Widget Dashboard > Modifying widget information display.

Changing Refresh Interval

Select the refresh interval from the drop-down menu on top-right.

Forcing a Refresh

To update the whole dashboard, select the refresh icon on the top-right menu.

PCI Logging Status Dashboard

A PCI Logging Status dashboard provides an overview of which devices in PCI are logging and logging correctly. The devices are displayed by CMDB Device Groups (for example Windows, Linux, Firewalls, and so on) and by Business Units.

- Setting Up Data Source
- Creating a Dashboard
- Analyzing Dashboard Data
- Searching Dashboard Data

Setting Up Data Source

Data source setup includes the following steps:

1. Creating CMDB Devices
2. Assigning Devices to Business Units
3. Assigning Devices to PCI Business Service
4. Specifying the Criteria for Logging Correctly
5. Specifying the Violation Time Limits

Creating CMDB Devices

The devices must be available in CMDB for displaying in the dashboard. This can be done in any of the following ways:

Manually

1. Go to **CMDB** > select the Device Group > click **New**.

Discovery

1. Create the credentials in **ADMIN > Setup > Credentials**.
2. Discover in **ADMIN** > **Setup** > **Discovery**.

Device Import

1. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
2. Click **New** and choose **Type** as "Device" and **Direction** as "Inbound".
3. Choose the **File Path** on the Supervisor node and place the CSV file there.

4. For **Content Mapping**, click the edit icon.
   a. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.
      i. Enter Source CSV column Name for **Source Column**.
      ii. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist.
         i. Enter a name for the **Destination Column** of the property from the drop-down list.
         ii. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.
      iii. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.
      iv. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.
      v. Click OK.
   b. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.
5. Click **Save**.
6. Select the Instance and click **Run**.

Assigning Devices to Business Units

For the PCI Logging dashboard to display the devices logging and logging correctly by business units, the Business Unit property needs to be set for a device. This can be done in any of the following ways:

Manually

1. Go to **CMDB** > select one or more devices > click **Edit** and set the Business Unit.
2. Click **Save**.

Device Import

1. Prepare a CSV file containing Device Host Names and Business Unit as two columns. Note that the Device host names must match the host names in CMDB, if they are present.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New** and choose **Type** as "Device" and **Direction** as "Inbound".
4. Choose the **File Path** on the Supervisor node and place the CSV file there.
5. For **Content Mapping**, click the edit icon.
   a. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.
      i. Enter Source CSV column Name for **Source Column**
      ii. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist
         i. Enter a name for the **Destination Column** of the property from the drop-down list.
         ii. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.

iii. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.

iv. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.

v. Click **OK**.

b. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.

6. Click **Save**.
7. Select the instance and click **Run**.

Assigning Devices to PCI Service

Devices in the PCI Logging Status Dashboard belong to the PCI Business Service. Assigning Devices to the PCI Service can be done in any of the following ways:

Manually

1. Go to **CMDB** > **Business Services** > **Compliance** > select the PCI Service > click **Edit** and add **Devices**.
2. Click **Save**.

Device Import

1. Prepare a CSV file containing Device Host Names and isPCI property. Host names must match the host names in CMDB. The **isPCI Device Property** takes TRUE or FALSE values.
2. Go to **ADMIN** > **Settings** > **General** > **External Integration**.
3. Click **New** and choose **Type** as "Device" and **Direction** as "Inbound".
4. Choose the **File Path** on the Supervisor node and place the CSV file there.
5. For **Content Mapping**, click the edit icon.
   a. For **Column Mapping**, click **+** and enter the mapping between columns in the **Source** CSV file and the **Destination** CMDB.
      i. Enter Source CSV column Name for **Source Column**
      ii. Check **Create Property if it Does not Exist** to create the new attribute in FortiSIEM if it does not exist
         i. Enter a name for the **Destination Column** of the property from the drop-down list.
         ii. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite it's current value.
      iii. If the property exists in the CMDB, select FortiSIEM CMDB attribute for **Destination Column**.
      iv. Select **Overwrite Existing Value** if the property exists in the CMDB, but you want to overwrite its current value.
      v. Click **OK**.
   b. For **Data Mapping**, click **+** and enter the mapping between data values in the external system and the destination CMDB.
6. Click **Save**.

7. Select the instance and click **Run**.

Note: Device Import options in Assigning Devices to Business Units and Assigning Devices to PCI Service can be combined. So it is possible to have a single file with three columns: Host Name, Business Unit, and isPCI.

Specifying Criteria for Logging Correctly

To specify a criteria for logging correctly, define the following:

- **Correctly Logging Reports** – these specify the criteria for devices in a device group to be correctly logging Authentication, FIM, and Change events. Reports must be defined separately for each CMDB device group and each functional category: Authentication, FIM, and Change. Several Correctly Logging Reports are pre-defined in **RESOURCES** > **Reports** > **Function** > **Compliance** > **Compliance Logging Policy**.
- **PCI Logging Policy** – these specify whether a CMDB Device Group needs to correctly send logs in the various functional categories: Authentication, FIM, and Change. Currently, these three functional categories are fixed. PCI Logging Policies can be specified in **ADMIN** > **Settings** > **Compliance** > **PCI**. Several PCI Logging Policies are pre-defined.

Complete these steps to customize correctly logging criteria:

1. Define a report in **RESOURCES** > **Reports** > **Function** > **Compliance** > **Compliance Logging Policy**.
2. Create a PCI Logging Policy in **ADMIN** > **Settings** > **Compliance** > **PCI** and specify the new report.

If you create your own correctly logging report, then it must have the following well-defined structure:

- **Group By Criteria** must have Customer ID and Reporting Device Name.
- **Select Clause** must have Customer ID, Reporting Device Name, and Last Event Receive Time.
- **Filtering Criteria** must be specific to the CMDB Device Group (for example: Firewalls, Routers, Windows Server, and so on) and functional logging category (for example: Authentication, FIM, and Change).

Note: It is highly recommended to clone an existing correctly logging report and modify the Filtering Criteria.

Specifying Violation Time Limits

Specify the time duration after which a device is reported to be not logging or not logging correctly. Four properties are defined in **ADMIN** > **Device Support** > **Custom Properties**:

- **lastAuthTimeLimit** - time limit for authentication logs (default 1 day)
- **lastFIMTimeLimit** - time limit for FIM logs (default 1 day)
- **lastChangeTimeLimit** - time limit for authentication log (default 1 day)
- **lastLogTimeLimit** - time limit for sending any log (default 1 day)

Similar to any other device property, you can change the global defaults and set them on a per-device basis.

Creating a Dashboard

Once you setup the data sources following the steps described in Setting up data source, the dashboard must be created manually.

The dashboard is updated nightly at 12:00 am (Supervisor time). At that time, the Supervisor:

- Runs the reports specified in **ADMIN** > **Settings** > **Compliance** > **PCI**.
- Updates the last reporting times.
- Calculates violations using the thresholds defined in **ADMIN** > **Device Support** > **Custom Properties**.

When you open the PCI Logging Status dashboard, the results are displayed from the daily run of previous night.

Analyzing Dashboard Data

The PCI Logging Status Dashboard displays:

- **Logging** - Percentage of PCI devices logging within the time period lastLogTimeLimit (default 1 day).
- **Logging Correctly** - Percentage of PCI devices logging correctly.
- **Logging By Group** - Percentage of PCI devices logging correctly broken down by Device Group.
- **Logging Correctly By Group** - Percentage of PCI devices logging correctly broken down by Device Group.
- **Logging Correctly By Business Unit, Group** - Percentage of PCI devices logging correctly broken down by Device Group.

The displays are color coded as Red, Yellow, and Green according to the tunable thresholds defined in **Dashboard** > **Threshold Setting**. By default:

- Red – less than 50%
- Yellow – between 50% and 80%
- Green – higher than 80%

If you click the entries, the devices in violation are shown in a tabular format along with the last time they reported events in each category.

Searching Dashboard Data

The Dashboard data can be searched by any Device Property, for example a Business Unit defined in **ADMIN** > **Device Support** > **Custom Properties** with Search (check-box) enabled. Click the search field under a specific category and enter the property values. Matches are exact and case sensitive.

Managing Tasks

FortiSIEM supports Data Anonymization to hide Personally Identifiable Information including IP addresses, host names, user names and email addresses in external and internal logs, Incidents, and CMDB records based on the user role for a specific period of time.

After assigning the user to anonymize a role and creating a Data Anonymization approver (To create a requestor and approver, see Adding a New Role - Activation, Data Obfuscation, and Approver for configuration options), the work-flow is as follows:

1. The user creates a de-anonymization request and sends to the approver.
2. The approver receives an email notification.
3. The approver then verifies and accepts the request for a specific period by setting a validity date. (An approver may also reject a request specifying a valid reason.)
4. If approved, the user can see the de-anonymized data until the validity period.
5. After the validity period, the data is hidden again. To de-anonymize the data, create a new request.

The following procedures describe how a user can submit a task request and the Data Anonymization approver approves or rejects.

- Requesting a De-anonymization Request
- Approving a De-anonymization Request

Requesting a De-anonymization Request

You can send a de-anonymization request with justification, to a Data Anonymization approver, to de-anonymize the requested data for a specific period of time.

1. Go to **TASKS** > **Request** tab.
2. Click **New** to create a de-anonymization request.
3. Select the **Approver** from the drop-down to send this request.
4. Select the **Type** of de-anonymization request.
5. Enter the **Justification** for viewing the data.
6. Click **Save** to send the request to the Data Anonymization approver.

Approving a De-anonymization Request

When a user sends a de-anonymization request, the Data Anonymization approver receives an email notification. The approver can see the list of de-anonymization requests under the **Approval** tab on login. The approver then verifies the justification and provides approval.

1. Go to **TASKS** > **Approval** tab.
2. Select the request from the list or search using the search bar and choose the following options from the drop-down list on the right:
   - **Approve** to allow de-anonymization for a specific time period under **Valid Till** or **For** the date and time listed in the time stamp field. You can click the time stamp field to choose a different date and time. The default time is two days, if no date/time is selected.
   - **Reject** to reject the de-anonymization request specifying a valid **Reason**.
3. Click **OK** to send the approval/rejection.
   The user can see the **Status** of this request under the **Request** tab on login.

Note: Fortinet understands that multiple approvers can be selected in a request. Fortinet's behavior in these situations is to acknowledge the approver who first provides approval (or rejection), and ignore any further responses. Furthermore, any approval or rejection is final, meaning it cannot be updated or changed.

If there is an approval for a task, but the another new request for the same task is sent again and another approval is granted, the approval with the shortest expiration takes precedence in this situation.

FortiAI

- Overview
- OpenAI Integration and Disclaimer
- How to ask FortiAI to Create a Report
- Anonymizing Sensitive Data
- FortiAI GUI Interface

Overview

FortiAI is available by clicking the FortiAI icon ( ) in the upper right corner of the UI.

FortiAI can be invoked from the following places in the GUI:

- **Analytics > Search > Raw message** column
- **Incidents > List By Time >** *<Select an Incident >* **> Action**
- **Incidents > List By Time >** *<Select an Incident>* **> Incident Details > Trigger Events > Raw Message**
- **Incidents > Risk > Entity** *<Drill down>* **>** *<Select an Incident>* **> Actions**
- **Incidents > Risk > Entity** *<Drill down>* **>** *<Select an Incident>* **> Details > Trigger Events > Raw Message**
- **Incidents > Investigation >** *<Select an Incident>* **> ...**
- **Incidents > Investigation >** *<Select an Incident>* **> Events > Raw Message**
- **Admin > Settings > Notification Policy > New Policy > Action**

After the FortiAI icon has been clicked, a **FortiAI** window appears. In the Input field, enter your English language question, Security Operations Center (SOC) question, aggregation query, or raw message query, and hit the Enter key, or click the Send icon.

Responses from questions are taken from 7.2.2 Product documentation and internal knowledge base articles.

FortiAI responds to the following Security Operations Center (SOC) queries:

- *Get FortiSIEM health* – This retrieves the current health of FortiSIEM nodes including Supervisor, Worker and Collector.
- *Get the latest known vulnerabilities* – This retrieves the list of vulnerabilities in your environment known to FortiSIEM. To get this data, you must enable FortiSIEM to collect data from FortiClient/EMS or vulnerability scanners.
- *Get my FortiSIEM environment* - This retrieves information on your FortiSIEM environment.
- *Get latest 10 high severity Incidents* - This retrieves the most recent top ten high severity incidents.
- *Get most frequent 10 Incidents* - This retrieves the 10 most frequent incidents.
- *Get Top 10 risky users* - This retrieves the top 10 users with risks.

- *Get Top 10 risky devices* - This retrieves the top 10 devices with security risks.

In the case of a report query, validated XML code is provided. You can push this code to the **Analytics** page by clicking on the **Action** drop-down option, selecting "Run on Analytics" (which will take you to the **Analytics** page). On the **Analytics** page, click **Run** to run the provided report. Incident analysis provided by OpenAI/ChatGPT-4 can be added to Incident Comments.

After FortiAI has responded, an **Action** drop-down option "Ask again" option is available in your previous inquiry dialogue windows. The "Ask again" action will paste the original inquiry you sent into the FortiAI Input field so that you can use it as a basis for modification, or use it as a basis to view other similar pre-selected questions (by pressing the UP key in the dialog window).

Use the following table to construct your query.

Notes:

- The FortiAI can be configured by following the instructions here.
- Click the UP key at any time to select from any pre-selected questions or report based off the current input.

OpenAI Integration and Disclaimer

FortiAI lets you connect FortiSIEM to your own OpenAI account, using your own OpenAI license key. This integration will send data from your FortiSIEM to OpenAI and will show you responses from OpenAI. Fortinet does not verify or correct these responses and has no responsibility for them. OpenAI is operated by a third party, not Fortinet. You must exercise discretion and independently verify any information or recommendations you receive from OpenAI before relying on them.

Note: FortiAI uses GPT3.5-Turbo and GPT4. Your OpenAI API key must support access to these models.

How to ask FortiAI to Create a Report

Query Type	Construct
Aggregation Query	**Create a report to show** <list> **where** <constraint>, **group them by** <list>, **order by** <list> Exact values have to be within single quotes. Examples: • **Create a report to show** the source IP, destination IP and total number of events **where** the reporting device IP belongs to the Firewall device group and event type belongs to the Permitted network connections group, **group them by** source IP, destination IP, and only show results for total number of events greater than 100, **order by** the number of events in descending order. • **Create a report to show** the destination IP, destination country and total number of events **where** the reporting device IP belongs to the Firewall device group, source IP is '10.1.1.1' and event type belongs to the Permitted network connections group, **group them by** destination IP, destination country and only show results for total number of events greater than 100, **order by** the number of connections in descending order.
Raw Message Query	**Create a report to show** <list> **where** <constraint>, **order by** <list> Exact values have to be within single quote Examples: • **Create a report to show** the event receive time, reporting device name, domain and user **where** event type is 'Win-Security-4624', **order by** event time in descending order. • **Create a report to show** the event receive time, reporting device name, domain and user **where** event type is Windows logon success, **order by** event time in descending order

In the **FortiAI** window, in the upper right corner, click **X** to exit FortiAI at any time.

Anonymizing Sensitive Data

When you ask ChatGPT for log and Incident analysis using the FortiAI menu option, then customer specific information is anonymized before being sent to ChatGPT. The returned results are converted back to the original values before being displaying to the user. Similar anonymization is performed when you invoke ChatGPT via Automation policy.

Note: If you manually enter a log or Incident and ask ChatGPT to analyze it, then the fields are *not* anonymized, since FortiSIEM does not parse the data on the fly. This method is not recommended.

The full list of anonymized event attributes is here.

A built-in report **FortiSIEM ChatGPT Queries** is provided. You can run this report to see what queries are sent to ChatGPT and how much it costs. The Query result shows the sensitive fields being anonymized.

FortiAI GUI Interface

- Expand/Reduce Input Field Size
- Maximize/Minimize FortiAI Window

Expand/Reduce Input Field Size

In the Input field, click the expand/reduce icon to increase/decrease the size of the input field.

Maximize/Minimize FortiAI Window

In the **FortiAI** window, in the upper right corner, click the window size icon to maximize/minimize the **FortiAI** window.

FortiSIEM Manager

FortiSIEM Manager can be used to monitor and manage multiple FortiSIEM instances. The FortiSIEM Manager needs to be installed on a separate Virtual Machine and requires a separate license.

Note: Only FortiSIEM Manager and FortiSIEM Supervisor instances 6.5.0+ are supported.

FortiSIEM Manager provides the following functionalities:

- Each FortiSIEM Instance needs to register to the FortiSIEM Manager. After successful registration, a 2-way HTTP(S) communication channel is set up between each Instance and the Manager.
- Incidents, License and Health information will be forwarded from each FortiSIEM instance to the FortiSIEM Manager. Incidents are forwarded in near-real time, Health information forwarded once every minute, and License information forwarded once every hour.
- FortiSIEM Manager retains Health information for the last 1 day. FortiSIEM Manager also stores Incidents and the latest License information in local PostGreSQL database. The number of incidents stored depends on the size of the local PostGreSQL database. Raw events are not stored in FortiSIEM Manager. When the user visits the **Triggering Event** tab on the **INCIDENTS** page, raw events are fetched on demand from the FortiSIEM Instance.
- All Incident status changes in each FortiSIEM instance are forwarded to the FortiSIEM Manager. If you create a new rule or make changes to a rule in a FortiSIEM instance, the changes are forwarded to the FortiSIEM Manager.
- From FortiSIEM Manager, you can do the following operations and the changes are propagated to the right FortiSIEM instance(s) with the right FortiSIEM Manager logged-in-user context:
  - Clear, Resolve and Add Comments to one or more Incidents
  - Disable one or more rules and change their severity.
  - Change the severity of an incident
  - Run FortiSOAR Playbooks and Connectors and update Incident Status and Comments
  - A one-click operation to log you into the appropriate FortiSIEM instance where an Incident occurred. This enables you quickly to investigate an Incident in depth.

Communication between FortiSIEM Manager and instances is via REST APIs over HTTP(S).

You have to upgrade FortiSIEM Manager first before upgrading all FortiSIEM Instances - this applies to both Content Update and Software Image Update.

For details in installing FortiSIEM Manager, see the VM or Hardware Installation Guides here.

For details on registering a FortiSIEM instance to the FortiSIEM Manager, see here.

For viewing health and license information in FortiSIEM Manager, see here.

The FortiSIEM Manager provides the following tools.

- FortiSIEM Manager Incidents
- FortiSIEM Manager CMDB Users
- FortiSIEM Manager Resources
- FortiSIEM Manager Admin

FortiSIEM Manager Incidents

When a correlation rule triggers, an incident is created in FortiSIEM. This section describes how to view and manage Incidents in FortiSIEM. There are 2 primary views:

- **Overview**: This view provides a "top down" view of the various types of Incidents and impacted hosts.
- **List View**: This tabular view enables the user to search incidents and take actions. (List by Time, Device, Incident)

To interact with an incident, see Acting on Incidents.

FortiSIEM can cross-correlate incident data and perform lookups on selected external ticketing/work flow systems. See Lookups Via External Websites.

FortiSIEM Manager Incidents Overview View

The Overview view provides a "top down" view of various types of Incidents and impacted hosts. Go to **INCIDENTS** > **Overview** to see this view. Overview can set as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list and **Overview** from the **Incident Home** drop-down list.

The panel is divided into four sections:

- **Top Instances by Incident** - displays Incident Counts by Instances and their Severity.
- **Incidents by Category** – displays Incident Counts By Function and Severity.
- **Top Incidents** – displays the Top Incidents sorted first by Severity and then Count.
- **Top Impacted Hosts** – displays Top impacted hosts by Severity or Risk Score.

To change the incident time range, choose the **Time Range** option on the top right. For Service provider installations, choose the appropriate Organizations on top right. By default, the data combined for all Organizations and the Organization is shown next to each host. This view will automatically refresh every minute by default. The refresh menu on top bar allows the user to disable the automatic refresh or choose a different refresh interval.

Incidents by Category

This pane shows the number of unique Security, Performance, Availability, and Change incidents that have triggered in the specified time range.

To drill into a specific category, click the number and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described inIncidents List View.

Top Incidents

This pane shows the Top Incidents, first by Severity and then by Count.

- Each box represents an Incident.
- The color of the box title reflects the Incident Severity.
- The number reflects the unique incidents that has triggered in the chosen time window.
- The entries inside the box represent the IP address and host names appearing in either the Incident Source or Incident Target.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each host and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Severity

This pane shows the Top Impacted Hosts, first by Severity and then by Count.

- Each box represents an impacted host (where an Incident has occurred during the specified time window).
- The color of the box title reflects the maximum of Severity over all Incidents.
- The number on the left of the box reflects the unique incidents that have triggered on the host in the chosen time window.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Incident Severity and then unique incident count. That means that the Red colored boxes (High Severity) appear first, then Yellow (Medium Severity), and finally Green (Low Severity). Within boxes of the same color, boxes with a higher number of Incident counts appear first. You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

Top Impacted Hosts by Risk Score

This pane shows the Top Impacted Hosts, first by Risk Score.

- Each Box represents an impacted host (where an Incident has occurred during the specified time window).
- The color of the box title reflects the Risk Score (80 and above is Red, 50-79 is Yellow, and less than 50 is Green).
- The number on the left of the box reflects the risk score.
- The entries inside the box represent the incidents that have triggered for that host.
- Boxes are ordered left to right by Risk Score. That means that Red colored boxes (High Risk) appear first, then Yellow colored boxes (Medium Risk), and Green colored boxes (Low Risk).
- You can scroll to the right.

To drill down, click the number in the left side bar or each incident and the matching incidents are displayed in a separate Incident List View. To return to the main view, click the **<** button. From this View, you can initiate the same actions as described in Incidents List View.

FortiSIEM Manager Incidents - List View

This tabular view enables the user to search incidents and take actions.

- Viewing Incidents
- Acting on Incidents

Viewing Incidents

To see this view, click **INCIDENTS** in the FortiSIEM header. By default, the **List by Time** view opens. The **INCIDENTS** view also allows you to filter data by device and by incident.

You can set **INCIDENTS** as the default view by selecting **User Profile > UI Settings** then choosing **Incidents** from the **Home** drop-down list. You can filter the **INCIDENTS** view further by choosing **List – by Time**, **List – by Device**, or **List – by Incident** from the **Incident Home** drop down list.

An incident's status can be one of the following:

- **Active**: An ongoing incident.
- **Manually Cleared**: Cleared manually by a user - the incident is no longer active.
- **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition.
- **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of **System Cleared**.
- **Externally Cleared**: Cleared in the external ticketing system.

The resolution for an incident can be:

- **Open**
- **True Positive**, or
- **False Positive**

When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.

The following sections describe the three views that are available through the **INCIDENTS** view:

- List by Time View
- List by Device View
- List by Incident View

List by Time View

The **List by Time** view displays a table of the incidents which have been active in the last 2 hours. The **Last Occurred** column contains the incidents sorted by time, with the most recent first. By default, the view refreshes automatically every minute. The refresh menu on the top bar allows the user to disable automatic refresh or choose a different refresh interval.

Unique to the **List by Time** view is a list of five time range buttons (15m 1h 1d 7d 30d) which appear above the paginator. They allow you to filter data by the last 15 minutes, 1 hour, 1 day, 7 days, or 30 days.

See the following table for information on the attributes shown for each incident. A caret will appear when you hover the cursor over some attributes for additional actions:

Attribute	Description
Severity	High (Red), MEDIUM (Orange), or LOW (Green).
ID	Incident's identification number.
Last Occurred	Last time this incident occurred.
Incident	Name of the incident. Click the caret icon for the following options: • Incident Details - Click to get more details on the incident. • Add to Filter - Click to add to filtered list.
Tactics	Name of the tactic involved with the incident.
Technique	Name of the technique involved with the incident. Click the caret icon for the following option: • Details - Click to get more Tactics and Technique information.
Reporting	Set of devices that is reporting the incident. Click the caret icon for the following options: • Quick info - Click to get information on the reporting device. • Device Health - Click to get more device health information. • Vulnerabilities - Click to view device vulnerability timeline. • Related Real-time Events - Click to check real-time events for the device. • Related Historical Events - Click to get older events for the device. • Real-time Performance - Click to get performance metrics. • Add to Filter - Click to add to filtered list. • Add to WatchList - Add IP address/host name to Watch List(s).
Source	Source of the incident (host name or IP address). Click the caret icon for the following options: • Quick info - Click to get information on the reporting device. • Device Health - Click to get more device health information. • Vulnerabilities - Click to view device vulnerability timeline. • Check Reputation - Click to check the source's reputation. • Related Real-time Events - Click to check real-time events for the device. • Related Historical Events - Click to get older events for the device. • Real-time Performance - Click to get performance metrics. • Add to Filter - Click to add to filtered list. • Add to WatchList - Add IP address/host name to Watch List(s). • Add to Application Group - Associate IP address with application group. See Working with Application Groups for more information.
Target	Target of the incident (host name or IP address or user). Click the caret icon for the following options:

Attribute	Description
	• Quick info - Click to get information on the reporting device. • Device Health - Click to get more device health information. • Vulnerabilities - Click to view device vulnerability timeline. • Check Reputation - Click to check the target's reputation. • Related Real-time Events - Click to check real-time events for the device. • Related Historical Events - Click to get older events for the device. • Real-time Performance - Click to get performance metrics. • Add to Filter - Click to add to filtered list. • Add to WatchList - Add IP address/host name/user to Watch List (s). • Add to Application Group - Associate IP address with application group. See Working with Application Groups for more information.
Detail	Other incident details, for example, Counts, Average CPU utilization, file name, and so on. Click the caret icon for the following option: • Check Reputation - Click to check the reputation based of the detail information.
Resolution	Current state of the incident. Click the caret icon for the following options: • Set Resolution to In Progress - Change the incident resolution to "In Progress". • Set Resolution to True Positive - Change the incident resolution to "True Positive". • Clear and set Resolution to False Positive - Change the incident to "False Positive".

To see the incident details, click the incident. Next, hover your cursor over the incident name, click the caret icon, and select **Incident Details**:

- **Incident Details** - Includes the full list of incident attributes in a separate pane.

Column	Description
Biz Service	Impacted biz services to which either the incident source or target belongs.
Case Status	Current status of the case associated with the incident.
Category	Category of incidents triggered.
Cleared Reason	For manually cleared incidents, this displays the reason the incident was cleared.
Cleared Time	Time when the incident was cleared.
Cleared User	User who cleared the incident.
Count	Number of times this incident has occurred with the same incident source and target criteria.
Detail	Event attributes that triggered the incident.
Event Name	Event name associated with the incident.
Event Type	Event type associated with this incident. All incidents with the same name have the same Incident Type.
External Cleared Time	Time when the incident was resolved in an external ticketing system.
External Resolve Time	Resolution time in an external ticketing system.
External Ticket ID	ID of a ticket in an external ticketing system such as ServiceNow, ConnectWise, etc.
External Ticket State	State of a ticket in an external ticketing system.
External Ticket Type	Type of the external ticketing system (ServiceNow, ConnectWise, Salesforce, Remedy).
External User	External user assigned to a ticket in an external ticketing system.
First Occurred	The first time that the incident was triggered.
Incident ID	Unique ID of the incident in the Incident database.
Incident Status	An incident's status can be one of the following: • **Active**: An ongoing incident. • **Manually Cleared**: Cleared manually by a user - the incident is no longer active. • **Auto Cleared**: Automatically cleared by the system when the rule clearing condition is met. Rule clearance logic can be set in the rule definition. • **System Cleared**: Cleared by the system. All non-security related incidents are cleared from the system every night at midnight local time, and will show a status of **System Cleared**. • **Externally Cleared**: Cleared in the external ticketing system.

Column	Description
Incident Title	A system default title or a user-defined title for an incident.
Last Occurred	The last time when the incident was triggered.
Notification Recipients	User who was notified about the incident.
Notification Status	Status of the Notification: Success or Fail.
Organization	Organization of the reporting device (for Service Provider installations).
Reporting	Reporting device.
Reporting Device Status	Status of the device: Approved or Pending. You must approve devices for the incidents to trigger, but they will still be monitored.
Reporting IP	IP addresses of the devices reporting the incident.
Resolution	The resolution for an incident can be: • **Open** (not defined or not known whether the incident is True Positive or False Positive) • **True Positive**, or • **False Positive** When an **Incident Status** is **Active**, Incident Resolution is **Open**. When an Incident is **Cleared**, then the user can set the **Incident Resolution** to be **True Positive** or **False Positive**. If you are changing the **Incident Resolution** to be **True Positive** or **False Positive**, then you must **Clear** the Incident.
Severity Category	Incident Severity Category: High, Medium or Low.
Source	Source IP or host name that triggered the incident.
Subcategory	Subcategory of the triggered incident. To add custom subcategories to an incident category, see here.
Tactics	Name of the tactics involved with the incident.
Tag	Name of the tag involved with the rule that triggered the incident.
Target	IP or host name where the incident occurred.
Technique	Name of the technique involved with the incident.
Ticket ID	ID of the ticket if created in FortiSIEM.
Ticket Status	Status of any tickets associated with the incident.
Ticket User	User assigned to a ticket if created in FortiSIEM.
View Status	Whether the Incident has been Read or Not.

- **Triggering Events** - this displays the set of events that triggered the incident. If an incident involves multiple sub-patterns, select the sub-pattern to see the events belonging to that sub-pattern. For **Raw Event Log** column, click **Show Details** from the drop-down to see the parsed fields for that event.

- **Rule Summary** - this displays the **Definition of Rule that Triggered the Incident** and the **Triggered Event Attributes**.

To close the incident details pane, click the highlighted incident, or click **X** in the upper right corner of the pane itself.

List by Device View

The upper pane of the **List by Device** view lists the devices that are experiencing incidents. In the list, the device can be identified by either an IP or a host name. The name of the device is followed by the number of incidents in parentheses. Click the device name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

List by Incident View

The upper pane of the **List by Incident** view lists the incidents detected by FortiSIEM. The name of the incident is followed by the number of incidents in parentheses. Click the incident name to see the incidents associated with the device. The lower portion of the view contains the same features and functionality as the **List by Time** view.

Acting on Incidents

The **Actions** menu provides a list of actions that can be taken on incidents. To see a Location View of the incidents, select **Locations** from the **Actions** menu. FortiSIEM has a built in database of locations of public IP addresses. Private IP address locations can be defined in **ADMIN** > **Settings** > **Discovery** > **Location**.

To change the incident attribute display columns in the List View, select **Change Display Columns** from the **Actions** menu, select the desired attributes and click **Close**.

You can perform the following operations using the **Actions** menu:

- Changing the Severity of an Incident
- Searching Incidents
- Clearing One or More Incidents
- Clearing All Incidents from the Incident View
- Disabling One or More Rules
- Adding or Editing Comments for One or More Incidents
- Exporting One or More Incidents into a PDF, RTF, or CSV File
- Emailing Incidents
- Executing a Playbook
- Running a Connector
- Resolve Incident

- Check Reputation
- Show in Instance

Changing the Severity of an Incident

1. Select the incident.
2. Select **Change Severity** from the **Actions** menu.
3. Select **Change to HIGH**, **MEDIUM**, or **LOW**.

Searching Incidents

1. Select **Search** from the **Actions** menu.
2. In the left pane, click an Incident attribute (for example, Function). All possible values of the selected attribute with a count next to it is shown (for example, Security, Availability and Performance for Function).
   Note: FortiSIEM Manager adds Manager Incident ID as a search parameter.
3. Select any value (for example, Performance) and the right pane updates with the relevant incidents.
4. Click and select other Incident Attributes to refine the Search or click **X** to cancel the selection.

Changing the Time Range for the Search

1. Select **Search** from the **Actions** menu.
2. Near the top of the left panel, click the time value.
3. Click **Relative** or **Absolute**:
   - If you click **Relative**, adjust the time value in the **Last** field.
   - If you click **Absolute** enter a time range. If you select **Always Prior**, enter a time period prior to the current time.

Saving the Search Criteria

Once you have performed your search, follow these steps to save the search criteria:

1. Click the **Save** icon ( ) which appears above the list of incident attributes, and to the right of **Search**.
2. In the **Save Search Filter under by Time as** dialog box, enter a name for the filter or accept the default. The default will be a time stamp value such as `Search Filters - 12/17/2019 17:04:59`.

The filter will appear in the **Search** (Search) drop-down list, for example:

- When saving a filter based on the List by Time View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Device View, it displays in the **Search** drop-down list.
- When saving a filter based on the List by Incident View, it displays in the **Search** drop-down list.

Clearing One or More Incidents

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.

3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Clear Incident** from the **Actions** menu.
5. Select whether the **Resolution** is **True Positive** or **False Positive**.
6. Enter a **Reason** for clearing.
7. Click **OK**.

Clearing All Incidents from the Incident View

You can remove all occurrences of selected incidents from the Incident View. This action can potentially span multiple pages.

1. Search for specific incidents and move them into the right pane.
2. Select **Clear All Incidents in View** from the **Actions** menu.
3. Select whether the **Resolution** is **True Positive** or **False Positive**.
4. Enter a **Reason** for clearing.
5. Click **OK**.

Disabling One or More Rules

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Disable Rule** from the **Actions** menu.
5. For Service Provider installations, select the Organizations for which to disable the rule.
6. Click **OK**.

Adding or Editing Comments for One or More Incidents

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Edit Comment** from the **Actions** menu.
5. Enter or edit the comment in the edit box.
6. Click **OK**.

Exporting One or More Incidents into a PDF, RTF or CSV File

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.

3. Press and hold the **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Export** from the **Actions** menu.
5. Enter or edit the comment in the edit box.
6. Select the **Output Format** and **Maximum Rows**.
7. Click **Generate**.
   A file will be downloaded in your browser.

Emailing Incidents

Incidents can be emailed to one or more recipients. Make sure that Email settings are defined in **ADMIN** > **Settings** > **System** > **Email**. Note that email notification from the Incident page is somewhat ad hoc and must be manually setup by the user after the incident has triggered. To define an automatic notification, create an Incident Automation Policy in **ADMIN** > **Settings** > **Automation Policy**. To email one or more incidents on demand:

1. Search for specific incidents and move them into the right pane.
2. Select the first incident.
3. Press and hold **Shift** key and select the last incident – all incidents between the first and the last are highlighted.
4. Select **Notify via Email** from the **Actions** menu and enter the following information:
   a. Send To – a list of receiver email addresses, separated by commas.
   b. Email template – Choose an email template. You can use the default email template, or create your own in **ADMIN** > **Settings** > **System** > **Email** > **Incident Email Template**.

Resolve Incident

You can directly resolve an incident by taking the following actions.

1. Select the incident.
2. From the **Actions** drop-down list, select **Resolve Incident**.
3. Select the resolution (Open, In Progress, True Positive, False Positive).
4. Click **OK**.

Check Reputation

FortiSIEM utilizes an external integration policy to perform a reputation check on incidents.

To create an external integration policy, navigate to **ADMIN > Settings > General > External Settings**. Click **New** to begin creating an external integration. For more information, see Configuring External Integration.

To perform a reputation check, take the following steps:

1. Select an incident.
2. Select **Check Reputation** from the **Actions** menu.

3. From the **Select Target** drop-down list, select the target you want the reputation check to be done on from the selected incident.
4. From the **Check from** drop-down list, select the reputation check policies to be applied to the target.
5. When done, click **Check**.
6. Click **View Result**.

Show in Instance

To show the incident from the Instance, take the following steps.

1. Select the incident.
2. Select **Show in instance** from the **Actions** menu.
3. Select **New windows** or **Current window**.

FortiSIEM Manager CMDB Users

The FortiSIEM Manager CMDB Users page contains information about the users of your system.

- FortiSIEM Manager CMDB Adding Users
- FortiSIEM Manager - Editing User Information

FortiSIEM Manager CMDB Adding Users

Complete these steps to add a user:

1. Navigate to **CMDB > Users**.
2. Click **New** to create a new user.
3. In the **New User** dialog box, from the **General** tab, enter the detailed information about this user:
   a. Add the user profile information including **User Name**, **Full Name**, **Job Title** and **Company**.
   b. Click the drop-down list to select the **Importance** of this user - "Normal", "Important", "Critical", or "Mission Critical".
   c. Enable **Active** if this is an active user.
   d. Enter the user's **Domain**.
   e. Enter the user's Distinguished Name **DN**.
   f. In the **Employee ID** field, enter the employee ID.
   g. From the **Manager** field, click **Select** and select the manager of the user.
   h. Click **Alias** to enter any alias information for the user.
      i. In the **Alias** field, provide the alias user name.
      ii. From the **Identity Provider** field, enter/select from AWS IAM, DUO, or Microsoft AD.
      iii. In the **Description** field, enter any additional information about the alias.
      iv. If another Alias is needed, in the **Row** column, click **+** to add another row for another alias, and repeat steps i-iii.
   i. Click **Save**.
4. Click the **Contact** tab to enter personal user contact information.
   a. Add user contact information to the appropriate contact information fields - **Work Phone**, **Mobile Phone**, **Home Phone**, **SMS**, **SMS Provider**, **ZIP**, **Email**, **Address**, **City**, **State**, and **Country** field.
   b. If your company uses S/MIME for email, make sure the **Email** field is filled out, and upload the S/MIME certificate in the **Certificate** field by clicking **Upload**, and selecting your certificate.
   c. Click **Save** when done.
5. Click **FortiSIEM Attributes** tab.
   a. For **User Unlock**, select **Unlock by Administrator** or **Delay next login for ## minutes**. If **Delay next login for ## minutes** is selected, enter the number of minutes the user will be unable to log into the system after five successive authentication failures.
   b. For **Idle Timeout**, enter the number of minutes after which an inactive user will be logged out.
   c. For **Password Reset**, enter the number of days after which a user's current password for logging in to the system will automatically expire. If left blank, the user's password will never expire.
   d. For **FortiSIEM Role**, enable by selecting the **FortiSIEM Role** checkbox.
      i. For **Mode**, select **Local** or **External**.
      If you select **Local**, enter and then reconfirm the user password. For **External**,

see Authentication Settings for more information about using external authentication.
Notes:

- If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.
- For local users, passwords must contain between 8 and 64 characters, and must include 1 letter, 1 numeric character and 1 special character.

ii. Select a **Default Role** for the user.
See the topic Role Settings for a list of default roles and permission. You can also create new roles, which will be available in this menu after you create them.

iii. Click **Save** when done.

Note:

- When viewing this user list as a Super global user, you may see repetitions of a few **User Names**, where those names exist in multiple Organizations. This can be determined by checking the contents of the Instance/Supervisor on FortiSIEM Manager.

FortiSIEM Manager - Editing User Information

Complete these steps to edit a CMDB user:

1. Complete these steps to edit a CMDB user:
2. Navigate to **CMDB > Users >**.
3. Click **Edit**.
4. In the **Edit User** dialog box, click the **General** tab to edit any available general fields about this user.
   a. Edit any available General fields.
   b. Click **Save** when done.
5. Click the **Contact** tab to edit any available personal user contact information.
   a. Edit any available Contact fields.
   b. Click **Save** when done.
6. Click **FortiSIEM Attributes** tab to edit FortiSIEM timeout or password reset configurations.
   a. Edit any available fields.
   b. Click **Save** when done.

See FortiSIEM Manager CMDB Adding Users for detailed information about the user fields.

You can also use the following function on the **Actions** menu:

1. **Unlock** - to unlock a user, select the user from the list and click **Actions** >**Unlock**.

FortiSIEM Manager Resources

The following sections provide the procedures for managing Resources from FortiSIEM Manager:

- FortiSIEM Manager Resources Rules
- FortiSIEM Manager Resources Connectors
- FortiSIEM Manager Resources Playbooks
- FortiSIEM Manager Resources - Event Types

FortiSIEM Manager Resources Rules

FortiSIEM continuously monitors your IT infrastructure and provides information to analyze performance, availability, and security. There may also be situations in which you want to receive alerts when exceptional, suspicious, or potential failure conditions arise. You can accomplish this using rules that define the conditions to watch out for, and which trigger an incident when those conditions arise. FortiSIEM includes over 500 system-defined rules, which you can see in **RESOURCES > Rules**.

From FortiSIEM Manager, you can export rules to enable, disable, or change the severity.

- Enable/Disable Rules
- Change Rule Severity

You cannot add, import, clone, or test rules from FortiSIEM Manager.

Enable/Disable Rules

To enable/disable rules, take the following steps.

1. Select the rule(s) you wish to enable or disable.
2. Click on the **Active** column where the rule(s) are selected.
3. Check or uncheck the **Active** box to enable or disable the rules, and select the organization(s).
4. Click **Save**.

Change Rule Severity

To change a rule's severity, take the following steps.

1. Select the rule you wish to change the severity of.
2. Click **Edit > Selected Rule**.
3. Click **Step 3: Define Action**.
4. From the **Severity** drop-down list, change the severity of the rule.
5. Click **Save**.

FortiSIEM Manager Resources Connectors

FortiSIEM Manager allows you to update Connectors from FortiSIEM Instances. See Updating Connectors for more information.

A connector is a solitary action that can be run by a user. Connectors can only be added, modified, or deleted through FortiSOAR. A connector can be run on an incident. After creating a FortiSIEM user in FortiSOAR and configuring Connector on FortiSIEM, connectors can be run through FortiSIEM. Additional information can also be found in Playbooks and Connectors under Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

FortiSIEM Manager Resources Playbooks

FortiSIEM Manager allows you to update Playbooks from FortiSIEM instances. See Updating Playbooks for more information.

A Playbook is a chain of actions that are taken based on logic programmed by a user. A Playbook can only be added, modified, or deleted through FortiSOAR. Playbooks can be executed on an incident. After creating a FortiSIEM user in FortiSOAR and configuring Playbook on FortiSIEM, playbooks can be executed through FortiSIEM. Additional information can also be found in Writing FortiSIEM Compatible FortiSOAR Playbooks available in the Appendix.

FortiSIEM Manager Resources - Event Types

The FortiSIEM Manager Resources Event Types page allows you to view existing event types.

FortiSIEM Manager Admin

The following sections provide the procedures under FortiSIEM Manager ADMIN:

- FortiSIEM Manager Setup
- FortiSIEM Manager Health
- FortiSIEM Manager License

See Settings for configuring FortiSIEM Manager as a FortiSIEM instance.

FortiSIEM Manager Setup

The FortiSIEM Manager Setup page allows you to add, edit, delete, or unregister FortiSIEM instances. Existing FortiSIEM instances appear on this page. For information about the existing FortiSIEM instances, see the table.

- Add a FortiSIEM Instance
- Edit a FortiSIEM Instance
- Delete a FortiSIEM Instance
- Unregister a FortiSIEM Instance

Column	Description
ID	Displays the ID of the FortiSIEM instance.
Name	Displays the name of the FortiSIEM instance.
FQDN	Displays the fully qualified domain name of the FortiSIEM instance.
Admin User	Displays the role.
Registered	Shows whether an instance is registered or not.
Description	Any additional information about the FortiSIEM instance is shown here.

Add a FortiSIEM Instance

To add a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

1. Click **New**.
2. In the **FortiSIEM Instance Name** field, enter the name of the FortiSIEM Instance.
3. In the **Admin User** field, enter the administrator user name.
4. In the **Admin Password** field, enter the password to be associated with the administrator user name.
   Note: The password must be between 8-64 characters, with at least one uppercase letter, one lowercase letter, one number and 1 special character.
5. In the **Confirm Admin Password** field, re-enter the password from step 4.
6. (Optional) In the **Description** field, enter any additional information you wish to have related to the FortiSIEM instance.
7. Click **Save**.

At this point, you can register the instance by following the steps in Configuring FortiSIEM Instance for FortiSIEM Manager.

Edit a FortiSIEM Instance

To edit a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

Note: The Admin User and Password cannot be changed.

1. Select the FortiSIEM instance you wish to edit.
2. Click **Edit**.
3. In the **FortiSIEM Instance Name** field, enter the name of the FortiSIEM Instance.
4. (Optional) In the **Description** field, enter any additional information you wish to have related to the FortiSIEM instance.
5. Click **Save**.

Delete a FortiSIEM Instance

To delete a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

1. Select the FortiSIEM instance you wish to delete.
2. Click **Delete**.
3. Click **Yes** to confirm.

Unregister a FortiSIEM Instance

To unregister a FortiSIEM instance, take the following steps from FortiSIEM Manager.

From **ADMIN > Setup**, take the following steps.

1. Select the FortiSIEM instance you wish to unregister.
2. Click **Unregister**.
3. Click **Yes** to confirm.

FortiSIEM Manager Health

The FortiSIEM Manager Health page displays the health of your FortiSIEM Manager, FortiSIEM Instances, and their worker's, collector's and agent's health, if applicable. The status is also color coded to quickly identify any health issues. Green is normal "Example FortiSIEM Instance", yellow is a risk "Example FortiSIEM Instace", and red is critical, "Example FortiSIEM Instance".

The name of the FortiSIEM Manager or FortiSIEM Instance is displayed in the header. Each row displays the health status of related FortiSIEM devices, and if more than one device exists for a worker, collector, or agent, the number is displayed as well.

Clicking on the header of the FortiSIEM Manager or a FortiSIEM instance will take you to the Cloud Health page. See FortiSIEM Manager Cloud Health for more information.

Clicking on the Collector link will take you to the Collector Health page. See FortiSIEM Manager Collector Health for more information.

FortiSIEM Manager Cloud Health

The FortiSIEM Manager Cloud Health page displays the status of the nodes in your deployment and the processes running on them. The top frame displays all of the available clouds and the lower frame provides information about the applications that are contained in the cloud selected in the main frame.

Click on the FortiSIEM Manager or FortiSIEM Instance heading (center top) to return to the FortiSIEM Manager Health Page.

Complete these steps to view the information about Cloud health:

- From the FortiSIEM Manager Health page, click on the FortiSIEM Manager header or a FortiSIEM instance header. The Cloud Health page displays the health of your FortiSIEM Manager or instance.
  See the FortiSIEM Back-End Processes table for more information about the system role played by each process.
  or
- From the FortiSIEM Manager Health page, click on a Collector link from a FortiSIEM instance to go to the Collector Health page for that FortiSIEM Instance's Collector(s).

First Frame

Note: For some settings, a chart icon will appear when hovering over a value. Click on the icon to get chart information.

Settings	Description
Name	Name of the available clouds
IP Address	IP address of the available clouds
Module Role	Module role, for example, 'Supervisor'
Health	Current health of the cloud. This is color coded (normal - green, warning - yellow, critical - red)
Last Status Updated	The date and time when the most recent status occurred.
Version	Current version of the cloud
Cores	Number of cores
Memory Size	The memory size
Swap Size	The swap size
EPS	Events per second **Note**: Only appears for instances, not FortiSIEM Manager.
Load Average	Average load of the cloud

Settings	Description
CPU	Percentage CPU used
Memory	Percentage Memory used
Swap	Percentage Swap space used
Disk	Percentage Disk used
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	The current upload buffer size (KB) and queue.
Content Version	The version of the content.

Second Frame

Settings	Description
Process Name	Name of the process
Owner	The owner of the process
Status	Status of the process
Uptime	Total up time of the process
CPU	Measure of the CPU that the process is using
Memory	Measure of the Memory that the process is using
Resident Memory	The amount of memory the process is allocated
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)
SharedStore Type	SharedStore type (reader, writer)
SharedStore Position	SharedStore location
SharedStore Percent	SharedStore utilization percentage

FortiSIEM Back-End Processes

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
Apache	Webserver for front-ending http(s) requests to AppSvr or other FortiSIEM nodes	x	x	x	x
AppSvr	Middleware for handling GUI requests, storing and managing PostgreSQL database and serving REST API requests from FortiSIEM nodes	x	x		
DBSvr	PostgreSQL Database for storing information displayed in FortiSIEM GUI other than events	x	x		
Node.js-charting	Message				
Node.js-pm2					
phAgentManager	Collects logs and metrics from devices or servers using protocols other than SNMP and WMI.		x	x	x
phCheckpoint	Collects logs from Checkpoint firewalls via LEA				
phDataManager	Stores the parsed events to event store (FortiSIEM EventDB or Elasticsearch)		x	x	
phDataPurger	Archives online event store (FortiSIEM EventDB or Elasticsearch). Implements event retention policy for FortiSIEM EventDB - both online FortiSIEM EventDB and archive.		x		

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
phDiscover	Discovers devices using various protocols such as SNMP, WMI and SSH		x		x
phEventForwarder	Forwards events from FortiSIEM to external Systems		x	x	x
phIpIdentityMaster	Merges Identity and location audit trails from multiple phIpIdentityWorker modules to produce the final Identity and location audit trail. Stores the trail in PostgreSQL Database.				
phIpIdentityWorker	Produces Identity and location audit trail based on its own view of events		x	x	
phMonitor	Monitors the health of FortiSIEM processes. Distributes tasks from AppSvr to various processes on Supervisor and to phMonitor on Worker for further distribution to processes on Worker nodes.	x	x	x	x
phParser	Parses raw events and prepares them for storing into event store (FortiSIEM EventDB or Elasticsearch)		x	x	x
phPerfMonitor	Continually collects performance monitoring and configuration change		x	x	x

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
	data after discovery completes				
phQueryMaster	Handles Adhoc queries from GUI for FortiSIEM EventDB. Paralellizes queries by sending them to phQueryWorkers and merges individual results to produce the final result.		x		
phQueryWorker	Handles individual FortiSIEM EventDB queries from phQueryMaster		x	x	
phReportLoader	Loads Report data into Report Server.		x		
phReportMaster	Handles individual FortiSIEM EventDB inline reports. Produces results every 5 minutes.		x		
phReportWorker	Handles inline event reports FortiSIEM EventDB.Merges individual inline report results multiple phReportMaster modules to produce the final result. Rolls up results from 5 minute intervals to 15 minute intervals and then to 60 minute intervals.		x		
phRuleMaster	Triggers a rule in real time by evaluating rule summaries from individual phRuleWorker		x		

Process	Function	Present in Manager	Present in Supervisor	Present in Worker	Present in Collector
	modules				
phRuleWorker	Evaluates a rule in real time based on events seen by the worker and sends a summary to the phRuleMaster module		x	x	
Redis	In-memory distributed database for holding results returned by Elasticsearch and for distributing CMDB objects between Supervisor and Worker nodes.		x	x	
Rsyslogd	Responsible for forwarding locally generated logs to FortiSIEM.	x	x	x	x
SVNLite	A light weight version of Subversion, this file revision management tool stores the file change history for windows/linux servers, routers/switches and windows/linux agents. **Note**: • Files are stored in `/svn/repos`. • To conserve space, files are automatically deleted when the disk gets full based on thresholds defined in `svnlite.revisions.purge` on the Supervisor.		x		

FortiSIEM Manager Collector Health

If your FortiSIEM deployment includes Collectors, you can monitor the status of the Collectors by clicking on a Collector link from the FortiSIEM Manager Health page.
Refer to the 'FortiSIEM Back-End Processes' table below for information about the processes that run on Collectors.

Click on the FortiSIEM Instance heading (center top) to return to the FortiSIEM Manager Health Page.

Properties Associated with Collector Health

Note: For some settings, a chart icon will appear when hovering over a value. Click on the icon to get chart information.

Collector Property	Description
Organization	Name of the organization to which the Collector belongs.
Name	Name of the Collector.
IP Address	IP address of the Collector.
Health	The health of the Collector. If Health is **Critical**, it means that one of the modules is not running on the Collector.
Last Status Updated	Health of the Collector based on the health of the modules running on it.
Collector Type	The Collector type is displayed.
Version	The version of the Collector is displayed.
Cores	The number of cores on the Collector is displayed.
Memory Size	The memory size of the Collector is displayed.
Swap Size	The swap size of the Collector is displayed.
Uptime	Total time that the Collector has been up.
EPS	The EPS that the Collector is currently seeing.
CPU	Overall CPU utilization of the Collector.
Memory	Overall memory utilization of the Collector.
Swap	Overall swap utilization of the Collector.
Disk	Overall disk utilization of the Collector.
Max Disk Read Wait	The maximum disk read/wait time (milliseconds).
Max Disk Write wait	The maximum disk write/wait time (milliseconds).
Upload Buffer	The total Buffer in KB used for upload.
Last Event Time	The time when the collector last reported events to the cloud.
Last File Received	The time when the collector last reported its performance status to the cloud.
Upgrade Version	If the Collector has been upgraded, the new version.
Build Date	Date on which the version of FortiSIEM the Collector is running on was built.
Content Version	Version of FortiSIEM the Collector is running on.
Content Update Status	The status of the content update is displayed.
Collector ID	The Collector's ID is displayed.
Install Status	The Install Status of the Collector is displayed.
Download Status	The download status for the Collector is displayed.

Process Properties

Process Property	Description
Process Name	Name of the process.
Owner	The owner of the process.
Status	Status of the process as either **Up** or **Down**.
Uptime	Total time that the process has been up.
CPU	Measure of the CPU that the process is using.
Memory	Measure of the Memory that the process is using.
Resident Memory	The amount of memory the process is allocated.
Disk Read Rate	The disk read rate speed (KBps)
Disk Write Rate	The disk write rate speed (KBps)

FortiSIEM Back-End Processes

Process	Function	Used by Supervisor	Used by Worker	Used by Collector
phAgentManager	Execute event pulling job	X	X	X
phCheckpoint	Execute checkpoint monitoring	X	X	X
phDiscover	Pulling basic data from target	X		X
phEventForwarder	Responsible for forwarding events and incidents from FortiSIEM to external systems	X	X	X
phEventPackage	Uploading event/SVN file to Supervisor/Worker			X
phMonitorAgent	Monitoring other processes	X	X	X
phParser	Parsing event to shared store (SS)	X	X	X
phPerfMonitor	Execute performance job	X	X	X
rsyslogd	Responsible for forwarding locally generated logs to FortiSIEM	X	X	X

Collector Property	Description
Host IP	The Host IP address of the tunnel.
Super Port	The supervisor port.
Protocol	The protocol used by the tunnel.
Protocol Port	The port used by the protocol.
Collector	The collector with the open tunnel.
PID	The Process ID.
Opened Time	The amount of time the tunnel is open.

FortiSIEM Manager License

The FortiSIEM Manager License page displays information about your FortiSIEM Manager license and any registered FortiSIEM instances. It is color coded.

- Green - License expiration date is greater than or equal to two weeks.
- Yellow - License expires in less than two weeks.
- Red - License has expired.

To upload a license, click **UPLOAD**, select your license, enter your User ID, Password, then click **Upload**.

To refresh the status, click **Refresh**.

FortiSIEM Manager	Description
Serial Number	Displays the serial number.
Hardware ID	Displays the hardware ID, if applicable.
License Type	Displays the license type.
FIPS Mode	Displays whether FIPS mode is enabled or disabled.
Instances	Displays the number of active instances, the total number of instances available under the license, and the expiration date of the license.
Maintenance and Support	Displays the status and expiration date for your maintenance and support license.

FortiSIEM Supervisor Instance	Description
Serial Number	Displays the serial number.
Hardware ID	Displays the hardware ID, if applicable.
License Type	Displays the license type.
FIPS Mode	Displays whether FIPS mode is enabled or disabled.
Devices	Displays the number of active devices under use from the license, the total number of devices allocated to the license, and expiration date.
EPS	Displays the total active Events Per Second (EPS) number, the total available EPS under the license, and expiration date. A chart icon can be clicked to view a chart showing EPS trends.
Agents	Displays the number of active Agents, the total number of Agents available under the license, and expiration date.
UEBA	Displays the number of User and Entity Behavior (UEBA) Analytics under use, the total number of User and Entity Behavior Analytics available and expiration date.
IOC Service	Displays the status and expiration date for your Indicator of Compromise (IOC) service license.
Support	Displays the status and expiration date for your support license.

Appendix

- Administrative Tools and Information
- ClickHouse Usage Notes
- Configuration Notes
- Elasticsearch Usage Notes
- Examples of Custom Performance Monitors
- Exporting QRadar Logs to FortiSIEM
- FortiEMS Endpoint Tagging
- FortiSOAR Integration Notes
- Functions in Analytics
- GUI Notes
- Knowledge Base
- License Enforcement
- Parser Specification
- Python Threat Feed Framework
- Sample Windows Agent Logs
- UEBA Information
- Windows Agent System Variables

Administrative Tools and Information

The following administrative tools and procedures are available.

- Adding Network Interfaces
- Backing Up and Restoring Databases
- Creating and Restoring ESX Snapshots
- Exporting Events from FortiSIEM
- Importing Events into FortiSIEM
- Increasing Collector Event Buffer Size
- Listing Event Attributes seen by Elasticsearch
- Managing Events in EventDB
- Managing FortiSIEM Operations

Adding Network Interfaces

FortiSIEM is configured to only use eth0 network interface by default. This section describes steps to add another interface, so that GUI traffic, storage traffic, and device access traffic can be split across multiple interface via proper routing.

Notes:

1. Primary (eth0) should not be removed or disabled and is required for normal operation of FortiSIEM.
2. These are general steps to add interfaces. These instructions do not cover making changes to the firewall.

To configure an additional network interface, choose the appropriate FortiSIEM deployment.

- Adding Interfaces for FortiSIEM Virtual Machine Based Deployments
- Adding Interfaces for FortiSIEM Hardware Appliances

Adding Interfaces for FortiSIEM Virtual Machine Based Deployments

Take the following steps to configure your FortiSIEM Virtual Machine based deployment with an additional network interface.

Step 1 – Modify VM Hardware Configuration on the Hypervisor

Log into the hypervisor and add a new network interface into FortiSIEM.

1. Edit the Supervisor VM.
2. Add a new network device to the VM.
3. Associate it with the desired network on the host.
4. Save configuration.
   Note: You may be required to reboot the FortiSIEM VM so that the network interface is available within the FortiSIEM VM.

Step 2 - Configure the Additional Interface on FortiSIEM

SSH into the Supervisor as root.

1. Verify if the interface added in Step 1 is available by running the following command.
   `ifconfig -a`
   Note: eth1, bolded in ifconfig -a Output, is the name of the new interface that was added.
   ifconfig -a Output

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.57.230  netmask 255.255.252.0  broadcast 172.30.59.255
        inet6 fe80::250:56ff:fea9:c9c9  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a9:c9:c9  txqueuelen 1000  (Ethernet)
        RX packets 50833491  bytes 30705896470 (28.5 GiB)
        RX errors 0  dropped 26644  overruns 0  frame 0
        TX packets 9726951  bytes 66973923534 (62.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::d215:a34c:98a5:6e23  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a9:78:29  txqueuelen 1000  (Ethernet)
        RX packets 1200  bytes 74944 (73.1 KiB)
        RX errors 0  dropped 5  overruns 0  frame 0
        TX packets 13  bytes 1790 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 110506670  bytes 72885247042 (67.8 GiB)
        RX errors 0  dropped 418  overruns 0  frame 0
        TX packets 110506670  bytes 72885247042 (67.8 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Configure the interface by taking the following steps.
   Note: The interface name may differ due to hypervisor naming of interfaces. Below is an example of interface named eth1.
   a. Run the following command to go to the network-scripts directory.
      `cd /etc/sysconfig/network-scripts/`
   b. Run the following command to create the ifcfg-eth1 file from ifcfg-eth0.
      `cp -a ifcfg-eth0 ifcfg-eth1`
   c. Edit the `ifcfg-eth1` file and save changes (can be done via vi editor for example), following the instructions that appear after "<<".

```
TYPE=Ethernet
BOOTPROTO=static
NAME=eth0   << change to new interface name
DEVICE=eth0 << change to new interface name
ONBOOT=yes
IPV6INIT=no

IPADDR=172.30.57.230  << change the IP to the new IP
NETMASK=255.255.252.0 << change the netmask to the new netmask
GATEWAY=172.30.56.1   << remove the line or comment as eth0 typically has the
```

```
default gateway defined.

DNS1=1.1.1.1
DNS2=172.30.1.106
```

d. Reset the interface to take the configuration in effect by running the following commands.

```
# ifdown eth1
# ifup eth1
```

3. Optional: Configure routes to other networks via the additional interface.
   Adding route example:
   `# ip route add <network_ip>/<cidr> via <gateway_ip> dev <network_card_name> metric <metric_value>`
   Example:
   `ip route add 172.30.0.0/16 via 172.30.52.1 dev eth1 metric 101`
   If you want to manually create a routing configuration file and make it persistent across reboots, then follow these steps. Suppose you want to create an IPv4 route to the 172.30.0.0/16 network via eth1 interface, with 172.30.52.1 as the default gateway. The gateway for the static route must be directly reachable on eth1.
   a. Add the static IPv4 route to the `/etc/sysconfig/network-scripts/route-eth1` file:
   `172.30.0.0/16 via 172.30.52.1 dev eth1`
   b. Restart the network:
   `# systemctl restart NetworkManager.service`
4. Verify connectivity through all interfaces.

Adding Interfaces for FortiSIEM Hardware Appliances

The physical interfaces should already be available. The number may vary depending on the HW appliance, e.g. the HW appliance may display 4 interfaces: eth0 thru eth3 (4 interfaces in total).

After you SSH onto the supervisor as root, take the following steps.

1. Verify the available interfaces by running the following command.
   `# ifconfig -a`
   Your ifconfig -a output should appear similar to the following, and allow you to confirm the available interfaces. In this case, eth1, eth2, eth3, which are bolded, are identified interfaces.
   ifconfig -a Output

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.65.20.201  netmask 255.255.252.0  broadcast 10.65.23.255
        inet6 fe80::ae1f:6bff:fe47:b318  prefixlen 64  scopeid 0x20<link>
        ether ac:1f:6b:47:b3:18  txqueuelen 1000  (Ethernet)
        RX packets 31177113  bytes 7280636740 (6.7 GiB)
        RX errors 0  dropped 3746071  overruns 0  frame 0
```

```
        TX packets 617574  bytes 142045223 (135.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb560000-fb57ffff

eth1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:1f:6b:47:b3:19  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb540000-fb55ffff

eth2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:1f:6b:47:b3:1a  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb520000-fb53ffff

eth3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:1f:6b:47:b3:1b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb500000-fb51ffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 7419278  bytes 387353322 (369.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7419278  bytes 387353322 (369.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Configure the new interface.
   Note: Choose any interface you would like to configure. This example provides an example for configuring eth1.
   a. Run the following command to go to the network-scripts directory.
      `cd /etc/sysconfig/network-scripts/`
   b. Run the following command to create ifcfg-eth1 using ifcfg-eth0.
      `cp -a ifcfg-eth0 ifcfg-eth1`
   c. Edit the ifcfg-eth1 file and save changes, following the instructions that appear after the "<<".

```
TYPE=Ethernet
BOOTPROTO=static
NAME=eth0   << change to new interface name
DEVICE=eth0 << change to new interface name
ONBOOT=yes
```

```
IPV6INIT=no

IPADDR=172.30.57.230  << change the IP to the new IP
NETMASK=255.255.252.0 << change the netmask to the new netmask
GATEWAY=172.30.56.1   << remove the line or comment as eth0 typically has the
default gateway defined.

DNS1=1.1.1.1  << add at least one DNS server
DNS2=172.30.1.106
```

If using vi, save the configuration by pressing ESC then :x!

d. Reset the interface to take the configuration in effect by running the following commands.

```
# ifdown eth1
# ifup eth1
```

3. Optional: Configure routes to other networks via the additional interface.
Adding route example:
`# ip route add <network_ip>/<cidr> via <gateway_ip> dev <network_card_name> metric <metric_value>`
Example:
`ip route add 172.30.0.0/16 via 172.30.52.1 dev eth1 metric 101`
If you want to manually create a routing configuration file and make it persistent across reboots, then follow these steps. Suppose you want to create an IPv4 route to the 172.30.0.0/16 network via eth1 interface, with 172.30.52.1 as the default gateway. The gateway for the static route must be directly reachable on eth1.

a. Add the static IPv4 route to the `/etc/sysconfig/network-scripts/route-eth1` file:
`172.30.0.0/16 via 172.30.52.1 dev eth1`

b. Restart the network.
`# systemctl restart NetworkManager.service`

4. Verify connectivity through all interfaces.

Backing Up and Restoring Databases

- Backing Up and Restoring CMDB
- Backing Up and Restoring EventDB
- Backing Up and Restoring SVN
- ClickHouse Backup and Restore Steps

Backing Up and Restoring CMDB

The FortiSIEM Configuration Management Database (CMDB) contains discovered information about devices, servers, networks and applications. You should create regular backups of the CMDB that you can use to restore it in the event of database corruption.

- CMDB Backup Procedure
- CMDB Restore Procedure

CMDB Backup Procedure

The database files are stored in `/cmdb/data`. FortiSIEM automatically backs up this data twice daily and the backup files are stored in `/data/archive/cmdb`. To perform a backup, move these files to another location. For example:

```
[root@SaaS-Sup cmdb] #cd /data/archive/cmdb
[root@SaaS-Sup cmdb] #cp phoenixdb* /<another>/<mount>/<point>
```

If your `/data` disk is on an external NFS mount then your CMDB backup is already separate from the VM infrastructure.

```
[root@SaaS-Sup cmdb]# pwd
/data/archive/cmdb
[root@SaaS-Sup cmdb]# ls -lt
total 1213952
-rw-rw-rw- 1 root root 95559457 Apr 20 03:02 phoenixdb_2011-04-20T03-00-01
-rw-rw-rw- 1 root root 93010144 Apr 19 13:04 phoenixdb_2011-04-19T13-00-02
-rw-rw-rw- 1 root root 91142941 Apr 19 03:02 phoenixdb_2011-04-19T03-00-01
-rw-rw-rw- 1 root root 89686080 Apr 18 13:03 phoenixdb_2011-04-18T13-00-02
```

CMDB Restore Procedure

If your database becomes corrupted, you can restore it from backup by performing these steps on your Supervisor node.

1. Perform a clean stop by running the following command:
   `systemctl stop phxctl`
2. Stop all processes with this phTools command:
   `phtools -stop all`
3. Wait for approximately 20 seconds for all processes to stop.
4. Run `killall -9 java; killall -9 phMonitor`
5. Copy the latest `phoenixdb_<timestamp>` file to a directory like `/tmp` on the Supervisor host.
6. Go to `/opt/phoenix/deployment`.
7. Run `db_restore /tmp/phoenixdb_<timestamp>`
8. When this process completes, reboot the system by running the following command:
   `reboot`

Backing Up and Restoring EventDB

- EventDB Backup Procedure
- EventDB Restore Procedure

EventDB Backup Procedure

The event data is stored in `/data/eventdb`. Since this data can become very large over time, you should use a program such as rsync to incrementally move the data to another location. From version 4.2.1, the rsync program is installed on FortiSIEM by default.

Use this command to back up the EventDB.

```
#rsync -a --progress /data/eventdb /<another>/<mount>/<point>
```

EventDB Restore Procedure

To restore EventDB there are two options:

- Mount the directory where the event database was backed up.
- Copy the backup to the **/data/eventdb** directory.

These instructions are for copying the backup to the **/data/eventdb** directory.

1. Stop all running processes.
   `#phtools --stop all`
2. Check that all processes have stopped.
   `#phstatus`

You will see that these processes are still running, which is expected behavior.
These processes will continue to run, which is expected behavior:

```
phMonitor      1-01:55:17     0            992m         540m
Apache         1-01:56:45     0            236m         9720
AppSvr         1-01:56:35     0            3908m        758m
DBSvr          1-01:57:06     0            383m         6656
```

3. Copy the EventDB to the event DB location `/data/eventdb`. If you use the `cp` command, it may appear that the command has hung if there is a lot of data to copy.
   `#cp -a /backup/eventdb /data/eventdb`
   Alternatively, you can use rsync and display the process status.
   `#rsync -a --progress /backup/eventdb /data/eventdb`
4. Once complete, restart all processes.
   `#phtools --start all`
5. Check that all processes have started.
   `#phstatus`

Backing Up and Restoring SVN

FortiSIEM uses an inbuilt SVN to store network device configuration and installed software versions.

- SVN Backup
- SVN Restore

SVN Backup

The SVN files are stored in `/svn`. Copy the entire directory to another location.

```
# cd /
# cp -r /svn /<another>/<mount>/<point>
```

SVN Restore

Copy the entire `/svn` from the backup location and rename the directory to `/svn`.

```
# cd /<another>/<mount>/<point>
# cp -r svn /
```

Creating and Restoring ESX Snapshots

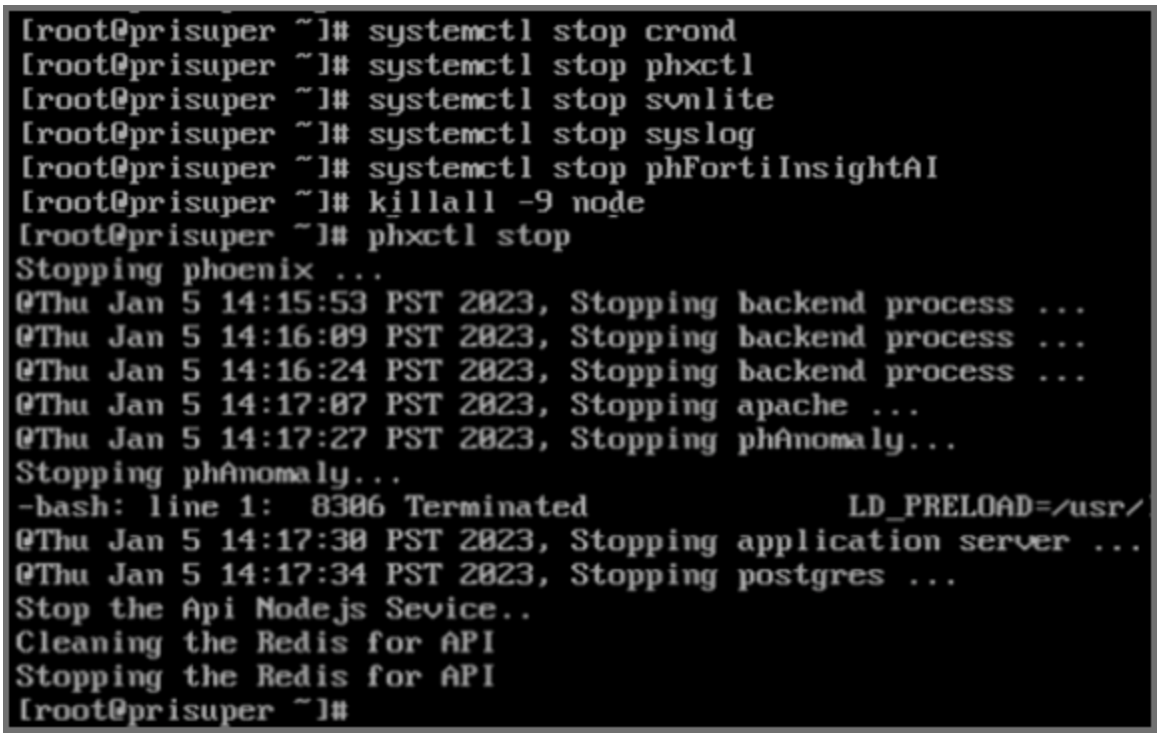
- Create FortiSIEM VM Snapshot
- Restoring FortiSIEM VM from Snapshot

Create FortiSIEM VM Snapshot

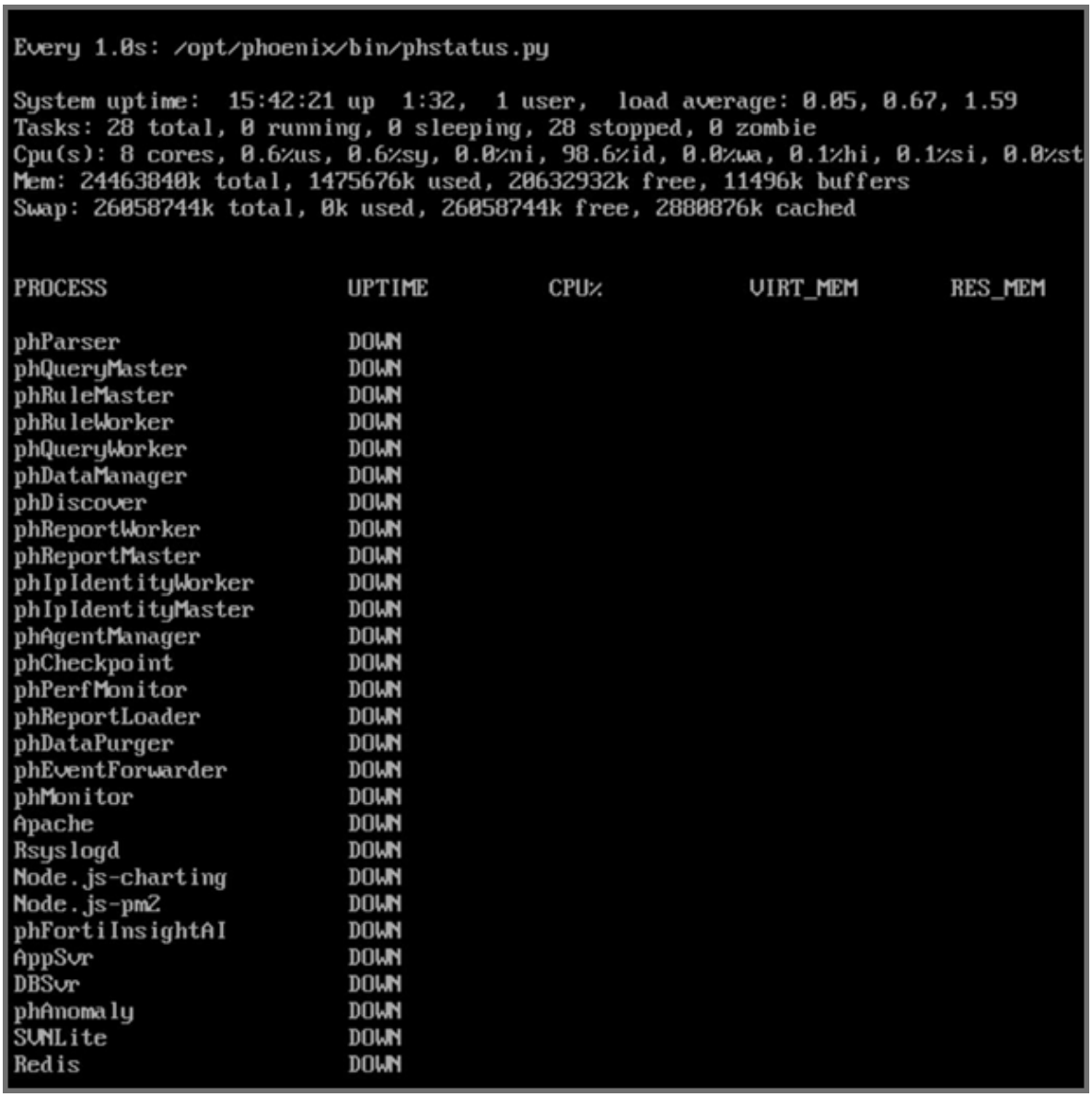
Follow these steps to create snapshots for FortiSIEM nodes.

1. ssh into the supervisor node as root.
2. Run the following commands to stop all essential FortiSIEM services.

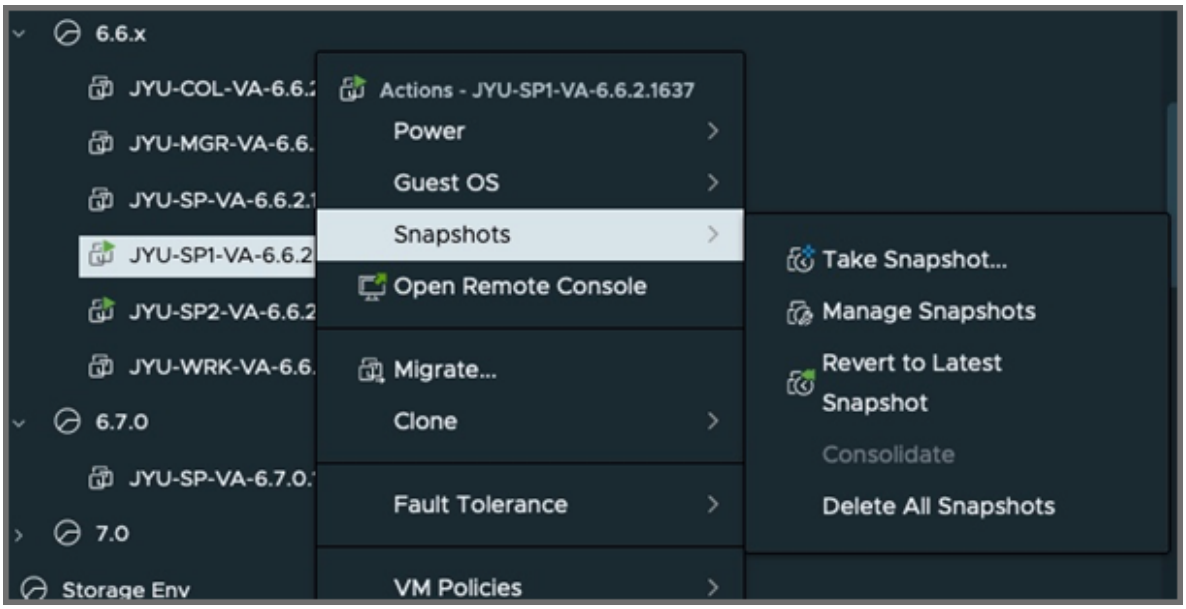
```
# systemctl stop crond
# systemctl stop phxctl
# systemctl stop svnlite
# systemctl stop syslog
# systemctl stop phFortiInsightAI
# killall -9 node
# phxctl stop
```



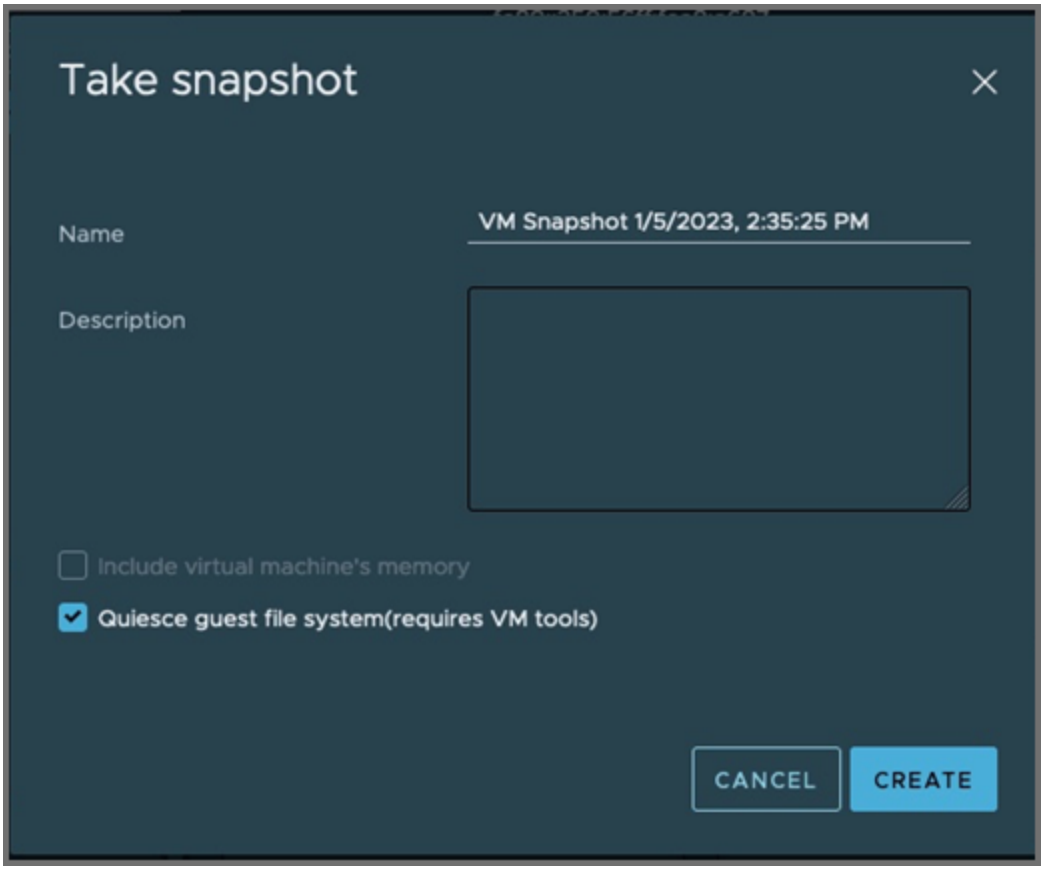
3. Run `phstatus` and verify all services are down.



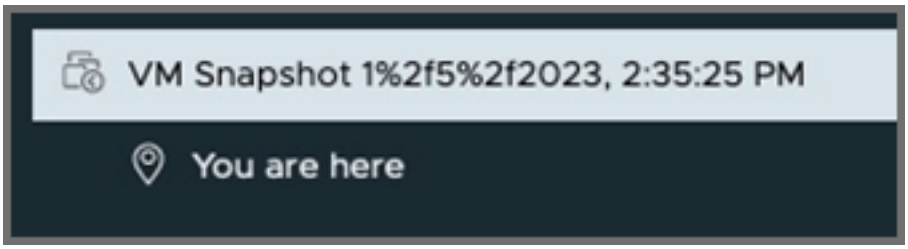
4. Find the FortiSIEM VM inside your hypervisor and click **Snapshots > Take Snapshot...**.



5. In the follow up dialog, take the following steps.
   a. Uncheck the **Include virtual machine's memory** checkbox for a quick snapshot.
   b. Check the **Quiesce guest file system** checkbox to ensure filesystem integrity.
   c. Click **CREATE**.

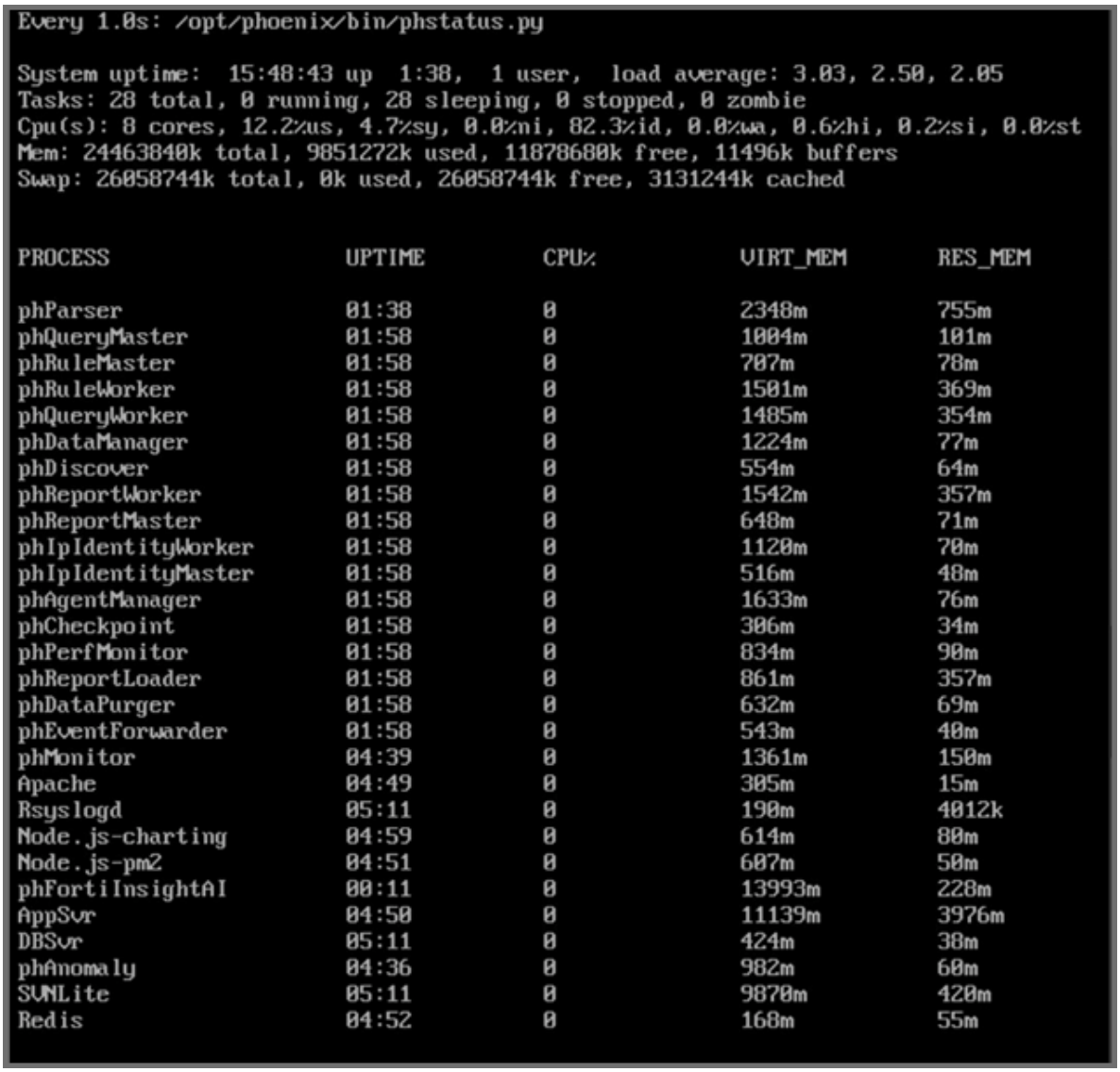


6. Check the Snapshot section of the VM in order to verify snapshot has been taken.



7. Restart all FortiSIEM Services after the snapshot has been taken, by running the following commands.

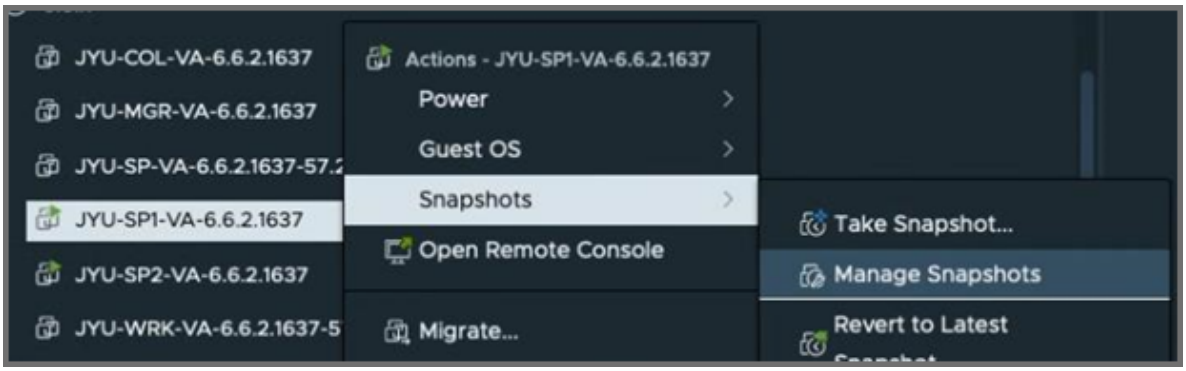
```
# systemctl start crond
# systemctl start phxctl
# systemctl start svnlite
# systemctl start syslog
# systemctl start phFortiInsightAI
# phxctl start
# phstatus
```



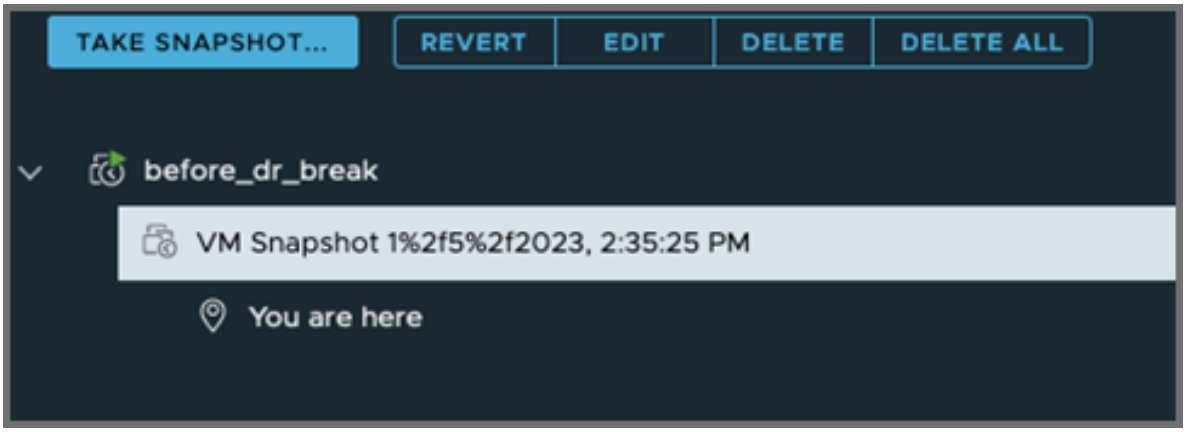
Restoring FortiSIEM VM from Snapshot

Take the following steps to restore a VM from a snapshot.

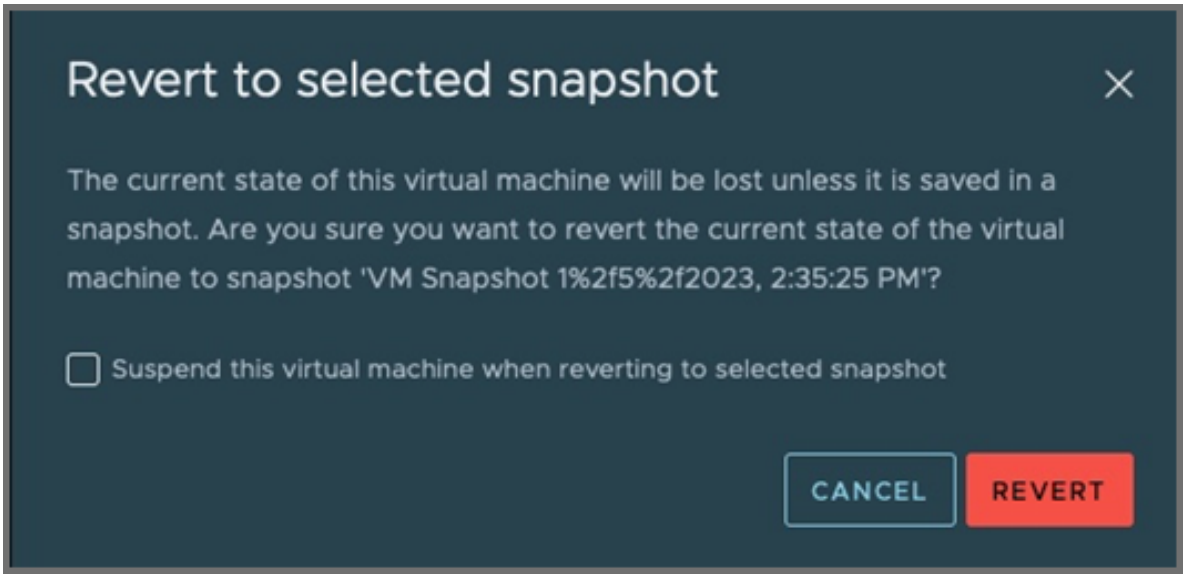
1. Find the currently running VM in vSphere, right click on the **VM**, and navigate to **Snapshots > Manage Snapshots**.



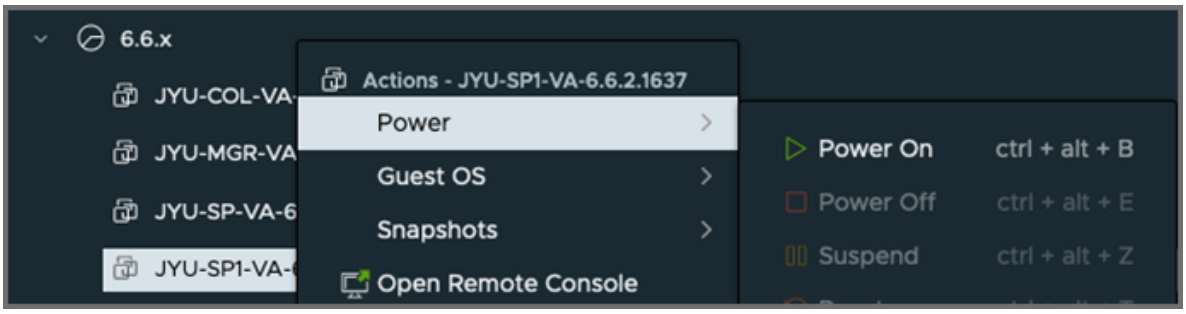
2. Select the snapshot in the list that you want to restore, and select **REVERT**.



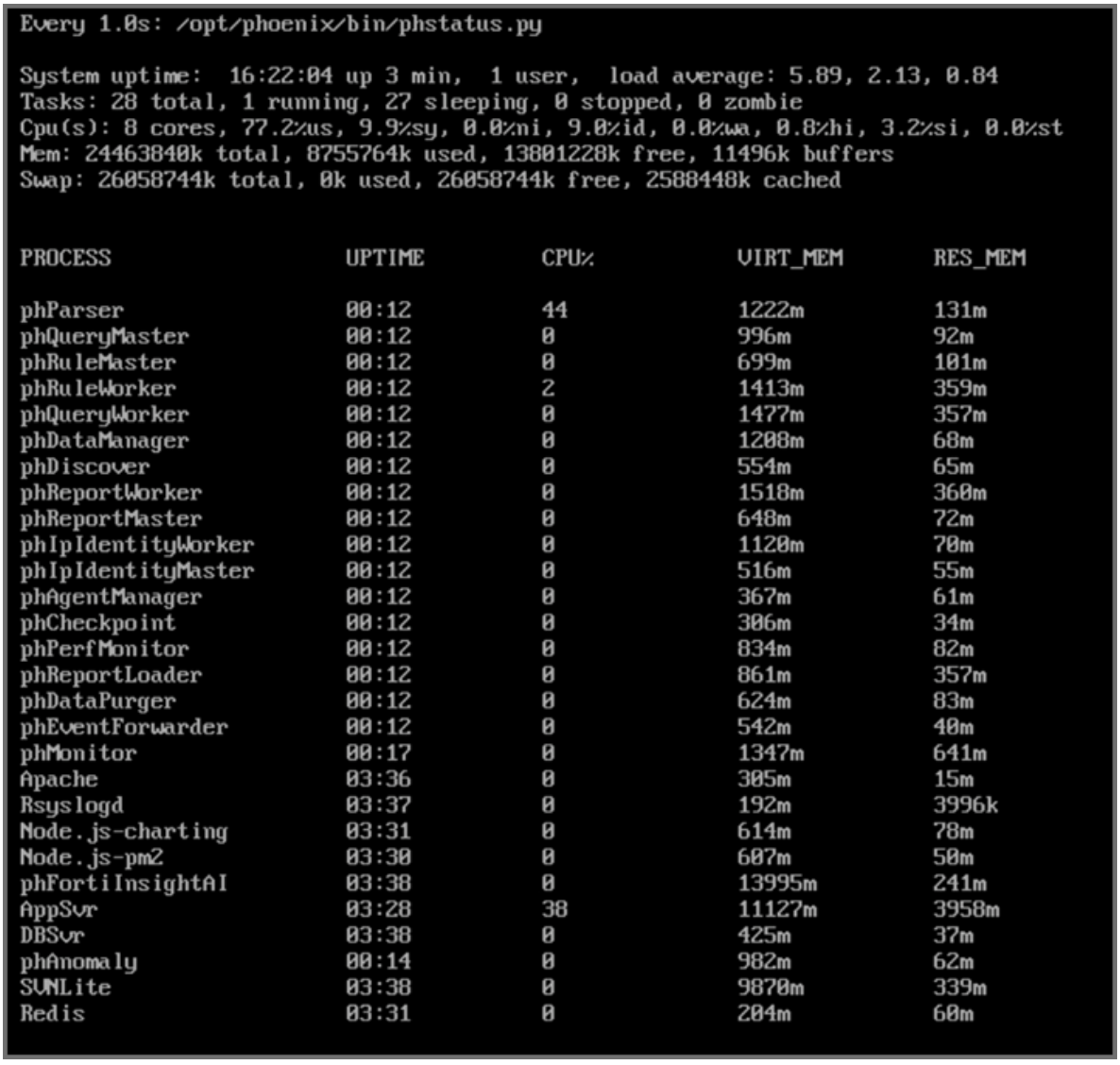
3. On the pop-up window, select **REVERT**.



4. The VM will be reverted to the selected snapshot and be left turned off. Right click the **VM**, and navigate to **Power > Power On**.



This will turn the VM on from the point of the snapshot and services will start up as normal.



Exporting Events from FortiSIEM

The following tools are provided:

- phExportESEvent Tool
- phExportEvent Tool
- TestESSplitter Tool
- phClickHouseCSVExport Tool

phExportESEvent Tool

Description: This tool exports events from Elasticsearch into a CSV file.

Usage: `phExportESEvent <ESUrl> <ESPort> <ESDeploymentType> "<ESUser>" "<ESPassword>" <ESIndexName> <ReportingDevIp> <destDir> <splitThreads> <LogLevel>`

Argument	Description
`ESUrl`	The Elasticsearch URL. Example, http://192.0.2.0.
`ESPort`	The Elasticsearch coordinating node port, e.g. 9200.
`ESType`	Provide the Elasticsearch type. 1: Native 2: AWS Elasticsearch Service 3: Elasticsearch Cloud
`ESUser`	Provide the Elasticsearch username. "" means no username.
`ESPassword`	Provide the Elasticsearch password. "" means no password.
`ESIndexName`	The name of the Elasticsearch index to be exported, for example, `fortisiem-event-2020.06.17-1`.
`ReportDevIp`	The IP address of the report device to be used to select events to export. "" means select all devices.
`destDir`	The export directory: `output_dir`.
`splitThreads`	The number of threads to be used for export, e.g., 10.
`logDevel`	The debug level for script output printing: `INFO` or `DEBUG`.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.

Examples:

Native Elasticsearch Deployment Example

```
phExportESEvent https://192.0.2.0 9200 1 "Joe.123--test" "password" fortisiem-event-2021.08.05-1-000001 "192.0.2.4" /archive/ 10 INFO
```

AWS Elasticsearch Service Deployment Example

```
phExportESEvent https://search-eesna78-aaaa4ysukru3ui4ayaz2yya3km.us-east-1.es.amazonaws.com 443 2 "key" "secret" fortisiem-event-2021.09.29-1 "" /archive/ 10 INFO
```

Elasticsearch Cloud Deployment Example

```
phExportESEvent https://cpaagg33-d11e01.es.us-central1.gcp.cloud.es.io 9243 3 "elastic" "password" fortisiem-event-2021.10.01-1-000001 "" /archive/ 10 INFO
```

phExportEvent Tool

Description: This tool exports events from EventDB into a CSV file. The CSV file contains the following columns:

- Customer Id (applicable to SP license)
- Reporting Device IP
- Reporting Device Name
- Event Received Time
- Raw Message

Usage: `phExportEvent {--dest DESTINATION_DIR} {--starttime START_TIME | --relstarttime RELATIVE_START_TIME} {--endtime END_TIME | --relendtime RELATIVE_END_TIME} [--dev DEVICE_NAME] [--org ORGANIZATION_NAME] [-t TIME_ZONE]`

Argument	Description
DESTINATION_DIR	Destination directory where the exported event files are saved.
START_TIME	Starting time of events to be exported. The format is YYYY-MM-DD HH:MM:SS {+|-} TZ. If TZ is not given, the local time zone of the machine where the script is running will be used. Example: `2010-03-10 23:00:00 -8` means Pacific Standard Time, 23:00:00 03/10/2010. `2010-07-29 10:20:00 +5:30` means India Standard Time 10:20:00 07/29/2010.
RELATIVE_ START_TIME	This must be used together with END_TIME. Starting time of events to be exported is relative backwards to the end time, specified using `--endtime` END_TIME. The format is `{NUM}{d|h|m}` where NUM is the number of days or hours or minutes. For example, `--relstarttime 5d` means the starting time is 5 days prior to the ending time.
END_TIME	Ending time of events to be exported. The format is the same as described for START_TIME.
RELATIVE_END_ TIME	This must be used together with START_TIME. Ending time of events to be exported is relative forward to the start time, specified using START_TIME. The format is the same that is used for RELATIVE_START_TIME.
DEVICE_NAME	Provide the host name or IP address of the device with the events to be exported. Use a comma-separated list to specify multiple IPs or host names, for example, `--dev 10.1.1.1,10.10.10.1,router1,router2`. Host name is case insensitive.
ORGANIZATION_ NAME	This is used only for Service Provider deployments. Provide the name of the organization with the events to be exported. To specify multiple organizations, enter a command for each organization, for example, `--org "Public Bank" --org "Private Bank"`. The organization name is case insensitive.
TIME_ZONE	Specifies the time zone used to format the event received time in the exported event files. The format is {+|-}TZ, for example, -8 means Pacific Standard Time, +5:30 means India Standard Time.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.

TestESSplitter Tool

Description: This tool exports events from ElasticSearch to a directory in FortiSIEM EventDB format.

Usage: `TestESSplitter <ESBroker> <ESPort> <ESClusterType> <ESUser> <ESPassword> <IndexName> <destDir> <splitThreads> <logLevel>`

Argument	Description
`ESBroker`	The IP of ElasticSearch Co-ordinator node.
`ESPort`	The port used for ElasticSearch.
`ESClusterType`	The ElasticSearch Cluster type. Values are "1" for Native, "2" for Amazon OpenSearch Service (previously known as Amazon Elasticsearch Service), and "3" for Elastic Cloud.
`ESUser`	The ElasticSearch username for authentication.
`ESPassword`	The ElasticSearch password for authentication.
`IndexName`	Provide an Index name. A new Index is created per day. Here is an example index name, `fortisiem-event-2021.05.14-2000-000001` where"fortisiem-event-2021.05.14" is the day and "2000" is the Organization ID. To find a list of indexes, run this command: `curl -XGET '10.10.2.5:9200/_cat/shards?v'` replacing `10.10.2.5` with the IP of a Co-ordinator node.
`destDir`	Destination directory where the exported events are saved in FortiSIEM eventDB format. **Note**: A trailing slash is mandatory. Example: `https://<destDir>/`.
`splitThreads`	Number of threads.
`logLevel`	INFO or DEBUG level log messages.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.
3. This tool is located in `/opt/phoenix/bin/`.

Example:

```
[root@fsm]# /opt/phoenix/bin/TestESSplitter 10.10.2.5 "" "" fortisiem-event-2021.05.14-
2000-000001 /root/output 10 INFO

[PH_MODULE_LOG_LEVEL_CHANGE]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=phBaseProcess.cpp,[lineNumber]=675,[oldLogLevel]=2047,[newLogLevel]=424,
[phLogDetail]=Module received log level change
[PH_MODULE_LOCAL_CONFIG_LOADED]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=phConfigLoader.cpp,[lineNumber]=166,[configName]=global,[phLogDetail]=Module
loaded local config successfully
[PH_MODULE_LOCAL_CONFIG_LOADED]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=phConfigLoader.cpp,[lineNumber]=166,[configName]=phdatamanager,
[phLogDetail]=Module loaded local config successfully
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=phHttpClientPool.cpp,[lineNumber]=46,[phLogDetail]=phHttpClientPool: init
hosts/port/auth/header=10.10.2.5/9200/:****/Content-Type: application/json
*   Trying 10.10.2.5...
```

```
* TCP_NODELAY set
* Connected to 10.10.2.5 (10.10.2.5) port 9200 (#0)
> GET / HTTP/1.1
Host: 10.10.2.5:9200
Accept: */*
Content-Type: application/json

< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 530
<
* Connection #0 to host 10.10.2.5 left intact
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1732,[phLogDetail]=Elastic init success: http://10.10.2.5:9200/
* Found bundle for host 10.10.2.5: 0x18f0870 [can pipeline]
* Re-using existing connection! (#0) with host 10.10.2.5
* Connected to 10.10.2.5 (10.10.2.5) port 9200 (#0)
> GET /_cat/indices/fortisiem-event-2021.05.14-2000-000001?h=pri,rep,docs.count HTTP/1.1
Host: 10.10.2.5:9200
Accept: */*
Content-Type: application/json
…
…
…
…

<
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 66 for index fortisiem-event-
2021.05.14-2000-000001 slice 1 max 10
* Connection #0 to host 10.10.2.5 left intact
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 61 for index fortisiem-event-
2021.05.14-2000-000001 slice 8 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0 seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0 seconds
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 47737
<
* Connection #0 to host 10.10.2.5 left intact
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 53 for index fortisiem-event-
2021.05.14-2000-000001 slice 3 max 10
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 47178
<
* Connection #0 to host 10.10.2.5 left intact
< HTTP/1.1 200 OK
```

```
< content-type: application/json; charset=UTF-8
< content-length: 41910
<
* Connection #0 to host 10.10.2.5 left intact
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 53258
<
* Connection #0 to host 10.10.2.5 left intact
< HTTP/1.1 200 OK
< content-type: application/json; charset=UTF-8
< content-length: 60587
<
* Connection #0 to host 10.10.2.5 left intact
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 59 for index fortisiem-event-
2021.05.14-2000-000001 slice 4 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 53 for index fortisiem-event-
2021.05.14-2000-000001 slice 7 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 68 for index fortisiem-event-
2021.05.14-2000-000001 slice 6 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=1974,[phLogDetail]=Elastic succeed hits total 46 for index fortisiem-event-
2021.05.14-2000-000001 slice 2 max 10
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0 seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0 seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0 seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0 seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=EventLoader.cpp,
[lineNumber]=2002,[phLogDetail]=Elastic index query completed 0 seconds
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,
[fileName]=TestESSplitter.cpp,[lineNumber]=82,[phLogDetail]=Events processed for split: 559
3.15
```

The result will be eventDB structured directories and files.

```
[root@fsm]# ls -l /root/output/
total 0
drwx------ 3 root root 22 May 14 15:25 CUSTOMER_2000
[root@fsm]# ls -l /root/output/CUSTOMER_2000/
total 0
drwx------ 3 root root 19 May 14 15:25 internal
[root@fsm]# ls -l /root/output/CUSTOMER_2000/internal/
total 0
drwx------ 3 root root 37 May 14 15:25 18761
[root@fsm]# ls -l /root/output/CUSTOMER_2000/internal/18761/
total 4
```

```
drwx------ 12 root root 4096 May 14 15:25 450264-450287-168428094
[root@fsm]# ls -l /root/output/CUSTOMER_2000/internal/18761/450264-450287-168428094/
total 0
drwx------ 3 root root 18 May 14 15:25 seg-1-0-48-1620951010-1620971132
drwx------ 3 root root 18 May 14 15:25 seg-1-1-70-1620950470-1620971172
drwx------ 3 root root 18 May 14 15:25 seg-1-2-35-1620950916-1620971172
drwx------ 3 root root 18 May 14 15:25 seg-1-3-66-1620951819-1620969371
drwx------ 3 root root 18 May 14 15:25 seg-1-4-61-1620950830-1620970642
drwx------ 3 root root 18 May 14 15:25 seg-1-5-59-1620950830-1620971132
drwx------ 3 root root 18 May 14 15:25 seg-1-6-53-1620950482-1620970632
drwx------ 3 root root 18 May 14 15:25 seg-1-7-46-1620951278-1620971182
drwx------ 3 root root 18 May 14 15:25 seg-1-8-53-1620950470-1620970452
drwx------ 3 root root 18 May 14 15:25 seg-1-9-68-1620950650-1620971132
```

phClickHouseCSVExport Tool

Description: This tool exports events from ClickHouse into a CSV file. The file will contain these fields:

- Event Receive Time
- Reporting IP
- Event Type
- Raw Event Log.

Usage: `phClickHouseCSVExport --starttime [Start Time] --endtime [End Time] --outfile [Output file] --deviceip [Reporting Device IP Address] --devicename [Reporting Device Name] --limit [Number of records to return] --debug --orgid [Organization ID (0 - 4294967295)] --orgname [Organization Name] --eventtype [Event Type]`

Argument	Description
`--starttime [Start Time]`	Starting time of events to be exported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the Start Time with quotation marks. Example: `phClickHouseCSVExport --outfile /home/user/report.csv --starttime "2022-01-20 10:10:00" --endtime "2022-01-20 11:10:00"`
`--endtime [End Time]`	The end time of events to be exported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the End Time with quotation marks. Example: `phClickHouseCSVExport --outfile /home/user/report.csv --starttime "2022-01-20 10:10:00" --endtime "2022-01-20 11:10:00"`
`--outfile [Output file]`	The output file where the exported events are saved in FortiSIEM, CSV format.
`--deviceip [Reporting Device IP Address]`	Provide the IP address of the device with the events to be exported. Only one reporting device IP address is supported. For example, `--deviceip 10.1.1.1`.
`--devicename [Reporting Device Name]`	Provide the host name of the device with the events to be exported. For example, `--devicename router1`. Host name is case insensitive.
`--limit [Number of records to return]`	Provide the number of records to return, default is no limit.
`--debug`	Output SQL statement generated for this report.
`--orgid [Organization ID]`	Provide the ID of the organization with the events to be exported. The number can be from 0 to 4294967295.
`--orgname [Organization Name]`	This is used only for Service Provider deployments. Provide the name of the organization with the events to be exported. To specify multiple organizations, enter a command for each organization, for example, `--org "Public Bank" --orgname "Private Bank"`. The organization name is case insensitive.
`--eventtype [Event Type]`	Specify the event types to be exported.

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.

Importing Events into FortiSIEM

The following tools are provided:

- phClickHouseImport Tool

phClickHouseImport Tool

Description: This tool is used to migrate EventDB data into your ClickHouse database.

Note: If importing remotely, then for data migration to succeed, the IP address of the source host to the ClickHouse cluster must be added to the destination host `ips.xml` file.
Example: If you want to import data from 192.0.2.0 (source host with EventDB) to 192.0.2.227 (destination host with ClickHouse), on the destination host (192.0.2.227), you must add the source host IP address 192.0.2.0 to the destination host's `ips.xml` file.

```
~]# cat /etc/clickhouse-server/users.d/ips.xml

<yandex>

  <users>
    <default>
      <networks>
        <ip>127.0.0.1</ip>
        <ip>192.0.2.227</ip>
        <ip>192.0.2.0</ip>
      </networks>
    </default>
  </users>

</yandex>
```

Usage: `phClickHouseImport --src [`*`Source Dir`*`] --srcorgid `*`Organization ID`*` --dstorgid `*`Organization ID`*` --starttime [`*`Start Time`*`] --endtime [`*`End Time`*`] --host [`*`IP Address of the ClickHouse Server that the data will be imported to`*`] --orgid [`*`Organization ID`*`]`

Argument	Description
`--src [Source Dir]`	Provide the source directory that contains the eventDB data. The default path is `/data/eventdb/` If a path is provided, the data path will be created as: *<user input path>* Example: If `--src /archive/CUSTOMER2000` is used, the data path will be created as `/archive/CUSTOMER2000/`
`--starttime [Start Time]`	Starting time of events to be imported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the Start Time with quotation marks. Example: `phClickHouseImport --src /data/eventdb --starttime "2022-01-27 10:10:00" --endtime "2022-02-01 11:10:00"`
`--endtime [End Time]`	The end time of events to be imported. It must be in the following format: "YYYY-MM-DD hh:mm:ss". The supported time zone is GMT. Make sure to enclose the End Time with quotation marks. Example: `phClickHouseImport --src /data/eventdb --starttime "2022-01-27 10:10:00" --endtime "2022-02-01 11:10:00"`
`--host [IP Address of the ClickHouse Server that the data will be imported to]`	The IP address of the ClickHouse server that the data will be imported to. If the host IP address is not provided, then localhost is used. The default IP address is 127.0.0.1.
`--orgid [Organization ID]`	Provide the ID of the organization with the events to be imported. The number can be from 0 to 4294967295. Multiple entries are allowed by adding `--orgid [Organization ID]` for each entry. Only matched orgid will be migrated. Example: `phClickHouseImport --src /data/eventdb --starttime "2022-01-01 23:00:00" --endtime "2022-02-01 10:00:00" --orgid 1 --orgid 2001 --host 192.0.20.0`
`--srcorgid [Organization ID]` `--dstorgid [Organization ID]`	The `--srcorgid` is the organization ID that data will be imported from and the `--dstorgid` is the target organization ID that the data will be imported into ClickHouse. Example: `phClickHouseImport --src /data/eventdb/ --starttime "2022-01-27 10:10:00" --endtime "2022-02-01 11:10:00" --srcorgid 2005 --dstorgid 2008 --host 192.0.20.0`

Notes:

1. Can be run from Supervisor or Worker.
2. Can be run as admin user.
3. `phClickHouseImport` tool requires FortiSIEM 6.5.0 or higher.
4. EventDB data needs to be copied to the machine where this tool can run.

Example:

```
phClickHouseImport --src /data/eventdb --starttime "2022-01-01 23:00:00" --endtime
"2022-02-01 10:00:00" --orgid 1 --orgid 2001 --host 192.0.20.0
```

Increasing Collector Event Buffer Size

Collectors can buffer events in case events cannot be uploaded fast enough to Worker(s) or Supervisor nodes or they are unavailable for a period of time. Events are stored in compressed format in the following location `/opt/phoenix/cache/parser/events` before being sent to Worker(s) or Supervisor nodes. By default, a maximum of 10K files are stored and each file has a maximum uncompressed file size of 10MB.

When the number of files reaches the limit, events are dropped by the Collector. To change this limit, modify the following line in `/opt/phoenix/config/phoenix_config.txt`.

```
[BEGIN phEventPackager]

max_num_event_files=10000
```

In case your Collectors are forwarding events to a 3rd party server, there is a similar limit of 10K files of events stored in `/opt/phoenix/cache/parser/fwd`. When this limit is reached, newer events are not forwarded. To change this limit, modify the following line in `/opt/phoenix/config/phoenix_config.txt`.

```
[BEGIN phEventForwarder]

max_num_fwd_files=10000
```

Note: You may need to increase the size of `/opt` disk if you significantly increase the number of files stored. For configuration information on how to increase your `/opt` disk size, see Collector with Different OPT Disk Sizes in the ESX Install Guide.

Listing Event Attributes seen by Elasticsearch

The following tools are provided:

- listElasticEventAttributes.sh Tool

listElasticEventAttributes.sh Tool

Description: This tool gathers Elasticsearch event attributes for the number of days specified with the days value into a CSV file that can be used to prepare a custom Elastic Search Event Attribute Template file. This file can be uploaded to replace the default Event Attribute template, potentially reducing the number of Event Attributes that Elasticsearch needs to search by default. For information on where to upload the custom file, see Configuring Elasticsearch Based Deployments.

Usage: `[root@FortiSIEM]#listElasticEventAtributes.sh` *`destURL httpPort(9200)`* `[`*`user passwd`*`]` *`dayssocketTimeoutInMinuteoutputFile`*

Argument	Description
`destURL`	The destination URL, normally the Elasticsearch URL.
`httpPort`	The port number used to connect to Elasticsearch.
`user`	Use your login username to access Elasticsearch.
`password`	Use your password associated with the username to access Elasticsearch
`days`	The number of days you want this custom configuration to be applied, starting when the custom template is added to your Elasticsearch Based Deployment.
`socketTimeoutInMinute`	The maximum time out period value in minutes for the socket .
`outputFile`	The name you wish to name your output file.

Notes:

1. You can change an Event Attribute type per your requirements if the default type is not suitable, but you will need to upload the custom Event Attribute template afterward.
2. This tool is located in `/opt/phoenix/config/javaQueryServer/`.

Example:

```
[root@FortiSIEM javaQueryServer# ./listElasticEventAttributes.sh https://172.30.56.180
9200 "username" "password" 3 10 /tmp/1.csv
```

Managing Events in EventDB

- TestDBPurger Tool
- EnforceRetentionPolicy Tool
- TestSegment Reader Tool

TestDBPurger Tool

Description: This tool is used to delete data for a single date.

Usage: `TestDBPurger {EVENTDB} {DEST} {MODE} {CUSTID} {DATES}`

Argument	Description
`EVENTDB`	The eventDB directory, for example: /data/eventdb.
DEST	The directory to retain output data.
MODE	Control where to put processed (purged) data. 0 - Output the processed DB to destDir. It is possible to copy it back to eventDB manually. 1 - Output the processed DB to eventDB to make it effect for query. Move original data to destDir.
CUSTID	Customer ID for the organization to be purged.
DATES	Comma separated list of dates or date-range to process. A date is specified as the number of days since the UNIX epoch, 1970-01-01. A date-range is range specified by two dates inclusively separated by '-'. Use the following Linux command to generate a epoch date (**Note**: Replace *MM/DD/YYYY* with actual date): echo $(($(date --utc --date="*MM/DD/YYYY*" +%s)/86400))

Notes:

1. You should only use this script to delete data for a single date and organization. If you try to delete data for multiple dates, the script may fail.
2. The script is located at `/opt/phoenix/bin/TestDBPurger`. Run it in terminal mode and follow the instructions.
3. Should be run as admin user.
4. Make sure enough space is available for the directory holding the output data (/tmp/eventdb in the example) which is actually a backup of events and can be deleted later if not needed.

Example:

```
TestDBPurger /data/eventdb /tmp/eventdb 1 2000 16230,16233-16235
```

EnforceRetentionPolicy Tool

Description: This tool can be used to enforce retention policy on dates earlier than the retention policy normally covers.

Usage: `EnforceRetentionPolicy {DATES}`

Argument	Description
DATES	Comma separated list of dates or date-range on which to enforce retention policy. DATES is specified as the number of days since the UNIX epoch began, 1970-01-01. A date-range can be specified by two dates inclusively separated by '-'. Use the following Linux command to generate a epoch date (**Note**: Replace *MM/DD/YYYY* with actual date): echo $(($(date --utc --date="*MM/DD/YYYY*" +%s)/86400))

Notes:

1. Run the tool as admin user.

Example:

```
EnforceRetentionPolicy 16230,16233-16235
```

This example command enforces retention policies on these dates: 6/8/2014 and from 6/11/2014 to 6/13/2014.

TestSegmentReader Tool

Description: This tool is used to quickly read data segments in the eventDB through the command line. You can use this to manually inspect data integrity and parsed event attributes.

Usage: `TestSegmentReader {segmentDir}`

Argument	Description
segmentDir	The segment directory.

Notes:

1. Run the tool as admin user.

Example:

```
TestSegmentReader /archive/CUSTOMER_3/default/17897/429628-423551-172384880/seg-1-0-
300000-1545300800-1543305001/
```

Managing FortiSIEM Operations

The following tools are provided:

- phstatus Tool
- phtools Tool

phstatus Tool

Description: This tool is used to check the status of services on FortiSIEM. It lists the status of services running in FortiSIEM

Usage: `phstatus`

Notes:

1. Run the tool as admin user.
2. Run `phstatus -a` from the root account, and it shows the detailed status of all FortiSIEM processes along with events per second and local I/O rates.

phtools Tool

Description: This tool allows you to start and stop backend processes, and also lets you get change log information. When you upgrade your deployment, for example, you would use phTools to stop all backend processes.

Usage:`phtools {--changelog ([ALL | ERROR | TRACE | INFO | DEBUG | CRITICAL]) | --start {[ALL | <PROCESS>]}| --stop {[ALL | <PROCESS>]}| --stats (ALL | <PROCESS>)}`

Argument	Description
`--changelog`	Use ERROR, TRACE, INFO, DEBUG, or CRITICAL to get specific change log information.
`--start`	Start a specific process, or start all processes.
`--stop`	Stop a specific process, or stop all processes.
`--stats`	Get statistics for a specific process or for all processes.
PROCESS	The name of the FortiSIEM process. Examples: `phDataPurger`, `phDiscover`, `phMonitor`, `phParser`.

Notes:

1. Run the tool as admin user.

Examples:

```
phtools --start all
phtools --stop all
phtools --start phDataPurger
phtools --stop phDataPurger
```

ClickHouse Usage Notes

- ClickHouse Index Design
- ClickHouse Operational Overview
- ClickHouse Query Optimization Guidelines
- Handling ClickHouse Node IP Change
- ClickHouse Backup and Restore Steps
- Deleting ClickHouse Organization Data
- Rebalancing Shards
- Advanced Operations
- Migrating ClickHouse Events from FortiSIEM 6.5.x to 6.6.0 or Later
- Post-7.1.1 Upgrade ClickHouse IP Index Rebuilding
- Reference

ClickHouse Index Design

ClickHouse uses Primary indices and Data Skipping indices to speed up queries. See the following links for more information:

Primary Index: https://clickhouse.com/docs/en/optimize/sparse-primary-indexes

Data Skipping Index: https://clickhouse.com/docs/en/optimize/skipping-indexes

Other helpful links:

https://clickhouse.com/docs/en/concepts/why-clickhouse-is-so-fast

In ClickHouse, the following event attributes are configured as Primary and data Skipping indices.

Primary Indices:

- phCustId (Organization ID)
- eventType (Event Type)

Data Skipping Indices:

- reptDevIpAddr (Reporting IP)
- reptDevName (Reporting Device Name)
- customer (Organization Name)
- eventId (Event ID)
- phEventCategory (System Event Category)
- collectorId (Collector ID)
- srcIpAddr (Source Ip Address)
- destIpAddr (Destination Ip Address)
- destIpPort (Destination TCP/UDP Port)
- user (User)
- hostIpAddr (Host Ip Address)
- hostName (Host Name)
- fileName (File Name)
- procName (Process Name)
- appName (Application Name)

ClickHouse Operational Overview

The following ClickHouse background topics are available.

- Shards and Replicas
- ClickHouse Related Processes
- Supervisor/Worker Nodes Running ClickHouse Functions
- ClickHouse Keeper Cluster Considerations
- Event Insertion Flow
- Event Replication Flow
- Query Flow

Shards and Replicas

A shard is a database partition designed to provide high insertion and query rates. Events are written to and read from multiple shards in parallel. You need to choose the number of shards based on your incoming EPS (see example below and the latest ClickHouse Sizing Guide located in Fortinet Documents Library here).

If you want replication, then you can have replicas within each shard. ClickHouse will replicate database writes to a node within a shard to all other replicas within the same shard. A typical choice for replication size = 2, implying that you will have 2 nodes in each shard. A replica provides (a) faster queries and (b) prevents data loss in case a node goes down.

It is important to understand how ClickHouse insertion, Replication and Query works in FortiSIEM.

If adding a new shard to an existing cluster, the data must be manually rebalanced as described in the Scaling FortiSIEM within ClickHouse section of the Reference Architecture, with detailed steps at Rebalancing Shards.

ClickHouse Related Processes

ClickHouse is a distributed database with replication capabilities. FortiSIEM Supervisor and Worker software images include ClickHouse binaries. The user does not need to install anything else. You can configure a ClickHouse cluster from the FortiSIEM GUI.

There are two main ClickHouse processes:

- `ClickHouseServer` process: This is the ClickHouse Database Service.
- `ClickHouseKeeper` process: This is the ClickHouse Keeper Service providing Replication Management.

In addition, two more FortiSIEM processes provide ClickHouse related services:

- `phClickHouseMonitor` process: This runs on the Supervisor and Worker nodes and provides the following services:
  - On Supervisor/Worker nodes: CMDB Group Query helper, Lookup Table Query helper and DeviceToCMDBAttr Query helper.
  - On Supervisor node only: Provides Online data display and the list of available ClickHouse nodes.
- `phMonitor` process: Provides ClickHouse configuration management on Supervisor node.

Supervisor/Worker Nodes Running ClickHouse Functions

A FortiSIEM Supervisor/Worker node can be of 3 types (not mutually exclusive):

- ClickHouse Keeper Node: This node runs ClickHouse Keeper service providing replication management.
- ClickHouse Data Node: This node inserts events into ClickHouse database.
- ClickHouse Query Node: This node provides ClickHouse query services.

FortiSIEM Supervisor/Worker node can be a specific node only, or a mix of the 3 node types. For example:

Small EPS Environments: One Supervisor node that is a Keeper, Data and Query node

Medium EPS Environments:

- Supervisor node as ClickHouse Keeper Node. Note that 2 additional Keeper nodes are recommended (see ClickHouse Keeper Cluster Considerations).

High EPS Environments (Option 1):

- Supervisor node does not run any ClickHouse service
- 3 separate Worker nodes as ClickHouse Keeper Nodes - these form the ClickHouse Keeper cluster (see ClickHouse Keeper Cluster Considerations).
- N Worker nodes, with each node acting as both ClickHouse Data Node and ClickHouse Query Node - these form the ClickHouse Database cluster.

High EPS environments (Option 2):

- Supervisor node does not run any ClickHouse service
- 3 separate Worker nodes as ClickHouse Keeper Nodes – these form the ClickHouse Keeper cluster (see ClickHouse Keeper Cluster Considerations).
- A ClickHouse Database cluster consisting of
  - N/2 Worker nodes as ClickHouse Data Node only
  - N/2 Worker nodes as ClickHouse Query Node only

In Option 1, events are ingested at all N nodes, query goes to all N nodes. In Option 2, events are ingested in N/2 nodes and queried from N/2 nodes. There are other options with N/2 Data Only nodes and N Query Nodes for better query performance. Option 1 is the most balanced Option that has been seen to work well.

ClickHouse Keeper Cluster Considerations

ClickHouse Keeper provides the coordination system for data replication and distributed DDL queries execution. You should use odd number of nodes in Keeper Cluster for maintaining quorum, although ClickHouse Allows even number of nodes.

- If you use 3 nodes and lose 1 node, the Cluster keeps running without any intervention.
- If you use 2 nodes and lose 1 node, then quorum is lost. You need to use the following steps in Recovering from Losing Quorum in ClickHouse Cluster to recover quorum.
- If you use 1 node and lose that node, then the ClickHouse event database becomes read only and insertion stops. You need to use the following steps in Recovering from Complete Loss of ClickHouse Keeper Cluster to recover the ClickHouse Keeper database.

Note that for high EPS environments, ClickHouse recommends running ClickHouse Keeper and Database services on separate nodes, to avoid disk and CPU contention between Query and Replication Management engines. If you have powerful servers with good CPU, memory and high throughput disks, and EPS is not high, it may be reasonable to co-locate ClickHouse Keeper and Data/Query nodes.

See ClickHouse Reference in the Appendix for related information.

Event Insertion Flow

1. Collectors send events to the Worker list specified in **ADMIN > Settings > System > Event Worker**.
2. Data Manager process on each Worker node will first select a ClickHouse Data Node and insert to that node. It may be local or remote.

Event Replication Flow

1. After insertion, ClickHouse Data Node will inform a ClickHouse Keeper Node.
2. The ClickHouse Keeper Node initiates replication to all other nodes in the same shard.

Query Flow

1. GUI sends request to App Server which sends to Query Master on Supervisor
2. Query Master provides Query management. It sends the request to a (randomly chosen) ClickHouse Query node. Each query may go to a different ClickHouse Query node.
3. The ClickHouse Query node co-ordinates the Query (like Elasticsearch Coordinating node)
   a. It sends the results to other ClickHouse Query nodes
   b. It generates the final result by combining partial results obtained from all ClickHouse Query nodes
   c. It sends the result back to Query Master
4. Query Master sends the results back to App Server; which in turn, sends it back to GUI.

ClickHouse Query Optimization Guidelines

See ClickHouse Index Design for list of ClickHouse Primary and Data Skipping indices.

Primary indices provide the best query performance followed by Data Skipping indices. The following guidelines are recommended for best query performance.

1. Use Primary indices in Filter conditions as much as possible.
2. Use Data Skipping indices in Query Filter conditions, specially when Primary indices are not possible.
3. Operator usage:
   - Operator "=" provides best performance.
   - Operators "IN" and "NOT IN" with a small set provides good performance. For these queries, a direct SQL Query is performed by enumerating the set, until the size of the resulting SQL Query is less than 200KB. When the size of the SQL Query is more than 200KB, the query is converted into a LookupTable query, which are somewhat slower. For an end user, it is not possible to measure the size of the SQL Query, but the general idea is to use as narrow a group as the problem dictates.
   - CONTAIN and REGEXP queries for string valued attributes may be relatively slow, unless there are additional conditions using Primary/Data Skipping indices in the same Filter condition.

In conclusion, the general idea is to choose the *narrowest possible Filter Condition by always including ClickHouse Primary and Data skipping indices*.

Examples

Queries with Filter conditions like "*Raw Event Log* CONTAIN "User1"" will perform poorly, since *Raw Event Log* is neither a Primary index nor a Data Skipping index. To improve query performance, consider adding Primary index or Data Skipping index to the Filter condition, e.g.

1. *Event Type* = "*FortiGate Traffic Denied*" AND *Raw Event Log* CONTAIN "User1"
2. *Event Type* IN "*Denied Traffic*" AND *Raw Event Log* CONTAIN "User1"
3. *Event Type* IN "*Regular Traffic*" AND *Raw Event Log* CONTAIN "User1"

Option 1 will provide better performance than Option 2. Option 2 will likely perform better than Option 3 since *Regular Traffic* event group has 1500+ members while *Denied Traffic* event group has about 700 members, therefore the SQL Query in Option 3 has a higher probability of crossing the 200KB size limit.

As another example, a query with Filter conditions like "*Win Logon Id* = 2" will also perform poorly, since *Win Logon Id* is neither a Primary index nor a Data Skipping index. To improve performance, change the filter condition to

- *Event Type* = "Win-Security-4624" AND *Win Logon Id* = 2

Handling ClickHouse Node IP Change

IP address are embedded in various ClickHouse configuration files and Redis. If you change the IP address of any ClickHouse node, then take these following steps to restore communication.

Step 1: If Keeper node IP changed, then update ClickHouse Keeper registry file on all Keeper nodes to reflect the new IP address.

1. Login to the node.
2. Open the file `data-clickhouse-hot-1/clickhouse-keeper/conf/keeper.xml`.
3. Change the following section for the node whose IP changed.

```
<raft_configuration>
   <server>
     <id>1</id>
     <hostname>172.30.57.174</hostname>
     <port>3888</port>
   </server>
   <server>
     <id>2</id>
     <hostname>172.30.57.175</hostname>
     <port>3888</port>
   </server>
 </raft_configuration>
```

Step 2: If Data/Query node IP changed, then update ClickHouse Keeper file on all ClickHouse Data/Query nodes.

1. Login to the node.
2. Open the file `/etc/clickhouse-server/config.d/zookeeper.xml`.
3. Change the following section.

```
<zookeeper>
    <node>
```

```
      <host>172.30.57.174</host>
      <port>2181</port>
    </node>
    <node>
      <host>172.30.57.175</host>
      <port>2181</port>
    </node>
  </zookeeper>
```

Step 3: If Keeper node IP changed, then update Redis key of ClickHouse Keeper node from Supervisor.

1. Login to Supervisor node.
2. Run the following command to find out the list of ClickHouse Keeper IP addresses.

```
#redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
cache:ClickHouse:clickhouseKeeperNodes
```

Example Execution and Output:

```
# redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
cache:ClickHouse:clickhouseKeeperNodes
Warning: Using a password with '-a' or '-u' option on the command line interface
may not be safe.
"172.30.57.235"
```

3. Update the IP list with the new IP address.

```
#redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
cache:ClickHouse:clickhouseKeeperNodes '<new_ip_list>'
```

Example Execution and Output:

```
# redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
cache:ClickHouse:clickhouseKeeperNodes '172.30.57.230'
Warning: Using a password with '-a' or '-u' option on the command line interface
may not be safe.
OK
```

Step 4: If Data/Query node IP changed, then update Redis key of ClickHouse Data/Query node.

1. Login to Supervisor node.
2. Run the following command to find out the list of ClickHouse Keeper IP addresses.

```
#redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
cache:ClickHouse:clickhouseNodes
```

Example Execution and Output:

```
# redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` get
cache:ClickHouse:clickhouseNodes
Warning: Using a password with '-a' or '-u' option on the command line interface
may not be safe.
"172.30.57.235"
```

3. Update the IP list with the new IP address.

```
#redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
cache:ClickHouse:clickhouseNodes '<new_ip_list>'
```

Example Execution and Output:

```
# redis-cli -p 6666 -a `phLicenseTool --showRedisPassword` set
cache:ClickHouse:clickhouseNodes '172.30.57.230'
Warning: Using a password with '-a' or '-u' option on the command line interface
may not be safe.
OK
```

Step 5: If Data/Query node IP changed, then update interserver_http_host and cluster file on this node where the IP changed.

`interserver_http_host` is the ip/hostname that can be used by other ClickHouse node to access this node.

1. Login to the Data/Query node where the IP changed.
2. Open `/etc/clickhouse-server/config.d/interserver_http_host.xml` file.
3. Change the following section to reflect the new IP.

```
<yandex>

  <interserver_http_host>172.30.58.241</interserver_http_host>

</yandex>
```

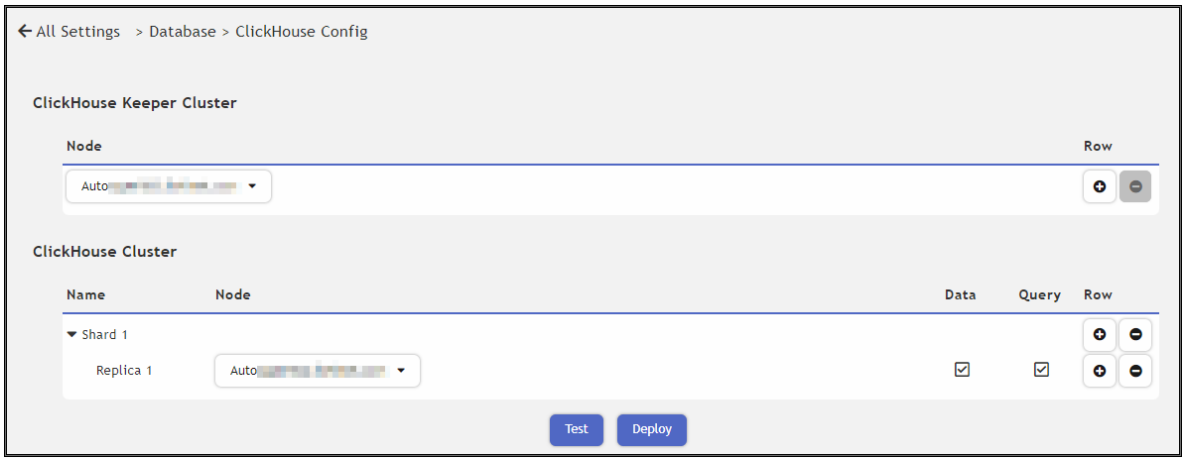
4. Update the IP address by opening the `/etc/clickhouse-server/config.d/cluster.xml` file.
5. Change the following section to reflect the new IP. In this example: 172.30.58.241.

```
<yandex>

  <remote_servers>
    <fsiem_cluster>
      <shard>
        <internal_replication>true</internal_replication>
        <replica>
          <host>172.30.58.241</host>
          <port>9000</port>
        </replica>
      </shard>
```

```
    </fsiem_cluster>
  </remote_servers>

</yandex>
```

Step 6: Test and Save from FortiSIEM GUI

1. Login to the GUI.
2. Go to **ADMIN > Settings > Database > ClickHouse Config**.
3. Click **Test**.
4. If successful, then click **Deploy**.



ClickHouse Backup and Restore Steps

This section covers the following ClickHouse backup/restore options:

- Backup to Remote SFTP Server
- Restore from Remote SFTP Server
- Backup to AWS S3
- Restore from AWS S3

Backup to Remote Server via SFTP

Backing up ClickHouse to a remote server via SFTP is done by creating a cron job to schedule a daily backup. The general steps that follow provide instructions to set up your cron job and verify that the backup is functioning.

Note: The following commands need to be run as root user in FortiSIEM.

- Step 1: Prepare the SFTP server
- Step 2: SSH to FortiSIEM node and Copy the ClickHouse Backup Config File
- Step 3: Modify the ClickHouse Backup Config File
- Step 4: Add a Crontab Job to Run the Backup Task Daily
- Step 5: Monitor the /var/log/clickhouse-backup.log to Verify if the Backup Task Happens Correctly
- Step 6: Back up All Other Shards

Step 1: Prepare the SFTP server

First install an SFTP server.

Then, edit `/etc/ssh/sshd_config` and ensure the following is configured.

```
#SFTP
Match Group <GROUP>
ChrootDirectory /<SFTP HOME>/%u
AllowTcpForwarding No
ForceCommand internal-sftp
```

Save and restart `sshd` by issuing the following command.

```
systemctl restart sshd
```

Next, create the SFTP user on the SFTP server by running the following commands.

```
useradd -d /<SFTP HOME>/<USER> -s /bin/false -g users -G <GROUP> <USER>
passwd <USER>
```

Test the SFTP connection. First `ssh` into another machine and try to `sftp` a file to the SFTP server.

```
sftp <USER>@<SFTP SERVER>
```

If you want to use SSH Keys for authentication, instead of a password, then take the following steps.

1. Create SSH key for SFTP user on FortiSIEM by issuing:

   ```
   ssh-keygen -C <USER>@<SFTP SERVER IP>
   ```

2. Take the generated public key and copy it to the SFTP server under `/<SFTP HOME>/<USER>/.ssh/authorized_keys`.
3. Restart sushi by issuing the following on the SFTP server.

   ```
   systemctl sshd restart
   ```

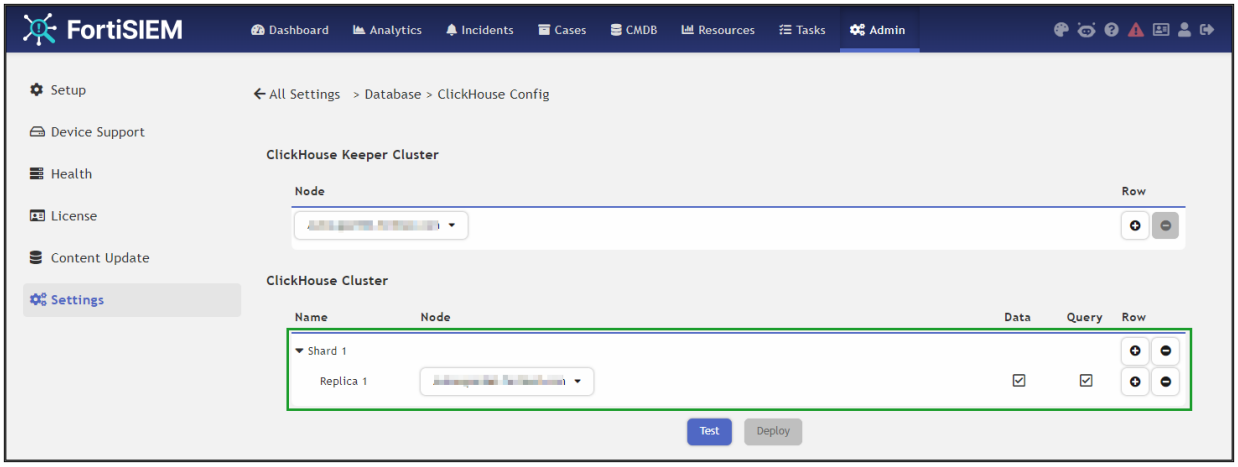
4. Now attempt to do `sftp` using SSH keys by running

   ```
   sftp <USER>@<SFTP SERVER>
   ```

The login should not ask for a password and it should be successful.

In Steps 2-5 below, you will create a process for backing up Shard 1 Replica 1. In Step 6, you will repeat this process for Replica 1 for all other shards.

To identify the FortiSIEM node hosting the first replica for the first shard, navigate to **Admin > Settings > Database > ClickHouse Config**, and look at the first line to see if it is Shard 1 Replica 1.



Step 2: SSH to FortiSIEM node and Copy the ClickHouse Backup Config File

Run the following command to copy the ClickHouse backup configuration from FortiSIEM to the backup server.

`cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup`

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml
/etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
[root@Autosuper56206 ~]#
```

Step 3: Modify the ClickHouse Backup Config File

Edit the `/etc/clickhouse-backup/config.yml` file. In the general section, set `remote_storage` to `sftp` and add the sftp server information in the sftp section. This is required for the cron job in Step 4. After modifying the file, run the following command.

`cat /etc/clickhouse-backup/config.yml`

The file content should look similar to the following (if using password):

```
general:
  remote_storage: sftp
… …
sftp:
  address: "172.30.56.216"
  port: 22
  username: "sftpuser"
  password: "password"
  key: ""
  path: "clickhouse-backup"
  compression_format: tar
  compression_level: 1
  concurrency: 1
  debug: false
…
```

If using SSK keys, the password should be empty and the key should be SSH PRIV KEY PATH , e.g.

```
general:
  remote_storage: sftp
… …
sftp:
  address: "172.30.56.216"
  port: 22
  username: "sftpuser"
  password: ""
  key: "/root/.ssh/id_rsa"
```

```
  path: "clickhouse-backup"
  compression_format: tar
  compression_level: 1
  concurrency: 1
  debug: false
…
```

Step 4: Add a Crontab Job to Run the Backup Task Daily

Run the following command to create a cron job that runs a daily backup task:

```
echo "0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-clickhouse-backup.sh >> /var/log/clickhouse-backup.log" >> /etc/cron.d/fsm-crontab
```

Verify the scheduled job is created as requested by running the following command:

```
cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-backup
```

Example Execution and Output:

```
[root@Autosuper56206 ~]# cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-backup
0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-clickhouse-backup.sh >> /var/log/clickhouse-backup.log
[root@Autosuper56206 ~]#
```

Step 5: Monitor the /var/log/clickhouse-backup.log to Verify if the Backup Task Happens Correctly

If Steps 2-4 were properly executed, you will see a log similar to the following:

```
2023-08-07T20-47-05: clickhouse-backup create and upload backup_shard1_2023-08-07T20-47-01 succeeded
```

Step 6: Back up All Other Shards

Now repeat Steps 2-5 for the first replica of every other existing shard that have not been backed up. You should see a log appear for each shard.

This is a sample log for after you have configured backup for shard2:

```
2023-08-07T20-56-04 clickhouse-backup create and upload backup_shard2_2023-08-07T20-56-01 succeeded
```

Restore from Remote SFTP Server

The following general steps that follow provide instructions that will restore a ClickHouse backup from a remote server.

The restore process removes all existing data in the destination table before populating with data from the backup. Please take caution before proceeding with the restore operation. Fortinet recommends creating a backup of the most recent days' data to prevent loss of any information that may not have been fully captured by the ClickHouse backup tool.

- Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File
- Step 2: Modify the ClickHouse Backup Config File
- Step 3: Drop Schema Objects, then Download and Restore Schema Only for the fsiem.events_replicated Table
- Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for the fsiem.events_replicated Table
- Step 5: Verify the Event Count in the FortiSIEM Setup
- Step 6: Restore Other Existing Shards

Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File

This operation must be run on every ClickHouse replica node.

Prepare the FortiSIEM setup where the ClickHouse database will be restored. Then SSH to FortiSIEM node and copy the ClickHouse backup config file to the right location by running the following command:

```
cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup
```

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml
/etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
[root@Autosuper56206 ~]#
```

Step 2: Modify the ClickHouse Backup Config File

This operation must be run on every ClickHouse replica node. This is required for the restore process from your SFTP server.

Modify the backup config file - `/etc/clickhouse-backup/config.yml` as follows:

Set the `remote_storage` in the general section to `sftp`. Then add the SFTP server information in sftp section. After you have modified the backup config file, run the following command:

`cat /etc/clickhouse-backup/config.yml`.

The file content should look similar to the following:

```
general:
  remote_storage: sftp
… …

sftp:
  address: "172.30.56.216"
  port: 22
  username: "sftpuser"
  password: "password"
  key: ""
  path: "clickhouse-backup"
  compression_format: tar
  compression_level: 1
  concurrency: 1
  debug: false
…
```

Do the restoration Steps 3-5 for every shard.

Step 3: Drop Schema Objects, then Download and Restore Schema Only for the fsiem.events_replicated Table

This operation must be run on every ClickHouse replica node.

Find the backup name that needs be restored from the SFTP server, e.g. backup_shard1_2023-08-07T20-47-01. Then run the following commands:

```
backup="backup_shard1_2023-08-07T20-47-01"
```

```
/usr/bin/clickhouse-backup restore_remote --rm --schema -t fsiem.events_replicated
"${backup}"
```

```
clickhouse-backup delete local "${backup}"
```

Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for the fsiem.events_replicated Table

This operation must be run on the first ClickHouse replica node of one shard.

Run the following two commands:

```
/usr/bin/clickhouse-backup restore_remote --rm -t fsiem.events_replicated "${backup}"
```

```
clickhouse-backup delete local "${backup}"
```

```
2023/08/07 15:29:36:182204 info done                      backup=backup_shard1_2023-08-
07T20-47-01 operation=restore table=fsiem.events_replicated
2023/08/07 15:29:36:182243 info done                      backup=backup_shard1_2023-08-
07T20-47-01 duration=559ms operation=restore
2023/08/07 15:29:36:182254 info done                      backup=backup_shard1_2023-08-
07T20-47-01 operation=restore
```

Step 5: Verify the Event Count in the FortiSIEM Setup

Run the following command to verify the event count in your FortiSIEM.

```
echo 'select count() from fsiem.events_replicated' | curl 'http://#.#.#.#:8123/' --data-
binary @-;
```

where #.#.#.# is your FortiSIEM IP address.

Example Execution and Output:

```
[root@Autoworker56226 ~]# echo 'select count() from fsiem.events_replicated' | curl
'http://172.30.56.225:8123/' --data-binary @-;echo 'select count() from fsiem.events_
replicated' | curl 'http://172.30.56.226:8123/' --data-binary @-; echo 'select count() from
fsiem.events_replicated' | curl 'http://172.30.56.224:8123/' --data-binary @-;
1065479
531974
1065479
```

Step 6: Restore Other Existing Shards

Repeat Steps 3-5 for all other shards that need to be restored. Note that the backup file will be different for every shard.

Backup to AWS S3

Backing up ClickHouse on AWS 3 is done by creating a cron job to schedule a daily backup. The general steps that follow provide the instructions to set up your cron job and verify that the backup is functioning.

- Step 1: Prepare the S3, Modify its Permission Policy
- Step 2: SSH to FortiSIEM Node and Copy the ClickHouse Backup Config File
- Step 3: Modify the ClickHouse Backup Config File
- Step 4: Add a Crontab Job to Run the Backup Task Daily
- Step 5: Verify that the Backup Task is Happening Correctly
- Step 6: Back up All Other Existing Shards

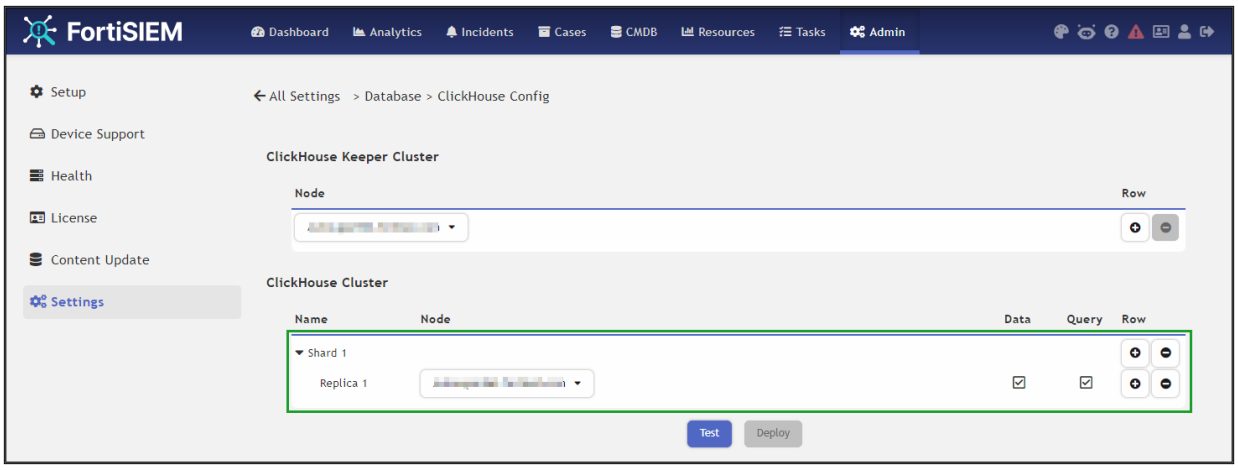
Step 1: Prepare the S3, Modify its Permission Policy

Modify your S3 permission policy.

```
{
	"Version": "2012-10-17",
	"Id": "PolicyXXXX",
	"Statement": [
		{
			"Sid": "StmtXXXX",
			"Effect": "Allow",
			"Principal": {
				"AWS": "arn:aws:iam::XXXX:user/USER"
			},
			"Action": "s3:*",
			"Resource": "arn:aws:s3:::USER-clickhouse-backup-restore"
		}
	]
}
```

Log in to the FortiSIEM node hosting the first replica for first shard and follow Steps 2-5.

To identify the FortiSIEM node hosting the first replica for the first shard, navigate to **Admin > Settings > Database > ClickHouse Config**, and look at the first line to see if it is Shard 1 Replica 1.



Step 2: SSH to FortiSIEM Node and Copy the ClickHouse Backup Config File

Copy the ClickHouse backup configuration file from your FortiSIEM to AWS S3 by running the following command:

`cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup`

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml
/etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
[root@Autosuper56206 ~]#
```

Step 3: Modify the ClickHouse Backup Config File

Edit the `/etc/clickhouse-backup/config.yml` file. In the general section, set the `remote_storage` to `s3`. Then add the S3 credentials and bucket information in the s3 section. This is required for the cron job in Step 4.

When you run the following command, your `etc/clickhouse-backup/config.yml` file content should be similar to the following.

`cat /etc/clickhouse-backup/config.yml`

```
general:
  remote_storage: s3
… …
```

```
s3:
  access_key: "XXXXXXX"
  secret_key: "XXXXXXX"
  bucket: "XXXX-clickhouse-backup-restore"
  endpoint: ""
  region: us-east-1
  acl: private
  assume_role_arn: ""
  force_path_style: false
  path: "clickhouse-backup"
  disable_ssl: false
  compression_level: 1
  compression_format: tar
  sse: ""
  disable_cert_verification: false
  use_custom_storage_class: false
  storage_class: STANDARD
  concurrency: 1
  part_size: 0
  max_parts_count: 10000
  allow_multipart_download: false
  debug: false
…
```

Step 4: Add a Crontab Job to Run the Backup Task Daily

Run the following command to create a cron job that runs a daily backup task:

```
echo "0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-clickhouse-backup.sh >> /var/log/clickhouse-backup.log" >> /etc/cron.d/fsm-crontab
```

Verify the job is created as requested:

```
cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-backup
```

Example Execution and Output:

```
[root@Autosuper56206 ~]# cat /etc/cron.d/fsm-crontab | grep -i cron-clickhouse-backup
0 1 * * * root /opt/phoenix/phscripts/clickhouse/backup_restore/cron-clickhouse-backup.sh >> /var/log/clickhouse-backup.log
[root@Autosuper56206 ~]#
```

Step 5: Verify that the Backup Task is Happening Correctly

Monitor the `/var/log/clickhouse-backup.log` file. If the backup task happens, then you will see a log entry similar to the following.

```
2023-08-07T21-26-48: clickhouse-backup create and upload backup_shard1_2023-08-07T21-26-01
succeeded
```

Step 6: Back up All Other Existing Shards

Now repeat Steps 2-5 for the first replica of every other shard. This is a sample log for after you have configured backup for shard2:

```
2023-08-07T21-26-27: clickhouse-backup create and upload backup_shard2_2023-08-07T21-26-01
succeeded
```

Restore from AWS S3

The general steps that follow provide instructions that will restore ClickHouse from your AWS S3 backup.

- Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File
- Step 2: Modify the ClickHouse Backup Config File
- Step 3: Drop Schema Objects, then Download and Restore Schema Only for fsiem.events_ replicated Table
- Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for fsiem.events_ replicated Table
- Step 5: Verify the Event Count in the FortiSIEM Setup
- Step 6: Restore All Other Shards

Step 1: Prepare the FortiSIEM Setup and Copy the ClickHouse Backup Config File

This operation has to be run on every ClickHouse replica node.

Prepare the FortiSIEM setup where the ClickHouse database will be restored. Then SSH to FortiSIEM node and copy the ClickHouse backup config file to the right location by running the following command:

```
cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml /etc/clickhouse-backup
```

Example Execution and Output:

```
[root@Autosuper56206 ~]# cp /opt/phoenix/phscripts/clickhouse/backup_restore/config.yml
/etc/clickhouse-backup
[root@Autosuper56206 ~]# ll /etc/clickhouse-backup/
total 8
-rwxr-xr-x 1 root root 3146 Aug  7 11:53 config.yml
-rw-r--r-- 1 root root 3112 Dec 26  2022 config.yml.example
[root@Autosuper56206 ~]#
```

Step 2: Modify the ClickHouse Backup Config File

This operation has to be run on every ClickHouse replica node.

Modify the backup config file - `/etc/clickhouse-backup/config.yml` as follows:

Set the `remote_storage` in the general section to `s3`. Then add the S3 information in the s3 section. After your edit, run the following command:

`cat /etc/clickhouse-backup/config.yml`

The file content will look similar to the following:

```
general:
  remote_storage: s3
… …
```

```
s3:
  access_key: "XXXXXXX"
  secret_key: "XXXXXXX"
  bucket: "XXXX-clickhouse-backup-restore"
  endpoint: ""
  region: us-east-1
  acl: private
  assume_role_arn: ""
  force_path_style: false
  path: "clickhouse-backup"
  disable_ssl: false
  compression_level: 1
  compression_format: tar
  sse: ""
  disable_cert_verification: false
  use_custom_storage_class: false
  storage_class: STANDARD
  concurrency: 1
  part_size: 0
  max_parts_count: 10000
  allow_multipart_download: false
  debug: false
…
```

Repeat the restoration Steps 3-5 for every shard.

Step 3: Drop Schema Objects, then Download and Restore Schema Only for fsiem.events_replicated Table

This operation must be run on every ClickHouse replica node.

Find the backup name that needs be restored from AWS S3, e.g. backup_shard1_2023-08-07T20-47-01. Then run the following commands:

```
backup="backup_shard1_2023-08-07T20-47-01"
```

```
/usr/bin/clickhouse-backup restore_remote --rm --schema -t fsiem.events_replicated "${backup}"
```

```
clickhouse-backup delete local "${backup}"
```

Step 4: Drop Schema Objects, then Download and Restore Both Schema and Data for fsiem.events_replicated Table

This operation must be run on the first ClickHouse replica node of one shard.

Run the following two commands:

```
/usr/bin/clickhouse-backup restore_remote --rm -t fsiem.events_replicated "${backup}"
```

```
clickhouse-backup delete local "${backup}"
```

```
2023/08/07 15:29:36:182204 info done                    backup=backup_shard1_2023-08-07T20-47-01 operation=restore table=fsiem.events_replicated
2023/08/07 15:29:36:182243 info done                    backup=backup_shard1_2023-08-07T20-47-01 duration=559ms operation=restore
2023/08/07 15:29:36:182254 info done                    backup=backup_shard1_2023-08-07T20-47-01 operation=restore
```

Step 5: Verify the Event Count in the FortiSIEM Setup

Verify the event count in your FortiSIEM by running the following command.

```
echo 'select count() from fsiem.events_replicated' | curl 'http://#.#.#.#:8123/' --data-binary @-;
```

where #.#.#.# is your FortiSIEM Supervisor IP address.

Example Execution and Output:

```
[root@Autoworker56226 ~]# echo 'select count() from fsiem.events_replicated' | curl
```

```
'http://172.30.56.224:8123/' --data-binary @-;echo 'select count() from fsiem.events_
replicated' | curl 'http://172.30.56.225:8123/' --data-binary @-; echo 'select count() from
fsiem.events_replicated' | curl 'http://172.30.56.226:8123/' --data-binary @-;
2327527
2327527
612053
```

Step 6: Restore All Other Shards

Repeat Steps 3-5 for all other shards that have not yet been restored. Note that the backup file will be different for every shard.

Deleting ClickHouse Organization Data

The following steps enable you to delete events belonging to an Organization in a Service Provider environment.

As a pre-requisite, collect the **Organization Id** for the "to-be-deleted" organization and the IP addresses of one data node from each shard.

1. Logon to any ClickHouse data node.
2. Run the following command as admin.
   `/opt/phoenix/phscripts/clickhouse/clickhouse-delete-org-events.sh <orgId> <data_node_shard1_ip>,<data_node_shard2_ip>`
   An example environment is provided below, for which we will run an example command.
   Shard1: Replica1: IP: 172.30.58.242
   Shard1: Replica2: IP: 172.30.58.243
   Shard2: Replica1: IP: 172.30.58.244
   Shard2: Replica2: IP: 172.30.58.245
   Org Id: 2002
   Run the following command:
   `/opt/phoenix/phscripts/clickhouse/clickhouse-delete-org-events.sh 2002 172.30.58.242,172.30.58.244`

This script uses ClickHouse Lightweight Delete concept, as illustrated here.

Rebalancing Shards

Suppose you have been running FortiSIEM on ClickHouse with one shard. The disks have become full, or your overall EPS has increased, and you want to add another shard. Then you should consider moving some data from the current shard (Shard1) to the new Shard (Shard2). Follow these steps to accomplish this objective.

1. Identify the Shard1 partition(s) that you want to move to Shard2.
2. For each partition to be moved, take the following steps:
   a. Logon to Supervisor node as admin.
   b. Copy the partition from Shard1 to one of the replicas of Shard2 running the following command. This is a replicated SQL, so you only need run it against one of the destination replicas.
   `clickhouse-client -h <Shard2_Replica1_IP> -q "ALTER TABLE fsiem.events_replicated FETCH PARTITION <partition_id> FROM '/clickhouse/tables/<source_shard_id>/fsiem.events'"`
   c. Detach the partition from the source shard by running the following command. This is a replicated SQL. You only need run it against one of the source replicas.
   `clickhouse-client -h <Shard1_Replica1_IP> -q "ALTER TABLE fsiem.events_replicated DETACH PARTITION <partition_id>"`
   d. Attach the partition to one of the destination replicas by running the following command. This is a replicated SQL. You only need run it against one of the destination replicas.
   `clickhouse-client -h <Shard2: Replica1_IP> -q "ALTER TABLE fsiem.events_replicated ATTACH PARTITION <partition_id>"`
   e. Delete the detached directories to release disk space by logging on to **each** node of Shard1 as root and running the following command. This is non-replicated SQL. You need run it against **all** source replicas.
   `clickhouse-client -q " select path from system.detached_parts where partition_id = '<partition_id>'" | xargs rm -rf`

Note: Data is not available for Query only during Step 2c and 2d above.

An example of shard rebalancing follows:

Suppose the existing ClickHouse Install has one shard (Shard1), and a new shard (Shard2) has been added.

Shard1: Replica1: IP: 172.30.58.242

Shard1: Replica2: IP: 172.30.58.243

Shard2: Replica1: IP: 172.30.58.244

Shard2: Replica2: IP: 172.30.58.245

To identify the partitions in Shard1 with the largest data, run the following command:

```
SELECT partition, formatReadableSize(sum(bytes_on_disk)) FROM system.parts where table = 'events_replicated' and active group by partition order by partition
```

The following example output appears:

```
┌─partition─────────┬─formatReadableSize(sum(bytes_on_disk))─┐
│ (18250,20231017) │ 3.15 GiB │
│ (18250,20231018) │ 3.15 GiB │
│ (18250,20231019) │ 3.71 GiB │
│ (18250,20231020) │ 7.85 GiB │
│ (18250,20231021) │ 7.99 GiB │
│ (18250,20231022) │ 8.00 GiB │
│ (18250,20231023) │ 5.61 GiB │
└──────────────────┴────────────────────────────────────────┘
```

Suppose you want to move partition (18250, 20231018) from Shard1 to Shard2. Proceed by taking the following steps:

1. **Copy Partition** (Step 2b above):
   `clickhouse-client -h 172.30.58.244 -q "ALTER TABLE fsiem.events_replicated FETCH PARTITION (18250, 20231018) FROM '/clickhouse/tables/1/fsiem.events'"`
2. **Detach Partition** (Step 2c above):
   `clickhouse-client -h 172.30.58.242 -q "ALTER TABLE fsiem.events_replicated DETACH PARTITION (18250, 20231018)"`
3. **Attach Partition** (Step 2d above):
   `clickhouse-client -h 172.30.58.244 -q "ALTER TABLE fsiem.events_replicated ATTACH PARTITION (18250, 20231018)"`
4. **Delete Detached Directories** (Step 2e above):
   a. Logon to Shard 1, Replica 1 (172.30.58.242).
   b. Run the following command as root:
      `clickhouse-client -q " select path from system.detached_parts where partition_id = '18250-20231018'" | xargs rm -rf`
   c. Logon to Shard 1, Replica 2 (172.30.58.243).
   d. Run the following command as root:
      `clickhouse-client -q " select path from system.detached_parts where partition_id = '18250-20231018'" | xargs rm -rf`

Advanced Operations

- Adding a Disk or Tier
- Deleting a Disk
- Deleting a Storage Tier
- Moving a Worker from One Shard to Another Shard
- Replacing a Worker with another Worker (within the same Shard)
- Recovering from Complete Loss of ClickHouse Keeper Cluster
- Recovering from Losing Quorum in ClickHouse Keeper Cluster
- Recovering from Read-Only Mode
- Mitigating a Non-Responsive ClickHouse Keeper Node

Adding a Disk or Tier

To add a disk or tier, take the following steps.

1. Navigate to **ADMIN > License > Nodes**.
2. Select the node which you wish to add a disk or tier.
3. Click **Edit**.
4. Update the **Storage Tiers** drop-down number to change the number to tiers.
5. Click **+** from the **Hot Tier** or **Warm Tier** Row column respectively to add another Hot Tier or Warm Tier field to add a disk.
6. Click **Test**.
7. Click **Save**.
8. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
9. Click **Test**.
10. Click **Deploy**.

Notes:

- After **Deploy** succeeds, `phClickHouseMonitor` and `ClickHouseServer` processes will restart.
- When additional disks are added, the data is written across all available disks. If a disk becomes full, then data will be written to the disks with free space until all disks are full, at which point data will be moved to other ClickHouse storage tiers, archived, or purged depending on your FortiSIEM configuration.

Deleting a Disk

To delete a disk, take the following steps.

1. Edit `/etc/fstab` and remove entry with target mount point. For example, for the target mount "/data-clickhouse=warm-1", you would delete a line similar to:
   `UUID=db920fd9-5cbb-454b-81b8-d6e427564ecf /data-clickhouse-hot-1 xfs defaults,nodev,noatime,inode 0 0`
2. Run the following command to sync fstab changes to the system.
   `systemctl daemon-reload`
3. Unmount the disk.
4. Delete the target mount point directory. For example, if the target mount point directory was "/data-clickhouse-warm-1", you would run the following command:
   `rm -rf /data-clickhouse-warm-1`
5. (Optional) To remove the data or reuse the disk as a ClickHouse data disk, format the disk by running the following command:
   `wipefs -a <device path>`
6. Navigate to **ADMIN > License > Nodes**.
7. Select the node with the disk you wish to delete.
8. Click **Edit**.
9. Click **-** from the **Hot Tier** or **Warm Tier** Row column respectively to remove the disk.
   Note: You may see some error logs getting generated in `/opt/clickhouse/log/clickhouse-server.err.log`.

```
2022.06.20 15:55:31.761484 [ 98091 ] {} <Warning> fsiem.events_replicated
(ReplicatedMergeTreePartCheckThread): Found parts with the same min block and with the
same max block as the missing part 18250-20220620_371_375_1 on replica 1. Hoping that
it will eventually appear as a result of a merge.

2022.06.20 15:55:31.764560 [ 98141 ] {} <Warning> fsiem.events_replicated
(ReplicatedMergeTreePartCheckThread): Checking part 18250-20220620_353_378_2

2022.06.20 15:55:31.764841 [ 98141 ] {} <Warning> fsiem.events_replicated
(ReplicatedMergeTreePartCheckThread): Checking if anyone has a part 18250-20220620_353_
378_2 or covering part.

2022.06.20 15:55:31.765138 [ 98141 ] {} <Error> fsiem.events_replicated
(ReplicatedMergeTreePartCheckThread): No replica has part covering 18250-20220620_353_
378_2 and a merge is impossible: we didn't find a smaller part with the same max block.

2022.06.20 15:55:31.766222 [ 98141 ] {} <Warning> fsiem.events_replicated (a5a85f1a-
6ebf-4cf1-b82b-686f928798cc): Cannot commit empty part 18250-20220620_353_378_2 with
error DB::Exception: Part 18250-20220620_353_378_2 (state Outdated) already exists, but
it will be deleted soon

2022.06.20 15:55:31.766574 [ 98141 ] {} <Warning> fsiem.events_replicated
(ReplicatedMergeTreePartCheckThread): Cannot create empty part 18250-20220620_353_378_2
instead of lost. Will retry later
```

These errors indicate that ClickHouse detected some missing data by comparing the local parts and the parts names stored in clickhouse-keeper. This is just a warning and does not affect operation. If you find this annoying, delete the entries in clickhouse-keeper by running the following commands on the Worker where the disk is deleted.

```
clickhouse-client --query "SELECT replica_path || '/queue/' || node_name FROM
system.replication_queue JOIN system.replicas USING (database, table) WHERE last_
exception LIKE '%No active replica has part%'" | while read i; do
/opt/zookeeper/bin/zkCli.sh deleteall $i; done
```

```
clickhouse-client --query "SYSTEM RESTART REPLICAS"
```

Reference: https://github.com/ClickHouse/ClickHouse/issues/10368

10. Click **Test**.
11. Click **Save**.
12. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
13. Click **Test**.
14. Click **Deploy**.

Note: After **Deploy** succeeds, `phClickHouseMonitor` and `ClickHouseServer` processes will restart.

Deleting a Storage Tier

To delete a storage tier, take the following steps for **EACH DISK** in the storage tier.

1. For EACH DISK in the storage tier, take the following steps.
   a. Edit `/etc/fstab` and remove entry with target mount point. For example, for the target mount "/data-clickhouse=warm-1", you would delete a line similar to:
   `UUID=db920fd9-5cbb-454b-81b8-d6e427564ecf /data-clickhouse-hot-1 xfs defaults,nodev,noatime,inode 0 0`
   b. Run the following command to sync fstab changes to the system.
   `systemctl daemon-reload`
   c. Unmount the disk.
   d. Delete the target mount point directory. For example, if the target mount point directory was "/data-clickhouse-warm-1", you would run the following command:
   `rm -rf /data-clickhouse-warm-1`
   e. (Optional) To remove the data or reuse the disk as a ClickHouse data disk, format the disk by running the following command:
   `wipefs -a <device path>`
   f. After following the above steps for **all** disks in the storage tier you wish to delete, proceed to step 2.
2. Navigate to **ADMIN > License > Nodes**.
3. Select the node with the disk you wish to delete.
4. Click **Edit**.
5. Change **Storage Tiers** from "2" to "1".
6. Click **Test**.

7. Click **Save**.
8. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
9. Click **Test**.
10. Click **Deploy**.

Note: After **Deploy** succeeds, `phClickHouseMonitor` and `ClickHouseServer` processes will restart.

Moving a Worker from One Shard to Another Shard

To move a Worker from one shard to another shard, take the following steps.

1. Remove the Worker from the ClickHouse Keeper and ClickHouse Cluster.
2. Login to the Worker and run the following commands.
```
clickhouse-client –q "DROP TABLE fsiem.events_replicated"
clickhouse-client –q "DROP TABLE fsiem.summary"
systemctl stop clickhouse-server
```
3. Login to any ClickHouse Keeper node and run the following commands to delete the registry entry from the ClickHouse Keeper cluster.
```
/opt/zookeeper/bin/zkCli.sh deleteall
/clickhouse/tables/<ShardID>/fsiem.events/replicas/<ReplicaID>
/opt/zookeeper/bin/zkCli.sh deleteall
/clickhouse/tables/<ShardID>/fsiem.summary/replicas/<ReplicaID>
```
4. Login to the Worker and navigate to `/etc/clickhouse-server/config.d`.
5. Remove all config xml under `/etc/clickhouse-server/config.d` **except** for `logger.xml`, `max_partition_size_to_drop.xml` and `max_suspicious_broken_parts.xml`.
6. Remove all config xml under `/etc/clickhouse-server/users.d/`.
7. For every disk in ClickHouse, take the following steps.
   a. Edit `/etc/fstab` and remove entry with target mount point. For example, for the target mount "/data-clickhouse=warm-1", you would delete a line similar to:
   ```
   UUID=db920fd9-5cbb-454b-81b8-d6e427564ecf       /data-clickhouse-hot-1      xfs
   defaults,nodev,noatime,inode 0 0
   ```
   b. Run the following command to sync fstab changes to the system.
   ```
   systemctl daemon-reload
   ```
   c. Unmount the disk.
   d. Delete the target mount point directory. For example, if the target mount point directory was "/data-clickhouse-warm-1", you would run the following command:
   ```
   rm -rf /data-clickhouse-warm-1
   ```
   e. (Optional) To remove the data or reuse the disk as a ClickHouse data disk, format the disk by running the following command:
   ```
   wipefs -a <device path>
   ```
   f. After following the above steps for **all** disks used by ClickHouse, proceed to step 8.
8. Login to the Supervisor GUI, and navigate to **ADMIN > Settings > Database > ClickHouse Config**.
9. Select the target Worker and delete it from the existing shard by clicking **-** from the Row column.

10. Click **Test**.
11. Click **Deploy**.
12. Navigate to **ADMIN > License > Nodes**.
13. Select the target Worker.
14. Click **Delete** to remove the target Worker.
15. Wait for the Supervisor `phMonitor` process to come up.
16. Re-add the target Worker into the License Node with the desired disk configuration, following the instructions for adding a Worker.
17. Wait for the Supervisor `phMonitor` process to com up again.
18. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
19. Add the target Worker to the destination shard.
20. Click **Test**.
21. Click **Deploy**.

Replacing a Worker with another Worker (within the same Shard)

Currently, the GUI allows you to choose to replace one Worker (W1) with another Worker (W2) in ClickHouse Configuration. However, clicking on Test will fail since the shard and replica Ids are in use by the previous Worker (W1).

Follow these steps to replace W1 with W2.

1. Navigate to **ADMIN > Settings > Database > ClickHouse Config**.
2. Note the shardID and ReplicaID of W1. If the GUI shows Shard 3 and Replica 2, the ShardID is 3 and ReplicaID is 2. This will be needed later in Step 7.
3. Delete W1 from the ClickHouse Cluster Table by clicking **-** from the Row column.
4. Click **Test**.
5. Click **Deploy**.
6. Login to W1 and run the following SQL command in clickhouse-client shell to drop the events table.
   `DROP TABLE fsiem.events_replicated`
7. Login to any ClickHouse Keeper node and run the following commands to delete the registry entry from the ClickHouse Keeper cluster.
   `/opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/fsiem.events/replicas/<ReplicaID>`
   `/opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/fsiem.summary/replicas/<ReplicaID>`
8. Add W2 from the ClickHouse Cluster Table in same place where W1 was. It can use the same Shard ID and Replica ID.
9. Click **Test**.
10. Click **Deploy**.

Recovering from Complete Loss of ClickHouse Keeper Cluster

Complete loss of Keeper cluster may happen if you have only 1 node and it goes down.

A normal ClickHouse cluster looks like this.

```
[root@FSM-660-CH-58-246 ~]# echo stat | nc <IP> 2181
ClickHouse Keeper version: v22.6.1.1985-testing-7000c4e0033bb9e69050ab8ef73e8e7465f78059
Clients:
[::ffff:172.30.58.246]:36518(recved=0,sent=0)

Latency min/avg/max: 0/0/0
Received: 0
Sent: 0
Connections: 0
Outstanding: 0
Zxid: 145730
Mode: follower
Node count: 305
```

If you see logs indicating ClickHouse event Table is read only, then you know that the ClickHouse Keeper needs to be restored:

```
grep PH_DATAMANAGER_HTTP_UPLOAD_ERROR /opt/phoenix/log/phoenix.log| grep TABLE_IS_READ_ONLY

2022-07-22T13:00:10.945816-07:00 FSM-Host phDataManager[9617]: [PH_DATAMANAGER_HTTP_UPLOAD_
ERROR]:[eventSeverity]=PHL_ERROR,[procName]=phDataManager,
[fileName]=ClickHouseWriterService.cpp,[lineNumber]=459,[errReason]=Uploading events to
ClickHouse failed. respCode:500 resp:Code: 242. DB::Exception: Table is in readonly mode
(replica path: /clickhouse/tables/1/fsiem.events/replicas/1). (TABLE_IS_READ_ONLY) (version
22.6.1.1985 (official build))
```

To recover, take the following steps:

1. Login to Supervisor's redis:
   ```
   redis-cli -p 6666 -a $(grep pass /opt/phoenix/redis/conf/6666.conf | awk '{print
   $2}')
   127.0.0.1:6666> del cache:ClickHouse:clickhouseKeeperNodes
   (integer) 1
   ```
2. Navigate to **ADMIN > Settings > Database > ClickHouse Config**, and replace the dead worker with a new worker to ClickHouse Keeper cluster.
3. Click **Test**.
4. Click **Deploy**.
5. Login in to clickhouse-client on each ClickHouse node and execute the following commands.
   ```
   SYSTEM RESTART REPLICA fsiem.events_replicated
   SYSTEM RESTORE REPLICA fsiem.events_replicated
   ```

Recovering from Losing Quorum in ClickHouse Keeper Cluster

Quorum is lost when more than half of the nodes in the Keeper cluster goes down.

To identify if a ClickHouse Keeper needs recovery, you can check via log or command line.

From Log:

```
/data-clickhouse-hot-1/clickhouse-keeper/app_logs/clickhouse-keeper.err.log

2022.07.22 12:27:10.415055 [ 52865 ] {} <Warning> RaftInstance: Election timeout, initiate
leader election
2022.07.22 12:27:10.415169 [ 52865 ] {} <Warning> RaftInstance: total 1 nodes (including
this node) responded for pre-vote (term 0, live 0, dead 1), at least 2 nodes should
respond. failure count 163
```

From Command Line:

```
[root@FSM-660-CH-58-246 ~]# echo stat | nc 172.30.58.216 2181
This instance is not currently serving requests
```

To recover, take the following steps:

Login to the ClickHouse Keeper node that needs recovery and run the following command.

`echo rcvr | nc localhost 2181`

Recovering from Read-Only Mode

A ClickHouse Data Node Table can become read-only due to various reasons including loss of connection to Keeper node, or disk capacity exceeding high threshold.

Step 1. Read-Only Check

Login to the Data Node and run the following command to identify which tables are read-only mode:

`# clickhouse-client -q "select database,table,is_readonly from system.replicas"`

`"database","table","is_readonly"`

`"fsiem","events_replicated",1`

`"fsiem","mv_t_events",1`

`"fsiem","summary",0`

In this case, `fsiem.events_replicated` and `fsiem. mv_t_events` tables are read-only.

Step 2. Simple Recovery

To recover, run the following commands from the Data Node for every read-only table:

`SYSTEM DROP REPLICA '<database.table>'`

`SYSTEM RESTART REPLICA <database.table>`

`SYSTEM RESTORE REPLICA <database.table>`

Then do the read-only check again as in Step 1. If there are no more read-only tables, you are done. Else proceed with Step 3 below.

Step 3. Advanced Recovery

Gather node's **shard id** and **replica id** from `/etc/clickhouse-server/config.d/macros.xml`.

```
<yandex>
  <macros>
     <shard>1</shard>
     <replica>1</replica>
  </macros>
</yandex>
```

Then **login to one keeper node** and run the following command for each read-only table:

`/opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/<table>/replicas/<ReplicaID>`

e.g. assuming shard id 1, replica id 1, and tables `fsiem.events_replicated`, `fsiem.mv_t_events`:

`/opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/1/fsiem.events_replicated/replicas/1`

`/opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/1/fsiem.mv_t_events/replicas/1`

Finally, login to the Data Node and run the following `RESTART` and `RESTORE` commands for every table with read-only status:

`SYSTEM RESTART REPLICA <database.table>`

`SYSTEM RESTORE REPLICA <database.table>`

For example:

`SYSTEM RESTART REPLICA fsiem.events_replicated`

`SYSTEM RESTORE REPLICA fsiem.events_replicated`

Mitigating a Non-Responsive ClickHouse Keeper Node

To resolve a non-responsive ClickHouse Keeper node, take the following steps.

1. Check the status of Keeper cluster by running the following command on EACH Keeper node.
   `echo stat | nc localhost 2181`
2. Restart any non-responsive Keeper by running the following command.
   `systemctl restart ClickHouseKeeper`
3. If the command from step 2 does not resolve the problem, take the following steps:
   a. On the non-responsive ClickHouse Keeper node, make sure that there is ONLY a single line of `ARG1=--force-recovery` in `/data-clickhouse-hot-1/clickhouse-keeper/.systemd_argconf`. Normally, the file contains `ARG1=`.
   Modify the file so that there is only a single line of `ARG1=--force-recovery` that appears in `/data-clickhouse-hot-1/clickhouse-keeper/.systemd_argconf`.
   b. Restart the Keeper by running the following command.
   `systemctl restart ClickHouseKeeper`
   c. Next, run the following command to check the recovery status.
   `echo stat | nc localhost 2181`

Migrating ClickHouse Events from FortiSIEM 6.5.x to 6.6.0 or Later

FortiSIEM 6.5.x ran ClickHouse on a single node and used the Merge Tree engine. FortiSIEM 6.6.0 onwards runs ClickHouse on a cluster using Replicated Merge Tree engine. You need to follow these special steps to move the old events previously stored in Merge Tree to Replicated Merge Tree.

From FortiSIEM 6.5.x, you MUST first upgrade to FortiSIEM 6.6.x PRIOR to upgrading to FortiSIEM 7.x or later. If you directly upgrade from 6.5.x to 7.0.0 or later, upgrade will fail.

To upgrade your FortiSIEM 6.5.x to 6.6.x, take the following steps

1. Navigate to **ADMIN >Settings > Database > ClickHouse Config**.
2. Click **Test**, then click **Deploy** to enable the ClickHouse Keeper service which is new in 6.6.x.
3. Migrate the event data in 6.5.x to 6.6.x by running the script `/opt/phoenix/phscripts/clickhouse/clickhouse-migrate-650.sh`.
4. Verify that all events have been moved to the new table through GUI Search.
5. When the data migration is deemed successful, run the following command on every node where the `clickhouse-migrate-650.sh` script was run successfully to drop the old event table.

   ```
   clickhouse-client -q "DROP TABLE fsiem.events_non_replicated"
   ```

Now you can upgrade to FortiSIEM 7.x or later, if needed.

Post-7.1.1 Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1, then after upgrade has completed, you need to run the following command to rebuild ClickHouse indices. If you are running a version later than 7.1.1, and have already executed the rebuilding steps, then nothing more needs to be done.

```
/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -h
```

Usage: `./script [-h for help] [-p for 10 oldest partitions] [-m manual commands] [-r <index id> index to be rebuilt]`

Here are indexes available for rebuild. Please choose one and specify the `id` in `-r` option.

`-r <index id>` option is mandatory.

1. reptDevIpAddr
2. srcIpAddr
3. destIpAddr
4. hostIpAddr

For example, to rebuild reptDevIpAddr index, issue the following command.

```
$ ./rebuild_ip_bloom_filter.sh -r 1
```

Notes before running the script:

1. The script should be run on only one node per shard. Only one instance of the script can be run at one time on a host. This is checked and enforced by the script.
2. The rebuilding of bloom filter index is a table-wide operation and it could take some time to complete, based on the amount of data and resources available.
3. Since the script could be long-running, please use screen or tmux sessions to launch the script.
4. During the rebuilding of bloom filter index, there will be a temporary spike in storage usage as ClickHouse goes through the existing data and rebuilds indexes for the whole table. The rebuilding of bloom filter index is a non-intrusive operation. After the DROP, ADD, MATERIALIZE requests are submitted to ClickHouse, ClickHouse will schedule the various tasks in an optimized way. The user has no control over the process.
5. All nodes in the target shard should have at least 10% free space on `/data-clickhouse-hot-1`. The script will also check the 10% space requirement on all nodes of the shard and suggests partitions that should be moved to a different tier to create space. If there are no more tiers to move the partitions to, please consult with Fortinet support to identify a reasonable solution.
6. The script will show the remaining parts to be processed for both DROP and MATERIALIZE phase. If the "parts to be processed" is stuck at a specific count for more than 24 hours, please contact Fortinet support to check if there are any underlying conditions that would have prevented the DROP or MATERIALIZE command to proceed further.

Detailed Steps are as follows:

1. Go to root shell by running the following command:
   `sudo -s`
2. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 1`
   The script will produce output similar to the following:

```
[root@server]# /opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 1
current attr is reptDevIpAddr
Materialize in progress "false" for reptDevIpAddr with 0 parts to process
Materialize in progress "false" for srcIpAddr with 0 parts to process
Materialize in progress "false" for destIpAddr with 0 parts to process
Materialize in progress "false" for hostIpAddr with 0 parts to process
drop in progress "false" for reptDevIpAddr
drop in progress "false" for srcIpAddr
drop in progress "false" for destIpAddr
drop in progress "false" for hostIpAddr
Processing index index_reptDevIpAddr_bloom_filter
Trying to rebuild index_reptDevIpAddr_bloom_filter
drop in progress "false"
There is enough storage on host 172.30.56.206.
done checking storage for index index_reptDevIpAddr_bloom_filter
dropping index index_reptDevIpAddr_bloom_filter
dropping index command issued
Start monitoring index index_reptDevIpAddr_bloom_filter for drop operation
drop index_reptDevIpAddr_bloom_filter done. Total time taken: 0 seconds
Total time to drop index_reptDevIpAddr_bloom_filter is 1 seconds
adding index_reptDevIpAddr_bloom_filter
Start monitoring index index_reptDevIpAddr_bloom_filter for materialize operation
parts left to materialize reptDevIpAddr index : 6 - time taken 0 seconds
materialize index_reptDevIpAddr_bloom_filter done. Total time taken: 10 seconds
Rebuilding index for reptDevIpAddr done. Total time taken for rebuild 13 seconds
```

3. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 2`
4. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 3`
5. Run the following command:
   `/opt/phoenix/phscripts/clickhouse/rebuild_ip_bloom_filter.sh -r 4`

Reference

The following ClickHouse References are available.

General Introduction

https://clickhouse.com/docs/en/intro

Concepts and Architecture

https://clickhouse.com/docs/en/development/architecture

ClickHouse Keeper

https://clickhouse.com/docs/en/operations/clickhouse-keeper

Performance Tuning

https://clickhouse.com/docs/en/operations/tips

Troubleshooting

https://kb.altinity.com/altinity-kb-schema-design/how-much-is-too-much/

https://clickhouse.com/docs/en/operations/system-tables/

https://clickhouse.com/docs/en/sql-reference/statements/system/#query_language-system-restore-replica

Configuration Notes

- Automated CMDB Disk Space Management
- Component Communication and Network Port Usage
- Configuring FortiSIEM Application Server for Proxy Connectivity
- Editing phoenix_config.txt File
- FortiSIEM Deployment Scenarios
- FortiSIEM OS Updates and Internet Connectivity
- Tuning PostgreSQL Configuration Parameters

Automated CMDB Disk Space Management

If the CMDB disk partition becomes full, then the system may not work correctly. To prevent this from happening, 6.3.2 introduced a CMDB disk space management framework.

Three parameters are introduced in `phoenix_config.txt`.

- `month_retain_limit`: Number of months for which incidents on the Supervisor node should be retained (default value 6 months).
- `cmdb_disk_space_low_threshold` (in MB): When free CMDB disk space falls below this defined threshold, disk management kicks in (default value 50MB).
- `cmdb_disk_space_high_threshold` (in MB): When disk management kicks in, incidents are purged until CMDB disk space reaches this defined threshold (default value 100MB).

Two audit events are introduced.

- `PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and old incidents and identity / location data were pruned to bring the free CMDB disk space above the high threshold (`cmdb_disk_space_high_threshold`).
- `PH_AUDIT_CMDB_DISK_PRUNE_FAILED`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and in spite of pruning older incidents and identity / location data, free CMDB disk space stays below the high threshold (`cmdb_disk_space_high_threshold`). To remedy this situation, the user must reduce the number of months of incidents and identity / location data in CMDB (`month_retain_limit`).

Two system defined rules are included.

- FortiSIEM: CMDB Disk space low - Prune successful.
- FortiSIEM: CMDB Disk space low - Prune failed to keep free disk space above high threshold.

Component Communication and Network Port Usage

Information on external communication ports needed for various FortiSIEM nodes to work can be found in the External Systems Configuration Guide, here.

Configuring FortiSIEM Application Server for Proxy Connectivity

Follow these steps to configure the FortiSIEM application server to support proxy connectivity for Integrations (for example, Incidents, CMDB, Indicators of Compromise).

1. Edit the Glassfish configuration file using your favorite text editor: `/opt/glassfish/domains/domain1/config/domain.xml`.
2. Replace the `172.30.57.100` host value in the sample configuration to the Proxy Server IP, port and/or username and password in the environment.
3. If no user name and password is required, then remove the `Dhttp.proxyUser` and `Dhttp.proxyPassword` lines from the configuration file..
4. If a proxy exclusion for certain destination hosts is required, then add the `http.nonProxyHosts` configuration option to exclude the proxy server. If this is not required, then delete the line.
5. If the proxy server allows only HTTPS, then add 's' to `http`. For example, change `http.proxyHost` to `https.proxyHost`.

The following is a sample configuration:

<jvm-options>-Dhttp.proxyHost=172.30.57.100</jvm-options>

<jvm-options>-Dhttp.proxyPort=3128</jvm-options>

<jvm-options>-Dhttp.proxyUser=foobar</jvm-options>

<jvm-options>-Dhttp.proxyPassword=password</jvm-options>

<jvm-options>-Dhttp.nonProxyHosts=172.30.59.130|localhost|update.fortiguard.com</jvm-options>

Editing phoenix_config.txt File

The file `/opt/config/phoenix_config.txt` contains FortiSIEM run-time parameters. The parameters belong to 2 classes:

- Group 1: Preserved between upgrades - these parameters can be changed by the user and the changes will be preserved. For example:
  # FSM upgrade preserves customer changes to parameter value
  num_event_parser=16 #timeWithinSec requires at least 2 parser when former event will depend on later event
- Group 2: Overwritten during upgrade - these parameters are considered internal to and owned by FortiSIEM and will be overwritten during upgrade. For example:
  # FSM internal parameter; FSM overwrites
  raw_sharedstore_size=268435456 #15M = 15728640, 64M = 67108864, 256M = 268435456, 512M = 536870912

Please follow these methods if you are intentionally making changes to these parameters.

1. For parameters *affecting Supervisor and Worker nodes*, you can safely change Group 1 parameters and they will be preserved across upgrades. For Group 2 parameters, the changes will be effective, but will be overwritten during upgrade. Please contact Fortinet Support if you really need to preserve Group 2 parameter changes.
2. For parameters *affecting Collectors*, instead of changing the `/opt/config/phoenix_config.txt` file, you need to change `/opt/phoenix/config/collector_config_template.txt` on the Supervisor. This ensures that new Collectors registering will get the new parameters and the changes are preserved across upgrades. If you want to change the parameters for an existing Collector, then you need to make the same change in 2 places:
   - Change the `/opt/config/phoenix_config.txt` file on the Collector and restart the Collector.
   - Make the same change on `/opt/phoenix/config/collector_config_template.txt` on the Supervisor. This ensures that new Collectors registering will get the new parameters and the changes are preserved across upgrades.

   Other than that, the same rules for Group 1 and Group 2 apply. You can safely change Group 1 parameters and they will be preserved across upgrades. For Group 2 parameters, the changes will be effective, but will be overwritten during upgrade.

FortiSIEM Deployment Scenarios

FortiSIEM can be deployed in Enterprise and Service Provider environments in a highly scale-out fashion.

- Enterprise Deployment
- Service Provider Deployment

Enterprise Deployment

Enterprise Deployments with Supervisor and no Collector

Enterprise deployment without Collector (Supervisor only) is the simplest setup where:

- Logs are sent to the Supervisor.
- Test Connectivity, Discovery performance monitoring, and Event pulling, (for example: Cloud Services, WMI based Windows log Collection, etc.) are all done from the Supervisor – Go to **ADMIN** > **Setup** > **Credentials** and **ADMIN** > **Setup** > **Discovery**.

This setup has the following drawbacks:

- Does not scale up when a large number of devices must be monitored or high EPS needs to be handled. This can be solved by deploying Workers – see here.
- Logs cannot be collected efficiently from devices across the Internet. Devices cannot be monitored across the Internet. This is because of latency and security issues over Wide Area Networks. This can be solved by deploying Collectors – see here.
- FortiSIEM Agents cannot be used as they need Collectors – see here.

Enterprise Deployment with Supervisor and Worker but no Collector

The scalability issue above can be resolved by deploying Worker nodes. To add a Worker node:

1. Install a Worker node.
2. Add the Worker to the Supervisor from **ADMIN** > **License** > **Nodes** > **Add**.

In this case:

- Logs can be sent to the Supervisor or Workers. Sending to Workers is recommended since you can load balance across multiple Workers.

- Test Connectivity and Discovery is always done from Super.
- However, Performance monitoring and Event pulling jobs (for example: Cloud Services, WMI based Windows log Collection and so on) are done by the Worker nodes in addition to the Supervisor nodes. After Test connectivity and Discovery, Supervisor node distributes the jobs to the Workers. When a new Worker is added to the FortiSIEM Cluster, jobs are re-distributed to the Workers.

Although it provides scalable event handling, this system has the following shortcomings:

- Logs cannot be collected efficiently from devices across the Internet. Devices cannot be monitored across the Internet. This is because of latency and security issues over Wide Area networks. This can be solved by deploying Collectors – see here.
- FortiSIEM Agents cannot be used, because they need Collectors – see here.

Enterprise Deployments with Supervisor, Worker and Collector

This solution provides the flexibility of log collection and performance across the Internet and behind firewalls. It also provides even more scalability because the Collectors, instead of the Workers, parse events.

To add a Collector node:

1. Go to **ADMIN** > **Setup** > **Collector** and create a Collector in the Supervisor.
2. If you have Workers, define the Workers that the Collectors will upload to (Go to **ADMIN > Settings > System > Worker Upload**).
3. If you are not using Workers you should define the Supervisor IP or DNS name of the Supervisor (Go to **ADMIN > Settings > System > Worker Upload**).
4. Install a Collector.
5. Register the Collector to the Supervisor using any FortiSIEM user credential with Admin privileges (see **CMDB** > **User**). The built-in admin credential will work. During registration, the Collector will get the Workers to upload events to.

In this case:

- Logs can be sent to Collectors (preferred). However, they can be sent to Workers or Super as well. Collectors will upload parsed logs to the Workers in a load-balanced fashion.
- For Test Connectivity and Discovery, choose the Collector for the job. Collectors will collect events and send them to Workers in a load-balanced fashion.

In this configuration, you can add FortiSIEM Windows and Linux Agents:

1. Go to **CMDB** > **User** > **Add** and create an Agent User for Agents to register to the Supervisor node.
2. Install the Agents and register them to the Supervisor using the Agent user credential created in the previous step.
3. Define the Agent Monitoring templates.
4. Assign templates to the Agents and choose Collectors from the set created earlier.

Agents will send logs to the Collectors in a load-balanced manner. Collectors can then send to Workers in a load-balanced manner. This enables log collection in a geographically distributed and scalable manner.

Service Provider Deployment

In a Service Provider deployment, there can be one or more Organizations. Devices and logs are kept logically separated for two Organizations.

Note: **It is very important to assign devices and logs to the correct Organization in FortiSIEM.**

A FortiSIEM Service Provider deployment consists of:

- Supervisor node
- Worker nodes for scalability
- Collector nodes for remote data collection
- Windows/Linux Agents for richer data collection without remote admin credentials

While Supervisor, Workers, and Agents are shared infrastructure across Organizations, Collectors may be present and may be dedicated or shared.

This section provides details on how various infrastructure components are deployed, with an eye towards assigning devices and logs to the right Organization.

- Organizations with Dedicated Collector
- Organizations with Shared Collector

Service Provider Deployment - Organizations with Dedicated Collector

In this case, Organization has one of more Collectors that belong to that Organization only. This is suited for large Organizations.

Setup

1. Create Organizations as follows:
   a. Log in to Super-Global Organization.
   b. Go to **ADMIN** > **Setup** > **Organizations** and create an Organization.
   c. Define Admin credentials (for Collector registration) and Agent credentials (for FortiSIEM Agent registration).
   d. Add Collectors to that Organization.
2. Install the Collectors and register them to Supervisor. Use any Organization Admin credentials defined in **ADMIN** > **Setup** > **Organizations**, to register the Collector.

Operations

Collecting Logs via Agents

1. Install Agents and register them to the Supervisor. Use the Agent credentials for the Organization that the Agents belong to.
2. Define the Agent Monitoring templates. Assign the templates to agents and designate Collectors belonging to the specific Organization.

Agents will send logs to Collectors in a load-balanced fashion. Since Agents are configured with the Organization ID, they include the Organization in every log. This information is used by Collectors to assign devices and logs to the correct Organization.

Collecting Logs without Agents

Configure devices to send logs to the Organization's Collectors. Since these collectors belong to one organization, it assigns received devices and logs to that Organization.

Discovery and Performance Monitoring by IP Address Range

Log in to the specific Organization and:

1. Define the credential.
2. Do Test Connectivity and Discovery using a specific Collector.

Event Pulling for Cloud Services

Log in to the specific Organization and:

1. Define the credential.
2. Do Test Connectivity and Discovery using a specific Collector.

Service Provider Deployment - Organizations with Shared Multi-tenant Collector

It may not be economically viable for smaller Organizations to deploy their own collectors. But Collectors may be needed to deploy Agents and to scale out data collection across many smaller Organizations managed under the same FortiSIEM.

Setup

In this setup, special multi-tenant Collectors must be defined under the Super/Local Organization as follows:

1. Log in to the Super-Local Organization. This is a built-in organization meant for the Service Provider's use only .

2. Go to **ADMIN** > **Setup** > **Collector** and add Collectors to that Organization. These are called multi-tenant Collectors as they handle devices and logs from multiple Organizations.
3. Install the Collectors and register them to the Supervisor. Use any Full Admin user in **CMDB** > **User** to register the Collector.
4. For each Collector that will be multi-tenant, do the following:
   SSH into the Collector and modify the following line under `/opt/phoenix/config/phoenix_config.txt`:
   `Multi_Tenant_Collectors=false`

   Change:
   `Multi_Tenant_Collectors=false`

   To:
   `Multi_Tenant_Collectors=true`
5. Reboot the Collector.

Then create Organizations as follows:

1. Log in to Super-Global Organization.
2. Go to **ADMIN** > **Setup** > **Organizations** and create an Organization.
3. Add Agent credentials for Agent registration.
4. Define the Include/Exclude IP Address ranges if devices belonging to various Organizations are going to send logs to multi-tenant Collectors.

Operations

Collecting Logs via Agents

1. Install Agents and register them to the Supervisor. Use the Agent credentials for the Organization that the Agents belong to.
2. Define Agent Monitoring templates. Assign templates to Agents and designate multi-tenant collectors belonging to the Super-local Organization.

FortiSIEM Agents will send logs to multi-tenant Collectors in a load-balanced fashion. Since Agents are configured with the Organization ID, they include the Organization in every log. This information is used by multi-tenant Collectors to assign devices and logs to the correct Organization.

Collecting Logs without Agents

Configure devices to send logs to the multi-tenant Collectors. Make sure the reporting device IP matches the Include/Exclude IP ranges defined for that Organization in **ADMIN** > **Setup** > **Organization**. A multi-tenant Collector uses the reporting device IP to assign devices and logs to the correct Organization.

Discovery and Performance Monitoring by IP Address Range

This is possible so long as the IP Address range matches the Include/Exclude IP ranges defined for that Organization in **ADMIN** > **Setup** > **Organizations**.

This can be done in two ways:

1. (Recommended) From Super/Global Organization:
   a. Define the credential.
   b. Do Test Connectivity and Discovery. We will automatically choose a multi-tenant collector
2. Alternatively, log in to the Super/Local Organization and:
   a. Define the credential.
   b. Do Test Connectivity and Discovery using a specific multi-tenant Collector.

Approach #1 is recommended because the Collector is automatically chosen.

Event Pulling for Cloud Services

From Super/Global Organization:

1. Define the credential. Specify the Organization in the credential.
2. Perform Test Connectivity and Discovery.
   FortiSIEM will automatically choose a multi-tenant Collector.

Collecting Logs from Multi-tenant Devices

A shared Collector also enables you to collect logs from multi-tenant devices such as FortiGate with Virtual Domains (VDOM). This assumes that the logs contain an attribute (such as FortiGate VDOM) that enables FortiSIEM to classify logs from multi-tenant devices to different Organizations.

From a Super/Global Organization:

1. Go to **ADMIN** > **Settings** > **Event Handling** > **Event Org Mapping**.
2. Click **New** and enter the Organization mappings for the discriminating log attribute (such as VDOM).
3. Click **Save**.

FortiSIEM OS Updates and Internet Connectivity

The following table details hosts that FortiSIEM will connect to for package verification, content updates, lookups and OS updates.

Required By	Used For	Host
Super	IOC feed and IOC lookups, validation of Collector & Agent packages, Content Updates	update.fortiguard.net / TCP / 443
Super, Worker, Collectors	OS updates*	os-pkgs-cdn.fortisiem.fortinet.com / TCP / 443 os-pkgs-r8.fortisiem.fortinet.com / TCP / 443

*Please check the FortiSIEM - OS Update Lifecycle guide for additional information.

Tuning PostgreSQL Configuration Parameters

FortiSIEM uses PostgreSQL database for many purposes. Some examples are:

- Store FortiSIEM configuration information
- Store CMDB information – devices, users, etc.
- Store Incidents and Cases and keeping them up to date
- Store External Threat Intelligence data
- Serve GUI users – provide information to display and store user changes
- Serve FortiSIEM Agents, Collectors and Workers with information needed to function
- Support Agent and Collector upgrades
- Integrate with help desk systems like ServiceNow
- Support public REST API

PostgreSQL performance is critical to FortiSIEM operations. This document describes how to tune important PostgreSQL configuration parameters for optimal performance. Note that the following are guidelines only and adjustments can be made based on the specific hardware, workload, and usage patterns to ensure the system runs efficiently while avoiding potential bottlenecks.

The following external reference may be helpful: Comprehensive Guide on How to Tune Database Parameters and Configuration in PostgreSQL

PostgreSQL configuration parameters are stored in `/cmdb/data/postgresql.conf` on the Supervisor or DB Server Node.

Important Configuration Parameters

1. **effective_cache_size**:
   - **Definition**: Specifies the available memory for PostgreSQL to assume for data caching.
   - **Recommended value**: 50%-75% of system memory, with a conservative approach of 50%.
   - **FortiSIEM settings**: FortiSIEM default is 4GB for All-In-One Supervisor Node. For FortiSIEM DB Node with 24GB memory, it can be increased to 12GB.
2. **maintenance_work_mem**:
   - **Definition**: Memory allocated for maintenance tasks such as `VACUUM`, `CREATE INDEX`, etc.
   - **FortiSIEM settings**: Default value: 64MB, can be adjusted as needed during maintenance tasks. Example of setting: `SET maintenance_work_mem TO '128MB';`
3. **max_connections**:
   - **Definition**: Specifies the maximum number of client connections.
   - **Recommended value**: Align with project needs, with a default value of 100.

- **FortiSIEM settings**: FortiSIEM's default for All-In-One Supervisor Node is 300, and for FortiSIEM DB Node, it's set to 500. Ensure that `max_connections` > `max-pool-size` defined in Glassfish (`max-pool-size=160` for DB connection pool) to leave room for other processes to access PostgreSQL.

4. **max_wal_size**:
   - **Definition**: Determines the threshold at which a checkpoint will be triggered.
   - **Recommended value**: Between 1GB and 2GB.
   - **FortiSIEM settings**: 2GB
5. **shared_buffers**:
   - **Definition**: Determines memory allocated to PostgreSQL for data caching.
   - **Recommended value**: 25% of total memory, up to a maximum of 8GB for FortiSIEM DB Node.
   - **FortiSIEM settings**: For FortiSIEM All-In-One Supervisor Node, adjust based on available memory. For example, allocate 2GB for PostgreSQL, and set `shared_buffers` to 512MB (1/4 of the 2GB).
6. **temp_buffers**:
   - **Definition**: Specifies the amount of memory for temporary buffers within each database session. Default value: 8MB.
   - **FortiSIEM settings**: For FortiSIEM DB Node, it is increased to 64MB for systems with 16GB allocated to PostgreSQL (on a total of 24GB system memory).
7. **work_mem**:
   - **Definition**: Determines memory usage for internal operations like sorting and hash tables.
   - **Recommended value**: Between 10MB and 50MB, depending on the number of connections.
   - **FortiSIEM settings**: FortiSIEM default is 16MB for All-In-One Supervisor Node and 32MB for FortiSIEM DB Node, but can be increased for faster sorting (be cautious of excessive values leading to memory bottlenecks).

Additional Configuration Parameters

8. **autovacuum_analyze_scale_factor**:
   - **Definition**: Controls the threshold for automatic analysis of tables. Reducing this value can help improve query performance by more frequently analyzing tables for better statistics.
   - **Recommended value**: Default is 0.1 (10% of the table's rows).
   - **FortiSIEM settings**: 0.1
9. **autovacuum_vacuum_scale_factor**:
   - **Definition**: Controls when automatic vacuuming occurs for tables. Lowering this value can help prevent table bloat by vacuuming tables more frequently.
   - **Recommended value**: Default is 0.2 (20% of the table's rows).
   - **FortiSIEM settings**: 0.2
10. **checkpoint_completion_target**:
    - **Definition**: Controls how much of the checkpoint interval is used to complete a checkpoint. Setting it closer to 1.0 helps in spreading I/O load, minimizing performance spikes during checkpoints.

- **Recommended value**: 0.9 (90% of the checkpoint time).
- **FortiSIEM settings**: 0.9

11. **checkpoint_timeout**:
    - **Definition**: Determines the maximum time between automatic write-ahead logging (WAL) checkpoints. A longer interval between checkpoints can improve performance but may risk more data loss in case of a crash.
    - **Recommended value**: Between 5 and 10 minutes.
    - **FortiSIEM settings**: 5 minutes
12. **effective_io_concurrency**:
    - **Definition**: Controls the number of simultaneous disk I/O operations PostgreSQL can perform. Higher values can benefit systems with multiple disks and parallel I/O operations, improving read/write performance.
    - **Recommended value**: Set to the number of available disk spindles (usually 2-4 for HDDs, or higher for SSDs).
    - **FortiSIEM settings**: 1
13. **log_min_duration_statement**:
    - **Definition**: Logs the duration of any query that takes longer than the specified value. Helps in identifying slow queries that may need optimization
    - **Recommended value**: 500ms or higher.
    - **FortiSIEM settings**: 500ms
14. **log_temp_files**:
    - **Definition**: Logs the use of temporary files during queries. Useful for debugging performance issues related to queries spilling to disk.
    - **Recommended value**: `-1` disables, `0` logs all temp files.
    - **FortiSIEM settings**: -1
15. **random_page_cost**:
    - **Definition**: Defines the cost estimate for non-sequentially accessed pages. For SSD-based storage, this value should be reduced to reflect the faster random access performance of SSDs.
    - **Recommended value**: Lower the value if using SSDs (e.g., 1.0) or leave at default (4.0) for HDDs.
    - **FortiSIEM settings**: 4.0
16. **seq_page_cost**:
    - **Definition**: Defines the cost estimate for sequentially accessed pages. Reducing this value can help PostgreSQL's query planner favor sequential scans more often.
    - **Recommended value**: Default is 1.0, which works well for most systems.
    - **FortiSIEM settings**: 1.0

Elasticsearch Usage Notes

Note: AWS Elasticsearch Service is now officially known as AWS OpenSearch Service (See here). References to "AWS Elasticsearch Service" in this documentation can be considered the same as "AWS OpenSearch Service".

- Configuring Elasticsearch Buffer
- Configuring Elasticsearch Timeout
- Dynamic Scripting Limits
- Elasticsearch Feature Compatibility
- Merging Small Elasticsearch Indices into a Big Index
- Differences in Analytics Semantics between EventDB and Elasticsearch
- Elasticsearch Known Issues

Configuring Elasticsearch Buffer

When there is a huge number of events, the Elasticsearch server may become overloaded with processing them and cannot accept all uploads during this time.

A solution to this issue is to save events to a local disk when events cannot be uploaded. FortiSIEM allows you to configure a disk based buffer to save these events until Elasticsearch is available again.

Fortinet recommends that a dedicated disk be used for this purpose. At a minimum, ensure it does not use shared NFS, which could cause latency. It is also strongly recommended that if you wish to use this feature on Workers, that all Workers be configured. If a Worker is not configured, it will be blocked, and consequently, will not accept Collector event uploads. In this situation, the Collector will fail to upload to the unconfigured Worker, and will attempt to connect to another Worker that accepts uploads.

To configure, access the `phoenix_config` file. If the buffer path is defined, the feature is enabled.

```
[BEGIN Elasticsearch]

log_buffer_per_customer_path=/eventbuffer #empty means disabled.

log_buffer_per_customer_reserved_disk_space=1 # GB

[END]
```

Next, in the `phoenix_config` file, in the Elastisearch section, modify `index_max_retry` to configure the number of times FortiSIEM will attempt to retry uploads. If the retry time is set to 0, FortiSIEM will never drop events and after the connection between FortiSIEM and Elasticsearch has recovered, all events will be uploaded.

After defining the event buffer path, restart `phDataManager`.

This feature can be enabled on the Supervisor and Workers.

Configuring Elasticsearch Timeout

To configure, go to the Elasticsearch section of `/opt/phoenix/config/phoenix_config.txt` and add the following line:

`restapi_timeout_in_seconds=<# of seconds>`

Example:

`restapi_timeout_in_seconds=300`

and restart phDataPurger.

Dynamic Scripting Limits

In FortiSIEM, Elasticsearch queries are run using dynamic scripts because of multi-field aggregation of query results. In Elasticsearch, there are two related limits.

1. Rate at which scripted queries can be compiled (cluster level limit)
2. Cache for the compiled scripts (node level limit)

If the compile limit is reached, then Elasticsearch will throw a circuit_breaking_exception error and the query will not run. If the cache limit is reached, then the query will need to be recompiled and may run a little slowly for the first time.

```
[PH_JAVA_QUERYSERVER_ERROR]:[eventSeverity]=PHL_ERROR,[phEventCategory]=3,
[methodName]=innerFromXContent,[className]=org.elasticsearch.ElasticsearchException,
[procName]=javaQueryServer,[lineNumber]=509,[errReason]=Elasticsearch exception
[type=circuit_breaking_exception, reason=[script] Too many dynamic script compilations
within, max: [75/5m]; please use indexed, or scripts with parameters instead; this limit
can be changed by the [script.context.aggs.max_compilations_rate] setting],
[phLogDetail]=Elasticsearch exception [type=search_phase_execution_exception, reason=all
shards failed]
```

Current limits in your environment can be obtained by running the following API.

```
GET /_nodes/stats?filter_path=nodes.*.script_cache.contexts
{
  "nodes": {
    "kISLOIv_QvGbFNnpDtLdyw": {
      "script_cache": {
        "contexts": [
          {
            "context": "aggregation_selector",
            "compilations": 0,
            "cache_evictions": 0,
            "compilation_limit_triggered": 0
          },
          {
            "context": "aggs",
            "compilations": 1795,
            "cache_evictions": 1695,
            "compilation_limit_triggered": 249
          },
    ...
}
```

You can change the compilation rates by running the query using the following API.

```
PUT _cluster/settings (For ES 7.9 and above)
{
    "persistent": {
        "script.context.aggs.max_compilations_rate": "150/5m"
```

```
    }
}

PUT _cluster/settings (For ES below 7.9)
{
    "persistent": {
        "script.max_compilations_rate": "150/5m"
    }
}
```

You can set `script.context.$CONTEXT.cache_max_size` in the `elasticsearch.yml` configuration file. For example, to set the max size for the aggs context, you would add the following to `elasticsearch.yml`.

`script.context.aggs.cache_max_size: 300`

This is a node level setting, which when changed, needs node restart.

References

1. https://www.elastic.co/guide/en/elasticsearch/reference/7.9/modules-scripting-using.html#prefer-params
2. https://alexmarquardt.com/2020/10/21/elasticsearch-too-many-script-compilations/

Elasticsearch Feature Compatibility

There are 3 distinct Elasticsearch deployments. This table shows the versions and features supported for each deployment type. Please also see the list of Elasticsearch related known issues in Elasticsearch Known Issues in Appendix - Elasticsearch Usage Notes.

Elasticsearch Deployment	API (Insertion and Search)	Supported Data Node Types	Disk Space based Retention	Age based retention (ILM)
Self-Managed (On-Prem or Hosted)	REST	Hot, Warm, Cold	Yes	Yes (6.8 and above)
AWS OpenSearch Service (Previously known as AWS Elasticsearch Service)	REST	N/A	Yes	No
Elastic Cloud	REST	N/A	Yes	No

Merging Small Elasticsearch Indices into a Big Index

In Elasticsearch, you may see older indices with few documents. You may want to merge these smaller indices into a bigger index and create an alias for them, by following these steps.

Elasticsearch reference: https://www.elastic.co/guide/en/elasticsearch/reference/7.13/docs-reindex.html

Notes:

1. Don't merge indices that belong to different organizations together.
2. The naming format for event index is: `fortisiem-event-<Year>.<Month>.<Date>-<OrgId>-<SeqNo>`
3. When merging indices from different days together, make sure to create aliases for the different days to point to the merged index

Steps

1. Create one new index.

```
curl -XPUT '172.30.56.182:9200/fortisiem-event-2021.07.30-3-000001-merged?pretty' -H
'Content-Type: application/json' -d'
{
    "settings" : {
        "index" : {
           "number_of_shards" : 1
        }
    }
}
'
```

2. Merge the smaller indices into the new index created in Step 1.

```
curl -XPOST '172.30.56.182:9200/_reindex?pretty' -H 'Content-Type: application/json' -
d'
{
    "conflicts": "proceed",
    "source": {
        "index": "fortisiem-event-2021.07.30-3-000001,fortisiem-event-2021.07.29-3-
000001"
    },
    "dest": {
```

```
        "index": "fortisiem-event-2021.07.30-3-000001-merged",
        "op_type": "create"
    }
}
'
```

3. Create aliases for all (newly created) merged indices.

```
curl -X POST 'http://172.30.56.182:9200/_aliases' -H 'Content-Type: application/json' -
d'
{
   "actions":[
      {
         "add":{
            "index":"fortisiem-event-2021.07.30-3-000001-merged",
            "alias":"fortisiem-event-2021.07.30-3"
         }
      }
   ]
}
'
```

4. Delete all old indices.

```
curl -XDELETE http://172.30.56.182:9200/fortisiem-event-2021.07.30-3-000001
curl -XDELETE http://172.30.56.182:9200/fortisiem-event-2021.07.29-3-000001
```

Differences in Analytics Semantics between EventDB and Elasticsearch

FortiSIEM can run on EventDB, its own proprietary NoSQL database, or Elasticsearch. To make analytics work correctly in both environments, it is important to understand the differences. Analytics includes real-time search, historical search, and rule correlation.

FortiSIEM rule correlation and real-time search work identically in both environments, because computation is done in-memory. The database is not used.

However, for historical search, results are obtained from the database and the following differences exist in the area of string comparisons, primarily because of the way Elasticsearch, a third-party product, works.

- Issues
- Example 1 - Matching Event Types
- Example 2 - Matching Raw Messages
- Elasticsearch Support for Regex

Issues

1. EventDB is a sub-string match while Elasticsearch is a word-based match with white space as a delimiter between words. This means that the EventDB will find a match anywhere in the string. For Elasticsearch, you must explicitly include wildcard characters. This affects string operations involving the following operators: =, IN, CONTAIN, REGEXP and their inverse versions: !=, NOT IN, NOT CONTAIN and NOT REGEXP.
2. For Elasticsearch query, if an expression is defined as a display parameter and the expression includes aggregate functions, then the aggregates must be separately added as display parameters. For example, if a user wants to display an expression such as *100 - (100.0 * SUM (System Downtime))/SUM(Polling Interval)*, then the user must also add *SUM(System Downtime)* and *SUM(Polling Interval)* to the list of display parameters.
3. Sorting does not work for
   - LAST and FIRST operators when the operand is a non-Date type.
   - HourOfDay and DayOfWeek operators
4. When sorting is used for multiple key values, e.g. Group By Source IP, Destination IP, COUNT(*) DESC, then the results are presented by the last attribute (e.g. Destination IP). FortiSIEM EventDB sorts by all the fields taken as a tuple, e.g. (Source IP, Destination IP). See

   https://www.elastic.co/guide/en/elasticsearch/reference/current/search-aggregations-bucket-terms-aggregation.html
   See also Example 1 - Matching Event Types and Example 2 - Matching Raw Messages
5. Elasticsearch (and lucene) do not support full Perl-compatible regex syntax.
   https://www.elastic.co/guide/en/elasticsearch/reference/current/regexp-syntax.html
   The table in Elasticsearch Support for Regex lists what is supported and workaround suggestions.

Example 1 - Matching Event Types

Suppose you are trying to match PH_DEV_MON for Event Type:

- In EventDB, you can write any of the following:
  - *EventType CONTAIN PH_DEV_MON*
  - *EventType CONTAIN _DEV_MON*
  - *EventType CONTAIN ph_dev_MON*
  - *EventType CONTAIN _DEV_mon*
- In Elasticsearch, you can write any of the following. Note that since event types do not end with PH_DEV_MON, you have to add the wildcard ".*" at the end.
  - *EventType CONTAIN PH_DEV_MON.**
  - *EventType CONTAIN .*_DEV_MON.**

Suppose you are trying to exactly match PH_DEV_MON_INTF_UTIL for Event Type:

- In EventDB, you can write any of the following:
  - *EventType = PH_DEV_MON_INTF_UTIL*
  - *EventType = ph_dev_mon_intf_util*
  - *EventType = ph_dev_MON_INTF_UTIL*
- In Elasticsearch, you must write:
  - *EventType = PH_DEV_MON_INTF_UTIL*

Example 2 - Matching Raw Messages

REGEX matching using the FortiSIEM eventDB is case insensitive.

Suppose the raw message is:

- *XYZ info="ABB123CCC"*

To match this raw message:

- In EventDB, you can write any of the following:
  - *Raw Message REGEX bb[0-9]*c*X?*
  - *Raw Message REGEX Abb[0-9]*c*X?"$*
- In Elasticsearch, you can write any of the following:
  - *Raw Message REGEX BB[0-9]*c*X?*
  - *Raw Message REGEX .*BB[0-9]*c*X?*

Elasticsearch Support for Regex

Regex syntax	Elasticsearch support	Workaround (if any)
. ? + * |	Yes	
?? +? *?	No	Not possible
()	Yes	
(?:)	No	Use () instead. Replace (?:com|net|org) with (com|net|org)
[]	Yes	
[^]	Yes	
{}	Yes	
{}?	No	Not possible
^ $	No	Elasticsearch requires full match. Add .* for partial match.
\d \D \w \W \s \S	No	Replace \d with [0-9] Replace \D with [^0-9] Replace \w with [a-zA-Z0-9_] Replace \W with [^a-zA-Z0-9_] Replace \s with [\t \n \r] Replace \S with [^ \t \n \r]
\b \A \Z	No	Not possible
(?i:)	No	Not possible
\1 \2	No	Not possible
(?=)	No	Not possible
(?!)	No	Not possible
(?#)	No	Not possible
Case sensitive match on keyword attributes	No	If an attribute is not a keyword, it will be stored as lower case in Elasticsearch. Use abc or [aA][bB][cC]
Entire raw message search	No	Elasticsearch tokenizes string attributes using space as tokens. So, it is not possible to search the whole string. Use CONTAIN operator.

Elasticsearch Known Issues

Note: AWS Elasticsearch Service is now officially known as AWS OpenSearch Service. References to "AWS Elasticsearch Service" can be considered the same as "AWS OpenSearch Service".

1. With pre-compute queries via Rollup, sorting on AVG() is not supported by Elasticsearch. See here.
2. Elasticsearch pre-compute is done using the Elasticsearch Rollup API, which requires raw events matching the pre-compute search condition be populated into a separate Elasticsearch index. This operation can become very expensive if a large number of events match the pre-compute search filter condition. Fortinet recommends that the user set up a report for pre-compute only if the search filter conditions for the pre-compute interval result in less than 100K entries. This allows the pre-computed result to exactly match the adhoc report for faster operation. Specifically, follow these steps:
   a. Suppose you want to run a report in pre-compute mode, with the operation running pre-computations hourly. This means the report will be run hourly, and when a user runs for a longer interval, the pre-computed results would be combined to generate the final result.
   b. Check for pre-compute eligibility.
      i. Run the report in adhoc mode for 1 hour by removing group by conditions.
      ii. If the number of rows is less than 100K, then the original report is a candidate for pre-computation.**Note**: This is for Elasticsearch only. If the number of results in #Bii is more than 100K, then the pre-computed results and adhoc results will be different since FortiSIEM caps the number of results retrieved via Rollup API to be less than 100K.
3. AWS Managed Elasticsearch 7.x limits search.max_buckets to 10K. In 6.8 there was no such limit. This may cause Elasticsearch to throw an exception and not return results for aggregated queries. Contact AWS Managed Elasticsearch Support to increase search.max_buckets to a large value (recommended 10M). There is an API to change this value, but this does not work in AWS Managed Elasticsearch. Therefore you must contact AWS Managed Elasticsearch Support before running queries.
   a. For general discussion about search.max_buckets, see here.
   b. For general discussion about this issue, see here.
   c. Elasticsearch does not consistently handle sorting functions when there are NULL values. For example:
      i. AVG(): NULL values are at the bottom.
      ii. MIN(): NULL values are considered to be the largest value possible, so if you choose ASC (respectively DESC) order, NULL values appear at the bottom (respectively top).
      iii. MAX():NULL values are considered to be the smallest value possible, so if you choose ASC (respectively DESC) order, NULL values appear at the top (respectively bottom).
4. Pre-compute queries do not work with the HAVING clause. Currently, the FortiSIEM GUI is preventing this operation. For public discussion about Rollup search and query scripts, see here.
5. The HourOfDay(Event Receive Time) and DayOfWeek(Event Receive Time) calculations are incorrect if Elasticsearch and Supervisor are in different time zones.
6. In Elasticsearch, a non-aggregated query spanning multiple display pages requires 1 open scroll context per shard. This enables the user to visit multiple pages and see the results. Elasticsearch has a (configurable) limit on open scroll contexts. This is defined in `phoenix_config.txt` on the

Supervisor node. By default, FortiSIEM limits to 1000 open scroll contexts and each context remains open for 60 seconds, as shown.

[BEGIN Elasticsearch]
```
...
max_open_scroll_context=1000
scroll_timeout=60000
...
```
[END Elasticsearch]

When the open scroll context limit is reached, Elasticsearch throws an exception and returns partial results. When 80% of the search context limit is reached, FortiSIEM writes a log in `/opt/phoenix/log/javaQueryServer.log`, as shown.

```
com.accelops.elastic.server.task.ChoresTask - [PH_JAVA_QUERYSERVER_WARN]:
[eventSeverity]=PHL_WARNING,[phEventCategory]=3,[procName]=javaQueryServer,
[phLogDetail]=node=node236, openContexts=1000, it has 80 percent of available search
contexts open
```

- You can increase `max_open_scroll_context`. However, AWS Elasticsearch does not allow more than 500 open scroll contexts, and will enforce a 500 limit. Be careful in choosing very high `max_open_scroll_context`. It is strongly recommended to use a test instance to experiment with your number prior to production.
- After changing `max_open_scroll_context`, you need to apply Test & Save from the GUI for changes to take effect. This is because `max_open_scroll_context` is a cluster level setting.
- You can change `scroll_timeout`, but after changing this value, you must restart the Java Query Server on the Supervisor for the change to take effect.
  For Elasticsearch discussion forum information on this topic, see here.

7. The maximum number of group by query result is 2,000 by default. You can change the setting in `phoenix_config.txt` on the Supervisor node by taking the following steps.
   a. Change the setting: `aggregation_size=2000`
   b. Restart the JavaQueryServer.
8. FortiSIEM uses dynamic mapping for Keyword fields to save Cluster state. Elasticsearch needs to encounter some events containing these fields before it can determine their type. For this reason, queries containing `group by` on any of these fields will fail if Elasticsearch has not seen any event containing these fields. Workaround is to first run a non-group by query with these fields to make sure that these fields have non-null haves.

Examples of Custom Performance Monitors

- Custom JDBC Performance Monitor for a Custom Table
- Custom SNMP Monitor for D-Link Interface Network Statistics
- Custom JMX Monitor for IBM Websphere
- Custom SNMP Monitor for D-Link HostName and SysUpTime
- Custom WMI Monitor for Windows Domain and Physical Registry

Custom JDBC Performance Monitor for a Custom Table

- Planning
- Adding New JDBC Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Examining the Table Structure

For this example, consider two custom Oracle tables that you want to monitor.

1. A table called `HEALTH_STATIC_DEMO` that does not have time stamp as a column. The table does not grow with time, and the `HEALTH` column is updated by the application.

```
create table HEALTH_STATIC_DEMO
{
   ID        VARCHAR2 (200) not null,
   HOST_NAME NVARCHAR2 (200) not null,
   HEALTH    NVARCHAR2 (50)
}
```

2. A table called `HEALTH_DYNAMIC_DEMO` that has a time-stamp in the column `create_time`. Only records with a more recent time-stamp than previous ones have to be pulled in, and every time a new record is written, it includes a time stamp.

```
create table HEALTH_DYNAMIC_DEMO
{
   ID          VARCHAR2 (200) not null,
   HOST_NAME   NVARCHAR2 (200) not null,
   HEALTH      NVARCHAR2 (50),
   CREATE_TIME DATE not null
}
```

Creating New Device Types, Event Attribute Types, and Event Types

To create these items, go to **Admin > Device Support**, and select the appropriate tab(s) to start.

In this case, you only need to create two new event types to handle the contents of the two tables.

Naming Custom Event Types

All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Event Types

Name	Device Type	Priority
PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC	Generic	Low
PH_DEV_MON_CUST_JDBC_PERFORMANCE_DYNAMIC	Generic	Low

Adding New JDBC Performance Objects

Each table requires its own performance object for monitoring.

Performance Object Configuration for Static Table HEALTH_STATIC_DEMO

Field	Setting
Name	jdbc_static_perfObj
Type	Application
Method	JDBC
Database Type	Oracle Database Server
SQL Query	select * from health_static_demo
List of Columns	**Column Name** **Name** **Format** **Event Attribute** host_name STRING hostName health STRING health
Where Clauses	Not applicable, since the table doesn't grow over time
Event Type	PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC
Polling Frequency	180 seconds

Performance Object Configuration for Dynamic Table HEALTH_DYNAMIC_DEMO

Field	Setting			
Name	`jdbc_dynamic_perfObj`			
Type	Application			
Method	JDBC			
Database Type	Oracle Database Server			
SQL Query	`select * from health_dynamic_demo`			
List of Columns	**Column Name**	**Name**	**Format**	**Event Attribute**
	host_name		STRING	hostName
	cpu_util		DOUBLE	cpuUtil
	mem_util		DOUBLE	memUtil
	create_time		STRING	createTime
Where Clauses	retrieve all new values since last retrieve time of column create_time			
Event Type	`PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC`			
Polling Frequency	180 seconds			

Associating Device Types to Performance Objects

In this example, the Oracle database runs on Microsoft Windows, so you must associate Microsoft Windows device types to the two performance objects. Because the discovered device type has to exactly match one of device types in this association for the discovery module to initiate monitoring, you must add other device types, such as Linux, if you also want to monitor Oracle databases over JDBC on those devices.

Edit Device to Performance Object

Field	Settings
Name	windows_oracle_perf_association
Device Types	• Microsoft Windows • Microsoft Windows 7 • Microsoft Windows 98 • Microsoft Windows ME • Microsoft Windows NT • Microsoft Windows Server 2000 • Microsoft Windows Server 2003

Field	Settings
	• Microsoft Windows Server 2008 • Microsoft Windows Vista • Microsoft Windows XP
Perf Objects	• jdbc_static_perfObj(JDBC) - Default Interval:3mins • jdbc_dynamic_perfObj(JDBC) - Default Interval:3mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the database server, created the IP address to credentials mapping, and tested connectivity to the server.

1. Go to **ADMIN** > **Device Support** > **Monitoring**.
2. Select one of the performance monitors you created, and then click **Test**.
3. For **IP**, enter the address of the Oracle database server, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.
   You should see `succeed` under **Result**, and a parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

1. Create a structured historical search, and in the **Filter Criteria**, enter `Event Type = "PH_DEV_MON_CUST_JDBC_PERFORMANCE_STATIC"; Group by:` [None]
   This should show the entries in the `HEALTH_STATIC_DEMO` table
2. Create a structured historical search, and in the **Filter Criteria**, enter `Event Type = "PH_DEV_MON_CUST_JDBC_PERFORMANCE_SDynamic"; Group by:` [None]
   This should show the entries in the `HEALTH_DYNAMIC_DEMO` table .

Custom SNMP Monitor for D-Link Interface Network Statistics

This example shows how to create a custom performance monitor for network interface statistics for D-link switches. In this case, the result is a table, with one set of metrics for each interface.

- Planning
- Adding the D-Link SNMP Performance Object
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Matching SNMP OIDs to FortiSIEM Event Attribute Types

If you run the command `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1` against the D-Link switch, you should see an output similar to this:

```
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
...
```

To get the interface index, you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.1`:

```
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
...
```

To get interface queue length (the `outQLen` event attribute in FortiSIEM), you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.21`:

```
IF-MIB::ifOutQLen.1 = Gauge32: 0
IF-MIB::ifOutQLen.2 = Gauge32: 0
IF-MIB::ifOutQLen.3 = Gauge32: 0
IF-MIB::ifOutQLen.4 = Gauge32: 0
```

```
IF-MIB::ifOutQLen.5 = Gauge32: 0
...
```

To get interface speed, you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.5`:

```
IF-MIB::ifSpeed.1 = Gauge32: 1000000000
IF-MIB::ifSpeed.2 = Gauge32: 1000000000
IF-MIB::ifSpeed.3 = Gauge32: 1000000000
IF-MIB::ifSpeed.4 = Gauge32: 1000000000
IF-MIB::ifSpeed.5 = Gauge32: 1000000000
...
```

To get received bytes (the `recvBitsPerSec` event attribute in FortiSIEM), you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.10`:

```
IF-MIB::ifInOctets.1 = Counter32: 0
IF-MIB::ifInOctets.2 = Counter32: 1247940872
IF-MIB::ifInOctets.3 = Counter32: 0
IF-MIB::ifInOctets.4 = Counter32: 0
IF-MIB::ifInOctets.5 = Counter32: 0
...
```

Finall,y to get sent bytes (the `sentBitsPerSec` event attribute in FortiSIEM), you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.2.2.1.16`:

```
IF-MIB::ifOutOctets.1 = Counter32: 0
IF-MIB::ifOutOctets.2 = Counter32: 1271371281
IF-MIB::ifOutOctets.3 = Counter32: 0
IF-MIB::ifOutOctets.4 = Counter32: 0
IF-MIB::ifOutOctets.5 = Counter32: 0
...
```

From these outputs you can see that if you want to create a performance monitor for D-Link switch uptime, you must:

1. Create a new device type, since D-Link switches are not supported in this release.
2. Create an event type, `PH_DEV_MON_CUST_DLINK_INTF_STAT`, that will contain the event attribute types `outQLen`, `recvBitsPerSec`, and `sentBitsPerSec`, which are already part of the FortiSIEM event attribute library, and `hostNameSnmpIndx` and `intfSpeed`, which you must create.
3. Create the mapping between the SNMP OIDs and the event attributes:
   a. OID `.1.3.6.1.2.1.2.2.1.1` and `hostNameSnmpIndx`
   b. OID `.1.3.6.1.2.1.2.2.1.5` and `intfSpeed`
   c. OID `.1.3.6.1.2.1.2.2.1.21` and `outQLen`
   d. OID `.1.3.6.1.2.1.2.2.1.10` and `recvBitsPerSec`
   e. OID .1.3.6.1.2.1.2.2.1.16 and `sentBitsPerSec`

Creating New Device Types, Event Attributes, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

Device Type

Create a new device type with these attributes:

Field	Setting
Vendor	D-Link
Model	DGS
Version	Any
Device/App Group	**Devices > Network Devices > Router Switch**
Biz Service Group	<no selection>
Description	D-Link Switch

Event Attribute Types

Create these event attribute types:

Name	Display Name	Value Type	Display Format Type
hostSnmpIndex	Host Interface SNMP Index	INT64	<left blank>
intfSpeed	Interface Speed in bits/sec	INT64	<left blank>

Event Types

Naming Custom Event Types: All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Create this event type:

Name	Device Type	Severity
`PH_DEV_MON_CUST_INTF_STAT`	D-Link DGS	Low

Adding the D-Link SNMP Performance Object

In this case, you will create one performance object that will map the SNMP OIDs to the FortiSIEM event attribute types, and then associate them with the `PH_DEV_MON_CUST_INTF_STAT` event type. When you create the `recvBitsPerSec` and `sentBitsPerSec` mapping you will also add a sequential transform to convert the cumulative metric to a rate, and then convert bytes per second to bits per second. .

Performance Object Configuration for Event Type PH_DEV_MON_CUST_INTF_STAT

Field	Setting
Name	D-LinkIntStat
Type	System
Method	SNMP
Parent OID	.1.3.6.1.2.1.2.2.1
Parent OID is Table	Selected
List of OIDs	**Object Attribute** / **Name** / **Format** / **Type** / **Event Attribute** .1.3.6.1.1.2.1.2.2.1.1 / IntfIndex / INTEGER / RawValue / `hostSnmpIndex` .1.3.6.1.1.2.1.1.2.1.5 / intfSpeed / Gauge32 / RawValue / `intfSpeed` .1.3.6.1.1.2.1.1.2.1.10 / recvBitsPerSec / Counter32 / Counter / recvBitsPerSec .1.3.6.1.1.2.1.1.2.1.16 / sentBitsPerSect / Counter32 / Counter / sentBitsPerSect .1.3.6.1.1.2.1.1.2.1.21 / outInftQ / Gauge32 / RawValue / OutQLen
Event Type	PH_DEV_MON_CUST_INTF_STAT
Polling Frequency	60 seconds

Transform Formula for recvBitsPerSec and sentBitsPerSec Event Attributes

Type	Formula
system	toRate
system	BytesPerSecToBitsPerSec

Associating Device Types to Performance Objects

In this case you would only need to make one association with the D-Link DGS device you created.

Field	Settings
Name	`D-LinkPerfObj`
Device Types	• D-Link DGS
Perf Objects	• D-LinkIntfStat(SNMP) - Default Interval:1mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the D-Link device, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Monitoring**.
2. Select the performance monitor you created, and then click **Test**.
3. For **IP**, enter the address of the device, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.
   You should see `succeed` under **Result**, and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

Filter Criteria	Display Columns	Time	For Organizations
Structured `Reporting IP IN <IP Range> AND Event Type =" PH_DEV_MON_CUST_INTF_STAT"; Group by: Host Name, Host Interface`	Host Name,Host Interface SNMP Index,MAX(Out Intf Queue), AVG(Intf Speed), AVG (Sent Bit Rate), AVG(Received Bit Rate)	Last 10 Minutes	All

Custom JMX Monitor for IBM Websphere

- Planning
- Adding New IBM WebSphere Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

This example illustrates how to write a custom performance monitor for retrieving IBM Websphere thread, heap memory, and non-heap memory metrics.

Planning

Creating New Device Types, Event Attribute Types, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

In this case, the IBM Websphere device type is already supported by FortiSIEM, but you must create new event attributes and event types for the metrics you want to retrieve.

Event Attribute Types

Name	Display Name	Value Type	Display Format Type
websphere_heapPCT	WebSphere HeapPct	INT64	
websphere_numThreads	WebSphere NumThreads	INT64	
websphere_maxThreads	WebSphere MaxThreads	INT64	
websphere_threadPct	WebSphere ThreadPct	INT64	
websphere_numClass	WebSphere NumClass	INT64	
websphere_heapUsed	WebSphere HeapUsed	INT64	Bytes
websphere_heapMax	WebSphere HeapMax	INT64	Bytes
websphere_heapCommitted	WebSphere HeapCommitted	INT64	Bytes
websphere_nonHeapUsed	WebSphere NonHeapUsed	INT64	Bytes
websphere_nonHeapMax	WebSphere NonHeapMax	INT64	Bytes
websphere_	WebSphere	INT64	Bytes

Name	Display Name	Value Type	Display Format Type
nonHeapCommitted	NonHeapCommitted		

Event Types

Naming Custom Event Types: All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Name	Device Type	Severity
PH_DEV_MON_CUST_WEBSPHERE_HEAPMEMORY	IBM WebSphere App Server	Low
PH_DEV_MON_CUST_WEBSPHERE_NON_HEAPMEMORY	IBM WebSphere App Server	Low
PH_DEV_MON_CUST_WEBSPHERE_THREAD	IBM WebSphere App Server	Low

Adding New IBM WebSphere Performance Objects

Each of the event types requires creating a performance object for monitoring.

Performance Object Configuration for Event Type PH_DEV_MON_CUST_WEBSPHERE_HEAPMEMORY

Field	Setting
Name	websphere_heapMemory_perfObj
Type	Application
Method	JMX
MBean	java.lang:type=Memory
List of Attributes	

Object Attribute	Private Key	Name	Format	Event Attribute
HeapMemoryUsage	committed	committed	Long	websphere_heapCommitted
HeapMemoryUsage	used	used	Long	websphere_heapUsed
HeapMemoryUsage	max	max	Long	websphere_heapMax
			Long	websphere_heapPCT

Field	Setting
Event Type	PH_DEV_MON_CUST_WEBSPHERE_HEAPMEMORY
Polling Frequency	180 seconds

Performance Object Configuration for Event Type PH_DEV_MON_CUST_WEBSPHERE_THREAD

For the webSphere_threadPct**Event Attribute**, you will enter a transform as shown in the second table.

Field	Setting				
Name	websphere_thread_perfObj				
Type	Application				
Method	JMX				
MBean	java.lang:type=Threading				
List of Attributes	**Object Attribute**	**Private Key**	**Name**	**Format**	**Event Attribute**
	ThreadCount		ThreadCount	Long	websphere_numThreads
	PeakThreadCount		PeakThreadCount	Long	websphere_maxThreads
				Long	websphere_threadPCT
Event Type	PH_DEV_MON_CUST_WEBSPHERE_THREAD				
Polling Frequency	180 seconds				

Transform Formula for websphere_threadPCT Event Attribute

Click **New** next to **Transforms** in the dialog to enter the formula.

Field	Settings
Object Attribute	<blank>
Name	<blank>
Private Key	<blank>
Format	Long
Event Attribute	websphere_threadPct

Field	Settings
Transforms	**Type** **Formula** custom ThreadCount*100/PeakThreadcount

Performance Object Configuration for Event Type PH_DEV_MON_CUST_WEBSPHERE_NON_HEAPMEMORY

Field	Setting
Name	`websphere_nonHeapMemory_perfObj`
Type	Application
Method	JMX
MBean	`java.lang:type=Memory`
List of Attributes	**Object Attribute** **Private Key** **Name** **Format** **Event Attribute** NonHeapMemoryUsage used Long `websphere_nonHeapUsed` NonHeapMemoryUsage committed Long `websphere_nonHeapCommitted` NonHeapMemoryUsage max Long `websphere_nonHeapMax`
Event Type	`PH_DEV_MON_CUST_WEBSPHERE_NON_HEAPMEMORY`
Polling Frequency	180 seconds

Associating Device Types to Performance Objects

In this example, IBM WebSphere runs on Microsoft Windows, so you must associate Microsoft Windows device types to the three performance objects. Because the discovered device type has to exactly match one of device types in this association for the discovery module to initiate these monitors, you must add other device types, such as Linux, if you also wanted to monitor IBM Websphere over JMX on those devices.

Edit Device to Performance Object

Field	Settings
Name	windows_oracle_perf_association
Device Types	• Microsoft Windows • Microsoft Windows 7 • Microsoft Windows 98 • Microsoft Windows ME • Microsoft Windows NT • Microsoft Windows Server 2000 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Vista • Microsoft Windows XP
Perf Objects	• websphere_thread_perfObj(JMX) - Default Interval:3mins • websphere_thread_perfObj(JMX) - Default Interval:3mins • websphere_nonHeapMemory_perfObj (JMX) - Default Interval:3mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the server, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Monitoring**.
2. Select one of the performance monitors you created, and then click **Test**.
3. For **IP**, enter the address of the Oracle database server, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test** .
   You should see `succeed` under **Result** , and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

Filter Criteria	Display Columns	Time	For Organizations

Structured
`Reporting IP IN <IP Range> AND Event Type CONTAIN "ph_dev_mon_cust_web";`
`Group by: [None]`
	Event Receive Time,Reporting IP, Event	Last 60 Minutes	All

Custom SNMP Monitor for D-Link HostName and SysUpTime

Although D-link switches and routers are not supported in this release of FortiSIEM, you can still use the custom monitor feature to create a system uptime event that will collect basic performance metrics like `hostName` and `SysUpTime`.

- Planning
- Adding New IBM WebSphere Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Mapping SNMP OIDs to FortiSIEM Event Attribute Types

If you run the command `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.1` against the D-Link switch, you should see an output similar to this:

```
SNMPv2-MIB::sysDescr.0 = STRING: DGS-1210-48          2.00.011
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.171.10.76.11
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (157556100) 18 days, 5:39:21.00
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: SJ-Test-Lab-D-Link
SNMPv2-MIB::sysLocation.0 = STRING: San Jose
```

```
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (157555949) 18 days, 5:39:19.49
```

To get sysUptime, you would run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.1.3`:

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (157577770) 18 days, 5:42:57.70
```

To get hostname, you run `snmpwalk -v 1 -c <community> <ip> .1.3.6.1.2.1.1.5`:

```
SNMPv2-MIB::sysName.0 = STRING: SJ-Test-Lab-D-Link
```

From these outputs you can see that if you want to create a performance monitor for D-Link switch uptime, you must:

1. Create a new device type, since D-Link switches are not supported in this release
2. Create an event type, `PH_DEV_MON_CUST_DLINK_UPTIME`, that will contain the event attribute types `hostName` and `SysUpTime`, which are already part of the FortiSIEM event attribute type library.
3. Create the mapping between the SNMP OIDs and the event attributes:
   - OID `.1.3.6.1.2.1.1.5` and `hostName`.
   - OID `.1.3.6.1.2.1.1.5` and `SysUpTime`.

Creating New Device Types, Event Attribute Types, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

Device Type:

Create a new device type with these attributes:

Field	Setting
Vendor	D-Link
Model	DGS
Version	Any
Device/App Group	**Devices > Network Devices > Router Switch**
Biz Service Group	<no selection>
Description	D-Link Switch

Event Attribute Types and Event Types

Both `sysUptime` and `hostName` are included in the **Event Attribute Types**, so you only need to create a new event type, `PH_DEV_MON_CUST_DLINK_UPTIME`, that will contain them.

Naming Custom Event Types

All custom event types must begin with the prefix `PH_DEV_MON_CUST_` .

Name	Device Type	Severity	Description
PH_DEV_MON_CUST_DLINK_UPTIME	D-Link DGS	0 - Low	D-Link Uptime

Adding the D-Link SNMP Performance Object

In this case, you will create one performance object that will map the SNMP OIDs to the FortiSIEM event attribute types hostName and SysUptime, and then associate them with the PH_DEV_MON_CUST_DLINK_UPTIME event type. When you create the SysUpTime mapping you will also add a transform to convert system time to centiseconds to seconds as shown in the second table.

Performance Object Configuration for Event Type PH_DEV_MON_CUST_DLINK_UPTIME

Field	Setting				
Name	D-LinkUptime				
Type	System				
Method	SNMP				
Parent OID	.1.3.6.1.1.2.1.1				
Parent OID is Table	<left cleared>				
List of OIDs	**Object Attribute**	**Name**	**Format**	**Type**	**Event Attribute**
	.1.3.6.1.1.2.1.1.5	Host Name	String	RawValue	hostName
	.1.3.6.1.1.2.1.1.3	Uptime	Timeticks	RawValue	SysUpTime
Event Type	PH_DEV_MON_CUST_DLINK_UPTIME				
Polling Frequency	10 seconds				

Transform Formula for SysUptime Event Attribute

Type	Formula
custom	uptime/100

Associating Device Types to Performance Objects

In this case you would only need to make one association with the D-Link DGS device you created.

Field	Settings
Name	`D-LinkPerfObj`
Device Types	D-Link DGS
Perf Objects	D-LinkUptime(SNMP) - Default Interval:0.17mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the D-Link device, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Performance Monitoring**.
2. Select the performance monitor you created, and then click **Test**.
3. For **IP**, enter the address of the device, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.
   You should see `succeed` under **Result**, and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

Filter Criteria	Display Columns	Time	For Organizations
Structured `Reporting IP IN <IP Range> AND Event Type = "PH_DEV_MON_CUST_DLINK_UPTIME"; Group by: [None]`	Event	Last 10 Minutes	All

Custom WMI Monitor for Windows Domain and Physical Registry

- Planning
- Adding New IBM WebSphere Performance Objects
- Associating Device Types to Performance Objects
- Testing the Performance Monitor
- Enabling the Performance Monitor
- Writing Queries for the Performance Metrics

Planning

Mapping Windows WMI Classes to FortiSIEM Event Attribute Types

If you run the command `wmic -U <domain>/<user>%<pwd> //<ip> "select * from Win32_ComputerSystem` against a Windows server, you will see an output similar to this:

```
CLASS: Win32_ComputerSystem

AdminPasswordStatus::SEP::AutomaticManagedPagefile::SEP::AutomaticResetBootOption::SEP::Au
tomaticResetCapability::SEP::BootOptionOnLimit::SEP::BootOptionOnWatchDog::SEP::BootROMSup
ported::SEP::BootupState::SEP::Caption::SEP::ChassisBootupState::SEP::CreationClassName::S
EP::CurrentTimeZone::SEP::DaylightInEffect::SEP::Description::SEP::DNSHostName::SEP::Domai
n::SEP::DomainRole::SEP::EnableDaylightSavingsTime::SEP::FrontPanelResetStatus::SEP::Infra
redSupported::SEP::InitialLoadInfo::SEP::InstallDate::SEP::KeyboardPasswordStatus::SEP::La
stLoadInfo::SEP::Manufacturer::SEP::Model::SEP::Name::SEP::NameFormat::SEP::NetworkServerM
odeEnabled::SEP::NumberOfLogicalProcessors::SEP::NumberOfProcessors::SEP::OEMLogoBitmap::S
EP::OEMStringArray::SEP::PartOfDomain::SEP::PauseAfterReset::SEP::PCSystemType::SEP::Power
ManagementCapabilities::SEP::PowerManagementSupported::SEP::PowerOnPasswordStatus::SEP::Po
werState::SEP::PowerSupplyState::SEP::PrimaryOwnerContact::SEP::PrimaryOwnerName::SEP::Res
etCapability::SEP::ResetCount::SEP::ResetLimit::SEP::Roles::SEP::Status::SEP::SupportConta
ctDescription::SEP::SystemStartupDelay::SEP::SystemStartupOptions::SEP::SystemStartupSetti
ng::SEP::SystemType::SEP::ThermalState::SEP::TotalPhysicalMemory::SEP::UserName::SEP::Wake
UpType::SEP::Workgroup

1::SEP::True::SEP::True::SEP::True::SEP::3::SEP::3::SEP::True::SEP::Normal
boot::SEP::WIN2008-ADS::SEP::3::SEP::Win32_ComputerSystem::SEP::-420::SEP::True::SEP::AT/AT
COMPATIBLE::SEP::WIN2008-
ADS::SEP::FortiSIEM.net::SEP::5::SEP::True::SEP::3::SEP::False::SEP::NULL::SEP::
(null)::SEP::3::SEP::(null)::SEP::VMware, Inc.::SEP::VMware Virtual Platform::SEP::WIN2008-
ADS::SEP::(null)::SEP::True::SEP::1::SEP::1::SEP::NULL::SEP::([MS_VM_
CERT/SHA1/27d66596a61c48dd3dc7216fd715126e33f59ae7],Welcome to the Virtual
```

```
Machine)::SEP::True::SEP::3932100000::SEP::0::SEP::NULL::SEP::False::SEP::0::SEP::0::SEP::
3::SEP::(null)::SEP::Windows User::SEP::1::SEP::-1::SEP::-1::SEP::(LM_Workstation,LM_
Server,Primary_Domain_
Controller,Timesource,NT,DFS)::SEP::OK::SEP::NULL::SEP::0::SEP::NULL::SEP::0::SEP::X86-
based PC::SEP::3::SEP::4293496832::SEP::FortiSIEM\Administrator::SEP::6::SEP::(null)
```

From this output you can see that the `Win32_ComputerSystem` WMI class has two attributes:

- `Domain`
- `TotalPhysicalMemory`

From these outputs you can see that if you want to create a performance monitor for Windows Domain and Physical Registry, you must:

1. Create an event type, `PH_DEV_MON_CUST_WIN_MEM`, that will contain the event attribute types `Domain` and `memTotalMB`, both of which are already contained in the FortiSIEM event attribute types library.
2. Create the mapping between the WMI class attributes and the FortiSIEM event attribute types:
   - WMI class attribute `Domain` and `Domain`.
   - WMI class attribute `TotalPhysicalMemory` (Bytes) and `memTotalMB` (type INT64). Because `TotalPhysicalMemory` returns in bytes, and `memTotalMB` is in `INT64`, a transform will be required to convert the metrics.

Creating New Device Types, Event Attributes, and Event Types

To create these items, go to **ADMIN > Device Support**, and select the appropriate tab(s) to start.

- **Device Type**
  Since Microsoft Windows is supported by FortiSIEM, you don't need to create a new device type.
- **Event Attribute Types and Event Types**
  Both `Domain` and `memTotalMB` are included in the FortiSIEM event attribute type library, so you only need to create a new event type, `PH_DEV_MON_CUST_WIN_MEM`, that will contain them.
- **Naming Custom Event Types**
  All custom event types must begin with the prefix `PH_DEV_MON_CUST_`.

Name	Device Type	Severity	Description
`PH_DEV_MON_CUST_WIN_MEM`	Microsoft Windows	0 - Low	Windows Domain and Memory

Adding the Microsoft Windows WMI Performance Object

In this case, you will create one performance object that will map the WMI Class attributes to the FortiSIEM event attribute types `Domain` and `memTotalMB`, and then associate them with the `PH_DEV_MON_CUST_WIN_MEM` event type. When you create the `memTotalMB` mapping you will also add a transform to convert bytes to INT64 as shown in the second table.

Performance Object Configuration for Event Type PH_DEV_MON_CUST_DLINK_UPTIME

Field	Setting
Name	WinMem
Type	System
Method	WMI
Parent Class	Win32_ComputerSystem
Parent Class is Table	<left cleared>
List of Attributes	**Attribute** / **Format** / **Type** / **Event Attribute** Domain / String / RawValue / `domain` TotalPhysicalMemory / Integer / RawValue / `memTotalMB`
Event Type	`PH_DEV_MON_CUST_WIN_MEM`
Polling Frequency	20 seconds

Transform Formula for TotalPhysicalMemory Event Attribute Type

Type	Formula
custom	TotalPhysicalMemory/1024/1024

Associating Device Types to Performance Objects

In this example, you must associate Microsoft Windows device types to the performance object.

Edit Device to Performance Object

Field	Settings
Name	WinMisc
Device Types	• Microsoft Windows • Microsoft Windows NT • Microsoft Windows Server 2000 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008

Field	Settings
	• Microsoft Windows Vista • Microsoft Windows XP
Perf Objects	• WinMem(WMI) - DefaultInterval:0.33mins

Testing the Performance Monitor

Before testing the monitor, make sure you have defined the access credentials for the server, created the IP address to credentials mapping, and tested connectivity.

1. Go to **ADMIN > Device Support > Monitoring**.
2. Select one of the performance monitors you created, and then click **Test**.
3. For **IP**, enter the address of the Microsoft Windows server, and select either the Supervisor or Collector node that will retrieve the information for this monitor.
4. Click **Test**.
   You should see `succeed` under **Result**, and the parsed event attributes in the test result pane.
5. When the test succeeds, click **Close**, and then click **Apply** to register the new monitor with the back-end module.

Enabling the Performance Monitor

1. Discover or re-discover the device you want to monitor.
2. Once the device is successfully discovered, make sure that the monitor is enabled and pulling metrics.

Writing Queries for the Performance Metrics

You can now use a simple query to make sure that the metrics are pulled correctly. The search results should display the metrics for the event attributes you defined.

Create a structured historical search with these settings:

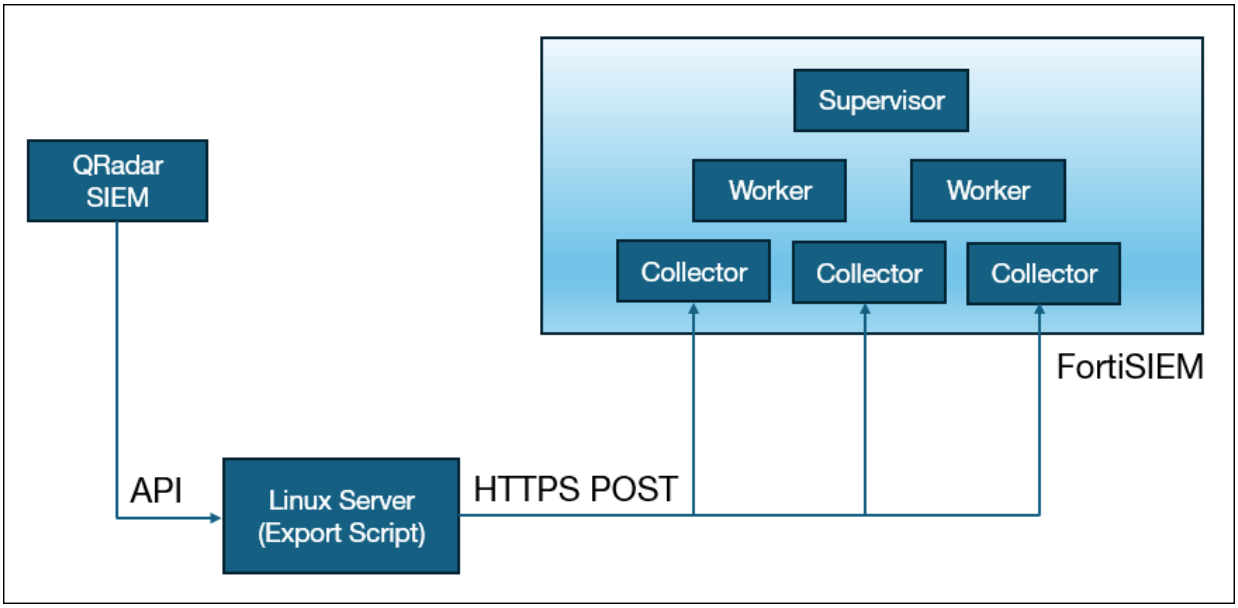
Filter Criteria	Display Columns	Time	For Organizations
`Host IP = <IP> AND Event Type = "PH_DEV_MON_CUST_WIN_MEM";Group by:[None]`	Event Receive Time,Reporting IP,Domain,Total Memory (MB)	Last 10 Minutes	All

Exporting QRadar Logs to FortiSIEM

The following document provides a procedure for exporting logs stored in QRadar SIEM into FortiSIEM.

- Overview
- Prerequisites
- Resource Considerations
- Planning the Export
- Export Procedure
- Export Procedure for Service Provider Deployments
- Validating Events Ingested

Overview



The export process works as follows:

1. The export script requires Python 3.9 or higher and can run on any server, including the FortiSIEM Collector itself. However, it is recommended to use a separate Linux server to reduce the load on the FortiSIEM Collectors.
2. The script connects to the QRadar SIEM via API on port 443 and collects raw logs along with the Reporting Device IP or Host Name and the time at which the log was received in QRadar.
3. The script then sends the logs to a FortiSIEM Collector via HTTPS POST.
4. The Collector parses the logs as if they were directly received from the external device and stores them in FortiSIEM.

Prerequisites

1. FortiSIEM 7.2.2 or later is needed. If you are running an older FortiSIEM version of 7.2.1 or above, then contact Fortinet for a Collector patch.
2. Ensure both the QRadar SIEM and the FortiSIEM Collector are reachable via TCP 443 from the server running the python script.
3. The raw logs in QRadar SIEM must be in the same format as supported by FortiSIEM, else parsing will fail, and the logs will be stored in FortiSIEM as Unknown Event Type. Refer to the FortiSIEM External Systems Configuration Guide for supported log formats for various vendors. To overcome formatting issues, you might like to write a parser first before beginning the ingestion process. Note that the raw logs can still be searched using keywords.

Resource Considerations

1. Ensure both the QRadar Instance and the FortiSIEM Collector is reachable via TCP 443 from the machine running the python script.
2. The QRadar instance should be properly sized for processing Ariel search queries from the Linux Server running the export script.
3. Fortinet recommends a large collector with at least 16vCPU, 32GB RAM to handle the bursty EPS during the export process.
4. The FortiSIEM Supervisor and Worker instances should be sufficiently sized to handle the bursty EPS during the export process. Refer to the appropriate FortiSIEM Sizing Guide from the FortiSIEM Documentation Library.
5. The Linux Server running the export script should be sufficiently sized with a large number of vCPU so it can have an increased thread worker count on the script. Fortinet recommends at least 16vCPU, 32GB RAM.

Planning the Export

To create the optimal way to export your data, take the following actions.

1. Identify how many days of data you want to export from QRadar.
2. Break up those days into test chunks.
   a. Complete the first week in 1 day chunks (run the script on a one day interval).
   b. Complete subsequent chunks of data 1 week at a time.
3. Observe execution time on 1 day chunk of exported data, after the script runs, and identify how long it took from the output.
4. Observe the CPU and memory utilization of the following instances. Increase vCPU or memory if better performance is required.

a. QRadar Instance
b. FortiSIEM Collector
c. Supervisor and Worker health as seen from FortiSIEM GUI
d. The host running the export script

How Time Range is Handled

The script breaks up the time range into chunks of minutes as defined by the `--interval-min` argument, which defaults to 1 minute chunks. This ensures that incredibly large queries can be evenly spread for each worker thread until the entire dataset is pushed to FortiSIEM.

Note: Even small chunks of time like 30 minutes can be an incredibly large dataset if the QRadar instance was ingesting 50K-100K events per second during the time range queried.

Example 1: High EPS - Small Query Intervals

The date range is 7 days, and `interval-min` is set to 1 minute. The script will break the time range into separate 1 minute API calls, or 1,440 queries per day x 7 days = 10,080 API (Ariel search queries) calls. These will be evenly spread over the number of worker threads (default, if not specified, is 5 worker threads).

The QRadar Instance will experience 5 concurrent Ariel search queries for 1 minute of data each. As each of these finish, a new worker thread issues another 1 minute query until all the data has been retrieved.

Example 2: Low EPS - Larger Query Intervals

The date range is 7 days, and `interval-min` is set to 10 minutes. The script will break the time range into separate 10 minute API calls, or 144 queries per day x 7 days = 1,008 API (Ariel search queries) calls. These will be evenly spread over the number of worker threads (default, if not specified, is 5 worker threads).

Export Procedure

The export procedure is comprised of 5 general steps.

- Step 1: Generate QRadar API Key for Log Export
- Step 2: Configure QRadar Payload Truncation of Raw Logs
- Step 3: Set up API Upload Credential in FortiSIEM Collector
- Step 4: Run Export Script
- Step 5: Confirm Ingested Data in FortiSIEM

Step 1: Generate QRadar API Key for Log Export

Reference: https://www.ibm.com/docs/en/qsip/7.5?topic=services-adding-authorized-service

1. Login to your QRadar Instance.
2. Navigate to **Admin > User Management > Authorized Services**.
3. Click **Add**, and enter the following information.
   a. In the **Authorized Service Label** field enter a name such as "FortiSIEM_Export".
   b. From the **Security Profile** list, select **Admin**.
   c. From the **User Role** list, select **Admin**.
   d. From **Expiry Settings**, uncheck any existing expiry settings to allow no expiry.
   e. Click **Save**.

A pop up will display the API key. Record this information.

Step 2: Configure QRadar Payload Truncation of Raw Logs

QRadar by default, truncates raw logs in storage (TCP syslog default 4,096, UDP syslog default 1,024), destroying part of the raw event. In order to adequately export and re-parse the syslog messages in FortiSIEM, the original non-truncated/unmodified raw event is needed.

To change the QRadar syslog payload length setting, take the following steps from your QRadar Instance.

1. Navigate to **Admin > System Configuration > System Settings**.
2. Click on the Advanced icon.
   a. Set **Max TCP Syslog Payload Length** to "24000".
   b. Set **Max UDP Syslog Payload Length** to "24000".
   c. Click **Save**.
3. From the **Admin** tab, click **Advanced > Deploy Full Configuration > Continue**.
   Note: This will not affect existing logs that were truncated, only new logs coming in, so we hope this setting was already set prior to export.

Step 3: Set up API Upload Credential in FortiSIEM Collector

Take the following steps:

1. Login to the FortiSIEM Collector via SSH.
2. Define a username and password and run the following command as user `root`:
   `htpasswd -b /etc/httpd/accounts/passwds <user> <password>`

Step 4: Run Export Script

The following script (`qradar_export.py`) will connect to QRadar SIEM via API, collect the logs and send them to FortiSIEM Collector via HTTPS POST.

Notes:

1. It is strongly recommended that you run the `qradar_export.py` script in a `screen` or `tmux` command on Linux, so it can effectively run for long periods in the background. Tmux is a Linux program that allows running a script in a background process. For really long operations, you can launch a tmux session first, then run the script, and then leave it running in the background. If you skip this step, and your SSH session times out, the script will stop executing.
   For a tutorial on tmux, see https://www.redhat.com/sysadmin/introduction-tmux-linux
2. This is a one-time script, so scheduling via `crond` is not recommended for any reason.
3. Go through the Prerequisites, Resource Considerations and Planning the Export sections above before running the script.
4. The script requires Python 3.9 or later. Required python modules: `requests` and `urllib3`. To get these modules, run the following command.
   `pip install requests urllib3`
   These modules are already installed on FortiSIEM Collectors.
5. The script resides in the following location on any FortiSIEM v7.2.2 or later installation:
   `/opt/phoenix/bin/qradar_export.py`

The Script:

```
qradar_export.py --qradar-host <host IP address> --api-token '<API token>' \
--start-date '<yyyy-mm-dd hh:mm:ss>' --end-date '<yyyy-mm-dd hh:mm:ss>' \
--fsm-collector '<FortiSIEM Collector FQDN/IP>' \
--fsm-user '<FortiSIEM Collector username>' \
--fsm-password '<FortiSIEM Collector password>' \
--no-verify-ssl --num-threads <Number of threads> --interval-min <minute time interval>
```

Note: Remember that the `--start-date` and `--end-date` time range is expectedin the QRadar instance server local time.

Example Usage

```
python qradar_export.py --qradar-host '1.1.1.1' \
--api-token 'xxxxx-xxxxxxx-xxxxxx-xxxxx' \
--start-date '2024-06-20 00:00:00' --end-date '2024-06-20 23:59:59' \
--fsm-collector '2.2.2.2' --fsm-user 'myuser' --fsm-password 'mypass' --no-verify-ssl
```

Script Arguments	Required	Description
`--api-token`	Yes	The QRadar API token collected in Step 1.
`--fsm-collector`	No	Target FortiSIEM Collector FQDN or IP address. Defaults to 127.0.0.1.
`--fsm-password`	Yes	FortiSIEM Collector API Password defined in Step 3.
`--fsm-user`	Yes	FortiSIEM Collector API Username defined in Step 3.
`--interval-min`	No	Time chunk interval in minutes that each thread handles. The time range is broken into query chunks of 1 minute by default.
`--no-verify-ssl`	No	If specified, this will disable SSL verification. Otherwise, all network connections will attempt SSL verification.
`--num-threads`	No	The number of allowed concurrent API calls to QRadar. The default number is 5. The following formula is recommended for the number of threads. 2 x number of cores.
`--qradar-host`	Yes	The QRadar host IP address.
`--start-date`	Yes	The start date for the query in `YYYY-MM-DD` format or `YYYY-MM-DD HH:MM:SS` - QRadar server local timezone expected. See How Time Range is Handled for more information.
`--end-date`	Yes	The end date for the query in `YYYY-MM-DD` format or `YYYY-MM-DD HH:MM:SS` - QRadar server local timezone expected. A large time range, for example 30 days, can be used, but it is recommended to initially use a smaller time range, such as a single day to check its performance. See How Time Range is Handled for more information.

Examples

The first example assumes a RHEL based system (RHEL, Rocky Linux, Alma Linux), and the second example runs the script directly on a FortiSIEM Collector. You can run the Python script in any environment however.

Example 1: Running the Script on a Third Party Linux Machine with Python 3.9 Installed as the Default Interpreter

```
pip install requests urllib3

sudo dnf install tmux -y

tmux

python qradar_export.py --qradar-host '1.1.1.1' --api-token 'xxxxx-xxxxxxx-xxxxxx-xxxxx'
--start-date '2024-06-20 00:00:00' --end-date '2024-06-20 23:59:59' --fsm-collector
'2.2.2.2' --fsm-user 'myuser' --fsm-password 'mypass' --no-verify-ssl –num-threads 16
```

(Optional) You can detach from a tmux session and let it run by pressing Ctrl + b, then releasing those keys, then pressing the letter ‘d’.

To view tmux sessions running in the background, enter the following command.

```
tmux ls
```

To reattach to a tmux session running in the background, enter the following command.

```
tmux attach-session -t <session_name_or_number>
```

To exit a tmux session, closing it down, while attached to the session, enter the following command and hit enter.

```
exit
```

Example 2: Running the Script on the FortiSIEM Collector Itself

The Collector runs the script that connects to the remote QRadar instance, and POSTS results to itself by running the following commands.

```
sudo dnf install tmux -y
```

```
tmux
```

```
python3.9 qradar_export.py --qradar-host '1.1.1.1' --api-token 'xxxxx-xxxxxxx-xxxxxx-xxxxx' --start-date '2024-06-20 00:00:00' --end-date '2024-06-20 23:59:59' --fsm-collector '127.0.0.1' --fsm-user 'myuser' --fsm-password 'mypass' --no-verify-ssl –num-threads 16
```

(Optional) You can detach from a tmux session and let it run by pressing Ctrl + b, then releasing those keys, then pressing the letter ‘d’.

To view tmux sessions running in the background, enter the following command.

```
tmux ls
```

To reattach to a tmux session running in the background, enter the following command.

```
tmux attach-session -t <session_name_or_number>
```

To exit a tmux session, closing it down, while attached to the session, simply enter the following command and hit enter.

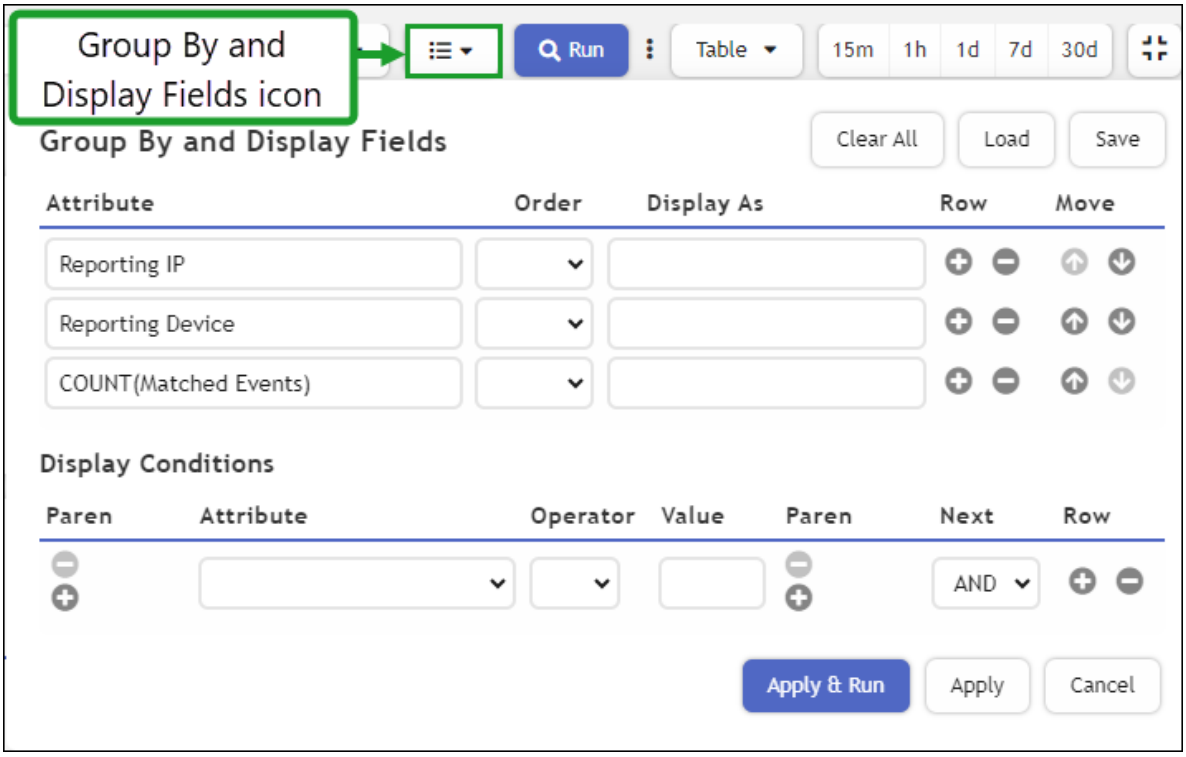
```
exit
```

Step 5: Confirm Ingested Data in FortiSIEM

When the script begins running, you should almost immediately start to see a stream of log events coming into FortiSIEM. To check, take the following steps.

1. Login to FortiSIEM GUI.
2. Navigate to **Analytics**.
3. Run a historical query for the data time range the script is actively exporting.
4. Examine the events in that time frame, and ensure the reporting IP (equivalent to QRadar Sending IP, or log source identifier (if IP address)), and ensure these are logs from the QRadar instance).
5. For an easier overview, you can run an aggregate query here over the same time range. Click the "Group By and Display Fields" icon, and add/include the following Attribute columns:
   - Reporting IP
   - Reporting Device
   - COUNT(Matched Events)

   and click **Apply & Run**.



You should see a breakdown of all the reporting devices (log sources in QRadar terminology), including those exported from QRadar. You can match this up to the QRadar log sources list to ensure your external log sources are getting migrated.

Export Procedure for Service Provider Deployments

If you are planning to export QRadar logs from a Service Provider Deployment into FortiSIEM, then follow the steps in Export Procedure with the minor modifications outlined below. *The concept of Tenant in QRadar is identical to Organization in FortiSIEM.*

1. Deploy a FortiSIEM in Service Provider mode and create all the Organizations corresponding to the Tenants in QRadar. For each Organization, define, deploy, and register the Collector(s). Note that the Organization name in FortiSIEM does not need to exactly match the Tenant name in QRadar. After the data is imported to FortiSIEM, events will have the Organization name defined in FortiSIEM.
   You must repeat the following steps 2-6 for each Organization (Tenant).
2. Perform Export Procedure Step 1, but create the API key with the tenant/domain restricted role and security profile for that tenant application.
   Note: Firefox is the recommended browser for the QRadar UI, as elements are missing in Chrome.
3. Identify the FortiSIEM Collector to receive logs for that Organization (Tenant).
4. Perform Export Procedure Step 3 for that Collector.
5. Perform Export Procedure Step 4 with that Collector in the argument in the script. The Collector will assign the received logs to that Organization.
6. Confirm that the data is ingested as in Export Procedure Step 5.

Validating Events Ingested

When the export script has finished for a given time interval, it will print the total number of events that were processed **AND** a replication of the entire query that you can run in QRadar to compare the total events.

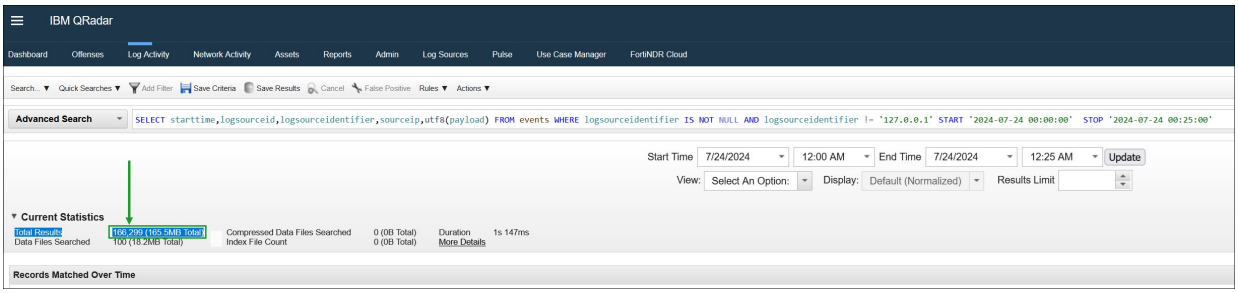
Example Script Output:

```
Script started at (UTC): 2024-07-25 22:30:41.764494+00:00

Script ended at (UTC): 2024-07-25 22:31:25.681156+00:00

Total execution time: 0:00:43.916662

Processed 166,299 events total, you can compare to the total result count returned by running the same query in QRadar

SELECT starttime,logsourceid,logsourceidentifier,sourceip,utf8(payload) FROM events WHERE logsourceidentifier IS NOT NULL AND logsourceidentifier != '127.0.0.1' START '2024-07-24 00:00:00' STOP '2024-07-24 00:10:00'
```

To compare, login to the QRadar Instance, navigate to Log Activity, and run the query that appeared at the end of the QRadar export. From our **Example Script Output** above, this query would be:

```
SELECT starttime,logsourceid,logsourceidentifier,sourceip,utf8(payload) FROM events
WHERE logsourceidentifier IS NOT NULL AND logsourceidentifier != '127.0.0.1' START
'2024-07-24 00:00:00' STOP '2024-07-24 00:10:00'
```

Notice the **Total Results** count in the screenshot, which should match the script output. In our example, the script output and query both display 166,299 events.



FortiEMS Endpoint Tagging

- Overview
- Updated Remediation Scripts
- Fortinet FortiEMS (Endpoint Management Server) Discovery Setup
- Best Practice Setup
- Scheduling Automatic Tagging Example

Overview

FortiSIEM now supports discovery of your FortiEMS servers using the FortiEMS Management Server API with basic authentication (username/password).

FortiSIEM will poll EMS, on a regular interval (default 5 min), and retrieve all vulnerabilities detected for managed FortiClient devices. FortiSIEM will send these as log events, which will create a CMDB entry for each device as unmanaged, if they don't already exist. You can then view vulnerability data about the FortiClient managed devices from the CMDB.

When FortiEMS discovery is done, FortiSIEM can tag or untag a host, using classification tags on FortiEMS server. In ZTNA, these tags are imported by member Fortinet devices, particularly FortiGate firewalls, and are referenced in ZTNA firewall rules.

A common use case would be tagging a host as suspicious, or potentially compromised, and having Firewall rules isolate or allow minimal network traffic for FortiClient managed devices that are assigned those tags.

Updated Remediation Scripts

FortiSIEM has updated several automated response (remediation) scripts to work with FortiEMS.

You can now, adhoc or via automation policy, execute a remediation script, via the **Incidents** page (From **Incidents**, select an incident and select **Remediate Incident** from the **Actions** drop-down list, and set/unset tag for the device in FortiEMS.) or **Analytics > Investigation** page.

This allows rules that have tags defined, to assign those tags to relevant hosts in the incident, that are also FortiClient managed devices.

The two primary remediation scripts are:

- Set tag for device in FortiEMS
- Unset tag for device in FortiEMS

Fortinet FortiEMS (Endpoint Management Server) Discovery Setup

To set up FortiEMS discovery, you will need to configure FortiEMS, then configure FortiSIEM.

Note: If you are just pulling in vulnerability data, you can just use a read-only user role. If you'd like to use FortiSIEM remediation scripts to set/unset EMS tags of FortiClient host devices, some write permissions are required.

- FortiEMS Configuration
- FortiSIEM Configuration

FortiEMS Configuration

Here, you will configure an admin role, and create an administrator user with the configured admin role. Take the following steps.

1. Login to FortiEMS Server.
2. Navigate to **Administration > Admin Roles**.
3. Click **Add**.
4. In the **Name** field, enter a name, such as "read_plus_tagging" (or your preferred role name).
   a. (Optional) In the **Description** field, enter a description, for example: "Used by FortiSIEM to ingest vulnerability data and create/set/unset EMS tags.".
   b. Under **Endpoint permissions**, select the following checkboxes.
      i. Block/Unblock/Quarantine/Unquarantine/Reregister endpoints
      ii. View group assignment rules
      iii. View endpoint filter bookmarks
      iv. View quarantine management
      v. View software inventory
   c. Under **Policy permissions**, select the following checkboxes.
      i. View endpoint policies
      ii. View endpoint profiles
      iii. View Zero Trust tagging rules
      iv. View installers
      v. View CA certificates
      vi. View on-fabric detection rules
   d. Under **Settings permissions**, select the following checkboxes.
      i. View EMS settings
      ii. View Fortinet services settings
      iii. View alert settings
      iv. View custom message settings
      v. View features select settings

   e. Click **Save**.
5. Navigate to **Administration > Administrators**.
6. Click **Add**.
7. In the **Add user** window, select **Create a new user**.
   a. In the **Username** field, enter a name, for example "fortisiem_user".
   b. From the **Role** drop-down list, select the role created, earlier - "read_plus_tagging".
   c. (optional) Toggle **Restrict Login to Trusted Hosts** on and add the IP of FortiSIEM component (IP of FortiSIEM node completing the discovery e.g. collector IP address).
   d. Click **Next**.
   e. In the **Password** and **Confirm Password** fields, enter a password that meets the FortiEMS requirements and click **Finish**.

FortiSIEM Configuration

With the FortiEMS admin user configured, you will set up FortiSIEM with the admin user credentials. Take the following steps.

1. Login to the FortiSIEM GUI.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the **Name** field, enter a credential, for example, "EMS_Server" (or your arbitrary name for the credential).
5. From the **Device Type** drop-down list, enter/select **Fortinet FortiClient EMS**.
6. Confirm **Access Protocol** is set to **FORTIEMS_API**. If not, select it.
7. Leave the **Pull Interval** at 5 minutes, or optionally change it to 1 minute to 24 hours (1440 minutes). 5 minutes is recommended.
8. Change the **Port** number if the admin port is different than the default 443.
9. In the **Serial Number** field, enter your serial number of your EMS server.
   Note: To get the EMS server serial number, login to your EMS server, navigate to **Dashboard > Status**. The serial number will appear next to **Serial Number**. The serial number is important for remediation script automation, discussed later.
10. In the **User Name** field, enter the FortiEMS admin username created earlier.
11. In the **Password** and **Confirm Password** fields, enter the password associated with the FortiEMS admin username.
12. Click **Save**.
13. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
14. In the **IP/Host Name** field, enter the IP address or hostname of the FortiEMS server.
15. From the **Credentials** drop-down list, select the EMS credential you just defined ("EMS_Server").
16. Click **Save**.
17. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results. Proceed to step 18 when connectivity succeeds.

18. Navigate to **ADMIN > Setup > Discovery** and click **New**.
    a. Enter the Name of the discovery entry.
    b. Select Discovery Type.
    c. Enter IP address or hostname of the FortiEMS server in the Include entry.
    d. Click **Save**.
19. Select the identified discovery, and click **Discover**.
20. Click the **Pull Events** tab at the top of the screen. A yellow star should appear next to your EMS server.
21. Wait approximately 5 minutes for the first job to start.
22. The Pull Events page will eventually show a green checkbox next to the EMS server job.
23. Navigate to **Analytics**, and confirm that EMS events are seen.

Best Practice Setup

The FortiEMS and the FortiGate firewall discoveries work in tandem to allow automatic tagging of devices via FortiSIEM triggering incidents.

The rough structure looks like this:

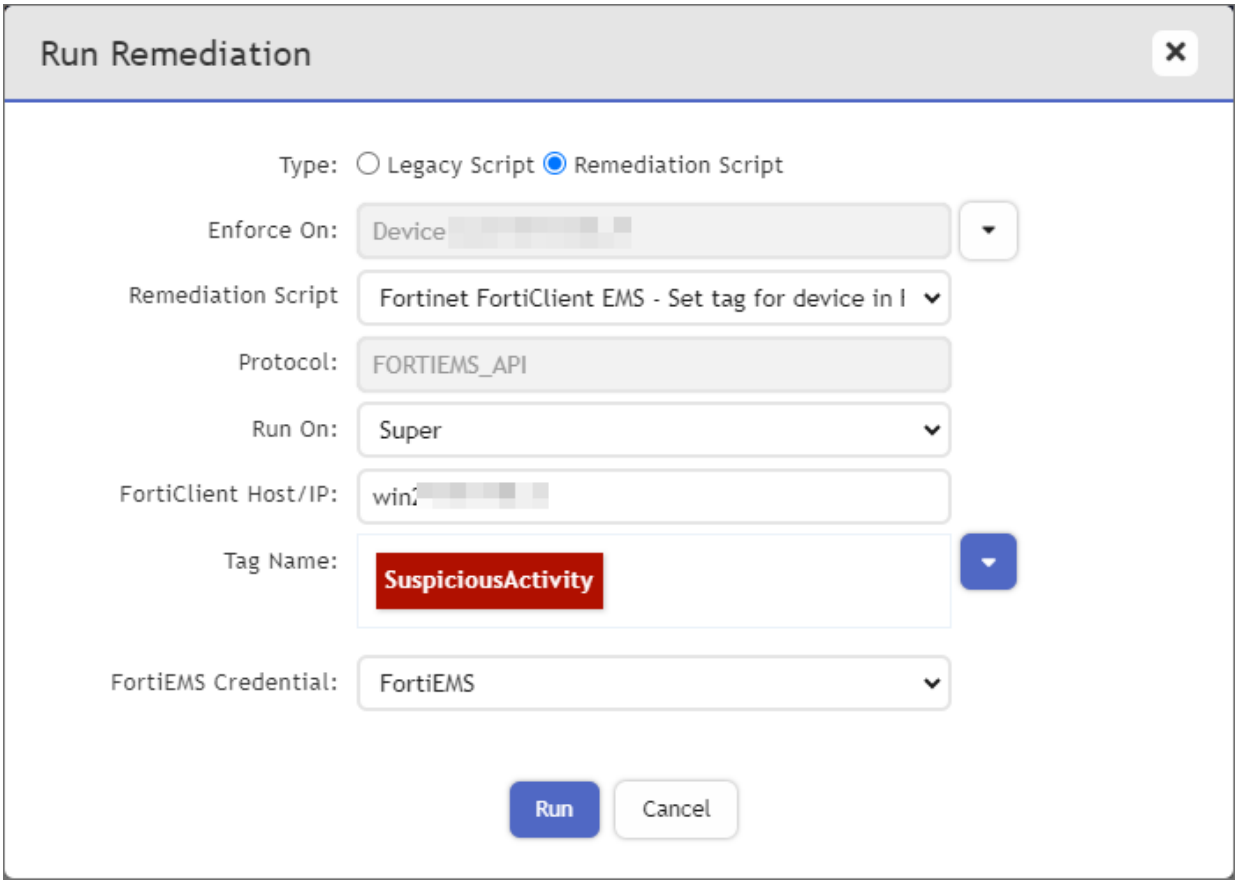
1. You configure your FortiGate firewalls for API discovery, and user device store observed FortiClient managed devices will be imported into FortiSIEM.
   Each of these devices is imported into FortiSIEM CMDB, each with a special attribute called the FortiEMS serial number, which is the EMS server identification that the device is registered to.
2. You configure your FortiEMS server credential in FortiSIEM. In the credential, you also hand define the FortiEMS serial number, along with the service user account to access FortiEMS.
3. You define a number of tags in FortiSIEM by navigating to **Admin > Settings > Analytics > Tags**, and clicking **New** to create a tag.
4. You edit any desired FortiSIEM rules by navigating to **Resources > Rules > <*selected rule*>**, and adding a tag by clicking **Edit**, navigating to **Step 3: Define Action**, selecting the tag from the **Tag** drop-down list, and clicking **Save**.
   Note: For System rules, you may have to clone the rule, disable the old system rule, and edit the cloned rule.
5. You create an automation policy that includes a remediation action when the given rule is triggered, in our example, we will use "Set tag for device in FortiEMS".
   a. Navigate to **Admin > Settings > General > Automation Policy**, and click **New**.
   b. From **Rules**, select the individual rule you have that contains uses of the tag you defined.
   c. From **Affected Orgs**, select the affected organizations, if any.
   d. Next to **Run Remediation / Script**, click the Edit icon (pencil), then click **New**.
      i. For **Type**, select **Remediation Script**.
      ii. From the **Script** drop-down list, select **Fortinet FortiClient EMS - Set tag for device in FortiEMS**.
      iii. Leave **Enforce On** blank.

iv. From the **Run On** drop-down list, select the target collector that you would like to execute the script from. Remember that if you have IP restrictions on user accounts, you must make sure that the node calling the API is allowed.
v. Leave the **Tag Name** drop-down list alone to allow auto selection, or select a tag to force a particular tag be used.
vi. Leave the **FortiEMS Credential** drop-down list alone to allow auto selection, or select which FortiEMS server to execute the script against.
vii. Click **Save**.

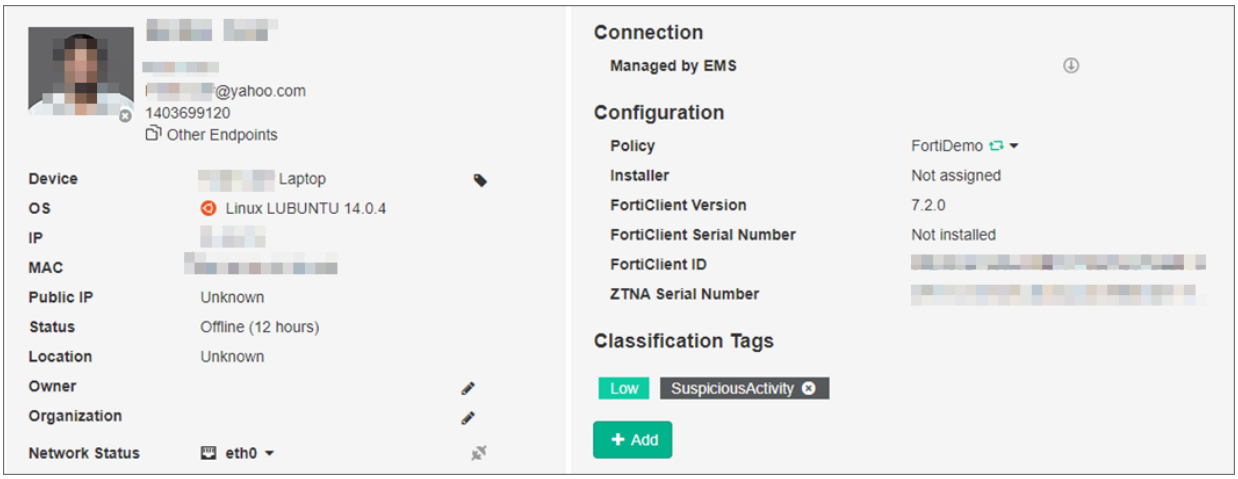
e. Ensure that the **Run Remediation/Script** checkbox is now checked.
f. Click **Save**.

You can tag FortiClient hosts by IP or Hostname using remediation scripts adhoc via the **Incidents** page, by taking the following steps.

1. Navigate to **Incidents**.
2. Select an incident.
3. Click the **Actions** drop-down list and select **Remediate Incident**.
4. Set/Unset the tag for the device in FortiEMS.



When tagged, the laptop from the screenshot example above now has the additional classification tag in the FortiEMS server below, as shown in the below screenshot:



Additional Information on Automatically Tagging a Host

When an incident triggers, and a matching automation policy action exists (in our case, Run Remediation Script), FortiSIEM must dynamically determine what to do.

In the context of tagging a host running FortiClient with a new tag in FortiEMS, it must determine the following based on the incident data.

1. Which host to tag
2. What tag to use
3. Which FortiEMS credential (which EMS server and authentication) to use.

FortiSIEM can only automatically do all 3 if you've followed the best practices above.

1. Which host to tag
   FortiSIEM looks at the incident source (either hostname or IP address), and if a value can be found, it checks if this device exists in the CMDB.
   If it exists in CMDB, it looks at the device's FortiEMS serial number attribute.
   If incident source is not found, it looks at incident destination (either hostname or IP address). It also checks if the device exists in CMDB and whether it has a FortiEMS serial number attribute.
2. What tag to use
   If the rule contains a tag value, it will read this.
   If the remediation script is executed adhoc by user, you can override this with your own.
3. Which FortiEMS credential (which FortiEMS server and authentication) to use.
   FortiSIEM lists all available FortiEMS Server credentials. Each has an associated serial number attribute.
   If the matching CMDB device found in the incident has a FortiEMS serial number match (This indicates the FortiEMS server it is registered to), it will use the associated credential.

Note: If a user is adhoc executing a FortiEMS remediation script (not automatically), then you can forcefully override the automatically detected host, tag, and credential to use.

Example Scenario

The rule "Traffic to FortiGuard Malware IP List" triggered for a given source device. This source is a Windows machine running FortiClient. This device was previously shallow discovered as unmanaged via a FortiGate firewall. Using this method, we know the FortiEMS serial number of the FortiEMS server it is registered to.

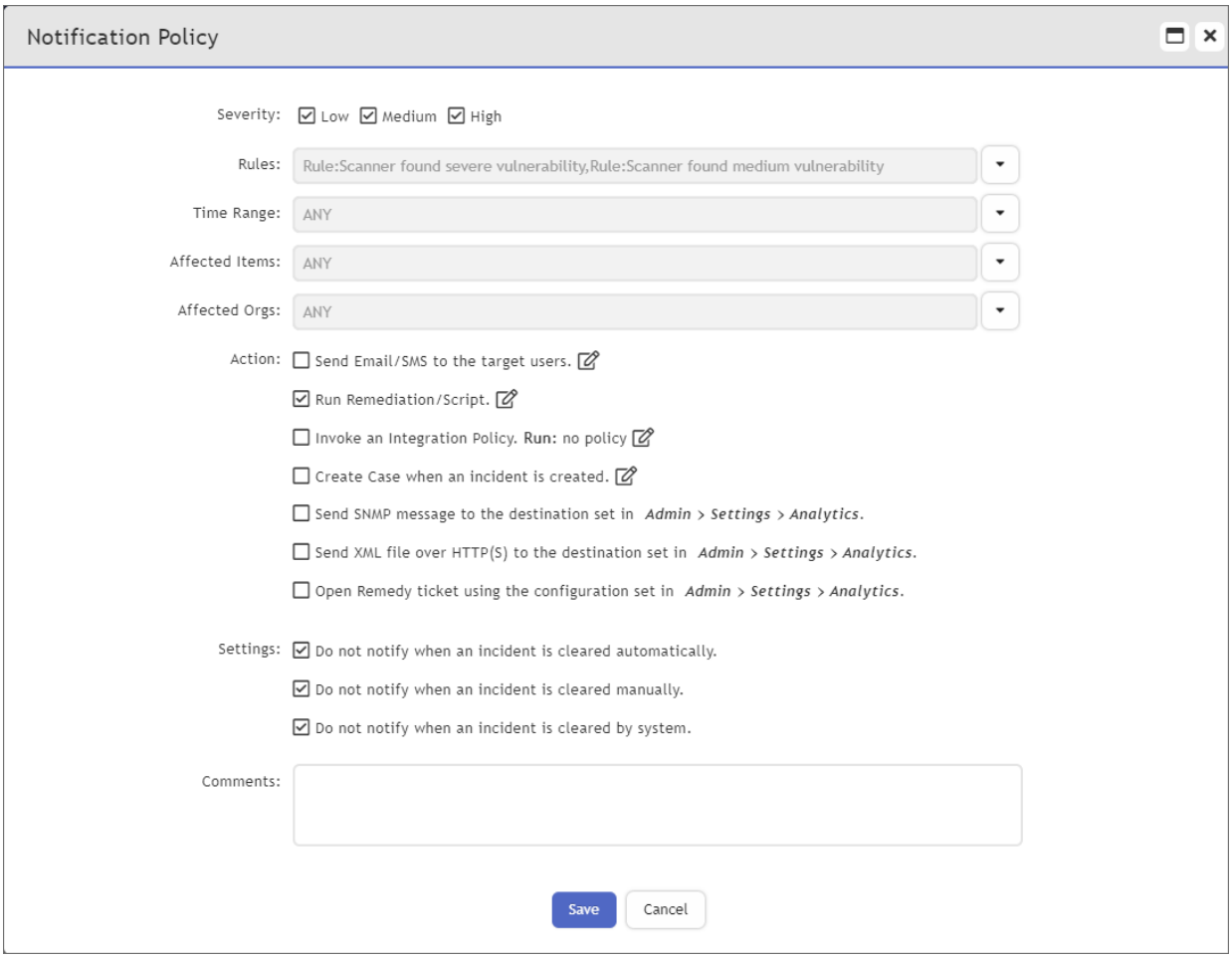
We can assign a tag, either within the rule, or during adhoc execution, such as "suspicious_activity", which will be assigned to the host in FortiEMS. Devices such as Firewalls that implement ZTNA policies based on this tag will take action according to how they are defined.

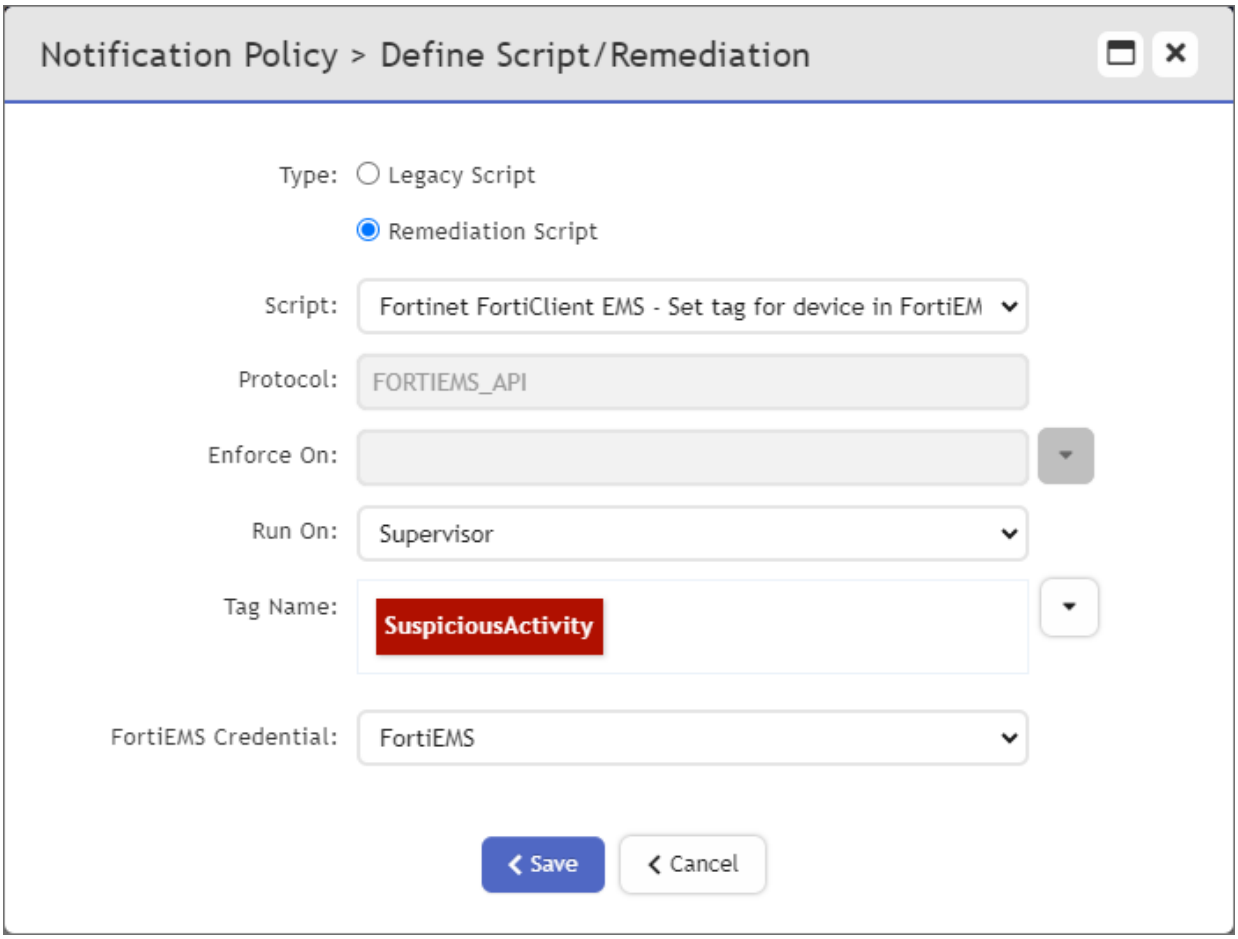
Action overview: FortiSIEM (tag a host) -> FortiEMS server -> Feed hosts and tag data -> FortiGate firewalls -> Implement ZTNA rules based on certain tags -> Take action if matching devices pass through Firewall.

Scheduling Automatic Tagging Example

You can schedule tagging for certain rules via Automation Policy, see here for more information. Two example screenshots below provide an illustration of the following:

If any of the 3 rules selected trigger, FortiSIEM will automatically check the incident source or incident target and if the device exists in the FortiEMS server, it will be tagged with the tag "SuspiciousActivity".


Notification Policy
Severity: Low Medium High
Rules: Rule:Scanner found severe vulnerability,Rule:Scanner found medium vulnerability
Time Range: ANY
Affected Items: ANY
Affected Orgs: ANY
Action: Send Email/SMS to the target users.
Run Remediation/Script.
Invoke an Integration Policy. Run: no policy
Create Case when an incident is created.
Send SNMP message to the destination set in Admin > Settings > Analytics.
Send XML file over HTTP(S) to the destination set in Admin > Settings > Analytics.
Open Remedy ticket using the configuration set in Admin > Settings > Analytics.
Settings: Do not notify when an incident is cleared automatically.
Do not notify when an incident is cleared manually.
Do not notify when an incident is cleared by system.
Comments:
Save
Cancel


Notification Policy > Define Script/Remediation
Type:
Legacy Script
Remediation Script
Script:
Fortinet FortiClient EMS - Set tag for device in FortiEM
Protocol:
FORTIEMS_API
Enforce On:
Run On:
Supervisor
Tag Name:
SuspiciousActivity
FortiEMS Credential:
FortiEMS
Save
Cancel

GUI Notes

- Flash to HTML GUI Mapping
- FortiSIEM Charts and Maps

Flash to HTML5 GUI Mapping

This section describes the mapping between FortiSIEM Flash-based GUI (available for all AccelOps and FortiSIEM versions up to 5.0.0) and FortiSIEM HTML5-based GUI (available from FortiSIEM version 5.0.0). This mapping enables you to familiarize with AccelOps/FortiSIEM Flash-based GUI to quickly find the corresponding functions in FortiSIEM HTML5-based GUI.

FortiSIEM HTML5-based GUI is similar to the earlier Flash-based GUI. In addition to the Dashboard, Analytics, Incidents, CMDB and Admin tabs from Flash-based GUI, the HTML5-based GUI adds two new tabs - CASES and RESOURCES.

The following tables show the mapping for each tab.

Dashboard

Flash Element	HTML5 Element
Executive Summary	DASHBOARD > Network Dashboard > Summary DASHBOARD > Server Dashboard > Summary DASHBOARD > Storage Dashboard > Summary
Incident Dashboard > Table View	INCIDENTS > List View
Incident Dashboard > Fishbone View	*Currently not available*
Incident Dashboard > Topological View	*Currently not available*
Incident Dashboard > Calendar View	*Currently not available*
Incident Dashboard > Location View	INCIDENTS > List View > Action > Locations
My Dashboard	DASHBOARD > New Dashboard (can be imported)
Summary Dashboard > Biz Service Summary	DASHBOARD > Click **+** to add new Dashboard and choose **Type** as 'Business Service Dashboard'.
Summary Dashboard > All Device	DASHBOARD > Network Dashboard > Summary DASHBOARD > Server Dashboard > Summary DASHBOARD > Storage Dashboard > Summary
Summary Dashboard > Network Device	DASHBOARD > Network Dashboard > Summary
Summary Dashboard > Servers	DASHBOARD > Server Dashboard > Summary

Flash Element	HTML5 Element
Summary Dashboard > EC2 Systems	DASHBOARD > Amazon Web Services Dashboard > Summary
Summary Dashboard > Azure Systems	*Currently not available as built-in (user can create their own)*
Summary Dashboard > All VMs	DASHBOARD > VMWare Dashboard > VM DASHBOARD > VMWare Dashboard > ESX
Summary Dashboard > My Devices	DASHBOARD > Any customized summary dashboard can be used to manage devices.
Availability / Performance > Hardware Summary	DASHBOARD > Network Dashboard > Hardware DASHBOARD > Server Dashboard > Hardware
Storage	DASHBOARD > NetApp Dashboard DASHBOARD > VNX Dashboard
Top Monitored Processes	*Currently not available*
Apache Servers	DASHBOARD > Web Server Dashboard
Exchange Servers	*Currently not available as built-in (user can create their own)*
Windows DHCP	*Currently not available as built-in (user can create their own)*
Windows DNS	*Currently not available as built-in (user can create their own)*
IIS Servers	DASHBOARD > Web Server Dashboard
ASP.NET Servers	*Currently not available*
MS Active Directory Servers	*Currently not available*
MS SQL Servers	DASHBOARD > Database Dashboard
Oracle DB Servers	DASHBOARD > Database Dashboard
MySQL Servers	DASHBOARD > Database Dashboard
VoIP Summary	*Currently not available as built-in (user can create their own)*
IPSLA Summary	*Currently not available as built-in (user can create their own)*
STM Summary	*Currently not available as built-in (user can create their own)*
Environmental Dashboard	*Currently not available as built-in (user can create their own)*

Flash Element	HTML5 Element
Dashboard By Function > Network > Generic	DASHBOARD > Network Dashboard > Availability DASHBOARD > Network Dashboard > Performance DASHBOARD > Network Dashboard > Login/Change DASHBOARD > Network Dashboard > Change
Dashboard By Function > Network > Netflow	DASHBOARD > Network Dashboard > Netflow
Dashboard By Function > Network > VoIP	DASHBOARD > Network Dashboard > VoIP
Dashboard By Function > Network > IPSLA	DASHBOARD > Network Dashboard > IPSLA
Dashboard By Function > Server	DASHBOARD > Server Dashboard
Dashboard By Function > Virtualization	DASHBOARD > VMWare Dashboard
Dashboard By Function > Application > Generic	DASHBOARD > Server Dashboard > Availability DASHBOARD > Server Dashboard > Performance
Dashboard By Function > Application > Mail	*Currently not available as built-in (user can create their own)*
Dashboard By Function > Application > Database	*Currently not available as built-in (user can create their own)*
Dashboard By Function > Application > Web	DASHBOARD > Web Server Dashboard
Dashboard By Function > Storage	DASHBOARD > NetApp Dashboard DASHBOARD > VNX Dashboard
Dashboard By Function > Environment	*Currently not available as built-in (user can create their own)*
Dashboard By Function > Event/Log Mgmt	DASHBOARD > FortiSIEM Dashboard
Dashboard By Function > Fortinet Security Fabric	DASHBOARD > Fortinet Security Fabric

Analytics

Flash Element	HTML5 Element
Real Time Search	ANALYTICS
Historical Search	ANALYTICS
Reports	RESOURCES > Reports
Generated Reports	ANALYTICS >
Identity and Location Report	DASHBOARD > Click **+** to add new Dashboard and choose **Type** as 'Identity and Location Dashboard'.
Rules	RESOURCES > Rules
Audit	*Currently not available*
Incident Automation Policy	ADMIN > Settings > General > Automation
Remediations	RESOURCES > Remediations
Display Column Sets	*Currently not available*
Filter Column Sets	*Currently not available*

Incidents

Flash Element	HTML5 Element
Incidents	INCIDENTS > List View
Tickets	CASE
IPS Vulnerability Map	*Currently not available*

CMDB

Flash Element	HTML5 Element
Topology	*Currently not available*
Devices	CMDB > Devices
Applications	CMDB > Applications
Users	CMDB > Users
Business Services	CMDB > Business Services
Networks	RESOURCES > Networks
Watch Lists	RESOURCES > Watch Lists
Protocols	RESOURCES > Protocols
Event Types	RESOURCES > Event Types
Malware Domains	RESOURCES > Malware Domains
Malware IP	RESOURCES > Malware IPs
Malware URLs	RESOURCES > Malware URLs
Malware Processes	RESOURCES > Malware Processes
CMDB Reports	CMDB > CMDB Reports
Country Groups	RESOURCES > Country Groups
Malware Hash	RESOURCES > Malware Hash
Default Password	RESOURCES > Default Password
Anonymity Networks	RESOURCES > Anonymity Networks
User Agents	RESOURCES > User Agents

Admin

Flash Element	HTML5 Element
Admin > Startup	*Not available*
Admin > Setup Wizard > Organizations	ADMIN > Setup > Organizations

Flash Element	HTML5 Element
Admin > Setup Wizard > Windows Agents	ADMIN > Setup > Windows Agents
Admin > Setup Wizard > Credentials	ADMIN > Setup > Credentials
Admin > Setup Wizard > Discovery	ADMIN > Setup > Discovery
Admin > Setup Wizard > Pull Events	ADMIN > Setup > Pull Events
Admin > Setup Wizard > Monitor Change/Performance	ADMIN > Setup > Monitor Performance
Admin > Setup Wizard > Synthetic Transaction Monitoring	ADMIN > Setup > STM
Admin > Device Support > Device/App Types	ADMIN > Device Support > Device/App
Admin > Device Support > Event Attribute Types	ADMIN > Device Support > Event Attribute
Admin > Device Support > Event Types	ADMIN > Device Support > Event
Admin > Device Support > Parsers	ADMIN > Device Support > Parser
Admin > Device Support > Performance Monitoring	ADMIN > Device Support > Monitoring
Admin > Device Support > Custom Properties	ADMIN > Device Support > Custom Property
Admin > Device Support > Dashboard Columns	*Currently not available*
Admin > Collector Health	ADMIN > Health > Collector Health
Admin > Cloud Health	ADMIN > Health > Cloud Health
Admin > Elasticsearch health	ADMIN > Health > Elasticsearch health
Admin > General Settings > System	ADMIN > Settings > System
Admin > General Settings > Analytics	ADMIN > Settings > Analytics
Admin > General Settings > Discovery	ADMIN > Settings > Discovery
Admin > General Settings > Monitoring	ADMIN > Settings > Monitoring
Admin > General Settings > UI	ADMIN > Settings > System > UI
Admin > General Settings > Email Template	ADMIN > Settings > System > Email
Admin > General Settings > Event Handling	ADMIN > Settings > Event Handling
Admin > General Settings > Kafka Config	ADMIN > Settings >System > Kafka
Admin > General Settings > External Authentication	ADMIN > Settings > General > Authentication

Flash Element	HTML5 Element
Admin > General Settings > Integration	ADMIN > Settings > General > Integration
Admin > General Settings > External Lookup	ADMIN > Settings > System > Lookup
Admin > General Settings > Escalation Policy	ADMIN > Settings > General > Escalation
Admin > Discovery Results	ADMIN > Setup > Discovery > History
Admin > License Management	ADMIN > License > License
Admin > Usage Information	ADMIN > License > Usage
Admin > Role Management	ADMIN > Settings > Role
Admin > Maintenance Calendar	ADMIN > Setup > Maintenance
Admin > Event DB Management	*Currently not available*
Admin > Data Update	ADMIN > Data Update

FortiSIEM Charts and Views

FortiSIEM provides a variety of charts and maps to better help you understand and analyze your incident data. You can access these charts and views from the widget dashboard settings (see Modifying widget information display) or by clicking the **TABLE** or drop-down icon in the ANALYTICS page (see Viewing Historical Search Results).

Chart/View	Description	Display Settings	Requirements
Table	Displays data in a tabular format.	You can choose to display the bar chart (**Show Bar**), the event type (**Show Event Type**), and the count (**Count**). Set the colors for the bar chart or reverse the color map.	None
Link Graph	Displays source, event, and destination relationships. Source nodes appear in light blue, Event nodes are color coded by their severity if event attribute "Event Severity Category" exists in the Display Fields on Table view. A node can be clicked and dragged to be repositioned. If a node can be represented by a recognizable device type from FortiSIEM, the appropriate icon will be displayed, otherwise a default monitor icon will appear. The Rows and Total number represent the number of data items in the table view, not the number of nodes. For example, one representation will consist of 3 nodes (source, event, destination), but if all the data items share the same source, event, and destination, only three nodes will appear. Click on any node and the following options appear: • Quick Info - Select to show more information about the selected node. • Add <*object*> to Filter - Adds the data from the selected node to a filter.	Select the **Source**, **Event**, and **Destination** from the drop - down lists. Auto Layout attempts to show all nodes in an optimal manner. To disable, deselect the **Auto Layout** checkbox.	A source and destination are required.

Chart/View	Description	Display Settings	Requirements
Bar Chart	Displays data similar to a bar chart.	Select the Aggregate Field (**Column**) to display and their colors. You can also reverse the color map.	At least one numeric column is required.
Chord Chart	A graphical method of displaying the inter-relationships between data in a matrix. The data is arranged radially around a circle with the relationships between the data points typically drawn as arcs connecting the data.	Select the incident **Source**, **Target**, and **Value** from the drop-down lists.	At least two key columns and one numeric column are required.
Choropleth Chart	A thematic map in which areas are shaded or patterned in proportion to the measurement of the statistical variable being displayed on the map.	Select the **Location** and **Value** from the drop-down lists.	At least one numeric column is required. Configure **Google Maps API Key** in **ADMIN > Settings > System > UI** See UI Settings.
Cluster Bubble Chart	You can use a bubble chart instead of a scatter chart if your data has three data series that each contain a set of values. The sizes of the bubbles are determined by the values in the third data series.	Select the **Column** from the drop-down list.	At least one numeric column is required.
Donut Chart	Displays data similar to a pie chart.	Select the Aggregate Field (**Column**) to display since the report may have multiple Aggregate Fields.	At least one numeric column is required.

Chart/View	Description	Display Settings	Requirements
GEO Map Chart	Displays the IP addresses in a geographic map.	Public or private IP addresses with location defined in **ADMIN > Settings > Discovery > Location**. See Setting Location.	At least one numeric column is required.
Heat Map Chart	Displays two event attributes and a numerical aggregate value.	Select the Heat map coordinates **X** and **Y**, and an associated **Value**.	At least two key columns and one numeric column are required.
Sankey Chart	A specific type of flow diagram, in which the width of the arrows is shown proportionally to the flow quantity.	Select the **Source**, **Target**, and **Value** from the drop-down lists.	At least two key columns and one numeric column are required.
Scatter Plot Chart	Plots two aggregate fields.	Select two aggregate fields, **X** and **Y**. Select the **Size** of the sample.	At least two numeric columns are required.
Sunburst Chart	Visualizes hierarchical data, depicted by concentric circles. The circle in the center represents the root node, with the hierarchy moving outward from the center.	Select the **Rank1**, **Rank2**, **Rank3** and **Count** from the drop-down lists.	Only one column can be used in one rank.
Tree Map Chart	Displays columns in a Tree Map.	Select the Tree Map **Ranks** and the **Count** attributes from the drop-down lists.	Only one column can be used in one rank.
Trend Line Chart	A "trend" line is superimposed on a chart that reveals the overall direction of the data.		
Trend Area Chart	A graph that shows trend changes over time, by displaying a series of data as different colored lines.		

Chart/View	Description	Display Settings	Requirements
Trend Bar Chart	Uses bars to track trends over time.		

FortiSOAR Integration Notes

For additional information on the FortiSOAR for FortiSIEM Integration solution, see here.

Sample playbooks are available here.

- Configuring FortiSOAR for FortiSIEM Integration
- Writing FortiSIEM Compatible FortiSOAR Playbooks

Configuring FortiSOAR for FortiSIEM Integration

To set up FortiSOAR with a role so FortiSIEM integration can occur, take the following steps.

Set Up Authentication

HTTP Basic Authentication for API is used for authentication. A user that FortiSIEM can use to read, execute playbooks and connectors can be created by taking the following steps.

1. Click the Setting icon on top right hand of the FortiSOAR GUI.
2. Select **Roles** on left hand toolbar.
3. Click **Add**.
4. Give the Role a Name. For example, "FortiSIEM-Role".
5. In **Set Role Permissions**, set the following:
   a. For All Modules Except for Users, set to **Read allow**.
   b. Set Connectors to **Read + Execute**.
   c. Set Playbooks to **Read + Execute**.
   d. Click **Save**.
6. Select **Users** on left hand toolbar.
7. Click **Add**.
8. Set the following:
   a. Fill out the **First Name** and **Last Name** fields, such as First Name "FortiSIEM", and "Last Name" User".
   b. For **User Type**, select **Vendor**.
   c. Enter a valid email address, such as *yourname@yourdomain.tld*.
   d. Select your **Desired Team**.
   Note: You must assign the user to a Team in addition to a Role, otherwise authentication for executing playbooks will fail.
   e. For **Select Role**, you can select FortiSIEM-Role for minimal access, or a desired Role.
   f. Under **Authentication**, for **User Type**, select **Application User**.
   g. Under **Authentication**, specify the username. Note, it can be different from the Name display value: fortisiem-user.
   h. Click **Save**. An email will be sent to the email address provided to change the password.
   i. Keep a record of the changed password.

   At this point, you can configure FortiSIEM for FortiSOAR Playbooks and FortiSOAR Connectors.

For additional information on the FortiSOAR for FortiSIEM Integration solution, see here.

Sample playbooks are available here. This contains:

- Playbook for getting IP address reputation via VirusTotal
- Playbook for getting Domain reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid, Alienvault OTX
- Playbook for getting URL reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid
- Playbook for getting file hash reputation via VirusTotal

Writing FortiSIEM Compatible FortiSOAR Playbooks

Introduction

Starting with 6.4.0, FortiSIEM provides the capability to adhoc execute FortiSOAR Playbooks and Connectors from the **INCIDENTS** page for individual incidents, or from the **ANALYTICS** page for individual events.

When FortiSIEM executes a Playbook, it provides the entire set of incident or raw event data , depending on execution from the **INCIDENTS** or **ANALYTICS** page respectively, as an argument to the Playbook in JSON format. The Playbook operates on that data, execute some actions, and returns the result to FortiSIEM.

For additional information on the FortiSOAR for FortiSIEM Integration solution, see here.

Sample playbooks are available here. This contains:

- Playbook for getting IP address reputation via VirusTotal
- Playbook for getting Domain reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid, Alienvault OTX
- Playbook for getting URL reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid
- Playbook for getting file hash reputation via VirusTotal

Prerequisites

In order to better understand the information here, it is recommended that you read the latest reference FortiSOAR **Playbooks Guide** under **Reference Manuals** first located here.

FortiSOAR Playbooks heavily use Jinja Templates. It is imperative that the Jinja template syntax is understood to design useful Playbooks. Jinja template designer documentation can be referenced here: https://jinja.palletsprojects.com/en/3.0.x/templates/

Playbooks and Connectors

A Playbook in FortiSOAR is a workflow that can be executed manually or automatically to complete some action within FortiSOAR itself, or to systems and applications in your environment. Playbooks can do entire chains of actions, while Connectors complete just one action at a time.

A Connector in FortiSOAR is an individual component integration to various FortiSOAR supported products. Playbooks can call multiple Connectors to create complex tasks. Every Connector can support one or more actions.

For example the Fortinet – FortiOS Connector can do the following actions on a FortiGate firewall, and return the response data to you:

- Get Policy
- Get Address Group
- Get Blocked IP Addresses
- Get Blocked URLs
- Get Web Filter Profiles
- Block IP Address
- Block URL
- Unblock URL
- Unblock IP Address
- Purge IP Block List
- Execute Command

You can adhoc execute a Connector from FortiSIEM, supplying the necessary arguments for any given action. The arguments required vary based on the action being completed.

Some examples of a Playbook with respect to FortiSIEM:

- An incident triggers in FortiSIEM, and you would like FortiSOAR to take that incident data, and do a reputation lookup of all the public IPs found in that incident.
- An incident triggers in FortiSIEM, and you would like FortiSOAR to generate an Alert on FortiSOAR, and block the source IP found in the incident on a specific firewall in your network for 24 hours.
- A raw event is observed in FortiSIEM on the **ANALYTICS** page by a security analyst, who decides to execute a Playbook that takes the following actions:
  - Disables the user observed in the event in Active Directory.
    and
  - Sends an email to the security team.

Some examples of a Connector execution from FortiSIEM:

- A security analyst observes a malicious IP in an incident, and executes a connector to block the IP on a firewall as a singular action.
- A security analyst observes suspicious behavior from a given user account in Active Directory, and executes the **Active Directory > Disable User Account** action on the account until further inspection can be completed.

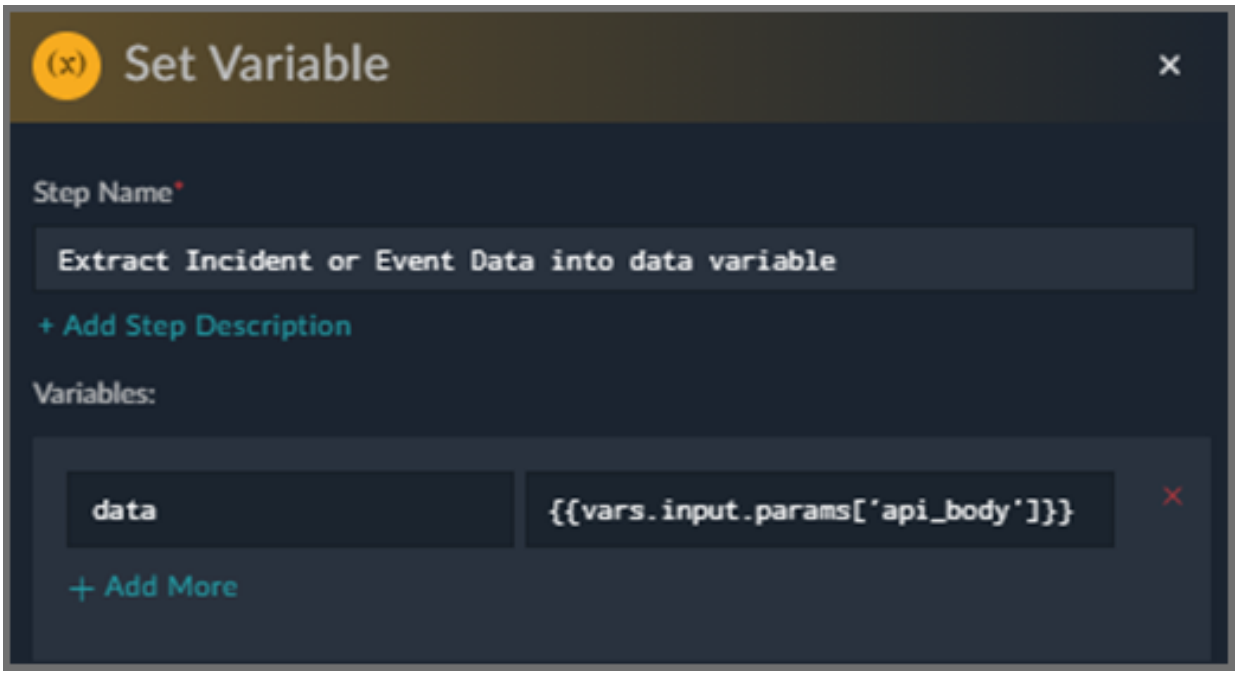
Jinja and its Use in Playbooks

Jinja is a templating engine that can be used to build complex documents dynamically. FortiSOAR uses this in their Playbook design interface so you can process variable data sent to or from various functions, utilities, or connectors.

There are a few kinds of delimiters. The default Jinja delimiters are configured as follows:

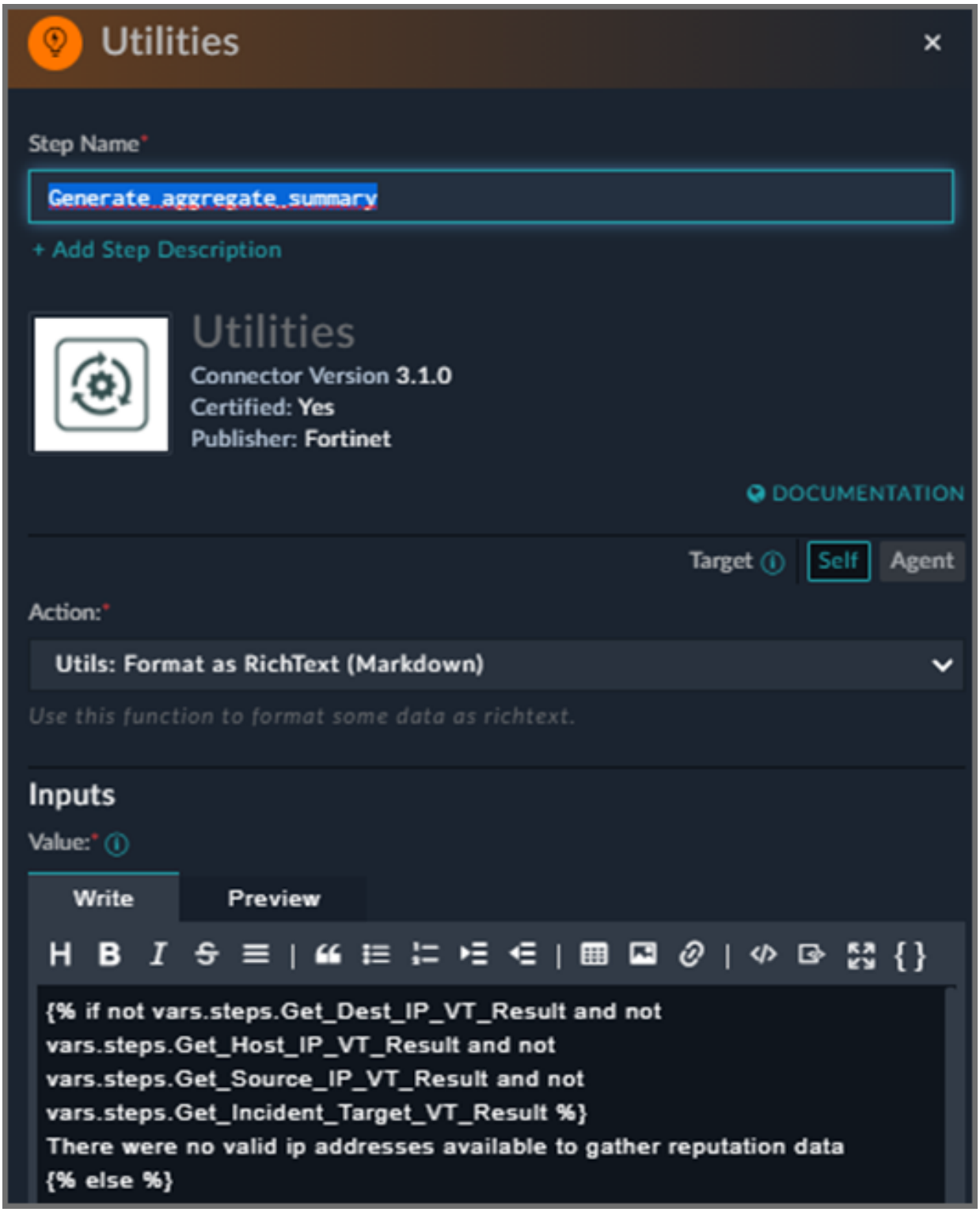
- {% ... %} for Statements
- {{ ... }} for Expressions to print to the template output
- {# ... #} for Comments not included in the template output

For example, in a FortiSOAR Playbook, the Set Variable Action can use the {{…}} expression to assign the FortiSIEM JSON data into a list variable called data.



For another example, using the step function Utility -> Format as RichText (Markdown), you can format a variable as a string of text, but use statements to only display text if certain conditions match.

The example here will only display the string “There were no valid ip addresses available to gather reputation data” if the following variables do not exist:



If the 4 variables named above do not exist, a single line of text explains no result data was found, otherwise the rest of the data after the `{% else %}` statement is processed.

Building Custom Playbooks

With Playbooks you can build anything you like to complete any action.

As FortiSIEM incidents are generated, or raw events are parsed from various products, they each provide concrete sets of data to act on, either completing enrichment (looking up reputations), or taking some action such as disabling a user.

FortiSIEM sends this data over to a given Playbook in JSON format.

The FortiSIEM incident is in the following JSON format when supplied to a Playbook. The playbook can access argument data from FortiSIEM in the JSON variable `{{vars.input.params['api_body']}}`

Sample Incident JSON


```
{
	"user": null,
	"count": 30,
	"srcName": null,
	"tagName": null,
	"customer": null,
	"destName": null,
	"hostName": null,
	"phCustId": 1,
	"procName": null,
	"resource": null,
	"eventName": null,
	"eventType": "PH_RULE_DNS_THREATSTREAM_MALWARE_DOMAIN",
	"srcGeoOrg": null,
	"srcIpAddr": "192.0.2.0",
	"bizService": null,
	"destGeoOrg": null,
	"destIpAddr": null,
	"hostGeoOrg": null,
	"hostIpAddr": null,
	"incidentId": 993,
	"phRecvTime": 1634249820000,
	"reptGeoOrg": null,
	"srcGeoCity": null,
	"destGeoCity": null,
	"hostGeoCity": null,
	"incidentSrc": "srcIpAddr:192.0.2.0,",
	"rawEventMsg": null,
	"reptGeoCity": null,
	"srcGeoState": null,
	"activityName": null,
	"attackTactic": "Exfiltration",
	"destGeoState": null,
	"hostGeoState": null,
```

```
      "incidentReso": 1,
      "reptGeoState": null,
      "eventSeverity": 9,
      "incidentCount": 30,
      "incidentRptIp": "198.51.100.0",
      "incidentTitle": "DNS Traffic from 192.0.2.0 to Threat Stream Malware Domain
example.net",
      "srcGeoCountry": null,
      "destGeoCountry": null,
      "hostGeoCountry": null,
      "incidentDetail": "",
      "incidentStatus": 0,
      "incidentTarget": "destName:example.net,",
      "reptGeoCountry": null,
      "srcGeoLatitude": null,
      "attackTechnique": "[{\"name\":\"Exfiltration Over Alternative Protocol: Exfiltration
Over Symmetric Encrypted Non-C2 Protocol\",\"techniqueid\":\"T1048.001\"}]",
      "destGeoLatitude": null,
      "hostGeoLatitude": null,
      "incidentExtUser": null,
      "incidentTagName": null,
      "phEventCategory": 1,
      "reptGeoLatitude": null,
      "srcGeoLongitude": null,
      "destGeoLongitude": null,
      "eventSeverityCat": "HIGH",
      "hostGeoLongitude": null,
      "incidentComments": "test comment\n\n",
      "incidentLastSeen": 1634249820000,
      "incidentTicketId": null,
      "reptGeoLongitude": null,
      "attackTechniqueId": "T1048.001",
      "incidentFirstSeen": 1627508130000,
      "incidentNotiStatus": null,
      "incidentRptDevName": "HOST-198.51.100.0",
      "incidentTicketUser": null,
      "incidentViewStatus": 1,
      "phIncidentCategory": null,
      "incidentClearedTime": 0,
      "incidentClearedUser": null,
      "incidentExtTicketId": null,
      "incidentRptDevStatus": 1,
      "incidentTicketStatus": 6,
      "incidentClearedReason": null,
      "incidentExtTicketType": null,
      "phSubIncidentCategory": null,
      "incidentExtClearedTime": null,
      "incidentExtTicketState": null,
      "incidentNotiRecipients": ""
    }
```

Please note that depending on the type of FortiSIEM incident that fired, and the data used to populate that incident, the fields will contain various values. Your playbook must properly handle situations such as a field you need is blank, or properly extract data from a field that contains multiple values.

Similar to FortiSIEM Incidents, when executing a playbook on a FortiSIEM raw event, an entire copy of the parsed event attributes for that event is sent in JSON format, which looks like the following.

Sample Event JSON


```
{
    "count": "1",
    "opName": "New-InboxRule",
    "status": "True",
    "userId": "test.user@example.com",
    "eventId": "8263823841277690829",
    "srcName": "HOST-192.0.2.22",
    "customer": "Super",
    "phCustId": 1,
    "ruleName": "For all messages from test@email.com",
    "eventName": "create Inbox rules in mailboxes. Inbox rules process messages in the
Inbox based on conditions and take actions such as moving a message to a specified folder
or deleting a message",
    "eventType": "MS_OFFICE365_Exchange_New-InboxRule",
    "reptModel": "Office365",
    "srcIpAddr": "203.0.113.0",
    "srcIpPort": 11022,
    "deviceTime": 1624869759000,
    "parserName": "Office365Parser",
    "phRecvTime": 1635195584000,
    "reptVendor": "Microsoft",
    "srcGeoCity": "Cheshunt",
    "collectorId": "1",
    "eventSource": "Exchange",
    "reptDevName": "HOST-198.51.100.24",
    "srcGeoState": "England",
    "timeSkewSec": "10325825",
    "eventParsedOk": 1,
    "eventSeverity": 7,
    "reptDevIpAddr": "198.51.100.24",
    "srcGeoCountry": "United Kingdom of Great Britain and Northern Ireland",
    "relayDevIpAddr": "198.51.100.24",
    "senderMailAddr": "nobody@example.com",
    "srcGeoLatitude": "51.69989",
    "phEventCategory": "0 (External)",
    "srcGeoLongitude": "-0.02849",
    "eventRuleTrigger": 1,
    "eventSeverityCat": "MEDIUM",
    "extEventRecvProto": "Syslog",
    "office365UserType": "2 (An administrator)",
    "office365RecordType": "1 (ExchangeAdmin - Events from the Exchange admin audit log)",
```

```
    "stopProcessingRules": "True",
    "srcGeoCountryCodeStr": "GB"
  }
```

Please also note that the contents in the event will vary based on the source. The fields present in a Firewall session log are not the same as a Windows login event, and certain attributes are not guaranteed to always be present, which is vendor dependent. Your Playbooks should properly handle edge cases where expected values are not present when the Playbook is called.

When a Playbook is executed, the FortiSIEM argument data is accessible in the following variable:

```
{{vars.input.params['api_body']}}
```

You are then free to parse that JSON data into its individual attributes to complete an action. These attribute names in the JSON match the programmatic attribute names in FortiSIEM. These can be observed in the FortiSIEM UI by navigating to **ADMIN > Device Support > Event Attributes**.

Below are some common attributes.

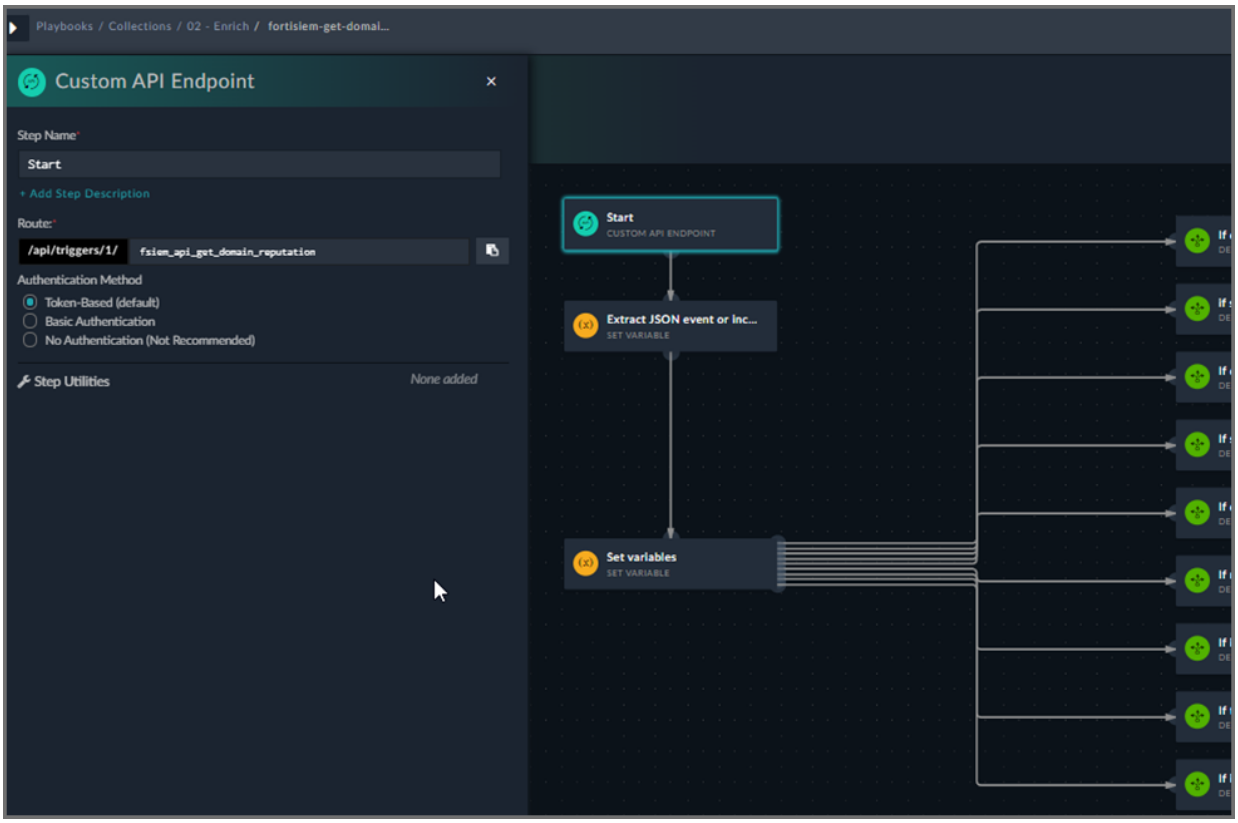
Sample Attribute Names

```
{
    "eventType": "PH_RULE_DNS_THREATSTREAM_MALWARE_DOMAIN",
    "srcIpAddr": "192.0.2.0",
    "destIpAddr": "203.0.113.0",
    "incidentSrc": "srcIpAddr:192.0.2.0,",
    "attackTactic": "Exfiltration",
    "eventSeverity": 9,
    "incidentCount": 30,
    "incidentRptIp": "198.51.100.0",
    "incidentTitle": "DNS Traffic from 192.0.2.0 to Threat Stream Malware Domain
westlady.net",
    "incidentTarget": "destName:westlady.net,",
    "attackTechnique": "[{\"name\":\"Exfiltration Over Alternative Protocol: Exfiltration
Over Symmetric Encrypted Non-C2 Protocol\",\"techniqueid\":\"T1048.001\"}]",
    "eventSeverityCat": "HIGH",
    "incidentRptDevName": "HOST-198.51.100.0"
}
```

Custom Playbook Requirements – API Endpoint Specification

FortiSIEM compatible Playbooks all start with a Step type called “Custom API Endpoint”. FortiSOAR then creates a URI for that specific Playbook that can be called.

Example:



The get domain reputation Playbook creates a route called "/api/triggers/1/fsiem_api_get_domain_reputation".

Authentication Method: Token-Based

FortiSIEM can then make API calls to this endpoint in the format

`https://<fortisoar-hostname>/api/triggers/1/fsiem_api_get_domain_reputation`

FortiSIEM Prebuilt Playbooks

FortiSIEM and FortiSOAR teams have provided a content pack installable in your FortiSOAR system with the following Playbooks, which are commonly used, but can also be a building block for your own custom Playbooks.

Content Pack Playbooks

- fortisiem-get-domain-reputation
- fortisiem-get-hash-reputation
- fortisiem-get-url-reputation
- fortisiem-get-ip-reputation-summary

Reference Playbooks

To support complex tasks completed by the above Playbooks, the following Playbooks are not called directly, and are only used by the above Playbooks (nested Playbooks) – Do not delete them, but do not call them directly.

- fortisiem-reference-get-domain-rep
- fortisiem-reference-get-hash-reputation
- fortisiem-reference-get-url-rep
- fortisiem-reference-validate-ip
- fortisiem-reference-virustotal-summary

The naming convention of the playbooks are as follows:

<system>-<call method>-<purpose>

fortisiem – Indicates this is a Playbook for use by FortiSIEM only. Within the FortiSIEM UI, you can execute these Playbooks.

get or reference – get indicates this Playbook can be called by FortiSIEM. Reference indicates it is a reference Playbook and not called directly. **Never call a "reference" Playbook from FortiSIEM, these reference Playbooks are only called automatically from other Playbooks.

Playbook Tagging

It is **required** that every FortiSOAR Playbook that is designed to work with, and be called by FortiSIEM, should have a Playbook tag called "**FortiSIEM**" in case sensitive format. FortiSIEM may filter for Playbooks tagged in this way to avoid polling a list of all possible Playbooks.

Formatting Playbook Result Data back to FortiSIEM

Once FortiSIEM has successfully executed a FortiSOAR Playbook, and supplied either Incident or Raw event JSON data for the Playbook to operate on, it will wait for a JSON response.

This response data is dynamically configured within your Playbook. You can return any variables you'd like, but there are a few special variables that you should standardize in your Playbooks that FortiSIEM will display in the results screen.

FortiSIEM Special Playbook Response Variables

- Summary – A string variable that shows high level result data from the execution of your Playbook. Short and high level.
- Details – A string variable that shows detailed result data that may be more verbose.

For a demonstration, take a look at the Playbook: fortisiem-get-ip-reputation

We have a final Set Variable step called “AggregateOutput” where we format resulting variables.

Set Variable
Step Name*
AggregateOutput
+ Add Step Description
Variables:
Summary
{{vars.steps.Generate_aggregate_summary.data['formatted_string']}}
Detailed Summary
{{vars.steps.Gen_Agg_Summary_Detail.data['formatted_string']}}
DestIP VirusTotal Result
{{vars.steps.Get_Dest_IP_VT_Result.json_response}}
Host IP VirusTotal Result
{{vars.steps.Get_Host_IP_VT_Result.json_response}}
Dest IP VirusTotal Summar
{{vars.steps.Get_Dest_IP_VT_Result.summary}}
Host IP VirusTotal Summar
{{vars.steps.Get_Host_IP_VT_Result.summary}}
Source IP VirusTotal Resu
{{vars.steps.Get_Source_IP_VT_Result.json_response}}
Source IP VirusTotal Summ
{{vars.steps.Get_Source_IP_VT_Result.summary}}
Incident Target VirusTota
{{vars.steps.Get_Incident_Target_VT_Result.json_response}}

We have a string formatting step result that is stored in a variable called “Summary”. FortiSIEM simply takes this particular variable and displays it prominently in the response UI for display and saving.

We also have a string formatting step result that is stored in a variable called “Detailed Summary”. As the name suggests, it is meant for more verbose data.

Only “Summary” should be considered a mandatory set variable, the others are optional and can be viewed in the GUI.

References

Playbooks Guide: https://docs.fortinet.com/document/fortisoar/7.0.2/playbooks-guide

Connector Guide: https://docs.fortinet.com/document/fortisoar/7.0.2/connectors-guide

Jinja Template Designer Documentation: https://jinja.palletsprojects.com/en/3.0.x/templates/

Functions in Analytics

This section describes the functions that are used in Analytics (Rules and Queries).

Type	Functions
Aggregation Functions	AVG, COUNT, COUNT DISTINCT, FIRST, LAST, MAX, MEDIAN, MIN, MODE, PctChange, Pctile95, PCTILE, STDDEV, SUM, VARIANCE
CMDB Lookup Function	DeviceToCMDBAttr
Conversion Functions	LOG, TO_DOUBLE, TO_INTEGER, TO_STRING
Date Conversion Functions	DayOfWeek, HourOfDay
Evaluate and Set Function	IF
Extraction Function	EXTRACT
LookupTable Functions	LookuptableGet, LookupTableHas
String Manipulation Functions	LEN, LTRIM, REPLACE, RTRIM, SUB_STR, TO_LOWER, TO_UPPER, TRIM
Time Window Functions	EMA, SMA

Aggregation Functions

- AVG Function
- COUNT Function
- COUNT DISTINCT Function
- FIRST Function
- LAST Function
- MAX Function
- MEDIAN Function
- MIN Function

- MODE Function
- PctChange Function
- Pctile95 Function
- PCTILE Function
- STDDEV Function
- SUM Function
- VARIANCE Function

AVG Function

Description

AVG(<eventAttribute>) returns the average of the values of the numerical field in all events matching the query criteria.

Scope

AVG() is available in EventDB, ClickHouse, Elasticsearch and Rules. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax

- *AVG(<eventAttribute>)* - *eventAttribute* must be a numerical type.
- *AVG (Function(<eventAttribute>))* – The *Function* must return a numerical value.
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions
  - Only LEN allowed in String Manipulation Functions
  - LOG not allowed in Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - Evaluate and Set Function, String Manipulation Functions, Conversion Functions, Date Conversion Functions
  - Only LEN allowed in String Manipulation Functions

Example

Event Type	Source IP	Sent Bytes
E1	10.1.1.1	10
E2	10.1.1.1	20
E3	10.1.1.2	30

If you choose Source IP and SUM(Sent Bytes) in **Group By and Display Fields**:

Source IP	SUM(Sent Bytes)
10.1.1.1	15.5
10.1.1.2	30

COUNT Function

Description

COUNT(*) returns the number of occurrences of each matched row in a query.

COUNT(<eventAttribute>) counts the number of occurrences of the event attribute in the query result.

Scope

- *COUNT(*)* is available for EventDB, ClickHouse, Elasticsearch queries and rules.
- *COUNT(<eventAttribute>)* is only available for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.
- Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax

- *COUNT(*)*
- *COUNT(<eventAttribute>)*
- *COUNT(Function(<eventAttribute>))*
- In Elasticsearch only these nested function categories are allowed:
  - Extraction Function e.g. *COUNT(EXTRACT<..>)*
- In ClickHouse, only these nested function categories are allowed:
  - Extraction Function e.g. *COUNT(EXTRACT<..>)*

Example

Event Type	Source IP	User
E1	10.1.1.1	Bob
E2	10.1.1.1	
E3	10.1.1.2	Bob

COUNT(Event Type) = 3

COUNT(Source IP) = 3

COUNT(User) = 2

COUNT(*) = 3

COUNT DISTINCT Function

Description

COUNT DISTINCT(<eventAttribute >) returns the number of *distinct* occurrences of the event attribute in the query result

Scope

COUNT DISTINCT is available in EventDB, ClickHouse, Elasticsearch queries and rules. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax

- *COUNT (DISTINCT <eventAttribute>)*
- *COUNT(DISTINCT Function(<eventAttribute>))*
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function e.g. *COUNT(DISTINCT EXTRACT<..>)*
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function e.g. *COUNT(DISTINCT EXTRACT<..>)*

Example

Event Type	Source IP	User
E1	10.1.1.1	Bob
E2	10.1.1.1	Alice
E3	10.1.1.2	Bob

COUNT DISTINCT (Event Type) = 3

COUNT DISTINCT (Source IP) = 2

COUNT DISTINCT (User) = 2

FIRST Function

Description

FIRST(<eventAttribute>) returns the value of the <eventAttribute> in the event with *earliest* **Event Receive Time** in the query result.

Note that for every event, **Event Receive Time** attribute is set to the time at which the event was first received at any FortiSIEM node (Collector, Worker or Supervisor).

Scope

FIRST() is available in EventDB, ClickHouse and Elasticsearch.

Syntax

- *FIRST (<eventAttribute>)* or *FIRST (FUNCTION(<eventAttribute>))*
- In Elasticsearch, nested functions are not allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function

Example

Event Receive Time	Event Type	User	Login Time
T1	Login Success	Alice	T5
T1+1	Login Success	Bob	T6
T1+2	Login Success	Bob	T7
T1+3	Login Success	Carl	T6

If you choose User in **Group By and Display Fields**:

User	FIRST(Login Time)
Alice	T5
Bob	T6
Carl	T6

LAST Function

Description

LAST(<eventAttribute>) returns the value of the <eventAttribute> in the event with *latest* **Event Receive Time** in the query result.

Note that for every event, **Event Receive Time** attribute is set to the time at which the event was first received at any FortiSIEM node (Collector, Worker or Supervisor).

Scope

LAST() is available in EventDB, ClickHouse and Elasticsearch for all releases.

Syntax

- *LAST(<eventAttribute>)* or *LAST (FUNCTION(<eventAttribute>))*
- In Elasticsearch, nested functions are not allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function

Example

Time	Event Type	user	loginTime
T1+1	Login Success	Bob	T6
T1+2	Login Success	Bob	T7
T1+3	Login Success	Carl	T6

With a Group By on user:

user	LAST(loginTime)
Alice	T5
Bob	T7
Carl	T6

MAX Function

Description

MAX(<eventAttribute>) returns the maximum value of event Attribute in the query result.

Scope

MAX() is available in EventDB, ClickHouse, Elasticsearch and Rules. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax

- *MAX(<eventAttribute>)* - *eventAttribute* must be a numerical type.
- *MAX (Function(<eventAttribute>))* – The *Function* must return a numerical value.
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions
  - Only LEN allowed in String Manipulation Functions
  - LOG not allowed in Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - Evaluate and Set Function, String Manipulation Functions, Conversion Functions, Date Conversion Functions
  - Only LEN allowed in String Manipulation Functions

Example

Event Type	Source IP	Sent Bytes
E1	10.1.1.1	10
E2	10.1.1.1	20
E3	10.1.1.2	30

If you choose Source IP and SUM(Sent Bytes) in **Group By and Display Fields**:

Source IP	SUM(Sent Bytes)
10.1.1.1	20
10.1.1.2	30

MEDIAN Function

Description

MEDIAN(<eventAttribute>) returns the value lying at the midpoint of the frequency distribution of the values of the event Attribute in the query result. In other words, it is the middle number in a sorted list of the values.

Scope

MEDIAN() is available in ClickHouse and Elasticsearch from release 7.0.0 onwards. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax

- *MEDIAN(<eventAttribute>)* - *eventAttribute* must be a numerical type.
- *MEDIAN(Function(<eventAttribute>))* – The *Function* must return a numerical value.
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions, Date Conversion Functions

Example

Event Receive Time	Host Name	CPU Util	Memory Util
T1	Host1	2.58%	1.33 %
T2	Host1	0.00 %	0.07 %
T3	Host1	0.04 %	0.00 %
T4	Host1	0.02 %	1.16 %

MEDIAN(CPU Util) = 0.03 (average of two midpoint values – 0.04 and 0.02)

MEDIAN(Memory Util) = 0.615

MIN Function

Description

MIN(<eventAttribute>) returns the *minimum value* of event Attribute in the query result.

Scope

MIN() is available in EventDB, ClickHouse, Elasticsearch and Rules. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax

- *MAX(<eventAttribute>)* - *eventAttribute* must be a numerical type.
- *MAX (Function(<eventAttribute>))* – The *Function* must return a numerical value.
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions
  - Only LEN allowed in String Manipulation Functions
  - LOG not allowed in Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - Evaluate and Set Function, String Manipulation Functions, Conversion Functions, Date Conversion Functions
  - Only LEN allowed in String Manipulation Functions

Example

Event Type	Source IP	Sent Bytes
E1	10.1.1.1	10
E2	10.1.1.1	20
E3	10.1.1.2	30

If you choose Source IP and SUM(Sent Bytes) in Group By and Display Fields:

Source IP	SUM(Sent Bytes)
10.1.1.1	10
10.1.1.2	30

MODE Function

Description

MODE(<eventAttribute>) returns the *most frequently appearing* value of the event Attribute in the query result.

Scope

MODE() is available in ClickHouse and Elasticsearch from release 7.0.0 onwards. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax and Restrictions

- *MODE(<eventAttribute>) or MODE (Function(<eventAttribute>))*
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, Date Conversion Function
- **Display Conditions** (i.e. SQL HAVING type of operation) is not supported.
- Trend displayed only if the argument in *MODE(X)* is a numeric value.

Example

Use Case - Identify the most common source IP address for each user

Event Receive Time	Event Type	User	Source IP
T1	Login Success	Alice	10.1.1.1
T2	Login Success	Bob	10.1.1.2
T3	Login Success	Bob	10.1.1.2
T4	Login Success	Carl	10.1.1.3
T5	Login Success	Bob	10.1.1.4

If you choose User in **Group By and Display Fields**:

User	MODE(Source IP)
Alice	10.1.1.1
Bob	10.1.1.2
Carl	10.1.1.3

PctChange Function

Description

PctChange(<eventAttribute >) returns the percentage change of < eventAttribute > from the first event and the last event in the query result.

Scope

Available for EventDB, ClickHouse and Elasticsearch queries.

Syntax

- PctChange(<eventAttribute>) - eventAttribute must be a numerical type.
- In Elasticsearch these nested function categories are allowed:
  - Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - Evaluate and Set Function, Conversion Functions

Example

Consider the following set of events matching the query conditions:

Raw Data

Event Receive Time (ascending)	Host Name	Disk Name	Disk Util
T1	Host1	D:\	10
T2	Host1	D:\	20
T3	Host1	D:\	30
T4	Host1	D:\	40

Query Result for the time window [T1,T4]:

Host Name	Disk Name	PctChange (Disk Util)
Host1	D:\	300%

Pctile95 Function

Description

Pctile95(<eventAttribute>) returns the 95th percentile value of the <eventAttribute> in the query result.

Scope

Available for EventDB, ClickHouse and Elasticsearch queries.

Syntax

- *Pctile95(<eventAttribute)* - *eventAttribute* must be a numerical type.
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, String Manipulation Functions, Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - String Manipulation Functions, Conversion Functions

Example

Event Receive Time	Host Name	Interface Name	Interface Util
T1	Host1	Wan	2.58
T2	Host1	Wan	0.00
T3	Host1	Wan	0.04
T4	Host1	Wan	0.02

Query Result for the time window [T1,T4]:

Host Name	Interface Name	Pctile95(Interface Util)
Host1	Wan	2.2

PCTILE Function

Description

PCTILE(N,<eventAttribute>) returns *Nth percentile value* of the *<eventAttribute>* in the query result. N is between 0 and 100. This generalizes the *Pctile95()* function.

Scope

Available for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Syntax

- *PCTILE (N,<eventAttribute>) - eventAttribute* must be a numerical type.
- *PCTILE (N,Function(<eventAttribute>))* – The *Function* must return a numerical value.
- In Elasticsearch, these nested function categories are allowed:
  - Extraction Function, String Manipulation Functions, Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - String Manipulation Functions (LEN), Conversion Functions

Example

Event Receive Time	Host Name	Interface Name	Interface Util
T1	Host1	Wan	2.58
T2	Host1	Wan	0.00
T3	Host1	Wan	0.04
T4	Host1	Wan	0.02

Query Result for the time window [T1,T4]:

Host Name	Interface Name	PCTILE(95,Interface Util)
Host1	Wan	2.2

Host Name	Interface Name	PCTILE(80,Interface Util)
Host1	Wan	1.06

STDDEV Function

Description

STDDEV(<eventAttribute>) returns the *standard deviation* of the values of *eventAttribute* in the query result. FortiSIEM calculates populationstandard deviation. *STDDEV(<eventAttribute>)* is the square root of *VARIANCE(<eventAttribute>)* defined below.

Scope

Works for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Syntax

- *STDDEV (<eventAttribute>) - eventAttribute* must be a numerical type.
- *STDDEV (Function(<eventAttribute>))* – The *Function* must return a numerical value.

- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions, Date Conversion Functions

Example

Event Receive Time	Host Name	CPU Util	Memory Util
T1	Host1	20	63
T2	Host1	35	65
T3	Host1	50	66
T4	Host1	60	70

If you choose Host Name in **Group By and Display Fields**:

Host Name	STDDEV(CPU Util)	STDDEV(Memory Util)
Host1	15.15	2.55

SUM Function

Description

SUM(<eventAttribute >) returns the sum of the values of the numerical event Attribute in the query result.

Scope

SUM is available in EventDB, ClickHouse, Elasticsearch and Rules. Nesting capability is available in ClickHouse and Elasticsearch from release 7.0.0 onwards.

Syntax

- *SUM(<eventAttribute>)* - *eventAttribute* must be a numerical type.
- *SUM (Function(<eventAttribute>))* – The *Function* must return a numerical value.
- In Elasticsearch these nested function categories are allowed:
  - All Extraction Functions, All Evaluate and Set Functions
  - Only LEN allowed in String Manipulation Functions
  - All Conversion Functions except LOG

- In ClickHouse, these nested function categories are allowed:
  - All Extraction Functions, All Evaluate and Set Functions
  - Only LEN allowed in String Manipulation Functions
  - All Conversion Functions except LOG

Example

Event Type	Source IP	Sent Bytes
E1	10.1.1.1	20
E2	10.1.1.1	20
E3	10.1.1.2	30

If you choose Source IP and SUM(Sent Bytes) in **Group By and Display Fields**:

Source IP	SUM(Sent Bytes)
10.1.1.1	40
10.1.1.2	30

VARIANCE Function

Description

VARIANCE(<eventAttribute>) returns the *variance* of the values of the *eventAttribute* in the query result. FortiSIEM calculates population variance.

Scope

Works for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Syntax

- *VARIANCE (<eventAttribute>)* - *eventAttribute* must be a numerical type.
- *VARIANCE (Function(<eventAttribute>))* – The *Function* must return a numerical value.
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions, Conversion Functions
- In ClickHouse, these nested function categories are allowed:
  - Evaluate and Set Function, String Manipulation Functions, Conversion Functions, Date Conversion Functions

Example

Event Receive Time	Host Name	CPU Util	Memory Util
T1	Host1	20	63
T2	Host1	35	65
T3	Host1	50	66
T4	Host1	60	70

If you choose Host Name in **Group By and Display Fields**:

Host Name	VARIANCE(cpuUtil)	VARIANCE(memUtil)
Host1	229.69	6.5

CMDB Lookup Function

- DeviceToCMDBAttr Function

DeviceToCMDBAttr Function

Description

DeviceToCMDBAttr(<deviceId>,<cmdbAttribute>) returns the value of *<cmdbAttribute>* for the device specified by *<deviceId>*. The device must be present in CMDB PostgreSQL database.

Scope

Available for EventDB, ClickHouse and Elasticsearch queries and Rules.

Syntax

- For simple CMDB Attributes that are attached to a device, the syntax is: *DeviceToCMDBAttr (<deviceId >,<cmdbAttr>)*, where *deviceId* can be any event attribute that can be used by FortiSIEM can look up the device in CMDB. Common examples are device name and Ip fields, e.g. hostName, hostIpAddr, srcName, srcIpAddr, destName, destIpAddr etc. *Note that cmdbAttr* are defined in **Admin > Device Support > Custom Properties**.
- Sometimes CMDB Attributes are attached to an interface or a disk of a device. In this case the syntax is: *DeviceToCMDBAttr(<deviceId >,<deviceAttr>,<cmdbAttr>)*, where
  - *deviceId* can be any event attribute that can be used by FortiSIEM can look up the device in CMDB. Common examples are device name and Ip fields, e.g. hostName, hostIpAddr, srcName, srcIpAddr, destName, destIpAddr etc.
  - *deviceAttr* is Device Attribute: *intfName*, *diskName*

- *cmdbAttr* are defined in **Admin > Device Support > Custom Properties**. Examples:
  - *DeviceToCMDBAttr(hostIpAddr,intfName,IntfErrPctThreshCrit))*
  - *DeviceToCMDBAttr(hostIpAddr,diskName,DiskSpaceUtilThreshCrit)*

Example

CMDB:

Device Name	country	intfName	NetIntfUtilThreshCrit
Host1	U.S.A	Intf1	75
Host2	France	Intf1	90
Host2	France	Intf2	75

Query Results:

phRecvTime	eventType	hostName	intfName	intfUtil	DeviceToCMDBAttr (hostname, city)	DeviceToCMDBAttr(hostName, intfName, NetIntfUtilThreshCrit)
T1	Intf_Usage	Host1	Intf1	40	U.S.A	75
T2	Intf_Usage	Host2	Intf1	80	France	90
T2	Intf_Usage	Host2	Intf2	60	France	75
T3	Intf_Usage	Host3	Intf1		<No match>	<No match>

Conversion Functions

- LOG Function
- TO_DOUBLE Function
- TO_INTEGER Function
- TO_STRING Function

LOG Function

Description

LOG(<eventAttribute>, <base>) calculates the log of a numeric *<eventAttribute>* to its *<base>*.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *LOG(<eventAttribute>, <base>)*
  - *<eventAttribute>* is a numeric eventAttribute.
  - *<base>* is optional and default is 10
- *LOG(Function(<eventAttribute>), <base>)*
  - *Function* must return a numeric value.
  - *<base>* is optional and default is 10.
- Elasticsearch does not support nested functions.
- In ClickHouse, these nested function categories are allowed:
  - Aggregation Functions, Evaluate and Set Function, Conversion Functions

Example

Host Name	recvBytes64	LOG (recvBytes64,10)	LOG (recvBytes64,"e")
Host1		6.67	15.36
Host2		7.35	16.73
Host3		2.66	6.12

TO_DOUBLE Function

Description

TO_DOUBLE(<eventAttribute>) converts a string valued event attribute X to a double number.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *TO_ DOUBLE (<eventAttribute>)*
  - *<eventAttribute>* is a string valued eventAttribute or a *Function* of an eventAttribute that returns a string.
- *TO_ DOUBLE (FUNCTION(<eventAttribute>))*
  - *Function* must return a STRING value.

- Elasticsearch does not support nested functions.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, String Manipulation Functions, Conversion Functions

Example

field	TO_DOUBLE(field)
“1234.56”	1234.56
“-1234.56”	-1234.56

TO_INTEGER Function

Description

TO_INTEGER(<eventAttribute>, <base>) converts a string valued *<eventAttribute>* to a integer with *<base>*. *<base>* is optional and default is 10.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *TO_ INTEGER (<eventAttribute>, <base>)*
  - *<eventAttribute>* is a string valued eventAttribute or a *Function* of an eventAtribute that returns a string.
  - *<base>* is an integer. It is optional and default is 10.
- *TO_ INTEGER (FUNCTION(<eventAttribute>), <base>)*
  - *Function* must return a STRING value.
  - *<base>* is an integer. It is optional and default is 10.
- *<eventAttribute>* has to be string representation of an integer.
- If *<base>* is 2 or 16, X must be a string representation of a positive integer.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, String Manipulation Functions, Conversion Functions

Example

field	TO_INTEGER (field,10)	TO_INTEGER (field,2)	TO_NUMBER (field,16)
“1000”	1000	1111101000	3E8
“1234”	1234	10011010010	4D2

TO_STRING Function

Description

TO_STRING(<eventAttribute>) converts an input *<eventAttribute>* to a string. If the *<eventAttribute>* is an integer, then it reformats the number as a string. If the *<eventAttribute>* is an Boolean value, then it returns “True” of “False”.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *TO_STRING(<eventAttribute>)*
  - *<eventAttribute>* is a numeric eventAttribute, or a Function returning a number, or a Boolean expression.
  - Return value:
    - If the *<eventAttribute>* is an integer, then it reformats the number as a string.
    - If the *<eventAttribute>* is a Boolean value, then it returns “True” of “False”.
- *TO_STRING(FUNCTION(<eventAttribute>))*
  - *Function* must return a numeric value or a Boolean expression.
  - Return value:
    - If the *<eventAttribute>* is an integer, then it reformats the number as a string.
    - If the *<eventAttribute>* is an Boolean value, then it returns “True” of “False”.
- Elasticsearch does not support nested functions.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, Conversion Functions

Example

attr1	TO_STRING(attr1)
1234	“1234”
1234.56	“-1234.56”

Date Conversion Functions

- DayOfWeek Function
- HourOfDay Function

DayOfWeek Function

Description

DayOfWeek(<eventAttribute>) returns the day of week in the DATE valued *<eventAttribute>*. 0 is returned for Sunday and 6 for Saturday.

Scope

- *DayOfWeek()* is available in EventDB, ClickHouse and Elasticsearch queries and rules.
- *DayOfWeek()* can be used in Filter By and Group By.

Syntax

- *DayOfWeek (<eventAttribute>)*
  - *<eventAttribute>* type must be DATE.
  - Returned values are:
    - 0 for Sunday
    - 1 for Monday
    - 2 for Tuesday
    - 3 for Wednesday
    - 4 for Thursday
    - 5 for Friday
    - 6 for Saturday

Example

Event Receive Time	Event Type	DayOfWeek(Event Receive Time)
Monday May 15, 10:37AM	Login-Success	1
Tuesday May 16, 7:37AM	Login-Success	2

HourOfDay Function

Description

HourOfDay (<eventAttribute>) returns the hour of day in the DATE valued argument. For times between 12:00AM and 12:59AM, *HourOfDay()* returns 0; between 1:00AM and 1:59AM, *HourOfDay()* returns 1, etc...

Scope

HourOfDay() is available in EventDB, ClickHouse and Elasticsearch Queries and Rules.

Syntax

- *HourOfDay (<eventAttribute>)* and *eventAttribute* type must be DATE.

Example

Event Receive Time	Event Type	HourOfDay(Event Receive Time)
Monday May 15, 10:37AM	Login-Success	10
Monday May 15, 7:37AM	Login-Success	19

Evaluate and Set Function

- IF Function

IF Function

Description

IF(<expression>,<trueValue>,<falseValue>) evaluates the <*expression*> and returns <*trueValue*> if <*expression*> is true, and <*falseValue*> if the <*expression*> is false.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *IF(<expression>,<trueValue>,<falseValue>)*
  - <*expression*> is a Boolean expression that evaluates to true or false. Currently expression can only be the following expressions joined by AND/OR: e.g. <*eventAttribute*><*Operator*><*ConstantValue*>.
  - <*trueValue*> is returned when <*expression*> evaluates to true – can be a string or an integer.
  - <*falseValue*> is returned when <*expression*> evaluates to false – can be a string or an integer.
- Nested functions is not supported for IF.

Example

Time	EventvType	User	IF(Event Type=" Login-Success",1,0)	IF(Event Type=" Login-Failure",1,0)
T1	Login-Success	User1	1	0
T2	Login-Success	User2	1	0
T3	Login-Failure	User1	0	1
T4	Login-Failure	User1	0	1
T5	Login-Success	User1	1	0

If you group by on User and then apply aggregate on the IF function, then you get the following result:

User	SUM(IF(eventType=" Login-Success",1,0))	SUM(IF(eventType=" Login-Failure",1,0
User1	2	2
User2	1	0

Extraction Function

- EXTRACT Function

EXTRACT Function

Description

EXTRACT(<eventAttribute>,<pattern>) extracts a value from <*eventAttribute*> after applying regular expression <*pattern*>, and then returns the extracted value. The returned type is determined from the regular expression. The EXTRACT function helps to parse new fields from the historical raw log which the parser may have missed.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards. Can extract only one value. Multiple extractions not supported.

Syntax

- *EXTRACT(<eventAttribute>,<pattern>)*
  - <*eventAttribute*> is a string valued *eventAttribute*.
  - <*pattern*> is a regular expression pattern for value extraction.

- *EXTRACT(Function(<eventAttribute>),<pattern>)*
  - *Function* returns a string value.
  - *<pattern>* is a regular expression pattern for value extraction.
- Elasticsearch does not support nested functions.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, String Manipulation Functions, Evaluate and Set Function, Conversion Functions

Example

rawEventMsg	EXTRACT (rawEventMsg,".*\ [recvBytes64\]= (\d+).*")
<134>Sep 19 17:55:01 172.30.52.10 java: [PH_DEV_MON_VM_NET_INTF_UTIL]: [eventSeverity]=PHL_INFO,[vmName]=CentOS7-7.2.1, [recvPkts64]=0, [sentPkts64]=0,[recvBytes64]=23000, [sentBytes64]=54999	23000
<134>Sep 19 17:55:01 172.30.52.10 java: [PH_DEV_MON_VM_NET_INTF_UTIL]: [eventSeverity]=PHL_INFO,[vmName]=CentOS7-7.2.1, [recvPkts64]=0, [sentPkts64]=0,[recvBytes64]= 368640, [sentBytes64]=54999	368640

Lookup Table Functions

- LookupTableGet Function
- LookupTableHas Function

LookupTableGet Function

Description

LookupTableGet (<tableName>,<eventAttribute>,<tableColumn>) searches the Lookup Table *<tableName>* and matches the values of its key columns with *<eventAttribute>*. If a matching row is found, then it returns the *<tableColumn>* from that row. If the Lookup Table has multiple keys, then corresponding event attributes must be specified.

LookupTables are defined in Resources tab and details on how to populate them can be found here.

Scope

Available for EventDB, ClickHouse and Elasticsearch queries and Rules.

Syntax

- *LookupTableGet (<tableName>,<eventAttribute>,<tableColumn>)*
- The number of eventAttributes in the argument match the key fields in the Lookup Table.

Example

LookupTable: **UserLoc**

User (Key)	Country	Department
Bob	U.S.A	Finance
Alice	Germany	Engineering
John	U.S.A	Marketing

The following table shows the *LookuptableGet* function applied to events.

Event receive Time	Event Type	User	LookupTableGet (UserLoc, User, Country)	LookupTableGet (UserLoc, User,Department)
T1	Login-Success	John	U.S.A	Marketing
T2	Login-Failure	Alice	Germany	Engineering
T3	Login-Success	Alice	Germany	Engineering

Notes:

- *User* field in events is matched with the *User* field in UserLoc Lookup Table.
- *LookupTableGet(UserLoc, User, Country)* returns the *Country* field for the matching row in UserLoc Lookup Table.
- *LookupTableGet(UserLoc, User, Department)* returns the *Department* field for the matching row in UserLoc Lookup Table.

LookupTableHas Function

Description

LookupTableHas (<tableName>,<eventAttribute>) searches the Lookup Table <tableName> and

- Returns 1 if there is a row in Lookup table <*tableName*> where the key field(s) match the specified <*eventAttribute*>.
- Returns 0 if there is no match.

If <*tableName*> has multiple Keys, then exactly same number of <*eventAttributes*> must be specified.

LookupTables are defined in Resources tab and details on how to populate them can be found here.

Scope

Available for EventDB, ClickHouse and Elasticsearch queries and Rules.

Syntax

- *LookupTableHas (<tableName>,<eventAttribute>)*
- The number of eventAttributes must match the key fields in the Lookup Table.

Example

LookupTable: **LoginCountry**

User (Key)	Country (Key)
Bob	U.S.A
Alice	Germany
John	U.S.A

The following table shows the LookuptableGet function applied to events:

Event receive Time	Event Type	User	Source Geo Country	LookupTableHas (LoginCountry, User, Source Geo Country)
T1	Login-Success	John	U.S.A	1
T2	Login-Failure	Alice	France	0
T3	Login-Success	Alice	Germany	1

Notes:

- Since **LoginCountry LookupTable has 2 Keys**:
  - *User* field in events is matched with the *User* field in **UserLoc** Lookup Table.
  - *Source Geo Country* field in events is matched with the *Country* field in **UserLoc** Lookup Table.
- *LookupTableGet(LoginCountry, User, Source Geo Country)* returns
  - *1 if BOTH User* field in events matches the *User* field in **UserLoc** Lookup Table. And *Source Geo Country* field in events is matched with the *Country* field in **UserLoc** Lookup Table.

String Manipulation Functions

- LEN Function
- LTRIM Function

- REPLACE Function
- RTRIM Function
- SUB_STR Function
- TO_LOWER Function
- TO_UPPER Function
- TRIM Function

LEN Function

Description

LEN(<eventAttribute>) returns the *length* of a string valued <eventAttribute>.

Scope

- Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions

Syntax

- *LEN(<eventAttribute>)* - *eventAttribute* must be a STRING type.
- *LEN(Function(<eventAttribute>))* - The *Function* must return a STRING value.

Example

Event Type	Raw Event Log	LEN(Raw Event Log)
E1	This is a short event	21
E2	This is a medium event	23
E3	This is a very very long event	30

LTRIM Function

Description

LTRIM(<eventAttribute>,<chars>) returns the string valued *<eventAttribute>* after trimming characters in *<chars>* from left side. If *<chars>* is not specified, then only spaces and tabs are removed.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *LTRIM(<eventAttribute >,<chars>)*
  - *<eventAttribute>* must be a STRING type.
  - *<chars>* is a list of characters.
- *LTRIM(Function(<eventAttribute>), <chars>)*
  - *Function* must return a STRING value.
  - *<chars>* is a list of characters.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions

Example

user	LTRIM(user)	LTRIM(user, “FORTINET\\”)
“ user1”	“user1”	“ user1”
“FORTINET\user3”	" “FORTINET\user3”	"user3”

REPLACE Function

Description

REPLACE(<eventAttribute>,<pattern>,<replaceWith>) returns a string formed by substituting string *<replaceWith>* for every occurrence of regex string *<pattern>* in string valued *<eventAttribute>*.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *REPLACE(<eventAttribute>,<pattern>,<replaceWith>))*
  - *<eventAttribute>* must be a STRING type.
  - *<pattern>* must be a regular expression and
  - *<replaceWith>* is a STRING type.
- *REPLACE (Function(<eventAttribute>),<pattern>,<replaceWith>)*
  - *Function* must return a STRING value.
  - *<pattern>* must be a regular expression and
  - *<replaceWith>* is a STRING type.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Functions, Evaluate and Set Function, String Manipulation Functions

Example

user	REPLACE(user, "FORTINET\\", "")	REPLACE(user, "Administrator", "admin")
Bob	Bob	Bob
FORTINET\John	John	John
alice@fortinet.com	alice@fortinet.com	alice@fortinet.com
Administrator	Administrator	admin

RTRIM Function

Description

RTRIM(<eventAttribute>,<chars>) returns the string valued <*eventAttribute*> after trimming characters in <*chars*> from the right side. If <*chars*> is not specified, then only spaces and tabs are removed.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *RTRIM(<eventAttribute >,<chars>)*
  - <*eventAttribute*> must be STRING type.
  - <*chars*> is a list of characters.
- *RTRIM(Function(<eventAttribute>), <chars>)*
  - *Function* must return a STRING value.
  - <*chars*> is a list of characters.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions

Example

user	RTRIM(user)	RTRIM(user, “@fortinet.com”)
“user1 ”	“user1”	“user1 ”
“user2@fortinet.com”	“user2@fortinet.com”	"user2”

SUB_STR Function

Description

SUB_STR(<eventAttribute>,<start>,<num>) returns a substring of string valued <*eventAttribute*>, starting at the index specified by <*start*> with the number of characters specified by <*num*>. If <*num*> is not specified, then the string <*eventAttribute*> starting at <*start*> to the end is returned.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *SUB_STR(<eventAttribute>,<start>[,<num>])*
  - <*eventAttribute*> must be STRING type.
  - <*start*> is an integer between 0 and the length of <*eventAttribute*>.
  - <*num*> is an integer and must be less than length of <*eventAttribute*> minus <*start*>.
- *SUB_STR(Function(<eventAttribute>),<start>[,<num>])*
  - *Function* must return a STRING value.
  - <*start*> is an integer between 0 and the length of <*eventAttribute*>.
  - <*num*> is an integer and must be less than length of <*eventAttribute*> minus <*start*>.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions

Example

User	SUB_STR(User,2)	SUB_STR(User,2,2)
aabbcc	bbcc	bb
123456	3456	12

TO_LOWER Function

Description

TO_LOWER(<eventAttribute >) changes the case of a string valued <*eventAttribute*> to all lower case.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *TO_LOWER (<eventAttribute>) - eventAttribute* must be a STRING type.
- *TO_LOWER (Function(<eventAttribute>))* - The *Function* must return a STRING value.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, the following nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions

Example

Event Type	User	TO_LOWER(User)
E1	Bob	bob
E2	ACME/John	acme/john
E3	ALICE	alice

TO_UPPER Function

Description

TO_UPPER(<eventAttribute >) changes the case of a string valued <*eventAttribute*> to all upper case.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *TO_UPPER (<eventAttribute>)* - *eventAttribute* must be a STRING type.
- *TO_UPPER (Function(<eventAttribute>))* - The *Function* must return a STRING value.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Function, Evaluate and Set Function, String Manipulation Functions

Example

Event Type	User	TO_UPPER(User)
E1	Bob	BOB
E2	ACME/John	ACME/JOHN
E3	ALICE	ALICE

TRIM Function

Description

TRIM(<eventAttribute>,<chars>) returns the string valued <*eventAttribute*> after trimming characters in <*chars*> from both sides. If <*chars*> is not specified, then only spaces and tabs are removed.

Scope

Available for ClickHouse and Elasticsearch queries from 7.0.0 onwards.

Syntax

- *TRIM(<eventAttribute >,<chars>)*
  - *<eventAttribute>* must be a STRING type.
  - *<chars>* is a list of characters.
- *TRIM(Function(<eventAttribute>), <chars>)*
  - *Function* must return a STRING value.
  - *<chars>* is a list of characters.
- In Elasticsearch, no nested function categories are allowed.
- In ClickHouse, these nested function categories are allowed:
  - Extraction Functions, Evaluate and Set Function, String Manipulation Functions

Example

user	TRIM(user)	TRIM(user, “FORTINET\\”)
“ user1”	“user1”	“ user1”
“user2 ”	"user2”	“user2 ”
“FORTINET\user3”	" “FORTINET\user3”	"user3”

Time Window Functions

- EMA Function
- SMA Function

EMA Function

Description

EMA(N,<eventAttribute>) returns *Exponential Moving Average* over N previous values of the *<eventAttribute>* in the query result.

Scope

Works for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Syntax

- *EMA(N, <eventAttribute>) - eventAttribute* must be a numerical type.
- *EMA(N,Function(<eventAttribute>)))* – The *Function* must return a numerical value and cannot be an aggregate attribute.
- Any query using EMA needs to have one time aggregation field. Supported time aggregation fields are:
  - Hourly (Event Receive Hour)
  - Daily (Event receive Date)

  - Weekly (Event Receive Week)
  - Monthly(Event Receive Month)
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, String Manipulation Functions
- In ClickHouse, these nested function categories are allowed:
  - Conversion Functions, String Manipulation Functions
- **Display Condition** (i.e. HAVING in SQL Language) is not supported

Example

Raw Data

Event Receive Time	Host Name	CPU Util
Apr 19, 2023, 12:00:00 PM	Host1	3.00%
Apr 19, 2023, 12:15:00 PM	Host1	2.37%
Apr 19, 2023, 12:30:00 PM	Host1	2.68%
Apr 19, 2023, 12:45:00 PM	Host1	2.72%
Apr 19, 2023, 13:00:00 PM	Host1	2.55%
Apr 19, 2023, 13:15:00 PM	Host1	2.43%
Apr 19, 2023, 13:30:00 PM	Host1	2.50%
Apr 19, 2023, 13:45:00 PM	Host1	2.74%
Apr 19, 2023, 14:00:00 PM	Host1	2.64%
Apr 19, 2023, 14:15:00 PM	Host1	3.74%
Apr 19, 2023, 14:30:00 PM	Host1	2.12%
Apr 19, 2023, 14:45:00 PM	Host1	3.84%

EMA Query Result:

Event Receive Hour	Host Name	EMA(2,CPU Util)
Apr 19, 2023, 12:00:00 PM	Host1	2.69
Apr 19, 2023, 13:00:00 PM	Host1	2.60
Apr 19, 2023, 14:00:00 PM	Host1	2.92

SMA Function

Description

SMA(N,<eventAttribute>) returns *Simple Moving Average* over N previous values of the numerical valued <*eventAttribute*> among all events matching the query criteria.

Scope

Available for ClickHouse and Elasticsearch queries from release 7.0.0 onwards.

Syntax

- *SMA(N, <eventAttribute>) - eventAttribute* must be a numerical type.
- *SMA(N,Function(<eventAttribute>)))* – The *Function* must return a numerical value and cannot be an aggregate attribute.
- Any query using SMA must have one of the time aggregation field. Supported time aggregation fields are:
  - Hourly (Event Receive Hour)
  - Daily (Event receive Date)
  - Weekly (Event Receive Week)
  - Monthly(Event Receive Month)
- In Elasticsearch these nested function categories are allowed:
  - Extraction Function, String Manipulation Functions
- In ClickHouse, these nested function categories are allowed:
  - Conversion Functions, String Manipulation Functions
- **Display Condition** (i.e. HAVING in SQL Language) is not supported.

Example

Raw Data

Event Receive Time	Host Name	CPU Util
Apr 19, 2023, 12:00:00 PM	Host1	3.00%
Apr 19, 2023, 12:15:00 PM	Host1	2.37%
Apr 19, 2023, 12:30:00 PM	Host1	2.68%
Apr 19, 2023, 12:45:00 PM	Host1	2.72%
Apr 19, 2023, 13:00:00 PM	Host1	2.55%
Apr 19, 2023, 13:15:00 PM	Host1	2.43%
Apr 19, 2023, 13:30:00 PM	Host1	2.50%
Apr 19, 2023, 13:45:00 PM	Host1	2.74%
Apr 19, 2023, 14:00:00 PM	Host1	2.64%
Apr 19, 2023, 14:15:00 PM	Host1	3.74%
Apr 19, 2023, 14:30:00 PM	Host1	2.12%
Apr 19, 2023, 14:45:00 PM	Host1	3.84%

SMA Query Result

Event Receive Hour	Host Name	SMA(2, CPU Util)
Apr 19, 2023, 12:00:00 PM	Host1	2.69
Apr 19, 2023, 13:00:00 PM	Host1	2.62
Apr 19, 2023, 14:00:00 PM	Host1	2.85

Knowledge Base

- FortiSIEM Event Attribute to CEF Key Mapping
- FortiSIEM Event Categories and Handling
- Public Domain Built-in Rules

FortiSIEM Event Attribute to CEF Key Mapping

FortiSIEM forwards externally received logs and internally generated events/incidents to an external system via CEF formatted syslog.

FortiSIEM Event Attribute to CEF Key Mappings

FortiSIEM event attributes	CEF key	Notes
appCategory	cat	
appTransportProto	app	
count	cnt	
destAction	act	
destDomain	destinationDnsDomain	
destIntfName	deviceOutboundInterface	
destIpAddr	destinationTranslated Address	
destIpAddr	dst	
destIpPort	destinationTranslatedPort	
destIpPort	dpt	
destMACAddr	dmac	
destName	dhost	
destServiceName	destinationServiceName	
destUser	duser	
destUserId	duid	
destUserPriv	dpriv	
deviceIdentification	deviceExternalId	
deviceTime	rt	
domain	deviceDnsDomain	
endTime	end	
errReason	reason	
extEventId	externalId	
fileAccess	filePermission	
fileId	fileId	
fileModificationTime	fileModificationTime	
fileName	fname	
filePath	filePath	
fileSize	fsize	
fileType	fileType	
hashCode	fileHash	

FortiSIEM event attributes	CEF key	Notes
hostIpAddr	dvc	
hostMACAddr	dvcmac	
hostName	dvchost	
httpCookie	requestCookies	
httpMethod	requestMethod	
httpReferrer	requestContext	
httpUserAgent	requestClientApplication	
infoURL	request	
ipProto	proto	
msg	msg	
postNATHostIpAddr	deviceTranslatedAddress	
postNATSrcIpAddr	sourceTranslatedAddress	
postNATSrcIpPort	sourceTranslatedPort	
procId	dvcpid	
procName	deviceProcessName	
recvBytes	in	
sentBytes	out	
serviceName	sourceServiceName	
srcDomain	sourceDnsDomain	
srcIntfName	deviceInboundInterface	
intfName	deviceInboundInterface	
srcIpAddr	src	
srcIpPort	spt	
srcMACAddr	smac	
srcName	shost	
srcUser	suser	
srcUserPriv	spriv	
startTime	start	
targetProcId	dpid	
targetProcName	dproc	

Mapping to CEF Custom Attributes

FortiSIEM event attributes	CEF key	Notes
supervisorName	cs1Label = SupervisorHostName	
customer	cs2Label = CustomerName	
incidentDetail	cs3Label=IncidentDetail	
ruleName	cs4Label=RuleName	
inIncidentEventIdList	cs5Label=IncidentEventIDList	
phCustId	cn1Label=CustomerID	
incidentId	cn2Label=IncidentID	
	type	0 = base event; 2 = incident

FortiSIEM Event Categories and Handling

This topic provides a brief description of various types of event categories in FortiSIEM.

System Event Category	Description	Counted in EPS License	phstatus -a outout	Stored in DB?
0	External events and not flow events (e.g. syslog, SNMP Trap, Event pulling)	Yes	EPS	Yes
1	Incidents (events that begin with PH_ RULE)	No	EPS INTERNAL	No
2	FortiSIEM Audit Events (events that begin with PH_AUDIT)	No	EPS INTERNAL	Yes
3	FortiSIEM Internal system logs, free format	No	EPS INTERNAL	Yes
4	External flow events (Netflow, Sflow)	Yes	EPS	Yes
5	FortiSIEM Internal health events for summary dashboards	No	EPS INTERNAL	Yes
6	FortiSIEM Performance Monitoring events (events that begin with PH_DEV_MON)	Yes	EPS PERF	Yes
7	AO Beaconing events	No	EPS INTERNAL	Yes
8	FortiSIEM Real Time Performance Probe Events	No	EPS INTERNAL	No
99	FortiSIEM Internal Rule Engine	No	EPS INTERNAL	No
1,100	Incidents (events that begin with PH_ RULE). When using "System Event Category IN 1,100" the eventDB is queried for incident events. Every time an incident is triggered, including subsequent triggers of the same incident an event is stored in the eventDB.	No	EPS INTERNAL	Yes

Public Domain Built-in Rules

The following table shows the public domain built-in rules incorporated into FortiSIEM.

Rules that are adopted from the SIGMA rule set are licensed under the Detection Rule License available here.

FortiSIEM Rule	Author	Source Link
AWS CloudTrail Important Changes	vitaliy0x1	https://github.com/SigmaHQ/sigma/blob/master/rules/cloud/aws_cloudtrail_disable_logging.yml
AWS EC2 Userdata Download	faloker	https://github.com/SigmaHQ/sigma/blob/master/rules/cloud/aws_ec2_download_userdata.yml
Linux: Attempt to Disable Crowdstrike Service	Ömer Günal	https://github.com/SigmaHQ/sigma/blob/master/rules/linux/lnx_security_tools_disabling.yml
Linux: Attempt to Disable CarbonBlack Service	Ömer Günal	https://github.com/SigmaHQ/sigma/blob/master/rules/linux/lnx_security_tools_disabling.yml
Windows: Turla Service Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apt_carbonpaper_turla.yml
Windows: StoneDrill Service Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apt_stonedrill.yml
Windows: Turla PNG Dropper Service	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apt_turla_service_png.yml
Windows: smbexec.py Service Installation	Omer Faruk Celik	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_hack_smbexec.yml
Windows: Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_service_installs.yml
Windows: Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_meterpreter_or_cobaltstrike_getsystem_service_installation.yml
Windows: PsExec Tool Execution	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_tool_psexec.yml

FortiSIEM Rule	Author	Source Link
Windows: Local User Creation	Patrick Bareiss	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_creation.yml
Windows: Local User Creation Via Powershell	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_create_local_user.yml
Windows: Local User Creation Via Net.exe	Endgame, JHasenbusch (adapted to sigma for oscd.community)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_net_user_add.yml
Windows: Suspicious ANONYMOUS LOGON Local Account Created	James Pemberton / @4A616D6573	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_local_anon_logon_created.yml
Windows: New or Renamed User Account with $ in Attribute SamAccountName	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_new_or_renamed_user_account_with_dollar_sign.yml
Windows: AD Privileged Users or Groups Reconnaissance	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_account_discovery.yml
Windows: Administrator and Domain Admin Reconnaissance	Florian Roth (rule), Jack Croock (method)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_net_recon_activity.yml
Windows: Access to ADMIN$ Share	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_admin_share_access.yml
Windows: Login with WMI	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_wmi_login.yml
Windows: Admin User Remote Logon	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_admin_rdp_login.yml
Windows: RDP Login from Localhost	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_localhost_login.yml

FortiSIEM Rule	Author	Source Link
Windows: Interactive Logon to Server Systems	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_interactive_logons.yml
Windows: Pass the Hash Activity	Ilias el Matani (rule), The Information Assurance Directorate at the NSA (method)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_pass_the_hash.yml
Windows: Pass the Hash Activity 2	Dave Kennedy, Jeff Warren (method) / David Vassallo (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_pass_the_hash_2.yml
Windows: Successful Overpass the Hash Attempt	Roberto Rodriguez (source), Dominik Schaudel (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_overpass_the_hash.yml
Windows: RottenPotato Like Attack Pattern	@SBousseaden, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_rottenpotato.yml
Windows: Hacktool Ruler	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_ruler.yml
Windows: Metasploit SMB Authentication	Chakib Gzenayi (@Chak092), Hosni Mribah	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_metasploit_authentication.yml
Windows: Kerberos Manipulation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_kerberos_manipulation.yml
Windows: Suspicious Kerberos RC4 Ticket Encryption	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_rc4_kerberos.yml
Windows: Persistence and Execution at Scale via GPO Scheduled Task	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_GPO_scheduledtasks.yml

FortiSIEM Rule	Author	Source Link
Windows: Powerview Add-DomainObjectAcl DCSync AD Extend Right	Samir Bousseaden; Roberto Rodriguez @Cyb3rWard0g; oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_account_backdoor_dcsync_rights.yml
Windows: AD Object WriteDAC Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_object_writedac_access.yml
Windows: Active Directory Replication from Non Machine Account	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_replication_non_machine_account.yml
Windows: AD User Enumeration	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_user_enumeration.yml
Windows: Enabled User Right in AD to Control User Objects	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_active_directory_user_control.yml
Windows: Eventlog Cleared	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_eventlog_cleared.yml
Windows: MSHTA Suspicious Execution 01	Diego Perez (@darkquassar), Markus Neis, Swisscom (Improve Rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_mshta_execution.yml
Windows: Dumpert Process Dumper	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_hack_dumpert.yml
Windows: Blue Mockingbird	Trent Liffick (@tliffick)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_blue_mockingbird.yml
Windows: Windows PowerShell Web Request	James Pemberton / @4A616D6573	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/win_powershell_web_request.yml
Windows: DNS Tunnel Technique from MuddyWater	@caliskanfurkan_	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_apt_muddywater_dnstunnel.yml

FortiSIEM Rule	Author	Source Link
Windows: Advanced IP Scanner Detected	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_advanced_ip_scanner.yml
Windows: APT29 Detected	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_apt29_thinktanks.yml
Windows: Baby Shark Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_babyshark.yml
Windows: Judgement Panda Credential Access Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_bear_activity_gtr19.yml
Windows: Logon Scripts - UserInitMprLogon Script	Tom Uetlschi (@c_APT_ure)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_logon_scripts_userinitmprlogonscript_proc.yml
Windows: BlueMashroom DLL Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_bluemashroom.yml
Windows: Password Change on Directory Service Restore Mode DSRM Account	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_dsrm_password_change.yml
Windows: Account Tampering - Suspicious Failed Logon Reasons	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logon_reasons.yml
Windows: Backup Catalog Deleted	Florian Roth (rule), Tom U. @c_APT_ure (collection)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_backup_delete.yml
Windows: Failed Code Integrity Checks	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_codeintegrity_check_failure.yml
Windows: DHCP Server Loaded the CallOut DLL	Dimitrios Slamaris	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_dhcp_config.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious LDAP-Attributes Used	xknow @xknow_infosec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_ldap_dataexchange.yml
Windows: Password Dumper Activity on LSASS		https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_lsass_dump.yml
Windows: Generic Password Dumper Activity on LSASS	Roberto Rodriguez, Teymur Kheirkhabarov, Dimitrios Slamaris, Mark Russinovich, Aleksey Potapov, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_lsass_dump_generic.yml
Windows: Suspicious PsExec Execution	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_psexec.yml
Windows: Suspicious Access to Sensitive File Extensions	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_raccess_sensitive_fext.yml
Windows: Secure Deletion with SDelete	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_sdelete.yml
Windows: Unauthorized System Time Modification	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_time_modification.yml
Windows: Windows Defender Exclusion Set	@BarryShooshooga	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_defender_bypass.yml
Windows: Windows Pcap Driver Installed	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_pcap_drivers.yml

FortiSIEM Rule	Author	Source Link
Windows: Weak Encryption Enabled and Kerberoast	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_enable_weak_encryption.yml
Windows: Remote Task Creation via ATSVC Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_atsvc_task.yml
Windows: Chafer Activity	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_chafer_mar18.yml
Windows: WMIExec VBS Script	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_cloudhopper.yml
Windows: CrackMapExecWin Activity	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_dragonfly.yml
Windows: Elise Backdoor	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_elise.yml
Windows: Emissary Panda Malware SLLauncher Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_emissarypanda_sep19.yml
Windows: Empire Monkey Activity	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_empiremonkey.yml
Windows: Equation Group DLL-U Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_equationgroup_dll_u_load.yml
Windows: EvilNum Golden Chickens Deployment via OCX Files	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_evilnum_jul20.yml
Windows: GALLIUM Artefacts Via Hash Match	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_gallium.yml

FortiSIEM Rule	Author	Source Link
Windows: GALLIUM Artefacts Via Hash and Process Match	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_gallium.yml
Windows: Windows Credential Editor Startup	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_hack_wce.yml
Windows: Greenbug Campaign Indicators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_greenbug_may20.yml
Windows: Hurricane Panda Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_hurricane_panda.yml
Windows: Judgement Panda Exfiltration Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_judgement_panda_gtr19.yml
Windows: Ke3chang Registry Key Modifications	Markus Neis, Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_ke3chang_regadd.yml
Windows: Lazarus Session Highjacker	Trent Liffick (@tliffick), Bartlomiej Czyz (@bczyz1)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_lazarus_session_highjack.yml
Windows: Mustang Panda Dropper Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_mustangpanda.yml
Windows: Defrag Deactivation	Florian Roth, Bartlomiej Czyz (@bczyz1)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_slingshot.yml
Windows: Sofacy Trojan Loader Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_sofacy.yml
Windows: Ps.exe Renamed SysInternals Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_ta17_293a_ps.yml

FortiSIEM Rule	Author	Source Link
Windows: TAIDOOR RAT DLL Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_taidoor.yml
Windows: TropicTrooper Campaign November 2018	@41thexplorer, Microsoft Defender ATP	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_tropictrooper.yml
Windows: Turla Group Commands May 2020	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_turla_comrat_may20.yml
Windows: Unidentified Attacker November 2018 Activity 1	@41thexplorer, Microsoft Defender ATP	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_unidentified_nov_18.yml
Windows: Unidentified Attacker November 2018 Activity 2	@41thexplorer, Microsoft Defender ATP	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_unidentified_nov_18.yml
Windows: Winnti Malware HK University Campaign	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_winnti_mal_hk_jan20.yml
Windows: Winnti Pipemon Characteristics	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_winnti_pipemon.yml
Windows: Operation Wocao Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_wocao.yml
Windows: ZxShell Malware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_zxshell.yml
Windows: Active Directory User Backdoors	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_ad_user_backdoors.yml
Windows: Mimikatz DC Sync	Benjamin Delpy, Florian Roth, Scott Dermott	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dcsync.yml

FortiSIEM Rule	Author	Source Link
Windows: Windows Event Auditing Disabled	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_disable_event_logging.yml
Windows: DPAPI Domain Backup Key Extraction	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dpapi_domain_backupkey_extraction.yml
Windows: DPAPI Domain Master Key Backup Attempt	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dpapi_domain_masterkey_backup_attempt.yml
Windows: External Disk Drive or USB Storage Device	Keith Wright	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_external_device.yml
Windows: Possible Impacket SecretDump Remote Activity	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_impacket_secretdump.yml
Windows: Obfuscated Powershell IEX invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_invoke_obfuscation_obfuscated_iex_services.yml
Windows: First Time Seen Remote Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_lm_namedpipe.yml
Windows: LSASS Access from Non-System Account	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_lsass_access_non_system_account.yml
Windows: Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_creddumper.yml
Windows: WCE wceaux dll Access	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_wceaux_dll.yml

FortiSIEM Rule	Author	Source Link
Windows: MMC20 Lateral Movement	@2xxeformyshirt (Security Risk Advisors) - rule; Teymur Kheirkhabarov (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mmc20_lateral_movement.yml
Windows: NetNTLM Downgrade Attack	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_net_ntlm_downgrade.yml
Windows: Denied Access To Remote Desktop	Pushkarev Dmitry	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_not_allowed_rdp_access.yml
Windows: Possible DCShadow	Ilyas Ochkov, oscd.community, Chakib Gzenayi (@Chak092), Hosni Mribah	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_possible_dc_shadow.yml
Windows: Protected Storage Service Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_protected_storage_service_access.yml
Windows: Scanner PoC for CVE-2019-0708 RDP RCE Vuln	Florian Roth (rule), Adam Bradbury (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_bluekeep_poc_scanner.yml
Windows: RDP over Reverse SSH Tunnel	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_reverse_tunnel.yml
Windows: Register new Logon Process by Rubeus	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_register_new_logon_process_by_rubeus.yml
Windows: Remote PowerShell Sessions	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_remote_powershell_session.yml
Windows: Remote Registry Management Using Reg Utility	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_remote_registry_management_using_reg_utility.yml

FortiSIEM Rule	Author	Source Link
Windows: SAM Registry Hive Handle Request	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_sam_registry_hive_handle_request.yml
Windows: SCM Database Handle Failure	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_scm_database_handle_failure.yml
Windows: SCM Database Privileged Operation	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_scm_database_privileged_operation.yml
Windows: Addition of Domain Trusts	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_add_domain_trust.yml
Windows: Addition of SID History to Active Directory Object	Thomas Patzke, @atc_project (improvements)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_add_sid_history.yml
Windows: Failed Logon From Public IP	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logon_source.yml
Windows: Failed Logins with Different Accounts from Single Source System	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logons_single_source.yml
Windows: Remote Service Activity via SVCCTL Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_svcctl_remote_service.yml
Windows: SysKey Registry Keys Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_syskey_registry_access.yml
Windows: Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_tap_driver_installation.yml
Windows: Transferring Files with Credential Data via Network Shares	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_transferring_files_with_credential_data_via_network_shares.yml

FortiSIEM Rule	Author	Source Link
Windows: User Added to Local Administrators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_added_to_local_administrators.yml
Windows: Failed to Call Privileged Service LsaRegisterLogon Process	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_couldnt_call_privileged_service_lsaregisterlogonprocess.yml
Windows: Suspicious Driver Loaded By User	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_driver_loaded.yml
Windows: Suspicious Driver Load from Temp	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/driver_load/sysmon_susp_driver_load.yml
Windows: File Created with System Process Name	Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_creation_system_file.yml
Windows: Credential Dump Tools Dropped Files	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_cred_dump_tools_dropped_files.yml
Windows: Detection of SafetyKatz	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_ghostpack_safetykatz.yml
Windows: LSASS Memory Dump File Creation	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_lsass_memory_dump_file_creation.yml
Windows: Microsoft Office Add-In Loading	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_office_persistence.yml
Windows: QuarksPwDump Dump File	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_quarkspw_filedump.yml
Windows: RedMimicry Winnti Playbook Dropped File	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_redmimicry_winnti_filedrop.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious ADSI-Cache Usage By Unknown Tool	xknow @xknow_infosec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_adsi_cache_usage.yml
Windows: Suspicious desktop.ini Action	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_desktop_ini.yml
Windows: Suspicious PROCEXP152 sys File Created In TMP	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_procexplorer_driver_created_in_tmp_folder.yml
Windows: Hijack Legit RDP Session to Move Laterally	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_tsclient_filewrite_startup.yml
Windows: Windows Web shell Creation	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_webshell_creation_detect.yml
Windows: WMI Persistence - Script Event Consumer File Write	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_wmi_persistence_script_event_consumer_write.yml
Windows: Suspicious Desktopimgdownldr Target File	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/win_susp_desktopimgdownldr_file.yml
Windows: In-memory PowerShell	Tom Kern, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_in_memory_powershell.yml
Windows: PowerShell load within System Management Automation DLL	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_powershell_execution_moduleload.yml
Windows: Fax Service DLL Search Order Hijack	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_fax_dll.yml

FortiSIEM Rule	Author	Source Link
Windows: Possible Process Hollowing Image Loading	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_image_load.yml
Windows: .NET DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_assembly_dll_load.yml
Windows: CLR DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_clr_dll_load.yml
Windows: GAC DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_gac_dll_load.yml
Windows: Active Directory Parsing DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dsparse_dll_load.yml
Windows: Active Directory Kerberos DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_kerberos_dll_load.yml
Windows: VBA DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_winword_vbadll_load.yml
Windows: WMI DLL Loaded Via Office Applications	Michael R. (@nahamike01)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_winword_wmidll_load.yml
Windows: Loading dbghelp dbgcore DLL from Suspicious Processes	Perez Diego (@darkquassar), oscd.community, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_suspicious_dbghelp_dbgcore_load.yml
Windows: Svchost DLL Search Order Hijack	SBousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_svchost_dll_search_order_hijack.yml

FortiSIEM Rule	Author	Source Link
Windows: Unsigned Image Loaded Into LSASS Process	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_unsigned_image_loaded_into_lsass.yml
Windows: Suspicious WMI Modules Loaded	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_wmi_module_load.yml
Windows: WMI Persistence - Command Line Event Consumer	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_wmi_persistence_commandline_event_consumer.yml
Windows: Registry Entries Found For Azorult Malware	Trent Liffick	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/mal_azorult_reg.yml
Windows: Registry Entries Found For FlowCloud Malware	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_flowcloud.yml
Windows: Octopus Scanner Malware Detected	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_octopus_scanner.yml
Windows: Registry Entries For Ursnif Malware	megan201296	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_ursnif.yml
Windows: Dllhost.exe Internet Connection	bartblaze	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_dllhost_net_connections.yml
Windows: Suspicious Typical Malware Back Connect Ports	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_malware_backconnect_ports.yml
Windows: Notepad Making Network Connection	EagleEye Team	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_notepad_network_connection.yml
Windows: PowerShell Network Connections	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_powershell_network_connection.yml

FortiSIEM Rule	Author	Source Link
Windows: RDP Over Reverse SSH Tunnel	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rdp_reverse_tunnel.yml
Windows: Regsvr32 Network Activity	Dmitriy Lifanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_regsvr32_network_activity.yml
Windows: Remote PowerShell Session	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_remote_powershell_session_network.yml
Windows: Rundll32 Internet Connection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rundll32_net_connections.yml
Windows: Network Connections From Executables in Suspicious Program Locations	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_susp_prog_location_network_connection.yml
Windows: Outbound RDP Connections From Suspicious Executables	Markus Neis - Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_susp_rdp.yml
Windows: Outbound Kerberos Connection From Suspicious Executables	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_suspicious_outbound_kerberos_connection.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_suspicious_outbound_kerberos_connection.yml
Windows: Microsoft Binary Github Communication	Michael Haag (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_win_binary_github_com.yml
Windows: Microsoft Binary Suspicious External Communication	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_win_binary_susp_com.yml

FortiSIEM Rule	Author	Source Link
Windows: Data Compressed - Powershell	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_data_compressed.yml
Windows: Dnscat Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_dnscat_execution.yml
Windows: PowerShell Credential Prompt	John Lambert (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_prompt_credentials.yml
Windows: Powershell Profile ps1 Modification	HieuTT35	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_suspicious_profile_create.yml
Windows: Credentials Dumping Tools Accessing LSASS Memory	Florian Roth, Roberto Rodriguez, Dimitrios Slamaris, Mark Russinovich, Thomas Patzke, Teymur Kheirkhabarov, Sherif Eldeeb, James Dickenson, Aleksey Potapov, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_cred_dump_lsass_access.yml
Windows: Suspicious In-Memory Module Execution	Perez Diego (@darkquassar), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_in_memory_assembly_execution.yml
Windows: Suspect Svchost Memory Asccess	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_invoke_phantom.yml
Windows: Credential Dumping by LaZagne	Bhabesh Raj	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_lazagne_cred_dump_lsass_access.yml
Windows: LSASS Memory Dump	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_lsass_memdump.yml

FortiSIEM Rule	Author	Source Link
Windows: Malware Shellcode in Verclsid Target Process	John Lambert (tech), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_malware_verclsid_shellcode.yml
Windows: Mimikatz through Windows Remote Management	Patryk Prauze - ING Tech	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_mimikatz_trough_winrm.yml
Windows: Turla Group Lateral Movement	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_turla_commands.yml
Windows: Hiding Files with Attrib exe	Sami Ruohonen	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_attrib_hiding_files.yml
Windows: Modification of Boot Configuration	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_bootconf_mod.yml
Windows: SquiblyTwo	Markus Neis / Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_bypass_squiblytwo.yml
Windows: Change Default File Association	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_change_default_file_association.yml
Windows: Cmdkey Cached Credentials Recon	jmallette	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_cmdkey_recon.yml
Windows: CMSTP UAC Bypass via COM Object Access	Nik Seetharaman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_cmstp_com_object_access.yml
Windows: Cmd exe CommandLine Path Traversal	xknow @xknow_infosec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_commandline_path_traversal.yml
Windows: Unusual Control Panel Items	Kyaw Min Thein, Furkan Caliskan (@caliskanfurkan_)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_control_panel_item.yml

FortiSIEM Rule	Author	Source Link
Windows: Copying Sensitive Files with Credential Data	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_copying_sensitive_files_with_credential_data.yml
Windows: Fireball Archer Malware Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_fireball.yml
Windows: Maze Ransomware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_maze_ransomware.yml
Windows: Snatch Ransomware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_snatch_ransomware.yml
Windows: Data Compressed - rar.exe	Timur Zinniatullin, E.M. Anhaus, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_data_compressed_with_rar.yml
Windows: DNS Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dns_exfiltration_tools_execution.yml
Windows: DNSCat2 Powershell Detection Via Process Creation	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dnscat2_powershell_implementation.yml
Windows: Encoded FromBase64String	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_encoded_frombase64string.yml
Windows: Encoded IEX	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_encoded_iex.yml
Windows: COMPlus-ETWEnabled Command Line Arguments	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_etw_modification_cmdline.yml

FortiSIEM Rule	Author	Source Link
Windows: Disabling ETW Trace	@neu5ron, Florian Roth, Jonhnathan Ribeiro, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_etw_trace_evasion.yml
Windows: Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exfiltration_and_tunneling_tools_execution.yml
Windows: Exploit for CVE-2015-1641	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2015_1641.yml
Windows: Exploit for CVE-2017-0261	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_0261.yml
Windows: Droppers Exploiting CVE-2017-11882	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_11882.yml
Windows: Exploit for CVE-2017-8759	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_8759.yml
Windows: Exploiting SetupComplete.cmd CVE-2019-1378	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2019_1378.yml
Windows: Exploiting CVE-2019-1388	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2019_1388.yml
Windows: Exploited CVE-2020-10189 Zoho ManageEngine	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_10189.yml
Windows: Suspicious PrinterPorts Creation CVE-2020-1048	EagleEye Team, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_1048.yml

FortiSIEM Rule	Author	Source Link
Windows: DNS RCE CVE-2020-1350	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_1350.yml
Windows: File/Folder Permissions Modifications Via Command line Utilities	Jakob Weinzettl, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_file_permission_modifications.yml
Windows: Grabbing Sensitive Hives via Reg Utility	Teymur Kheirkhabarov, Endgame, JHasenbusch, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_grabbing_sensitive_hives_via_reg.yml
Windows: Bloodhound and Sharphound Hack Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_bloodhound.yml
Windows: Koadic Execution	wagga	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_koadic.yml
Windows: Rubeus Hack Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_rubeus.yml
Windows: SecurityXploded Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_secutyxploded.yml
Windows: HH exe Execution	E.M. Anhaus (originally from Atomic Blue Detections, Dan Beavin), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hh_chm.yml
Windows: CreateMiniDump Hacktool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hktl_createminidump.yml
Windows: HTML Help Shell Spawn	Maxim Pavlunin	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_html_help_spawn.yml
Windows: Suspicious HWP Sub Processes	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hwp_exploits.yml

FortiSIEM Rule	Author	Source Link
Windows: Impacket Lateralization Detection	Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_impacket_lateralization.yml
Windows: Indirect Command Execution	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_indirect_cmd.yml
Windows: Suspicious Debugger Registration Cmdline	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_install_reg_debugger_backdoor.yml
Windows: Interactive AT Job	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_interactive_at.yml
Windows: Invoke-Obfuscation Obfuscated IEX Invocation when to create process	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_invoke_obfuscation_obfuscated_iex_commandline.yml
Windows: Windows Kernel and 3rd-Party Drivers Exploits Token Stealing	Teymur Kheirkhabarov (source), Daniil Yugoslavskiy (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_kernel_and_3rd_party_drivers_exploits_token_stealing.yml
Windows: MSHTA Spawned by SVCHOST	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_lethalhta.yml
Windows: Local Accounts Discovery	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_local_system_owner_account_discovery.yml

FortiSIEM Rule	Author	Source Link
Windows: LSASS Memory Dumping Using procdump	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_lsass_dump.yml
Windows: Adwind Remote Access Tool JRAT	Florian Roth, Tom Ueltschi	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mal_adwind.yml
Windows: Dridex Process Pattern	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_dridex.yml
Windows: DTRACK Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_dtrack.yml
Windows: Emotet Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_emotet.yml
Windows: Formbook Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_formbook.yml
Windows: QBot Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_qbot.yml
Windows: Ryuk Ransomware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_ryuk.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_ryuk.yml
Windows: WScript or CScript Dropper	Margaritis Dimitrios (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_script_dropper.yml
Windows: Trickbot Malware Recon Activity	David Burkett, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_trickbot_recon_activity.yml
Windows: WannaCry Ransomware	Florian Roth (rule), Tom U. @c_APT_ure (collection)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_wannacry.yml

FortiSIEM Rule	Author	Source Link
Windows: MavInject Process Injection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mavinject_proc_inj.yml
Windows: Meterpreter or Cobalt Strike Getsystem Service Start	Teymur Kheirkhabarov, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_meterpreter_or_cobaltstrike_getsystem_service_start.yml
Windows: Mimikatz Command Line	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mimikatz_command_line.yml
Windows: MMC Spawning Windows Shell	Karneades, Swisscom CSIRT	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mmc_spawn_shell.yml
Windows: Mouse Lock Credential Gathering	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mouse_lock.yml
Windows: Mshta JavaScript Execution	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mshta_javascript.yml
Windows: MSHTA Spawning Windows Shell	Michael Haag	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mshta_spawn_shell.yml
Windows: Quick Execution of a Series of Suspicious Commands	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_multiple_suspicious_cli.yml
Windows: Windows Network Enumeration	Endgame, JHasenbusch (ported for oscd.community)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_net_enum.yml
Windows: Netsh RDP Port Opening	Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_allow_port_rdp.yml
Windows: Netsh Port or Application Allowed	Markus Neis, Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_fw_add.yml

FortiSIEM Rule	Author	Source Link
Windows: Netsh Program Allowed with Suspcious Location	Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_fw_add_susp_image.yml
Windows: Network Trace with netsh exe	Kutepov Anton, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_packet_capture.yml
Windows: Netsh Port Forwarding	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_port_fwd.yml
Windows: Netsh RDP Port Forwarding	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_port_fwd_3389.yml
Windows: Harvesting of Wifi Credentials Using netsh exe	Andreas Hunkeler (@Karneades)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_wifi_credential_harvesting.yml
Windows: Network Sniffing	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_network_sniffing.yml
Windows: New Service Creation via sc.exe	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_new_service_creation.yml
Windows: Non Interactive PowerShell	Roberto Rodriguez @Cyb3rWard0g (rule), oscd.community (improvements)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_non_interactive_powershell.yml
Windows: Microsoft Office Product Spawning Windows Shell	Michael Haag, Florian Roth, Markus Neis, Elastic, FPT.EagleEye Team	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_shell.yml
Windows: MS Office Product Spawning Exe in User Directory	Jason Lynch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_spawn_exe_from_users_directory.yml

FortiSIEM Rule	Author	Source Link
Windows: Executable Used by PlugX in Uncommon Location	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_plugx_susp_exe_locations.yml
Windows: Possible Applocker Bypass	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_possible_applocker_bypass.yml
Windows: Detection of Possible Rotten Potato	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_possible_privilege_escalation_using_rotten_potato.yml
Windows: Powershell AMSI Bypass via NET Reflection	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_amsi_bypass.yml
Windows: Audio Capture via PowerShell	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_audio_capture.yml
Windows: PowerShell Base64 Encoded Shellcode	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_b64_shellcode.yml
Windows: Suspicious Bitsadmin Job via PowerShell	Endgame, JHasenbusch (ported to sigma for oscd.community)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_bitsjob.yml
Windows: Suspicious PowerShell Execution via DLL	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_dll_execution.yml
Windows: PowerShell Downgrade Attack	Harish Segar (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_downgrade_attack.yml
Windows: Download via PowerShell URL	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_download.yml

FortiSIEM Rule	Author	Source Link
Windows: FromBase64String Command Line	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_frombase64string.yml
Windows: Suspicious PowerShell Parameter Substring	Florian Roth (rule), Daniel Bohannon (idea), Roberto Rodriguez (Fix)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_suspicious_parameter_variation.yml
Windows: Suspicious XOR Encoded PowerShell Command Line	Sami Ruohonen, Harish Segar (improvement)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_xor_commandline.yml
Windows: Default PowerSploit and Empire Schtasks Persistence	Markus Neis, @Karneades	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powersploit_empire_schtasks.yml
Windows: Windows Important Process Started From Suspicious Parent Directories	vburov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_proc_wrong_parent.yml
Windows: Bitsadmin Download	Michael Haag	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_process_creation_bitsadmin_download.yml
Windows: Process Dump via Rundll32 and Comsvcs dll	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_process_dump_rundll32_comsvcs.yml
Windows: PsExec Service Start	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_psexesvc_start.yml
Windows: Query Registry	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_query_registry.yml
Windows: MSTSC Shadowing	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_rdp_hijack_shadowing.yml
Windows: RedMimicry Winnti Playbook Execute	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_redmimicry_winnti_proc.yml

FortiSIEM Rule	Author	Source Link
Windows: Remote PowerShell Session for creating process	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_remote_powershell_session_process.yml
Windows: System Time Discovery	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_remote_time_discovery.yml
Windows: Renamed Binary	Matthew Green - @mgreen27, Ecco, James Pemberton / @4A616D6573, oscd.community (improvements), Andreas Hunkeler (@Karneades)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_binary.yml
Windows: Highly Relevant Renamed Binary	Matthew Green - @mgreen27, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_binary_highly_relevant.yml
Windows: Renamed jusched exe	Markus Neis, Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_jusched.yml
Windows: Execution of Renamed PaExec	Jason Lynch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_paexec.yml
Windows: Renamed PowerShell	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_powershell.yml
Windows: Renamed ProcDump	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_procdump.yml
Windows: Renamed PsExec	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_psexec.yml
Windows: Run PowerShell Script from ADS	Sergey Soldatov, Kaspersky Lab, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_run_powershell_script_from_ads.yml

FortiSIEM Rule	Author	Source Link
Windows: Possible Shim Database Persistence via sdbinst exe	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_sdbinst_shim_persistence.yml
Windows: Manual Service Execution	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_service_execution.yml
Windows: Stop Windows Service	Jakob Weinzettl, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_service_stop.yml
Windows: Shadow Copies Access via Symlink	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_access_symlink.yml
Windows: Shadow Copies Creation Using Operating Systems Utilities	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_creation.yml
Windows: Shadow Copies Deletion Using Operating Systems Utilities	Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_deletion.yml
Windows: Windows Shell Spawning Suspicious Program	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shell_spawn_susp_program.yml
Windows: SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_silenttrinity_stage_use.yml
Windows: Audio Capture via SoundRecorder	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_soundrec_audio_capture.yml

FortiSIEM Rule	Author	Source Link
Windows: Possible SPN Enumeration	Markus Neis, keepwatch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_spn_enum.yml
Windows: Possible Ransomware or Unauthorized MBR Modifications	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_bcdedit.yml
Windows: Application Allowlisting Bypass via Bginfo	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_bginfo.yml
Windows: Suspicious Calculator Usage	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_calc.yml
Windows: Possible App Allowlisting Bypass via WinDbg CDB as a Shell code Runner	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cdb.yml
Windows: Suspicious Certutil Command	Florian Roth, juju4, keepwatch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_certutil_command.yml
Windows: Certutil Encode	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_certutil_encode.yml
Windows: Suspicious Commandline Escape	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cli_escape.yml
Windows: Command Line Execution with Suspicious URL and AppData Strings	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cmd_http_appdata.yml
Windows: Suspicious Code Page Switch	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_codepage_switch.yml
Windows: Reconnaissance Activity with Net Command	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_commands_recon_activity.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Compression Tool Parameters	Florian Roth, Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_compression_params.yml
Windows: Process Dump via Comsvcs DLL	Modexp (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_comsvcs_procdump.yml
Windows: Copy from Admin Share	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_copy_lateral_movement.yml
Windows: Suspicious Copy From or To System32	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_copy_system32.yml
Windows: Covenant Launcher Indicators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_covenant.yml
Windows: CrackMapExec Command Execution	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_crackmapexec_execution.yml
Windows: CrackMapExec PowerShell Obfuscation	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_crackmapexec_powershell_obfuscation.yml
Windows: Suspicious Parent of Csc.exe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_csc.yml
Windows: Suspicious Csc.exe Source File Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_csc_folder.yml
Windows: Suspicious Curl Usage on Windows	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_download.yml
Windows: Suspicious Curl File Upload	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_fileupload.yml

FortiSIEM Rule	Author	Source Link
Windows: Curl Start Combination	Sreeman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_start_combo.yml
Windows: ZOHO Dctask64 Process Injection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dctask64_proc_inject.yml
Windows: Suspicious Desktopimgdownldr Command	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_desktopimgdownldr.yml
Windows: Devtoolslauncher.exe Executing Specified Binary	Beyu Denis, oscd.community (rule), @_felamos (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_devtoolslauncher.yml
Windows: Direct Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_direct_asep_reg_keys_modification.yml
Windows: Disabled IE Security Features	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_disable_ie_features.yml
Windows: DIT Snapshot Viewer Use	Furkan Caliskan (@caliskanfurkan_)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ditsnap.yml
Windows: Application Allowlisting Bypass via Dnx.exe	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dnx.yml
Windows: Suspicious Double File Extension	Florian Roth (rule), @blu3_team (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_double_extension.yml
Windows: Application Allowlisting Bypass via Dxcap.exe	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dxcap.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Eventlog Clear or Configuration Using Wevtutil or Powershell or Wmic	Ecco, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_eventlog_clear.yml
Windows: Executables Started in Suspicious Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_exec_folder.yml
Windows: Execution in Non-Executable Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_execution_path.yml
Windows: Execution in Webserver Root Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_execution_path_webserver.yml
Windows: Explorer Root Flag Process Tree Break	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_explorer_break_proctree.yml
Windows: Suspicious File Characteristics Due to Missing Fields	Markus Neis, Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_file_characteristics.yml
Windows: Findstr Launching lnk File	Trent Liffick	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_findstr_lnk.yml
Windows: Firewall Disabled via Netsh	Fatih Sirin	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_firewall_disable.yml
Windows: Fsutil Suspicious Invocation	Ecco, E.M. Anhaus, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_fsutil_usage.yml
Windows: Suspicious GUP.exe Usage	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_gup.yml
Windows: IIS Native-Code Module Command Line Installation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_iss_module_install.yml

FortiSIEM Rule	Author	Source Link
Windows: Windows Defender Download Activity	Matthew Matchen	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_mpcmdrun_download.yml
Windows: Suspicious MsiExec Directory	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msiexec_cwd.yml
Windows: MsiExec Web Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msiexec_web_install.yml
Windows: Malicious Payload Download via Office Binaries	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msoffice.yml
Windows: Net.exe Execution For Discovery	Michael Haag, Mark Woan (improvements), James Pemberton / @4A616D6573 / oscd.community (improvements)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_net_execution.yml
Windows: Suspicious Netsh.DLL Persistence	Victor Sergeev, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_netsh_dll_persistence.yml
Windows: Invocation of Active Directory Diagnostic Tool ntdsutil exe	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ntdsutil.yml
Windows: Application Allowlisting Bypass via DLL Loaded by odbcconf exe	Kirill Kiryanov, Beyu Denis, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_odbcconf.yml
Windows: OpenWith.exe Executing Specified Binary	Beyu Denis, oscd.community (rule), @harr0ey (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_openwith.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Execution from Outlook	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_outlook.yml
Windows: Execution in Outlook Temp Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_outlook_temp.yml
Windows: Ping Hex IP	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ping_hex_ip.yml
Windows: Empire PowerShell Launch Parameters	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_empire_launch.yml
Windows: Empire PowerShell UAC Bypass	Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_empire_uac_bypass.yml
Windows: Suspicious Encoded PowerShell Command Line	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml
Windows: PowerShell Encoded Character Syntax	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_encoded_param.yml
Windows: Malicious Base64 Encoded PowerShell Keywords in Command Lines	John Lambert (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_hidden_b64_cmd.yml
Windows: Suspicious PowerShell Invocation Based on Parent Process	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_parent_combo.yml
Windows: Suspicious PowerShell Parent Process	Teymur Kheirkhabarov, Harish Segar (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_parent_process.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Use of Procdump	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_procdump.yml
Windows: Programs starting from Suspicious Location	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_prog_location_process_starts.yml
Windows: PowerShell Script Run in AppData	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ps_appdata.yml
Windows: PowerShell DownloadFile	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ps_downloadfile.yml
Windows: Psr.exe Capture Screenshots	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_psr_capture_screenshots.yml
Windows: Rar with Password or Compression Level	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rar_flags.yml
Windows: Suspicious RASdial Activity	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rasdial_activity.yml
Windows: Suspicious Reconnaissance Activity via net group or localgroup	Florian Roth, omkar72	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_recon_activity.yml
Windows: Suspicious Regsvr32 Usage	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_regsvr32_anomalies.yml
Windows: Regsvr32 Flags Anomaly	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_regsvr32_flags_anomaly.yml
Windows: Renamed ZOHO Dctask64	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_renamed_dctask64.yml

FortiSIEM Rule	Author	Source Link
Windows: Renamed SysInternals Debug View	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_renamed_debugview.yml
Windows: Suspicious Process Start Locations	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_run_locations.yml
Windows: Suspicious Arguments in Rundll32 Usage	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rundll32_activity.yml
Windows: Suspicious DLL Call by Ordinal	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rundll32_by_ordinal.yml
Windows: Scheduled Task Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_schtask_creation.yml
Windows: WSF JSE JS VBA VBE File Execution	Michael Haag	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_script_execution.yml
Windows: Suspicious Service Path Modification	Victor Sergeev, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_service_path_modification.yml
Windows: Squirrel Lolbin	Karneades / Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_squirrel_lolbin.yml
Windows: Suspicious Svchost Process	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost.yml
Windows: Suspect Svchost Activity	David Burkett	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost_no_cli.yml
Windows: Sysprep on AppData Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_sysprep_appdata.yml
Windows: Suspicious SYSVOL Domain Group Policy Access	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_sysvol_access.yml

FortiSIEM Rule	Author	Source Link
Windows: Taskmgr Created By Local SYSTEM Account	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_taskmgr_localsystem.yml
Windows: Process Launch from Taskmgr	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_taskmgr_parent.yml
Windows: Suspicious tscon.exe Created By Local SYSTEM Account	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_tscon_localsystem.yml
Windows: Suspicious RDP Redirect Using tscon.exe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_tscon_rdp_redirect.yml
Windows: Suspicious Use of CSharp Interactive Console	Michael R. (@nahamike01)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_use_of_csharp_console.yml
Windows: Suspicious Userinit Child Process	Florian Roth (rule), Samir Bousseaden (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_userinit_child.yml
Windows: Whoami Execution	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_whoami.yml
Windows: Suspicious WMI Execution	Michael Haag, Florian Roth, juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_wmi_execution.yml
Windows: Sysmon Driver Unload	Kirill Kiryanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_sysmon_driver_unload.yml
Windows: System File Execution Location Anomaly	Florian Roth, Patrick Bareiss	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_system_exe_anomaly.yml
Windows: Tap Installer Execution	Daniil Yugoslavskiy, Ian Davis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_tap_installer_execution.yml
Windows: Tasks Folder Evasion	Sreeman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_task_folder_evasion.yml

FortiSIEM Rule	Author	Source Link
Windows: Terminal Service Process Spawn	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_termserv_proc_spawn.yml
Windows: Domain Trust Discovery	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community, omkar72	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dsquery_domain_trust_discovery.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_trust_discovery.yml
Windows: Bypass UAC via CMSTP	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_cmstp.yml
Windows: Bypass UAC via Fodhelper.exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_fodhelper.yml
Windows: Bypass UAC via WSReset exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_wsreset.yml
Windows: Possible Privilege Escalation via Weak Service Permissions	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_using_sc_to_change_sevice_image_path_by_non_admin.yml
Windows: Java Running with Remote Debugging	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_vul_java_remote_debugging.yml
Windows: Webshell Detection With Command Line Keywords	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_detection.yml

FortiSIEM Rule	Author	Source Link
Windows: Webshell Recon Detection Via CommandLine Processes	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_recon_detection.yml
Windows: Shells Spawned by Web Servers	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_spawn.yml
Windows: Run Whoami as SYSTEM	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_whoami_as_system.yml
Windows: Windows 10 Scheduled Task SandboxEscaper 0-day	Olaf Hartong	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_win10_sched_task_0day.yml
Windows: WMI Backdoor Exchange Transport Agent	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_backdoor_exchange_transport_agent.yml
Windows: WMI Persistence - Script Event Consumer	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_persistence_script_event_consumer.yml
Windows: WMI Spawning Windows PowerShell	Markus Neis / @Karneades	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_spwns_powershell.yml
Windows: Wmiprvse Spawning Process	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmiprvse_spawning_process.yml
Windows: Microsoft Workflow Compiler	Nik Seetharaman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_workflow_compiler.yml
Windows: Wsreset UAC Bypass	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wsreset_uac_bypass.yml
Windows: XSL Script Processing	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_xsl_script_processing.yml

FortiSIEM Rule	Author	Source Link
Windows: Leviathan Registry Key Activity	Aidan Bracher	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apt_leviathan.yml
Windows: OceanLotus Registry Activity	megan201296	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apt_oceanlotus_registry.yml
Windows: Pandemic Registry Key	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apt_pandemic.yml
Windows: Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_asep_reg_keys_modification.yml
Windows: Suspicious New Printer Ports in Registry CVE-2020-1048	EagleEye Team, Florian Roth, NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_cve-2020-1048.yml
Windows: DHCP Callout DLL Installation	Dimitrios Slamaris	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_dhcp_calloutdll.yml
Windows: Disable Security Events Logging Adding Reg Key MiniNt	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_disable_security_events_logging_adding_reg_key_minint.yml
Windows: DNS ServerLevelPlugin Dll Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_dns_serverlevelplugindll.yml
Windows: COMPlus-ETWEnabled Registry Modification	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_etw_modification.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_etw_disabled.yml
Windows: Windows Credential Editor Install Via Registry	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_hack_wce_reg.yml

FortiSIEM Rule	Author	Source Link
Windows: Logon Scripts UserInitMprLogon Script Registry	Tom Uetschi (@c_APT_ure)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_logon_scripts_userinitmprlogonscript_reg.yml
Windows: Narrator s Feedback-Hub Persistence	Dmitriy Lifanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_narrator_feedback_persistance.yml
Windows: New DLL Added to AppCertDlls Registry Key	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_new_dll_added_to_appcertdlls_registry_key.yml
Windows: New DLL Added to AppInit-DLLs Registry Key	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_new_dll_added_to_appinit_dlls_registry_key.yml
Windows: Possible Privilege Escalation via Service Permissions Weakness	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_possible_privilege_escalation_via_service_registry_permissions_weakness.yml
Windows: RDP Registry Modification	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_registry_modification.yml
Windows: RDP Sensitive Settings Changed	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_settings_hijack.yml
Windows: RedMimicry Winnti Playbook Registry Manipulation	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_redmimicry_winnti_reg.yml
Windows: Office Security Settings Changed	Trent Liffick (@tliffick)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_reg_office_security.yml
Windows: Windows Registry Persistence COM Key Linking	Kutepov Anton, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_persistence_key_linking.yml

FortiSIEM Rule	Author	Source Link
Windows: Windows Registry Persistence COM Search Order Hijacking	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_persistence_search_order.yml
Windows: Windows Registry Trust Record Modification	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_trust_record_modification.yml
Windows: Security Support Provider SSP Added to LSA Configuration	iwillkeepwatch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_ssp_added_lsa_config.yml
Windows: Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_stickykey_like_backdoor.yml
Windows: Suspicious RUN Key from Download	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_download_run_key.yml
Windows: DLL Load via LSASS	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_lsass_dll_load.yml
Windows: Suspicious Camera and Microphone Access	Den Iuzvyk	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_mic_cam_access.yml
Windows: Registry Persistence via Explorer Run Key	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_reg_persist_explorer_run.yml
Windows: New RUN Key Pointing to Suspicious Folder	Florian Roth, Markus Neis, Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_run_key_img_folder.yml
Windows: Suspicious Service Installed	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_service_installed.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Keyboard Layout Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_suspicious_keyboard_layout_load.yml
Windows: Usage of Sysinternals Tools	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_sysinternals_eula_accepted.yml
Windows: UAC Bypass via Event Viewer	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_uac_bypass_eventvwr.yml
Windows: UAC Bypass via Sdclt	Omer Yampel	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_uac_bypass_sdclt.yml
Windows: Registry Persistence Mechanisms	Karneades	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_win_reg_persistence.yml
Windows: Azure Browser SSO Abuse	Den Iuzvyk	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_abusing_azure_browser_sso.yml
Windows: Executable in ADS	Florian Roth, @0xrawsec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_ads_executable.yml
Windows: Alternate PowerShell Hosts Pipe	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_alternate_powershell_hosts_pipe.yml
Windows: Turla Group Named Pipes	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_apt_turla_namedpipes.yml
Windows: CactusTorch Remote Thread Creation	@SBousseaden (detection), Thomas Patzke (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cactustorch.yml
Windows: CMSTP Execution	Nik Seetharaman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_cmstp_execution.yml
Windows: CobaltStrike Process Injection	Olaf Hartong, Florian Roth, Aleksey Potapov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cobaltstrike_process_injection.yml

FortiSIEM Rule	Author	Source Link
Windows: CreateRemoteThread API and LoadLibrary	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_createremotethread_loadlibrary.yml
Windows: Cred Dump Tools Via Named Pipes	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cred_dump_tools_named_pipes.yml
Windows: Malicious Named Pipe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_mal_namedpipes.yml
Windows: Password Dumper Remote Thread in LSASS	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_password_dumper_lsass.yml
Windows: Possible DNS Rebinding	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_possible_dns_rebinding.yml
Windows: Raw Disk Access Using Illegitimate Tools	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_raw_disk_access_using_illegitimate_tools.yml
Windows: PowerShell Rundll32 Remote Thread Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_susp_powershell_rundll32.yml
Windows: Suspicious Remote Thread Created	Perez Diego (@darkquassar), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_suspicious_remote_thread.yml
Windows: WMI Event Subscription	Tom Uetlschi (@c_APT_ure)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_wmi_event_subscription.yml
Windows: Suspicious Scripting in a WMI Consumer	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_wmi_susp_scripting.yml

License Enforcement

This section describes how FortiSIEM enforces CMDB Device license, Agent license, EPS License and Raw Event Size Based License.

- CMDB Device
- Agent
- Events Per Second (EPS)
- Raw Event Size

CMDB Device License Enforcement

Customer purchases an overall CMDB Device license, which specifies how many managed devices can be stored in CMDB. Managed devices can send logs and can be monitored. In an MSSP environment, customer can set a device limit for a specific organization in **Admin > Setup > Organizations > Edit** or **New > Max Devices**. The following device types are excluded from license:

- Devices > Mobile
- Devices > VoIP
- Devices > Decommission
- Devices with Status = Unmanaged.

When you try to add a device to the system, either via discovery or manually, then the global device limit and the per-org device limit is enforced. If the limit is reached, then the device is either not added to CMDB or added and set as Unmanaged. If you decommission a managed device, then the license is returned to the pool. If you recommission a device, then a license is consumed.

CMDB Device License is shown in **Admin > License > General** and the usage is shown in **Admin > License > Usage > Device Usage**.

Agent License Enforcement

Customer purchases Agent License, which specifies how many Agents can register and send events. CMDB Device License is shown in **Admin > License > General** and the usage is shown in **Admin > License > Usage > Agent Usage**.

If Agent License limit is reached, then a new Agent cannot register. If Agent license is reduced to lower than the number of registered Agents, then a few agents are randomly unregistered to bring the value lower than licensed limit.

EPS License Enforcement

Mechanism

FortiSIEM is a distributed system consisting of Supervisor, Worker and Collector nodes. Events can be received at any node and the phParser module at that node handles the events and enforces EPS license. An Elastic EPS allocation method distributes unused EPS to the node where it is needed the most.

- Every 3 minutes, phParser module on every node calculates *Incoming* EPS and sends it to the Supervisor node.
- Every 3 minutes, phParser module on Supervisor node collects *Incoming* EPS from all nodes and calculates *Allocated* EPS and *Unused* Events to be used by every node for the next 3 minutes. Unused event is the difference between licensed EPS and incoming EPS accumulated since the system is installed. These parameters are sent to the phParser modules on every node. The following information is used to calculate *Allocated* EPS:
  - Global Licensed EPS
  - Collector Guaranteed EPS (note the total Guaranteed EPS for all Collectors must be less than Global Licensed EPS).
  - Incoming EPS
- For the next 3 minutes, the phParser module enforces license based on *Allocated EPS and Unused Events information received from the Supervisor node*. At the end of 3 minutes, it sends incoming EPS to the Supervisor node and the cycle continues.

Collector enforces Licensed EPS as follows:

- If incoming EPS is *less* than licensed EPS, events are ingested with no event drop.
- If incoming EPS is *more* than licensed EPS, then the following steps are taken.
  - Unused events are allocated.
  - After consuming unused events, if incoming EPS still exceeds (1.1 * Licensed EPS), then incoming events are dropped. For example, if licensed EPS is 5k, so FortiSIEM allows (5000 * 1.1 * 180 = 990000) events in each 3-minute window, after using up unused events. phParser will parse the first 990,000 events and drop the others in the 3-minute window.

Events

phParser on every node generates the following PH_SYSTEM_EPS_NODE event every 3 minutes. To query these system events, the Analytics search filter must also include “System Event Category” = 3.

```
[PH_SYSTEM_EPS_NODE]:[eventSeverity]=PHL_INFO,[fileName]=parserProcess.cpp,
[lineNumber]=6169,[role]=Super,[hostName]=FSM-Host,[incomingEventsPerSec]=10.0,
[peakIncomingEventsPerSec]=35.0,[dropPolicyEvents]=0,[dropPolicyEventsPerSec]=0.0,
[peakDropPolicyEventsPerSec]=0.0,[dropLicenseEvents]=0,[dropLicenseEventsPerSec]=0.0,
[peakDropLicenseEventsPerSec]=0.0,[dropLicenseEventRatio]=0
```

Attributes:

- incomingEventsPerSec: Total received events in 3 minutes divided by 180.
- peakIncomingEventsPerSec: The maximum value of incomingEventsPerSec over all 3-minute periods, since phParser started.
- dropPolicyEvents: The number of events that are dropped by Event Dropping rules in last 3 minutes.
- dropPolicyEventsPerSec: dropPolicyEvents divided by 180.
- peakDropPolicyEventsPerSec: The maximum value of dropPolicyEventsPerSec over all 3-minute periods, since phParser started.
- dropLicenseEvents: The number of events that are dropped because of exceeding license in last 3 minutes.
- dropLicenseEventsPerSec: dropLicenseEvents divided by 180.
- peakDropLicenseEventsPerSec: The maximum value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
- dropLicenseEventRatio: Ratio of dropped events because of license to total incoming events in last 3 minutes.

phParser on Supervisor node generates the following PH_SYSTEM_EPS_ORG event every 3 minutes. This event provides Organization level EPS information by combining information from every node.

```
[PH_SYSTEM_EPS_ORG]:[eventSeverity]=PHL_INFO,[fileName]=parserProcess.cpp,
[lineNumber]=6205,[phCustId]=1,[customer]=Super,[incomingEventsPerSec]=0.000000,
[peakIncomingEventsPerSec]=0.000000,[dropLicenseEventsPerSec]=0.000000,
[peakDropLicenseEventsPerSec]=0.000000,[phLogDetail]=
```

Attributes:

- customer: name of organization
- incomingEventsPerSec: Total received events in 3 minutes divided by 180 for this Organization.
- peakIncomingEventsPerSec: The maximum value of incomingEventsPerSec over all 3-minute periods for this Organization, since phParser started.
- dropLicenseEvents: The number of events that are dropped because of exceeding license in last 3 minutes.
- dropLicenseEventsPerSec: dropLicenseEvents divided by 180.
- peakDropLicenseEventsPerSec: The maximum value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.

phParser on Supervisor node generates the following PH_SYSTEM_EPS_GLOBAL event every 3 minutes. This event provides Global EPS information by combining information from every node.

```
[PH_SYSTEM_EPS_GLOBAL]:[eventSeverity]=PHL_INFO,[fileName]=parserProcess.cpp,
[lineNumber]=6252,[licenseEventsPerSec]=13000,[incomingEventsPerSec]=0.000000,
[peakIncomingEventsPerSec]=0.000000,[dropLicenseEventsPerSec]=0.000000,
[peakDropLicenseEventsPerSec]=0.000000,[unusedEvents]=1897731307,[phLogDetail]=
```

Attributes:

- licenseEventsPerSec: Global licensed events per second
- incomingEventsPerSec: Total received events in 3 minutes divided by 180.
- peakIncomingEventsPerSec: The maximum value of incomingEventsPerSec over all 3-minute periods for this Organization, since phParser started.

- dropLicenseEvents: The number of events that are dropped because of exceeding license in last 3 minutes.
- dropLicenseEventsPerSec: dropLicenseEvents divided by 180.
- peakDropLicenseEventsPerSec: The maximum value of dropLicenseEventsPerSec over all 3-minute periods, since phParser started.
- unusedEvents: difference between licenseEventsPerSec and incomingEventsPerSec accumulated since system installed.

phParser on an event handling node (e.g. a Collector) generates the following PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE event when it starts to drop events.

```
<174>Mar 12 11:33:20 PARSER-HOST phParser[1234]: [PH_SYSTEM_EVENT_RATE_EXCEED_LICENSE]:
[eventSeverity]=PHL_INFO,[procName]=phParser,[fileName]=parserProcess.cpp,
[eventsPerSec]=120.49,[phLogDetail]=120.49 events/sec exceeds licensed event rate of 100
events/sec
```

Attributes:

- eventsPerSec: Total received events per second

phParser on Supervisor node generates the following PH_PARSER_GLOBAL_LICENSE_EXCEED event every 3 minutes, when it sees dropped events.

```
[PH_PARSER_GLOBAL_LICENSE_EXCEED]:[eventSeverity]=PHL_ERROR,
[fileName]=LicenseEnforce.cpp,[lineNumber]=1098,[phLogDetail]=Elastic EPS: global
license has already exceeded, cannot realloc
```

In this case, the following incidents “FortiSIEM EPS License Exceeded” and “External Event Dropped By License” triggers.

Raw Event Size Based License Enforcement

This license type requires FortiSIEM 7.2.2 or later. It is only available for on-premises VM based deployments. License is based on:

- Total Raw event size per day (GB/Day)
- Number of Agents
- Number of UEBA Agents
- FortiGuard IOC

The user is allowed to have 11 violations in a rolling 30-day window. After that, the **Analytics** and **Dashboard** pages are disabled for 1 day.

In this license scheme, users can have as many devices and events per second (EPS) as can be supported by their deployed hardware, without violating the Total Raw event size per day (GB/Day) limits.

Parser Specification

A Parser file is written using XML syntax. It consists of the following sections:

- **General Parsing Patterns**: This is a list of regular expressions of parsing patterns that can be used in parsing instructions.
- **Event Format Recognizer**: This section specifies the condition that a log must match to be able to be parsed by the instructions in this file.
- **Parsing Instructions**: This specifies instructions for parsing the logs matching the Event Format Recognizer.

The overall structure of a Parser XML file is

```
<patternDefinitions> </patternDefinitions>
```

```
<eventFormatRecognizer> </eventFormatRecognizer>
```

```
<parsingInstructions> </parsingInstructions>
```

The following Parser Specification topics are available:

- General Parsing Patterns
- Event Format Recognizer Specification
- Parsing Instructions

General Parsing Patterns

Global Built-in Patterns:

Several built-in patterns are defined – see Built-in Patterns. The names begin with "gPat". One example is the month pattern

```
<pattern name="gPatMon"><![CDATA[Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec|\d
{1,2}]]></pattern>
```

You can then use `gPatMon` directly instead of `"Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec|\d{1,2}"`.

Suppose the log is

```
Nov 28 2007 17:20:48: %ASA-6-302013: Built outbound TCP connection 76118 for
outside:192.168.0.1/80 (192.168.0.1/80) to inside:192.168.20.31/3530 (192.168.0.1/5967)
```

The log is always stored in the temporary variable `_rawMsg`. To pick up the month from `_rawMsg` and store into a local variable `_mon` and the rest of the string into another variable, one can write:

```
<collectFieldsByRegex src="$_rawmsg">
```

```
<regex><![CDATA[<_mon:gPatMon>\s<_body:gPatMesgBody>]]></regex>
```

```
</collectFieldsByRegex>
```

After parsing, _mon is set to Nov and _body is set to "28 2007 17:20:48: %ASA-6-302013: Built outbound TCP connection 76118 for outside:192.168.0.1/80 (192.168.0.1/80) to inside:192.168.20.31/3530 (192.168.0.1/5967)"

The full list of global built-in patterns is here.

Local User defined Patterns:

In addition to the global patterns, you can define your own regular expression patterns for parsing your logs. You can name these patterns, so that they can be re-used later during actual parsing. These can only be used **locally** within this parser. If you want to reuse this pattern in another parser, then you have to repeat the definition in the other parser.

Each pattern has a name and the regular expression pattern within the CDATA section. This the basic syntax:

```
<pattern name="patternName"><!\[CDATA\[pattern\]\]></pattern>
```

This is an example of a pattern definition:

```
<patternDefinitions>
```

```
<pattern name="patIpV4Dot"><!\[CDATA\[\\d{1,3}.\\d{1,3}.\\d{1,3}.\\d{1,3}\]\]></pattern>
```

```
<pattern name="patComm"><!\[CDATA\[\[^,\]+\]\]></pattern>
```

```
<pattern name="patUpDown"><!\[CDATA\[up|down\]\]></pattern>
```

```
<pattern name="patStrEndColon"><!\[CDATA\[\[^:\]*\]\]></pattern>
```

```
</patternDefinitions>
```

You can also write a *long pattern* definition in multiple lines and indicate their order as shown in this example. The value of the `list` attribute should be `begin` in first line and `end` in last line. If there are more than two lines, the attribute should be set to `continue` for the other lines.

The general syntax is:

```
<pattern list="begin" name="myPattern"> <![CDATA[…]]></pattern>
```

```
<pattern list="continue" name="myPattern"><![CDATA[…]]></pattern>
```

```
<pattern list="continue" name="myPattern"><![CDATA[…]]></pattern>
```

```
<pattern list="end" name="myPattern"><![CDATA[…]]></pattern>
```

As an example:

```
<pattern name="patSolarisMod" list="begin"><![CDATA[sshd|login|]]></pattern>
```

```
<pattern name="patSolarisMod" list="continue"><![CDATA[inetd|lpstat|]]></pattern>
```

```
<pattern name="patSolarisMod" list="end"><![CDATA[su|sudo]]></pattern>
```

Event Format Recognizer Specification

The specification for the format recognizer section is:

```
<eventFormatRecognizer><![CDATA[regex_pattern]]></eventFormatRecognizer>
```

In the `regex_pattern` block, a pattern can be directly specified using regex or a previously defined pattern can be referenced. Patterns are defined two places:

- Built-in patterns - see Built-in Patterns for more information.
- Local patterns: Within this section `<patternDefinitions> </patternDefinitions>`

Examples:

1. Cisco ASA Firewalls

   All Cisco ASA events have the pattern `ASA-severity-id` pattern, for example `ASA-6-302013`.

   ```
   <134>Nov 28 2007 17:20:48: %ASA-6-302013: Built outbound TCP connection 76118 for
   outside:192.168.0.1/80 (192.168.0.1/80) to inside:192.168.20.31/3530
   (192.168.0.1/5967
   ```

   For this scenario, the event format recognizer is simple:

   ```
   <eventFormatRecognizer><![CDATA[ASA-d-d+]]></eventFormatRecognizer>
   ```

2. FortiGate Firewalls

   Two examples of FortiGate firewall logs are shown below.

   ```
   <185>Jun  5 10:11:03 date=2016-09-13 time=13:33:19 devname=FGT_Edge
   devid=FGT90D3Z13007389 logid=0419016384 type=utm subtype=ips eventtype=signature
   level=alert vd=root severity=critical srcip=42.83.201.2 srccountry="Taiwan"
   dstip=10.10.50.13 srcintf="wan1" dstintf="HoneyZone" policyid=6 sessionid=51928140
   action=detected proto=6 service="SMB" attack="MS.DCERPC.netAPI32.Buffer.Overflow"
   srcport=2293 dstport=445 direction=outgoing attackid=15995 profile="Honeydrive_
   monitor" ref="http://www.fortinet.com/ids/VID15995" incidentserialno=176226761
   msg="netbios: MS.DCERPC.netAPI32.Buffer.Overflow
   ```

   ```
   <185>date=2023-04-06 time=11:21:20 devname="Fortigate-lab-doe" device_
   id="FGVMULTM23001223" eventtime=1680805281059447154 tz="-0700" logid="0100032002"
   type="event" subtype="system" level="alert" vd="root" logdesc="Admin login failed"
   sn="0" user="root" ui="ssh(172.30.58.81)" method="ssh" srcip=10.1.1.1 dstip=10.1.1.2
   ```

```
action="login" status="failed" reason="name_invalid" msg="Administrator root login
failed from ssh(10.1.1.1) because of invalid user name"
```

The unique format for these logs is highlighted in bold, but since it is too generic, the part of the log leading up to them has to be captured also.

```
<185>Jun  5 10:11:03 date=2016-09-13 time=13:33:19 devname=FGT_Edge devid=FGT…
```

```
<185>date=2023-04-06 time=11:21:20 devname="Fortigate-lab-doe" device_id="FGVM…
```

Note the generic built-in patterns (See Built-in Patterns).

The following patterns define the various FortiGate model prefixes that can be substituted for FGT, FGVM:

- `<pattern name="patFormat1"><![CDATA[(?:APS|FG|FGD|FGP|FGR|FGT|FOSVM|FP [^AX]|FR|LF|LFG|FWF|FW|FGV|FD[^C])[\d\w-]+]]></pattern>`
- `<pattern name="patFormat2"><![CDATA[(?:FGTAWS|FGTAZR|FGVM|F\d+K) [\d\w-]+]]></pattern>`

Then format recognizer for FortiGate logs becomes:

<eventFormatRecognizer>`<![CDATA[(?:^|<:gPatSyslogPRI>|\s)(?:device_id|devid)="? (?:<:patFormat2>|<:patFormat1>)"?\s]]>`**</eventFormatRecognizer>**

3. 3. Cisco IOS Router

   A few samples of Cisco IOS logs are as follows:

```
<190>109219: Jan  9 18:03:35.281: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session:
initiator (192.168.20.33:1876) -- responder (192.168.0.10:445)
```

```
<186>Aug 13 17:39:28:647 UTC: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Gi0/25
with BPDU Guard enabled. Disabling port.)
```

```
<188>84354: Dec  6 08:15:20: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: Admin]
[Source: 192.168.135.125] [localport: 80] [Reason: Login Authentication Failed -
BadPassword] at 08:15:20 PST Mon Dec 6 2020
```

To handle this, the list of all Cisco IOS logging modules must be defined: `FW, SEC, SSH, SEC_LOGIN, SYS, SNMP, STACKMGR, HSRP, LINK, SPANTREE, LINEPROTO`, etc. These patterns can be concatenated together using `begin`, `continue`, `end` primitives.

```
<pattern list="begin" name="patCiscoIOSMod"> <![CDATA[FW|SEC|SSH|SEC_
LOGIN|SYS|SNMP|STACKMGR|HSRP|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA
[LINK|SPANTREE|LINEPROTO|DTP|PARSER|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[CDP|DHCPD|CONTROLLER|PORT_
SECURITY-SP|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[AUTHMGR|MAB|DOT1X|PFINIT|WS_
IPSEC_3|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[PLATFORM_
UCAST|WCCP|ILPOWER|MAC_MOVE|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[CLEAR|DUAL|DHCP_
SNOOPING|STACKMGR|EIGRP|MGBL|ROUTING|SECURITY|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA
[FMANFP|TRACKING|CRYPTO|ENVMON|ISDN|LAPP_ON_MSGS|SW_MATM|SWITCH_QOS_TB|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[OIR-SP|C6KPWR-SP|C6KERRDETECT-
SP|C6KPWR|CFIB|CONST_DIAG-SP|CPU_MONITOR|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[CPU_MONITOR-SP|EARL_L3_ASIC-
SP|EARL_NETFLOW|EC-SP|ETHCNTR|L3_ASIC-DFC3|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[MCAST-SP|MISTRAL-SP|MLS_
STAT|MLS_STAT-SP|MROUTE|PM_SCP|PM_SCP-SP|QM|SYSTEM|]]></pattern>
```

```
<pattern list="continue" name="patCiscoIOSMod"><![CDATA[SYSTEM_CONTROLLER-SP|SYSTEM_
CONTROLLER-SW2_SPSTBY|]]></pattern>
```

```
<pattern list="end" name="patCiscoIOSMod"><![CDATA[BGP|BGP_SESSION|OSPF|C4K_
IOSMODPORTMAN|C4K_REDUNDANCY|C4K_SWITCHINGENGINEMAN|IP|DHCP|PM|SW_DAI|ENTITY_
ALARM]]></pattern>
```

Another pattern is defined:

```
<pattern name="patStrEndColon"><![CDATA[[^:]*]]></pattern>
```

The event recognizer for Cisco IOS can now be defined using the patterns defined above and the built-in patterns (see below):

```
<eventFormatRecognizer><![CDATA[^[^%=]*%<:patCiscoIOSMod>(?:-<:gPatStr>){0,2}-
<:gPatInt>-<:patStrEndColon>:]]></eventFormatRecognizer>
```

Parsing Instructions

The parsing instructions specify how to recognize patterns in a log message and populate parsed event attributes. The dictionary of FortiSIEM event attributes is specified in **Admin > Device Support > Event Attributes**. In addition to the built-in ones (which have **Scope** set to **System**), you can also define your own (with **Scope** set to **User**).

Before storing in event attributes, you might want to store as local variables and perform some operations on the local variables. For readability, local variables should begin with an underscore (_), although this is not enforced.

The following topics are available:

- Setting Event Attributes
- When Construct

- Choose Construct
- Switch Construct

Setting Event Attributes

Setting an Event Attribute to a Constant

```
<setEventAttribute attr="eventSeverity">1</setEventAttribute>
```

Setting an Event Attribute from another variable

The $ symbol is used to specify the content of a variable. In the example below, attribute `hostMACAddr` gets the value stored in the local variable `_mac`.

```
<setEventAttribute attr="hostMACAddr">$_mac</setEventAttribute>
```

An example of a function operating on a local variable before storing into an event attribute is:

```
<setEventAttribute attr="hostMACAddr">normalizeMAC($_mac)</setEventAttribute>
```

`normalizeMAC` is a built-in function defined in Compute Functions.

Setting an Event Attribute by regular expression match

Several Collect and Set functions can be used to set event attributes by matching specific regular expressions on an input string.

See the Collect and Set Functions in Built-in Functions.

When Construct

A When construct can be used to test whether a parsed field matches a value or a regular expression pattern.

Case 1: The following checks whether the `type` field contains 'Success' (case sensitive match) anywhere in the string.

```
<when test="matches($type,'Success')">
```

```
…
```

```
</when>
```

Case 2: The following checks whether the `httpsStatusCode` field begins with 40, e.g. 400-409

```
<when test="matches($httpStatusCode,'^40')">
```

```
…..
```

```
</when>
```

Case 3: The following checks whether the `eventType` field does not contain `PH_SYSTEM` (case sensitive match) anywhere in the string

```
<when test="not_matches($eventType, 'PH_SYSTEM_')">
```

```
</when>
```

Case 4: The following checks whether the `severity` field is 6 or 7.

```
<when test="$severity IN '6,7'">
```

```
…
```

```
</when>
```

Case 5: The following checks whether the `direction` field is 'inbound' (exact case-sensitive match)

```
<when test="$direction = 'inbound'">
```

```
….
```

```
</when>
```

Case 6: The following checks whether the `direction` field is not 'inbound' (exact case-sensitive match)

```
<when test="$direction != 'inbound'">
```

```
….
```

```
</when>
```

Case 7: The following checks whether the `srcIpAddr` field is set to some value.

```
<when test="exist srcIpAddr">
```

```
</when>
```

Case 8: The following checks whether the `srcIpAddr` field is not set to some value.

```
<when test="not_exist srcIpAddr">
```

```
</when>
```

Case 9: The following checks whether the `destIpAddr` field is not in the RFC 1918 private IP range.

```
<when test="not_private_ip destIpAddr">
```

```
</when>
```

Choose Construct

If you want to do successive checks like "if-else" or "if-else if – else if", then you can use the Choose construct.

The format is:

```
<choose>
  <when>
    ...
  </when>
  <when>
    ...
  </when>
  <otherwise>
    ...
  </otherwise>
</choose>
```

If first `<when>` condition matches, then the instructions within that section are executed. Else, the second `<when>` condition is attempted. If none of the when condition matches, then the instructions within the `<otherwise>` section are executed. The `<otherwise>` section is optional.

The following concrete example shows a full choose statement.

```
<choose>
  <when test="$_severity IN '6, 7'">
    <setEventAttribute attr="eventSeverity">1</setEventAttribute>
  </when>

  <when test="$_severity = '1'">
    <setEventAttribute attr="eventSeverity">10</setEventAttribute>
  </when>

  <when test="$_severity = '2'">
    <setEventAttribute attr="eventSeverity">8</setEventAttribute>
  </when>

  <when test="$_severity IN '3, 4'">
    <setEventAttribute attr="eventSeverity">5</setEventAttribute>
  </when>

  <when test="$_severity = '5'">
    <setEventAttribute attr="eventSeverity">2</setEventAttribute>
  </when>
    <otherwise>
```

```
      <setEventAttribute attr="eventSeverity">1</setEventAttribute>
    </otherwise>
</choose>
```

Results of execution:

- If `severity` is 2 then `eventSeverity` is 8.
- If `severity` is 11 then `eventSeverity` is 1.

Switch Construct

The Switch construct enables you to test several regular expression patterns sequentially to find a match. The format is:

```
<switch>
  <case>
    ...
  </case>
  <case>
    ...
  </case>
  <default>
    ...
  </default>
</switch>
```

Inside a Case, only regular expression match is allowed to see if execution will enter that case.

The following example illustrates a Switch statement. Suppose a log can follow two formats. We want to parse each format using a switch statement.

- Log 1: SSH session from 10.1.1.1 on interface Ethernet1 for user Joe terminated normally.
- Log 2: SSH session from 10.1.1.2 on interface Ethernet2 for user Bob disconnected by SSH server, reason: timeout expired.

The following switch statement accomplishes this.

```
<switch>
  <case>
    <collectFieldsByRegex src="$_body">
      <regex><![CDATA[SSH session from <srcIpAddr:gPatIpAddr> on interface
<srcIntfName:gPatStr> for user "<user:gPatStrDQ>" terminated normally]]></regex>
    </collectFieldsByRegex>
    <setEventAttribute attr="eventType">ASA-315011-Logoff</setEventAttribute>
  </case>
  <case>
    <collectFieldsByRegex src="$_body">
      <regex><![CDATA[SSH session from <srcIpAddr:gPatIpAddr> on interface
<srcIntfName:gPatStr> for user "<user:gPatStr>" disconnected by SSH server,
reason:\s+"<errReason:gPatMesgBodyMin>"]]></regex>
    </collectFieldsByRegex>
  </case>
```

```
  <default/>
</switch>
```

For Log 1, the following values are parsed.

- srcIpAddr: 10.1.1.1
- srcIntfName: Ethernet 1
- user: Joe

For Log 2, the following values are parsed.

- SrcIpAddr: 10.1.1.2
- SrcIntfName: Ethernet 2
- user: Bob
- errReason: time out expired

Built-in Patterns

The following built-in patterns are available and can be used in any parser.

- Event Log Patterns
- FQDN Pattern
- Network Patterns
- Time Patterns
- Type Patterns

Event Log Patterns

```
<pattern name="gPatSyslogPRI"><![CDATA[<\d+>]]></pattern>
```

```
<pattern name="gPatMesgBody"><![CDATA[.*]]></pattern>
```

```
<pattern name="gPatMesgBodyMin"><![CDATA[.*?]]></pattern>
```

```
<pattern name="gPatSyslogNGHeader"><![CDATA[\w{3}\s+\d{1,2}\s\d{1,2}:\d{1,2}:\d{1,2}\s\d
{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}]]></pattern>
```

FQDN Pattern

```
<pattern name="gPatFqdn"><![CDATA[\w+[.\w+]+]]></pattern>
```

Network Patterns

```
<pattern name="gPatIpV4Dot"><![CDATA[\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}]]></pattern>
```

```
<pattern name="gPatIpAddr"><![CDATA[[0-9A-Fa-f]{0,4}(?::[0-9A-Fa-f]{0,4}){1,5}:(?:\d{1,3}
(?:\.\d{1,3}){3}|[0-9A-Fa-f]{0,4}(?::[0-9A-Fa-f]{0,4})?)|\d{1,3}(?:\.\d{1,3})
{3}]]></pattern>
```

```
<pattern name="gPatIpPort"><![CDATA[\d{1,5}]]></pattern>
```

```
<pattern name="gPatProto"><![CDATA
[ftp|icmp|tcp|udp|http|ip|smb|smtp|snmp|others|FTP|ICMP|UDP|TCP|HTTP|IP|SMB|SMTP|SNMP|OTHE
RS]]></pattern>
```

Time Patterns

```
<pattern name="gPatMon"><![CDATA[Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec|\d
{1,2}]]></pattern>
```

```
<pattern name="gPatMonNum"><![CDATA[\d{1,2}]]></pattern>
```

```
<pattern name="gPatDay"><![CDATA[\d{1,2}]]></pattern>
```

```
<pattern name="gPatTime"><![CDATA[\d{1,2}:\d{1,2}:\d{1,2}]]></pattern>
```

```
<pattern name="gPatYear"><![CDATA[\d{2,4}]]></pattern>
```

```
<pattern name="gPatMSec"><![CDATA[\d{1,3}]]></pattern>
```

```
<pattern name="gPatTimeMSec"><![CDATA[\d{1,2}:\d{1,2}:\d{1,2}\.\d{1,3}]]></pattern>
```

```
<pattern name="gPatTimeZone"><![CDATA[Z|UTC|GMT|[+-]\d{1,2}:?\d{2}]]></pattern>
```

```
<pattern name="gPatWeekday"><![CDATA[Mon|Tue|Wed|Thu|Fri|Sat|Sun]]></pattern>
```

Type Patterns

```
<pattern name="gPatWord"><![CDATA[\w+]]></pattern>
<pattern name="gPatStr"><![CDATA[[^\s]*]]></pattern>
<pattern name="gPatHostName"><![CDATA[[\w.-]+]]></pattern>
<pattern name="gPatStrComma"><![CDATA[[^,]*]]></pattern>
<pattern name="gPatStrLeftParen"><![CDATA[[^\(]*]]></pattern>
<pattern name="gPatStrRightSB"><![CDATA[[^\]]*]]></pattern>
<pattern name="gPatInt"><![CDATA[\d+]]></pattern>
<pattern name="gPatSpace"><![CDATA[\s+]]></pattern>
<pattern name="gPatStrEndColon"><![CDATA[[^:]*]]></pattern>
<pattern name="gPatStrSQ"><![CDATA[[^']*]]></pattern>
<pattern name="gPatStrDQ"><![CDATA[[^"]*]]></pattern>
<pattern name="gPatSentence"><![CDATA[\w[\s+\w]*]]></pattern>
```

Built-in Functions

- Collect and Set Functions
- Compute Functions
- Conversion Functions
- Extraction Functions
- String Functions

Collect and Set Functions

These functions can be used to extract fields from log fragments.

1. collectFieldsByRegex
2. collectFieldsByKeyValuePair
3. collectAndSetAttrByKeyValuePair
4. collectAndSetAttrByKeyValuePairMultiValue
5. collectAndSetAttrByPos
6. collectAndSetAttrByPosWithQuotes
7. collectAndSetAttrByPosWithNestedSep
8. collectFieldsByCsvFile
9. collectFieldsByCsvValue
10. collectFieldsBySNMPTrap
11. collectAndSetAttrBySymbol
12. collectAndSetAttrByXPath
13. collectFieldsByXPath
14. collectAndSetAttrFromAnotherEvent
15. collectAndSetAttrByJSON
16. collectAndSetAttrByJsonArray
17. collectAndSetAttrByJsonSymbol

The following are deprecated

1. collectAndSetAttrByRegex
2. collectAndSetAttrByKeyValPair

collectFieldsByRegex

Description: This function extracts event fields from a raw message using regular expression.

Syntax:

```
<collectFieldsByRegex src="$Arg1">
  <regex>
         <Arg2>
  </regex>
</collectFieldsByRegex>
```

`Arg1`: Input string from which fields are to be extracted.

Arg2: Regular expression for extracting the fields from input string.

Example:

Suppose the following log fragment is saved in _body variable.

```
Configured from console by vty1 (192.168.29.8)
```

The following example uses collectFieldsByRegex to extract user and srcIpAddr variables from _body.

```
<collectAndSetAttrByRegex src="$_body">
  <regex><![CDATA[Configured from console by <user:gPatWord> \(<srcIpAddr:gPatIpAddr>\)]]>

  </regex>
</collectAndSetAttrByRegex>
```

After execution:

- user is set to vty1.
- srcIpAddr is set to 192.168.29.8.

collectFieldsByKeyValuePair

Description: This function extracts Key values when logs are structured as

```
Key1 = value1 <separator> Key2 = value2 <separator> ....
```

You can specify the separator between key and value (e.g. '=') and also the separator between Key-value construct (e.g. <separator> above).

Note:

Regarding collectFieldsByKeyValuePair vs. collectAndSetAttrByKeyValuePair per the lines below:

1. <collectFieldsByKeyValuePair sep="$Arg3" kvsep="$Arg2" src="$Arg1">
2. <collectAndSetAttrByKeyValuePair sep="$Arg2" src="$Arg1">

In general, **2**(collectAndSetAttrByKeyValuePair) can be added before **1** (collectFieldsByKeyValuePair) as **2** is simpler, working for most cases, whereas **1** is more efficient, but also more strict.

Syntax:

```
<collectFieldsByKeyValuePair sep="Arg3" kvsep="Arg2" src="$Arg1">
      <attrKeyMap attr="Arg5" key="Arg4"/>
      <attrKeyMap attr="Arg7" key="Arg6"/>
</collectFieldsByKeyValuePair>
```

Arg1: Input string from which fields are to be extracted.

Arg2: Character for separating Key and Value.

Arg3: Character for separating two key value pairs.

Arg4: Key in the event.

Arg5: FortiSIEM event attribute to which the value should be set.

Arg6: Key in the event.

Arg7: FortiSIEM event attribute to which the value should be set.

Example:

Suppose the following log fragment is stored in local _body variable.

```
time=21:02:30 filename=readme.txt mname="MSIL/Small.AXD!tr.dldr"
```

The collectFieldsByKeyValuePair function extracts readme.txt and MSIL/Small.AXD!tr.dldr from the _body attribute. The separator is space character.

```
<collectFieldsByKeyValuePair sep=" " kvsep="=" src="$_body">
        <attrKeyMap attr="fileName" key="filename"/>
       <attrKeyMap attr="virusName" key="mname"/>
</collectFieldsByKeyValuePair>
```

After execution:

- filename is set to readme.txt.
- virusName is set to MSIL/Small.AXD!tr.dldr.

collectAndSetAttrByKeyValuePair

Description: This function extracts Key values when logs are structured as

Key1 = value1 <separator> Key2 = value2 <separator> ....

Note: Regarding collectFieldsByKeyValuePair vs. collectAndSetAttrByKeyValuePair per the lines below:

1. <collectFieldsByKeyValuePair sep="$Arg3" kvsep="$Arg2" src="$Arg1">
2. <collectAndSetAttrByKeyValuePair sep="$Arg2" src="$Arg1">

In general, **2**(collectAndSetAttrByKeyValuePair) can be added before **1** (collectFieldsByKeyValuePair) as **2** is simpler, working for most cases, whereas **1** is more efficient, but also more strict.

Syntax:

```
<collectAndSetAttrByKeyValuePair sep="$Arg2" src="$Arg1">
  <attrKeyMap attr="Arg4" key="Arg3"/>
  <attrKeyMap attr="Arg6" key="Arg5"/>
</collectFieldsByKeyValuePair>
```

Note:

Arg1: Input string from which fields are to be extracted.

Arg2: Character for separating two key value pairs.

Arg3: Key in the event.

Arg4: FortiSIEM event attribute to which the value should be set.

Arg5: Key in the event.

Arg6: FortiSIEM event attribute to which the value should be set.

Example:

Suppose the following log fragment is stored in local _body variable.

```
[time]=21:02:30 [filename]=readme.txt [mname]="MSIL/Small.AXD!tr.dldr"
```

The collectFieldsByKeyValuePair function extracts readme.txt and MSIL/Small.AXD!tr.dldr from the _body attribute. The separator is " [".

```
<collectAndSetAttrByKeyValuePair sep=" [" src="$_body">
  <attrKeyMap attr="fileName" key="[filename]="/>
  <attrKeyMap attr="virusName" key="[mname]="/>
</collectAndSetAttrByKeyValuePair>
```

After execution:

- filename is set to readme.txt.
- virusName is set to MSIL/Small.AXD!tr.dldr.

collectAndSetAttrByKeyValuePairMultiValue

Description: This function extends collectAndSetAttrByKeyValuePair, by allowing *multiple* values for the same key. If the log contains multiple values for the same key, the function will store all the values for the same key in a comma separated string format and assign it to the specified variable.

Syntax:

```
<collectAndSetAttrByKeyValuePairMultiValue src="$Arg1" sep="Arg2">
         <attrKeyMap attr="Arg4" key="Arg3"/>
         <attrKeyMap attr="Arg6" key="Arg5"/>
</collectAndSetAttrByKeyValuePairMultiValue>
```

Arg1: Input string from which fields are to be extracted.

Arg2: Character separator for multiple values.

Arg3: Key in the event.

Arg4: FortiSIEM event attribute to which the value of Arg3 should be set.

Arg5: Key in the event.

Arg6: FortiSIEM event attribute to which the value of Arg5 should be set.

Example:

Suppose the following log fragment is set in _body variable. Note there are 2 values for NetworkDeviceGroups key.

```
... , NetworkDeviceGroups=Routers; NetworkDeviceGroups=Firewalls, ...
```

The following example extracts the values of all NetworkDeviceGroups= from _body

```
<collectAndSetAttrByKeyValuePairMultiValue src="$_body" sep=";">
         <attrKeyMap attr="deviceType" key="NetworkDeviceGroups="/>
</collectAndSetAttrByKeyValuePairMultiValue>
```

After execution:

```
deviceType: Routers; Firewalls
```

collectAndSetAttrByPos

Description: Certain application logs, such as those from Microsoft IIS, are structured as a list of values with a separator. There are no corresponding Keys in the log. These logs can be parsed using the collectAndSetAttrByPos function. It splits the string by the separator, and extracts values by position.

Syntax:

```
<collectAndSetAttrByPos sep="Arg2" src="$Arg1">
        <attrPosMap attr="Arg4" pos="Arg3"/>
        <attrPosMap attr="Arg6" pos="Arg5"/>
</collectAndSetAttrByPos>
```

Arg1: Input string from which fields are to be extracted.

Arg2: Character separator for multiple values.

Arg3: Position in the event.

Arg4: FortiSIEM event attribute to which the value in position Arg3 must be set.

Arg5: Key in the event.

Arg6: FortiSIEM event attribute to which the value in position Arg5 must be set.

Example:

Suppose the following log fragment is set in _detail variable:

```
OB JOY *FILESRV CRTSTRMFIL QPWFSERVSO LNS0811 000112 00023
```

The following example extracts the 2 attributes from _detail variable, based on position and using space as a separator.

```
<collectAndSetAttrByPos sep=" " src="$_detail">
  <attrPosMap attr="opName" pos="4"/>
  <attrPosMap attr="seqNum" pos="8"/>
</collectAndSetAttrByPos>
```

After execution:

```
opName: CRTSTRMFIL
```

```
seqNum: 00023
```

collectAndSetAttrByPosWithQuotes

Description: This function extends the `collectAndSetAttrByPos` function with the added functionality that it can extract quoted string values.

Syntax:

```
<collectAndSetAttrByPosWithQuotes src="$Arg1" sep="Arg2" quo="Arg3">
      <attrPosMap attr="Arg5" pos="Arg4"/>
      <attrPosMap attr="Arg7" pos="Arg6"/>
</collectAndSetAttrByPosWithQuotes>
```

`Arg1`: Input string from which fields are to be extracted.

`Arg2`: Character separator for multiple values.

`Arg3`: Quote Character.

`Arg4`: Position in the event.

`Arg5`: FortiSIEM event attribute to which the value in position `Arg4` must be set.

`Arg6`: Key in the event.

`Arg7`: FortiSIEM event attribute to which the value in position `Arg6` must be set.

Example:

Suppose the following log fragment is set in `_detail` variable:

```
0,,"Routing and Remote Access Service Policy",
```

The following example extracts the 2 attributes from `_msg` string, based on position and using comma as separator. The double quote here escaped to `"` as for XML standard.

```
<collectAndSetAttrByPosWithQuotes src="$_detail" sep="," quo="&quot;">
      <attrPosMap attr="nasId" pos="1"/>
      <attrPosMap attr="policyName" pos="3"/>
</collectAndSetAttrByPosWithQuotes>
```

After execution:

```
nasId: 0
```

```
policyName: Routing and Remote Access Service Policy
```

collectAndSetAttrByPosWithNestedSep

Description: This function extends `collectAndSetAttrByPosWithQuotes` function by allowing the values to be inside any character pair, e.g. [..] or ".." or {..}.

Syntax:

```
<collectAndSetAttrByPosWithNestedSep src="$Arg1" L1Sep="Arg2" L2Sep="Arg3">
        <attrPosMap attr="Arg5" pos="Arg4"/>
        <attrPosMap attr="Arg7" pos="Arg6"/>
        …..
</collectAndSetAttrByPosWithNestedSep>
```

`Arg1`: Input string from which fields are to be extracted.

`Arg2`: Character separator for multiple values.

`Arg3`: Start and End character pairs separated by comma – values within (start,end) is set to one event attribute, e.g. in the example below: `""` and [] separated by comma.

`Arg4`: Position in the event.

`Arg5`: FortiSIEM event attribute to which the value in position `Arg3` must be set.

`Arg6`: Key in the event.

`Arg7`: FortiSIEM event attribute to which the value in position `Arg5` must be set.

Example:

Suppose the following log fragment is set in `_body` variable:

```
[25/Sep/2015:17:39:43 +0100] GET "http://example.net/ping?" HTTP/1.1 200 356 921
"http://example.com/news/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/44.0.2403.157 Safari/537.36"
```

Note that

- time is within []: `[25/Sep/2015:17:39:43 +0100]`
- URL is within "": `http://example.net/ping?`

To parse this function, you need to specify

- L1Sep: Level 1 separator (in this case space character)
- L2Sep: Level 2 separator (in this case "" or [])

```
<collectAndSetAttrByPosWithNestedSep src="$_body" L1Sep=" " L2Sep="&quot;&quot;,[]">
       <attrPosMap attr="_devTime" pos="1"/>
       <attrPosMap attr="httpMethod" pos="2"/>
       <attrPosMap attr="uriStem" pos="3"/>
       <attrPosMap attr="httpVersion" pos="4"/>
       <attrPosMap attr="httpStatusCode" pos="5"/>
       <attrPosMap attr="recvBytes64" pos="6"/>
       <attrPosMap attr="sentBytes64" pos="7"/>
       <attrPosMap attr="httpReferrer" pos="8"/>
```

```
       <attrPosMap attr="httpUserAgent" pos="9"/>
</collectAndSetAttrByPosWithNestedSep>
```

After execution:

```
_devTime:       25/Sep/2015:17:39:43 +0100
```

```
httpMethod:     GET
```

```
uriStem:        http://example.net/ping?
```

```
httpVersion:    HTTP/1.1
```

```
httpStatusCode: 200
```

```
recvBytes64:    356
```

```
sentBytes64:    921
```

```
httpReferrer:   http://example.com/news/
```

```
httpUserAgent:  Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/44.0.2403.157 Safari/537.36
```

collectFieldsByCsvFile

Description: This function replaces the value of one or more event attributes by looking up a CSV file. A typical use case is to replace error codes in parsed events to descriptions.

Syntax:

```
<collectFieldsByCsvFile file="Arg1" key="$Arg2" reloadInterval="Arg3">
         <attrKeyMap attr="Arg5" column="Arg4"/>
         <attrKeyMap attr="Arg7" column="Arg6"/>
         …
</collectFieldsByCsvFile>
```

`Arg1`: CSV File specified with absolute path containing value mappings.

`Arg2`: FortiSIEM event attribute whose value must be looked up.

`Arg3`: Time in seconds specifying how often the file should be re-read to capture new values.

`Arg4`: Column in CSV file.

`Arg5`: FortiSIEM event attribute to which the value in position `Arg4` must be set.

`Arg6`: Column in CSV file.

`Arg7`: FortiSIEM event attribute to which the value in position `Arg6` must be set.

Note: Column number starts from 0.

Example:

Suppose the csv file: `/tmp/winLogonFailCode2.csv` has 3 columns: Failure Code, Description, Severity:

Failure Code	Description	Severity
0XC000005E	Login failed – No logon servers	3
0XC0000064	Login failed - Misspelled or bad user account	10

Suppose the `subStatus` field in a log is parsed to a value that matches the first column "Failure Code". The following function will look up the corresponding value in the second (respectively third) column and set to `errReason` (respectively `eventSeverity`) field in the log.

Note: The column number starts from 0. So, to get the first column's value, column="0", second column: column="1".

```
<collectFieldsByCsvFile file="/tmp/winLogonFailCode2.csv" key="$subStatus"
reloadInterval="3600">
        <attrKeyMap attr="errReason" column="1"/>
        <attrKeyMap attr="eventSeverity" column="2"/>
</collectFieldsByCsvFile>
```

If `subStatus` is parsed as `0XC000005E`, then

- `errReason` will be set to `"Login failed – No logon servers."`
- `eventSeverity` will be set to `3`.

collectFieldsByCsvValue

Description: This function is similar to `collectFieldsByCsvFile` function, but allows you to look up *multiple* log fields. This is typically done to replace codes to descriptions in parsed events.

Syntax:

```
<collectFieldsByCsvValue file="Arg1" pattern="Arg2" delimiter="Arg3" reloadInterval="Arg4">
       <attrKeyMap attr="Arg5"/>
       <attrKeyMap attr="Arg6"/>
       ….
</collectFieldsByCsvValue>
```

`Arg1`: CSV file specified with absolute path.

`Arg2`: Required pattern for FortiSIEM event attributes.

`Arg3`: Delimiter for updated value, when there are multiple matches.

`Arg4`: Time in seconds specifying how often the file should be re-read to capture new values.

`Arg5`: FortiSIEM event attribute whose value should be matched and updated.

Arg6: FortiSIEM event attribute whose value should be matched and updated.

Example:

Suppose the csv file: /opt/phoenix/data-definition/WindowsServerMessageTable.csv has 2 columns: Code, Description.

Code	Description
%%1538	READ_CONTROL
%%1539	WRITE_DAC
%%1540	WRITE_OWNER

```
<collectFieldsByCsvValue file="/opt/phoenix/data-definition/WindowsServerMessageTable.csv"
pattern="^%%\d+$" delimiter="," reloadInterval="3600">
       <attrKeyMap attr="userPerm"/>
       <attrKeyMap attr="groupPerm"/>
       <attrKeyMap attr="otherPerm"/>
</collectFieldsByCsvValue>
```

If userPerm is parsed as %%1538, then this function will update userPerm to "READ_CONTROL".

If userPerm is parsed as %%1538,%%1539, then this function will update userPerm to "READ_CONTROL,WRITE_DAC".

If groupPerm is parsed as %%1540, then this function will update groupPerm to "WRITE_OWNER".

If groupPerm is parsed as 1540, then this function will not update the value since the pattern (pattern="^%%\d+$") does not match.

collectFieldsBySNMPTrap

Description: This function collects fields from SNMP Traps. This is a version of collectFieldsByKeyValuePair specialized for SNMP Trap.

Syntax:

```
<collectFieldsBySNMPTrap src="$Arg1">
      <attrKeyMap attr="Arg3" key="Arg2"/>
      <attrKeyMap attr="Arg5" key="Arg4"/>
      ….
</collectFieldsBySNMPTrap>
```

Arg1: Input string from which fields are to be extracted.

Arg2: SNMP OID.

Arg3: FortiSIEM event attribute to which the value corresponding to Arg2 must be set to.

Arg4: SNMP OID.

Arg5: FortiSIEM event attribute to which the value corresponding to Arg4 must be set to.

Example:

Suppose the following log fragment is set in _body variable:

```
... SNMPv2-SMI::enterprises.25597.1.1.2.1.9.417081 = STRING: "01:02:03:04:05:06" SNMPv2-
SMI::enterprises.25597.1.1.2.1.36.417081 = STRING: "1.2.3.4" ...
```

The function searches for the Keys in the logs and extracts trailing values, e.g. ignores 417081 in `SNMPv2-SMI::enterprises.25597.1.1.2.1.9.417081`.

```
<collectFieldsBySNMPTrap src="$_body">
      <attrKeyMap attr="srcMACAddr" key="SNMPv2-SMI::enterprises.25597.1.1.2.1.9"/>
      <attrKeyMap attr="srcIpAddr" key="SNMPv2-SMI::enterprises.25597.1.1.2.1.36"/>
</collectFieldsBySNMPTrap>
```

After execution:

```
srcMACAddr: 01:02:03:04:05:06
```

```
srcIpAddr: 1.2.3.4
```

collectAndSetAttrBySymbol

Description: This function collects fields from logs generated by FortiSIEM itself. This is a version of `collectFieldsByKeyValuePair` specialized for FortiSIEM Logs. These logs are in key, value format and the keys are exact event attributes within `[]`, e.g. `[srcIpAddr]=192.168.20.45`.

Syntax:

```
<collectAndSetAttrBySymbol src="$Arg1" sep="Arg2" symStart="Arg3" symEnd="Arg4">
       <excludeAttr>Arg5</excludeAttr>
</collectAndSetAttrBySymbol>
```

`Arg1`: Input string from which fields are to be extracted.

`Arg2`: Separator between Attribute, Value pairs.

`Arg3`: Start of FortiSIEM Event Attribute.

`Arg4`: End of FortiSIEM Event Attribute.

`Arg5`: Comma separated list of FortiSIEM Event Attributes that should not be extracted.

Example:

Suppose the following log fragment is set in _body variable:

```
[phEventCategory]=2,[srcIpAddr]=192.168.20.45,[phCustId]=1,
[sessionId]=0ab028e5b665b36e5944ae48b2f5, [phLogDetail]= this is a standard log
```

The function looks for FortiSIEM Event attributes between "[" and "]=" characters: e.g. `[phEventCategory]=2` search results in `phEventCategory`.

```
<collectAndSetAttrBySymbol src="$_body" sep=",[" symStart="[" symEnd="]=">
       <excludeAttr>phLogDetail</excludeAttr>
</collectAndSetAttrBySymbol>
```

After execution:

```
phEventCategory: 2
```

```
srcIpAddr: 192.168.20.45
```

```
phCustId: 1
```

Note: `phLogDetail` is not parsed as it is in `<excludeAttr>`.

collectAndSetAttrByXPath

Description: This function collects fields from XML formatted logs generated by FortiSIEM. This is similar to `collectAndSetAttrBySymbol`, but for *FortiSIEM generated* XML formatted logs, such as FortiSIEM Incidents. The keys are exact event attributes, e.g. `<deviceTime>1409271060</deviceTime>`.

Syntax:

```
<collectAndSetAttrByXPath src="$Arg1" xpath="Arg2"/>
```

Arg1: Input string from which fields are to be extracted

Arg2: The children of this path should be mapped

Example:

Suppose the following log fragment is set in `_body` variable:

```
<event name="phRuleIncident">
         <deviceTime>1409271060</deviceTime>
         <firstSeenTime>1409271060</firstSeenTime>
         <count>1</count>
</event>
```

The following example searches for `XPath /event/*` and iterates all the returned XML nodes. If the tag name is a FortiSIEM Event Attribute, then it is set to the tag value.

```
<collectAndSetAttrByXPath src="$_body" xpath="/event/*"/>
```

After execution:

```
deviceTime: 1409271060
```

```
firstSeenTime: 1409271060
```

```
count: 1
```

collectFieldsByXPath

Description: This function collects fields from general XML formatted logs. This is a general version of `collectAndSetAttrByXPath`.

Note: It is not a full-featured XPath function. It is mainly for WinOSXmlParser, and does not support non-leaf node with attribute value, such as

```
/root/node[@Name='A']/leaf
```

This is due to performance concerns.

Syntax:

```
<collectFieldsByXPath src="$Arg1">
    <attrKeyMap attr="Arg3" key="Arg2"/>
    <attrKeyMap attr="Arg5" key="Arg4"/>
    …
</collectFieldsByXPath>
```

`Arg1`: Input string from which fields are to be extracted.

`Arg2`: an XPath in the event.

`Arg3`: FortiSIEM Event attribute to which the value of `Arg2` is set.

`Arg4`: an XPath in the event.

`Arg5`: FortiSIEM Event attribute to which the value of `Arg4` is set.

Example:

Suppose the following log fragment is set in _body variable:

```
<Event>
       <System>
              <EventID>5156</EventID>
              <Computer>WIN2019</Computer>
       </System>
       <EventData>
              <Data Name='Application'>System</Data>
       </EventData>
       <RenderingInfo Culture='en-US'>
              <Keywords>
                     <Keyword>Audit Success</Keyword>
              </Keywords>
       </RenderingInfo>
</Event>
```

The following example evaluates each key as XPath, and sets the returned values to specified attributes.

```
<collectFieldsByXPath src="$_xml">
    <attrKeyMap attr="type" key="/Event/RenderingInfo/Keywords/Keyword"/>
    <attrKeyMap attr="appName" key="/Event/EventData/Data[@Name='Application']"/>
```

```
    <attrKeyMap attr="hostName" key="/Event/System/Computer"/>
</collectFieldsByXPath>
```

After execution:

```
type: Audit Success
```

```
appName: System
```

```
hostName: WIN2019
```

collectAndSetAttrFromAnotherEvent

Description: This function enables you to correlate two events by using a common attribute (typically some sort of ID) to set attributes in a latter event from an earlier event. A common case is where the earlier event has user or source IP, but the latter event does not and there is a common logonID to correlate the two events. By populating key information in the latter event, analysts can focus on the second event without having to join the two events during analysis.

Syntax:

```
<collectAndSetAttrFromAnotherEvent AnotherEventType="Arg1">
    <when test="Arg3 = $AnotherEvent.Arg2">
            <setEventAttribute attr="Arg5">$AnotherEvent.Arg4</setEventAttribute>
            <setEventAttribute attr="Arg7">$AnotherEvent.Arg6</setEventAttribute>
    </when>
  </collectAndSetAttrFromAnotherEvent>
```

`Arg1`: Other Event Type.

`Arg2`: Key Attribute of Other Event.

`Arg3`: Attribute of current event that must match `Arg2`.

`Arg4`: Attribute of Other Event.

`Arg5`: Attribute of Current Event that must be set to the value in `Arg4`.

`Arg6`: Attribute of Other Event.

`Arg7`: Attribute of Current Event that must be set to the value in `Arg6`.

Example:

ASA-302013 (inbound TCP connection) – has ipConnId, and srcIpAddr.

```
<134>Nov 28 2007 17:20:48: %ASA-6-302013: Built outbound TCP connection 76118 for
outside:207.68.178.45/80 (207.68.178.45/80) to inside:192.168.20.31/3530
(99.129.50.157/5967)
```

ASA-302014 (teardown TCP connection) - has ipConnId only (the directionality of the network traffic is not clear in the log and has to be derived from the ASA-302013 log).

```
<134>Nov 28 2007 17:22:08: %ASA-6-302014: Teardown TCP connection 76118 for
outside:77.67.126.83/80 to inside:192.168.20.31/3531 duration 0:01:05 bytes 6410 TCP Reset-
I
```

After receiving ASA-302014, the following function looks for ASA-302013 with same ipConnId (76118 in the example above), and sets ASA-302013's srcIpAddr to ASA-302014.

```
<when test="$eventType = 'ASA-302014'">
  <collectAndSetAttrFromAnotherEvent AnotherEventType="ASA-302013">
    <when test="$ipConnId = $AnotherEvent.ipConnId">
      <setEventAttribute attr="srcIpAddr">$AnotherEvent.srcIpAddr</setEventAttribute>
    </when>
  </collectAndSetAttrFromAnotherEvent>
</when>
```

After execution, the ASA-302014 event will have ASA-302013's srcIpAddr value.

collectAndSetAttrByJSON

Description: This function collects fields from a JSON formatted log. This is like collectFieldsByXPath, but for JSON.

Syntax:

```
<collectAndSetAttrByJSON src="$Arg1">
      <attrKeyMap attr="Arg3" key="Arg2"/>
      <attrKeyMap attr="Arg5" key="Arg4"/>
      …..
</collectAndSetAttrByJSON>
```

Arg1: Variable storing the Input string from which fields are to be extracted.

Arg2: JSON Object in the event.

Arg3: FortiSIEM Event attribute to which the value corresponding the path Arg2 must be mapped to.

Arg4: JSON Object in the event.

Arg5: Variable to which the value corresponding the path Arg4 must be mapped to.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

Suppose the following log fragment is set in _body variable:

```
{
  "geo": {
    "city": "ASHBURN",
    "country": "US"
  },
  "httpMessage": {
```

```
    "bytes": "266",
    "host": "www.example.com",
    "method": "GET",
    "path": "/",
    "port": "80"
  }
}
```

The following function parses host and country:

```
<collectAndSetAttrByJSON src="$_body">
      <attrKeyMap attr="hostName" key="httpMessage.host"/>
      <attrKeyMap attr="srcGeoCountry" key="geo.country"/>
</collectAndSetAttrByJSON>
```

After execution:

```
hostName: www.example.com
```

```
srcGeoCountry: US
```

collectAndSetAttrByJsonArray

Description: This function collects multiples values for a key in a JSON array and sets the *concatenated* values to an event attribute.

Syntax:

```
<collectAndSetAttrByJsonArray src="$Arg1" sep="Arg2">
     <attrKeyMap attr="Arg4" key="Arg3"/>
     <attrKeyMap attr="Arg6" key="Arg5"/>
     …
</collectAndSetAttrByJsonArray>
```

`Arg1`: Variable storing the Input string from which fields are to be extracted.

`Arg2`: Separator for concatenated matched value.

`Arg3`: JSON Object in the event.

`Arg4`: Variable to which the value corresponding the path `Arg3` must be mapped to.

`Arg5`: JSON Object in the event.

`Arg6`: Variable to which the value corresponding the path `Arg5` must be mapped to.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

Suppose the following log fragment is set in `_body` variable:

```
{
  "categories": [
    {
      "id": 23,
      "type": "content",
      "label": "Search Engines",
      "integration": false,
      "deprecated": true
    },
    {
      "id": 25,
      "type": "content",
      "label": "Software/Technology",
      "integration": false,
      "deprecated": true
    }
  ]
}
```

The following example extracts all matched values and joins by comma:

```
<collectAndSetAttrByJsonArray src="$_body" sep=",">
     <attrKeyMap attr="webCategories" key="label"/>
</collectAndSetAttrByJsonArray>
```

After execution:

```
webCategories: Search Engines,Software/Technology
```

collectAndSetAttrByJsonSymbol

Description: This is specialized function for collecting fields for *FortiSIEM generated* JSON log. This function is similar to `collectAndSetAttrBySymbol`, but for JSON events. This function can be also considered a special version of `collectAndSetAttrByJSON` where you do not have to specify all the parsed fields, if the key is an FortiSIEM event attribute, then the field is automatically parsed.

Syntax:

```
<collectAndSetAttrByJsonSymbol src="$Arg1">
       <excludeAttr>Arg2</excludeAttr>
</collectAndSetAttrByJsonSymbol>
```

`Arg1`: Variable storing Input string from which fields are to be extracted.

`Arg2`: Comma separated list of values that must be excluded from mapping.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

Suppose the following log fragment is set in `_body` variable:

```
{
  "collectorId": 10007,
  "computer": "WIN-ANQ35T4NKLL",
  "user": "Administrator",
  "phLogDetail":"Standard log"
}
```

The following function parses all the fields except `phLogDetail`. You do not need to specify the parsed fields one by one.

```
<collectAndSetAttrByJsonSymbol src="$_json">
    <excludeAttr>phLogDetail</excludeAttr>
</collectAndSetAttrByJsonSymbol>
```

After execution:

```
collectorId: 10007
```

```
computer: WIN-ANQ35T4NKLL
```

```
user: Administrator
```

collectAndSetAttrByRegex (Deprecated)

This is the same as `collectFieldsByRegex` and is provided for backward compatibility. We recommend the use of `collectFieldsByRegex` function instead of `collectAndSetAttrByRegex` function.

collectAndSetAttrByKeyValPair (Deprecated)

This is the same as `collectAndSetAttrByKeyValuePair` and is provided for backward compatibility. We recommend the use of `collectAndSetAttrByKeyValuePair` function instead.

Compute Functions

These functions perform some computations on parsed values before setting to the event attributes.

1. add
2. calculateDomainEntropy
3. calculateLatency
4. compIntfSecVal
5. combineMsgId
6. compare
7. decodeBase64
8. decodeHex
9. divide
10. normalizeMAC
11. resolveDNSName
12. scale
13. shiftTimeSec
14. swap
15. unzip
16. URLDecode

add

Description: This function adds two numbers and stores the sum in an event attribute.

Syntax:

```
<setEventAttribute attr="Arg3">
      add(Arg1, Arg2)
</setEventAttribute>
```

`Arg1`: Variable storing the first value.

`Arg2`: Variable storing the second value.

`Arg3`: Variable where the sum of `Arg1` and `Arg2` would be saved.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="totBytes">
      add($sentBytes, $recvBytes)
</setEventAttribute>
```

Given `sentBytes = 10` and `recvBytes = 30`, this function sets `totBytes = 40`.

calculateDomainEntropy

Description: This function calculates entropy of the event field using the Shannon entropy function. Entropy indicates how random the value looks based on words in an English dictionary. Names like "asdfjklqwerty.org", "8xhj9vzk.biz" have high entropy.

Syntax:

```
<setEventAttribute attr="Arg2">
        calcDomainEntropy(Arg1)
</setEventAttribute>
```

`Arg1`: Variable whose entropy would be calculated.

`Arg2`: Variable where the domain entropy of `Arg1` would be saved.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

The following function calculates the `destName` field and sets it to `domainEntropy` field.

```
<setEventAttribute attr="domainEntropy">
        calcDomainEntropy($destName)
</setEventAttribute>
```

calculateLatency

Description: This function compares 2 timestamps and calculate the latency (difference) between the two. The values are in seconds.

Syntax:

```
<setEventAttribute attr="Arg3">
     calculateLatency(Arg1, Arg2)
</setEventAttribute>
```

`Arg1`: Variable storing first time stamp.

`Arg2`: Variable storing second time stamp.

`Arg3`: Variable where (`Arg1-Arg2`) would be saved.

If `Arg1` is later than `Arg2`, then `Arg3` in set to seconds. Otherwise, `Arg3` is set to 0.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

The following function computes the latency between `phRecvTime` and `deviceTime`. If `phRecvTime` is later than `deviceTime`, the latency in set to seconds. Otherwise, latency is set to 0.

```
<setEventAttribute attr="latency">
     calculateLatency($phRecvTime, $deviceTime)
</setEventAttribute>
```

compIntfSecVal

Description: This function is specific for Cisco ASA Firewalls where each interface has a Security Level and FortiSIEM knows about it by discovering the configuration from Cisco ASA firewalls. This function compares the Security Level of `srcIntf` and `destIntf`. The result may be "LESS", "GREATER" or "EQUAL".

Syntax:

```
<setEventAttribute attr="Arg3">
           compIntfSecVal(Arg1, Arg2)
</setEventAttribute>
```

`Arg1`: Variable storing first interface name.

`Arg2`: Variable storing second interface name.

`Arg3`: Variable where security level comparison result is saved.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="_result">
           compIntfSecVal($srcIntf, $destIntf)
</setEventAttribute>
```

combineMsgId

Description: This function combines two or more strings into one string. Strings need to double quoted.

Syntax:

```
<setEventAttribute attr="ArgN">
           combineMsgId(Arg1,Arg2,Arg3, …)
</setEventAttribute>
```

Arg1: First string – can be a Variable storing the string value or a specific string with double quotes, e.g. "PH-".

Arg2: Second string – can be a Variable storing the string value or a specific string with double quotes, e.g. "PH-".

...

ArgN: Variable storing the concatenated result.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="eventType">
           combineMsgId("PH-", $_evIdPrefix, "-", $_evIdSuffix)
</setEventAttribute>
```

Given

```
_evIdPrefix: prefix
```

```
_evIdSuffix: suffix
```

This function sets eventType to PH-prefix-suffix.

compare

Description: This function compares 2 numbers and returns strings GREATER, EQUAL or LESS.

Syntax:

```
<setEventAttribute attr="Arg3">compare(Arg1, Arg2)</setEventAttribute>
```

Arg1: Variable storing the first numeric value.

Arg2: Variable storing the second numeric value.

Arg3: Variable storing the comparison result.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

In the following example:

- If confidence > 66 then eventSeverity will be set to 9.
- If confidence is between 33 and 66 then eventSeverity will be set to 5.
- else eventSeverity will be set to 1.

```
<when test="exist confidence">
  <setEventAttribute attr="_result">compare($confidence, 66)</setEventAttribute>
  <choose>
     <when test="$_result = 'GREATER'">
```

```
            <setEventAttribute attr="eventSeverity">9</setEventAttribute>
    </when>
    <otherwise>
            <setEventAttribute attr="_result">compare($confidence, 33)</setEventAttribute>
            <when test="$_result = 'GREATER'">
                 <setEventAttribute attr="eventSeverity">5</setEventAttribute>
            </when>
            <setEventAttribute attr="eventSeverity">1</setEventAttribute>
    </otherwise>
  </choose>
</when>
```

decodeBase64

Description: This function decodes a base64 encoded string.

Syntax:

```
<setEventAttribute attr="Arg2">decodeBase64(Arg1)</setEventAttribute>
```

Arg1: Variable storing the base64 encoded string.

Arg2: Variable storing the decoded value.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="msg">decodeBase64($_msg)</setEventAttribute>
```

Input:

```
_msg: bWVzc2FnZQ==
```

Output:

```
msg: message
```

decodeHex

Description: This function converts UTF-8 string in HEX form to its original form.

Syntax:

```
<setEventAttribute attr="Arg2">decodeHex(Arg1)</setEventAttribute>
```

Arg1: Variable storing the UTF-8 string in HEX form.

Arg2: Variable storing the decoded string.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="command">decodeHex($_command)</setEventAttribute>
```

Input:

```
_command: 61776B007B7072696E742024312C24332C24342C24362C2431327D
```

Output:

```
command: touch .test_file2
```

divide

Description: This function returns the result of division of two numbers.

Syntax:

```
<setEventAttribute attr="Arg3">
      compare(Arg1, Arg2)
</setEventAttribute>
```

Arg1: Variable storing the first numeric value.

Arg2: Variable storing the second numeric value.

Arg3: Variable storing the division result.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="memUtil">
     divide($usedMem, $totalMem)
</setEventAttribute>
```

Input:

```
usedMem: 1000
```

```
totalMem: 10000
```

Output:

```
memUtil: 0.1
```

normalizeMAC

Description: This function normalizes MAC address string to the form 01:23:45:67:89:ab

Syntax:

```
<setEventAttribute attr="Arg2">
         normalizeMAC(Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the unnormalized MAC address.

`Arg2`: Variable storing the normalized MAC address.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="hostMACAddr">
         normalizeMAC($_mac)
</setEventAttribute>
```

Input:

```
_mac: 1-2-3-4-ab-c
```

Output:

```
hostMACAddr: 01:02:03:04:ab:0c
```

resolveDNSName

Description: This function resolves a host name or FQDN to IP address. The resolution is done first by looking up FortiSIEM CMDB. If it fails and the variable `use_dns_lookup` is set to yes in `phoenix_config.txt`, then DNS Server, defined on the host, is used. Note that this may result in event latency. If `use_dns_lookup` is set to no, then DNS lookup is not attempted.

Syntax:

```
<setEventAttribute attr="Arg2">
      resolveDNSName(Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the host name or FQDN.

`Arg2`: Variable storing the resolved IP Address.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="destIpAddr">
      resolveDNSName($destName)
</setEventAttribute>
```

```
CMDB   Host1 -> 10.1.1.1
```

Input:

```
destName: Host1
```

Output:

```
destIpAddr: 10.1.1.1
```

scale

Description: This function calculates the product of two or more numbers.

Syntax:

```
<setEventAttribute attr="Arg3">
    scale(Arg1, Arg2)
</setEventAttribute>
```

`Arg1`: Variable storing the value to be scaled.

`Arg2`: Scaling factor (integer).

`Arg3`: Variable where the result is stored.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="durationMSec">
    scale($_durationSec, 1000)
</setEventAttribute>
```

Input:

```
_durationSec = 5
```

Output:

```
durationMSec = 5000
```

shiftTimeSec

Description: This function shifts time backward by a duration.

Syntax:

```
<setEventAttribute attr="Arg6">
    scale(Arg1, Arg2,Arg3,Arg4,Arg5)
</setEventAttribute>
```

`Arg1`: Variable storing the month value (1-12 in MM format).

`Arg2`: Variable storing the day value (1-31 in DD format).

`Arg3`: Variable storing the year value (YYYY format).

`Arg4`: Variable storing the time value (HH:MM:SS format).

`Arg5`: Variable storing the duration to be shifted in seconds.

`Arg6`: Variable where the result is stored as Unix epoch.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="logonTime">
     shiftTimeSec($_mon, $_day, $_year, $_time, $_durationSec)
</setEventAttribute>
```

Input:

```
_mon: 1
```

```
_day: 1
```

```
_year: 2000
```

```
_time: 01:00:10
```

```
_durationSec: 10
```

Output:

```
logonTime: epoch int of "01:00:00 01/01/2000"
```

swap

Description: This function swap the values of 2 variables.

Syntax:

```
<swap>$srcIntfName, $destIntfName</swap>
```

Arg1: Variable storing the first value.

Arg2: Variable storing the second value.

After swap, Arg1 has Arg2's old value and Arg2 has Arg1's old value.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<swap>$srcIntfName, $destIntfName</swap>
```

Before execution:

```
srcIntfName: Ethernet1
```

```
destIntfName: Ethernet2
```

```
After execution:
```

```
srcIntfName: Ethernet2
```

```
destIntfName: Ethernet1
```

unzip

Description: This function unzips a zip-formatted string.

Syntax:

```
<setEventAttribute attr="Arg2">unzip($Arg1)</setEventAttribute>
```

Arg1: Variable storing the zip-formatted string.

Arg2: Variable storing the unzipped string.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="msg">unzip($_zipMsg)</setEventAttribute>
```

Assuming _zipMsg field is zipped string, after execution, msg is set to the unzipped string.

URLDecode

Description: This function decodes URL-encoded string.

Syntax:

```
<setEventAttribute attr="httpFullRequest">
        URLDecode($httpFullRequest)
</setEventAttribute>
```

`Arg1`: Variable storing the URL-encoded string.

`Arg2`: Variable storing the decodes string.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="httpFullRequest">
        URLDecode($httpFullRequest)
</setEventAttribute>
```

Suppose

```
httpFullRequest: https://www.example.com/search?q=my%20search%20term
```

After execution:

```
httpFullRequest: https://www.example.com/search?q=my search term
```

Conversion Functions

These functions convert formats before setting to the event attributes.

1. calculateMSec
2. calculateSec
3. convertHexStrToInt
4. convertIpDecimalToStr
5. convertStrToIntIpPort
6. convertStrToIntIpProto
7. toLower
8. toUpper
9. toDateTime
10. toUnixTime

The following are deprecated

1. convertHexStrToStr
2. convertHostNameToIp

calculateMSec

Description: This function converts a time duration in HH:MM:SS format to milliseconds.

Syntax:

```
<setEventAttribute attr="durationMSec">
            calculateMSec($_duration)
     </setEventAttribute>
```

`Arg1`: Variable storing the time duration (HH:MM:SS format) to be converted to milliseconds.

`Arg2`: Variable storing the time duration in milliseconds (integer).

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
     <setEventAttribute attr="durationMSec">
            calculateMSec($_duration)
     </setEventAttribute>
```

Suppose `_duration` is parsed as 00:01:05

After execution:

```
durationMSec: 65000
```

calculateSec

Description: This function converts a time duration in HH:MM:SS format to seconds.

Syntax:

```
<setEventAttribute attr="Arg2">
            calculateMSec(Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the time duration (HH:MM:SS format) to be converted to seconds.

`Arg2`: Variable storing the time duration in seconds (integer).

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="vulnScanDuration">
     calculateSec($_duration)
</setEventAttribute>
```

Suppose `_duration` is parsed as 00:01:05.

After execution:

```
vulnScanDuration: 65
```

convertHexStrToInt

Description: This function converts a hex number to integer.

Syntax:

```
<setEventAttribute attr="Arg2">
      convertHexStrToInt(Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the value in hex format to be converted to integer.

`Arg2`: Variable storing the converted integer value.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="ipConnId">
      convertHexStrToInt($_ipConnId)
</setEventAttribute>
```

Input:

```
_ipConnId: 0xA
```

Output:

```
ipConnId =10
```

convertIpDecimalToStr

Description: This function converts decimal IP address to string.

Syntax:

```
<setEventAttribute attr="Arg2">
     convertIpDecimalToStr(Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the IPV4 value as integer.

`Arg2`: Variable storing the converted IPV4 value in string format.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="srcIpAddr">
     convertIpDecimalToStr($_srcIpAddr)
</setEventAttribute>
```

Input:

```
_srcIpAddr = 16843009
```

Output:

```
srcIpAddr = 1.1.1.1
```

convertStrToIntIpPort

Description:This function converts TCP/UDP Port name to port number, e.g. HTTP -> 80.

Syntax:

```
<setEventAttribute attr="Arg2">
         convertStrToIntIpPort($Arg1)
</setEventAttribute>
```

Arg1: Variable storing the TCP/UDP Port name in string format.

Arg2: Variable storing the converted TCP/UDP Port name in integer format.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="destIpPort">
         convertStrToIntIpPort($appTransportProto)
</setEventAttribute>
```

Input:

```
appTransportProto = "http"
```

Output:

```
destIpPort = 80
```

convertStrToIntIpProto

Description:This function converts an IP protocol name (e.g. TCP, UDP, ICMP, etc.) to integer form.

Syntax:

```
<setEventAttribute attr="Arg2">
     convertStrToIntIpProto (Arg1)
</setEventAttribute>
```

Arg1: Variable storing the IP protocol name in string format.

Arg2: Variable storing the converted IP protocol name in integer format.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="ipProto">
      convertStrToIntIpProto($_proto)
</setEventAttribute>
```

Input:

```
_proto = "TCP"
```

Output:

```
ipProto = 6
```

toLower

Description: This function converts string to lower case.

Syntax:

```
<setEventAttribute attr="Arg2">
         toLower ($Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the string to be converted to lower case.

`Arg2`: Variable storing the converted string in lower case.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="filePath">
         toLower($filePath)
</setEventAttribute>
```

Input:

```
filePath = "C:\WINDOWS"
```

Output:

```
filePath = "c:\windows"
```

toUpper

Description: This function converts string to upper case.

Syntax:

```
<setEventAttribute attr="Arg2">
         toUpper ($Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the string to be converted to upper case.

`Arg2`: Variable storing the converted string in upper case.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="filePath">
         toUpper($filePath)
</setEventAttribute>
```

```
```

Input:

```
filePath = "C:\Windows"
```

Output:

```
filePath = "C:\WINDOWS"
```

toDateTime

Description: This function converts string formatted timestamp to Unix epoch time.

Syntax:

```
<setEventAttribute attr="Arg6">
         toDateTime($Arg1, $Arg2, $Arg3,[$Arg4],[$Arg5])
</setEventAttribute>
```

`Arg1`: Variable storing the month: Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec or 1/2/3.../12.

`Arg2`: Variable storing the day: 01-31.

`Arg3`: Variable storing the time in HH:MM:SS format.

`Arg4`: Optional – Variable storing the year in YY or YYYY format.

`Arg5`: Optional - Variable storing the time zone in Z; UTC; GMT; -0700; +05:30; or AM / PM. Regex pattern is Z|UTC|GMT|[+-]\d{1,2}:?\d{2}|AM|PM. If AM or PM is passed directly, then $ is not required.

`Arg6`: Variable storing converted Unix epoch time.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

Three argument format – Month, Day, Time

```
<setEventAttribute attr="deviceTime">
      toDateTime($_mon, $_day, $_time)
</setEventAttribute>
```

Input:

```
_mon: 06
```

```
_day: 20
```

```
_time: 06:04:00
```

Output (server local timezone assumed e.g CST time):

```
deviceTime: 1750460640
```

Four argument format – Month, Day, Year, Time

```
<setEventAttribute attr="deviceTime">
      toDateTime($_mon, $_day, $_year, $_time)
</setEventAttribute>
```

Input:

```
_mon: 06
```

```
_day: 20
```

```
_year: 2025
```

```
_time: 06:04:00
```

Output (server local timezone assumed e.g CST time):

```
deviceTime: 1750460640
```

Five argument format - Month, Day, Year, Time, Timezone

```
<setEventAttribute attr="deviceTime">
    toDateTime($_mon, $_day, $_year, $_time,$_timezone)
</setEventAttribute>
```

Input:

```
_mon: 06
```

```
_day: 20
```

```
_year: 2025
```

```
_time: 06:04:00
```

```
_timezone: -06:00
```

Output:

```
deviceTime: 1750460640
```

Five argument format - Month, Day, Year, Time, AM/PM

```
<setEventAttribute attr="deviceTime">
    toDateTime($_mon, $_day, $_year, $_time, "PM")
</setEventAttribute>
```

Input:

```
_mon: 06
```

```
_day: 20
```

```
_year: 2025
```

```
_time: 06:04:00
```

Output:

```
deviceTime: 1750460640
```

toUnixTime

Description: This function is designed to convert LDAP / Active Directory (GeneralizedTime) format to Unix epoch.

The time format is YYYYMMDDHHMMSS.ffffff[+-]ZZZ e.g. 20100505222910.822003-000. Human readable representation of this timestamp is: 2010-05-05 22:29:10Z (UTC time)

Syntax:

```
<setEventAttribute attr="Arg2">
         toUnixTime ($Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing time in GeneralizedTime format: YYYYMMDDHHMMSS.ffffff[+-]ZZZ

`Arg2`: Variable storing converted Unix epoch time

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="deviceTime">
      toUnixTime($_deviceTime)
</setEventAttribute>
```

Input:

```
deviceTime: 20100505222910.822003-000
```

Output:

```
deviceTime: 1273098550
```

convertHexStrToStr (Deprecated)

Description: This function is deprecated.

convertHostNameToIp (Deprecated)

Description: This function is deprecated. Use this function instead: `resolveDNSName`.

Extraction Functions

These functions extract values from parsed values before setting to event attributes.

1. extractHostFromFQDN
2. getEventSeverityFromSyslogPriority
3. DeviceToCMDBAttr
4. extractHostFromURL

extractHostFromFQDN

Description: This function extracts host name from Fully Qualified Domain name (FQDN). If FQDN contains dot character, then it returns the string before the first dot; otherwise, returns the whole string.

Syntax:

```
<setEventAttribute attr="Arg2">
         extractHostFromFQDN ($Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing Fully Qualified Domain name (FQDN).

`Arg2`: Variable storing the extracted host name.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="hostName">
    extractHostFromFQDN($_fqdn)
</setEventAttribute>
```

Input:

```
_fqdn = host2.example.com
```

Output:

```
hostName: host2
```

getEventSeverityFromSyslogPriority

Description: This function calculates integer priority from syslog priority. The last 3 bits of the priority indicate the severity: http://en.wikipedia.org/wiki/Syslog

Syntax:

```
<setEventAttribute attr="Arg2">
         getEventSeverityFromSyslogPriority ($Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing syslog priority

`Arg2`: Variable storing the converted integer priority

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="eventSeverity">
      getEventSeverityFromSyslogPriority($_pri)
</setEventAttribute>
```

Input:

```
_pri: 52
```

Output:

```
eventSeverity: 5
```

DeviceToCMDBAttr

Description: This function returns the host name for an IP by looking up FortiSIEM CMDB.

Syntax:

```
<setEventAttribute attr="Arg2">
        DeviceToCMDBAttr("cpSelectedIp"|"cpDeviceId", $Arg1, "hostName")
</setEventAttribute>
```

`Arg1`: Event Attribute containing Device IP Address or Device Natural ID.

`Arg2`: The event attribute to which returned CMDB hostName value is set.

Example:

```
<setEventAttribute attr="reptDevName">
        DeviceToCMDBAttr("cpSelectedIp", $reptDevIpAddr, "hostName")
</setEventAttribute>
```

The function finds a CMDB device matching the IP address in `reptDevIpAddr`. Then the hostname value is set to `reptDevName`.

CMDB

Host Name	IP Address
Host1	10.1.1.1
Host2	10.1.1.2
Host3	10.1.1.3

Input:

`reptDevIpAddr = 10.1.1.2`

Output

`reptDevName = Host2`

extractHostFromURL

Description: This function extracts hostname from a URL.

Syntax:

```
<setEventAttribute attr="Arg2">
         extractHostFromURL ($Arg1)
</setEventAttribute>
```

`Arg1`: Variable storing the URL.

`Arg2`: Variable storing the extracted host name.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
      <setEventAttribute attr="destName">
               extractHostFromURL($infoURL)
     </setEventAttribute>
```

Input:

```
infoURL: http://www.example.com:80/request
```

Output:

```
destName: www.example.com
```

String Functions

These functions perform operations on strings.

1. replaceStringByRegex
2. replaceStrInStr
3. splitJsonEvent
4. trimAttribute

replaceStringByRegex

Description: This function replaces each portion that matches a regular expression in a string to another string.

Syntax:

```
<setEventAttribute attr="Arg4">
         replaceStringByRegex ($Arg1,Arg2,Arg3)
</setEventAttribute>
```

`Arg1`: Variable storing the string to be converted.

`Arg2`: Regular expression specifying the replacement pattern (to be specified within double quotes).

`Arg3`: Replacement String (to be specified within double quotes).

`Arg4`: Variable storing `Arg1` after replacement.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="eventType">
          replaceStringByRegex($_eventType, "\s+", "_")
</setEventAttribute>
```

Input:

```
_eventType: Event Type 124 456
```

Output:

```
eventType: Event_Type_123_456
```

replaceStrInStr

Description: This function replaces each portion that matches a specific string to another string. This is a simpler version of `replaceStringByRegex` function.

Syntax:

```
<setEventAttribute attr="Arg4">
         replaceStrInStr ($Arg1,Arg2,Arg3)
</setEventAttribute>
```

`Arg1`: Variable storing the string to be converted.

`Arg2`: String to be replaced (to be specified within double quotes).

`Arg3`: Replacement String (to be specified within double quotes).

`Arg4`: Variable storing `Arg1` after replacement.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="computer">
        replaceStrInStr($_computer, "$", "")
</setEventAttribute>
```

Input:

```
_computer: host$
```

Output:

```
computer: host
```

splitJsonEvent

Description: This function splits a JSON array of multiple events into multiple events.

Syntax:

```
<setEventAttribute attr="_resultCount">
           splitJsonEvent($Arg1,Arg2,Arg3, Arg4, Arg5)
</setEventAttribute>
```

`Arg1`: Variable storing the string to be split: a JSON array containing multiple events.

`Arg2`: JSON selector (same as the key in `collectAndSetAttrByJSON`) which returns the array.

`Arg3`: Prefix to be prepended to the extracted string (typically the syslog header).

`Arg4`: Suffix to be appended to the extracted string.

Arg5: True or False (case insensitive) to drop the input event (Arg1) or not.

Example:

```
<setEventAttribute attr="_resultCount">
           splitJsonEvent($_body, "params.events", "", "", "true")
</setEventAttribute>
```

Suppose _body (Arg1) is

```
{
  "jsonrpc": "2.0",
  "method": "addEvents",
  "params": {
    "events": [
      {
        "computer_name": " fc-win7-example ",
        "computer_fqdn": "fc-win7-example",
        "computer_ip": "10.10.10.11",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "malware_type": "file",
        "malware_name": "EICAR-Test-File (not a virus)",
        "file_path": "C:\\eicar0000001.txt",
        "hash": "8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71",
        "final_status": "deleted",
        "timestamp": "2017-09-08T12:01:36.000Z",
        "companyId": "62a92960315a119dbe0b0246",
        "module": "av",
        "_testEvent_": true
      },
      {
        "computer_name": " fc-win8-example ",
        "computer_fqdn": " fc-win8-example ",
        "computer_ip": "10.10.10.12",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "malware_type": "file",
        "malware_name": "EICAR-Test-File (not a virus)",
        "file_path": "C:\\eicar0000001.txt",
        "hash": "8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71",
        "final_status": "deleted",
        "timestamp": "2017-09-08T12:01:36.000Z",
        "companyId": "62a92960315a119dbe0b0246",
        "module": "av",
        "_testEvent_": true
      },
      {
        "computer_name": " fc-win9-example",
        "computer_fqdn": "fc-win9-example",
        "computer_ip": "10.10.10.13",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
```

```
        "malware_type": "file",
        "malware_name": "EICAR-Test-File (not a virus)",
        "file_path": "C:\\eicar0000001.txt",
        "hash": "8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71",
        "final_status": "deleted",
        "timestamp": "2017-09-08T12:01:36.000Z",
        "companyId": "62a92960315a119dbe0b0246",
        "module": "av",
        "_testEvent_": true
      }
    ]
  },
  "id": 1660923455412
}
```


FortiSIEM will drop this event and send 3 new events (Event 1, Event 2, Event 3), which are extracted from this event:

Event 1:


```
{
        "computer_name": " fc-win7-example ",
        "computer_fqdn": "fc-win7-example",
        "computer_ip": "10.10.10.11",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "malware_type": "file",
        "malware_name": "EICAR-Test-File (not a virus)",
        "file_path": "C:\\eicar0000001.txt",
        "hash": "8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71",
        "final_status": "deleted",
        "timestamp": "2017-09-08T12:01:36.000Z",
        "companyId": "62a92960315a119dbe0b0246",
        "module": "av",
        "_testEvent_": true
    }
```


Event 2:


```
{
        "computer_name": " fc-win8-example ",
        "computer_fqdn": " fc-win8-example ",
        "computer_ip": "10.10.10.12",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "malware_type": "file",
        "malware_name": "EICAR-Test-File (not a virus)",
        "file_path": "C:\\eicar0000001.txt",
        "hash": "8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71",
        "final_status": "deleted",
        "timestamp": "2017-09-08T12:01:36.000Z",
        "companyId": "62a92960315a119dbe0b0246",
```

```
        "module": "av",
        "_testEvent_": true
      }
```

Event 3:

```
{
        "computer_name": " fc-win9-example",
        "computer_fqdn": "fc-win9-example",
        "computer_ip": "10.10.10.13",
        "computer_id": "59a1604e60369e06733f8abb",
        "product_installed": "BEST",
        "malware_type": "file",
        "malware_name": "EICAR-Test-File (not a virus)",
        "file_path": "C:\\eicar0000001.txt",
        "hash": "8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71",
        "final_status": "deleted",
        "timestamp": "2017-09-08T12:01:36.000Z",
        "companyId": "62a92960315a119dbe0b0246",
        "module": "av",
        "_testEvent_": true
      }
```

trimAttribute

Description: This function trims characters from a given string in the beginning or at the end.

Syntax:

```
 <setEventAttribute attr="Arg3">
      trimAttribute($Arg1,Arg2)
</setEventAttribute>
```

`Arg1`: Variable storing the input string.

`Arg2`: Characters to be trimmed (to be specified within double quotes).

`Arg3`: Variable storing the string after trim operation.

Note: Variable can be a local variable or a FortiSIEM event attribute.

Example:

```
<setEventAttribute attr="destName">
    trimAttribute($destName, "./")
</setEventAttribute>
```

Input:

```
destName: .example.com/
```

Output:

```
destName: example.com
```

Python Threat Feed Framework

In release 7.0.0, FortiSIEM introduces a Python framework for FortiSIEM threat feed integrations.

Traditionally, customers or technical assistance center (TAC) engineers had to use a Java package framework to build threat feed integrations. However, adoption of the Java based framework was extremely low. This feature uses the Python framework to make custom threat feed integrations more accessible, with a well defined structure for data.

In this framework, FortiSIEM calls a Python module based threat feed, passing it a number of arguments necessary for communication with a threat feed. This framework then writes the threat entries to a CSV file which AppServer will parse. The framework is also extendable. If the customer knows the natural ID of the threat feed, the customer can run a script externally from FortiSIEM, providing their username and password for basic authentication to call AppServer's API to update the threat feed.

Updating a threat feed via Python can be done in two ways.

- **FortiSIEM Internal Threat Feed Update**: Python integration built into FortiSIEM – Threat feed update schedule passes standard set of arguments to python script, which uses these to obtain threat feed information, and saves it to CSV file for AppServer to process.
- **FortiSIEM External Threat Feed Update**: Python integration is executed externally from FortiSIEM in some customer environment. Provided customer has access to FortiSIEM credential, Threat feed natural ID, Threat feed URL and credentials. Python script collects threat feed data, and does an HTTP POST to FortiSIEM to push the data to Threat feed via API.

To update a threat feed, you will need to take the following steps.

1. From the new threat feed, obtain the URL endpoint, and credentials, if applicable.
2. Create your custom Python threat feed integration by taking the following steps.
   a. Obtain a copy of the Firehol and/or Anomail (TAXII2.x) threat feed integration script.
   b. Place your Python script in the `/opt/phoenix/data-definition/threatfeedIntegrations/` folder on the FortiSIEM Supervisor.
3. From the FortiSIEM Supervisor GUI, navigate to **RESOURCES**, and from the left pane, select **Malware Domains**, **Malware IPs**, **Malware Hash**, or **Malware URLs**.
4. In the same left pane, click **+** to create a new Malware Threat Feed Group.
5. From the Create New Malware Group Window, take the following steps.
   a. In the **Group** field, enter a name for the Malware Group threat feed.
   b. In the **Description** field, enter any information you wish to make available about the Malware Group threat feed.
   c. If Malware IPs was selected, from the Value Type drop-down list, select **IP** or **IP Range**.
   d. Click **Save**.
6. Select your malware threat feed group from the left pane, and from the main pane, click on **More**, and select **Update**.
7. From the Update Malware window, take the following steps.
   a. Select **Update via API**.
   b. From the **URL** row, click the Edit icon.
   c. In the **URL** field, enter the threat feed endpoint being used by your custom threat feed service. **Note**: Ensure you enter the http:// or https:// prefix.

d. In the **User Name** field, if required, enter the user name associated with the API access.
Note: Your script can manipulate these fields. If the threat feed requires an API key, you can simply place that in the password field, and dummy value in the username field.

e. In the **Password** field, enter the password associated with the user name.

f. For **Plugin Type**, select **Python**.

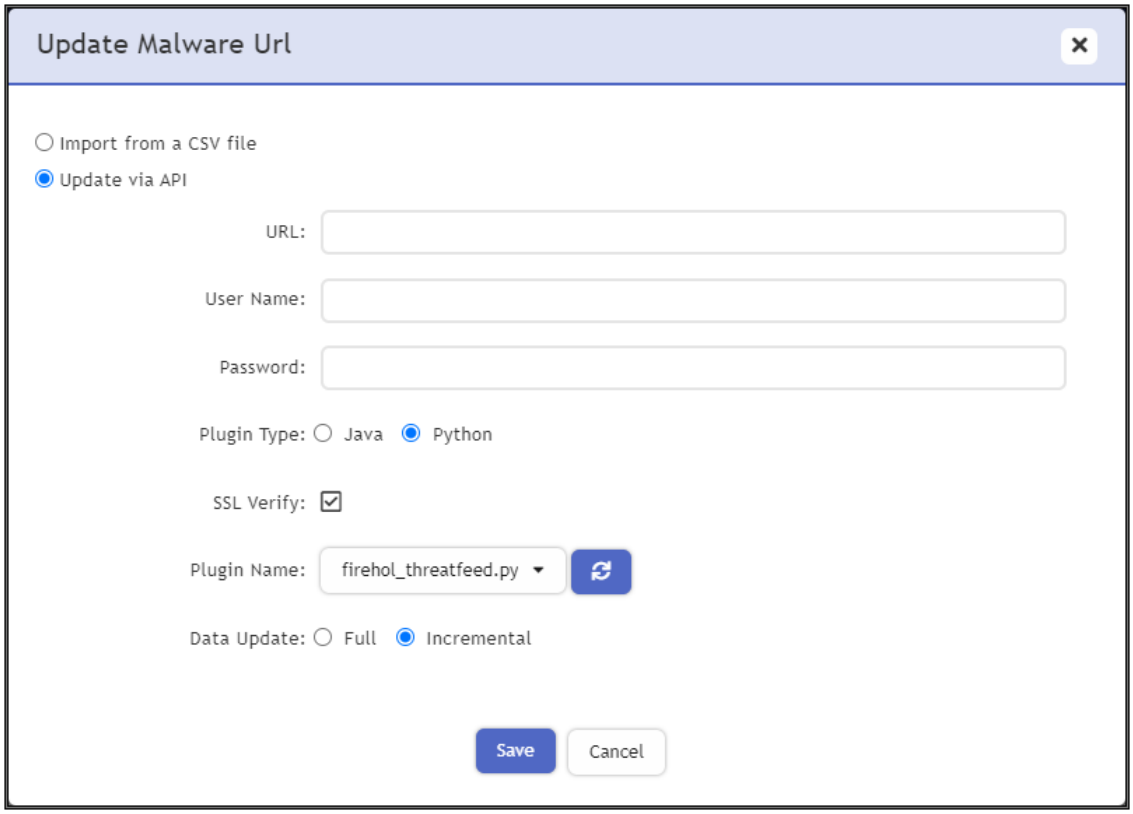
g. In the **Plugin Class** row, click the refresh button next to plugin class to refresh the list of python integrations available. This enumerates all .py files in the `/opt/phoenix/data-definition/threatfeedIntegrations/` folder.

h. Select your Python file from the drop-down list.
Note: You can click the refresh icon to refresh the drop-down list after copying your .py file to the `/opt/phoenix/data-definition/threatfeedIntegrations/` folder.

i. For **Data Update**, select **Full** or **Incremental**.

Option	Description
Full	Each time a scheduled trigger occurs, your threat feed data will be completely replaced with a new copy. In most cases, select “Full” to prevent accumulation of ineffective/aged threat indicators.
Incremental	Preserves existing data, and adds to it.

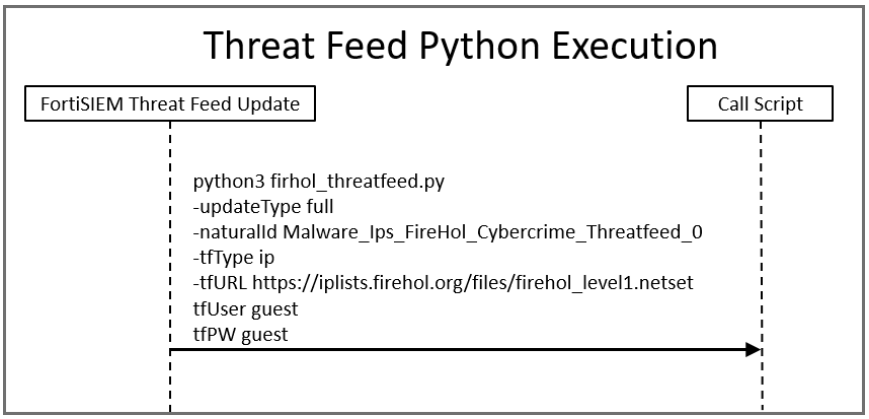
j. Click **Save**.



8. To create a schedule, see Specifying a Schedule.
After the first schedule has been executed, confirm that the entries are populated.

Threat Feed Workflow

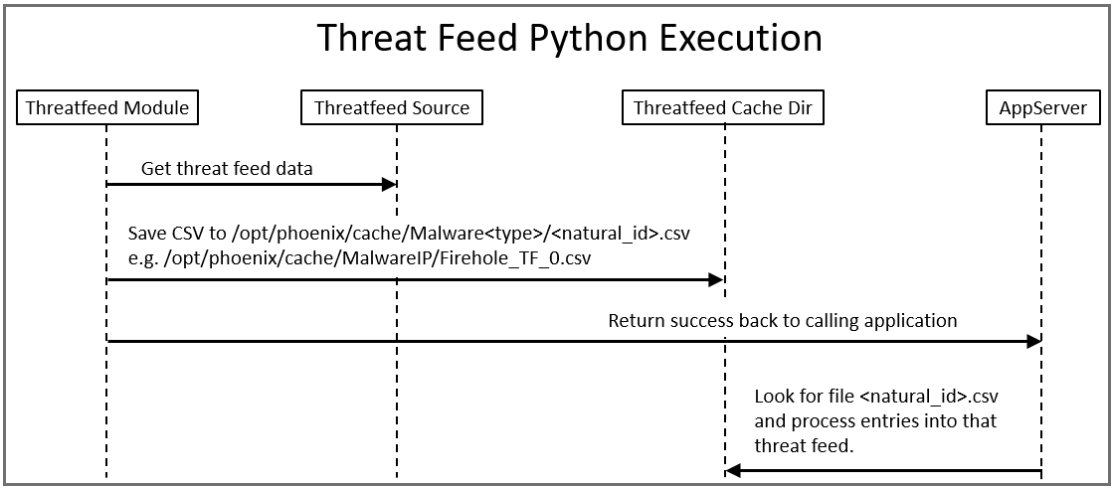
In this scenario, FortiSIEM's threat feed update schedule will gather the threat feed configuration data you provided during setup, and pass those as arguments to your custom python script. If you use Fortinet's provided framework, the threat feed data can be passed to a function which will store the data in the appropriate cache folder to update FortiSIEM.



Internal/Scheduled by FortiSIEM Execution Scenario:

In this scenario, the python script, when called by FortiSIEM, obtains the threat feed data from the remote source, parses the data into a list of dictionary objects, and passes that to a framework function which will save it to a local CSV file on the FortiSIEM Supervisor.

Remember that your custom python script must exist on the Supervisor, and be placed in this folder: `/opt/phoenix/data-definition/threatfeedIntegrations/`



External Execution Scenario:

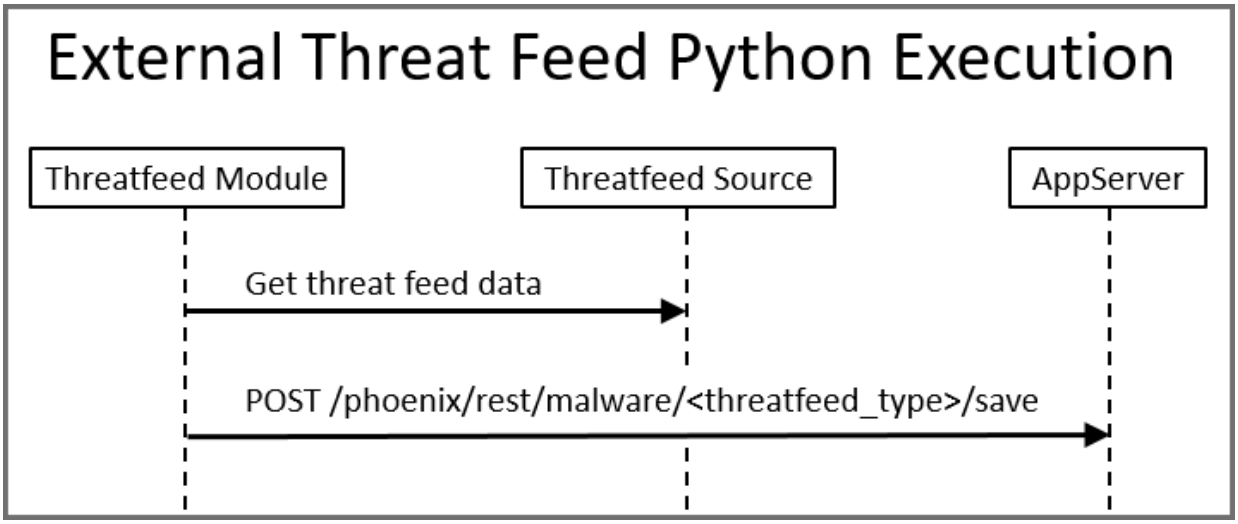
For Advanced Users Only: In this scenario, you can download all these python scripts to a remote location (not on FortiSIEM Supervisor), and execute the threat feed update. This however, requires that you securely store all the required arguments needed, and pass them to the script on execution. In addition, you need to provide the script 3 extra arguments (FortiSIEM base URL, a FortiSIEM user account with authorization (org/user), and FortiSIEM password)

In this scenario, the script uses the FortiSIEM public API to POST threat feed data in a defined JSON format.

Note: The naturalId of the threat feed you created is the most difficult item to obtain here, you must obtain it via Postgres in order to run it externally to FortiSIEM.

Listing available threat feeds to update:

```
select display_name,natural_id from ph_group where type=27;
        display_name         |             natural_id
-----------------------------+------------------------------------
 Emerging Threat Malware IP  | PH_SYS_EMER_THREAT
 ThreatStream Malware IP     | PH_SYS_THREATSTREAM_BLOCKED_IP
 FortiGuard Malware IP       | PH_SYS_FORTIGUARD_BLOCKED_IP
 TruSTAR Malware IP          | PH_SYS_TRUSTAR_BLOCKED_IP
 ThreatConnect Malware IP    | PH_SYS_THREATCONNECT_BLOCKED_IP
 Dragos Worldview Malware IP | PH_SYS_DRAGOSWORLDVIEW_BLOCKED_IP
```



Threatfeed Module

The threat feed package is located here: `/opt/phoenix/data-definition/threatfeedIntegrations/`

Directory Structure

The Threatfeed module directory consists of the following files and folders.

Directory File/Folder	Description
anomaly_threatfeed.py	An example working threat feed file implementing TAXII2.0 and TAXII2.1 threat feed integration. This is actually implemented in the helper modules “threatfeed_integration”.
firehol_threatfeed.py	An example working threat feed file implementing Firehol IP threat feeds.
fsiem_utils/	This is the package directory for the “fsiem_utils” python package.
fsiem_utils/__init__.py	Empty, simply the designated directory for package.
fsiem_utils/threatfeed_integration.py	Helper module defining the classes representing a threat feed integration and data objects.

Overview of Threat Feed Integrations

Required import: from fsiem_utils.threatfeed_integration import

All custom threat feeds inherit from the parent class ThreatfeedIntegration using the following statement:

class MyCustomThreatFeed(ThreatfeedIntegration):

This parent class handles a lot of the internals of handling input arguments and handling format of data that FortiSIEM can understand.

Script Input Arguments

The sample threat feeds have built in handling for the expected script input, so do not deviate from them. You can merely replace your custom class name with the existing example.

- Required Input Arguments: updateType,naturalId,tfType,tfURL
- (Optional) Input Arguments: tfUser,tfPW, appUser = None, appPW = None, appHost = 'https://127.0.0.1')

Data Object Classes

For ease of formatting data to FortiSIEM expected format, Fortinet has a number of helper classes for representation of an IP object, URL object, Domain object,, or Hash object.

Data Object Class Member Functions

<data_obj>.get_dict() – Returns dictionary form of object

Each of the classes representing a threat feed object (IP_entry, URL_entry, Domain_entry, and Hash_entry) have a function called get_dict() that returns the dictionary representation of the object, which is

on the format that AppServer expects. This can be dumped to JSON, which will be in AppServer's public API json format, or it can be dumped to CSV where the field order is preserved.

Class IP_entry()

Creates an object representing a single IP and/or contiguous network range indicator

Example Definition

IP_entry(name="Test IP",low_ip="1.1.1.1",high_ip="2.2.2.2",description="This is ransomware C2 server",date_found=now)

Required Arguments

- name
- low_ip

Optional Arguments

- high_ip
- malware_type
- confidence
- severity
- asn
- org
- country
- description
- date_found – datetime object
- lastSeen – datetime object

Class Domain_entry()

Creates an object representing a single domain indicator.

Example Definition

Domain_entry(domainName="google.com",ip="9.9.9.9")

Required Arguments

- domainName

Optional Arguments

- ip
- reverseLookup
- malware_type
- confidence
- severity
- asn
- org
- country
- description
- date_found – datetime object
- lastSeen – datetime object

Class URL_entry()

Creates an object representing a single URL indicator.

Example Definition

URL_entry(url="google.com/test2.xml",origin="https://google.com",description="Test URL")

Required Arguments

- url

Optional Arguments

- origin
- malware_type
- confidence
- description
- lastSeen – datetime object

Class Hash_entry()

Creates an object representing a single hash indicator.

Example Definition

Hash_entry(name="REvil Hash1",algorithm="SHA256",hashcode="XXXXXXXXX",description="test")

Required Arguments

- names
- algorithm
- hashcode

Optional Arguments

- controller_ip
- malware_type
- confidence
- severity
- asn
- org
- country
- description
- date_found – datetime object
- lastSeen – datetime object

Important Member Variables of the ThreatfeedIntegration Class

If you properly follow the example threat feeds by inheriting from the ThreatfeedIntegration class, these are automatically populated by the scripts input arguments.

```
        self.updateType = updateType #full or incremental, indicates if threatfeed does a
full replace or append
        self.appserverUsername = appUser #Optional if run external to FortiSIEM
        self.appserverPassword = appPW #Optional if run external to FortiSIEM
        self.threatfeed_natural_id = naturalId #Threatfeed natural ID to update
        self.threatfeed_type = tfType #Threatfeed type (ip,site,url,hash,proc)
        self.threatfeed_url = tfURL #Threatfeed source URL
        self.threatfeed_username = tfUser #Threatfeed optional user
        self.threatfeed_password = tfPW #Threatfeed optional pw
        self.appserver_host = appHost #FortiSIEM super IP if script run externally
```

Important Member Functions of the ThreatfeedIntegration Class

Member Function	Description
getThreatFeedData (self)	You must override this function in your script's child class. It references the above member variables to authenticate to your given threat feed source, and calls the save function to send to FortiSIEM.
saveThreatFeedData (self,post_data)	Call this function once you have retrieved your threat feed data. It accepts a python list of dictionary objects, which represent either IP, URL, Domain, or Hash objects. You only call this function, you do not override it.

Instructions on Creating a New Python Integration

Take the following steps to create a new python integration.

1. Copy an existing example file.
   For example:
   `cp firehol_threatfeed.py my_example.py`
2. Rename the class "FireHolThreatFeed" to your new class name. It is referenced in 3 locations in this file.
3. Override the `getThreatFeedData` function, as this is where all your work will be done. You will build a list of dictionary objects using the existing integrations as an example.
4. Call `saveThreatFeedData(post_data)`. This will convert the list of dictionary objects into a CSV file (if run locally on Supervisor) or call AppServer save API if run externally to Supervisor. You can review the file `example_threatfeed.py` to see an example of how to convert data ingested from a threat feed into a representation that the framework can convert to a CSV file.

Python Script

The python script which is user defined e.g. "threatfeed_script_name.py" is called with the input arguments listed in the following table.

Argument Number	Argument	Argument Type	Description
Arg1	updateType	String	Either "full" or "incremental". If script is externally run, calls to the save API can override whether the threat feed does a full replace of data ("full") or an append ("incremental").
Arg2	naturalId	String	String literal of the threat feed (to update)s' natural ID.
Arg3	tfType	String	Threat feed type, which will be one of the following: ip, hash, site, or url. This allows a single script to add handling for the type of threat feed if the service provides multiple types of threat feeds.
Arg4	tfURL	String	URL endpoint for the threat feed service.
Arg5	tfUser	String	(Optional) Username value for basic authentication to threat feed service.
Arg6	tfPW	String	(Optional)Password value for threat feed basic authentication. In other cases, it can be used for holding the API secret key instead. The script can manipulate these values as desired.
Arg7	appUser	String	(Optional) Username for FortiSIEM in the format (org/user) e.g. super/admin. This is only needed if the script is executed externally from FortiSIEM and not executed via AppServer schedule.
Arg8	appPW	String	(Optional) Password for FortiSIEM user. This is only needed if the script is executed externally from FortiSIEM and not executed via AppServer schedule.
Arg9	appHost	String	(Optional) If script is run externally to FortiSIEM, this can override the app server (Supervisor) URL. It normally defaults to https://127.0.0.1 as it is only executed programmatically on the FortiSIEM Supervisor.

Example Adhoc Script Run Locally on FortiSIEM

Caution: Script must only be run as user "admin", **never** as root.

```
python3 /opt/phoenix/data-definition/threatfeedIntegrations/firehol_threatfeed.py -
updateType full -naturalId Malware_IPs_FireHol_Cybercrime_Threatfeed_0 -tfType ip -tfURL
https://iplists.firehol.org/files/firehol_level1.netset -tfUser guest -tfPW guest
```

This generates a CSV file for AppServer to consume: `/opt/phoenix/cache/MalwareIP/Malware_IPs_FireHol_Cybercrime_Threatfeed_0.csv`

Note: When you manually run the script, you'll notice that it doesn't actually update in the GUI. This is because normally, FortiSIEM is the one executing the script, and will only look for this CSV file after it executes. You can manually run this to test for errors and ensure the CSV file is populated appropriately. Afterward, you can try an end to end test by configuring FortiSIEM to call your new threat feed script.

Example Adhoc Script Run Externally to FortiSIEM (e.g. remote customer machine) – This assumes you have a FortiSIEM user account and know the threat feed's natural ID.

```
python3 /opt/phoenix/data-definition/threatfeedIntegrations/firehol_threatfeed.py -
updateType full -naturalId Malware_IPs_FireHol_Cybercrime_Threatfeed_0 -tfType ip -tfURL
https://iplists.firehol.org/files/firehol_level1.netset -tfUser guest -tfPW guest -appUser
'super/admin' -appPW ‘xxxxx’ –appHost ‘https://192.168.1.25’
```

The only difference here is the addition of appUser, appPW, and appHost, indicating to the script that it must call the app server API which is on a remote system using HTTP POST with basic authentication. If run locally, the script will merely generate a CSV file in the `/opt/phoenix/cache` directory for AppServer to consume (removing the need for app server credentials).

Save Imported Data to Database

Normally the details of the CSV file location, and its format are completely abstracted and handled by the parent class "ThreatfeedIntegration". The content here is for informational purposes only.

- Python script has to save data in following directories depending on threat feed type.
  - /opt/phoenix/cache/MalwareDomain
  - /opt/phoenix/cache/MalwareIP
  - /opt/phoenix/cache/MalwareHash
  - /opt/phoenix/cache/MalwareUrl
- Supported file type is CSV
- File Name: <natural_id>.csv e.g. Malware_IPs_FireHol_Cybercrime_Threatfeed_0.csv
- CSV structure:
  - IPs: name, malwareType, lowIp, highIp, description, confidence ,severity, org, country, asn, dateFound, lastSeen
  - Domains: domainName, malwareType, description, ipAddr, reverseLookup, asn, confidence, severity, org, country, dateFound, lastSeen
  - Hash: botnetName, algorithm, hash, controllerIp, confidence, country, malwareType, severity, asn, org, description, dateFound, lastSeen
  - URL: url, description, malwareType, confidence, lastSeen

Performance Considerations

There are no performance concerns a this time. When selecting the threat feed update type in the GUI, in almost all cases you want to select "Full". FortiSIEM has been enhanced to handle massive threat feed lists. Only in exceedingly rare cases would you choose update type of "Incremental". Doing

"Incremental" can create problems as threat lists quickly become exceedingly large (not truncated), and often contain stale, and non-effective indicators.

Custom python scripts can be either configured to do either of the following:

- **Incremental** (append only) - Updates to the threat feed, new calls are append only, and does not delete and re-enter the same data. Care should be taken to periodically do a full replace on a maintenance schedule to replace stale entries.
- **Full** - Updates to the threat feed, each call to the script does a complete replace of the threat feed data with the latest copy from the source threat feed source. **This should be considered the default option even in really large threat feeds in the hundreds of thousands of entries**.

Public APIs

These public APIs are only important if you plan to execute this script outside of FortiSIEM as part of your own custom application. Normally FortiSIEM will hold all these scripts locally and execute them on a schedule, removing the need for these public APIs.

AppServer provides the following two public REST APIs to import or delete malware data. These are only needed if the python script is executed external to FortiSIEM. This allows external systems to integrate with FortiSIEM threat feeds, as opposed to having FortiSIEM execute an update on a schedule.

- Import API
- Delete API

Import API

API Endpoint: `POST phoenix/rest/malware/{type}/save`

Query Parameters

1. groupNaturalId : String [*required field]
2. updateType : String [full | incremental]

Path Parameters

1. type: String [*required field]
   a. Accepted values for type - [hash, site, url, ip]

POST Body

Example for IP:

```
        [
        {
            "name":"RansomwareIP",
            "lowIp":"1.1.1.1",
            "highIp":"1.1.1.1"
        },
        {
            "name":"RansomwareIP2",
            "lowIp":"2.1.1.1",
            "highIp":"2.1.1.1"
        },
        {
            "name":"RansomwareIP3",
            "lowIp":"3.1.1.1",
            "highIp":"3.1.1.1"
        }
    ]
```

Example 2 for Domain:

```
[
{
"domainName":"",
"ip":"",
"name":""
} //This JSON Object keys are defined in ThreatFeedDTO
]
```

JSON Structure: Array of Objects: ThreatFeedDTO

See the following tables for their **ThreatFeedDTO JSON Object Structure**.

Malware Domain Threat Feed Parameter	Value Type
domainName	String
ip	String
reverseLookup	String

Malware IP Threat Feed Parameter	Value Type
name	String
lowIp	String
highIp	String

Malwre Hash Threat Feed Parameter	Value Type
botnetName	String
algorithm	String
hash	String
controllerIp	String

Malware Url Threat Feed Parameter	Value Type
url	String
origin	String

Common Malware Threat Feed Parameter	Value Type
active	Boolean
malwareType	String
confidence	String
severity	String
asn	String
org	String
country	String
description	String
dateFound	String
lastSeen	String

Delete API

API Endpoint: `POST phoenix/rest/malware/threatfeed/deleteall`

Query Parameter

1. groupNaturalId : String [*required field]

Return: Success | Error

Notes about Threat Feed Authentication

The python threat feed GUI still only has the ability to pass basic authentication credentials to the Python script (e.g. username and password). You can place values such as an API key in one of these fields and manipulate that data in your custom threat feed integration. So although the UI only displays an optional user/pw fields, you can still put anything you want in these fields and manipulate accordingly. Note that only the password field is encrypted, so try not to place sensitive data in the username field if overriding them for a different authentication type.

Installing New Python Packages

Using new packages not already installed on the Supervisor need to be manually installed with care. Fortinet uses the requests API which covers the most common use cases. The system python3 install already contains many useful packages such as requests and urllib3.

Here are recommended steps to help keep your system secure.

1. Follow your organization's change control procedures
2. Backup your FortiSIEM Supervisor prior to making the change
3. Ensure you have a rollback/revert plan
4. Document the time of the change and the purpose
5. Make the change only on the Supervisor appliances

Sample Windows Agent Logs

FortiSIEM Windows Agent Manager generates Windows logs in an easy way to analyze "attribute=value" style without losing any information.

- Certificate Monitoring Logs
- System Logs
- Sysmon Logs
- PowerShell Logs
- Application Logs
- Security Logs
- DNS Logs
- DHCP Logs
- IIS Logs
- DFS Logs
- File Content Monitoring Logs
- File Integrity Monitoring Logs
- Installed Software Logs
- Registry Change Logs
- Removeable Media Logs
- WMI Logs

Certificate Monitoring Logs

- Certificate Added
- Certificate Removed
- Certificate Expired
- Certificate Expiring

Certificate Added

```
2023-10-25T19:45:14Z DESKTOP-3NKROF5 192.0.2.0 AccelOps-WUA-Certificate [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="72f70ae7-1111-
4dc0-1111-0c953f46f87e" [timeZone]="-0800" [extEventRecvProto]="Windows Agent"
[certAction]="Added" [authority_key_id]="F4B6E1201DFE29AED2E461A5B2A225B2C817356E" [ca]="0"
[common_name]="DigiCert Timestamp 2021" [issuer]="US, DigiCert Inc, www.digicert.com,
DigiCert SHA2 Assured ID Timestamping CA" [key_algorithm]="RSA" [key_strength]="2160" [key_
usage]="CERT_DIGITAL_SIGNATURE_KEY_USAGE" [not_valid_after]="1925424000" [not_valid_
```

```
before]="1609459200" [path]="LocalMachine\Trusted Publishers" [self_signed]="0"
[serial]="0D424AE0BE3A88F1111021CE1400F0DD"
[sha1]="E1D782A8E191BEEF6BCA1691B5AAB494A6249BF3" [sid]="" [signing_algorithm]="sha256RSA"
[store]="Trusted Publishers" [store_id]="" [store_location]="LocalMachine" [subject]="US,
\"DigiCert, Inc.\", DigiCert Timestamp 2021" [subject_key_
id]="3644868EA4BAB066BEBC2821111436DDE36A7ABC" [user]=""
```

Certificate Removed

```
2023-10-25T19:52:31Z DESKTOP-3NKROF5 192.0.2.0 AccelOps-WUA-Certificate [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="72f70ae7-1111-
4dc0-1111-0c953f46f87e" [timeZone]="-0800" [extEventRecvProto]="Windows Agent"
[certAction]="Removed" [authority_key_id]="" [ca]="0" [common_name]="expiring913"
[issuer]="expiring913" [key_algorithm]="RSA" [key_strength]="2160" [key_usage]="CERT_KEY_
ENCIPHERMENT_KEY_USAGE,CERT_DIGITAL_SIGNATURE_KEY_USAGE" [not_valid_after]="1694630930"
[not_valid_before]="1694457530" [path]="LocalMachine\Trusted People" [self_signed]="1"
[serial]="347CD406C649FDA94507BFA863904500"
[sha1]="8E3D8330748D4FB01848E6663E6E209735893199" [sid]="" [signing_algorithm]="sha256RSA"
[store]="Trusted People" [store_id]="" [store_location]="LocalMachine"
[subject]="expiring913" [subject_key_id]="35EF93076396C311112C51BF121247284686090A"
[user]=""
```

Certificate Expired

```
2023-10-25T19:46:48Z DESKTOP-3NKROF5 192.0.2.0 AccelOps-WUA-Certificate [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="72f70ae7-1111-
4dc0-1111-0c953f46f87e" [timeZone]="-0800" [extEventRecvProto]="Windows Agent"
[certAction]="Expired" [authority_key_id]="" [ca]="-1" [common_name]="expiring1021"
[issuer]="expiring1021" [key_algorithm]="RSA" [key_strength]="2160" [key_usage]="CERT_KEY_
ENCIPHERMENT_KEY_USAGE,CERT_DIGITAL_SIGNATURE_KEY_USAGE" [not_valid_after]="1697911109"
[not_valid_before]="1697478510" [path]="LocalMachine\Trusted People" [self_signed]="1"
[serial]="1F3EB6C111E7478E4DEE1F13EDF3935B"
[sha1]="946499B4B192D27682D86F9F93522B11BF0F1AE0" [sid]="" [signing_algorithm]="sha256RSA"
[store]="Trusted People" [store_id]="" [store_location]="LocalMachine"
[subject]="expiring1021" [subject_key_id]="4DC106FF2111117C13B5E5C62F4C106D12C44C63"
[user]=""
```

Certificate Expiring

```
2023-10-25T21:40:51Z DESKTOP-3NKROF5 192.0.2.0 AccelOps-WUA-Certificate [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="72f70ae7-1111-
4dc0-1111-0c953f46f87e" [timeZone]="-0800" [extEventRecvProto]="Windows Agent"
[certAction]="Expiring" [authority_key_id]="" [ca]="-1" [common_name]="expiring1029"
[issuer]="expiring1029" [key_algorithm]="RSA" [key_strength]="2160" [key_usage]="CERT_KEY_
```

```
ENCIPHERMENT_KEY_USAGE,CERT_DIGITAL_SIGNATURE_KEY_USAGE" [not_valid_after]="1698596479"
[expiry_in_days]="3" [not_valid_before]="1698163880" [path]="LocalMachine\Preview Build
Roots" [self_signed]="1" [serial]="2085D79E2DE08A9A4FE011108525F91D"
[sha1]="8DA053FCEFE792FC2E57F3A218751F6070E91B78" [sid]="" [signing_algorithm]="sha256RSA"
[store]="Preview Build Roots" [store_id]="" [store_location]="LocalMachine"
[subject]="expiring1029" [subject_key_id]="362A38630797FF2C78B1A9AE1E1116927C633FA0"
[user]=""
```

System Logs

- System Logs generated by pre-7.1.4 Windows Agent
- System Logs generated by 7.1.4 and later Windows Agent

System Logs generated by pre-7.1.4 Windows Agent

```
2024-02-20T23:24:58Z FSM-GFU-Windows2019-WIN2019-172-30-56-129 172.30.56.129 AccelOps-WUA-
WinLog-System [phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-
US" [MachineGuid]="1e749ab9-bf6e-4052-806b-02068b2d4465" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [eventName]="System" [eventSource]="Service Control
Manager" [eventId]="7036" [eventType]="Information" [domain]="" [computer]="FSM-GFU-
Windows2019-WIN2019-172-30-56-129" [user]="" [userSID]="" [userSIDAcctType]=""
[eventTime]="Feb 20 2024 23:24:57" [deviceTime]="Feb 20 2024 23:24:57" [msg]="The Microsoft
Store Install Service service entered the stopped state."
```

System Logs generated by 7.1.4 and later Windows Agent

The events are generated in XML format.

```
2024-02-26T22:22:42Z FSM-GFU-Windows2019-WIN2019-172-30-56-129 172.30.56.129 FSM-WUA-
WinLog-System [phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-
US" [MachineGuid]="1e749ab9-bf6e-4052-806b-02068b2d4465" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Service Control Manager' Guid='{555908d1-a6d7-4695-8e1e-26931d2012f4}'
EventSourceName='Service Control Manager'/><EventID
Qualifiers='16384'>7036</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode
>0</Opcode><Keywords>0x8080000000000000</Keywords><TimeCreated SystemTime='2024-02-
26T22:22:41.078643000Z'/><EventRecordID>168290</EventRecordID><Correlation/><Execution
ProcessID='744' ThreadID='3880'/><Channel>System</Channel><Computer>FSM-GFU-Windows2019-
WIN2019-172-30-56-129</Computer><Security/></System><EventData><Data Name='param1'>Network
Setup Service</Data><Data
```

```
Name='param2'>stopped</Data><Binary>4E00650074005300650074007500700053007600630002F00310000
00</Binary></EventData><RenderingInfo Culture='en-US'><Message>The Network Setup Service
service entered the stopped
state.</Message><Level>Information</Level><Task></Task><Opcode></Opcode><Channel></Channel
><Provider>Microsoft-Windows-Service Control
Manager</Provider><Keywords><Keyword>Classic</Keyword></Keywords></RenderingInfo></Event>
```

Sysmon Logs

- Sysmon Logs generated by pre-7.1.4 Windows Agent
- Sysmon Logs generated by 7.1.4 and later Windows Agent

Sysmon Logs generated by pre-7.1.4 Windows Agent

```
2024-02-27T23:06:35Z FSM-GFU-Windows2019-WIN2019-172-30-56-129 172.30.56.129 AccelOps-WUA-
WinLog-Microsoft-Windows-Sysmon/Operational [phCustId]="2000" [customer]="org1"
[monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="1e749ab9-bf6e-4052-806b-
02068b2d4465" [timeZone]="-0800" [extEventRecvProto]="Windows Agent"
[eventName]="Microsoft-Windows-Sysmon/Operational" [eventSource]="Microsoft-Windows-Sysmon"
[eventId]="1" [eventType]="Information" [domain]="NT AUTHORITY" [computer]="FSM-GFU-
Windows2019-WIN2019-172-30-56-129" [user]="SYSTEM" [userSID]="S-1-5-18"
[userSIDAcctType]="User" [eventTime]="Feb 27 2024 23:06:35" [deviceTime]="Feb 27 2024
23:06:35" [msg]="Process Create:
RuleName: -
UtcTime: 2024-02-27 23:06:35.046
ProcessGuid: {1e749ab9-6afb-65de-c644-000000001600}
ProcessId: 2068
Image: C:\\Windows\\System32\\HOSTNAME.EXE
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Hostname APP
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: hostname.exe
CommandLine: \"C:\\Windows\\system32\\HOSTNAME.EXE\"
CurrentDirectory: C:\\Windows\\system32\\
User: NT AUTHORITY\\SYSTEM
LogonGuid: {1e749ab9-4516-65c0-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes:
MD5=7F95220A65A5A5D4A98873E86EF2E549,SHA256=1BFF2907C456F99277F45F9B2A21B1B3F11F6C01587D9E
6D6F0B2B5F1472FE92,IMPHASH=5CD891320C666621E9783444DB8CBA78
ParentProcessGuid: {1e749ab9-6775-65de-7344-000000001600}
ParentProcessId: 6884
ParentImage: C:\\Program Files\\Fortinet\\FortiSIEM\\FSMLogAgent.exe
```

```
ParentCommandLine: \"C:\\Program Files\\Fortinet\\FortiSIEM\\FSMLogAgent.exe\"
ParentUser: NT AUTHORITY\\SYSTEM"
```

Sysmon Logs generated by 7.1.4 and later Windows Agent

The events are generated in XML format.

```
2024-02-27T22:18:54Z FSM-GFU-Windows2019-WIN2019-172-30-56-129 172.30.56.129 FSM-WUA-
WinLog-Microsoft-Windows-Sysmon/Operational [phCustId]="2000" [customer]="org1"
[monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="1e749ab9-bf6e-4052-806b-
02068b2d4465" [timeZone]="-0800" [extEventRecvProto]="Windows Agent" [level]="Information"
[xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-
06f5698ffbd9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><O
pcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-02-
27T22:18:53.386292600Z'/><EventRecordID>42662</EventRecordID><Correlation/><Execution
ProcessID='3196' ThreadID='5432'/><Channel>Microsoft-Windows-
Sysmon/Operational</Channel><Computer>FSM-GFU-Windows2019-WIN2019-172-30-56-
129</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-
Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2024-02-27
22:18:53.373</Data><Data Name='ProcessGuid'>{1e749ab9-5fc0-65de-a843-
000000001600}</Data><Data Name='ProcessId'>4372</Data><Data
Name='Image'>C:\\Windows\\system32\\CompatTelRunner.exe</Data><Data
Name='TargetObject'>\\REGISTRY\\A\\{41ae3209-e80b-5fb1-d81b-
7b9b2464bf78}\\Root\\InventoryApplicationFile\\osquery.exe|7bec5ef138bedfec\\LowerCaseLong
Path</Data><Data Name='Details'>c:\\program
files\\fortinet\\fortisiem\\osquery.exe</Data><Data Name='User'>NT
AUTHORITY\\SYSTEM</Data></EventData><RenderingInfo Culture='en-US'><Message>Registry value
set:
RuleName: InvDB-Path
EventType: SetValue
UtcTime: 2024-02-27 22:18:53.373
ProcessGuid: {1e749ab9-5fc0-65de-a843-000000001600}
ProcessId: 4372
Image: C:\\Windows\\system32\\CompatTelRunner.exe
TargetObject: \\REGISTRY\\A\\{41ae3209-e80b-5fb1-d81b-
7b9b2464bf78}\\Root\\InventoryApplicationFile\\osquery.exe|7bec5ef138bedfec\\LowerCaseLong
Path
Details: c:\\program files\\fortinet\\fortisiem\\osquery.exe
User: NT AUTHORITY\\SYSTEM</Message><Level>Information</Level><Task>Registry value set
(rule:
RegistryEvent)</Task><Opcode>Info</Opcode><Channel></Channel><Provider></Provider><Keyword
s></Keywords></RenderingInfo></Event>
```

PowerShell Logs

- PowerShell Logs generated by pre-7.1.4 Windows Agent
- PowerShell Logs generated by 7.1.4 and later Windows Agent

PowerShell Logs generated by pre-7.1.4 Windows Agent

```
"2024-02-27T23:36:35Z FSM-GFU-Windows2019-WIN2019-172-30-56-129 172.30.56.129 AccelOps-WUA-
WinLog-Windows PowerShell [phCustId]=""2000"" [customer]=""org1""
[monitorStatus]=""Success"" [Locale]=""en-US"" [MachineGuid]=""1e749ab9-bf6e-4052-806b-
02068b2d4465"" [timeZone]=""-0800"" [extEventRecvProto]=""Windows Agent""
[eventName]=""Windows PowerShell"" [eventSource]=""PowerShell"" [eventId]=""600""
[eventType]=""Information"" [domain]="""" [computer]=""FSM-GFU-Windows2019-WIN2019-172-30-
56-129"" [user]="""" [userSID]="""" [userSIDAcctType]="""" [eventTime]=""Feb 27 2024
23:36:35"" [deviceTime]=""Feb 27 2024 23:36:35"" [msg]=""Provider \""WSMan\"" is Started.
Details:
                ProviderName=WSMan
                NewProviderState=Started

                SequenceNumber=55

                HostName=Default Host
                HostVersion=5.1.17763.1432
                HostId=98d60fba-a813-4b20-9052-b56a1d052bc8
                HostApplication=C:\\Program Files\\Fortinet\\FortiSIEM\\FSMLogAgent.exe
                EngineVersion=
                RunspaceId=
                PipelineId=
                CommandName=
                CommandType=
                ScriptName=
                CommandPath=
                CommandLine="""
```

PowerShell Logs generated by 7.1.4 and later Windows Agent

The events are generated in XML format.

```
2024-02-27T23:16:39Z GFU-Win11.getest.com 172.30.56.124 FSM-WUA-WinLog-Windows PowerShell
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [level]="Information" [xml]=<Event
```

```
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='PowerShell'/><EventID
Qualifiers='0'>403</EventID><Version>0</Version><Level>4</Level><Task>4</Task><Opcode>0</O
pcode><Keywords>0x80000000000000</Keywords><TimeCreated SystemTime='2024-02-
27T23:16:39.7709133Z'/><EventRecordID>416398</EventRecordID><Correlation/><Execution
ProcessID='6064' ThreadID='0'/><Channel>Windows PowerShell</Channel><Computer>GFU-
Win11.getest.com</Computer><Security/></System><EventData><Data>Stopped</Data><Data>Availa
ble</Data><Data>                NewEngineState=Stopped
                PreviousEngineState=Available

                SequenceNumber=2219

                HostName=Default Host
                HostVersion=5.1.22000.2538
                HostId=b0f192dd-bf79-4fed-9740-8f556f9f63d8
                HostApplication=C:\\Program Files\\Fortinet\\FortiSIEM\\FSMLogAgent.exe
                EngineVersion=5.1.22000.2538
                RunspaceId=0812ae9a-0717-469e-a4de-1103ff4404b3
                PipelineId=
                CommandName=
                CommandType=
                ScriptName=
                CommandPath=
                CommandLine=</Data></EventData><RenderingInfo Culture='en-
US'><Message>Engine state is changed from Available to Stopped.

Details:
                NewEngineState=Stopped
                PreviousEngineState=Available

                SequenceNumber=2219

                HostName=Default Host
                HostVersion=5.1.22000.2538
                HostId=b0f192dd-bf79-4fed-9740-8f556f9f63d8
                HostApplication=C:\\Program Files\\Fortinet\\FortiSIEM\\FSMLogAgent.exe
                EngineVersion=5.1.22000.2538
                RunspaceId=0812ae9a-0717-469e-a4de-1103ff4404b3
                PipelineId=
                CommandName=
                CommandType=
                ScriptName=
                CommandPath=
                CommandLine=</Message><Level>Information</Level><Task>Engine
Lifecycle</Task><Opcode>Info</Opcode><Channel></Channel><Provider></Provider><Keywords><Ke
yword>Classic</Keyword></Keywords></RenderingInfo></Event>
```

Application Logs

- Application Logs generated by pre-7.1.4 Windows Agent
- Application Logs generated by 7.1.4 and later Windows Agent

Application Logs generated by pre-7.1.4 Windows Agent

```
2024-02-27T17:32:20Z FSM-GFU-Windows8-George-172-30-56-122 172.30.56.122 AccelOps-WUA-
WinLog-Application [phCustId]="2000" [customer]="org1" [monitorStatus]="Success"
[Locale]="en-US" [MachineGuid]="69c490e4-9c32-49cb-aefa-3ff10bcfc98a" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [eventName]="Application" [eventSource]="Microsoft-
Windows-Security-SPP" [eventId]="16384" [eventType]="Information" [domain]=""
[computer]="FSM-GFU-Windows8-George-172-30-56-122" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="Feb 27 2024 17:32:20" [deviceTime]="Feb 27 2024 17:32:20"
[msg]="Successfully scheduled Software Protection service for re-start at 2024-02-
28T00:55:20Z. Reason: RulesEngine."
```

Application Logs generated by 7.1.4 and later Windows Agent

The events are generated in XML format.

```
2024-02-27T20:07:07Z GFU-Win11.getest.com 172.30.56.124 FSM-WUA-WinLog-Application
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="f91bb25d-8ac1-45ea-8345-6263c2168970" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Microsoft-Windows-Security-SPP' Guid='{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}'
EventSourceName='Software Protection Platform Service'/><EventID
Qualifiers='16384'>16384</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcod
e>0</Opcode><Keywords>0x80000000000000</Keywords><TimeCreated SystemTime='2024-02-
27T20:07:07.0902766Z'/><EventRecordID>75607</EventRecordID><Correlation/><Execution
ProcessID='5284' ThreadID='0'/><Channel>Application</Channel><Computer>GFU-
Win11.getest.com</Computer><Security/></System><EventData><Data>2024-02-
28T19:25:07Z</Data><Data>RulesEngine</Data></EventData><RenderingInfo Culture='en-
US'><Message>Successfully scheduled Software Protection service for re-start at 2024-02-
28T19:25:07Z. Reason:
RulesEngine.</Message><Level>Information</Level><Task></Task><Opcode></Opcode><Channel></C
hannel><Provider>Microsoft-Windows-Security-
SPP</Provider><Keywords><Keyword>Classic</Keyword></Keywords></RenderingInfo></Event>
```

Security Logs

- Security Logs generated by pre-7.1.4 Windows Agent
- Security Logs generated by 7.1.4 and later Windows Agent
- Security Logs in French Windows generated by pre-7.1.4 Windows Agent
- Security Logs in French Windows generated by 7.1.4 and later Windows Agent

Security Logs generated by pre-7.1.4 Windows Agent

```
2024-02-22T01:07:51Z GFU-Win10.gfu.com 172.30.56.127 AccelOps-WUA-WinLog-Security
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="72f70ae7-fedf-4dc0-92e7-0c953f46f87e" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [eventName]="Security" [eventSource]="Microsoft-
Windows-Security-Auditing" [eventId]="4703" [eventType]="Information" [domain]=""
[computer]="GFU-Win10.gfu.com" [user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="Feb
22 2024 01:07:51" [deviceTime]="Feb 22 2024 01:07:51" [msg]="A token right was adjusted."
[[Subject]][Security ID]="S-1-5-18" [Account Name]="GFU-WIN10$" [Account Domain]="GFU"
[Logon ID]="0x3E7" [[Target Account]][Security ID]="S-1-5-18" [Account Name]="GFU-WIN10$"
[Account Domain]="GFU" [Logon ID]="0x3E7" [[Process Information]][Process ID]="0x3348"
[Process Name]="C:\\Windows\\System32\\msiexec.exe" [Enabled Privileges]="" [Disabled
Privileges]="SeRestorePrivilege,SeTakeOwnershipPrivilege"
```

Security Logs generated by 7.1.4 and later Windows Agent

The events are generated in XML format.

```
2024-02-27T21:19:33Z FSM-GFU-Windows2019-WIN2019-172-30-56-129 172.30.56.129 FSM-WUA-
WinLog-Security [phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-
US" [MachineGuid]="1e749ab9-bf6e-4052-806b-02068b2d4465" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-a5ba-
3e3b0328c30d}'/><EventID>4703</EventID><Version>0</Version><Level>0</Level><Task>13317</Ta
sk><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2024-
02-
27T21:19:32.430796700Z'/><EventRecordID>9064813051</EventRecordID><Correlation/><Execution
ProcessID='4' ThreadID='5944'/><Channel>Security</Channel><Computer>FSM-GFU-Windows2019-
WIN2019-172-30-56-129</Computer><Security/></System><EventData><Data
Name='SubjectUserSid'>S-1-5-18</Data><Data Name='SubjectUserName'>FSM-GFU-
WINDOWS$</Data><Data Name='SubjectDomainName'>WORKGROUP</Data><Data
Name='SubjectLogonId'>0x3e7</Data><Data Name='TargetUserSid'>S-1-0-0</Data><Data
Name='TargetUserName'>FSM-GFU-WINDOWS$</Data><Data
Name='TargetDomainName'>WORKGROUP</Data><Data Name='TargetLogonId'>0x3e7</Data><Data
```

```
Name='ProcessName'>C:\\Windows\\System32\\svchost.exe</Data><Data
Name='ProcessId'>0xbdc</Data><Data
Name='EnabledPrivilegeList'>SeAssignPrimaryTokenPrivilege
   SeIncreaseQuotaPrivilege
   SeSecurityPrivilege
   SeTakeOwnershipPrivilege
   SeLoadDriverPrivilege
   SeSystemtimePrivilege
   SeBackupPrivilege
   SeRestorePrivilege
   SeShutdownPrivilege
   SeSystemEnvironmentPrivilege
   SeUndockPrivilege
   SeManageVolumePrivilege</Data><Data Name='DisabledPrivilegeList'>-
</Data></EventData></Event>
```

Security Logs in French Windows generated by pre-7.1.4 Windows Agent

```
2024-02-27T21:59:31Z WIN-H8PJIB0G6QJ 172.30.56.128 AccelOps-WUA-WinLog-Security
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="fr-FR"
[MachineGuid]="d1a2dfa9-a8a3-4d5d-b151-2264a07678b4" [timeZone]="+0100"
[extEventRecvProto]="Windows Agent" [eventName]="Security" [eventSource]="Microsoft-
Windows-Security-Auditing" [eventId]="4798" [eventType]="Information" [domain]=""
[computer]="WIN-H8PJIB0G6QJ" [user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="Feb
27 2024 21:59:31" [deviceTime]="Feb 27 2024 21:59:31" [msg]="Une adhésion au groupe local
d'un utilisateur a été énumérée." [[Objet]][ID de sécurité]="S-1-5-18" [Nom du
compte]="WIN-H8PJIB0G6QJ$" [Domaine du compte]="WORKGROUP" [ID d'ouverture de
session]="0x3E7" [[Utilisateur]][ID de sécurité]="S-1-5-21-1726319904-1389896535-
1900308177-500" [Nom du compte]="Administrateur" [Domaine du compte]="WIN-H8PJIB0G6QJ"
[[Informations sur le processus]][ID du processus]="0x1270" [Nom du processus]="C:\\Program
Files\\Fortinet\\FortiSIEM\\osquery.exe"
```

Security Logs in French Windows generated by 7.1.4 and later Windows Agent

The events are generated in XML format.

```
2024-02-27T21:50:49Z WIN-H8PJIB0G6QJ 172.30.56.128 FSM-WUA-WinLog-Security
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="fr-FR"
[MachineGuid]="d1a2dfa9-a8a3-4d5d-b151-2264a07678b4" [timeZone]="+0100"
[extEventRecvProto]="Windows Agent" [level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-a5ba-
```

```
3e3b0328c30d}'/><EventID>4798</EventID><Version>0</Version><Level>0</Level><Task>13824</Ta
sk><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2024-
02-27T21:50:49.478751700Z'/><EventRecordID>217951</EventRecordID><Correlation ActivityID='
{dc36aa0a-69c4-0001-58aa-36dcc469da01}'/><Execution ProcessID='612'
ThreadID='4748'/><Channel>Security</Channel><Computer>WIN-
H8PJIB0G6QJ</Computer><Security/></System><EventData><Data
Name='TargetUserName'>WDAGUtilityAccount</Data><Data Name='TargetDomainName'>WIN-
H8PJIB0G6QJ</Data><Data Name='TargetSid'>S-1-5-21-1726319904-1389896535-1900308177-
504</Data><Data Name='SubjectUserSid'>S-1-5-18</Data><Data Name='SubjectUserName'>WIN-
H8PJIB0G6QJ$</Data><Data Name='SubjectDomainName'>WORKGROUP</Data><Data
Name='SubjectLogonId'>0x3e7</Data><Data Name='CallerProcessId'>0x128</Data><Data
Name='CallerProcessName'>C:\\Program
Files\\Fortinet\\FortiSIEM\\osquery.exe</Data></EventData></Event>
```

DNS Logs

- DNS System Logs generated by pre-7.1.4 Windows Agent
- DNS System Logs generated by 7.1.4 and later Windows Agent

DNS System Logs generated by pre-7.1.4 Windows Agent

```
2024-02-28T00:05:04Z GFU-WIN2016.getest.com 172.30.56.121 AccelOps-WUA-WinLog-DNS Server
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="4a2804f4-e1b6-4e28-ac76-de5aa103d255" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [eventName]="DNS Server" [eventSource]="Microsoft-
Windows-DNS-Server-Service" [eventId]="2" [eventType]="Information" [domain]="NT AUTHORITY"
[computer]="GFU-WIN2016.getest.com" [user]="SYSTEM" [userSID]="S-1-5-18"
[userSIDAcctType]="User" [eventTime]="Feb 28 2024 00:05:03" [deviceTime]="Feb 28 2024
00:05:03" [msg]="The DNS server has started."
```

DNS System Logs generated by 7.1.4 and later Windows Agent

The events are generated in XML format.

```
2024-02-27T23:50:52Z GFU-WIN2016-126.gfu.com 172.30.56.126 FSM-WUA-WinLog-DNS Server
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="967fcbac-7d74-445f-99de-c5a1f0acf59d" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
```

```
Name='Microsoft-Windows-DNS-Server-Service' Guid='{71A551F5-C893-4849-886B-
B5EC8502641E}'/><EventID>2</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opc
ode>0</Opcode><Keywords>0x8000000000001000</Keywords><TimeCreated SystemTime='2024-02-
27T23:50:51.965038300Z'/><EventRecordID>330</EventRecordID><Correlation/><Execution
ProcessID='6448' ThreadID='6892'/><Channel>DNS Server</Channel><Computer>GFU-WIN2016-
126.gfu.com</Computer><Security UserID='S-1-5-18'/></System><EventData Name='DNS_EVENT_
STARTUP_OK'></EventData><RenderingInfo Culture='en-US'><Message>The DNS server has
started.</Message><Level>Information</Level><Task></Task><Opcode>Info</Opcode><Channel></C
hannel><Provider>Microsoft-Windows-DNS-Server-
Service</Provider><Keywords></Keywords></RenderingInfo></Event>
```

DHCP Logs

```
AccelOps-WUA-DHCP-Generic
Thu May 07 05:44:44 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="00" [Date]="05/07/15"
[Time]="13:44:08" [Description]="Started" [IP Address]="" [Host Name]="" [MAC Address]=""
[User Name]="" [ TransactionID]="0"
[ QResult]="6" [Probationtime]="" [ CorrelationID]="" [Dhcid.]=""
```

```
#AccelOps-WUA-DHCP-IP-ASSIGN
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="10" [Date]="05/07/15"
[Time]="13:56:37" [Description]="Assign" [IP Address]="10.1.2.124" [Host Name]="Agent-
247.yj" [MAC Address]="000C2922118E"
[User Name]="" [ TransactionID]="2987030242" [ QResult]="0" [Probationtime]="" [
CorrelationID]="" [Dhcid.]=""
```

```
#AccelOps-WUA-DHCP-Generic(Release)
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="12" [Date]="05/07/15"
[Time]="13:56:33" [Description]="Release" [IP Address]="10.1.2.124" [Host Name]="Agent-
247.yj" [MAC Address]="000C2922118E"
[User Name]="" [ TransactionID]="2179405838" [ QResult]="0" [Probationtime]="" [
CorrelationID]="" [Dhcid.]=""
```

```
#AccelOps-WUA-DHCP-IP-LEASE-RENEW
Wed Feb 25 02:53:28 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="11" [Date]="02/25/15"
[Time]="10:53:19" [Description]="Renew" [IP Address]="10.1.2.123" [Host Name]="WIN-2008-
249.yj" [MAC Address]="0050568F1B5D"
```

```
[User Name]="" [ TransactionID]="1136957584" [ QResult]="0" [Probationtime]="" [
CorrelationID]="" [Dhcid.]=""
```

IIS Logs

```
#AccelOps-WUA-IIS-Web-Request-Success
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-IIS
[monitorStatus]="Success" [date]="2015-05-07"
[time]="03:44:28" [s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-
ip]="10.1.2.242" [cs-method]="GET"
[cs-uri-stem]="/welcome.png" [cs-uri-query]="-" [s-port]="80" [cs-username]="-" [c-
ip]="10.1.20.232" [cs-version]="HTTP/1.1"
[cs(User-Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/42.0.2311.135+Safari/537.36"
[cs(Cookie)]="-" [cs(Referer)]="http://10.1.2.242/" [cs-host]="10.1.2.242" [sc-
status]="200" [sc-substatus]="0" [sc-win32-status]="0"
[sc-bytes]="185173" [cs-bytes]="324" [time-taken]="78" [site]="Default Web Site"
[format]="W3C"
```

```
#AccelOps-WUA-IIS-Web-Client-Error
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-IIS
[monitorStatus]="Success" [date]="2015-05-07" [time]="03:44:37"
[s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-ip]="10.1.2.242" [cs-
method]="GET" [cs-uri-stem]="/wrongpage" [cs-uri-query]="-"
[s-port]="80" [cs-username]="-" [c-ip]="10.1.20.232" [cs-version]="HTTP/1.1" [cs(User-
Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/42.0.2311.135+Safari/537.36" [cs(Cookie)]="-" [cs(Referer)]="-"
[cs-host]="10.1.2.242" [sc-status]="404"
[sc-substatus]="0" [sc-win32-status]="2" [sc-bytes]="1382" [cs-bytes]="347" [time-
taken]="0" [site]="Default Web Site" [format]="W3C"
```

```
#AccelOps-WUA-IIS-Web-Forbidden-Access-Denied
Thu May 07 03:30:39 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-IIS
[monitorStatus]="Success" [date]="2015-05-07" [time]="03:30:15" [s-ip]="10.1.2.249" [cs-
method]="POST" [cs-uri-stem]="/AOCACWS/AOCACWS.svc" [cs-uri-query]="-" [s-port]="80" [cs-
username]="-"
[c-ip]="10.1.2.42" [cs(User-Agent)]="-" [sc-status]="403" [sc-substatus]="4" [sc-win32-
status]="5" [time-taken]="1" [site]="Default Web Site"
[format]="W3C"
```

DFS Logs

```
#Win-App-DFSR-1002
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1002" [eventType]="Information" [domain]=""
[computer]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015 11:01:12"
[msg]="The DFS Replication service is starting."
```

```
#Win-App-DFSR-1004
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1004" [eventType]="Information" [domain]=""
[computer]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015 11:01:12"
[msg]="The DFS Replication service has started."
```

```
#Win-App-DFSR-1006
Thu May 07 03:01:10 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1006" [eventType]="Information" [domain]=""
[computer]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:10" [deviceTime]="May 07 2015 11:01:10"
[msg]="The DFS Replication service is stopping."
```

```
#Win-App-DFSR-1008
Thu May 07 03:01:11 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1008" [eventType]="Information" [domain]=""
[computer]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:11" [deviceTime]="May 07 2015 11:01:11"
[msg]="The DFS Replication service has stopped."
```

File Content Monitoring Logs

```
#AccelOps-WUA-UserFile
Thu May 07 05:40:08 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-UserFile
```

```
[monitorStatus]="Success" [fileName]="C:\test\i.txt"
[msg]="another newline adddeddddd"
```

File Integrity Monitoring Logs

The following sections describe various use cases that can be detected by File Integrity Monitoring Logs.

- Use Case 1: File or Directory Created
- Use Case 2: File or Directory Deleted
- Use Case 3: File Content Modified
- Use Case 4: File Content Modified and Upload is Selected
- Use Case 5: File Renamed
- Use Case 6: File Permission Changed
- Use Case 7: File Ownership Changed
- Use Case 8: File Archive Bit Changed
- Use Case 9: File Baseline Changed

Use Case 1: File or Directory Created

Event Type

`AO-WUA-FileMon-Added`

The 'added' event is triggered when a file or directory is added into a directory that is being monitored. Actions such as the following will cause this event to generate:

- Copying a file/directory
- Creating a shortcut of a file/directory
- Sending to compressed zip
- Restoring a file/directory
- Downloading or saving a file

Important Event Attributes

- `userId`: The ID of the user who added the file.
- `domain`: The user's domain for a Domain computer.
- `osObjType`- Can be either File or Directory.
- `fileName`: The name of the file or directory that was added.
- `hashCode, hashAlgo`: The file hash obtained by using the specified algorithm.
- `procName`: The name of the Windows process that was used to create the file.
- `fileOwner`: The owner of the file.
- `targetUserType, targetUser`: The user or group to whom the permission applies.
- `targetFilePermit`: The permitted file operations.

- `targetFileDeny`: The denied file operations.
- `archiveSet`: Is `true` if the Archive bit is set for this file; `false` otherwise.

Reports

`Agent FIM: Windows File/Directory Created/Deleted/Renamed`

Rules

`Agent FIM - Windows File or Directory Created`

Sample Log

```
2020-03-25T07:30:50Z Win-167 10.30.2.167 AccelOps-WUA-FileMon [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="e892a6e4-bbfa-
4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe" [domain]="ACME" [eventTime]="Mar
25 2020 07:30:48" [fileName]="C:\\test\\New Text Document.txt" [osObjAction]="Added"
[objectType]="File"
[hashCode]="e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
[hashAlgo]="SHA256" [procName]="C:\\Windows\\explorer.exe" [msg]="" [archiveSet]="true"
[fileOwner]=""
```

Use Case 2: File or Directory Deleted

Event Type

`AO-WUA-FileMon-Removed`

The 'removed' event is triggered when a file or directory is removed. Actions such as the following will cause this event to generate:

- Moving a file from one directory to another
- Deleting a file or directory

Important Event Attributes

- `userId`: The ID of the user who removed the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The name of the file that was removed.
- `procName`: The Windows process that was used to remove the file.

Report

`Agent FIM: Windows File/Directory Creation/Deletion/Rename`

Rule

`Agent FIM - Windows File or Directory Deleted`

Sample Log

```
2020-03-25T07:43:24Z Win-167 10.30.2.167 AccelOps-WUA-FileMon [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="e892a6e4-bbfa-
4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe" [domain]="ACME" [eventTime]="Mar
25 2020 07:43:21" [fileName]="C:\\test\\test1.txt" [osObjAction]="Removed"
```

```
[objectType]="Unknown" [hashCode]="" [hashAlgo]="SHA256"
[procName]="C:\\Windows\\explorer.exe" [msg]="" [archiveSet]="false" [fileOwner]=""
```

Use Case 3: File Content Modified

Event Type

`AO-WUA-FileMon-Modified`

The 'modified' event is triggered when a file or directory is modified. Actions such as the following will cause this event to generate:

- Add or delete 'text' from the file
- Simply saving a file, even without a change, will trigger this event

Important Event Attributes

- `userId`: The user who modified the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The name of the file that was modified.
- `procName`: The Windows process that was used to modify the file.
- `hashCode, hashAlgo`: The file hash after modification and the algorithm used to calculate the hash.

Report

`Agent FIM: Windows File Content Modified`

Rule

`Agent FIM - Windows File Content Modified`

Sample Log

```
2020-03-25T10:50:40Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe"
[domain]="ACME" [eventTime]="Mar 25 2020 10:50:37" [fileName]="C:\\test\\test.txt"
[osObjAction]="Modified" [objectType]="File"
[hashCode]="6396e3c19b155770f3ae25afa5f29832d6f35b315407ed88820339b705fd2bcc"
[hashAlgo]="SHA256" [procName]="C:\\Windows\\System32\<br/>otepad.exe" [msg]=""
[archiveSet]="true" [fileOwner]=""
```

Use Case 4: File Content Modified and Upload is Selected

Event Type

`PH_DEV_MON_FILE_CONTENT_CHANGE`

Important Event Attributes

- `userId`: The ID of the user who modified the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The name of the file that was modified.
- `procName`: The Windows process that was used to modify the file.
- `hashCode, hashAlgo`: The file hash after modification and the algorithm used to calculate the hash.
- `oldSVNVersion`: The SVN revision number of file before the change.
- `newSVNVersion`: The SVN revision number of file after the change.
- `addedItem`: The lines that were added to the file.
- `deletedItem`: The lines that were removed from the file.

Report

`Agent FIM: Windows File Content Modified in SVN`

Rule

`Audited file or directory content modified in SVN`

Sample Log

```
<14>Mar 25 20:30:44 sp3 phPerfMonitor[17521]: [PH_DEV_MON_FILE_CONTENT_CHANGE]:
[eventSeverity]=PHL_INFO,[procName]=phPerfMonitor,[fileName]=phSvnUpdate.cpp,
[lineNumber]=306,[phCustId]=2000,[hostName]=Win-169,[hostIpAddr]=10.30.3.169,
[fileName]=/C:/test/test.txt,[hashCode]=08998b2cce90ee6695bd8dae82d43137,
[oldSVNVersion]=50,[newSVNVersion]=51,[deletedItem]=(none),[addedItem]=333;,
[user]=Administrator,[hashAlgo]=SHA256,[phLogDetail]=
```

Use Case 5: File Renamed

Event Type

`AO-WUA-FileMon-Renamed-New-Name`

The 'new-name' event is triggered when a file or directory is renamed. This event encapsulates the new name of the file/directory.

Important Event Attributes

- `userId`: The ID of the user who renamed the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The new name of the file.
- `procName`: The Windows process that was used to rename the file.
- `hashCode, hashAlgo`: The new file hash using the specified algorithm.

Report

`Agent FIM: Windows File/Directory Creation/Deletion/Rename`

Rule

None

Sample Log

```
2020-03-25T09:59:34Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe"
[domain]="ACME" [eventTime]="Mar 25 2020 09:59:32" [fileName]="C:\\test\\test5.txt"
[osObjAction]="Renamed [New Name]" [objectType]="File"
[hashCode]="2b64c6d9afd8a34ed0dbf35f7de171a8825a50d9f42f05e98fe2b1addf00ab44"
[hashAlgo]="SHA256" [procName]="C:\\Windows\\explorer.exe" [msg]="" [archiveSet]="true"
[fileOwner]=""
```

Event Type

`AO-WUA-FileMon-Renamed-Old-Name`

Important Event Attributes

`userId`: The ID of the user who modified the file.

`domain`: The user's domain for a Domain computer.

`fileName`: The old name of the file before renaming.

`procName`: The Windows process that was used to remove the file.

Report

`Agent FIM: Windows File/Directory Creation/Deletion/Rename`

Rule

None

Sample Log

None

Use Case 6: File Permission Changed

Event Type

`AO-WUA-FileMon-PermissionChange`

The 'permission change' event is triggered when a file or directory undergoes a change in permissions. Actions such as the following will cause this event to generate:

- Sharing out a directory
- Modification of the permissions
- Add group or user to file or directory

Important Event Attributes

- `userId`: The ID of the user who modified the file permission.
- `domain`: The user's domain for a Domain computer.
- `objectType`: The type of object. Can be `File` or `Directory`.
- `fileName`: The name of the file or directory whose permission was changed.
- `procName`: The Windows process that was used to change the permission.

- `hashCode, hashAlgo`: The file hash using the specified algorithm.
- `fileOwner`: The name of the owner of the file.
- `targetUserType, targetUser`: The name of the user or group to whom the permission below applies.
- `targetFilePermit`: The permitted file operations after change.
- `targetFileDeny`: The denied file operations after change.
- `archiveSet`: Is `true` if the `Archive` bit is set for this file; `false` otherwise.

Report

`Agent FIM: Windows File/Directory Permission Changes`

Rule

`Agent FIM - Windows File Permission Changed`

Sample Log

```
2020-03-25T10:21:00Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe"
[domain]="ACME" [eventTime]="Mar 25 2020 10:20:58" [fileName]="C:\\test\\test.txt"
[osObjAction]="PermissionChange" [objectType]="File"
[hashCode]="7936d255ef43706a93fdd15f4bbfde45e3b2d2b9a0d4cc7c39184cf745ab78c5"
[hashAlgo]="SHA256" [procName]="C:\\Windows\\System32\\dllhost.exe" [msg]=""
[archiveSet]="true" [fileOwner]="Joe" [targetUserType]="USER"
[targetUser]="BUILTIN\Administrators" [targetFilePermit]="ALL" [targetFileDeny]="WRITE"
```

Use Case 7: File Ownership Changed

Event Type

`AO-WUA-FileMon-OwnershipChange`

The 'ownership change' event is triggered when a file or directory's owner has been changed.

Important Event Attributes

- `userId`: The ID of the user who modified the file ownership.
- `domain`: The user's domain for a Domain computer.
- `objectType`: The type of object whose ownership was changed: `File` or `Directory`.
- `fileName`: The name of the file or directory whose ownership was changed.
- `procName`: The Windows process that was used to change ownership.
- `hashCode, hashAlgo`: The file hash using the specified algorithm.
- `fileOwner`: The name of the new file owner.
- `archiveSet`: Is `true` if the `Archive` bit is set for this file; `false` otherwise.

Report

`Agent FIM: Windows File/Directory Ownership Changes`

Rule

`Agent FIM - Windows File Ownership Changed`

Sample Log

```
2020-03-06T07:08:56Z Win-167 10.30.2.167 AccelOps-WUA-FileMon [phCustId]="1"
[customer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="e892a6e4-bbfa-
4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="Administrator" [domain]="WIN-167"
[eventTime]="Mar 06 2020 07:08:53" [fileName]="C:\\test\\test1.txt"
[osObjAction]="OwnershipChange" [objectType]="File"
[hashCode]="d17f25ecfbcc7857f7bebea469308be0b2580943e96d13a3ad98a13675c4bfc2"
[hashAlgo]="SHA256" [procName]="C:\\Windows\\System32\\dllhost.exe" [msg]=""
[archiveSet]="true" [fileOwner]="Joe"
```

Use Case 8: File Archive Bit Changed

Event Type

`AO-WUA-FileMon-ArchivedBitChange`

The 'archived bit change' event is triggered when a file or directory undergoes an archive change. Actions such as the following will cause this event to generate:

- Under the General tab of the files' properties:
  - Checking the Read-only or Hidden checkboxes in the Attributes row.
  - Click Advanced... and checking or unchecking any of the checkboxes for File attributes or Compress or Encrypt attributes.

Important Event Attributes

- `userId`: The ID of the user who modified the file.
- `domain`: The user's domain for a Domain computer.
- `objectType`: The type of object whose `Archive` bit was changed: `File` or `Directory`.
- `fileName`: The name of the file whose archive bit was changed.
- `procName`: The Windows process that was used to change archive bit.
- `hashCode, hashAlgo`: The file hash using the specified algorithm.
- `archiveSet`: Is `true` if the `Archive` bit is set for this file; `false` otherwise.

Report

`Agent FIM: Windows File/Directory Archive Bit Changes`

Rule

`Agent FIM - Windows File/Directory Archive Bit Changed`

Sample Log

```
2020-03-25T10:02:38Z WIN-167.fortinet.wulei.com 10.30.2.167 AccelOps-WUA-FileMon
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="e892a6e4-bbfa-4ba6-bc8c-00d2c31812b4" [timeZone]="+0800" [userId]="jdoe"
[domain]="ACME" [eventTime]="Mar 25 2020 10:02:35" [fileName]="C:\\test\\test.txt"
[osObjAction]="ArchivedBitChange" [objectType]="File"
[hashCode]="7936d255ef43706a93fdd15f4bbfde45e3b2d2b9a0d4cc7c39184cf745ab78c5"
[hashAlgo]="SHA256" [procName]="C:\\Windows\\System32\\attrib.exe" [msg]=""
[archiveSet]="false" [fileOwner]=""
```

Use Case 9: File Baseline Changed

Event Type

`AO-WUA-FileMon-BaselineChange`

Important Event Attributes

- `userId`: The ID of the user who modified the file.
- `domain`: The user's domain for a Domain computer.
- `fileName`: The name of the file that was changed.
- `procName`: The Windows process that was used to remove the file.
- `hashCode, hashAlgo`: The file hash using the specified algorithm.
- `targetHashCode`: The hash of the target file (defined in the GUI).

Report

`Agent FIM: Windows File Change from Baseline`

Rule

`Agent FIM - Windows File Changed From Baseline`

Sample Log

```
2020-03-25T12:52:42Z Win-169 10.30.3.169 AccelOps-WUA-FileMon [phCustId]="2000"
[customer]="org1" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="5c83ec12-73fd-
4e06-a396-1f128564f09e" [timeZone]="+0800" [userId]="Administrator" [domain]="WINSRV2012-
169" [fileName]="C:\\test\\test.txt" [osObjAction]="BaselineChange"
[hashCode]="c1f79ea2bbfb77bf30446a4c9be762eb" [hashAlgo]="MD5"
[targetHashCode]="74DE7651DFC55294CC59240AE514A676" [msg]="
```

Installed Software Logs

```
#AccelOps-WUA-InstSw-Added
Thu May 07 05:28:17 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-InstSw
[monitorStatus]="Success" [osObjAction]="Added"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVersion]="9.20.00.0"
```

```
#AccelOps-WUA-InstSw-Removed
Thu May 07 05:28:30 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-InstSw
[monitorStatus]="Success" [osObjAction]="Removed"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVersion]="9.20.00.0"
```

Registry Change Logs

```
#AccelOps-WUA-Registry-Modified
Thu May 07 04:01:58 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-Registry
[monitorStatus]="Success"
[regKeyPath]="HKLM\\SOFTWARE\\Microsoft\\ExchangeServer\\v14\\ContentIndex\\CatalogHealth\\
{0d2a342a-0b15-4995-93db-d18c3df5860d}" [regValueName]="TimeStamp" [regValueType]="1"
[osObjAction]="Modified"
[oldRegValue]="MgAwADEANQAtADAANQAtADAANwAgADAAMwA6ADQAOQA6ADQANwBaAAAA"
[newRegValue]="MgAwADEANQAtADAANQAtADAANwAgADAANAA6ADAAMQA6ADQAOABaAAAA"
```

```
#AccelOps-WUA-Registry-Removed
Thu May 07 05:25:09 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-Registry
[monitorStatus]="Success"
[regKeyPath]="HKLM\\SOFTWARE\\RegisteredApplications" [regValueName]="Skype"
[regValueType]="1" [osObjAction]="Removed"
[oldRegValue]="UwBPAEYAVABXAEEAUgBFAFwAQwBsAGkAZQBuAHQAcwBcAEkAbgB0AGUAcgBuAGUAdAAgAEMAYQB
sAGwAXABTAGsAeQBwAGUAXABDAGEAcABhAGIAaQBsAGkAdABpAGUAcwBkAGgAZABoAGQAaABkAGgAZABoAGQAAAA="
[newRegValue]=""
```

Removeable Media Monitoring Logs

AO-WUA-RemovableMedia-Insert

```
2022-06-24T19:06:55Z CD-DESK-S 0.0.0.0 AccelOps-WUA-RemovableMedia-Insert [phCustId]="1"
[customer]="super" [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-
41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]="" [domain]="" [eventTime]="Jun 24 2022
19:06:55" [fileName]="" [diskName]="D:" [isMediaEncrypted]="false" [osObjAction]=""
[diskType]="USB" [diskDisplayName]="Samsung USB" [diskVendor]="samsung"
[hwDiskModel]="flash_drive_fit 1100" [msg]="Storage media inserted."
```

AO-WUA-RemovableMedia-Write-ModifyFile

```
2022-06-24T19:25:06Z CD-DESK-S 192.168.1.147 AccelOps-WUA-RemovableMedia-Write
[phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]=""
[domain]="" [eventTime]="Jun 24 2022 19:25:02" [fileName]="D:\\agenttest\\Wireshark-win64-
3.6.6.exe" [diskName]="D:" [isMediaEncrypted]="false" [osObjAction]="Modified"
[diskType]="USB" [diskDisplayName]="Samsung USB" [diskVendor]="samsung"
[hwDiskModel]="flash_drive_fit 1100" [msg]=""
```

AO-WUA-RemovableMedia-Write-AddFile

```
2022-06-24T19:25:01Z CD-DESK-S 192.168.1.147 AccelOps-WUA-RemovableMedia-Write
[phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]=""
[domain]="" [eventTime]="Jun 24 2022 19:25:00" [fileName]="D:\\agenttest\\Wireshark-win64-
3.6.6.exe" [diskName]="D:" [isMediaEncrypted]="false" [osObjAction]="Added"
[diskType]="USB" [diskDisplayName]="Samsung USB" [diskVendor]="samsung"
[hwDiskModel]="flash_drive_fit 1100" [msg]=""
```

AO-WUA-RemovableMedia-Write-RemoveFile

```
2022-06-24T19:24:01Z CD-DESK-S 192.168.1.147 AccelOps-WUA-RemovableMedia-Write
[phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="38ba7825-34a2-41b8-8e3d-0548878bef5b" [timeZone]="-0500" [user]=""
[domain]="" [eventTime]="Jun 24 2022 19:23:56" [fileName]="D:\\agenttest\\WinSCP-5.17.8-
Setup.zip" [diskName]="D:" [isMediaEncrypted]="false" [osObjAction]="Removed"
[diskType]="USB" [diskDisplayName]="Samsung USB" [diskVendor]="samsung"
[hwDiskModel]="flash_drive_fit 1100" [msg]=""
```

WMI Logs

```
#AccelOps-WUA-WMI-Win32_Processor
Thu May 07 03:53:33 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WMI
[monitorStatus]="Success"  [__CLASS]="Win32_Processor"
[AddressWidth]="64" [Architecture]="9" [Availability]="3" [Caption]="Intel64 Family 6 Model
26 Stepping 5" [ConfigManagerErrorCode]="" [ConfigManagerUserConfig]="" [CpuStatus]="1"
[CreationClassName]="Win32_Processor" [CurrentClockSpeed]="2266" [CurrentVoltage]="33"
[DataWidth]="64" [Description]="Intel64 Family 6 Model 26 Stepping 5" [DeviceID]="CPU0"
[ErrorCleared]="" [ErrorDescription]=""
[ExtClock]="" [Family]="12" [InstallDate]="" [L2CacheSize]="0" [L2CacheSpeed]=""
[L3CacheSize]="0" [L3CacheSpeed]="0"
[LastErrorCode]="" [Level]="6" [LoadPercentage]="8" [Manufacturer]="GenuineIntel"
[MaxClockSpeed]="2266"
[Name]="Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz" [NumberOfCores]="1"
[NumberOfLogicalProcessors]="1"
[OtherFamilyDescription]="" [PNPDeviceID]="" [PowerManagementCapabilities]=""
[PowerManagementSupported]="0"
[ProcessorId]="0FEBFBFF000106A5" [ProcessorType]="3" [Revision]="6661" [Role]="CPU"
[SocketDesignation]="CPU socket #0"
[Status]="OK" [StatusInfo]="3" [Stepping]="" [SystemCreationClassName]="Win32_
ComputerSystem" [SystemName]="WIN-2008-LAW-AG"
UniqueId]="" [UpgradeMethod]="4" [Version]="" [VoltageCaps]="2"
```

UEBA Information

The following UEBA content is available.

- Comparing UEBA Sources
- UEBA based on Log
- UEBA Sample Logs

Comparing UEBA Sources

- Windows UEBA vs Log Based UEBA
- UEBA Rules Trigger Based on Log Source

Windows UEBA vs Log Based UEBA

The following table provides details on Windows UEBA Agent versus log based UEBA.

Scenario	Windows UEBA Agent	Windows Security Log	Windows Sysmon	Linux Agent	Linux Log
File create	Yes	No	Yes	No	No
File delete	Yes	Yes	Yes	No	No
File read	Yes	No	No	No	No
File write	Yes	No	No	No	No
File move	Yes	No	No	No	No
File rename	Yes	No	No	No	No
File print	Yes	No	No	No	No
Process stop	Yes	Yes	Yes	No	No
Process create	Yes	Yes	Yes	Yes	No
File upload	Yes	No	No	No	No
File download	Yes	No	No	No	No
Machine on	Yes	Yes	No	No	No
Machine off	Yes	Yes	No	No	No
Drive mount	Yes	No	No	No	No
Drive un-mount	Yes	No	No	No	No
Host logon	Yes	Yes	No	No	Yes
Host logoff	Yes	Yes	No	No	Yes

UEBA Rules Trigger Based on Log Source

Rule Name	Windows UEBA Agent	Win Log (Win Security AND/OR Sysmon)	Linux Agent	Linux Log
UEBA AI detects unusual drive unmounted	Yes	No	No	No
UEBA AI detects unusual file creation	Yes	Yes (Sysmon)	No	No
UEBA AI detects unusual file deletion	Yes	Yes (Win Security OR Sysmon)	No	No
UEBA AI detects unusual file download	Yes	No	No	No
UEBA AI detects unusual file movement	Yes	No	No	No
UEBA AI detects unusual file printed	Yes	No	No	No
UEBA AI detects unusual file reading	Yes	No	No	No
UEBA AI detects unusual file renamed	Yes	No	No	No
UEBA AI detects unusual file upload	Yes	No	No	No
UEBA AI detects unusual file writing	Yes	No	No	No
UEBA AI detects unusual host logon	Yes	Yes (Win Security)	No	Yes
UEBA AI detects unusual machine off	Yes	Yes (Win Security)	No	No
UEBA AI detects unusual machine on	Yes	Yes (Win Security)	No	No
UEBA AI detects unusual new drive mounted	Yes	No	No	No
UEBA AI detects unusual process created	Yes	Yes (Win Security OR Sysmon)	Yes	No
UEBA AI detects unusual process not restarted	Yes	No	No	No
UEBA AI detects unusual process started	Yes	Yes (Win Security OR Sysmon)	No	No
UEBA AI detects unusual process stopped	Yes	Yes (Win Security OR Sysmon)	No	No

Rule Name	Windows UEBA Agent	Win Log (Win Security AND/OR Sysmon)	Linux Agent	Linux Log
UEBA AI detects unusual user logoff	Yes	Yes (Win Security)	No	Yes
UEBA Policy detects antivirus not started	Yes	No	No	No
UEBA Policy detects antivirus stopped	Yes	No	No	No
UEBA Policy detects backup applications	Yes	No	No	No
UEBA Policy detects browser download	Yes	No	No	No
UEBA Policy detects browser upload	Yes	No	No	No
UEBA Policy detects cloud upload	Yes	No	No	No
UEBA Policy detects email download	Yes	No	No	No
UEBA Policy detects email upload	Yes	No	No	No
UEBA Policy detects encryption tools	Yes	No	No	No
UEBA Policy detects file archiver application	Yes	No	No	No
UEBA Policy detects file printed	Yes	No	No	No
UEBA Policy detects files copied over remote desktop	Yes	No	No	No
UEBA Policy detects gaming application	Yes	No	No	No
UEBA Policy detects hacking tool and footprints	Yes	No	No	No
UEBA Policy detects hacking tool usage	Yes	No	No	No
UEBA Policy detects malicious powershell execution	Yes	No	No	No
UEBA Policy detects MTP read	Yes	No	No	No
UEBA Policy detects MTP write	Yes	No	No	No

Rule Name	Windows UEBA Agent	Win Log (Win Security AND/OR Sysmon)	Linux Agent	Linux Log
UEBA Policy detects NFS read	Yes	No	No	No
UEBA Policy detects nfs write	Yes	No	No	No
UEBA Policy detects potential leaver editing a CV at work	Yes	No	No	No
UEBA Policy detects potential pirated media	Yes	No	No	No
UEBA Policy detects ransomware	Yes	No	No	No
UEBA Policy detects ransomware file names	Yes	No	No	No
UEBA Policy detects ransomware file types	Yes	No	No	No
UEBA Policy detects removable media read	Yes	No	No	No
UEBA Policy detects removable media write	Yes	No	No	No
UEBA Policy detects snipping tool	Yes	No	No	No
UEBA Policy detects software installation	Yes	No	No	No
UEBA Policy detects suspicious applications	Yes	No	No	No
UEBA Policy detects Tor client usage	Yes	No	No	No
UEBA Policy detects uncommon VPN client	Yes	No	No	No

UEBA Based on Log

In earlier releases, User Entity Behavior Analytics (UEBA) was done based on proprietary logs collected by the FortiSIEM Windows UEBA Agent. Now, the analytics is extended to the following regular logs. Note that regular logs only cover a subset of the user activities compared to the FortiSIEM UEBA Agent.

Windows Security logs

- Unusual machine on activity based on Win-Security-4608 log
- Unusual machine off activity based on Win-Security-4609 log
- Unusual host logon activity based on Win-Security-4624 log
- Unusual host logoff activity based on Win-Security-4634 log
- Unusual file deletion based on Win-Security-4660 log
- Unusual process created based on Win-Security-4688 log
- Unusual process stopped based on Win-Security-4689 log

Windows Sysmon

- Unusual process created based on Win-Sysmon-1-Create-Process log
- Unusual process stopped based on Win-Sysmon-5-Process-Terminated log
- Unusual file creation based on Win-Sysmon-11-FileCreate log
- Unusual file deletion based on Win-Sysmon-23-File-Delete-archived and Win-Sysmon-26-File-Delete-logged log

Linux Agent

- Unusual process created based on LINUX_PROCESS_EXEC log
- Unusual machine off activity based on Generic_Unix_System_Shutdown log
- Unusual host logon activity based on Generic_Unix_Successful_SSH_Login log

For detailed comparison of Windows UEBA Agent versus log based UEBA, see Appendix - Comparing UEBA Sources.

UEBA Sample Logs

UEBA Events File Interaction sample logs are provided here.

FINS-Windows-new-drive-mounted

```
2022-06-24T19:06:58Z CD-DESK-S 0.0.0.0 [phCustId]="1" [customer]="super"
[monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-
0548878bef5b" [timeZone]="-0500" FortiInsight-Windows-Agent msg = {"ac":"new drive
mounted","ap":"ntoskrnl.exe","d":"2022-06-24T15:06:57.128-
04:00","r":"\\\\?\\swd#wpdbusenum#_??_usbstor#disk&ven_samsung&prod_flash_drive_fit&rev_
1100#0374216040008546&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}#{6ac27878-a6fa-4155-ba85-
f98f491d4f33} -> samsung usb","u":"__"}
```

FINS-Windows-file-written

```
2022-06-24T19:25:06Z CD-DESK-S 192.0.2.0  [phCustId]="1" [customer]="super"
[monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-
0548878bef5b" [timeZone]="-0500"  FortiInsight-Windows-Agent msg = {"ac":"file
written","ap":"explorer.exe","d":"2022-06-24T15:25:00.992-
04:00","r":"rm:\\d:\\agenttest\\wireshark-win64-3.6.6.exe","u":"cd-desk-s__durki"}
```

FINS-Windows-file-created

```
2022-06-24T19:25:00Z CD-DESK-S 192.0.2.0  [phCustId]="1" [customer]="super"
[monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-
0548878bef5b" [timeZone]="-0500"  FortiInsight-Windows-Agent msg = {"ac":"file
created","ap":"explorer.exe","d":"2022-06-24T15:25:00.215-
04:00","r":"rm:\\d:\\agenttest\\wireshark-win64-3.6.6.exe","u":"cd-desk-s__durki"}
```

FINS-Windows-file-deleted

```
2022-06-24T19:23:57Z CD-DESK-S 192.0.2.0  [phCustId]="1" [customer]="super"
[monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="38ba7825-34a2-41b8-8e3d-
0548878bef5b" [timeZone]="-0500"  FortiInsight-Windows-Agent msg = {"ac":"file
deleted","ap":"explorer.exe","d":"2022-06-24T15:23:56.794-
04:00","r":"rm:\\d:\\agenttest\\winscp-5.17.8-setup.zip","u":"cd-desk-s__durki"}
```

Windows Agent System Variables

A list of Windows Agent supported system variables is provided in the following table.

Windows Agent System Variable	Description
%WINDIR%	Windows directory (e.g., C:\Windows)
%SYSTEMROOT%	System root directory (often the same as %WINDIR%)
%SYSTEMDRIVE%	The drive on which Windows is installed (e.g., C:).
%TEMP%	Temporary files directory for the current user.
%TMP%	Temporary files directory for the current user.
%APPDATA%	Application data directory for the current user (e.g., C:\Users\Username\AppData\Roaming).
%LOCALAPPDATA%	Local application data directory for the current user (e.g., C:\Users\Username\AppData\Local).
%PROGRAMDATA%	Application data directory for all users (e.g., C:\ProgramData).
%ALLUSERSPROFILE%	The path to the All Users profile (e.g., C:\ProgramData).
%PROGRAMFILES%	The path to the Program Files directory (e.g., C:\Program Files).
%PROGRAMFILES(X86)%	The path to the Program Files (x86) directory on 64-bit systems (e.g., C:\Program Files (x86)).
%COMMONPROGRAMFILES%	The path to the common Program Files directory (e.g., C:\Program Files\Common Files).
%COMMONPROGRAMFILES (X86)%	The path to the common Program Files (x86) directory on 64-bit systems (e.g., C:\Program Files (x86)\Common Files).

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.