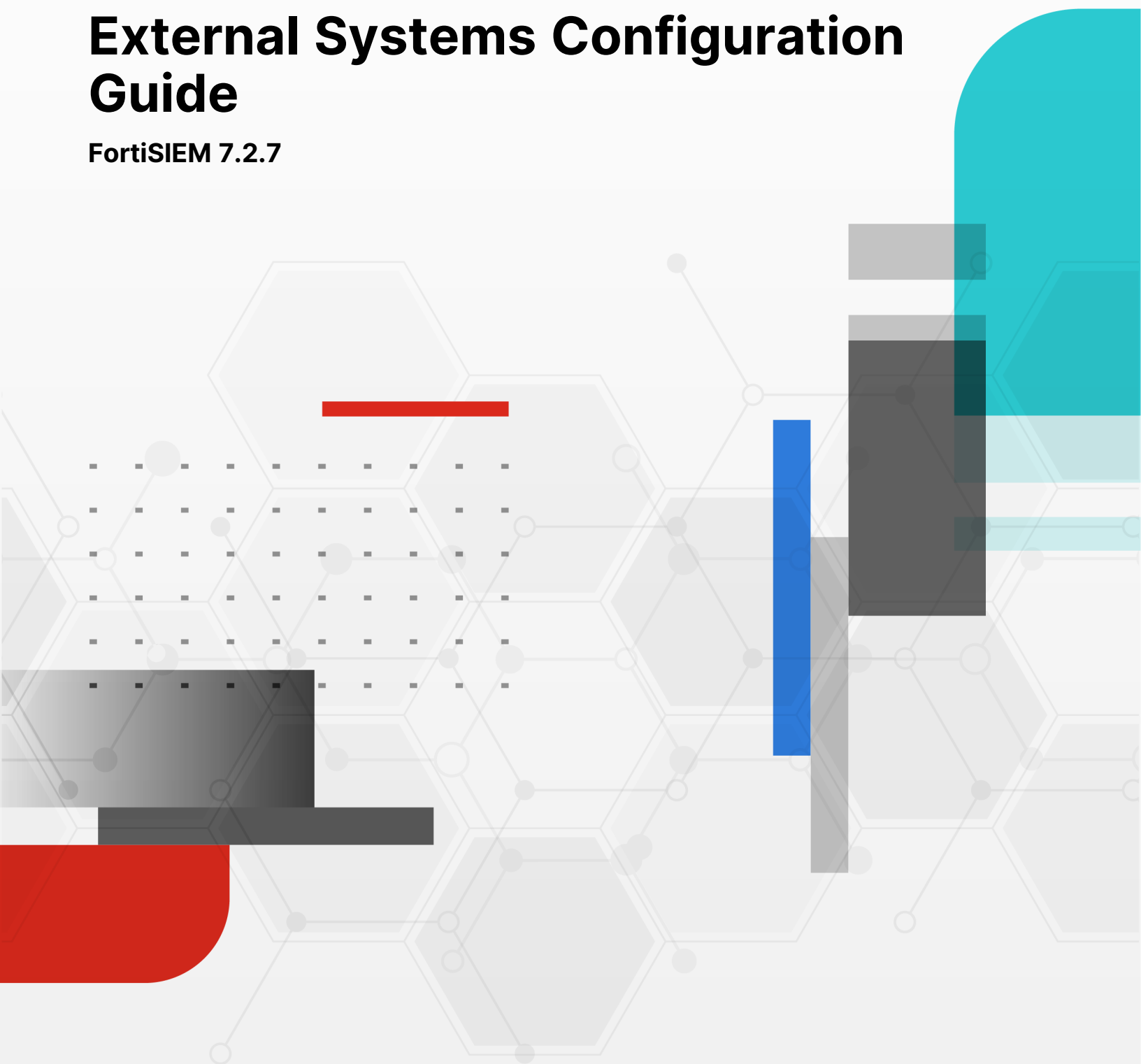


External Systems Configuration Guide

FortiSIEM 7.2.7



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



03/02/2026

FortiSIEM 7.2.7 External Systems Configuration Guide

Change Log

Date	Change Description
2018-05-23	Initial version of the guide.
2018-07-24	Revision 2 with a new section under Windows Server Configuration - Configuring Log Monitoring for Non-Administrative User.
2018-08-07	Revision 3 with updated section: Fortinet FortiGate Firewall
2018-09-12	Revision 4 with updated section: Microsoft Azure Audit
2018-09-26	Revision 5 with updated section: WatchGuard Firebox Firewall
2018-11-28	Revision 6 with updated section: Fortinet FortiGate Firewall > Configuring SSH on FortiSIEM to communicate with FortiGate
2019-01-29	Revision 7: updated section: Cisco FireSIGHT
2019-03-15	Revision 8: new section: Threat Intelligence
2019-03-28	Revision 9: updates the guide to reflect the new menu hierarchy in the FortiSIEM tool.
2019-04-24	Revision 10: added Carbon Black Security Platform under End Point Security Software.
2019-07-24	Revision 11: updated integration instructions for Microsoft Office 365 Audit.
2019-10-22	Revision 12: added Clavister Firewall and FortiADC devices. Added Active Directory User Discovery section to Microsoft Active Directory device. Corrections to SQL Server DDL Event Creation Script and SQL Server Database Level Event Creation Script.
2019-11-22	Revision 13: added Zeek (Bro) installation instructions for Security Onion, Cyberoam FortiADC, Epic SecuritySIEM, FortiEDR, FortiNAC, FortiDeceptor, Microsoft Network Policy Server, TrendMicro Deep Discovery. Changed the name of Cisco FireAMP to Cisco AMP Cloud V0. Changed the name of Cisco AMP to Cisco AMP Cloud V1.
2020-01-03	Revision 14: added CradlePoint.
2020-04-15	Revision 15: added Alert Logic Iris API, AWS Kinesis, AWS Security Hub, Cisco Amp, GitLab Cli, Azure Event Hub, Azure Compute, McAfee ePolicy Orchestrator, LastLine, Imperva Securesphere Web App Firewall, Imperva Securesphere DB Security Gateway, Imperva Securesphere DB Monitoring Gateway, Green League WVSS, FortiInsight, Damballa Failsafe, AWS EC2, Cisco Fireamp, Novell Netware, Green League RSAS, Checkpoint SmartCenter, FortiTester, Cisco Viptela, MobileIron, Duo, Indegy Industrial Cybersecurity Suite, Netwrix, Darktrace DCIP, Hirschmann SCADA Firewalls and Switches.
2020-07-22	Revision 16: Edits to Cisco AMP Cloud V0 and Cisco AMP Cloud V1.
2020-10-09	Revision 17: Added Alcide io KAudit, Stormshield Network Security and Tigera Calico

Date	Change Description
2020-12-18	Revision 18: Added note to AWS CloudTrail API Configuration
2021-01-05	Revision 19: Added Mapping Active Directory User Attributes to FortiSIEM User Attributes.
2021-02-03	Revision 20: Updated Malwarebytes to Malwarebytes Endpoint Protection.
2021-03-03	Revision 21: Added NetApp Data ONTAP Supported Version.
2021-03-18	Revision 22: Added Claroty Continuous Threat Detection, Corero Smartwall Threat Defense, Dragos Platform, Malwarebytes Breach Remediation, Oracle Cloud Access Security Broker (CASB), Proofpoint.
2021-04-05	Revision 23: Updated Linux server section.
2021-04-07	Revision 24: Updated AWS Kinesis for 6.2.0.
2021-04-16	Revision 25: Updated Microsoft Office 365 Audit "Create the Office 365 API Credential" steps.
2021-04-23	Revision 26: Added Salesforce Configuration for 6.2.0, 6.1.x, 5.4.0, 5.3.x, 5.2.x releases.
2021-07-06	Revision 27: Added Security Orchestration and FortiGate SNMPv3 setup example. Updated: Cisco Firepower Threat Defense, Linux Server Rsyslog and Syslog-NG, AWS Security Hub, EC2 Cloudwatch API, AWS EC2 Discovery, Office365 API integration, Microsoft Azure Compute, Microsoft Windows Defender for Endpoint (Windows Defender ATP), Cisco IOS, Cisco FireSIGHT, Cisco Duo, Cisco FireAmp, Cisco Meraki Access Points, Rapid7 Nexpose, Rapid7 InsightVM, Google Workspace, Carbon Black Syslog setup, FortiManager syslog, FortiWeb syslog, FortiSandbox syslog, FortiAuthenticator syslog, FortiClient syslog, FortiADC syslog, FortiDeceptor syslog, FortiNAC syslog, FortiEDR syslog, FortiSOAR syslog. Environmental Sensors updated to Operational Technology, Syslog over TLS. New Device Support: Microsoft Windows Print Service Log, AWS Elasticsearch Load Balancer Log, CyberX OT/IoT Security via Log, Digital Defense Vulnerability Scanner via API, FortiAI via Log, FortiCASB integration via API, HP ILO via SNMP Trap, Palo Alto Cortex XDR via Log, Palo Alto WildFire via Log through Palo Alto Firewall. Device Support Extensions: CloudTrail Logs via AWS Kinesis, CyberArk Vault integration via REST API, FortiAnalyzer System Event Logs via Syslog, FortiEDR integration via API, FortiGate, FortiAP and FortiSwitch via FortiGate API, GCC High Tenant for Azure Audit, VPC Flow Logs via AWS Kinesis.
2021-07-22	Revision 28: Updated AWS Kinesis Configuration for Configuring AWS CloudTrail Logs through Kinesis Streams, and Configuring VPC Flow Logs through Kinesis Streams.
2021-07-26	Revision 29: Updated Epilog/snare link for Oracle Database Server, Juniper Steel Belted RADIUS, and Apache Web Server configuration.
2021-07-30	Revision 30: Updated Tenable Nessus Vulnerability Scanner configuration.
2021-08-02	Revision 31: Updated Cisco FireSIGHT Configuration.
2021-08-26	Revision 32: Updated AWS EC2 CloudWatch API, Google Workspace / GSUITE, Zeek

Date	Change Description
	Network Security Monitor (Previously Bro). Added Microsoft Advanced Threat Analytics (ATA) On Premise Platform, KVM, FortiProxy, Google Cloud Platform, Mac OS, Otorio RAM2, UserGate UTM Firewall to 6.3.1.
2021-08-30	Revision 33: Updated Microsoft SQL Server for 6.x Guides.
2021-08-31	Revision 34: Added Syslog CEF Format configuration to Check Point FireWall-1 for 6.3.1 Guide.
2021-09-16	Revision 35: Updated Dell Force10 Router and Switch, Dell NSeries Switch, and Dell PowerConnect Switch and Router for 6.3.1, and Microsoft Office 365 Audit for 6.3.x Guides.
2021-09-17	Revision 36: Updated MySQL Server and CyberArk Password Vault for 6.3.x Guides. Added example syslog for Dell Force10 Router and Switch, Dell NSeries Switch, and Dell PowerConnect Switch and Router for 6.3.1 Guides.
2021-09-24	Revision 37: Updated Squid Web Proxy with syslog configuration for versions 4.1.1 and later for 6.1.1-6.3.x Guides.
2021-10-06	Revision 38: Added ArubaOS-CX Switch platform, Barracuda Web Application Firewall, and Cisco Umbrella to 6.3.2 Guide.
2021-10-08	Revision 39: Updated Microsoft Windows Server SNMP Configuration and Removed older Microsoft SQL Scripts in 6.3.x Guides.
2021-10-29	Revision 40: Updated Cisco Firepower Management Center (FMC) - Formerly FireSIGHT and FirePower Threat Defense : Using Cisco eStreamer Client for 6.x Guides.
2021-11-01	Revision 41: Updated Configuring FortiSIEM through FortiOS REST API - Step 2: Create an Administrator Profile for 6.3.x.
2021-11-08	Revision 42: Updated Cisco Umbrella Prefix Configuration Information for 6.3.2.
2021-11-16	Revision 43: Updated FortiSIEM External Ports with sFlow port number and protocol from External Devices to Supervisor/Worker/Collector.
2021-11-30	Revision 44: Updated FortiSIEM External Ports Collector Communication table.
2021-12-06	Revision 45: Updated Enable WinRM and set authentication in Microsoft Windows Server.
2021-12-08	Revision 46: Updated Syslog over TLS section for 6.x.
2022-12-23	Revision 47: Google Cloud Platform configuration updated for 6.3.1 and later.
2022-01-07	Revision 48: SNMP V3 Traps section added.
2022-01-11	Revision 49: Microsoft Windows Server section updated with OMI for 6.3.3 and later.
2022-01-13	Revision 50: CrowdStrike Endpoint Security section updated for 6.2.x and later.
2022-01-18	Revision 51: Dell Force10 S4048T-ON added to Dell Force10 Router and Switch section for 6.4.0. Updated Configuring Box.com Service section for 6.4.0. Added Oracle Cloud Infrastructure for 6.4.0. Cisco Umbrella Prefix Configuration Functionality enhanced for 6.4.0. Windows Server 2022 support added for 6.4.0.

Date	Change Description
2022-02-04	Revision 52: Added Configuring Windows Agent for Terminal Services for Microsoft Windows Server to 6.4.0 Guide.
2022-02-15	Revision 53: Added Ports for OMI based monitoring and log collection in FortiSIEM External Ports section for 6.3.3 and later.
2022-03-01	Revision 54: Added Flow Support section.
2022-03-02	Revision 55: Updated MySQL Server - Settings for MySQL Server JDBC Access Credentials for Database Auditing - Audit Table field.
2022-03-16	Revision 56: Microsoft Defender for Endpoint Legacy note updated. Also moved from Cloud Applications to End Point Security Software.
2022-03-22	Revision 57: Configuring Tigera Calico to Send Logs link updated.
2022-03-23	Revision 58: Fortinet FortiGate Firewall - REST API added to What is Discovered and Monitored.
2022-03-25	Revision 59: Syslog via Rsyslog added for Apache Web Server and NGINX Web Server. Updated Configuration provided for Microsoft Defender for Endpoint.
2022-03-28	Revision 60: Updated Microsoft Azure Audit Configuration section. Updated NGINX Web Server Syslog via Rsyslog configuration.
2022-03-29	Revision 61: Updated Supported Devices and Applications by Vendor.
2022-04-04	Revision 62: Added Zscaler Cloud Firewall.
2022-04-08	Revision 63: Microsoft Defender for Endpoint content moved so current and legacy information are on the same page.
2022-05-09	Revision 64: Added Nutanix Prism, AWS Simple Queue Service (aws-sqs), kerberos configuration for Microsoft Windows Servers for OMI Access Credentials, AWS S3 (Simple Storage Service), VMware NSX for vSphere, Cybereason. Modified MySQL Server. Updated SNMP v3 Traps.
2022-05-10	Revision 65: Added Security Information and Event Management (SIEM) category, SAP Enterprise Threat Detection (ETD), and Ingesting JSON Formatted Events Received via HTTP(S) POST.
2022-05-12	Revision 66: FortiSIEM External Ports/Ports Used by FortiSIEM for Discovery and Monitoring renamed to FortiSIEM Port Usage. FortiSIEM Port Usage updated.
2022-05-27	Revision 67: AWS CloudTrail: Understanding AWS CloudTrail Configuration section added.
2022-06-06	Revision 68: Supported Versions information added to Flow Support.
2022-06-08	Revision 69: Updated Setup in FortiSIEM section in Cisco Umbrella Configuration.
2022-06-15	Revision 70: FortiAI product name updated to FortiNDR.
2022-06-27	Revision 71: Note added to FortiSIEM Port Usage.
2022-07-13	Revision 72: Updated Using Cisco eStreamer Client section in Cisco FireSIGHT and

Date	Change Description
	FirePower Threat Defence.
2022-07-25	Revision 73: Updated Microsoft Exchange.
2022-07-26	Revision 74: Added: Appendix - Generic Log API Poller (HTTPS Advanced) Integration, Configuring Cisco Umbrella API Endpoints using Generic HTTPS Poller in Cisco Umbrella, and Configuring Microsoft Graph Incident API using Generic HTTPS Poller for 6.6.0.
2022-08-09	Revision 75: Updated Configuring FortiSIEM for Sophos Central for API Access.
2022-08-15	Revision 76: Updated FortiSIEM Port Usage with ClickHouse ports.
2022-08-17	Revision 77: Updated FortiSIEM Port Usage section.
2022-09-07	Revision 78: Updated FortiSIEM Port Usage section.
2022-09-15	Revision 79: Updated Microsoft Windows Server and FortiSIEM Port Usage sections.
2022-09-16	Revision 80: Updated Microsoft Windows Server section.
2022-10-06	Revision 81: Added Workday Enterprise Suite (Workday Report API via Generic HTTPS Poller). Note: Requires Content Update 305 for FortiSIEM 6.6.x.
2022-10-10	Revision 82: Updated FortiSIEM Port Usage section.
2022-10-14	Revision 83: Updated Microsoft Windows Server winexe note.
2022-10-31	Revision 84: Updated Citrix Netscaler Application Delivery Controller (ADC) Configuration section.
2022-11-01	Revision 85: Added Bitdefender GravityZone and Kaspersky to End Point Security Software section.
2022-11-08	Revision 86: Updated Amazon Simple Storage Service (AWS S3)
2022-12-01	Revision 87: Updated Microsoft Windows Server Data Collection Comparison - Agentless (WMI/OMI) versus FortiSIEM Windows Agent table.
2022-12-22	Revision 88: Updated Microsoft Azure Event Hub - Configuration in Azure Step 4.
2023-01-03	Revision 89: Updated Amazon Simple Storage Service (AWS S3) - Enable Event Notifications section and Upload Log File to AWS S3 section.
2023-01-10	Revision 90: Updated Cisco Call Manager - Configure FortiSIEM to Receive CDR Records from Cisco Call Manager.
2023-03-08	Revision 91: Updated Cisco Umbrella section.
2023-03-09	Revision 92: Updated Microsoft Azure Audit - Create IP Range to Credential Association and Test Connectivity in FortiSIEM section.
2023-03-24	Revision 93: Updated Box/Box.com - "Configuring Box.com Service" section.
2023-04-10	Revision 94: Updated Oracle WebLogic section.

Date	Change Description
2023-05-10	Revision 95: Updated Enable Office 365 Audit Log Search section for Microsoft Office 365 Audit.
2023-05-30	Revision 96: For 6.7.4 and later, added Syslog and added Netflow IPv4 and IPv6 to Flow Support.
2023-05-30	Revision 97: Added FortiClient EMS. Updated FortiGate Firewall.
2023-06-22	Revision 98: Added Windows 11 to OS Supported Versions for Microsoft Windows Server in FortiSIEM 6.5.0 and later.
2023-07-11	Revision 99: Added Configuring JMX on JBoss 7.1 EAP to Red Hat JBoss section for 7.1.0.
2023-07-28	Revision 100: Added Nessus10 to Tenable Nessus Vulnerability Scanner for 7.x.
2023-08-03	Revision 101: Updated Blue Coat Web Proxy section.
2023-08-10	Revision 102: Added Fortinet FortiRecon (FortiRecon API via Generic HTTPS Poller) for 7.1.0
2023-08-25	Revision 103: Content Update - Added Armis Asset Intelligence Platform, Hillstone Firewall, Ubiquiti Wireless LAN.
2023-09-11	Revision 104: Added G42 Cloud in Cloud Applications.
2023-09-28	Revision 105: Updated Microsoft Windows Server.
2023-10-04	Revision 106: Added Fortinet FortiNDR Cloud.
2023-10-18	Revision 107: Updated Fortinet FortiGate Firewall.
2023-11-03	Revision 108: Added Zscaler Nanolog Streaming Service (NSS).
2023-11-13	Revision 109: Added Trend Vision One for 7.1.1.
2023-12-13	Revision 110: Updated Note in "FortiGate User Device Store Discovery". Added AWS Access Key IAM Permissions and IAM Policies link to Amazon AWS EC2 section.
2024-01-08	Revision 111: Added Network Access Control category. FortiNAC moved to Network Access Control. Added HPE Aruba Networking ClearPass Policy Manager to Network Access Control.
2024-01-10	Revision 112: Microsoft Defender for Endpoint (Previously Microsoft Windows Defender Advanced Threat Protection (ATP)) API endpoints updated (no longer beta). Added Microsoft Entra Identity Protection to Cloud Applications category.
2024-01-16	Revision 113: Default LDAP and LDAPS ports (Global Catalog ports) updated for FortiSIEM LDAP/LDAPS configurations (IBM AIX, HP UX Server, Microsoft Active Directory, Microsoft Windows Server).
2024-02-06	Revision 114: Added SQL Server 2022 support for Microsoft SQL Server. Added 7928 port entry for Supervisor Communication and Worker Communication in FortiSIEM Port Usage.
2024-02-26	Revision 115: Changed "JDBC for Database Auditing - Oracle Database Server" to

Date	Change Description
	"JDBC for Database Auditing Via Unified Audit Trail" and updated configuration for Oracle Database Server.
2024-03-04	Revision 116: Added "Create Access Token" to Configuring GitHub Server section for GitHub.
2024-03-06	Revision 117: Moved "Generic Log API Poller (HTTPS Advanced) Integration" and "Ingesting JSON Formatted Events Received via HTTP(S) POST" out from Appendix.
2024-03-21	Revision 118: Added the following FortiRecon API support information to FortiRecon section- /aci/<org_id>/leaked_creds - Displays any detected leaked credentials for your organization.
2024-03-26	Revision 119: Updated CLI command in "Configuring FortiGate to send Syslog to FortiSIEM" for FortiGate.
2024-03-27	Revision 120: Added "Collecting Microsoft Exchange Message Track Logs" in Microsoft Exchange.
2024-04-01	Revision 121: Added Akamai Connected Cloud.
2024-04-02	Revision 122: Updated FortiSIEM Port Usage Supervisor Communication, Worker Communication gRPC ports.
2024-04-11	Revision 123: Updated Microsoft Windows Server 2012 R2 WinRM configuration.
2024-04-16	Revision 124: Added "Required API Permissions for Trend Vision One Integration" for Trend Vision One.
2024-04-17	Revision 125: Added "Syslog via Rsyslog Forwarding" under Syslog Integration to GitLab API.
2024-04-23	Revision 126: Updated Performance Monitoring for Windows Agent in Microsoft Windows Server Performance Feature table. Updated FortiSIEM Port Usage table.
2024-04-29	Revision 127: Recommendation updated for Microsoft Windows Server under What is Discovered and Monitored. Protocol updated for Tanium Connect.
2024-06-05	Revision 128: Webhook Integration, Atlassian Beacon, GitLab, Mimecast Cloud Gateway, FortiPAM added. GitHub updated with Webhook configuration. How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate added to Appendix.
2024-07-18	Revision 129: Added SolarWind Orion.
2024-08-21	Revision 130: Updated QNAP Turbo NAS.
2024-09-13	Revision 131: Updated Fortinet FortiRecon. - FortiRecon_Generic_Poller_Templates.zip. - Manual Method (Defining the API Components) - Leaked Cards Walkthrough table. 2 APIs added. One API updated.
2024-09-26	Revision 132: Carbon Black Security Platform Configuration updated.
2024-10-02	Revision 133: Updated Microsoft Office 365 Audit - Configuring Office 365 Auditing Step 2 and Step 3.

Date	Change Description
2024-10-23	Revision 134: Added Microsoft Windows Server via Agent, Updated configuration for Apache Web Server, Juniper Networks Steel-Belted RADIUS, and Oracle Database Server.
2024-11-01	Revision 135: Updated FortiGate section.
2024-12-06	Revision 136: Updated FortiSIEM Port Usage - Supervisor, Worker and Collector Communication tables.
2024-12-17	Revision 137: Updated QNAP Turbo NAS configuration.
2025-01-21	Revision 138: Added EU region in FortiSIEM configuration for Fortinet FortiNDR Cloud.
2025-01-23	Revision 139: Updated Microsoft SQL Server.
2025-01-24	Revision 140: Updated Google Workspace.
2025-02-10	Revision 141: Updated Cisco Umbrella.
2025-03-31	Revision 142: Updated FortiSIEM Port Usage Supervisor Communication phRuleWorker to phRuleMaster Communication gRPC port.
2025-05-08	Revision 143: Updated FortiAnalyzer, and FortiGate > FortiAnalyzer sub-section.

TABLE OF CONTENTS

Change Log	3
Overview	20
FortiSIEM Port Usage	22
FortiSIEM Manager Communication	22
Supervisor Communication	22
Worker Communication	27
Collector Communication	30
Supported Devices and Applications by Vendor	33
Applications	71
Application Server	72
Apache Tomcat	73
IBM WebSphere	77
Microsoft ASP.NET	85
Oracle GlassFish Server	86
Oracle WebLogic	90
Red Hat JBoss	97
Authentication Server	103
Cisco Access Control Server (ACS)	104
Cisco Identity Solution Engine (ISE)	110
Cisco Duo	112
CyberArk Password Vault	115
Fortinet FortiAuthenticator	123
Juniper Networks Steel-Belted Radius	125
Microsoft Internet Authentication Server (IAS)	127
Microsoft Network Policy Server (RAS VPN)	128
One Identity Safeguard (previously Balabit Privileged Session Management)	130
Vasco DigiPass	131
Database Server	133
IBM DB2 Server	134
Microsoft SQL Server	140
MySQL Server	160
Oracle Database Server	167
DHCP and DNS Server	177
Infoblox DNS/DHCP	178
ISC BIND DNS	181
Linux DHCP	183
Microsoft DHCP	185
Microsoft DNS	187
Directory Server	189
Microsoft Active Directory	190
Document Management Server	195
Microsoft SharePoint	196
Healthcare IT	197
Epic EMR/EHR System	198

Mail Server	200
Microsoft Exchange	201
Management Server/Appliance	205
Cisco Application Centric Infrastructure (ACI)	206
Fortinet FortiManager	211
HPE Integrated Lights-Out (iLO)	213
ManageEngine Endpoint Central	214
SolarWinds Orion	215
VMware NSX for vSphere	216
Remote Desktop	218
Citrix Receiver (ICA)	219
Source Code Control	223
GitHub	224
GitLab	231
GitLab API	236
GitLab CLI	241
Unified Communication Server Configuration	244
Avaya Call Manager	245
Cisco Call Manager	247
Cisco Contact Center	253
Cisco Presence Server	254
Cisco Tandberg Telepresence Video Communication Server (VCS)	255
Cisco Telepresence Multipoint Control Unit (MCU)	257
Cisco Telepresence Video Communication Server	259
Cisco Unity Connection	260
Web Server	261
Apache Web Server	262
Microsoft IIS for Windows 2000 and 2003	269
Microsoft IIS for Windows 2008	271
NGINX Web Server	273
Blade Servers	276
Cisco UCS Server	277
HP BladeSystem	280
Cloud Access Security Broker	281
Fortinet FortiCASB	281
Oracle Cloud Access Security Broker (CASB)	283
Cloud Applications	287
Akamai Connected Cloud	287
Alcide.io KAudit	290
Atlassian Beacon	291
AWS Access Key IAM Permissions and IAM Policies	296
AWS CloudTrail	298
Amazon AWS EC2	304
AWS EC2 CloudWatch API	306
AWS Elastic Load Balancer (ELB)	310
AWS Kinesis	314
AWS RDS	327

AWS Security Hub	329
AWS Simple Queue Service (SQS)	335
Amazon Simple Storage Service (AWS S3)	337
Box/Box.com	343
Cisco Umbrella	345
G42 Cloud	353
Google Cloud Platform (GCP)- Pub/Sub Integration	356
Google Workspace (Formerly G Suite and Google Apps)	365
Microsoft Azure Audit	373
Microsoft Azure Compute	376
Microsoft Azure Event Hub	382
Microsoft Cloud App Security	393
Microsoft Defender for Identity (Previously Microsoft Azure Advanced Threat Protection (ATP))	395
Microsoft Entra Identity Protection	396
Microsoft Office 365 Audit	402
Okta	415
Oracle Cloud Infrastructure	420
Salesforce CRM Audit	426
Cloud Email Security	430
Fortinet FortiMail Workspace Security	430
Mimecast Cloud	432
Console Access Devices	442
Lantronix SLC Console Manager	443
Customer Relationship Management	444
Workday Enterprise Suite (Workday Report API via Generic HTTPS Poller)	444
Digital Risk Protection	452
Fortinet FortiRecon	452
End Point Security Software	458
Bit9 Security Platform	459
Bitdefender GravityZone	460
Carbon Black Security Platform	464
Cisco AMP for Endpoints API V0 - Previously Cisco AMP Cloud V0	467
Cisco AMP for Endpoints API V1 - Previously Cisco AMP Cloud V1	474
Cisco Security Agent (CSA)	482
CloudPassage Halo	485
CrowdStrike Endpoint Security	488
Cybereason	490
Digital Guardian Code Green DLP	492
ESET NOD32 Anti-Virus	494
FortiClient	495
Fortinet FortiClient EMS	498
Fortinet FortiEDR	501
Kaspersy	503
Malwarebytes Breach Remediation	504
Malwarebytes Endpoint Protection	506
McAfee ePolicy Orchestrator (ePO)	508
Microsoft Defender for Endpoint (Previously Microsoft Windows Defender)	511

Advanced Threat Protection (ATP))	
[Legacy] Microsoft Defender for Endpoint (Previously Microsoft Windows Defender Advanced Threat Protection (ATP))	525
MobileIron Sentry and Connector	528
Netwrix Auditor (via Correlog Windows Agent)	530
Palo Alto Traps Endpoint Security Manager	532
SentinelOne Singularity	533
Sophos Central	539
Sophos Endpoint Security and Control	541
Symantec Endpoint Protection	543
Symantec SEPM	546
Tanium Connect	547
Trend Micro Interscan Web Filter	548
Trend Micro Intrusion Defense Firewall (IDF)	550
Trend Micro OfficeScan	551
Trend Vision One	551
Firewalls	555
Check Point FireWall-1	556
Check Point Provider-1 Firewall	560
Configuring CMA for Check Point Provider-1 Firewalls	562
Configuring CLM for Check Point Provider-1 Firewalls	565
Configuring MDS for Check Point Provider-1 Firewalls	567
Configuring MLM for Check Point Provider-1 Firewalls	570
Check Point VSX Firewall	572
Cisco Adaptive Security Appliance (ASA)	576
Cisco Firepower Threat Defense (FTD)	582
Clavister Firewall	586
Cyberoam Firewall	588
Dell SonicWALL Firewall	590
Fortinet FortiGate Firewall	593
Hillstone Firewall	611
Imperva SecureSphere Web App Firewall	613
Juniper Networks SSG Firewall	615
McAfee Firewall Enterprise (Sidewinder)	619
Palo Alto Firewall	621
Sophos UTM	626
Stormshield Network Security	628
Tigera Calico	629
UserGate UTM Firewall	630
WatchGuard Firebox Firewall	632
Zscaler Internet Access (ZIA)	633
Load Balancers and Application Firewalls	645
Barracuda Web Application Firewall	645
Brocade ServerIron ADX	647
Citrix Netscaler Application Delivery Controller (ADC)	650
F5 Networks Application Security Manager	652
F5 Networks Local Traffic Manager	654
F5 Networks Web Accelerator	657
Fortinet FortiADC	659

Qualys Web Application Firewall	661
Log Aggregators	664
Fortinet FortiAnalyzer	664
Network Access Control	667
Fortinet FortiNAC	668
HPE Aruba Networking ClearPass Policy Manager	669
Network Compliance Management Applications	672
Cisco Network Compliance Manager	673
PacketFence Network Access Control (NAC)	675
Network Detection and Response	676
Fortinet FortiNDR (Formerly FortiAI)	676
Fortinet FortiNDR Cloud	677
Zeek Network Security Monitor (Previously known as Bro)	681
Network Intrusion Detection System	693
Microsoft Advanced Threat Analytics (ATA) On Premise Platform	693
Network Intrusion Prevention Systems (IPS)	696
3Com TippingPoint UnityOne IPS	697
AirTight Networks SpectraGuard	699
Alert Logic IRIS API	702
Armis Asset Intelligence Platform	704
Cisco Firepower Management Center (FMC) - Formerly FireSIGHT and FirePower Threat Defense	707
Cisco Intrusion Prevention System	713
Cisco Stealthwatch	716
Claroty Continuous Threat Detection (CTD) Platform	716
Corero Smartwall Threat Defense System	718
Cylance Protect Endpoint Protection	721
Cyphort Cortex Endpoint Protection	723
Damballa Failsafe	725
Darktrace CyberIntelligence Platform	726
Dragos Platform	731
FireEye Malware Protection System (MPS)	733
FortiDDoS	735
Fortinet FortiDeceptor	739
Fortinet FortiSandbox	741
Fortinet FortiTester	743
IBM Internet Security Series Proventia	744
Indegy Security Platform	748
Juniper DDoS Secure	749
Juniper Networks IDP Series	751
McAfee Network Security Platform (formerly known as McAfee IntruShield)	753
McAfee Stonesoft IPS	756
Motorola AirDefense	758
Nozomi Central Management Control	759
Palo Alto Networks Cortex XDR	760
Radware DefensePro	766
Snort Intrusion Prevention System	768

Sourcefire 3D and Defense Center	773
Trend Micro Deep Discovery	775
Zeek (Bro) Installed on Security Onion	777
Operational Technology	779
APC Netbotz Environmental Monitor	780
APC UPS	783
Claroty Continuous Threat Detection (CTD) Platform	784
Dragos Platform	786
Generic UPS	788
Hirschmann SCADA Firewalls and Switches	789
Liebert FPC	791
Liebert HVAC	793
Liebert UPS	795
Microsoft Defender for IoT (Was CyberX OT/IoT Security)	796
Nozomi Central Management Control	797
Nozomi SCADAguardian	798
OTORIO RAM2 (Risk Assessment, Monitoring and Management)	801
Siemens Simatic PLC	802
Privileged Access Management	804
Fortinet FortiPAM / FortiSRA	804
ManageEngine PAM360	807
WALLIX Bastion	808
Routers and Switches	811
Alcatel TiMOS and AOS Switch	812
Arista Router and Switch	814
ArubaOS-CX Switching Platform	816
Brocade NetIron CER Routers	819
Cisco 300 Series Routers	821
Cisco IOS Router and Switch	823
How CPU and Memory Utilization is Collected for Cisco IOS	834
Cisco Meraki Cloud Controller and Network Devices	836
Cisco NX-OS Router and Switch	839
Cisco ONS	844
Cisco Viptela SDWAN Router	846
Dell Force10 Router and Switch	848
Dell N-Series Switch	852
Dell PowerConnect Switch and Router	856
Foundry Networks IronWare Router and Switch	859
HP/3Com ComWare Switch	864
HP ProCurve Switch	866
HP Value Series (19xx) and HP 3Com (29xx) Switch	869
Hirschmann SCADA Firewalls and Switches	872
Juniper Networks JunOS Switch	874
MikroTik Router	878
Nortel ERS and Passport Switch	880
Secure Access Service Edge	882
Zscaler Private Access (ZPA)	882

Security Gateways	889
Barracuda Networks Spam Firewall	890
Blue Coat Web Proxy	892
Cisco IronPort Mail Gateway	895
Cisco IronPort Web Gateway	898
Fortinet FortiMail	901
Fortinet FortiProxy	903
Fortinet FortiWeb	906
Imperva SecureSphere DB Monitoring Gateway	908
Imperva SecureSphere Security Gateway	909
McAfee Web Gateway	911
Microsoft ISA Server	913
Proofpoint	919
Squid Web Proxy	922
SSH Comm Security CryptoAuditor	925
Vormetric Data Security Manager	927
Websense Web Filter	928
Security Information and Event Management (SIEM)	930
SAP Enterprise Threat Detection (ETD)	930
SAP Enterprise Threat Detection Cloud	933
Security Orchestration (SOAR)	939
Fortinet FortiSOAR	939
Servers and Workstations	941
Apple MacOS Servers and Workstations	941
HP UX Server	942
IBM AIX Server	946
IBM OS400 Server	950
Linux Server	952
Microsoft Windows Server via OMI/SNMP/WMI	960
Microsoft Windows Server via Agent	986
QNAP Turbo NAS	1044
Sun Solaris Server	1046
Storage	1049
Brocade SAN Switch	1050
Dell Compellent Storage	1052
Dell EqualLogic Storage	1054
EMC Clariion Storage	1056
EMC Isilon Storage	1061
EMC VNX Storage Configuration	1063
NetApp Data ONTAP	1067
NetApp Filer Storage	1069
Nimble Storage	1072
Nutanix Storage	1074
Threat Intelligence	1078
Fortinet FortiInsight	1079
Lastline	1082
ThreatConnect	1084

Virtualization	1086
Hyper-V	1087
HyTrust CloudControl	1091
KVM	1092
Nutanix Prism	1094
VMware ESX	1097
VPN Gateways	1099
Cisco VPN 3000 Gateway	1100
Cyxtera AppGate	1102
Juniper Networks SSL VPN Gateway	1103
Microsoft PPTP VPN Gateway	1106
Pulse Secure	1108
Vulnerability Scanners	1110
AlertLogic Intrusion Detection and Prevention Systems (IPS)	1111
Digital Defense Frontline Vulnerability Manager	1112
Green League WVSS	1117
McAfee Foundstone Vulnerability Scanner	1118
Qualys QualysGuard Scanner	1120
Qualys Vulnerability Scanner	1121
Rapid7 Nexpose Vulnerability Scanner (Vulnerability Management On-Premises)	1123
Rapid7 InsightVM (Platform Based Vulnerability Management)	1125
Tenable.io	1127
Tenable Nessus Vulnerability Scanner	1130
Tenable Security Center	1133
YXLink Vulnerability Scanner	1136
WAN Accelerators	1137
Cisco Wide Area Application Server	1138
Riverbed SteelHead WAN Accelerator	1141
Wireless LANs	1144
Aruba Networks Wireless LAN	1145
Cisco Wireless LAN	1147
CradlePoint	1150
FortiAP	1152
FortiWLC	1154
Motorola WiNG WLAN AP	1157
Ruckus Wireless LAN	1159
Ubiquiti Wireless LAN	1160
Using Virtual IPs to Access Devices in Clustered Environments	1162
Generic Log API Poller (HTTPS Advanced) Integration	1162
Overview	1162
Common Errors	1171
Ingesting JSON Formatted Events Received via HTTP(S) POST	1171
Syslog	1174
Syslog IPv4 and IPv6	1174
Syslog over TLS	1175
Common Reasons to use Syslog over TLS	1175

Prerequisites	1175
How to Generate a Public SSL/TLS Certificate	1176
How to Generate a Self Signed SSL/TLS Certificate	1177
SNMP V3 Traps	1179
Manual File Configuration	1179
Configuration via Discover	1181
Webhook Integration	1182
Flow Support	1188
Netflow IPv4 and IPv6	1188
Appendix	1189
CyberArk to FortiSIEM Log Converter XSL	1190
Access Credentials	1195
How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate	1200
Step 1 - Generate CSR	1200
Step 2 - Generate Certificate	1200
Configure Collector	1201

Overview

This document describes how to configure third party devices for monitoring by FortiSIEM.

- [FortiSIEM Port Usage](#)
- [Supported Devices and Applications by Vendor](#)
- [Applications](#)
- [Blade Servers](#)
- [Cloud Access Security Broker](#)
- [Cloud Applications](#)
- [Cloud Email Security](#)
- [Console Access Devices](#)
- [Customer Relationship Management](#)
- [Digital Risk Protection](#)
- [End Point Security Software](#)
- [Firewalls](#)
- [Load Balancers and Application Firewalls](#)
- [Log Aggregators](#)
- [Network Access Control](#)
- [Network Compliance Management Applications](#)
- [Network Detection and Response](#)
- [Network Intrusion Detection System](#)
- [Network Intrusion Protection Systems \(IPS\)](#)
- [Operational Technology](#)
- [Privileged Access Management](#)
- [Routers and Switches](#)
- [Secure Access Service Edge](#)
- [Security Gateways](#)
- [Security Information and Event Management \(SIEM\)](#)
- [Security Orchestration \(SOAR\)](#)
- [Servers and Workstations](#)
- [Storage](#)
- [Threat Intelligence](#)
- [Virtualization](#)
- [VPN Gateways](#)
- [Vulnerability Scanners](#)
- [WAN Accelerators](#)
- [Wireless LANs](#)
- [Generic Log API Poller \(HTTPS Advanced\) Integration](#)
- [Ingesting JSON Formatted Events Received via HTTP\(S\) POST](#)
- [Using Virtual IPs to Access Devices in Clustered Environments](#)

- [Syslog](#)
- [Syslog over TLS](#)
- [SNMP V3 Traps](#)
- [Webhook Integration](#)
- [Flow Support](#)
- [Appendix](#)

FortiSIEM Port Usage

This chapter describes the external communication ports needed for various FortiSIEM nodes to work. The ports are broken down for:

- [FortiSIEM Manager Communication](#)
- [Supervisor Communication](#)
- [Worker Communication](#)
- [Collector Communication](#)

In release 7.2, some clear communication has been replaced by SSL communication. If an entry in the tables below has 5.3, then that entry is valid for releases 5.3 and below. If an entry in the tables below has 7.2, then that entry is valid for releases 7.2 and above.



Since there will be intercommunication between FortiSIEM nodes (Worker to Worker, Worker to Supervisor, Supervisor to Worker), Fortinet suggests not to firewall block any type of communication between internal FortiSIEM nodes.

FortiSIEM Manager Communication

From	To	Inbound or Outbound	Ports	Services
Supervisor	FortiSIEM Manager	Inbound	TCP/443	Handle FortiSIEM Instance Registration and Incidents, license, and health upload from Instance
FortiSIEM Manager	Supervisor	Outbound	TCP/443	Incident drill down and Incident Management from FortiSIEM Manager

Supervisor Communication

From	To	Inbound or Outbound	Ports	Services
FortiSIEM Management User	Supervisor	Inbound	ICMP	Monitoring via ICMP
Supervisor	Mail Gateway	Outbound	TCP/SMTP	Sending email notification

From	To	Inbound or Outbound	Ports	Services
External Device	Supervisor	Inbound	TCP/21	FTP (for receiving Bluecoat logs via ftp)
FortiSIEM Management User	Supervisor	Inbound	TCP/22	Admin access via SSH
Supervisor	Whois Servers	Outbound	43	Whois lookup service • whois.geektools.com • whois.arin.net • whois.networksolutions.com • whois.internic.net • whois.nic.af • whois.ripe.net • whois.apnic.net • whois.amnic.net • whois.nic.gov • whois.nic.ad.jp • whois.nic.mx • whois.nic.us
Supervisor	External Device	Outbound	TCP/110	POP3 for email monitoring (STM)
Supervisor	NFS Server	Outbound	UDP/111, TCP/111	NFS Portmapper for writing events in NFS based deployments
Supervisor	External Windows Devices	Outbound	TCP/135	WMI based monitoring and log collection
Supervisor	External Windows Devices	Outbound	TCP/135, UDP/137, TCP/5985-5986	OMI based monitoring and log collection
Supervisor	External Device	Outbound	TCP/143	IMAP for email monitoring (STM)
Supervisor	External Device	Outbound	UDP/161	SNMP based monitoring
External Device	Supervisor	Inbound	UDP/162	SNMP Trap
Supervisor	External Devices	Outbound	TCP/389	LDAP discovery
Supervisor	Elasticsearch Coordinating Node	Outbound	HTTPS/443 (configurable) or HTTPS/9300	Querying events for Elasticsearch based deployments

From	To	Inbound or Outbound	Ports	Services
Supervisor	FortiSIEM Manager	Outbound	TCP/443	Register to FortiSIEM Manager and upload Incidents, license and health
FortiSIEM Manager	Supervisor	Inbound	TCP/443	Incident drill down and Incident Management from FortiSIEM Manager
FortiSIEM Management User	Supervisor	Inbound	TCP/443	GUI access via HTTPS
Collector, Worker, Windows Agent, Linux Agent	Supervisor	Inbound	TCP/443	REST API access via HTTPS
Supervisor	External Device	Outbound	TCP/443	HTTPS based log collection
Supervisor	External Device	Inbound, Outbound	TCP/443	IOC lookups connect to productapi.fortinet.com, IOC feed download connects to FortiGuard Services (update.fortiguard.net), Validation of Collector & Agent packages connects to FortiGuard Services (update.fortiguard.net), Upgrade connects to os-pkgs-cdn.fortisiem.fortinet.com and os-pkgs-r8.fortisiem.fortinet.com for OS updates.
External Device	Supervisor	Inbound	TCP/514	TCP syslog
External Device	Supervisor	Inbound	UDP/514	UDP syslog
Supervisor	External Devices	Outbound	TCP/636	LDAPS discovery
Supervisor	External Device	Outbound	TCP/993	IMAP/SSL for email monitoring (STM)
Supervisor	External Device	Outbound	TCP/995	POP/SSL for email monitoring (STM)
Supervisor	External Devices	Outbound	TCP/1433	JDBC based monitoring and data collection
External Device	Supervisor	Inbound	TCP/1470	TCP syslog
External Device	Supervisor	Inbound	UDP/2055	NetFlow

From	To	Inbound or Outbound	Ports	Services
Supervisor	External Devices	Outbound	TCP/3268	LDAP discovery (Global Catalog port, Global Catalog TLS port)
Supervisor	External Devices	Outbound	TCP/3269	LDAPS discovery (Global Catalog port)
Supervisor	Worker	Inbound, Outbound	RAFT/3888	ClickHouse Keeper Traffic <i>if Supervisor node is part of ClickHouse Keeper Cluster</i>
Supervisor	Report Server	Outbound	TCP/5432	PostgreSQL (report loading)
Worker	Supervisor	Inbound	TCP/5555	phFortiInsightAI module data collection
External Device	Supervisor	Inbound	UDP/6343	sFlow
External Device	Supervisor	Inbound	TLS (Supporting v1.2 & v1.3)/6514	Syslog over TLS
Supervisor	Worker	Outbound	TCP/6666	Redis communication
Supervisor	Spark Master Node	Outbound	HTTPS/7077 (configurable)	Querying events for HDFS based deployments
Worker	Supervisor	Inbound	TLS (Supporting v1.3)/7900	phMonitorWorker to phMonitorSuper communication
Supervisor	Worker	Outbound	TLS (Supporting v1.3)/7900	phMonitorSuper to phMonitorWorker Communication
Supervisor (Primary)	Supervisor (Secondary for DR)	Inbound, Outbound	TCP/7900	Disaster Recovery Setup
Worker	Supervisor	Inbound	TLS (Supporting v1.3)/7914	phParser on Worker to phParser on Supervisor for EPS enforcement
Supervisor	Worker	Outbound	TLS (Supporting v1.3)/7916	phQueryMaster to phQueryWorker communication
Worker	Supervisor	Inbound	TLS (Supporting v1.3)	phQueryWorker to phQueryMaster Communication
Worker 6.1	Supervisor	Outbound	TLS (Supporting v1.3)/7920	phQueryMaster to phDataManager for trigger event query

From	To	Inbound or Outbound	Ports	Services
Worker	Supervisor	Inbound	TLS (Supporting v1.3)	phRuleWorker to phRuleMaster communication
Worker	Supervisor	Inbound	TLS (Supporting V1.3)/7928	phParser on Worker to phDiscover on Supervisor to trigger a device discovery after detecting Cisco IOS BGP or OSPF Adjacency Change
Worker	Supervisor	Inbound	TLS (Supporting v1.3)	phReportWorker to phReportMaster Communication
Worker	Supervisor	Inbound	TLS (Supporting v1.3)/7938	phIdentityWorker to phIdentityMaster
Supervisor	Worker	Outbound	HTTP/8123, HTTPS/8443	ClickHouse Database Query
Supervisor	Worker	Outbound	HTTP/8123, HTTPS/8443	ClickHouse Database Insert <i>if Supervisor receives events from Collectors or Workers and it is not chosen as a Data Node</i>
Worker	Supervisor	Inbound	HTTP/8123, HTTPS/8443	ClickHouse Database Insert <i>if Supervisor is chosen as a Data Node</i>
Supervisor	External Devices	Outbound	UDP/8686	JMX based monitoring and data collection
Supervisor	HDFS Name Node	Outbound	HTTPS/9000 (configurable)	Archiving events for HDFS based deployments
Supervisor	Worker	Inbound, Outbound	9000, 9440	ClickHouse Internal Communication
Supervisor	Worker	Inbound, Outbound	HTTP/9009, HTTPS/9010	ClickHouse Database Replication <i>if Supervisor is chosen as a Data Node</i>
Supervisor	Elasticsearch Coordinating Node	Outbound	HTTPS/9200 (configurable)	Storing events for Elasticsearch based deployments
Supervisor	Checkpoint	Outbound	TCP/18184	Checkpoint LEA based log collection
Supervisor	Checkpoint	Outbound	TCP/18190	Checkpoint CPML based data collection

From	To	Inbound or Outbound	Ports	Services
Collector	Supervisor	Inbound	TCP/19999	Collector to Supervisor Reverse SSH Tunnel (disabled by default)
Supervisor	Collector	Outbound	TCP/20000-30000	Collector to Super Reverse SSH Tunnel (disabled by default)
Worker	Supervisor	Inbound	gRPC (TLS v1.2)/27918	phQueryWorker to phQueryMaster Communication
Worker	Supervisor	Inbound	gRPC (TLS v1.2)/27922	phRuleWorker to phRuleMaster Communication
Worker	Supervisor	Inbound	gRPC (TLS v1.2)/27934	phReportWorker to phReportMaster Communication
Spark Nodes	Supervisor	Inbound	TCP/60002-60003	Elasticsearch to HDFS Archive

Worker Communication

From	To	Inbound or Outbound	Ports	Services
FortiSIEM Management User	Worker	Inbound	ICMP	ICMP
External Device	Worker	Inbound	TCP/21	FTP (for receiving Bluecoat logs via ftp)
FortiSIEM Management User	Worker	Inbound	TCP/22	Admin access via SSH
Worker	External Device	Outbound	TCP/110	POP3 for email monitoring (STM)
Worker	NFS Server	Outbound	UDP/111, TCP/111	NFS Portmapper for writing events in NFS based deployments
Worker	External Windows Devices	Outbound	TCP/135	WMI based monitoring and log collection
Worker	External Windows Devices	Outbound	TCP/135, UDP/137, TCP/5985-5986	OMI based monitoring and log collection

From	To	Inbound or Outbound	Ports	Services
Worker	External Device	Outbound	TCP/143	IMAP for email monitoring (STM)
Worker	External Device	Outbound	UDP/161	SNMP based monitoring
External Device	Worker	Inbound	UDP/162	SNMP Trap
Worker	External Devices	Outbound	TCP/389	LDAP discovery
Worker	External Device	Outbound	TCP/443	HTTPS based log collection
Collector	Worker	Inbound	TCP/443	REST API access via HTTPS
Worker	External Device	Inbound, Outbound	TCP/443	Upgrade connects to os-pkgs-cdn.fortisiem.fortinet.com and os-pkgs-r8.fortisiem.fortinet.com for OS updates.
External Device	Worker	Inbound	TCP/514	TCP syslog
External Device	Worker	Inbound	UDP/514	UDP syslog
Worker	External Device	Outbound	TCP/993	IMAP/SSL for email monitoring (STM)
Worker	External Device	Outbound	TCP/995	POP/SSL for email monitoring (STM)
Worker	External Devices	Outbound	TCP/1433	JDBC based monitoring and data collection
External Device	Supervisor	Inbound	TCP/1470	TCP syslog
External Device	Worker	Inbound	UDP/2055	NetFlow
Worker	Worker (ClickHouse Keeper)	Inbound, Outbound	TCP/2181	Worker (Data/Query) Node to Keeper node traffic
Worker	Worker	Inbound, Outbound	RAFT/3888	ClickHouse Keeper Traffic for Worker nodes that are part of ClickHouse Keeper Cluster
Worker	Supervisor	Outbound	TCP/5555	phFortiInsightAI module data collection

From	To	Inbound or Outbound	Ports	Services
External Device	Worker	Inbound	UDP/6343	sFlow
External Device	Worker	Inbound	TLS (Supporting v1.2 & v1.3)/6514	Syslog over TLS
Supervisor	Worker	Inbound	TCP/6666	Redis communication
Worker	Supervisor	Outbound	TLS (Supporting v1.3)/7900	phMonitorWorker to phMonitorSuper communication
Supervisor	Worker	Inbound	TLS (Supporting v1.3)/7900	phMonitorSuper to phMonitorWorker Communication
Worker	Supervisor	Outbound	TLS (Supporting v1.3)/7914	phParser on Worker to phParser on Supervisor for EPS enforcement
Supervisor	Worker	Inbound	TLS (Supporting v1.3)/7916	phQueryMaster to phQueryWorker communication
Worker	Supervisor	Outbound	TLS (Supporting v1.3)	phQueryWorker to phQueryMaster Communication
Worker 6.1	Supervisor	Outbound	TLS (Supporting v1.3)/7920	phQueryMaster to phDataManager for trigger event query
Worker	Supervisor	Outbound	TLS (Supporting v1.3)	phRuleWorker to phRuleMaster communication
Worker	Supervisor	Outbound	TLS (Supporting V1.3)/7928	phParser on Worker to phDiscover on Supervisor to trigger a device discovery after detecting Cisco IOS BGP or OSPF Adjacency Change change
Worker	Supervisor	Outbound	TLS (Supporting v1.3)	phReportWorker to phReportMaster Communication
Worker	Supervisor	Outbound	TLS (Supporting v1.3)/7938	phIdentityWorker to phIdentityMaster
Worker	Worker	Inbound, Outbound	HTTP/8123, HTTPS/8443	ClickHouse Database Insert
Worker	External Devices	Outbound	UDP/8686	JMX based monitoring and data collection
Worker	HDFS Name Node	Outbound	HTTPS/9000 (configurable)	Archiving events for HDFS based deployments
Worker	Worker	Inbound, Outbound	9000, 9440	ClickHouse Internal Communication

From	To	Inbound or Outbound	Ports	Services
Worker	Worker	Inbound, Outbound	HTTP/9009, HTTPS/9010	ClickHouse Database Replication
Worker	Elasticsearch Coordinating Node	Outbound	HTTPS/9200 (configurable)	Storing events for Elasticsearch based deployments
Worker	Checkpoint	Outbound	TCP/18184	Checkpoint LEA based log collection
Worker	Checkpoint	Outbound	TCP/18190	Checkpoint CPML based data collection
Worker	Supervisor	Outbound	gRPC (TLS v1.2)/27918	phQueryWorker to phQueryMaster Communication
Worker	Supervisor	Outbound	gRPC (TLS v1.2)/27922	phRuleWorker to phRuleMaster Communication
Worker	Supervisor	Outbound	gRPC (TLS v1.2)/27934	phReportWorker to phReportMaster Communication
Spark Nodes	Supervisor	Inbound	TCP/60002-60003	Elasticsearch to HDFS Archive

Collector Communication

From	To	Inbound or Outbound	Ports	Services
FortiSIEM Management User	Collector	Inbound	ICMP	ICMP
External Device	Collector	Inbound	TCP/21	FTP (for receiving Bluecoat logs via ftp)
FortiSIEM Management User	Collector	Inbound	TCP/22	Admin access via SSH
Collector	External Device	Outbound	TCP/110	POP3 for email monitoring (STM)
Collector	External Windows Devices	Outbound	TCP/135	WMI based monitoring and log collection

From	To	Inbound or Outbound	Ports	Services
Collector	External Windows Devices	Outbound	TCP/135, UDP/137, TCP/5985-5986	OMI based monitoring and log collection
Collector	External Device	Outbound	TCP/143	IMAP for email monitoring (STM)
Collector	External Device	Outbound	UDP/161	SNMP based monitoring
External Device	Collector	Inbound	UDP/162	SNMP Trap
Collector	External Devices	Outbound	TCP/389	LDAP discovery
Collector	External Device	Outbound	TCP/443	HTTPS based log collection
Collector	Collector	Outbound	TCP/443	REST API access via HTTPS
Collector	Supervisor	Outbound	TCP/443	REST API access via HTTPS
Collector	External Device	Outbound	TCP/443	Upgrade connects to os-pkgs-cdn.fortisiem.fortinet.com and os-pkgs-r8.fortisiem.fortinet.com for OS updates.
External Device	Collector	Inbound	UDP/514	UDP syslog
External Device	Collector	Inbound	TCP/514	TCP syslog
Collector	External Devices	Outbound	TCP/636	LDAPS discovery
Collector	External Device	Outbound	TCP/993	IMAP/SSL for email monitoring (STM)
Collector	External Device	Outbound	TCP/995	POP/SSL for email monitoring (STM)
Collector	External Devices	Outbound	TCP/1433	JDBC based monitoring and data collection
External Device	Supervisor	Inbound	TCP/1470	TCP syslog
External Device	Collector	Inbound	UDP/2055	NetFlow
Collector	External Devices	Outbound	TCP/3268	LDAP discovery (Global Catalog port, Global Catalog TLS port)

From	To	Inbound or Outbound	Ports	Services
Collector	External Devices	Outbound	TCP/3269	LDAPS discovery (Global Catalog port)
External Device	Collector	Inbound	UDP/6343	sFlow
External Device	Collector	Inbound	TLS (Supporting v1.2 & v1.3)/6514	Syslog over TLS
Collector	External Devices	Outbound	UDP/8686	JMX based monitoring and data collection
Collector	Checkpoint	Outbound	TCP/18184	Checkpoint LEA based log collection
Collector	Checkpoint	Outbound	TCP/18190	Checkpoint CPML based data collection
Collector	Supervisor	Inbound	TCP/19999	Collector to Super Reverse SSH Tunnel (disabled by default)
Supervisor	Collector	Outbound	TCP/20000-30000	Collector to Super Reverse SSH Tunnel (disabled by default)

Supported Devices and Applications by Vendor

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
AirTight Networks	SpectraGuard	Discovered via LOG only	Not natively supported - Custom monitoring needed	CEF format: Over 125 event types parsed covering various Wireless suspicious activities	Currently not natively supported	AirTight Networks SpectraGuard
Akamai	Akamai Connected Cloud					Akamai Connected Cloud
Alcatel	TiMOS Routers and Switches	SNMP: OS, Hardware	SNMP: CPU, memory, interface utilization, hardware status	Not natively supported - Custom parsing needed	Currently not natively supported	Alcatel TiMOS and AOS Switch Configuration
Alcatel	AOS Routers and Switches	SNMP: OS, Hardware	SNMP: CPU, memory, interface utilization, hardware status	Not natively supported - Custom parsing needed	Currently not natively supported	Alcatel TiMOS and AOS Switch Configuration
Alert Logic	Intrusion Detection and Prevention Systems (IPS)	Host name and Device type	Not supported		Not supported	Alert Logic IPS
Alert Logic	Iris API	Host name and Device type	Not supported		Not supported	Alert Logic IRIS API
Alcide.io	KAudit	Not natively supported	Not natively supported	Kubernetes Audit logs	Not natively supported	Alcide io KAudit
Amazon	AWS Servers	AWS API: Server Name, Access IP, Instance ID, Image Type, Availability Zone	CloudWatch API: System Metrics: CPU, Disk I/O, Network	CloudTrail API: Over 325 event types parsed covering various AWS activities	CloudTrail API: various administrative changes on AWS systems and users	AWS CloudWatch AWS CloudTrail
Amazon	AWS Elastic Block Storage (EBS)	CloudWatch API: Volume ID, Status, Attach Time	CloudWatch API: Read/Write Bytes, Ops, Disk Queue			AWS EBS and RDS

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Amazon	AWS EC2					AWS EC2
Amazon	AWS Elastic Load Balancer (ELB)					AWS ELB
Amazon	AWS Kinesis					AWS Kinesis
Amazon	AWS Relational Database Storage (RDS)		CloudWatch API: CPU, Connections, Memory, Swap, Read/Write Latency and Ops			AWS EBS and RDS
Amazon	Security Hub					AWS Security Hub
Amazon	Simple Queue Service					AWS Simple Queue Service
Amazon	AWS S3 (Simple Storage Service)					AWS S3 (Simple Storage Service)
Apache	Tomcat Application Server	JMX: Version	JMX: CPU, memory, servlet, session, database, threadpool, request processor metrics	Currently not natively supported - Custom parsing needed	Currently not natively supported	Apache Tomcat
Apache	Apache Web server	SNMP: Process name	SNMP: process level cpu, memory HTTPS via the mod-status module: Apache level metrics	Syslog: W3C formatted access logs - per HTTP (S) connection: Sent Bytes, Received Bytes, Connection Duration	Currently not natively supported	Apache Web Server
APC	NetBotz Environmental Monitor	SNMP: Host name, Hardware model, Network interfaces	SNMP: Temperature, Relative Humidity, Airflow, Dew point, Current, Door switch sensor etc.	SNMP Trap: Over 125 SNMP Trap event types parsed covering various environmental exception conditions	Currently not natively supported	APC Netbotz
APC	UPS	SNMP: Host name, Hardware model, Network interfaces	SNMP: UPS metrics	SNMP Trap: Over 49 SNMP Trap event types parsed covering various environmental exception conditions	Currently not natively supported	APC UPS
Apple	MacOS Servers and Workstations					Apple MacOS Servers and Workstations
Arista Networks	Routers and Switches	SNMP: OS, Hardwar; SSH:	SNMP: CPU, Memory, Interface utilization, Hardware Status	Syslog and NetFlow	SSH: Running config, Startup	Arista Router and Switch

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		configuration, running processes			config	
Armis	Armis Asset Intelligence Platform					Armis Asset Intelligence Platform
Aruba Networks	CX Switching Platform			Syslog: Audit logs, General Performance and Availability logs		ArubaOS-CX Switching Platform
Aruba Networks	Aruba Wireless LAN	SNMP: Controller OS, hardware, Access Points	SNMP: Controller CPU, Memory, Interface utilization, Hardware Status SNMP: Access Point Wireless Channel utilization, noise metrics, user count	SNMP Trap: Over 165 event types covering Authentication, Association, Rogue detection, Wireless IPS events	Currently not natively supported	Aruba WLAN
Atlassian	Beacon					Atlassian Beacon
Avaya	Call Manager	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status	CDR: Call Records	Currently not natively supported	Avaya Call Manager
Avaya	Session Manager	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		Currently not natively supported	
Barracuda Networks	Spam Firewall	Application type discovery via LOG	Currently not natively supported	Syslog: Over 20 event types covering mail scanning and filtering activity	Currently not natively supported	Barracuda Spam
Barracuda Networks	Web Application Firewall			Syslog: System logs, Web Firewall logs, Access logs, Audit logs and Network Firewall logs		Barracuda Web Application Firewall
Bit9	Security platform	Application type discovery via LOG	Currently not natively supported	Syslog: Over 259 event types covering various file monitoring activities	Currently not natively supported	Bit9 Security Platform
Bitdefender				Syslog		Bitdefender GravityZone
Blue Coat	Security Gateway Versions v4.x	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Proxy performance metrics	Syslog: Admin access to Security Gateway ; SFTP: Proxy traffic	Currently not natively supported	Blue Coat Web Proxy

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	and later			analysis		
Box.com	Cloud Storage	Currently not natively supported	Currently not natively supported	Box.com API: File creation, deletion, modify, file sharing	Currently not natively supported	Box.com
Brocade	SAN Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	Currently not natively supported	Currently not natively supported	Brocade SAN Switch
Brocade	ServerIron ADX switch	SNMP: Host name, serial number, hardware	SNMP: Uptime, CPU, Memory, Interface Utilization, Hardware status, Real Server Statistics			Brocade ADX
Carbon Black	Security platform	Application type discovery via LOG	Currently not natively supported	Syslog: Over 259 event types covering various file monitoring activities	Currently not natively supported	Carbon Black Security Platform
CentOS / Other Linux distributions	Linux	SNMP: OS, Hardware, Software, Processes, Open Ports SSH: Hardware details, Linux distribution	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification; SSH: File integrity monitoring, Command output monitoring, Target file monitoring; FortiSIEM LinuxFileMon Agent: File integrity monitoring	SSH: File integrity monitoring, Target file monitoring; Agent: File integrity monitoring	Linux Server
CentOS / Other Linux distributions	DHCP Server	Currently not natively supported	Currently not natively supported	Syslog: DHCP activity (Discover, Offer, Request, Release etc) - Used in Identity and Location	Not Applicable	Linux DHCP
Checkpoint	FireWall-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, R75, R80	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	LEA from SmartCenter or Log Server: Firewall Log, Audit trail, over 940 IPS Signatures	LEA: Firewall Audit trail	Check Point Provider-1 Firewall
Checkpoint	GAIA	Host name and Device type		Over 9 event types		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Checkpoint	Provider-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, and R75	Currently not natively supported	Currently not natively supported	LEA: Firewall Log, Audit trail	LEA: Firewall Audit trail	Check Point Provider-1
Checkpoint	VSX	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	LEA from SmartCenter or Log Server: Firewall Log, Audit trail	LEA: Firewall Audit trail	Check Point Provider-1
Citrix	NetScaler Application Delivery Controller	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status, Application Firewall metrics	Syslog: Over 465 event types covering admin activity, application firewall events, health events	Currently not natively supported	Citrix Netscaler
Citrix	ICA	SNMP: Process Utilization	SNMP: Process Utilization; WMI: ICA Session metrics	Currently not natively supported	Currently not natively supported	Citrix ICA
Cisco	ASA Firewall (single and multi-context) version 7.x and later	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Firewall Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity; NetFlow V9: Traffic log	SSH: Running config, Startup config	Cisco ASA
Cisco	AMP					Cisco AMP for Endpoints API V1 - Previously Cisco AMP
Cisco	FireAMP					Cisco AMP for Endpoints API V0 - Previously Cisco FireAMP Cloud
Cisco	ASA firepower SFR Module	SNMP: OS, Hardware SSH: interface security level needed for	SNMP: CPU, Memory, Interface utilization, Firewall Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity;	SSH: Running config, Startup config	Cisco ASA

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		parsing traffic logs, Configuration		NetFlow V9: Traffic log		
Cisco	Firepower Threat Defense					Cisco FTD
Cisco	CatOS based Switches	SNMP: OS, Hardware (Serial Number, Image file, Interfaces, Components); SSH: configuration running process	SNMP: CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 700 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, IPS activity NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config	Cisco IOS
Cisco	Duo		Not natively supported - Custom Monitoring needed	Via API	Not natively supported - Custom Configuration collection needed	Cisco Duo
Cisco	PIX Firewall	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity	SSH: Running config, Startup config	Cisco ASA
Cisco	FWSM	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity	SSH: Running config, Startup config	Cisco ASA

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
n						
Cisco	Identity Services Engine (ISE)	Host name and Device type				Cisco ISE
Cisco	IOS based Routers and Switches	SNMP: OS, Hardware; SSH: configuration, running process, Layer 2 connectivity	SNMP: CPU, Memory, Interface utilization, Hardware Status; SNMP: IP SLA metrics; SNMP: BGP metrics, OSPF metrics; SNMP: Class based QoS metrics; SNMP: NBAR metrics	Syslog: Over 200 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, IPS activity; NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config	Cisco IOS
Cisco	Nexus OS based Routers and Switches	SNMP: OS, Hardware; SSH: configuration running process, Layer 2 connectivity	SNMP: CPU, Memory, Interface utilization, Hardware Status; SNMP: IP SLA metrics, BGP metrics, OSPF metrics, NBAR metrics; SNMP: Class based QoS metrics	Syslog: Over 3500 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, hardware status, software and hardware errors; NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config	Cisco NX-OS
Cisco	ONS	SNMP: OS, Hardware		SNMP Trap: Availability and Performance Alerts		Cisco NX-OS
Cisco	ACE Application Firewall	SNMP: OS, Hardware				
Cisco	UCS Server	UCS API: Hardware components - processors, chassis, blades, board, cpu, memory, storage, power supply unit, fan unit	UCS API: Chassis Status, Memory Status, Processor Status, Power Supply status, Fan status	Syslog: Over 500 event types parsed for situations covering hardware errors, internal software errors etc	Currently not natively supported	Cisco UCS
Cisco	WLAN Controller	SNMP: OS,	SNMP: Controller CPU,	SNMP Trap: Over 88	Currently not	Cisco Wireless

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	and Access Points	Hardware, Access Points	Memory, Interface utilization, Hardware Status; SNMP: Access Point Wireless Channel utilization, noise metrics, user count	event types parsed for situations covering Authentication, Association, Rogue detection, Wireless IPS events	natively supported	LAN
Cisco	Call Manager	SNMP: OS, Hardware, VoIP Phones	SNMP: Call manager CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage; SNMP: VoIP phone count, Gateway count, Media Device count, Voice mail server count and SIP Trunks count; SNMP: SIP Trunk Info, Gateway Status Info, H323 Device Info, Voice Mail Device Info, Media Device Info, Computer Telephony Integration (CTI) Device Info	Syslog: Over 950 messages from Cisco Call Manager as well as Cisco Unified Real Time Monitoring Tool (RTMT); CDR Records, CMR Records: Call Source and Destination, Time, Call Quality metrics (MOS Score, Jitter, latency)	Currently not natively supported	Cisco Call Manager
Cisco	Contact Center	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Contact Center
Cisco	Presence Server	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Presence Server
Cisco	Tandberg Tele-presence Video Communication Server (VCS)	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Tandberg Telepresence VCS
Cisco	Tandberg Tele-presence Multiple Control Unit (MCU)	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Telepresence MCU
Cisco	Unity Connection	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization,	Currently not natively supported - Custom	Currently not natively	Cisco Unity

Supported Devices and Applications by Vendor

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
			Hardware Status, Process level resource usage, Install software change	parsing needed	supported	
Cisco	IronPort Mail Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Syslog: Over 45 event types covering mail scanning and forwarding status	Currently not natively supported	Cisco IronPort Mail
Cisco	IronPort Web Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	W3C Access log (Syslog): Over 9 event types covering web request handling status	Currently not natively supported	Cisco IronPort Web
Cisco	Cisco Network IPS Appliances	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status	SDEE: Over 8000 IPS signatures	Currently not natively supported	Cisco NIPS
Cisco	Sourcefire 3D and Defense Center	SNMP: OS, Hardware				Sourcefire 3D and Defense Center
Cisco	Cisco Firepower Management Center (FMC) - Previously FireSIGHT Console			eStreamer SDK: Intrusion events, Malware events, File events, Discovery events, User activity events, Impact flag events		Cisco Firepower Management Center (FMC) - Previously Cisco FireSIGHT
Cisco	Cisco Security Agent	SNMP or WMI: OS, Hardware	SNMP or WMI: Process CPU and memory utilization	SNMP Trap: Over 25 event types covering Host IPS behavioral signatures.	Currently not natively supported	Cisco CSA
Cisco	Cisco Access Control Server (ACS)	SNMP or WMI: OS, Hardware	SNMP or WMI: Process CPU and memory utilization	Syslog: Passed and Failed authentications, Admin accesses	Currently not natively supported	Cisco ACS
Cisco	VPN 3000	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	Syslog: Successful and Failed Admin Authentication, VPN Authentication, IPSec Phase 1 and Phase 2 association, VPN statistics	Currently not natively supported	Cisco VPN 3000
Cisco	Meraki Cloud	SNMP: OS,	SNMP: Uptime, Network	Currently not natively	Currently not	Cisco Meraki

Supported Devices and Applications by Vendor

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	Controllers	Hardware, Meraki devices reporting to the Cloud Controller	Interface Utilization; SNMP Trap: Various availability scenarios	supported - Custom parsing needed	natively supported	Cloud Controller and Network Devices
Cisco	Meraki Firewalls	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization	Syslog: Firewall log analysis	Currently not natively supported	Cisco Meraki Cloud Controller and Network Devices
Cisco	Meraki Routers/Switches	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization		Currently not natively supported	Cisco Meraki Cloud Controller and Network Devices
Cisco	Meraki WLAN Access Points	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization		Currently not natively supported	Cisco Meraki Cloud Controller and Network Devices
Cisco	MDS Storage Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status	Currently not natively supported - Custom parsing needed	Currently not natively supported	
Cisco	Network Control Manager (NCM)			Syslog: Network device software update, configuration analysis for compliance, admin login		Cisco Network Compliance Manager
Cisco	Stealthwatch	Host name and Device type	Not supported		Not supported	Cisco Stealthwatch
Cisco	Umbrella			DNS logs, Proxy logs, IP logs, Admin Audit logs		Cisco Umbrella
Cisco	Viptela	Discovered Via LOG only	Not natively supported - Custom monitoring needed	Over 289 Events Types parsed	Not natively supported - Custom configuration collection needed	Cisco Viptela SDWAN Router
Cisco	Wide Area Application Services (WAAS)	SNMP: Host name, Version,	SNMP: CPU, Memory, Interface utilization, Disk utilization, Process			Cisco WAAS

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		Hardware model, Network interfaces	cpu/memory utilization			
Claroty	Continuous Threat Detection (CTD)					Claroty Continuous Threat Detection (CTD)
CloudPassage	Halo	Host name and Device type	Not supported		Not supported	CloudPassage Halo
Corero	Smartwall Threat Defense System					Corero Smartwall Threat Defense System
CradlePoint	CradlePoint	Discovered via LOG only	Not natively supported. Custom monitoring needed	29 Event types covering Security Violations, Config Changes, Authentications and informational events	Not currently supported.	CradlePoint
CrowdStrike	Falcon	Host name and Device type	Not supported		Not supported	CrowdStrike Falcon
Cybereason	Cybereason					Cybereason
Cyberoam	Cyberoam	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Event, Security, and Traffic logs	Connection - permit and deny, system events, malware events	Cyberoam Firewall
Cylance	Cylance Protect Endpoint Protection			Syslog: Endpoint protection alerts		Cylance Protect
Cyphort	Cyphort Cortex Endpoint Protection			Syslog: Endpoint protection alerts		Cyphort Cortex
Cyxtera	AppGate SDP	Host name and Device type	Not supported		Not supported	Cyxtera AppGate SDP
Damballa	Failsafe					Damballa

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
						Failsafe
Darktrace	CyberIntelligence Platform	Discovered via LOG only	Not natively supported - Custom monitoring needed	Over 40 Events Types parsed	Not Natively Supported - Custom Configuration collection needed	Darktrace CyberIntelligence Platform
Dell	SonicWall Firewall	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Firewall session count	Syslog: Firewall log analysis (over 1000 event types)	Currently not natively supported	Dell SonicWALL
Dell	Force10 Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Interface Status, Hardware Status		SSH: Running config, Startup config	Dell Force10
Dell	NSeries Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		SSH: Startup config	Dell NSeries
Dell	PowerConnect Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		SSH: Startup config	Dell PowerConnect
Dell	Dell Hardware on Intel-based Servers	SNMP: Hardware	SNMP: Hardware Status: Battery, Disk, Memory, Power supply, Temperature, Fan, Amperage, Voltage		Currently not natively supported.	
Dell	Compellent Storage	SNMP: OS, Hardware	SNMP: Network Interface utilization, Volume utilization, Hardware Status (Power, Temperature, Fan)		Currently not natively supported.	Dell Compellent
Dell	EqualLogic Storage	SNMP: OS, Hardware (Network interfaces, Physical Disks, Components)	SNMP: Uptime, Network Interface utilization; SNMP: Hardware status: Disk, Power supply, Temperature, Fan, RAID health; SNMP: Overall Disk health metrics: Total disk count, Active disk count, Failed disk count, Spare disk count; SNMP: Connection metrics: IOPS, Throughput; SNMP: Disk performance metrics: IOPS, Throughput; SNMP: Group level performance metrics:		Currently not natively supported.	Dell EqualLogic

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Storage, Snapshot						
Digital Defense	Frontline Vulnerability Manager			Frontline API: Host name, Vulnerability name, Vulnerability CVE ID, Vulnerability score, and operating system in event.		Digital Defense Frontline Vulnerability Manager
Digital Guardian	Code Green DLP	LOG Discovery	Currently not natively supported	1 broad event Type	Currently not natively supported	Digital Guardian Code Green DLP
Dragos	Platform - Industrial control systems (ICS) and OT (operational technology)					Dragos Platform
EMC	Clariion Storage	Naviseccli: Host name, Operating system version, Hardware model, Serial number, Network interfaces, Installed Software, Storage Controller Ports; Naviseccli: Hardware components, RAID Groups and assigned disks, LUNs and LUN -> RAID Group mappings, Storage Groups and memberships	Naviseccli: Storage Processor utilization, Storage Port I/O, RAID Group I/O, LUN I/O, Host HBA Connectivity, Host HBA Unregistered Host, Hardware component health, Overall Disk health, Storage Pool Utilization		Currently not natively supported.	EMC Clariion

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
EMC	VNX Storage	Naviseccli: Host name, Operating system version, Hardware model, Serial number, Network interfaces, Installed Software, Storage Controller Ports Naviseccli: Hardware components, RAID Groups and assigned disks, LUNs and LUN -> RAID Group mappings, Storage Groups and memberships	Naviseccli: Storage Processor utilization, Storage Port I/O, RAID Group I/O, LUN I/O, Host HBA Connectivity, Host HBA Unregistered Host, Hardware component health, Overall Disk health, Storage Pool Utilization			EMC VNX
EMC	Isilon Storage	SNMP: Host name, Operating system, Hardware (Model, Serial number, Network interfaces, Physical Disks, Component s)	SNMP: Uptime, Network Interface metrics; SNMP: Hardware component health: Disk, Power supply, Temperature, Fan, Voltage; SNMP: Cluster membership change, Node health and performance (CPU, I/O), Cluster health and performance, Cluster Snapshot, Storage Quota metrics, Disk performance, Protocol performance	5 event types		EMC Isilon
Epic	SecuritySIEM	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Authentication Query, Client login Query	Currently not natively supported	Epic EMR/EHR System

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
ESET	Nod32 Anti-virus	Application type discovery via LOG		Syslog (CEF format): Virus found/cleaned type of events		ESET NOD32
FireEye	Malware Protection System (MPS)	Application type discovery via LOG		Syslog (CEF format): Malware found/cleaned type of events		FireEye MPS
FireEye	HX Appliances for Endpoint protection	Application type discovery via LOG		Syslog (CEF format): Malware Acquisition, Containment type of events		
F5 Networks	Application Security Manager	Discovery via LOG		Syslog (CEF Format); Various application level attack scenarios - invalid directory access, SQL injections, cross site exploits		F5 Application Security Manager
F5 Networks	Local Traffic Manager	SNMP: Host name, Operating system, Hardware (Model, Serial number, Network interfaces, Physical Disks), Installed Software, Running Software	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start	SNMP Trap: Exception situations including hardware failures, certain security attacks, Policy violations etc; Syslog: Permitted and Denied Traffic		F5 Networks Local Traffic Manager
F5 Networks	Web Accelerator	Discovery via LOG		Syslog: Permitted Traffic		F5 Networks Web Accelerator
Fortinet	FortiNDR (Formerly FortiAI)					Fortinet FortiNDR (Formerly FortiAI)

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Fortinet	FortiNDR Cloud					Fortinet FortiNDR Cloud
Fortinet	FortiAnalyzer					Fortinet FortiAnalyzer
Fortinet	FortiAP	Access point – Name, OS, Interfaces, Controller (FortiGate)	FortiAP CPU, Memory, Clients, Sent/Received traffic	Wireless events via FortiGate		FortiAP
Fortinet	FortiAuthenticator	Vendor, OS, Model	Interface Stat, Authentication Stat	Over 150 event types	Currently not natively supported.	Fortinet FortiAuthenticator
Fortinet	FortiCASB					Fortinet FortiCASB
Fortinet	FortiClient	Discovered via LOG only		Syslog: Traffic logs, Event logs	Not supported	FortiClient
Fortinet	FortiClient EMS					FortiClient EMS
Fortinet	FortiDeceptor	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Authentication logs, Decoy activity	Currently not natively supported.	Fortinet FortiDeceptor
Fortinet	FortiEDR	Discovered via LOG only	Not natively supported. Custom monitoring needed.	System and security events (e.g. file blocked)	Currently not natively supported	Fortinet FortiEDR
Fortinet	FortiGate firewalls	SNMP: OS, Host name, Hardware (Serial Number, Interfaces, Components)	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics	Syslog: Over 11000 Traffic and system logs; Netflow: traffic flow, Application flow	SSH: Running config, Startup config	Fortinet FortiGate
Fortinet	FortiManager	SNMP: Host name, Hardware model, Network interfaces, Operating system version	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics			FortiManager

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Fortinet	FortiMail Workspace Security					Fortinet FortiMail Workspace Security
Fortinet	FortiNAC	Discovered via LOG only	Not natively supported. Custom monitoring needed	Administrative and User Admission Control events	Currently not natively supported	Fortinet FortiNAC
Fortinet	FortiPAM / FortiSRA					Fortinet FortiPAM / FortiSRA
Fortinet	FortiProxy					Fortinet FortiProxy
Fortinet	FortiRecon					Fortinet FortiRecon
Fortinet	FortiTester	Discovered Via LOG only	Not natively supported - Custom monitoring needed	CEF format: Over 14 Event types parsed	Not natively supported - Custom configuration collection needed	Fortinet FortiTester
Fortinet	FortiWLC	SNMP - Controller - Name, OS, Serial Number, Interfaces, Associated Access Points - name, OS, Interfaces	Controller - CPU, Memory, Disk, Throughput, QoS statistics, Station count	Hardware/Software errors, failures, logons, license expiry, Access Point Association / Disassociation	Not supported	FortiWLC
Foundry Networks	IronWare Router and Switch	SNMP: OS, Hardware SSH: configuration, running process	SNMP: Uptime, CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 6000 event types parsed for situations covering admin access, configuration change, interface up/down	SSH: Running config, Startup config	Foundry Networks IronWare
FreeBSD						
G42 Cloud	G42 Cloud					G42 Cloud
GitHub.com	GitHub	Host name and Device type	Not supported		Not supported	GitHub

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
GitLab	GitLab					GitLab
GitLab API	GitLab	Host name and Device type	Not supported		Not supported	GitLab API
GitLab CLI	GitLab	Host name and Device type	Not supported		Not supported	GitLab CLI
Google	Google Cloud Platform					Google Cloud Platform - Pub/Sub Integration
Google	Google Workspace (Formerly G Suite and Google Apps)					Google Workspace (Formerly G Suite and Google Apps)
Green League	WVSS					Green League WVSS
Hillstone Networks	Hiistone Firewall					Hiistone Firewall
Hirschmann	Switches	Host Name, OS	SNMP – Uptime, CPU, Memory, Interface utilization, hardware Status, OSPF metrics	Not natively supported - Custom parsing needed	Not natively supported - Custom configuration collection needed	Hirschmann SCADA Firewalls and Switches
HP	BladeSystem	SNMP: Host name, Access IP, Hardware components	SNMP: hardware status			HP BladeSystem
HP	HP-UX servers	SNMP: OS, Hardware	SNMP: Uptime, CPU, Memory, Network Interface, Disk space utilization, Network Interface Errors, Running Process Count, Running process CPU/memory utilization, Running process start/stop; SNMP: Installed Software change; SSH : Memory paging			HP UX Server

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
			rate, Disk I/O utilization			
HP	HP Hardware on Intel-based Servers	SNMP: hardware model, hardware serial, hardware components (fan, power supply, battery, raid, disk, memory)	SNMP: hardware status	SNMP Trap: Over 100 traps covering hardware issues		
HP	TippingPoint UnityOne IPS	SNMP: OS, Hardware	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors	Syslog: Over 4900 IPS alerts directly or via NMS		TippingPoint IPS
HP	ProCurve Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors; SNMP: hardware status		SSH: Running config, Startup config	HP ProCurve
HP	Value Series (19xx) Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors		SSH: Startup config	HP Value Series (19xx) and HP 3Com (29xx) Switch
HP	3Com (29xx) Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors		SSH: Startup config	HP Value Series (19xx) and HP 3Com (29xx) Switch

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
HP	HP/3Com Comware Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors; SNMP: hardware status	Syslog: Over 6000 event types parsed for situations covering admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup config	HP/3Com ComWare
HPE	Aruba Networking ClearPass Policy Manager					HPE Aruba Networking ClearPass Policy Manager
HPE	Integrated Lights-Out (iLO)					HPE Integrated Lights-Out (iLO)
Huawei	VRP Router and Switch	SNMP: OS, Hardware; SSH: configuration, running process, Layer 2 connectivity	SNMP: Uptime, CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 30 event types parsed for situations covering admin access, configuration change, interface up/down	SSH: Running config, Startup config	
HyTrust	CloudControl	LOG Discovery	Currently not natively supported	Over 70 event types	Currently not natively supported	HyTrust CloudControl
IBM	WebSphere Application Server	SNMP or WMI: Running processes	HTTP(S): Generic Information, Availability metrics, CPU / Memory metrics, Servlet metrics, Database pool metrics, Thread pool metrics, Application level metrics, EJB metrics			IBM WebSphere
IBM	DB2 Database Server	SNMP or WMI: Running processes	JDBC: Database Audit trail: Log on, Database level and Table level CREATE/DELETE/MODIFY operations			IBM DB2
IBM	ISS Proventia IPS Appliances			SNMP Trap: IPS Alerts: Over 3500 event types		IBM ISS Proventia
IBM	AIX Servers	SNMP: OS,	SNMP: CPU, Memory, Disk,	Syslog: General logs		IBM AIX

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		Hardware, Installed Software, Running Processes, Open Ports; SSH: Hardware details	Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	including Authentication Success/Failure, Privileged logons, User/Group Modification		
IBM	OS 400			Syslog via PowerTech Agent: Over 560 event types		IBM OS400
Imperva	Securesphere DB Monitoring Gateway					Imperva Securesphere DB Monitoring Gateway
Imperva	Securesphere Security Gateway			Syslog in CEF format		Imperva Securesphere Security Gateway
Imperva	Securesphere Web App Firewall					Imperva SecureSphere Web App Firewall
Indegy	Security Platform	Discovered via LOG only			Not natively supported - Custom configuration collection needed	Indegy Security Platform
Infoblox	DNS/DHCP Appliance	SNMP: OS, Hardware, Installed Software, Running Processes	; SNMP: Zone transfer metrics, DNS Cluster Replication metrics, DNS Performance metrics, DHCP Performance metrics, DDNS Update metrics, DHCP subnet usage metrics ; SNMP: Hardware Status ; SNMP Trap: Hardware/Software Errors	Syslog: DNS logs - name resolution activity - success and failures		Infoblox DNS/DHCP
ISC	Bind DNS			Syslog: DNS logs - name resolution activity - success and		ISC BIND DNS

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				failures		
Juniper	JunOS Router/Switch	SNMP: OS, Hardware; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status ;	Syslog: Over 1420 event types parsed for situations covering admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks JunOS
Juniper	SRX Firewalls	SNMP: OS, Hardware; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 700 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks JunOS
Juniper	SSG Firewall	SNMP: OS, Hardware ; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 40 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks SSG Firewall
Juniper	ISG Firewall	SNMP: OS, Hardware ; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 40 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks SSG Firewall
Juniper	Steel-belted Radius	Discovered via LOG		Syslog - 4 event types covering admin access and AAA authentication		Juniper Networks Steel-Belted Radius
Juniper	Secure Access Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk, Interface utilization	Syslog - Over 30 event types parsed for situations covering		Juniper Networks SSL VPN Gateway

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				VPN login, Admin access, Configuration Change		
Juniper	Netscreen IDP			Syslog - directly from Firewall or via NSM - Over 5500 IPS Alert types parsed		Juniper Networks IDP Series
Juniper	DDoS Secure			Syslog - DDoS Alerts		Juniper DDoS
Kaspersky				Syslog		Kaspersky
KVM						KVM
Lantronix	SLC Console Manager			Syslog - Admin access, Updates, Commands run		Lantronix SLC Console Manager
LastLine				Syslog in CEF format		LastLine
Liebert	HVAC	SNMP: Host Name, Hardware model	SNMP: HVAC metrics: Temperature: current value, upper threshold, lower threshold, Relative Humidity: current value, upper threshold, lower threshold, System state etc			Liebert HVAC
Liebert	FPC	SNMP: Host Name, Hardware model	SNMP: Output voltage (X-N, Y-N, Z-N), Output current (X, Y, Z), Neutral Current, Ground current, Output power, Power Factor etc			Liebert FPC
Liebert	UPS	SNMP: Host Name, Hardware model	SNMP: UPS metrics: Remaining battery charge, Battery status, Time on battery, Estimated Seconds Remaining, Output voltage etc			Liebert UPS
Malwarebytes	Malwarebytes Breach Remediation					Malwarebytes Breach Remediation
Malwarebytes	Malwarebytes Endpoint Protection					Malwarebytes Endpoint Protection

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
ManageEngine	Endpoint Central					ManageEngine Endpoint Central
ManageEngine	PAM360					ManageEngine PAM360
McAfee	ePolicy Orchestrator (ePO)	SNMP: Related process name and parameters	SNMP: Process resource utilization	SNMP Trap: Over 170 event types		McAfee ePolicy Orchestrator (ePO)
McAfee	Network Security Platform	SNMP: OS, Hardware	SNMP: Hardware status	Syslog: IPS Alerts		McAfee Network Security Platform (formerly McAfee IntruShield)
McAfee	Stonesoft Intrusion Prevention System (IPS)			Syslog: IPS Alerts		McAfee Stonesoft
McAfee	McAfee Web Gateway			Syslog: Web server log		McAfee Web Gateway
Microsoft	ASP.NET	SNMP: Running Processes	SNMP or WMI: Process level resource usage ; WMI: Request Execution Time, Request Wait Time, Current Requests, Disconnected Requests etc			Microsoft ASP.NET
Microsoft	Microsoft Advanced Threat Analytics (ATA) On Premise Platform					Microsoft Advanced Threat Analytics (ATA) On Premise Platform
Microsoft	Microsoft Defender for Identity/Azure Advanced Threat Protection (ATP)	Host name and Device type	Not supported		Not supported	Microsoft Defender for Identity/Microsoft Azure ATP
Microsoft	Azure Compute					Microsoft Azure Compute
Microsoft	Azure Event Hub					Microsoft Azure Event Hub

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Microsoft	Cloud App Security	Host name and Device type	Not supported		Not supported	Microsoft Cloud App Security
Microsoft	DHCP Server - 2003, 2008	SNMP: Running Processes	WMI: DHCP metrics: request rate, release rate, decline rate, Duplicate Drop rate etc	FortiSIEM Windows Agent (HTTPS): DHCP logs - release, renew etc; Snare Agent (syslog): DHCP logs - release, renew etc; Correllog Agent (syslog): DHCP logs - release, renew etc		Microsoft DHCP (2003, 2008)
Microsoft	DNS Server - 2003, 2008	SNMP: Running Processes	WMI: DNS metrics: Requests received, Responses sent, WINS requests received, WINS responses sent, Recursive DNS queries received etc	FortiSIEM Windows Agent (HTTPS): DNS logs - name resolution activity; Snare Agent (syslog): DNS logs - name resolution activity; Correllog Agent (syslog): DNS logs - name resolution activity		Microsoft DNS (2003, 2008)
Microsoft	Domain Controller / Active Directory - 2003, 2008, 2012	SNMP: Running Processes; LDAP: Users	WMI: Active Directory metrics: Directory Search Rate, Read Rate, Write Rate, Browse Rate, LDAP search rate, LDAP Bind Rate etc; WMI: "dcdiag -e" command output - detect successful and failed domain controller diagnostic tests; WMI: "repadmin /replsummary" command output - Replication statistics; LDAP: Users with stale passwords, insecure password settings			Microsoft Active Directory
Microsoft	Entra Identity Protection					Microsoft Entra Identity Protection
Microsoft	Exchange Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage; WMI: Exchange performance		Exchange Tracker Logs via FSM Advanced	Microsoft Exchange

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
			metrics, Exchange error metrics, Exchange mailbox metrics, Exchange SMTP metrics, Exchange ESE Database, Exchange Database Instances, Exchange Mail Submission Metrics, Exchange Store Interface Metrics etc		Windows Agent	
Microsoft	Hyper-V Hypervisor		Powershell over winexe: Guest/Host CPU usage, Memory usage, Page fault, Disk Latency, Network usage ;			Hyper-V
Microsoft	IIS versions	SNMP: Running Processes	SNMP or WMI: Process level resource usage WMI: IIS metrics: Current Connections, Max Connections, Sent Files, Received Files etc	FortiSIEM Windows Agent (HTTPS): W3C Access logs - Per instance Per Connection - Sent Bytes, Received Bytes, Duration ; Snare Agent (syslog): W3C Access logs; Coralog Agent (syslog): W3C Access logs		Microsoft IIS for Windows 2000 and 2003; Microsoft IIS for Windows 2008
Microsoft	Internet Authentication Server (IAS)	SNMP: Running Processes	SNMP or WMI: Process level resource usage	FortiSIEM Windows Agent (HTTPS): AAA logs - successful and failed authentication ; Snare Agent (syslog): AAA logs - successful and failed authentication ; Coralog Agent (syslog): AAA logs - successful and failed authentication		Microsoft Internet Authentication Server (IAS)
Microsoft	Network Policy Server	Discovered via LOG only.	Not natively supported. Custom monitoring needed.	AAA-based login events	Currently not natively supported	Microsoft Network Policy Server
Microsoft	PPTP VPN Gateway			FortiSIEM Windows Agent (HTTPS): VPN		Microsoft PPTP

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				Access - successful and failed Share Agent (syslog): VPN Access - successful and failed ; Correllog Agent (syslog): VPN Access - successful and failed		
Microsoft	SharePoint Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage	LOGBinder Agent: SharePoint logs - Audit trail integrity, Access control changes, Document updates, List updates, Container object updates, Object changes, Object Import/Exports, Document views, Information Management Policy changes etc		Microsoft SharePoint
Microsoft	SQL Server - 2014, 2016, 2017, 2019	SNMP: Running Processes	SNMP or WMI: Process resource usage; JDBC: General database info, Configuration Info, Backup Info,; JDBC: Per-instance like Buffer cache hit ratio, Log cache hit ratio etc; JDBC: per-instance, per-database Performance metrics Data file size, Log file used, Log growths etc; JDBC: Locking info, Blocking info	JDBC: database error log; JDBC: Database audit trail		Microsoft SQL Server
Microsoft	Microsoft Defender for Endpoint/Windows Defender Advanced Threat Protection (ATP)	Host name and Device type	Not supported		Not supported	Microsoft Defender for Endpoint/Windows Defender ATP
Microsoft	Windows 2000, Windows 2003, Windows 2008, Windows 2008 R2, Windows	SNMP: OS, Hardware (for Dell and HP), Installed	SNMP: CPU, Memory, Disk, Interface utilization, Process utilization ; WMI: SNMP: CPU, Memory, Disk, Interface utilization, Detailed	WMI pulling: Security, System and Application logs; FortiSIEM Windows Agent (HTTPS): Security,	SNMP: Installed Software Change; FortiSIEM	Microsoft Windows Servers

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	2012, Windows 2012 R2	Software, Running Processes; WMI: OS, Hardware (for Dell and HP), BIOS, Installed Software, Running Processes, Services, Installed Patches	CPU/Memory usage, Detailed Process utilization	System and Application logs, File Content change; Snare Agent (syslog): Security, System and Application logs; Correlog Agent (syslog): Security, System and Application logs	Windows Agent: Installed Software Change, Registry Change; FortiSIEM Windows Agent: File Integrity Monitoring	
Mimecast	Mimecast Cloud Gateway					Mimecast
MobileIron Sentry and Connector	Sentry	Discovered Via LOG only	Not natively supported - Custom monitoring needed	Over 18 Events Types parsed	Not natively supported - Custom configuration collection needed	MobileIron Sentry
Motorola	AirDefense Wireless IDS			Syslog: Wireless IDS logs		Motorola AirDefense
Motorola	WiNG WLAN Access Point			Syslog: All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health		Motorola WLAN
Mikrotek	Mikrotech Switches and Routers	Host name, OS, Hardware model, Serial number, Components	SNMP: Uptime CPU utilization, Network Interface metrics			Mikrotek Router
NetApp	DataONTAP					NetApp DataONTAP
NetApp	DataONTAP based Filers	SNMP: Host name, OS, Hardware model, Serial number,	SNMP: CPU utilization, Network Interface metrics, Logical Disk Volume utilization; SNMP: Hardware component health, Disk	SNMP Trap: Over 150 alerts - hardware and software alerts		NetApp Filer

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		Network interfaces, Logical volumes, Physical Disks	health ONTAP API: Detailed NFS V3/V4, ISCSI, FCP storage IO metrics, Detailed LUN metrics, Aggregate metrics, Volume metrics, Disk performance metrics			
Nessus	Vulnerability Scanner			Nessus API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence, etc		Nessus Vulnerability Scanner
Netwrix	Auditor	Not natively supported	Not natively supported	2 Event Types parsed (via Windows Correllog Agent)	Not natively supported	Netwrix Auditor
NGINX	Web Server	SNMP: Application name	SNMP: Application Resource Usage	Syslog: W3C access logs: per HTTP(S) connection: Sent Bytes, Received Bytes, Connection Duration		NGINX Web Server
Nimble	NimbleOS Storage	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	SNMP: Uptime, Network Interface metrics, Storage Disk Utilization SNMP: Storage Performance metrics: Read rate (IOPS), Sequential Read Rate (IOPS), Write rate (IOPS), Sequential Write Rate (IOPS), Read latency, etc			Nimble Storage
Nortel	ERS Switches and Routers	SNMP: Host name, OS, Hardware model, Serial number,	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Hardware Status			Nortel ERS and Passport Switch

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Components						
Nortel	Passport Switches and Routers	SNMP: Host name, OS, Hardware model, Serial number, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Hardware Status			Nortel ERS and Passport Switch
Nozomi	Central Management Control (CMC)					Nozomi Central Management Control
Nozomi	Guardian	No	No	Yes	No	Nozomi SCADAguardian
Nutanix	Controller VM	SNMP: Host name, OS, Hardware model, Serial number, Network interfaces, Physical Disks, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Disk Status, Cluster Status, Service Status, Storage Pool Info, Container Info			Nutanix
Nutanix	Nutanix Prism			API Audit, Audit, Security Policy Hitlogs, and Flow Service Logs		Nutanix Prism
Okta.com	SSO	Okta API: Users		Okta API: Over 90 event types covering user activity in Okta website		Okta Configuration
One Identity	Safeguard		Not supported			One Identity Safeguard
OpenLDAP	OpenLDAP	LDAP: Users				
Oracle	Cloud Access Security Broker (CASB)					Oracle Cloud Access Security Broker
Oracle	Cloud Infrastructure					Oracle Cloud Infrastructure
Oracle	Enterprise Database Server - 10g, 11g, 12c,	SNMP or WMI: Process resource	JDBC: Database performance metrics: Buffer cache hit ratio,	Syslog: Listener log, Alert log, Audit Log		Oracle Database

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	18/19c, 21c	usage ;	Row cache hit ratio, Library cache hit ratio, Shared pool free ratio, Wait time ratio, Memory Sorts ratio etc ; JDBC: Database Table space information: table space name, table space type, table space usage, table space free space, table space next extent etc; JDBC: Database audit trail: Database logon, Database operations including CREATE/ALTER/DROP/TRUNCATE operations on tables, table spaces, databases, clusters, users, roles, views, table indices, triggers etc.			
Oracle	MySQL Server	SNMP or WMI: Process resource usage	JDBC: User Connections, Table Updates, table Selects, Table Inserts, Table Deletes, Temp Table Creates, Slow Queries etc; JDBC: Table space performance metrics: Table space name, table space type, Character set and Collation, table space usage, table space free space etc; JDBC: Database audit trail: Database log on, Database/Table CREATE/DELETE/MODIFY operations			MySQL Server
Oracle	WebLogic Application Server	SNMP or WMI: Process resource usage	JMX: Availability metrics, Memory metrics, Servlet metrics, Database metrics, Thread pool metrics, EJB metrics, Application level metrics			Oracle WebLogic
Oracle	Glassfish Application Server	SNMP or WMI: Process resource usage	JMX: Availability metrics, Memory metrics, Servlet metrics, Session metrics, Database metrics, Request			Oracle GlassFish Server

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
			processor metrics, Thread pool metrics, EJB metrics, Application level metrics, Connection metrics			
Oracle	Sun SunOS and Solaris	SNMP: OS, Hardware, Software, Processes, Open Ports ; SSH: Hardware details	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification		Sun Solaris Server
OTORIO	RAM2 (Risk Assessment, Monitoring and Management)					OTORIO RAM2 (Risk Assessment, Monitoring and Management)
PacketFence	Network Access Control	Host name and Device type	Not supported		Not supported	PacketFence Network Access Control
Palo Alto Networks	Palo Alto Cortex XDR					Palo Alto Cortex XDR
Palo Alto Networks	Palo Alto Traps Endpoint Security Manager	LOG Discovery	Currently not natively supported	Over 80 event types	Currently not natively supported	Palo Alto Traps Endpoint Security Manager
Palo Alto Networks	PAN-OS based Firewall	SNMP: Host name, OS, Hardware, Network interfaces; SSH: Configuration	SNMP: Uptime, CPU utilization, Network Interface metrics, Firewall connection count	Syslog: Traffic log, Threat log (URL, Virus, Spyware, Vulnerability, File, Scan, Flood and data subtypes), config and system logs, wildfire logs	SSH: Configuration Change	Palo Alto Firewall
Proofpoint	Proofpoint					Proofpoint
PulseSecure	PulseSecure VPN			Syslog: VPN events, Traffic events, Admin events		PulseSecure
QNAP	Turbo NAS					QNAP Turbo NAS
Qualys	QualysGuard					Qualys

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	Scanner					QualysGuard Scanner
Qualys	Vulnerability Scanner			Qualys API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence etc		Qualys Vulnerability Scanner
Qualys	Web Application Firewall			syslog (JSON formatted): web log analysis		Qualys Web Application Firewall
Radware	DefensePro	LOG Discovery	Currently not natively supported	Over 120 event types	Currently not natively supported	Radware DefensePro
Rapid7	InsightVM (Platform Based Vulnerability Management)	Host name and Device type	Not supported			Rapid7 InsightVM (Vulnerability Management On-Premises)
Rapid7	NeXpose Vulnerability Scanner (Vulnerability Management On-Premises)			Rapid7 NeXpose API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence etc		Rapid7 NeXpose Vulnerability Scanner (Platform Based Vulnerability Management)
Red Hat	Linux	SNMP: OS, Hardware, Software, Processes, Open Ports ;	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons,	SSH: File integrity monitoring, Target file monitoring	Linux Server

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		SSH: Hardware details, Linux distribution		User/Group Modification SSH: File integrity monitoring, Command output monitoring, Target file monitoring Agent: File integrity monitoring	Agent: File integrity monitoring	
Red Hat	JBoss Application Server	SNMP: Process level CPU/Memory usage	JMX: CPU metrics, Memory metrics, Servlet metrics, Database pool metrics, Thread pool metrics, Application level metrics, EJB metrics	;		Red Hat JBoss
Red Hat	DHCP Server	SNMP: Process level CPU/Memory usage		Syslog: DHCP address release/renew events		Linux DHCP
Riverbed	Steelhead WAN Accelerators	SNMP: Host name, Software version, Hardware model, Network interfaces	SNMP: Uptime, CPU / Memory / Network Interface / Disk space metrics, Process cpu/memory utilization; SNMP: Hardware Status SNMP: Bandwidth metrics: (Inbound/Outbound Optimized Bytes - LAN side, WAN side; Connection metrics: Optimized/Pass through / Half-open optimized connections etc); SNMP: Top Usage metrics: Top source, Top destination, Top Application, Top Talker; SNMP: Peer status: For every peer: State, Connection failures, Request timeouts, Max latency	SNMP Trap: About 115 event types covering software errors, hardware errors, admin login, performance issues - cpu, memory, peer latency issues ; Netflow: Connection statistics		Riverbed SteelHead WAN Accelerator
Ruckus	Wireless LAN	SNMP: Controller host name, Controller hardware model, Controller	SNMP: Controller Uptime, Controller Network Interface metrics, Controller WLAN Statistics, Access Point Statistics, SSID performance Stats			Ruckus WLAN

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		network interfaces, Associated WLAN Access Points				
SAP	SAP Enterprise Threat Detection (ETD)					SAP Enterprise Threat Detection (ETD)
SAP	SAP Enterprise Threat Detection Cloud					SAP Enterprise Threat Detection Cloud
Security Onion	Zeek (Bro)	Discovered via LOG only	Not natively supported - Custom monitoring needed	Syslog JSON format: 6 event types parsed	Currently not natively supported	Zeek (Bro) Installed on Security Onion
SentinelOne	SentinelOne Singularity	Discovered via LOG only	Not natively supported. Custom monitoring needed.	System and security events (e.g. file blocked)	Currently not natively supported	SentinelOne Singularity
Siemens	Simatic PLC					Siemens Simatic PLC
Snort	IPS	SNMP: Process level CPU/Memory usage		Syslog: Over 40K IPS Alerts DBC: Over 40K IPS Alerts - additional details including TCP/UDP/ICMP header and payload in the attack packet		Snort IPS
SolarWinds	Orion	SNMP				SolarWinds Orion
Sophos	Central	Host name and Device type	Not supported		Not supported	Sophos Central
Sophos	Sophos Endpoint Security and Control			SNMP Trap: Endpoint events including Malware found/deleted, DLP events		Sophos Endpoint Security and Control
Squid	Web Proxy	SNMP: Process level CPU/Memory usage		Syslog: W3C formatted access logs - per HTTP (S) connection: Sent Bytes, Received Bytes, Connection Duration		Squid Web Proxy

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
SSH Com Security	CryptoAuditor	LOG Discovery	Currently not natively supported	Many event types	Currently not natively supported	SSH Com Security CryptoAuditor
Stormshield	Network Security	Not natively supported	Not natively supported	Firewall logs	Not natively supported	Stormshield Network Security
Symantec	Symantec Endpoint Protection			Syslog: Over 5000 event types covering end point protection events - malware/spyware/adware, malicious events		Symantec Endpoint Protection
Tanium	Connect	Host name and Device type	Not supported		Not supported	Tanium Connect
Tenable	Tenable.io	Host name and Device type	Not supported		Not supported	Tenable.io
Thales	Vormetric Data Security Manager	LOG Discovery	Currently not natively supported	1 broad event Type	Currently not natively supported	Vormetric Data Security Manager
Tigera	Calico	Not natively supported	Not natively supported	Flow, Audit and DNS logs	Not natively supported	Tigera Calico
Trellix	Sidewinder Firewall	SNMP: OS, Hardware, Installed Software, Running Processes	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start	Syslog: Firewall logs		McAfee Firewall Enterprise (Sidewinder)
Trellix	McAfee Vulnerability Manager			JDBC: Vulnerability data		McAfee Vulnerability Manager (Formerly McAfee Foundstone Vulnerability Scanner)r
Trend Micro	Deep Discovery	Discovered via LOG only	Not natively supportedCustom monitoring needed.	Malicious file detection	Currently not natively supported	TrendMicro Deep Discovery
Trend Micro	Deep Security Manager			Syslog: Over 10 event types covering end	Not supported	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				point protection events		
Trend Micro	Interscan Web Filter	LOG Discovery	Currently not natively supported	15 event Types	Currently not natively supported	TrendMicro Interscan Web Filter
Trend Micro	Intrusion Defense Firewall (IDF)			Syslog: Over 10 event types covering end point firewall events		Trend Micro IDF
Trend Micro	Office scan			SNMP Trap: Over 30 event types covering end point protection events - malware/spyware/adware, malicious events		Trend Micro OfficeScan
Trend Micro	Trend Vision One					Trend Vision One
Ubiquiti	Wireless LAN Controller					Ubiquiti Wireless LAN
UserGate	UTM Firewall					UserGate UTM Firewall
Vasco	DigiPass			Syslog - Successful and Failed Authentications, Successful and Failed administrative logons		Vasco DigiPass
VMware	VMware ESX and VCenter	VMWare SDK: Entire VMWare hierarchy and dependencies - Data Center, Resource Pool, Cluster, ESX and VMs	VMWare SDK: VM level: CPU, Memory, Disk, Network, VMware tool status VMWare SDK: ESX level: CPU, Memory, Disk, Network, Data store VMWare SDK: ESX level: Hardware Status VMWare SDK: Cluster level: CPU, Memory, Data store, Cluster Status VMWare SDK: Resource pool level: CPU, Memory	VMWare SDK: Over 800 VCenter events covering account creation, VM creation, DRS events, hardware/software errors		
VMware	NSX for vSphere					VMware NSX for vSphere
VMware	vShield			Syslog: Over 10 events covering permitted and denied connections, detected attacks		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
VMware	VCloud Network and Security (vCNS) Manager			Syslog: Over 10 events covering various activities		
WALLIX	Bastion					WALLIX Bastion
WatchGuard	Firebox Firewall			Syslog: Over 20 firewall event types		WatchGuard Firebox Firewall
Websense	Web Filter			Syslog: Over 50 web filtering events and web traffic logs		Websense Web Filter
Workday	Workday Enterprise Suite					Workday Enterprise Suite (Workday Report API via Generic HTTPS Poller)
YXLink	Vulnerability Scanner					YX Link Vulnerability Scanner
Zeek	Network Security Monitor (Previously known as Bro)					Zeek Network Security Monitor (Previously known as Bro)
Zscaler	Zscaler Internet Access (ZIA)					Zscaler Internet Access (ZIA)
Zscaler	Zscaler Private Access (ZPA)					Zscaler Private Access (ZPA)

Applications

This section describes how to configure applications for discovery and for providing information to FortiSIEM.

- [Application Server](#)
- [Authentication Server](#)
- [Database Server](#)
- [DHCP and DNS Server](#)
- [Directory Server](#)
- [Document Management Server](#)
- [Healthcare IT](#)
- [Mail Server](#)
- [Management Server/Appliance](#)
- [Remote Desktop](#)
- [Source Code Control](#)
- [Unified Communication Server](#)
- [Web Server](#)

Application Server

FortiSIEM supports the discovery and monitoring of these application servers.

- [Apache Tomcat](#)
- [IBM WebSphere](#)
- [Microsoft ASP.NET](#)
- [Oracle GlassFish Server](#)
- [Oracle WebLogic](#)
- [Red Hat JBoss](#)

Apache Tomcat

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Event for Tomcat Metrics

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		Generic information: Application version, Application port Availability metrics: Uptime, Application Server State CPU metrics: CPU utilization Memory metrics: Total memory, Free memory, Memory utilization, Virtual committed memory, Total Swap Memory, Free Swap Memory, Swap memory utilization, Heap Utilization, Heap Used Memory, Heap max memory, Heap commit memory, Non-heap Utilization, Non-heap used memory, Non-heap max memory, Non-heap commit memory Servlet metrics: Web application name, Servlet Name, Count allocated, Total requests, Request errors, Load time, Avg Request Processing time Session metrics: Web context path, Peak active sessions, Current active sessions, Duplicate sessions, Expired sessions, Rejected sessions, Average session lifetime, Peak session lifetime, Session processing time, Session create rate, Session expire rate, Process expire frequency, Max session limited, Max inactive Interval	Performance Monitoring
JMX		Database metrics: Web context path, Data source, Database driver, Peak active sessions, Current active sessions, Peak idle sessions, Current idle sessions Thread pool metrics: Thread pool name, Application port, Total threads, Busy threads, Keep alive threads, Max threads, Thread priority, Thread pool daemon flag Request processor metrics: Request processor name, Received Bytes, Sent Bytes, Average Request Process time, Max Request Processing time, Request Rate, Request Errors	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "tomcat" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "tomcat" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

FortiSIEM uses SNMP to discover and classify the target device as a valid asset in the CMDB. Without SNMP-based discovery, JMX monitoring jobs cannot be mapped or applied to the asset. Please configure SNMP on the device first, then modify the appropriate JMX parameters.

JMX

Add the necessary parameters to the Tomcat startup script.

- [Windows](#)
- [Linux](#)

Windows

Modify the file `${CATALINA_BASE}\bin\catalina.bat` by adding these arguments for JVM before the comment:

```
rem ----Execute The Requested Command -----
```

JMX Configuration for Windows

```
set JAVA_OPTS=-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=${Your  
JMX Port} \ -Dcom.sun.management.jmxremote.authenticate=true \ -  
Dcom.sun.management.jmxremote.ssl=false \ -  
Dcom.sun.management.jmxremote.access.file=jmxremote.access \ -  
Dcom.sun.management.jmxremote.password.file=jmxremote.password \
```

Linux

Modify the file `${CATALINA_BASE}/bin/catalina.sh` by adding these arguments for JVM before the comment:

```
# ----Execute The Requested Command -----
```

JMX Configuration for Linux

```
JAVA_OPTS=" $ JAVA_OPTS -Dcom.sun.management.jmxremote \ -  
Dcom.sun.management.jmxremote.port=${ Your JMX Port} \ -  
Dcom.sun.management.jmxremote.authenticate=true \ -Dcom.sun.management.jmxremote.ssl=false  
\ -Dcom.sun.management.jmxremote.access.file=jmxremote.access \ -  
Dcom.sun.management.jmxremote.password.file=jmxremote.password" \
```

1. Edit the access authorization file `jmxremote.access`.

```
monitorRole  readonly
controlRole  readwrite
```

2. Edit the password file `jmxremote.password`.
The first column is user name and the second column is password). FortiSIEM only needs monitor access.

```
monitorRole  <FortiSIEMUserName>controlRole  <userName>
```

3. In Linux, set permissions for the `jmxremote.access` and `jmxremote.password` files so that they are read-only and accessible only by the Tomcat operating system user.

```
chmod 600 jmxremote.access
chmod 600 jmxremote.password
```

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Apache Tomcat application server over JMX:

Setting	Value
Name	Enter a name for the credential.
Device Type	Apache Apache Tomcat
Access Protocol	JMX
Pull Interval (minutes)	5
Port	0
User Name	The user you created in step 3
Password	The password you created in step 3

Sample Event for Tomcat Metrics

```
<134>Jan 22 01:57:32 10.1.2.16 java: [PH_DEV_MON_TOMCAT_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[appServerState]=STARTED,[sysUpTime]=2458304,[cpuUtil]=0
```

```
<134>Jan 22 01:57:32 10.1.2.16 java: [PH_DEV_MON_TOMCAT_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[appServerState]=STARTED,[freeMemKB]=116504,
[freeSwapMemKB]=2974020,[memTotalMB]=4095,[swapMemTotalMB]=8189,[virtMemCommitKB]=169900,
[memUtil]=98,[swapMemUtil]=65,[heapUsedKB]=18099,[heapMaxKB]=932096,[heapCommitKB]=48896,
```

```
[heapUtil]=37,[nonHeapUsedKB]=22320,[nonHeapMaxKB]=133120,[nonHeapCommitKB]=24512,[nonHeapUtil]=91

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[webAppName]=//localhost/host-manager,
[servletName]=HTMLHostManager,[countAllocated]=0,[totalRequests]=0,[reqErrors]=0,[loadTime]=0,
[reqProcessTimeAvg]=0,[maxInstances]=20,[servletState]=STARTED

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_SESSION]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[webContextPath]=/host-manager,[activeSessionsPeak]=0,
[activeSessions]=0,[duplicateSession]=0,[expiredSession]=0,[rejectedSession]=0,
[sessionLifetimeAvg]=0,[sessionLifetimePeak]=0,[sessionProcessTimeMs]=0,[sessionCreateRate]=0,
[sessionExpireRate]=0,[webAppState]=STARTED,[processExpiresFrequency]=6,[maxSessionLimited]=-1,
[maxInactiveInterval]=1800

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_DB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[webContextPath]=/host-manager,[dataSource]="jdbc/postgres1",
[dbDriver]=org.postgresql.Driver,[activeSessionsPeak]=20,[activeSessions]=0,[idleSessionsPeak]=10,
[idleSessions]=0

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_THREAD_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[threadPoolName]=ajp-apr-18009,[appPort]=18009,[totalThreads]=0,
[busyThreads]=0,[keepAliveThreads]=0,[maxThreads]=200,[threadPriority]=5,[threadPoolIsDaemon]=true

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[reqProcessorName]="http-apr-18080",[recvBytes]=0,
[sentBytes]=62748914,[totalRequests]=4481,[reqProcessTimeAvg]=44107,[reqProcessTimeMax]=516,
[reqRate]=0,[reqErrors]=7
```


IBM WebSphere

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

HTTPS Preferred for Monitoring over JMX IBM WebSphere performance metrics can be obtained via HTTP(S) or JMX. The HTTP(S) based method is highly recommended since it consumes significantly less resources on FortiSIEM.

Protocol	Information discovered	Metrics collected	Used for
HTTP / HTTP(S)		Generic information: Application version, Application port Availability metrics: Uptime, Application Server State CPU metrics: Application server instance, CPU utilization Memory metrics: Heap utilization, Heap used memory, Heap free memory, Heap max memory, Heap commit memory Servlet metrics: Application name, Web application name, Servlet Name, Invocation count Database pool metrics: Application server instance, JDBC provider, Data source, Pool size, Closed connections, Active Connections, Requests wait for connections, Connection use time, Connection factory type, Peak connections Thread pool metrics: Application server instance, Thread pool name, Execute threads, Peak execute threads Transaction metrics: Application server instance, Active Transaction, Committed Transaction, Rolled back Transaction Authentication metrics: Application name, Application server instance, Authentication Method, Count	Performance Monitoring
JMX		Generic information: Application version, Application port Availability metrics: Uptime, Application Server State CPU metrics: Application server instance, CPU utilization Memory metrics: Heap utilization, Heap used memory, Heap free memory, Heap max memory, Heap commit memory, Max System dumps on disk, Max heap dumps on disk	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Servlet metrics: Application name, Web application name, Servlet Name, Invocation count, Request errors Database pool metrics: Application server instance, JDBC provider, Data source, Pool size, Closed connections, Active Connections, Requests wait for connections, Connection use time, Connection factory type, Peak connections Thread pool metrics: Application server instance, Thread pool name, Execute threads, Peak execute threads Application level metrics: Application name, Web application name, Application server instance, Web application context root, Active sessions, Peak active sessions EJB metrics: Application name, Application server instance, EJB component name	
Syslog			Log analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "websphere" to see the event types associated with this device.

- PH_DEV_MON_WEBSPHERE_CPU (from HTTPS)

```
<134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,[destDevPort]=9443,
[appVersion]=8.5.5.3,[appServerInstance]=server1,[cpuUtil]=0,[sysUpTime]=2340206,
[appServerState]=RUNNING
```

- PH_DEV_MON_WEBSPHERE_CPU (from JMX)

```
<134>Jan 22 02:15:23 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=8880,
[appVersion]=IBM WebSphere Application Server 7.0.0.11,[appServerInstance]=server1,
[cpuUtil]=0,[sysUpTime]=42206,[appServerState]=STARTED
```

- PH_DEV_MON_WEBSPHERE_MEMORY (from HTTPS)

```
<134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,[destDevPort]=9443,
[appVersion]=8.5.5.3,[appServerInstance]=server1,[appServerState]=running,[heapFreeKB]=93208,
[heapUsedKB]=168936,[heapCommitKB]=232576,[heapMaxKB]=262144,[heapUtil]=72
```

- PH_DEV_MON_WEBSPHERE_MEMORY (from JMX)

```
<134>Jan 22 02:15:25 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=8880,
[appVersion]=IBM WebSphere Application Server 7.0.0.11,[appServerInstance]=server1,
[appServerState]=STARTED,[maxSystemDumpsOnDisk]=10,[maxHeapDumpsOnDisk]=10,[heapFreeKB]=48140,
[heapUsedKB]=172018,[heapCommitKB]=217815,[heapMaxKB]=262144,[heapUtil]=78
```

- PH_DEV_MON_WEBSPHERE_APP (from HTTPS)

```
<134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,[destDevPort]=9443,
[appVersion]=8.5.5.3,[appServerInstance]=server1,[appName]=isclite,
[webAppName]=ISCAAdminPortlet.war,[activeSessions]=0,[activeSessionsPeak]=1
```

- PH_DEV_MON_WEBSPHERE_APP (from JMX)

```
<134>Jan 22 02:18:24 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=8880,
[appVersion]=IBM WebSphere Application Server 7.0.0.11,[appServerInstance]=server1,
[appName]=isclite,[webAppName]=isclite.war,[webContextRoot]=admin_host/ibm/console,
[activeSessions]=0,[activeSessionsPeak]=1
```

- PH_DEV_MON_WEBSPHERE_SERVLET (from HTTPS)

```
<134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,[destDevPort]=9443,
[appVersion]=8.5.5.3,[appServerInstance]=server1,[appName]=isclite,[webAppName]=isclite.war,
[servletName]=/com.ibm.ws.console.servermanagement/collectionTableLayout.jsp,
[invocationCount]=2
```

- PH_DEV_MON_WEBSPHERE_SERVLET (from JMX)

```
<134>Jan 22 02:15:24 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=8880,
[appVersion]=IBM WebSphere Application Server 7.0.0.11,[appServerInstance]=server1,
[appName]=isclite,[webAppName]=isclite.war,[servletName]=action,[reqErrors]=0,
[invocationCount]=14
```

- PH_DEV_MON_WEBSPHERE_DB_POOL (from HTTPS)

```
<134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_DB_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,[destDevPort]=9443,
[appVersion]=8.5.5.3,[appServerInstance]=server1,[jdbcProvider]=Derby JDBC Provider (XA),
[dataSource]=jdbc/DefaultEJBTimerDataSource,[poolSize]=0,[closedConns]=0,[activeConns]=0,
[waitForConnReqs]=0,[connUseTime]=0
```

- PH_DEV_MON_WEBSPHERE_DB_POOL (from JMX)

```
<134>Jan 22 02:15:23 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_DB_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=8880,
[appVersion]=IBM WebSphere Application Server 7.0.0.11,[appServerInstance]=server1,
```

```
[jdbcProvider]=Derby JDBC Provider (XA),[dataSource]=DefaultEJBTimerDataSource,[poolSize]=0,
[closedConns]=0,[activeConns]=0,[waitForConnReqs]=0,[connUseTime]=0,[connFactoryType]=,
[peakConns]=0
```

- PH_DEV_MON_WEBSPHERE_THREAD_POOL (from HTTPS)

```
<134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_THREAD_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,
[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,
[threadPoolName]=WebContainer,[executeThreads]=2,[executeThreadPeak]=6
```

- PH_DEV_MON_WEBSPHERE_THREAD_POOL (from JMX)

```
<134>Jan 22 02:18:25 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_THREAD_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
[destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
[appServerInstance]=server1,[threadPoolName]=ORB.thread.pool,[executeThreads]=0,
[executeThreadPeak]=0
```

- PH_DEV_MON_WEBSPHERE_TRANSACTION (from HTTPS)

```
<134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_TRANSACTION]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,
[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,[activeTxCount]=0,
[committedTxCount]=3406,[rolledBackTxCount]=0
```

- PH_DEV_MON_WEBSPHERE_AUTHENTICATION (from HTTPS)

```
<134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_AUTHENTICATION]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-
10.1.2.16,[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,
[authenMethod]=TokenAuthentication,[count]=0
```

- PH_DEV_MON_WEBSPHERE_EJB (from JMX)

```
<134>Jan 22 02:15:24 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_EJB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=8880,
[appVersion]=IBM WebSphere Application Server 7.0.0.11,[appServerInstance]=server1,
[appName]=SchedulerCalendars,[ejbComponentName]=Calendars.jar
```

Reports

In **RESOURCES > Reports**, search for "websphere" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- HTTP(S)
 - Install the perfServletApp Application
 - Configure Security for the Application
 - Start the Application
- JMX
 - Configuring the Default JMX Port

HTTP(S)

Install the perfServletApp Application

1. Log in to your Websphere administration console.
2. Go to **Applications > Application Types > WebSphere enterprise application**.
3. Click **Install**.
4. Select **Remote file system** and browse to {WebSphere_Home}/AppServer/installableApps/PerfServletApp.ear.
5. Click **Next**.
The **Context Root** for the application will be set to /wasPerfTool, but you can edit this during installation.

Configure Security for the Application

1. Go to **Security > Global Security**.
2. Select **Enable application security**.
3. Go to **Applications > Application Types > Websphere Enterprise Applications**.
4. Select **perfServletApp**.
5. Click **Security role to user/group mapping**.
6. Click **Map Users/Groups**.
7. Use the Search feature to find and select the FortiSIEM user you want to provide with access to the application,
8. Click **Map Special Subjects**.
9. Select **All Authenticated in Application's Realm**.
10. Click **OK**.

Start the Application

1. Go to **Applications > Application Types > WebSphere enterprise application**.
2. Select **perfServletApp**.
3. Click **Start**.
4. In a web browser, launch the application by going to `http://<ip>:<port>/wasPerfTool/servlet/perfservlet`. Default HTTP Port The default port for HTTP

is 9080, HTTPS is 9443. You can change these by going to **Servers > Server Types > WebSphere application servers > {serverInstance} > Configuration > Ports**.

JMX

Configuring the Default JMX Port

By default, your Websphere application server uses port 8880 for JMX. You can change this by logging in to your application server console and going to **Application servers > {Server Name} > Ports > SOAP_CONNECTOR_ADDRESS**. The username and password for JMX are the same as the credentials logging into the console. To configure JMX communications between your Websphere application server and FortiSIEM, you must copy several files from your application server to the Websphere configuration directory for each FortiSIEM virtual appliance that will be used for discovery and performance monitoring jobs. FortiSIEM does not include these files because of licensing restrictions.

1. Copy these files to the directory `/opt/phoenix/config/websphere/` for each Supervisor, Worker, and Collector in your FortiSIEM deployment.

File Type	Location
Client Jars	• <code>\${WebSphere_Home}/AppServer/runtimes/com.ibm.ws.admin.client.jar</code> • <code>\${WebSphere_Home}/AppServer/plugins/com.ibm.ws.security.crypto.jar</code>
SSL files	• <code>\${WebSphere_Home}/AppServer/profiles/\${Profile_Name}/etc/DummyClientKeyFile.jks</code> • <code>\${WebSphere_Home}/AppServer/profiles/\${Profile_Name}/etc/DummyClientTrustFile.jks</code>

2. Install IBM JDK 1.6 or higher in the location `/opt/phoenix/config/websphere/java` for each Supervisor, Worker, and Collector in your FortiSIEM deployment.

You can now configure FortiSIEM to communicate with your device by following the instructions in the *User Guide > Section: Setting Credentials*, and then initiate discovery of the device as described in the topics under *Discovery Settings*.

Settings for Access Credentials

Use these **Access Method Definition** options to let FortiSIEM access your IBM Websphere device over HTTPS and SNMP. When you set the **Device Credential Mapping Definition**, make sure to map both the HTTPS and SNMP credentials to the same IP address for your Websphere device.

- [Settings for IBM Websphere HTTPS Access Credentials](#)
- [Settings for IBM Websphere SNMP Access Credentials](#)
- [SNMP Access Credentials for All Devices](#)
- [Settings for IBM Websphere JMX Access Credentials](#)

Settings for IBM Websphere HTTPS Access Credentials

Setting	Value
Name	websphere_https
Device Type	IBM Websphere App Server
Access Protocol	HTTPS
Port	9443
URL	/wasPerfTools/servlet/perfservlet
User Name	Use the user name that you provided with access to the application
Password	The password associated with the user that has access to the application

Settings for IBM Websphere SNMP Access Credentials

Use these **Access Method Definition** settings to let FortiSIEM access your IBM Websphere device over SNMP. When you set the **Device Credential Mapping Definition**, make sure to map both the HTTPS and SNMP credentials to the same IP address for your Websphere device.

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Settings for IBM Websphere JMX Access Credentials

Use these **Access Method Definition** settings to let FortiSIEM access your IBM Websphere device over JMX.

Setting	Value
Name	websphere
Device Type	IBM Websphere App Server
Access Protocol	JMX

Setting	Value
Pull Interval (minutes)	5
Port	8880
User Name	The administrative user for the application server
Password	The password associated with the administrative user

Microsoft ASP.NET

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Sample Event for ASP.NET Metrics

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
WMI		Request Execution Time, Request Wait Time, Current Requests, Disconnected Requests, Queued requests, Disconnected Requests	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "asp.net" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "asp.net" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

Sample Event for ASP.NET Metrics

```
[PH_DEV_MON_APP_ASPNET_MET]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=4868,
[hostName]=QA-EXCHG,[hostIpAddr]=172.16.10.28,
[appGroupName]=Microsoft ASPNET,[aspReqExecTimeMs]=0,[aspReqCurrent]=0,[aspReqDisconnected]=0,
[aspReqQueued]=0,[aspReqRejected]=0,[aspReqWaitTimeMs]=0
```

Oracle GlassFish Server

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Event for Glassfish Metrics](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		Generic information: Application version, Application port Availability metrics: Uptime, Application Server State CPU metrics: CPU utilization Memory metrics: Total memory, Free memory, Memory utilization, Virtual committed memory, Total Swap Memory, Free Swap Memory, Swap memory utilization, Heap Utilization, Heap Used Memory, Heap max memory, Heap commit memory, Non-heap Utilization, Non-heap used memory, Non-heap max memory, Non-heap commit memory Servlet metrics: Web application name, Servlet Name, Count allocated, Total requests, Request errors, Avg Request Processing time	Performance Monitoring
JMX		Session metrics: Web context path, Peak active sessions, Current active sessions, Duplicate sessions, Expired sessions, Rejected sessions, Average session lifetime, Peak session lifetime, Session processing time, Session create rate, Session expire rate, Process expire frequency, Max session limited, Max inactive Interval Database metrics: Data source Thread pool metrics: Current live threads, Max live threads Request processor metrics: Request processor name, Received Bytes, Sent Bytes, Total requests, Average Request Process time, Max Request Processing time, Request Rate, Request Errors, Max open connections, Current open connections, Last Request URI, Last Request method, Last Request completion time	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Application level metrics: Cache TTL, Max cache size, Average request processing time, App server start time, Cookies allowed flag, Caching allowed flag, Linking allowed flag, Cross Context Allowed flag EJB metrics: EJB component name, EJB state, EJB start time Connection metrics: Request processor name, HTTP status code, HTTP total accesses	

Event Types

In **ADMIN > Device Support > Event Types**, search for "glassfish" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "glassfish" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

JMX

1. The default JMX port used by Oracle GlassFish is 8686. If you want to change it, modify the node `jmx-connector` of the file `${GlassFish_Home}\domains\${Domain_Name}\config\domain.xml`.
2. The username and password for JMX are the same as the web console.

You can now configure FortiSIEM to communicate with your device by following the instructions in "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Oracle GlassFish JMX Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Oracle GlassFish device over JMX.

Setting	Value
Name	glassfish
Device Type	SUN Glassfish App Server

Setting	Value
Access Protocol	JMX
Pull Interval (minutes)	5
Port	8686
User Name	The administrative user for the application server
Password	The password associated with the administrative user

Sample Event for Glassfish Metrics

```
<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,
[appVersion]=Sun Java System Application Server 9.1_02,[webContextRoot]=,[webAppState]=RUNNING,
[cacheMaxSize]=10240,[cacheTTL]=5000,[reqProcessTimeAvg]=0,[startTime]=1358755971,
[cookiesAllowed]=true,[cachingAllowed]=false,[linkingAllowed]=false,[crossContextAllowed]=true

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,
[appVersion]=Sun Java System Application Server 9.1_02,[sysUpTime]=35266,[cpuUtil]=60

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,
[appVersion]=Sun Java System Application Server 9.1_02,[freeMemKB]=479928,[freeSwapMemKB]=6289280,
[memTotalMB]=16051,[memUtil]=98,[swapMemUtil]=1,[swapMemTotalMB]=6142,[virtMemCommitKB]=4025864,
[heapUsedKB]=1182575,[heapMaxKB]=3106432,[heapCommitKB]=3106432,[heapUtil]=38,
[nonHeapUsedKB]=193676,[nonHeapMaxKB]=311296,[nonHeapCommitKB]=277120,[nonHeapUtil]=69

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_SESSION]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,
[appVersion]=Sun Java System Application Server 9.1_02,[webContextPath]=/_JWSappclients,
[activeSessionsPeak]=0,[duplicateSession]=0,[activeSessions]=0,[expiredSession]=0,
[rejectedSession]=0,[sessionProcessTimeMs]=85,[sessionLifetimeAvg]=0,[sessionLifetimePeak]=0,
[maxSessionLimited]=-1,[maxInactiveInterval]=1800

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,
[appVersion]=Sun Java System Application Server 9.1_02,[webAppName]=phoenix,[webAppState]=RUNNING,
[servletName]=DtExportServlet,[totalRequests]=0,[reqErrors]=0,[reqProcessTimeAvg]=0

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_CONN_STAT]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,
[appVersion]=Sun Java System Application Server 9.1_02,[reqProcessorName]=http8181,
```

```
[httpStatusCode]=304,[httpTotalAccesses]=0
```

```
<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_EJB]:[eventSeverity]=PHL_INFO,  
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,  
[appVersion]=Sun Java System Application Server 9.1_02,[ejbComponentName]=phoenix-domain-1.0.jar,  
[ejbState]=RUNNING,[startTime]=1358755963,
```

```
<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_JMS]:[eventSeverity]=PHL_INFO,  
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,  
[appVersion]=Sun Java System Application Server 9.1_02,[jmsSource]=jms/RequestQueue
```

```
<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR]:  
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-  
10.1.2.201,[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,  
[reqProcessorName]=http4848,[recvBytes]=0,[sentBytes]=0,[totalRequests]=0,[reqRate]=0,  
[reqProcessTimeAvg]=0,[reqProcessTimeMax]=0,[maxOpenConnections]=0,[lastRequestURI]=null,  
[lastRequestMethod]=null,[lastRequestCompletionTime]=0,[openConnectionsCount]=0,[reqErrors]=0
```

```
<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_THREAD_POOL]:[eventSeverity]=PHL_INFO,  
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,  
[appVersion]=Sun Java System Application Server 9.1_02,[liveThreads]=106,[liveThreadsMax]=138
```

```
<134>Jan 22 02:06:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_DB_POOL]:[eventSeverity]=PHL_INFO,  
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,[destDevPort]=8686,  
[appVersion]=Sun Java System Application Server 9.1_02,[dataSource]=jdbc/phoenixDS
```

Oracle WebLogic

Supported Added: FortiSIEM 4.7.2

Last Modification: FortiSIEM 6.7.0

Vendor Version Tested: Oracle WebLogic 12c

Vendor: Oracle

Product Information: <https://www.oracle.com/java/weblogic/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [WebLogic Configuration](#)
- [Create WebLogic Credential in FortiSIEM](#)
- [Sample Event for WebLogic Metrics](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		Generic information: Application version, Application port, SSL listen port, Listen port enabled flag, SSL listen port enabled Availability metrics: Uptime, Application Server State Memory metrics: Total memory, Free memory, Used memory, Memory utilization, Heap utilization, Heap used memory, Heap max memory, Heap commit memory, Total nursery memory Servlet metrics: Application name, App server instance, Web application name, Web context name, Servlet name, Invocation count, Servlet execution time Database pool metrics: Application name, App server instance, Data source, Active connection count, Connection limit, Leaked connections, Reserve requests, Requests wait for connections Thread pool metrics: App server instance, Completed requests, Execute threads, Pending requests, Standby threads, Total threads	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		EJB metrics: EJB component name, EJB state, EJB idle beans, EJB used beans, EJB pooled beans, EJB Waiter threads, EJB committed Transactions, EJB timedout transactions, EJB rolledback transactions, EJB activations, EJB Passivations, EJB cache hits, EJB cache misses, EJB cache accesses, EJB cache hit ratio Application level metrics: Application name, App server instance, Web application name, Web context root, Peak active sessions, Current active sessions, Total active sessions, Servlet count, Single threaded servlet pool count,	

Event Types

In **ADMIN > Device Support > Event Types**, search for "WebLogic" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "WebLogic" in the main content panel **Search...** field to see the reports associated with this application or device.

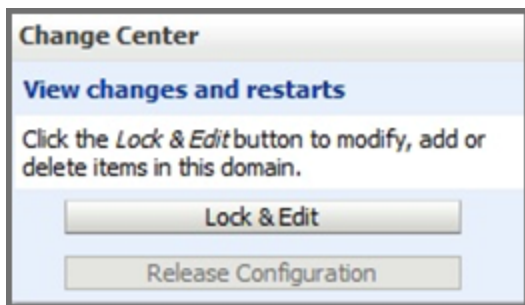
WebLogic Configuration

- [Enable IIOP](#)
- [Create a WebLogic User for FortiSIEM](#)

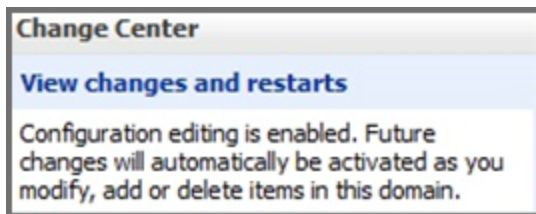
Enable IIOP

To configure Oracle WebLogic for FortiSIEM, take the following steps.

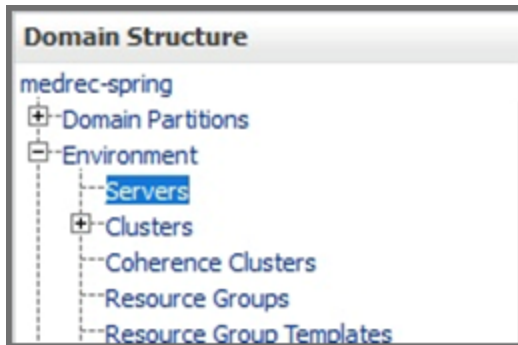
1. Login to the WebLogic 12c administrative console.
2. In the upper left pane labeled **Change Center**, take the following steps.
 - a. If a **Lock & Edit** button appears, click it.



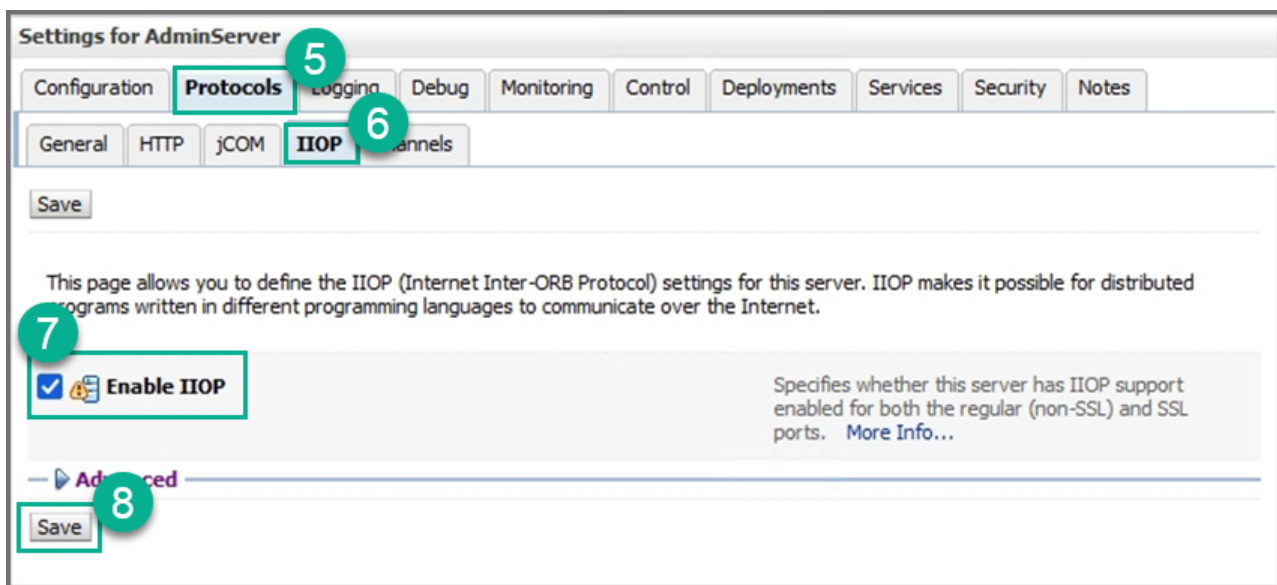
If no **Lock & Edit** button is visible, proceed to the next step.



3. Go to the **Domain Structure** pane, and expand **Environment > Servers**.

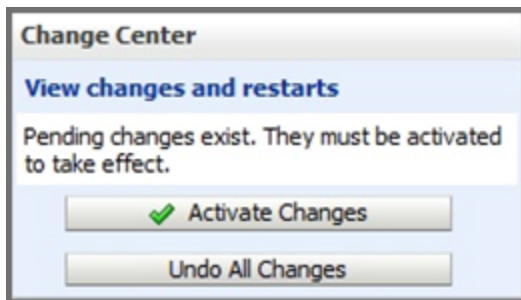


4. On the right pane, click on the server that you want to monitor by clicking its name.
5. Click on the **Protocols** tab.
6. Click the **IIOP** sub-tab.
7. Enable IIOP by clicking on the **Enable IIOP** checkbox.
8. Click **Save**.



9. Push the configuration change by taking one of the following steps.

- a. If **Lock & Edit** was performed in step 2a, under **Change Center**, click **Activate Changes**.



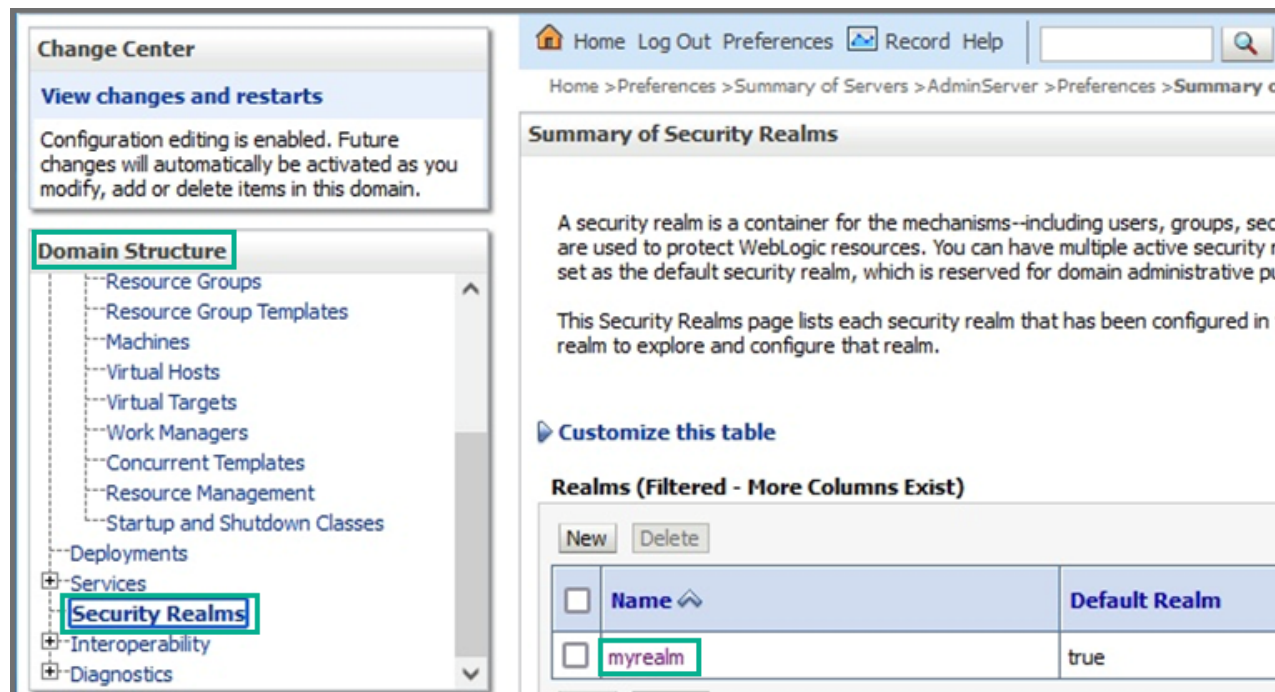
- b. If the **Lock & Edit** button was not present in step 2a, Oracle WebLogic will request a restart for changes to take effect.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the [User Guide](#).

Create a WebLogic User for FortiSIEM

To add an Oracle WebLogic user, take the following steps.

1. Go to the **Domain Structure** pane, and expand **Security Realms**.
2. On the right pane, click on **myrealm**.



3. Select user and groups.
4. Under user, click **New**.
5. Configure the following fields:
 - a. In the **Name** field, enter the user's name.
 - b. From the **Provider** drop-down list, leave it as **DefaultAuthenticator**.

- c. In the **Password** field, enter the user's password.
- d. In the **Confirm Password** field, re-enter the user's password.
- e. Click **OK**.
6. Click on the newly created user.
7. Go to the **Groups** tab.
8. Choose **Operators**, so it appears in the **Chosen** window.
9. Click **Save**.

Settings for adminuser

General Passwords Attributes **Groups**

Save

Use this page to configure group membership for this user.

Parent Groups:

Available:

- ☐ AdminChannelUsers
- ☐ Administrators
- ☐ AppTesters
- ☐ CrossDomainConnectors
- ☐ Deployers
- ☐ Monitors
- ☐ OracleSystemGroup

Chosen:

- ☐ Operators

Save

Create WebLogic Credential in FortiSIEM

Use these **Access Method Definition** settings to allow FortiSIEM to access your Oracle WebLogic application server over JMX.

The port for JMX is the same as the web console, and the default value is 7001.

Setting	Value
Name	weblogic
Device Type	Oracle WebLogic App Server
Access Protocol	JMX

Setting	Value
Pull Interval (minutes)	5
Port	7001
User Name	WebLogic user created in Create a WebLogic User for FortiSIEM .
WebLogic user password created in previous step	WebLogic user password created in Create a WebLogic User for FortiSIEM .

Sample Event for WebLogic Metrics

```
<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_GEN]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3 Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appServerState]=RUNNING,[sysUpTime]=1358476145,[appPort]=7001,
[sslListenPort]=7002,[listenPortEnabled]=true,[sslListenPortEnabled]=true

<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3 Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appServerState]=RUNNING,[heapUsedKB]=153128,
[heapCommitKB]=262144,[heapFreeKB]=109015,[heapUtil]=59,[heapMaxKB]=524288,[usedMemKB]=4086224,
[freeMemKB]=107624,[memTotalMB]=4095,[memUtil]=97,[nurserySizeKB]=88324

<134>Jan 22 02:12:22 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3 Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appName]=consoleapp,[webAppName]=examplesServer_/console,
[servletName]=/framework/skeletons/wlsconsole/placeholder.jsp,[webContextRoot]=/console,
[invocationCount]=1094,[servletExecutionTimeMs]=63

<134>Jan 22 02:15:24 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_DB_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3 Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appName]=examples-demoXA-2,[dataSource]=examples-demoXA-2,
[activeConns]=0,[connLimit]=1,[leakedConns]=0,[reserveRequests]=0,[waitForConnReqs]=0

<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_THREAD_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3 Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[completedRequests]=14066312,[executeThreads]=7,
[pendingRequests]=0,[standbyThreads]=5,[totalThreads]=43

<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_EJB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
```

```
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[ejbComponentName]=ejb30,[ejbIdleBeans]=0,[ejbUsedBeans]=0,
[ejbPooledBeans]=0,[ejbWaiter]=0,[ejbCommitTransactions]=0,[ejbTimedOutTransactions]=0,
[ejbRolledBackTransactions]=0,[ejbActivations]=0,[ejbPassivations]=0,[ejbCacheHits]=0,
[ejbCacheMisses]=0,[ejbCacheAccesses]=0,[ejbCacheHitRatio]=0

<134>Jan 22 02:12:23 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appName]=webservicesJwsSimpleEar,[webAppName]=examplesServer_
/jws_basic_simple,[webContextRoot]=/jws_basic_simple,[activeSessions]=0,[activeSessionsPeak]=0,
[activeSessionTotal]=0,[numServlet]=4,[singleThreadedServletPool]=5
```

Red Hat JBoss

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Event for JBoss Metrics

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		Generic information: Application version, Application port Availability metrics: Uptime, Application Server State CPU metrics: Application server instance, CPU utilization Memory metrics: Heap utilization, Heap used memory, Heap free memory, Heap max memory, Heap commit memory, Max System dumps on disk, Max heap dumps on disk Servlet metrics: Application name, Web application name, Servlet Name, Invocation count, Request errors Database pool metrics: Application server instance, JDBC provider, Data source, Pool size, Closed connections, Active Connections, Requests wait for connections, Connection use time, Connection factory type, Peak connections Thread pool metrics: Application server instance, Thread pool name, Execute threads, Peak execute threads Application level metrics: Application name, Web application name, Application server instance, Web application context root, Active sessions, Peak active sessions EJB metrics: Application name, Application server instance, EJB component name	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "jboss" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "jboss" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- [Configuring JMX on JBoss 7.1 EAP](#)
- [Configuring JMX on the JBoss Application Server](#)
- [Configuring FortiSIEM to Use the JMX Protocol with JBoss Application Server](#)

Configuring JMX on JBoss 7.1 EAP

- [Standalone Server Configuration](#)
- [Managed Domain Host Configuration](#)

Standalone Server Configuration

For the standalone server configuration, take the following steps.

1. Ensure that you have created a management user.

```
${EAP_HOME}/bin/add-user.sh
```

Example:

```
[root@SP136 jboss-eap-7.1]# ./bin/add-user.sh
```

```
What type of user do you wish to add?
  a) Management User (mgmt-users.properties)
  b) Application User (application-users.properties)
(a): a

Enter the details of the new user to add.
Using realm 'ManagementRealm' as discovered from the existing property files.
Username : test2
Password recommendations are listed below. To modify these restrictions edit the add-
user.properties configuration file.
  - The password should be different from the username
  - The password should not be one of the following restricted values {root, admin,
administrator}
  - The password should contain at least 8 characters, 1 alphabetic character(s), 1 digit(s), 1
non-alphanumeric symbol(s)
Password :
WFLYDM0099: Password should have at least 8 characters!
Are you sure you want to use the password entered yes/no? yes
Re-enter Password :
What groups do you want this user to belong to? (Please enter a comma separated list, or leave
blank for none)[ ]:
About to add user 'test2' for realm 'ManagementRealm'
```

```

Is this correct yes/no? yes
Added user 'test2' to file '/svn/projects/jboss-eap-7.1/standalone/configuration/mgmt-
users.properties'
Added user 'test2' to file '/svn/projects/jboss-eap-7.1/domain/configuration/mgmt-
users.properties'
Added user 'test2' with groups to file '/svn/projects/jboss-eap-
7.1/standalone/configuration/mgmt-groups.properties'
Added user 'test2' with groups to file '/svn/projects/jboss-eap-7.1/domain/configuration/mgmt-
groups.properties'
Is this new user going to be used for one AS process to connect to another AS process?
e.g. for a slave host controller connecting to the master or for a Remoting connection for
server to server EJB calls.
yes/no? yes
To represent the user add the following to the server-identities definition <secret
value="dGVzdCoxMQ==" />
[root@SP136 jboss-eap-7.1]#

```

2. The default port is 9990. If you don't want to change the port, skip this step, and proceed to step 3.
``${EAP_HOME}`/standalone/configuration/standalone.xml`
 Look for the "socket-binding-group" attribute. Within that attribute, search for the "management-http" socket binding. Typically, in most systems, JMX is enabled on the "management-http" socket binding only - i.e., JMX listens on the management-http port only. The port used for management-http is set as 9990. This is the port that you should use when configuring the JMX Remote Port parameter.
3. When starting JBoss EAP, bind the management interface to the IP address that you will use to remotely monitor the server by running the following command.
``${EAP_HOME}`/bin/standalone.sh -bmanagement=IP_ADDRESS`
4. Copy ``${JBoss_Home}`/bin/client/jboss-client.jar` to `/opt/phoenix/java/lib/` in the FortiSIEM device which you will connect to JBoss.
5. Use the following command to test in the FortiSIEM device.
`/opt/phoenix/bin/runTestConnJavaAgent.sh jboss IP_ADDRESS 9990 username password test`

Managed Domain Host Configuration

For the managed domain host configuration, take the following steps.

1. Ensure that you have created a management user.
``${EAP_HOME}`/bin/add-user.sh`
2. The default port is 9990. If you don't want to change the port, skip this step, and proceed to step 3.
``${EAP_HOME}`/domain/configuration/host.xml`
 Look for the "management-interfaces" attribute. Within that attribute, search for the "http-interface" socket binding. Typically, The port used for http-interface is set as 9990.
3. Start your JBoss EAP managed domain host.
``${EAP_HOME}`/bin/domain.sh -bmanagement=IP_ADDRESS`
4. Copy ``${JBoss_Home}`/bin/client/jboss-client.jar` to `/opt/phoenix/java/lib/` in the FortiSIEM device which you will connect to JBoss.
5. Use the following command to test in the FortiSIEM device.

```
/opt/phoenix/bin/runTestConnJavaAgent.sh jboss IP_ADDRESS 9990 username password test
```

Configuring JMX on the JBoss Application Server

Changing the Default JMX Port

The default port for JMX is 1090. If you want to change it, modify the file `${JBoss_Home}\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml`.

```
<bean class="org.jboss.services.binding.ServiceBindingMetadata">  <property
name="serviceName">jboss.remoting:service=JMXConnectorServer,protocol=rmi</property>  <property
name="port">1090</property>  <property name="description">RMI/JRMP socket for connecting to the
JMX MBeanServer</property></bean>
```

1. Enable authentication security check. Open the file `${JBoss_Home}\server\default\deploy\jmx-jboss-beans.xml`, find the `JMXConnector` bean, and uncomment the `securityDomain` property.

```
<bean name="JMXConnector" class="org.jboss.system.server.jmx.JMXConnector"><!-- configuration
properties -->
<!-- To enable authentication security checks, uncomment the following --!><!--UNCOMMENT THIS
--><property name="securityDomain">jmx-console</property>
```

2. Modify the file `${JBoss_Home}\server\default\conf\props\jmx-console-roles.properties` to configure the JMX administrator role.

```
admin=JBossAdmin,HttpInvoker
```

3. Modify the file `${JBoss_Home}\server\default\conf\props\jmx-console-users.properties` to configure the username and password for JMX.

```
admin=yourpassword
```

4. Configure DNS resolution for the JBoss application server in your FortiSIEM Supervisor, Workers, and Collectors by adding the IP address and DNS name of the JBoss application server to their `/etc/hosts` files. If DNS is already configured to resolve the JBoss application server name, you can skip this step.
5. Start JBoss.

```
${JBoss_Home}/bin/run.sh -b 0.0.0.0
or
${JBoss_Home}/bin/run.sh -b ${Binding IP}
```

Configuring FortiSIEM to Use the JMX Protocol with JBoss Application Server

To configure JMX communications between your JBoss application server and FortiSIEM, you must copy several files from your application server to the JBoss configuration directory for each FortiSIEM virtual appliance that will be used for discovery and performance monitoring jobs. FortiSIEM does not include these files because of licensing restrictions.

JBoss Version	Files to Copy
4.x, 5.x, 6.x	Copy <code>\${JBoss_Home}/lib/jboss-bootstrap-api.jar</code>

JBoss Version	Files to Copy
	to /opt/phoenix/config/JBoss/
7.0	No copying is necessary.
7.1	Copy \${JBoss_Home}/bin/client/jboss-client.jar to /opt/phoenix/config/JBoss/

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Red Hat JBoss device over JMX:

Setting	Value
Name	jboss
Device Type	Redhat JBOSS App Server
Access Protocol	JMX
Pull Interval (minutes)	5
Port	8880
User Name	The user you created in step 2
Password	The password you created for the user in step 3

Sample Event for JBoss Metrics

```
<134>Feb 06 11:38:35 10.1.2.16 java: [PH_DEV_MON_JBOSS_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[appServerState]=STARTED,[sysUpTime]=6202359,[cpuUtil]=2
```

```
<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[appServerState]=STARTED,[freeMemKB]=264776,
[freeSwapMemKB]=1427864,[memTotalMB]=4095,[memUtil]=94,[swapMemUtil]=83,[swapMemTotalMB]=8189,
[virtMemCommitKB]=1167176,[heapUsedKB]=188629,[heapMaxKB]=466048,[heapCommitKB]=283840,
[heapUtil]=66,[nonHeapUsedKB]=106751,[nonHeapMaxKB]=311296,[nonHeapCommitKB]=107264,
[nonHeapUtil]=99
```

```
<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
```

```
[appVersion]=6.1.0.Final "Neo",[webContextRoot]=//localhost/, [webAppState]=RUNNING,
[cacheMaxSize]=10240,[cacheTTL]=5000,[reqProcessTimeAvg]=10472,[startTime]=1353919592,
[cookiesAllowed]=true,[cachingAllowed]=true,[linkingAllowed]=false,[crossContextAllowed]=true

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[webAppName]=//localhost/admin-console,[servletName]=Faces Servlet,
[totalRequests]=6,[reqErrors]=0,[loadTime]=0,[reqProcessTimeAvg]=10610

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_DB_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[dataSource]=DefaultDS,[dataSourceState]=Started

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_REQUEST_PROCESSOR]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[reqProcessorName]=ajp-0.0.0.0-8009,[recvBytes]=0,[sentBytes]=0,
[reqProcessTimeAvg]=0,[reqProcessTimeMax]=0,[totalRequests]=0,[reqRate]=0,[reqErrors]=0

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_EJB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[ejbComponentName]=ejbjar.jar,[ejbBeanName]=HelloWorldBeanRemote,
[ejbAvailCount]=0,[ejbCreateCount]=0,[ejbCurrCount]=0,[ejbMaxCount]=0,[ejbRemovedCount]=0,
[ejbInstanceCacheCount]=null,[ejbPassivations]=null,[ejbTotalInstanceCount]=null

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_THREAD_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[threadPoolName]=ajp-0.0.0.0-8009,[appPort]=8009,[totalThreads]=0,
[busyThreads]=0,[maxThreads]=2048,[threadPriority]=5,[pollerSize]=32768,[threadPoolIsDaemon]=true
```

Authentication Server

FortiSIEM supports these authentication servers for discovery and monitoring.

- [Cisco Access Control Server \(ACS\)](#)
- [Cisco Duo](#)
- [Cisco Identity Solution Engine \(ISE\)](#)
- [CyberArk Password Vault](#)
- [Fortinet FortiAuthenticator](#)
- [Juniper Networks Steel-Belted RADIUS](#)
- [Microsoft Internet Authentication Server \(IAS\)](#)
- [Microsoft Network Policy Server \(RAS VPN\)](#)
- [One Identity Safeguard](#)
- [Vasco DigiPass](#)

Cisco Access Control Server (ACS)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O	Performance Monitoring
Syslog	Application type	Successful and Failed Authentications, Successful and Failed administrative logons, RADIUS accounting logs	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco secure acs" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [WMI](#)
- [Syslog](#)

SNMP

1. Log into the device you want to enable SNMP for as an administrator.
2. Go to **Control Panel > Program and Features**.
3. Click **Turn Windows features on or off**.
4. If you are installing on a Windows 7 device, select **Simple Network Management Protocol (SNMP)**. If you are installing on a Windows 2008 device, in the **Server Manager** window, go to **Features > Add features > SNMP Services**.
5. If necessary, select SNMP to enable the service.

6. Go to **Programs > Administrative Tools > Services**.
7. to set the SNMP community string and include FortiSIEM in the list of hosts that can access this server via SNMP.
8. Select **SNMP Service** and right-click **Properties**.
9. Set the community string to **public**.
10. Go to the **Security** tab and enter the FortiSIEM IP Address.
11. Restart the SNMP service.

WMI

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- [Creating a Generic User Who Does Not Belong to the Local Administrator Group](#)
- [Creating a User Who Belongs to the Domain Administrator Group](#)

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add**.
6. Find the user you created, and then click **OK**.
This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **EditDefault**.

7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Enable remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.

8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch, Remote Launch, Local Activation, and Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch, Remote Launch, Local Activation, and Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2**.
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced**.
8. Select the user you created for the monitoring account, and then click **Edit**.
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add  
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and then click **OK**.

Syslog

1. Log in to your Cisco Access Controls Server as an administrator.
2. Go to **Start > All Programs > CiscoSecure ACS v4.1 > ACS Admin**.
3. In the left-hand navigation, click System Configuration, then click **Logging**.
4. Select **Syslog** for **Failed Attempts**, **Passed Authentication**, and **RADIUS Accounting** to send these reports to FortiSIEM.
5. For each of these reports, click **Configure** under **CSV**, and select the following attributes to include in the CSV output.

Report	CSV Attributes
Failed Attempts	• Message-Type • User-Name • NAS-IP-Address • Authen-Failure-Code • Author-Failure-Code • Caller-ID • NAS-Port • Author-Date • Group-Name • Filter Information • Access Device • AAA Server
Passed Authentication	• Message-Type • User-Name • NAS-IP-Address • Authen-Failure-Code • Author-Failure-Code • Caller-ID • NAS-Port • Author-Date • Group-Name • Filter Information • Access Device • AAA Server • Proxy-IP-Address • Source-NAS

Report	CSV Attributes
	• PEAP/EAP-FAST-Clear-Name • Real Name
RADIUS Accounting	• User-Name • NAS-IP-Address • NAS-Port • Group-Name • Service-Type • Framed-Protocol • Framed-IP-Address • Calling-Station-Id • Acct-Status-Type • Acct-Input-Octets • Acct-Output-Octets • Acct-Session-Id • Acct-Session-Time • Acct-Input-Packets • Acct-Output-Packets

- For each of these reports, click **Configure** under **Syslog**, and for **Syslog Server**, enter the **IP** address of the FortiSIEM virtual appliance that will receive the syslog as the syslog server, enter 514 for **Port**, and set **Max message length** to **1024**.
- To make sure your changes take effect, go to **System Configuration > Service Control**, and click **Restart ACS**.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Cisco Identity Solution Engine (ISE)

- [Integration Points](#)
- [Event Types](#)
- [Configuration](#)
- [Access Credentials](#)

Integration Points

Protocol	Information Discovered	Used For
Syslog	AAA log - authentication	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "Cisco-ISE" in the main content panel **Search...** field to see the event types associated with this device.

Configuration

- [Configuring Cisco ISE](#)
- [Configuring FortiSIEM](#)

Configuring Cisco ISE

Follow Cisco ISE documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes Cisco ISE syslog as long it follows the following format as shown in the sample syslog:

```
<181>Sep 21 06:50:51 fcmb-hq-psn01 CISE_Passed_Authentications 0000066354 3 0 2016-09-21
06:50:51.516 +01:00 2915312533 5200 NOTICE Passed-Authentication: Authentication succeeded,
ConfigVersionId=287, Device IP Address=1.1.1.1, DestinationIPAddress=1.1.1.2,
DestinationPort=1812, UserName=00-15-65-20-33-E5, Protocol=Radius, RequestLatency=33,
NetworkDeviceName=ACME, User-Name=johndoe, NAS-IP-Address=1.1.1.2, NAS-Port=50009, Service-
Type=Call Check, Framed-IP-Address=1.1.1.2, Framed-MTU=1500, Called-Station-ID=38-1C-1A-87-87-
09, Calling-Station-ID=00-15-65-20-33-E5, NAS-Port-Type=Ethernet, NAS-Port-Id=FastEthernet0/9,
EAP-Key-Name=, cisco-av-pair=service-type=Call Check, cisco-av-pair=audit-session-
id=AC1B35F8000001240FC38F8A, OriginalUserName=0015652033e5, AcsSessionID=fcmb-hq-
psn01/251903157/22970712, AuthenticationIdentityStore=Internal Endpoints,
```

AuthenticationMethod=Lookup, SelectedAccessService=Default Network Access,
SelectedAuthorizationProfiles=IP_Phones,

Access Credentials

For Device Type Cisco Identity Solutions Engine, see [Access Credentials](#).

Cisco Duo

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOGs Collected	Used For
API	Host name and Device Type from LOG, Login Audit Trail	4 log types	Security and Compliance

Event Types

Go to **Admin > Device Type > Event Types** and search for "Cisco-Duo".

Rules

None

Reports

None

Configuration

- [Configuring Cisco Duo](#)
- [Configuring FortiSIEM](#)

Configuring Cisco Duo

Follow these steps to configure Cisco Duo to send logs to FortiSIEM.

1. Contact Cisco Duo support to enable the Admin API.
2. Get a credential for Cisco Duo: open the Cisco Duo dashboard and go to **Application > Admin API**.

3. Select the **Integration key**, **Secret key**, and **API hostname** options.

The screenshot shows the FortiSIEM Admin API configuration interface. On the left is a sidebar with navigation links like Dashboard, Device Insight, Policies, Applications, Users, Groups, 2FA Devices, Administrations, Reports, Settings, Billing, and Support. The main content area is titled 'Admin API' and includes a 'Remove Application' button. Below the title is a 'Details' section with three fields: 'Integration key', 'Secret key', and 'API hostname', each with a 'select' button. A 'Reset Secret Key' button is also present. Below the details is a 'Settings' section with 'Type' set to 'Admin API', 'Name' set to 'Admin API', and a 'Permissions' section with three checkboxes: 'Grant administrations' (unchecked), 'Grant read information' (checked), and 'Grant applications' (checked).

Configuring FortiSIEM

Follow these steps to configure FortiSIEM to receive Cisco Duo logs.

1. In the FortiSIEM UI, go to **ADMIN > Setup > Credentials**.
2. In **Step 1: Enter Credentials**, click **New** to create a Cisco Duo credential.
3. Use these Access Method Definition settings to allow FortiSIEM to access Cisco Duo logs.

Setting	Value
Name	Enter a name for the credential.
Device Type	Cisco Duo Security
Access Protocol	Cisco Duo Admin REST API
Pull Interval (minutes)	2
Integration Key	Enter the integration key you obtained from Cisco Duo.
Secret Key	Enter the secret key you obtained from Cisco Duo.
Description	Enter an optional description for the credential.

4. In **Step 2: Enter IP Range to Credentials Associations**, click **New** to create a new association between the credential and the API hostname.
 - a. Select the name of the Cisco Duo credential created from the **Credentials** drop-down list.
 - b. Enter the host into the **IP/Host Name** field.
 - c. Click **Save**.

5. Click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the connectivity results.
6. Go to the **Analytics** page and check for Cisco Duo logs.

Sample Events

These events are collected via API:

```
FSM-CiscoDuo-Auth] [1] {"access_device":{"browser":"Chrome","browser_
version":"67.0.3396.99","flash_
version":"uninstalled","hostname":"null","ip":"169.232.89.219","java_
version":"uninstalled","location":{"city":"Your City","country":"United
States","state":"Michigan"},"os":"Mac OS X","os_version":"10.14.1"},"application":
{"key":"DIY231J8BR23QK4UKBY8","name":"Microsoft Azure Active Directory"},"auth_device":
{"ip":"192.168.225.254","location":{"city":"Your City","country":"United
States","state":"Michigan"},"name":"My iPhone X (555-555-0001)"}, "event_
type":"authentication","factor":"duo_push","reason":"user_
approved","result":"success","timestamp":1532951962,"trusted_endpoint_status":"not
trusted","txid":"340a23e3-23f3-23c1-87dc-1491a23dfdbb","user":
{"key":"DU3KC77WJ06Y5HIV7XKQ","name":"johndoe@example.com"}}
```

CyberArk Password Vault

- Using CyberArk as a Credential Vault with FortiSIEM
- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- CyberArk Configuration for Sending syslog in a Specific Format

Using CyberArk as a Credential Vault with FortiSIEM

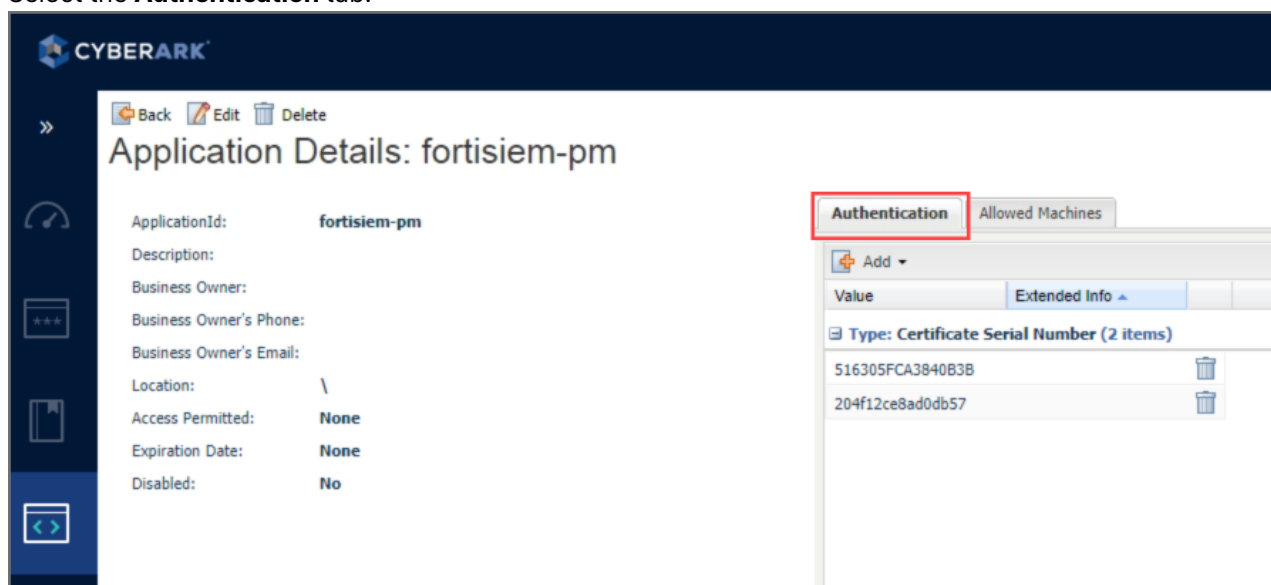
The CyberArk Vault can be utilized by FortiSIEM to securely access and retrieve usernames and passwords for authentication against devices and applications. To use this feature, both CyberArk and FortiSIEM must be configured.

Configuring CyberArk

There are two methods to integrate CyberArk with FortiSIEM, using the REST API (CCP) or Java SDK. FortiSIEM supports both methods, however the preferred method is the REST API. The following steps provide instructions for configuration through the REST API.

After logging into CyberArk, take the following steps:

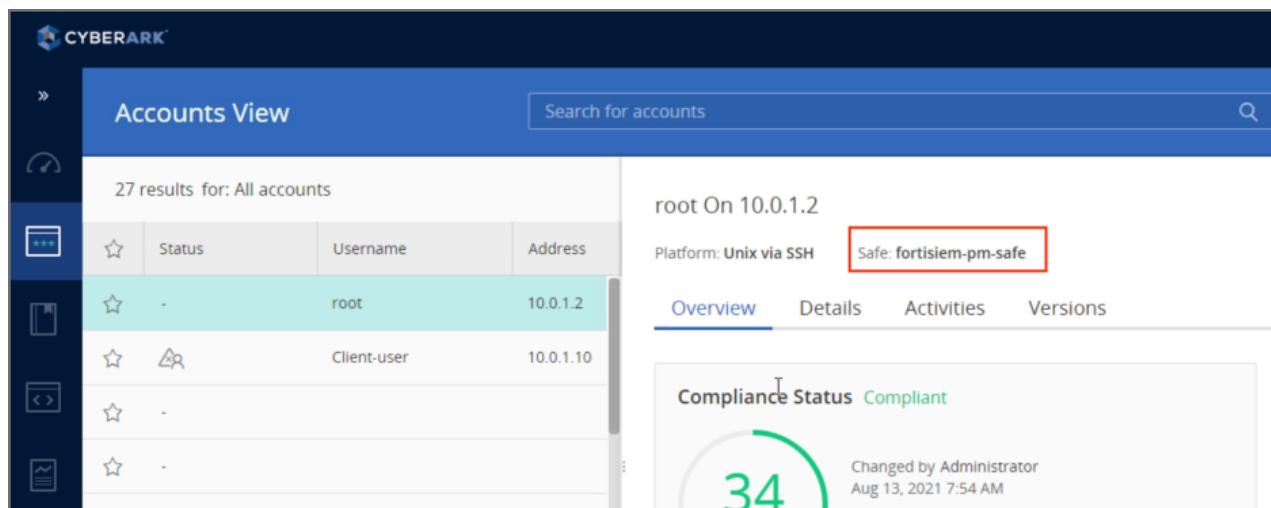
1. Go to the **Applications** section.
2. Create a new application and in the **Name** field, enter a name.
or
Select an existing application.
3. Select the **Authentication** tab.



4. Create certificates, and download the following:

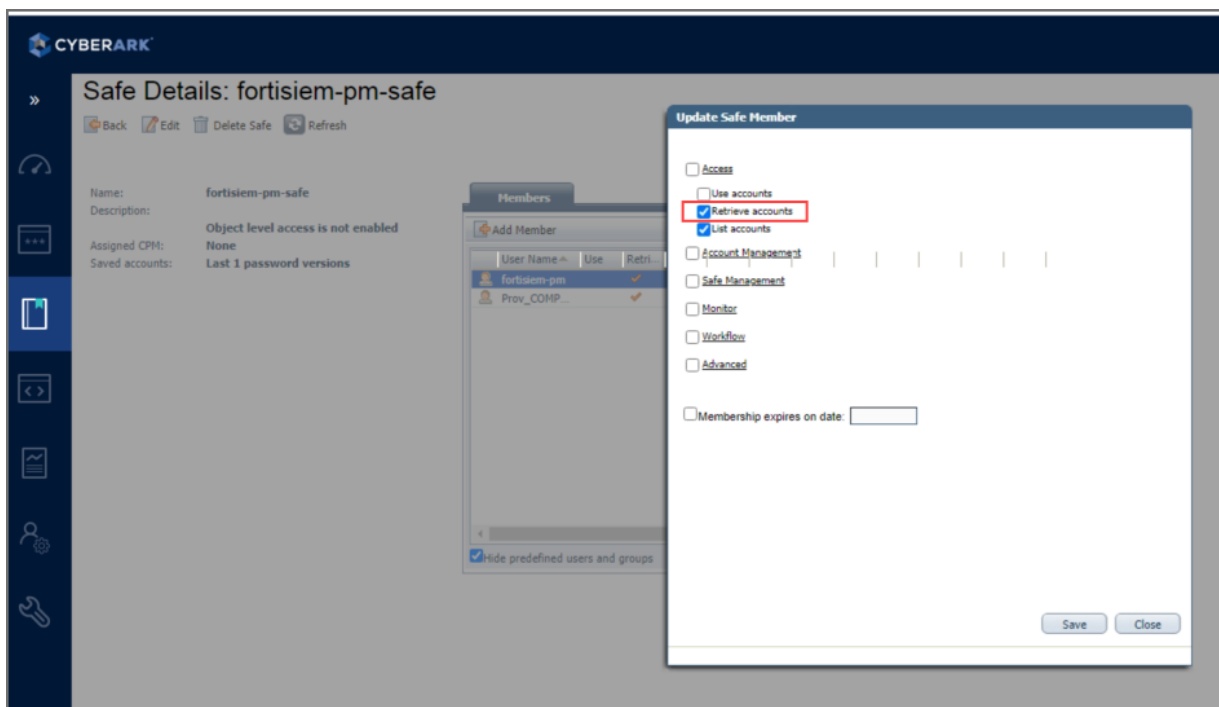
Note: FortiSIEM requires the use of certificates as part of the authentication.

- Root CA
- SSL Certificate
- SSL Key File

5. Ensure that the application has access to the Safe where the Credentials are stored.

If you need to associate the Credential with a Safe, take the following steps:

- a. Navigate to **Policy**.
- b. Locate the Safe.
- c. Click **Members**.
- d. Click **Add Member**.
- e. Add the Application.
- f. Ensure the **Retrieve accounts** checkbox is checked. If it isn't, enable it.



Configuring FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Navigate to **ADMIN > Setup** and click the **Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Setting	Value
Name	Enter the name of the credential.
Device Type	Define the device type.
Access Protocol	Define the access protocol.
Password Config	Select CyberArk Rest API .
Endpoint	Enter the DNS name or IP of the CyberArk server. The format should be <code>https://<server>:<port></code>
Root CA	Upload the Root CA from CyberArk.
SSL Certificate	Upload the SSL Certificate from CyberArk.
SSL Key File	Upload the SSL Key File from CyberArk.
App ID	Provide the application defined in

Setting	Value
	CyberArk.
Safe	Provide the safe defined in CyberArk.
Folder	Provide the folder from the CyberArk configuration. If folders are not used, specify "root".
Object	Provide the credential Account Name from CyberArk. This can be found in CyberArk under Accounts > <your account> > Details > <Account Name>. Note: See screenshot below for example Account Name. If the Object is defined in the FortiSIEM credential, then the follow additional details should not be needed: • Username • Platform (Policy ID) • Database • (Checkbox) Include Address for Query If this information is required, it can be obtained by using the thick client CyberArk tool PrivateArk. Take the following steps: 1. Open PrivateArk. 2. Open the Vault. 3. Find the Safe you wish to use. 4. Locate the credential, right click and select Properties. Here you will find the Username and Policy ID.

The screenshot displays the CyberArk Accounts View interface. On the left, a sidebar contains navigation icons. The main area is titled "Accounts View" and includes a search bar. Below the search bar, it indicates "27 results for: All accounts". A table lists accounts with columns for Status, Username, and Address. The first account, "root" at "10.0.1.2", is selected and highlighted in teal. To the right of the table, the details for the selected account are shown. The details include the platform "Unix via SSH", the safe "fortisiem-pm-safe", and tabs for Overview, Details, Activities, and Versions. The Details tab is active, showing fields for Safe, Platform, Address, and Username. The Account name is highlighted with a red box.

Status	Username	Address
-	root	10.0.1.2
-	Client-user	10.0.1.10
-	-	-
-	-	-
-	SCIM-user	10.0.1.10
-	ttrinh	amazon.co
-	AKIAJT7I5QKXFU3HIQ...	AWS-CLOU
-	root	172.30.58.2
-	ttrinh	172.30.56.2

root On 10.0.1.2

Platform: Unix via SSH Safe: fortisiem-pm-safe

Overview Details Activities Versions

Safe fortisiem-pm-safe Logon Account None

Platform Unix via SSH ⓘ Account Groups

Address 10.0.1.2 Group Name None

Username root Group Platform None

Account name
Operating System-UnixSSH-10.0.1.2-root

Access Method Definition

Name:

cyberark - ssh

Device Type:

Redhat Linux

Access Protocol:

SSH

Port:

22

Password config:

CyberArk REST API

Endpoint:

https://[REDACTED]

Root CA:

RootCAH15SSLZzTF.crt

Upload

SSL Certificate:

clientzX4igZEBrZ.crt

Upload

SSL Key File:

clientzX4igZEBrZ.pem

Upload

App ID:

fortisiem-pm

Safe:

fortisiem-pm-safe

Folder:

root

Object:

Operating System-UnixSSH-10.0.1.2-root

Save

Cancel

What is Discovered and Monitored

Protocol	Information discovered	Logs parsed	Used for
Syslog (CEF formatted and others)		CyberArk Safe Activity	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "CyberArk-Vault" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "CyberArk" in the in the main content panel **Search...** field:

- CyberArk Vault Blocked Failure
- CyberArk Vault CPM Password Disables
- CyberArk Vault Excessive Failed PSM Connections
- CyberArk Vault Excessive Impersonations
- CyberArk Vault Excessive PSM Keystroke Logging Failure
- CyberArk Vault Excessive PSM Session Monitoring Failure
- CyberArk Vault Excessive Password Release Failure
- CyberArk Vault File Operation Failure
- CyberArk Vault Object Content Validation Failure
- CyberArk Vault Unauthorized User Stations
- CyberArk Vault User History Clear

Reports

In **RESOURCES > Reports**, search for "CyberArk" in the main content panel **Search...** field:

- CyberArk Blocked Operations
- CyberArk CPM Password Disables
- CyberArk CPM Password Retrieval
- CyberArk File Operation Failures
- CyberArk Impersonations
- CyberArk Object Content Validation Failures
- CyberArk PSM Monitoring Failures
- CyberArk Password Resets
- CyberArk Privileged Command Operations
- CyberArk Provider Password Retrieval
- CyberArk Trusted Network Area Updates
- CyberArk Unauthorized Stations
- CyberArk User History Clears
- CyberArk User/Group Modification Activity
- CyberArk Vault CPM Password Reconciliations
- CyberArk Vault CPM Password Verifications
- CyberArk Vault Configuration Changes

- CyberArk Vault Failed PSM connections
- CyberArk Vault Modification Activity
- CyberArk Vault PSM Keystore Logging Failures
- CyberArk Vault Password Changes from CPM
- CyberArk Vault Password Release Failures
- CyberArk Vault Successful PSM Connections
- Top CyberArk Event Types
- Top CyberArk Safes, Folders By Activity
- Top CyberArk Users By Activity

CyberArk Configuration for Sending syslog in a Specific Format

1. Open \PrivateArk\Server\DBParm.ini file and edit the SYSLOG section:
 - a. SyslogServerIP – Specify FortiSIEM supervisor, workers and collectors separated by commas.
 - b. SyslogServerProtocol – Set to the default value of UDP.
 - c. SyslogServerPort – Set to the default value of 514.
 - d. SyslogMessageCodeFilter – Set to the default range 0-999.
 - e. SyslogTranslatorFile – Set to Syslog\FortiSIEM.xml.
 - f. UseLegacySyslogFormat – Set to the default value of No.
2. Copy the relevant [XSL](#) translator file here to the Syslog subfolder specified in the SyslogTranslatorFile parameter in DBParm.ini.
3. Stop and Start Vault (Central Server Administration) for the changes to take effect.

Make sure the syslog format is as follows.

```
<5>1 2016-02-02T17:24:42Z SJCDVWVCARK01 CYBERARK:
Product="Vault";Version="9.20.0000";MessageID="295";Message="Retrieve
password";Issuer="Administrator";Station="10.10.110.11";File="Root\snmpCommunity";
Safe="TestPasswords";Reason="Test";Severity="Info"
<30>Mar 22 20:13:42 VA461_1022 CyberArk AIM[2453]: APPAP097I Connection to the Vault has been
restored
<27>Mar 22 20:10:50 VA461_1022 CyberArk AIM[2453]: APPAP289E Connection to the Vault has failed.
Further attempts to connect to the Vault will be avoided for [1] minutes.
<27>Mar 24 23:41:58 VA461_1022 CyberArk AIM[2453]: APPAU002E Provider [Prov_VA461_1022] has failed
to fetch password with query [Safe=TestPutta;Object=Telnet91] for application [FortiSIEM]. Fetch
reason: [APPAP004E Password object matching query
```

Fortinet FortiAuthenticator

- What is Discovered and Monitored
- Event Types
- Configuration
- FortiSIEM Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
SNMP	Vendor, OS, Model, Network Interfaces	Interface Stat, Authentication Stat	Performance Monitoring
Syslog	LOG Discovery	Over 150 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "FortiAuthenticator" in the main content panel **Search...** field.

Sample Event Type:

```
<14>Aug 14 22:32:52 db[16987]: category="Event" subcategory="Authentication" typeid=20995  
level="information" user="admin" nas="" action="Logout" status="" Administrator 'admin' logged out
```

Configuration

FortiAuthenticator logging instructions can be found here: <https://docs.fortinet.com/document/fortiauthenticator/6.3.1/administration-guide/964220/log-configuration>

Configure FortiAuthenticator to send logs to FortiSIEM by taking the following steps:

Create a Syslog Server

1. From FortiAuthenticator, navigate to **Logging > Log Config > Syslog Servers**.
2. Click **Create New**.
3. In the **Name** field, enter a name such as "FortiSIEM Collector".
4. In the **Server name/IP** field, enter the FortiSIEM Collector IP address.
5. In the **Port** field, ensure 514 is configured.
6. Click **OK** to add the syslog server.

Configure Remote Logging

1. Navigate to **Logging > Log Config > Log Settings**.
2. Go to **Remote Syslog** and make sure **Send system logs to remote Syslog servers** is enabled.
3. Move the "FortiSIEM Collector" syslog server to which logs will be sent from the **Available Syslog Servers** box to the **Chosen Syslog Servers** box.
4. Select **OK** to save your settings.

FortiSIEM Access Credentials

For **Device Type**, select Fortinet FortiAuthenticator from the drop-down list. See [Access Credentials](#) for more information on configuration.

Juniper Networks Steel-Belted Radius

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O	Performance Monitoring
Syslog	Application type	Successful and Failed Authentications, Successful and Failed administrative logons, RADIUS accounting logs	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Juniper-Steelbelt" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [Syslog](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

- [Configuring Windows Agent](#)
- [Configuring Linux Agent](#)

For Windows Agent, take the following steps:

1. Login to FortiSIEM GUI.
2. Navigate to **Admin > Setup**, and click the **Windows Agent** tab.
3. Under **Windows Agent Monitor Templates**, click **New** to create a new template, or click an existing template and click **Edit**.
4. If creating a new template, on the **Generic** tab, in the **Name** field, enter a name for the template.
5. Click the **User Log** tab, and click **New**.
 - a. In the **Full File Name** field, enter the full file name (including path) to be monitored.
 - b. In the **Log Prefix** field, enter a log prefix that needs to be added to the log.
 - c. Click **Save**.
6. Click **Save**.
7. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
8. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
9. From the **Host** drop-down list, select the host(s).
10. At **Template**, attach the template to one or more server hosts by selecting its checkbox, then click **Save**.
11. Under **Host to Template Associations**, click **Apply**.

The logs will have a prefix set by **Log Prefix** that can be used to write a Parser for these files.

For details, see [Configuring Windows Agent](#).

For Linux Agent, take the following steps:

1. Login to FortiSIEM GUI.
2. Navigate to **Admin > Setup**, and click the **Linux Agent** tab.
3. Under **Linux Agent Monitor Templates**, click **New** to create a new template, or click an existing template and click **Edit**.
4. If creating a new template, on the **Generic** tab, in the **Name** field, enter a name for the template.
5. Click the **Log File** tab, and click **New**.
 - a. In the **Full File Name** field, enter the full file name (including path) to be monitored.
 - b. In the **Log Prefix** field, enter a log prefix that needs to be added to the log.
 - c. Click **Save**.
6. Click **Save**.
7. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
8. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
9. From the **Host** drop-down list, select the host(s).
10. At **Template**, attach the template to one or more server hosts by selecting its checkbox, then click **Save**.
11. Under **Host to Template Associations**, click **Apply**.

The logs will have a prefix set by **Log Prefix** that can be used to write a Parser for these files.

For details, see [Configuring Linux Agent](#).

Microsoft Internet Authentication Server (IAS)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
WMI			
Syslog			
Windows Agent			IAS logs

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft isa" to see the event types associated with this device.

Configuration

- [WMI](#)
- [Syslog](#)

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

Syslog

You must configure your Microsoft Internet Authentication Server to save logs, and then you can use the Windows Agent Manager to configure the type of log information you want sent to FortiSIEM.

1. Log in to your server as an administrator.
2. Go to **Start > Administrative Tools > Internet Authentication Service**.
3. In the left-hand navigation, select Remote Access Logging, then select **Local File**.
4. Right-click on **Local File** to open the **Properties** menu, and then select **Log File**.
5. For **Directory**, enter C:\WINDOWS\system32\LogFiles\IAS.
6. Click **OK**.

You can now use [Windows Agent Installation Guide](#) to configure what information will be sent to FortiSIEM.

Microsoft Network Policy Server (RAS VPN)

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Setting for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	AAA based login events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "MS-NPS" to see the event types associated with this device.

Rules

No specific rules are written for Microsoft Network Policy Server, but regular AA Server rules apply.

Reports

No specific reports are written for Microsoft Network Policy Server, but regular AA Server reports apply.

Configuration

Configure Microsoft Network Policy Server system to send logs to FortiSIEM in the supported format (see [Sample Events](#)). See <https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-accounting-configure>.

Settings for Access Credentials

None required.

Sample Events

```
"HOSTXXVPN", "RAS", 03/10/2019, 03:47:04, 4, "domain\\user", , "10.1.1.130", "192.168.22.2", , "172.17.220.130",  
"HOSTXXVPN", "10.5.5.212", 387, , "10.5.5.212", "HOSTXXVPN", 1552214822, , 5, , 1, 2, , , 0,  
"311 1 fe80::a1bf:5c1c:7ebc:6ab7 02/07/2019 04:24:00  
4805", , , , 2, , 268050551, 253119217, "4806", 3, 69101, 833955, 726102, 1, "1251", 1, , 79617, 1,  
"192.168.22.2", "10.1.1.130", , , , , "MSRASV5.20", 311, , "0x00504F4C42", 0, ,  
"Microsoft Routing and Remote Access Service Policy", , , , "MSRAS-0-HOST123413", "MSRASV5.20"
```

One Identity Safeguard (previously Balabit Privileged Session Management)

- [Integration Points](#)
- [Event Types](#)
- [Configuration](#)

Integration Points

Protocol	Information Discovered	Used For
Syslog	Privileged session management events	Security and Compliance

Event Types

Over 50 events are parsed. In **RESOURCES > Event Types**, search for "OneIdentity-Safeguard-" in the main content panel **Search...** field.

Configuration

- [Configuring One Identity Safeguard](#)
- [Configuring FortiSIEM](#)

Configuring One Identity Safeguard

Follow the [One Identity Safeguard documentation](#) to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes One Identity Safeguard syslog as long as it follows the following format in the sample syslog:

```
<123>2018-10-08T22:59:49+08:00 scbdemo.balabit zorp/scb_rdp[31769]: core.debug(4):  
(svc/i9CTbTzV2wrRur3quVRzF4/GET_gateway_rdp:498:2): After NAT mapping; nat_type='0', src_  
addr='AF_INET(10.19.9.245:0)', dst_addr='AF_INET(10.46.26.196:3389)', new_addr='AF_INET  
(10.11.101.30:0)'
```

Vasco DigiPass

- What is Discovered and Monitored
- Event Types
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		Successful and Failed Authentications, Successful and Failed administrative logons	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Vasco-DigiPass" to see the event types associated with this device. Some important ones are:

- Vasco-DigiPass-KeyServer-AdminLogon-Success
- Vasco-DigiPass-KeyServer-UserAuth-Success
- Vasco-DigiPass-KeyServer-UserAuth-Failed
- Vasco-DigiPass-KeyServer-AccountLocked
- Vasco-DigiPass-KeyServer-AccountUnlocked

Configuration

Configure the Vasco DigiPass management Console to send syslog to FortiSIEM. FortiSIEM is going to parse the logs automatically. Make sure the syslog format is as follows.

```
May 16 18:21:50 vascoservername ikeyserver[3575]: {Success}, {Administration}, {S-001003}, {A
command of type [User] [Unlock] was successful.}, {0xA46B6230BA60B240CE48011B0C30D393}, {Source
Location:10.1.2.3}, {Client Location:10.1.2.3}, {User ID:flast}, {Domain:company.com}, {Input
Details: {User ID : flast} {Domain Name : company.com}}, {Output Details: {User ID : flast}
{Password : *****} {Created Time : 2013/05/13 19:06:52} {Modified Time : 2013/05/16 18:21:49}
{Has Digipass : Unassigned} {Status : 0} {Domain Name : company.com} {Local Authentication :
Default} {Back-end Authentication : Default} {Disabled : no} {Lock Count : 0} {Locked : no} {Last
Password Set Time : 2013/05/13 19:06:52} {Static Password History :
d0NdVMhSdv dNEQJkkKTWmiq8iB4K1dWreMf5FQlZM7U=} {Key ID : SSMINSTALLSENSITIVEKEY}}, {Object:User},
{Command:Unlock}, {Client Type:Administration Program}

May 15 20:27:35 vascoservername ikeyserver[3575]: {Success}, {Administration}, {S-004001}, {An
```

```
administrative logon was successful.}, {0x25AB20F3222F554A96CFFD2886AE4C71}, {Source  
Location:10.1.2.3}, {Client Location:10.1.2.3}, {User ID:admin}, {Domain:company.com}, {Client  
Type:Administration Program}
```

```
May 17 18:43:22 vascoservername ikeyserver[3582]: {Info}, {Initialization}, {I-002010}, {The SOAP  
protocol handler has been initialized successfully.}, {0x0E736D24D54E717E6F5DA6C09E89F8EE},  
{Version:3.4.7.115}, {Configuration Details:IP-Address: 10.1.2.3, IP-Port: 8888, Supported-Cipher-  
Suite: HIGH, Server-Certificate: /var/identikay/conf/certs/soap-custom.pem, Private-Key-Password:  
*****, CA-Certificate-Store: /var/identikay/conf/certs/soap-ca-certificate-store.pem, Client-  
Authentication-Method: none, Reverify-Client-On-Reconnect: False, DPX-Upload-Location: /var/dpx/}
```


Database Server

FortiSIEM supports these database servers for discovery and monitoring.

- [IBM DB2 Server](#)
- [Microsoft SQL Server](#)
- [MySQL Server](#)
- [Oracle Database Server](#)

IBM DB2 Server

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials
- Sample Events

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
JDBC	None	Database audit trail: Successful and failed database log on, Database CREATE/DELETE/MODIFY operations, Table CREATE/DELETE/MODIFY/INSERT operations	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "db2" to see the event types associated with this device.

Configuration

- [Configuring IBM DB2 Audit on Linux - DB2 side](#)
- [Configuring IBM DB2 Audit on Windows - DB2 side](#)

Configuring IBM DB2 Audit on Linux - DB2 side

1. Log in to IBM Installation Manager.
2. Click the **Databases** tab, and click the + icon to create a new **Database Connection**.
3. Enter these settings.

Setting	Value
Database	Enter a name for the connection, such as FortiSIEM

Setting	Value
Connection Name	
Data Server Type	DB2 for Linux, Unix, and Windows
Database Name	Name of the database
Host name	db2.org
Port number	50000
JDBC Security	Clear text password
User ID	The username you want to use to access this Server from FortiSIEM
JDBC URL	jdbc:db2://db2.org:50000/<databasename>: retrieveMessagesFromServerOnGetMessage=true;secur i

4. In the **Job Manager** tab, click **Add Job**.
5. For **Name**, enter **audit**.
6. For **Type**, select **DB2 CLP Script**.
7. Click **OK**.
8. Add script.
9. Add schedule detail to audit task.
10. Add database to audit task.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections 'Discovering Infrastructure' and 'Setting Access Credentials' for Device Discovery under Chapter: Configuring FortiSIEM.

Configuring IBM DB2 Audit on Windows - DB2 side

1. Create a non-admin user on Windows, for example "AoAuditUser", and set password
2. Login DB2 task center, add the user to DB Users, connect it to database
3. Grant Permission (use Administrator), use commands below
 - a. Grant audit permission to db2admin

```
db2 connect to sample user administrator using 'ProspectHills!'
DB2 GRANT EXECUTE ON PROCEDURE SYSPROC.AUDIT_ARCHIVE TO DB2ADMIN
DB2 GRANT EXECUTE ON PROCEDURE SYSPROC.AUDIT_DELIM_EXTRACT TO DB2ADMIN
db2 grant load on database to db2admin
db2 grant secadm on database to db2admin
db2 connect reset
```

b. Grant query permission to non-admin user

```
db2 connect to sample user db2admin using 'ProspectHills!'
db2 grant select on AUDIT to AOAuditUser
db2 grant select on CHECKING to AOAuditUser
db2 grant select on OBJMAINT to AOAuditUser
db2 grant select on SECMAINT to AOAuditUser
db2 grant select on SYSADMIN to AOAuditUser
db2 grant select on VALIDATE to AOAuditUser
db2 grant select on CONTEXT to AOAuditUser
db2 grant select on EXECUTE to AOAuditUser
db2 connect reset
```

c. Check permission for non-admin user

```
db2 connect to sample user AOAuditUser using 'ProspectHills!'
db2 select count (*) from DB2ADMIN.AUDIT
db2 select count (*) from DB2ADMIN.CHECKING
db2 select count (*) from DB2ADMIN.OBJMAINT
db2 select count (*) from DB2ADMIN.SECMAINT
db2 select count (*) from DB2ADMIN.SYSADMIN
db2 select count (*) from DB2ADMIN.VALIDATE
db2 select count (*) from DB2ADMIN.CONTEXT
db2 select count (*) from DB2ADMIN.EXECUTE
db2 connect reset
```

4. Create Catalog with db2admin**5. Create task in DB2 user Administrator:**

- a. Open DB2 task center, create a task like below
- b. Add schedule
- c. Add task

Settings for Access Credentials

Settings for IBM DB2 JDBC Access Credentials

- [Values for Used For = Audit](#)
- [Values for Used For = Synthetic Transaction Monitoring](#)

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device:

Values for Used For = Audit:

Setting	Value
Name	db2_linux
Device Type	IBM DB2
Access Protocol	JDBC

Setting	Value
Used For	audit
Pull Interval (minutes)	5
Port	50000
Database Name	<database_name>
Audit Table	AUDIT
Checking Table	CHECKING
ObjMaint Table	OBJMAINT
SecMaint Table	SECMAINT
SysAdmin Table	SYSADMIN
Validate Table	VALIDATE
Context Table	CONTEXT
Execute Table	EXECUTE
Account Name	The administrative user for your IBM DB2 server
Password	The password associated with the administrative user for your IBM DB2 server

Values for Used For = Synthetic Transaction Monitoring:

Setting	Value
Name	db2_linux
Device Type	IBM DB2
Access Protocol	JDBC
Used For	Synthetic Transaction Monitoring
Pull Interval (minutes)	5
Port	50000
Database Name	<database_name>
Account Name	The administrative user for your IBM DB2 server
Password	The password associated with the administrative user for your IBM DB2 server

Sample Events

IBMDB2_CHECKING_OBJECT

```
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_CHECKING_OBJECT]:[eventSeverity]=PHL_INFO,
[objName]=TABLES,[srcIpAddr]=127.0.0.1,[srcApp]=DB2HMON,[dbName]=SAMPLE,[appVersion]=DB2
v10.1.0.0,[instanceName]=db2inst1,[eventTime]=2014-05-14-13.44.41.085567,[user]=db2inst1,
[eventCategory]=CHECKING,[dbRetCode]=0
```

IBMDB2_CHECKING_FUNCTION

```
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_CHECKING_FUNCTION]:[eventSeverity]=PHL_INFO,
[objName]=CHECKING,[srcIpAddr]=127.0.0.1,[srcApp]=DB2HMON,[dbName]=SAMPLE,[appVersion]=DB2
v10.1.0.0,[instanceName]=db2inst1,[eventTime]=2014-05-14-13.44.40.739649,[user]=db2inst1,
[eventCategory]=CHECKING,[dbRetCode]=0
```

IBMDB2_STATEMENT

```
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_STATEMENT]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.48.59.433204,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
```

IBMDB2_COMMIT

```
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_COMMIT]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=10.1.2.81,[srcApp]=db2jcc_application,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.51.30.447924,[srcName]=SP81,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
```

IBMDB2_ROLLBACK

```
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_ROLLBACK]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.43.43.827986,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
```

IBMDB2_CONNECT

```
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_CONNECT]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=DB2HMON,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.44.39.991288,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
```

IBMDB2_CONNECT_RESET

```
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_CONNECT_RESET]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.43.43.829149,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
```

IBMDB2_CREATE_OBJECT

```
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_CREATE_OBJECT]:[eventSeverity]=PHL_INFO,
[objName]=CAN_MONITOR=CAN_MONITOR_FUNC,[srcIpAddr]=10.1.2.68,[srcApp]=DS_ConnMgt_,[dbName]=SAMPLE,
[appVersion]=DB2 v10.1.0.0,[instanceName]=db2inst1,[eventTime]=2014-05-14-13.30.14.827242,
[srcName]=10.1.2.68,[user]=db2inst1,[eventCategory]=OBJMAINT,[dbRetCode]=0
```

IBMDB2_JDBC_PULL_STAT

```
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_JDBC_PULL_STAT]:[eventSeverity]=PHL_INFO,
[reptModel]=DB2,[dbName]=SAMPLE,[instanceName]=db2inst1,[reptVendor]=IBM,[rptIp]=10.1.2.68,
[auditEventCount]=30,[relayIp]=10.1.2.68,[dbEventCategory]=db2inst1.AUDIT,[appGroupName]=IBM DB2
Server
```

IBMDB2_ARCHIVE

```
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_ARCHIVE]:[eventSeverity]=PHL_INFO,  
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,  
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.43.44.002046,[user]=db2inst1,  
[eventCategory]=AUDIT,[dbRetCode]=0  
IBMDB2_EXTRACT  
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_EXTRACT]:[eventSeverity]=PHL_INFO,  
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,  
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.38.45.865016,[user]=db2inst1,  
[eventCategory]=AUDIT,[dbRetCode]=0  
IBMDB2_LIST_LOGS  
<134>May 14 14:03:39 10.1.2.68 java: [IBMDB2_LIST_LOGS]:[eventSeverity]=PHL_INFO,  
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,  
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.58.43.204054,[user]=db2inst1,  
[eventCategory]=AUDIT,[dbRetCode]=0
```

Microsoft SQL Server

Support Added: FortiSIEM 4.7.2

Last Modification: FortiSIEM 6.3.1

Vendor: Microsoft

Product Information: <https://www.microsoft.com/en-us/sql-server/>

Supported Versions

- SQL Server 2014
 - SQL Server 2016
 - SQL Server 2017
 - SQL Server 2019
 - SQL Server 2022
-
- [What is Discovered and Monitored](#)
 - [Recommended Configuration](#)
 - [SNMP Configuration](#)
 - [OMI or Windows Agent Configuration](#)
 - [Configuration for Database Audit Logs](#)
 - [JDBC Configuration for Database Performance Metrics](#)
 - [JDBC Configuration for DDL Changes](#)
 - [Sample Events](#)

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Microsoft SQL server.

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
WMI		Windows application event logs - successful and failed login	Security Monitoring

Protocol	Information discovered	Metrics collected	Used for
JDBC		General database info: database name, database version, database size, database owner, database created date, database status, database compatibility level Database configuration Info: Configure name, Configure value, Configure max and min value, Configure running value Database backup Info: Database name, Last backup date, Days since last backup	Availability Monitoring
JDBC		Database performance metrics (per-instance): Buffer cache hit ratio, Log cache hit ratio, Transactions /sec, Page reads/sec, Page writes/sec, Page splits/sec, Full scans/sec, Deadlocks/sec, Log flush waits/sec, Latch waits/sec, Data file(s) size, Log file(s) used, Log growths, Log shrinks, User connections, Target server memory, Total Server Memory, Active database users, Logged-in database users, Available buffer pool pages, Free buffer pool pages, Average wait time Database performance metrics (per-instance, per-database): Database name, Data file size, Log file used, Log growths, Log shrinks, Log flush waits/sec, Transaction /sec, Log cache hit ratio	Performance Monitoring
JDBC		Locking info: Database id, Database object id, Lock type, Locked resource, Lock mode, Lock status Blocking info: Blocked Sp Id, Blocked Login User, Blocked Database, Blocked Command, Blocked Process Name, Blocking Sp Id, Blocking Login User, Blocking Database, Blocking Command, Blocking Process Name, Blocked duration	Performance Monitoring
JDBC		Database error log Database audit trail: Failed database logon is also collected through performance monitoring as logon failures cannot be collected via database triggers.	Availability / Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
JDBC		Various database operation audit trail including CREATE/ALTER/DROP/TRUNCATE operations on tables, table spaces, databases, clusters, users, roles, views, table indices, triggers etc	Security Monitoring and compliance
OMI or Windows Agent		Successful database logon (Win-App-MSSQLSERVER-18454) and Failed database logon (Win-App-MSSQLSERVER-18456) via Windows Application log	Security Monitoring and compliance

Recommended Configuration

1. [OMI or FortiSIEM Windows Agent for discovery and system level performance metrics](#) (See [FortiSIEM Windows Agent Discovery configuration](#), [FortiSIEM Windows Agent System Level Performance Metrics configuration](#) for more information).
2. [FortiSIEM Windows Agent for Database Successful and Failed Login](#) – Note that these logs can also be pulled via OMI, however performance is limited because of OMI limitations.
3. [JDBC for Database Performance Metrics](#)
4. [JDBC for DDL Changes](#)

SNMP Configuration

See [SNMP Configurations](#) in *Microsoft Windows Server via OMI/ SNMP/ WMI*.

OMI or Windows Agent Configuration

See [Microsoft Windows Server via OMI/ SNMP/ WMI](#) for OMI configurations.

See [Microsoft Windows Server via Agent](#) for FortiSIEM Windows Agent configurations.

Configuration for Database Audit Logs

Database Audit logs include failed and successful logons and other C2 audit activity. These logs are written to the Windows Application logs.

Configuration occurs in two parts.

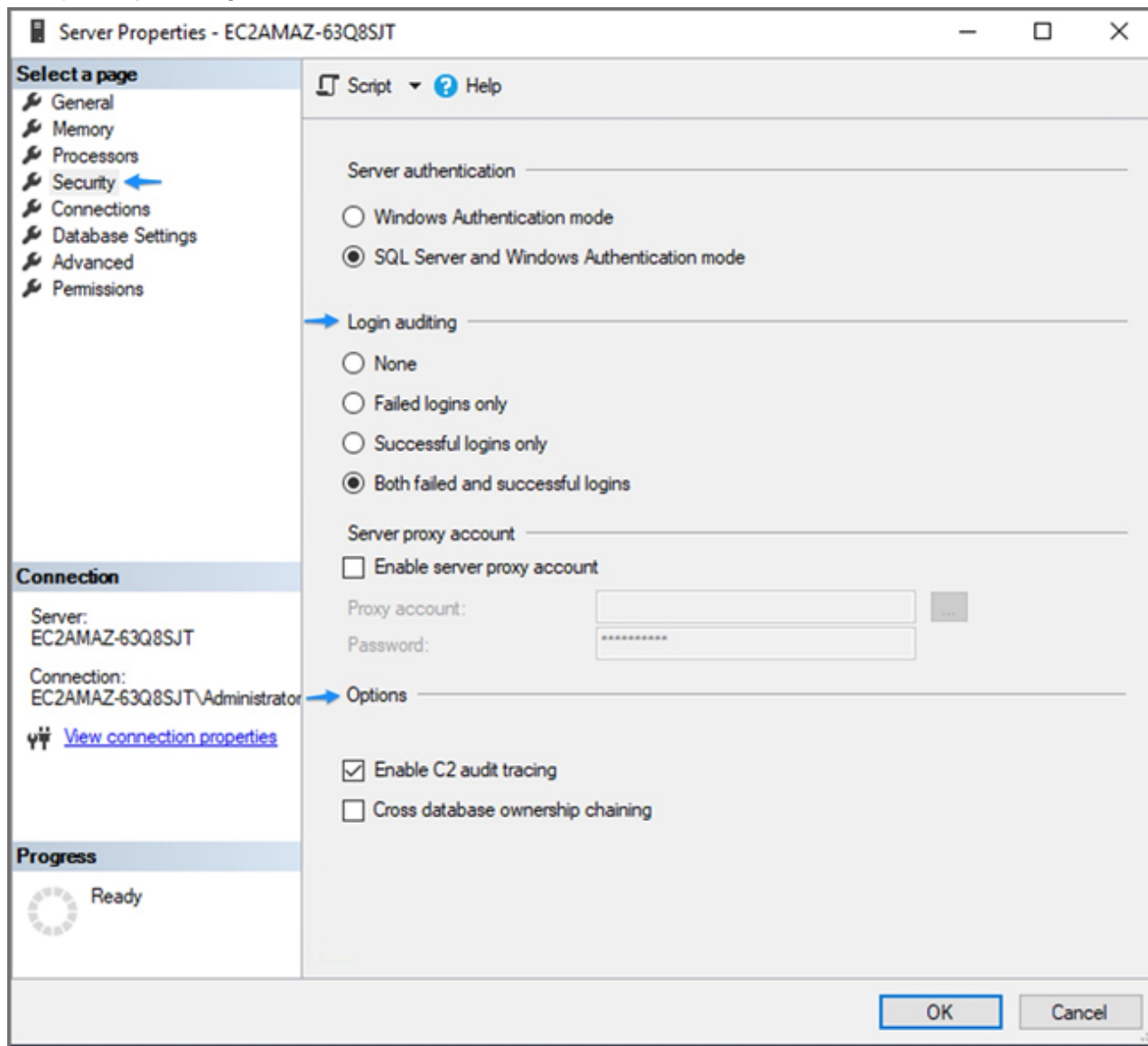
- [SQL Server Configuration](#)
- [FortiSIEM Configuration](#)

SQL Server Configuration

Step 1: Configure Login Auditing using SQL Server Management studio

Take the following steps to configure Login Auditing.

1. In SQL Server Management Studio, connect to an instance of the SQL Server Database Engine with Object Explorer.
2. In Object Explorer, right-click the server name, and then click **Properties**.
3. On the **Security** page, under **Login auditing**, select the desired option
4. On the **Security** page, under **Options**, click on the **Enable C2 audit tracing** check box and close the **Server Properties** page.
5. In Object Explorer, right-click the server name, and then click **Restart**.

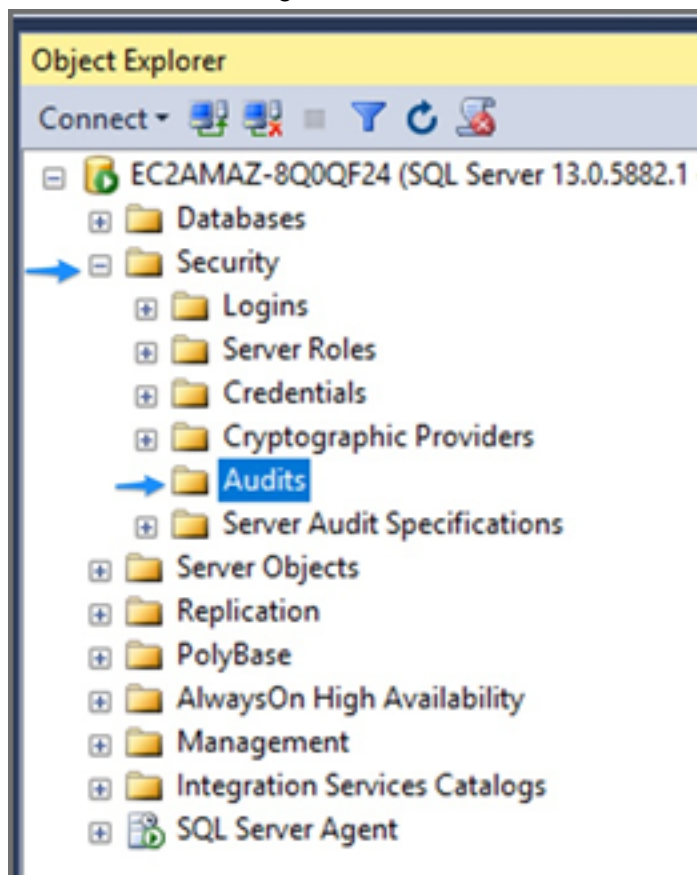


Note: You must **restart** the SQL Server before this option will take effect.

Step 2: Enabling SQL Server Audit

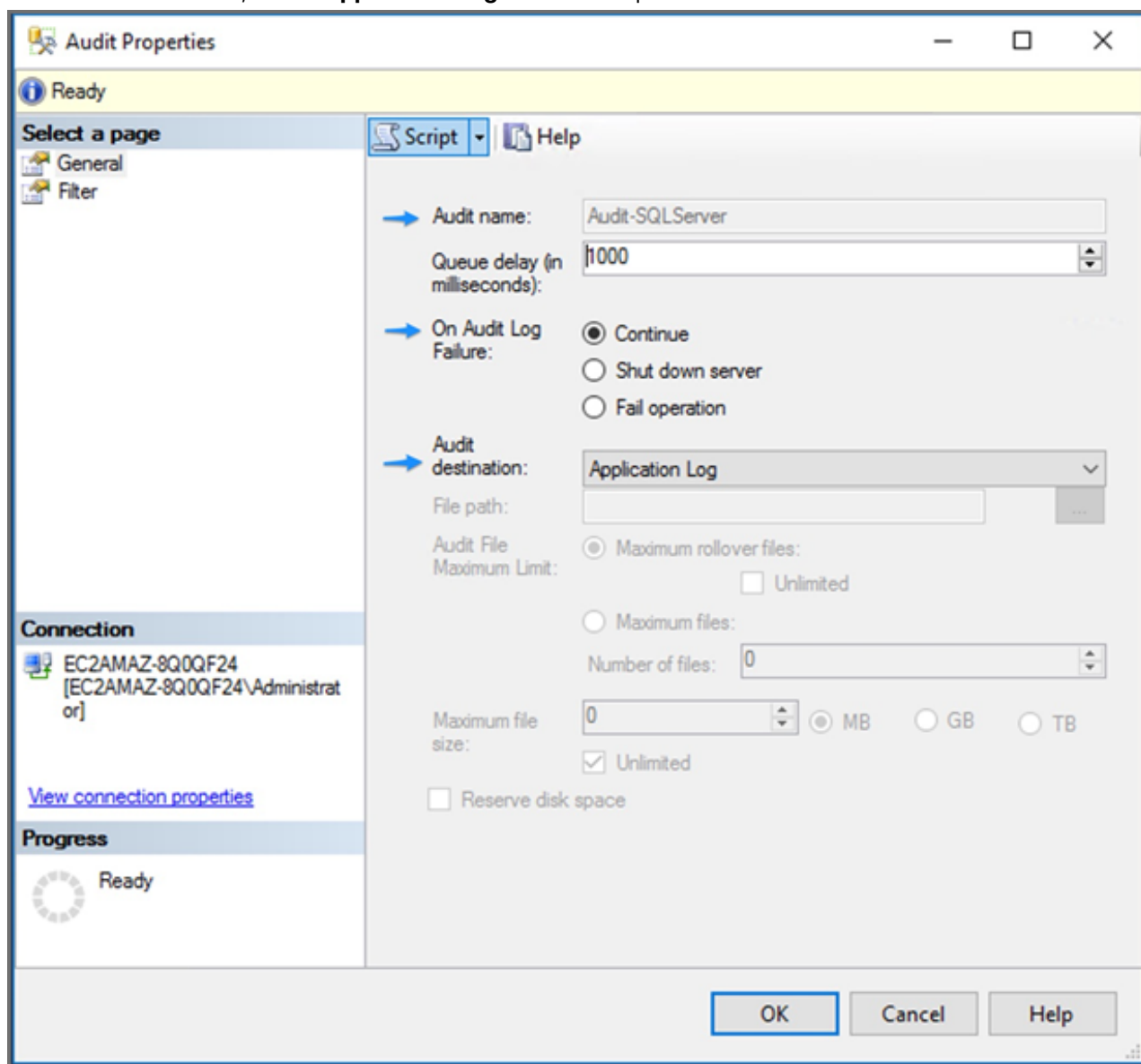
Create a Server-level audit object by taking the following steps:

1. In SQL Server Management Studio, connect to an instance of the SQL Server Database Engine with Object Explorer.
2. In the Object Explorer panel on the left, expand **Security**.
3. Right-click **Audits**, and select **New Audit...** from the menu. This will create a new SQL Server Audit object for server-level auditing.

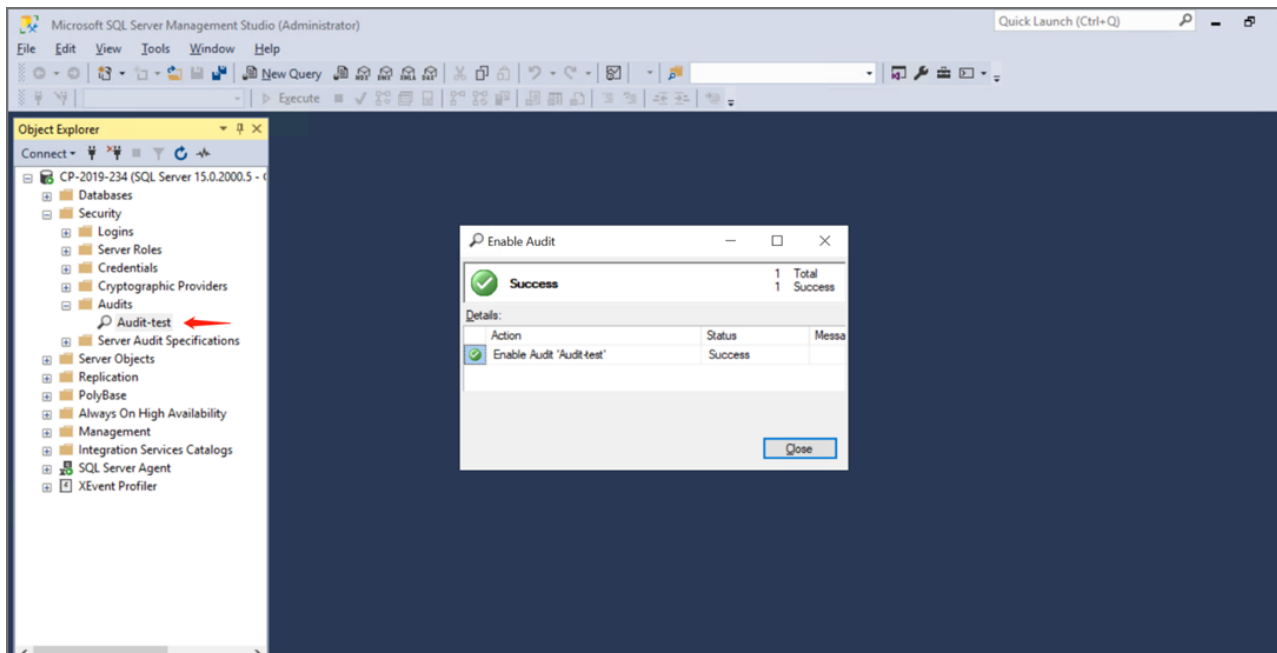


4. In the Create Audit window, give the audit settings a name in the **Audit name** field.
5. For **On Audit Log Failure**, select the **Continue** option.

6. For **Audit destination**, select **Application Log** from the drop-down list.



7. Click **OK**.
8. You will now find the new audit configuration in Object Explorer below Security > Audits. Right-click the new Audit configuration and select **Enable Audit** from the menu.



9. Click **Close** in the Enable Audit dialog.

FortiSIEM Configuration

Step 1: Define the Windows Agent Monitor Template for SQL Server

Complete these steps to add a Windows Agent Monitor Template:

1. Navigate to **ADMIN > Setup** and click the **Windows Agent** tab.
2. Under **Windows Agent Monitor Templates** click **New**.
3. In the **Windows Agent Monitor Template** dialog box, in the **Name** field, enter a name.
4. Click on **Event** tab, and take following steps:
 - a. In the **Event Log** row, click **New**.
 - b. From the **Type** drop-down list, select **Security** and click **Save**.
 - c. In the **Event Log** row, click **New** again.
 - d. From the **Type** drop-down list, select **Application**.
 - e. From the **Source** drop-down list, select **SQL Server**.

- f. Click **Save**.

Add Windows Agent Monitor Template

Generic Monitor **Event** UEBA User Log FIM Change Script Certificate Monitoring Osquery

File Log: ☐ IIS ☐ DHCP

Event Log: Lines: 2

Type	Include Event	Exclude Event
Security	All Events	
Application/SQL Server	All Events	

Step 2: Associate Windows Agents to Templates

Complete these steps to associate a Host to Template:

- Under **Host To Template Associations**, click **New**.
- In the **Host To Template Associations** dialog box, enter the following information.

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.

- Associate the recently added SQL Server template to SQL server host.

4. Click **Save and Apply**.

Step 3: Check Events via Analytics

To check for events, take the following steps.

1. Navigate to **Analytics**.
2. Click inside the **Edit Filters and Time Range...** field.
3. Create a search, such as the example in the following table:

Attribute	Operator	Value
Reporting IP	=	<IP address of server>
Organization ID	=	<Org ID where server resides>

4. Set the **Time Range**, for example 1 Day.
5. Click **Apply & Run**.

JDBC Configuration for Database Performance Metrics

FortiSIEM can pull SQL Server performance metrics via JDBC.

Configuration occurs in two parts.

- [SQL Server Configuration](#)
- [FortiSIEM Configuration](#)

SQL Server Configuration

Step 1: Create a Read-Only User for SQL Server Monitoring

A regular Windows account cannot be used for SQL Server monitoring. FortiSIEM runs on Linux and certain Windows libraries needed for SQL Server monitoring are not available on Linux. You have to create a separate user with read-only privileges.

1. Log in to your SQL Server with sa account, and then create a read-only user to access system tables.

```
EXEC SP_ADDLOGIN 'AOPerfLogin','ProspectHills!','master';
EXEC SP_ADDROLE 'AOPerfRole';
EXEC SP_ADDUSER 'AOPerfLogin', 'AOPerfUser', 'AOPerfRole';
GRANT VIEW SERVER STATE TO AOPerfLogin;
GRANT SELECT ON dbo.sysperfinfo TO AOPerfRole;
GRANT EXEC on xp_readerrorlog to AOPerfRole;
```

2. Log in with your newly created read-only account (AOPerfLogin) and run these commands.

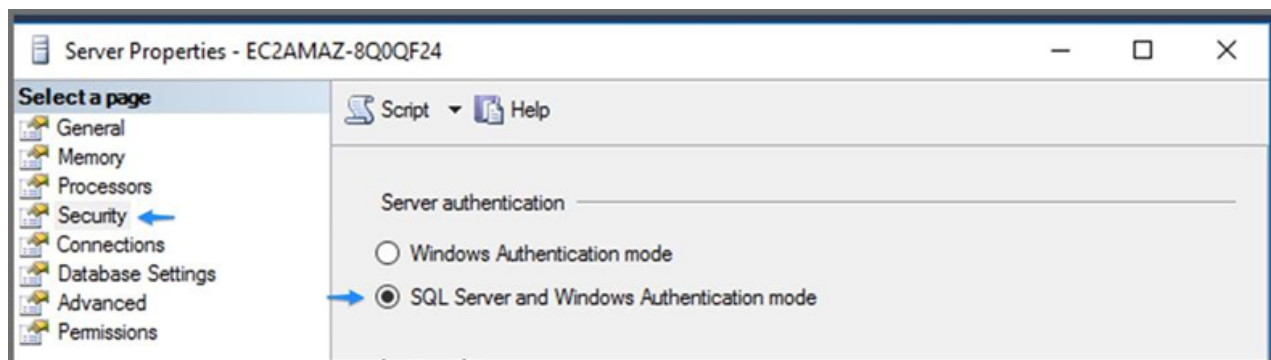
```
SP_WHO2 'active';
SELECT * FROM sys.databases; SELECT * FROM dbo.sysperfinfo;
SELECT COUNT(*) as count FROM sysprocesses GROUP BY loginame;
```


Check to see if you get the same results with your read-only account (AOPerfLogin) as you do with your sa account. You should get the same results.

Step 2: Changing Authentication mode to SQL Server and Windows Authentication Mode

It is common practice to enable SQL Server and Windows Authentication mode before accessing read-only user. To enable this mode, take the following steps:

1. In **SQL Server Management Studio Object Explorer**, right click the server, then click **Properties**.
2. On the **Security** page, under **Sever authentication**, select **SQL Server and Windows Authentication mode**.



3. Click **OK**.
4. In the **SQL Server Management Studio** dialog box, click **OK** to acknowledge the requirement to **restart** the SQL Server.
5. In **Object Explorer**, right click your server, and then click **Restart**. If the SQL Server Agent is running, it must also be restarted.

FortiSIEM Configuration

Settings for SQL Server JDBC Access Credentials for Performance Monitoring

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your SQL Server over JDBC for performance monitoring:

Step 1: Create a Separate Credential for Each Database Instance

If multiple database instances are running on the same server, then each instance must run on a separate port, and you must create a separate access credential for each instance. You must also remember to associate each instance with the server's IP number for the **Device Credential Mapping Definition**.

Take the following steps:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the **Access Method Definition** dialog box and click **Save** when done:

c.

Setting	Value
Name	The name of the database instance you're creating the credential for.
Access Protocol	JDBC
Used For	Performance Monitoring
Pull Interval (minutes)	5
Port	1433
Database Name	<leave this field blank>
User Name	The user you created in step 1 of the JDBC configuration.
Password	The password associated with the user you created in step 1.

Access Method Definition

Name:

SQL-Performance

Device Type:

Microsoft SQL Server

Access Protocol:

JDBC

Authentication:

SQL Server Authentication

Used For:

Performance Monitoring

Pull Interval:

5

Minute(s)

Port:

1433

Database Name:

User Name:

AQPerfLogin

Password:

Confirm Password:

Description:

Save

Cancel

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Select the name of your credential from the **Credentials** drop-down list.
 - b. In the **IP/Host Name** field, enter a host name, an IP, or an IP range.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the Microsoft SQL Server.
5. To discover the device, take the following steps:
 - a. Navigate to **ADMIN > Setup > Discovery**.
 - b. Create a Discovery entry using the information here. For more information on how to create a discovery entry, see [here](#).

Setting	Value
Name	The name of the device to discover
Discovery Type	Leave as default (Range Scan).
Include	Provide the IP address of the device you want discovered.

- c. Click **Save** when done.

Discovery Definition

Name: MSSQL

Discovery Type: Range Scan

Include: 172.30.56.124

Exclude:

Include Types: ALL

Exclude Types: NONE

Name Resolution: ☐ DNS first ☒ SNMP/WMI first

Options:

Save Cancel

6. Select the discovery entry you created and click **Discover**.
7. After Discovery is completed, navigate to **ADMIN > Setup > Monitor Performance** to check the monitor performance job.

FortiSIEM DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES TASKS ADMIN

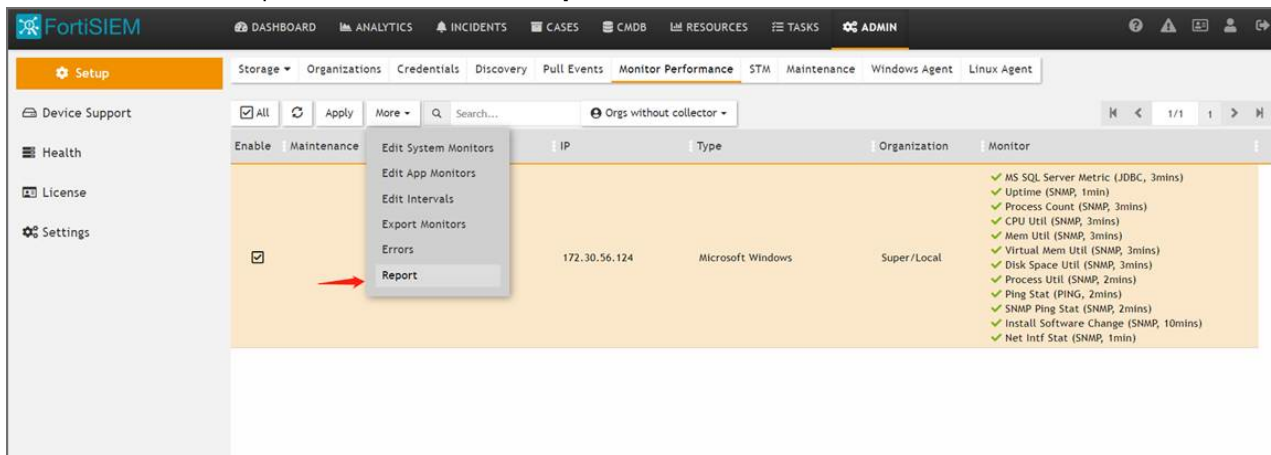
Setup Organizations Credentials Discovery Pull Events **Monitor Performance** STM Maintenance Windows Agent Linux Agent

Device Support Health License Settings

Enable Maintenance Device IP Type Organization Monitor

Enable	Maintenance	Device	IP	Type	Organization	Monitor
☒		CP-2019-234	172.30.56.124	Microsoft Windows	Super/Local	✓ MS SQL Server Metric (JDBC, 3mins) ✓ Uptime (SNMP, 1min) ✓ Process Count (SNMP, 3mins) ✓ CPU Util (SNMP, 3mins) ✓ Mem Util (SNMP, 3mins) ✓ Virtual Mem Util (SNMP, 3mins) ✓ Disk Space Util (SNMP, 3mins) ✓ Process Util (SNMP, 2mins) ✓ Ping Stat (PING, 2mins) ✓ SNMP Ping Stat (SNMP, 2mins) ✓ Install Software Change (SNMP, 10mins) ✓ Net Intf Stat (SNMP, 1min)

8. Click on the **More** drop-down list and select **Report** to check related events.



JDBC Configuration for DDL Changes

FortiSIEM can pull SQL Server Data Definition Language (DDL) changes via JDBC. These changes include CREATE, ALTER, DROP, GRANT, DENY, REVOKE or UPDATE STATISTICS operations on database tables. This information is not naturally generated by a SQL Server. Hence, this involves creating database tables to store them and then creating triggers to populate those tables. Then FortiSIEM can pull them via JDBC.

Configuration occurs in two parts.

- [SQL Server Configuration](#)
- [FortiSIEM Configuration](#)

SQL Server Configuration

1. Save the SQL Server script (provided – link [here](#)) as separate file to **My Documents > SQL Server Management Studio > SQLServer_DDL_Events.sql**.
2. Login to SQL Server Management Studio with *sa* account.
3. Browse to and execute the **SQLServer_DDL_Events.sql** script to create the database, tables and trigger events.

Creating a Database Truncate Script

Since DDL tables grow after time, it is often a good idea to create a database truncate script that can run as a maintenance task and keep the table size under control. It is often necessary to create a database truncate procedure as follows.

1. Log into Microsoft SQL Management Studio and connect to the DB instance.
2. Under **Management**, go to **Maintenance Plans**, and create a new plan with the name **RemoveOldLogs**.
3. For **Subplan**, enter **TRUNCATE**, and for **Description**, enter **TRUNCATE TABLE**.
4. Click the **Calendar** icon to create a recurring, daily task starting at 12:00AM and running every 30 minutes until 11:59:59PM.

5. Go to **View > Tool Box > Execute T-SQL Statement**. A T-SQL box will be added to the subplan.
6. In the T-SQL box, enter this command

```
use PH_Events;  
EXEC sp_MSForEachTable 'TRUNCATE TABLE DDLEvents';
```
7. Click **OK**.

You will be able to see the history of this script's actions by right-clicking on the maintenance task, and then selecting **View History**.

FortiSIEM Configuration

Settings for SQL Server JDBC Access Ccredentials for DDL Events Collection

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your SQL Server database instance over JDBC for database DDL events collection.

Step 1: Create a Separate Credential for Each Database Instance

If multiple database instances are running on the same server, then each instance must run on a separate port, and you must create a separate access credential for each instance. You must also remember to associate each instance with the server's IP number for the **Device Credential Mapping Definition**.

Take the following steps:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the **Access Method Definition** dialog box, and click **Save** when done:

Setting	Value
Name	The name of the database instance you are creating the credential for
Device Type	Microsoft SQL Server
Used For	Audit
Pull Interval (minutes)	5
Port	1433
Database Name	<leave this field blank>
Logon Event Table	PH_Events.dbo.LogOnEvents
DDL Event Table	PH_Events.dbo.DDLEvents
User Name	The user you created in step 1 of the JDBC configuration

Setting	Value
Password	The password associated with the user you created in step 1.

Access Method Definition

Name:

SQL-Audit

Device Type:

Microsoft SQL Server

Access Protocol:

JDBC

Authentication:

Used For:

Audit

Pull Interval:

5

Minute(s)

Maximum Records:

1000

Port:

1433

Database Name:

Logon Event Table:

PH_Events.dbo.LogonEvents

DDL Event Table:

PH_Events.dbo.DDLEvents

User Name:

AOPerfLogin

Password:

.....

Confirm Password:

.....

Description:

Save

Cancel

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Select the name of your credential from the **Credentials** drop-down list.
 - b. In the **IP/Host Name** field, enter a host name, an IP, or an IP range.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the Microsoft SQL Server.
5. To discover the device, take the following steps:
 - a. Navigate to **ADMIN > Setup > Discovery**.
 - b. Create a Discovery entry using the information here. For more information on how to create a discovery entry, see [here](#).

Setting	Value
Name	The name of the device to discover
Discovery Type	Leave as default (Range Scan).
Include	Provide the IP address of the device you want discovered.

- c. Click **Save** when done.

Discovery Definition

Name: MSSQL

Discovery Type: Range Scan

Include: 172.30.56.124

Exclude:

Include Types: ALL

Exclude Types: NONE

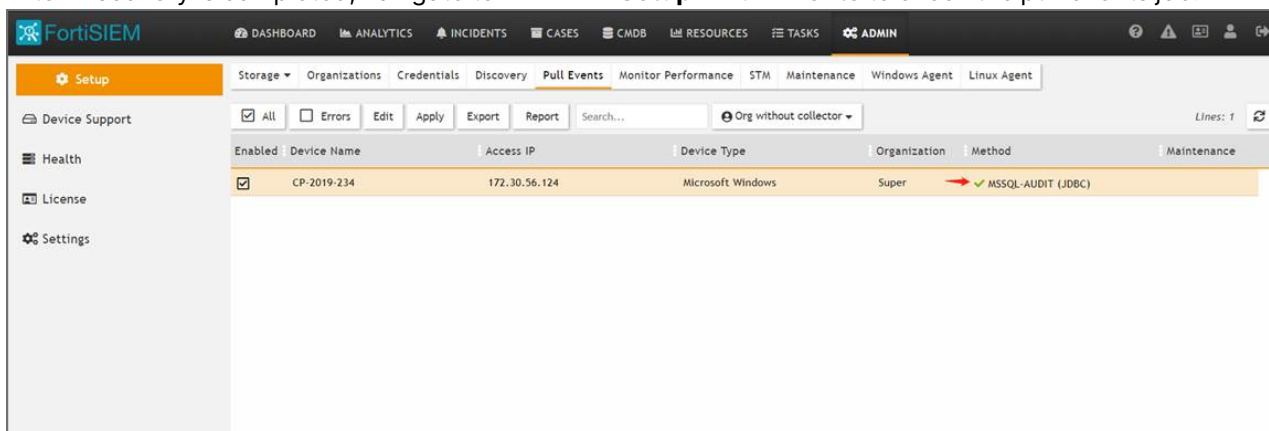
Name Resolution: ☐ DNS first ☒ SNMP/WMI first

Options:

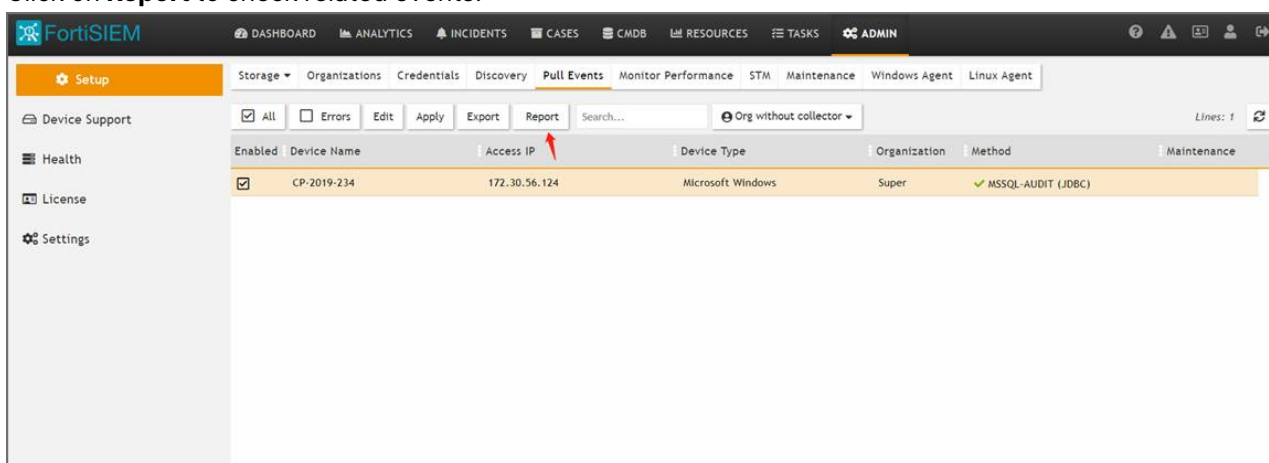
Save Cancel

6. Select the discovery entry you created and click **Discover**.

7. After Discovery is completed, navigate to **ADMIN > Setup > Pull Events** to check the pull events job.



8. Click on **Report** to check related events.



Sample Events

- Per Instance Performance Metrics
- Per Instance, per Database Performance Metrics
- Generic Info
- Config Info
- Locking Info
- Blocking Info
- Error Log
- Logon Events
- DDL Events - Create Database
- DDL Events - Create Index

Per Instance Performance Metrics

```
<134>Apr 16 10:17:56 172.16.22.100 java: [PH_DEV_MON_PERF_MSSQL_SYS|PH_DEV_MON_PERF_MSSQL_SYS]:
[eventSeverity]=PHL_INFO,[hostIpAddr]=172.16.22.100,[hostName]=wwwin.example.net,
[appGroupName]=Microsoft SQL Server,[dbDataFileSizeKB]=13149056,[dbLogFileUsedKB]=26326,
[dbLogGrowthCount]=4,[dbLogShrinkCount]=0,[dbLogFlushPerSec]=1.69,[dbTransPerSec]=4.44,
[dbDeadLocksPerSec]=0,[dbLogCacheHitRatio]=60.01,[dbUserConn]=16,[dbTargetServerMemoryKB]=1543232,
[dbTotalServerMemoryKB]=1464760,[dbPageSplitsPerSec]=0.45,
[dbPageWritesPerSec]=0.01,[dbLatchWaitsPerSec]=0.77,[dbPageReadsPerSec]=0.01,
[dbFullScansPerSec]=1.83,[dbBufferCacheHitRatio]=100,[dbCount]=8,[dbUserCount]=25,
[dbLoggedinUserCount]=2,[dbPagesInBufferPool]=116850,[dbPagesFreeInBufferPool]=2336,
[dbAverageWaitTimeMs]=239376,
[appVersion]=Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64),[serverName]=WIN-08-VCENTER,
[instanceName]=MSSQLSERVER,[appPort]=1433
```

Per Instance, per Database Performance Metrics

```
[PH_DEV_MON_PERF_MSSQL_PERDB]:[eventSeverity]=PHL_INFO,[hostIpAddr]=172.16.22.100,
[hostName]=wwwin.example.net,[dbName]=tempdb,[appGroupName]=Microsoft SQL Server,
[dbDataFileSizeKB]=109504,[dbLogFileUsedKB]=434,[dbLogGrowthCount]=4,[dbLogShrinkCount]=0,
[dbTransPerSec]=0.96,[dbLogFlushPerSec]=0.01,[dbLogCacheHitRatio]=44.44,
[appVersion]=Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64),[serverName]=WIN-08-VCENTER,
[instanceName]=MSSQLSERVER,[appPort]=1433
```

Generic Info

```
[PH_DEV_MON_PERF_MSSQL_GEN_INFO]:[eventSeverity]=PHL_INFO,[dbName]= tempdb,[dbSize]= 3.0,
[dbowner]= sa,[dbId]= 2,[dbcreated]= 1321545600,
[dbstatus]= Status=ONLINE; Updateability=READ_WRITE; UserAccess=MULTI_USER; Recovery=SIMPLE;
Version=655; Collation=SQL_Latin1_General_CP1_CI_AS; SQLSortOrder=52; IsAutoCreateStatistics;
IsAutoUpdateStatistics,
[dbcompatibilityLevel]= 100,[spaceAvailable]= 0.9,[appVersion]= Microsoft SQL Server 2008 (RTM) -
10.0.1600.22 (Intel X86),[serverName]= WIN03MSSQL\SQLEXPRESS
```

Config Info

```
[PH_DEV_MON_PERF_MSSQL_CONFIG_INFO]:[eventSeverity]=PHL_INFO,[configureName]= user instances
enabled,[configMinimum]= 0,[configMaximum]= 1,[dbConfigValue]= 1,
[configRunValue]= 1,[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86),
[serverName]= WIN03MSSQL\SQLEXPRESS
```

Locking Info

```
[PH_DEV_MON_PERF_MSSQL_LOCK_INFO]:[eventSeverity]=PHL_INFO,[dbId]= 4,[objId]= 1792725439,
[lockType]= PAG,[lockedResource]= 1:1256,[lockMode]= IX,
[lockStatus]= GRANT,[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86),
[serverName]= WIN03MSSQL\SQLEXPRESS
```

Blocking Info

```
[PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO]:[eventSeverity]=PHL_INFO,[blockedSpId]= 51,
[blockedLoginUser]= WIN03MSSQL\Administrator,[blockedDbName]= msdb,
[blockedCommand]= UPDATE,[blockedProcessName]= Microsoft SQL Server Management Studio - Query,
[blockingSpId]= 54,[blockingLoginUser]= WIN03MSSQL\Administrator,
[blockingDbName]= msdb,[blockingCommand]= AWAITING COMMAND,[blockingProcessName]= Microsoft SQL
Server Management Studio - Query,[blockedDuration]= 5180936,
[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86),[serverName]=
WIN03MSSQL\SQLEXPRESS
```

Error Log

```
[PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO]:[eventSeverity]=PHL_INFO,[logDate]= 1321585903,
[processInfo]= spid52,[logText]= Starting up database 'ReportServer$SQLEXPRESSTempDB'. ,
[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86),[serverName]=
WIN03MSSQL\SQLEXPRESS
```

Logon Events

```
134>Feb 08 02:55:34 10.1.2.54 java: [MSSQL_Logon_Success]:[eventSeverity]=PHL_INFO,
[eventTime]=2014-02-08 02:54:00.977, [rptIp]=10.1.2.54, [relayIp]=10.1.2.54, [srcName]=<local
machine>, [user]=NT SERVICE\ReportServer$MSSQLSERVER$JIANFA, [srcApp]=Report Server,
[instanceName]=MSSQLSERVER$JIANFA, [procId]=52, [loginType]=Windows (NT) Login,
[securityId]=AQYAAAAAAVQAAAAALJAZf5XMbcLh8PUDY31LioZ3Uwo=, [isPooled]=1, [destName]=WIN-
S2EDLFIUPQK, [destPort]=1437,
```

DDL Events - Create Database

```
<134>Sep 29 15:34:48 10.1.2.54 java: [MSSQL_Create_database]:[eventSeverity]=PHL_INFO,
[eventTime]=2013-09-29 15:34:05.687, [rptIp]=10.1.2.54, [relayIp]=10.1.2.54, [user]=WIN-
S2EDLFIUPQK\Administrator, [dbName]=JIANFA, [instanceName]=MSSQLSERVER, [objName]=, [procId]=59,
[command]=CREATE DATABASE JIANFA, [destName]=WIN-S2EDLFIUPQK, [destPort]=1433,
```

DDL Events - Create Index

```
<134>Sep 29 15:34:48 10.1.2.54 java: [MSSQL_Create_index]:[eventSeverity]=PHL_INFO,
[eventTime]=2013-09-29 15:30:40.557, [rptIp]=10.1.2.54, [relayIp]=10.1.2.54, [user]=WIN-
S2EDLFIUPQK\Administrator, [dbName]=master, [instanceName]=MSSQLSERVER, [objName]=IndexTest,
[procId]=58, [command]=create index IndexTest on dbo.MSreplication_options(optname);,
[schemaName]=dbo, [objType]=INDEX, [destName]=WIN-S2EDLFIUPQK, [destPort]=1433
```

MySQL Server

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.5.0

Supported Versions: :

- MySQL 5.7 and earlier
- MySQL 8.0

Vendor: Oracle

Product Information: <https://www.mysql.com/products/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
JDBC		Generic database information: Version, Character Setting	
JDBC		Database performance metrics: User Connections, Table Updates, table Selects, Table Inserts, Table Deletes, Temp Table Creates, Slow Queries, Query cache Hits, Queries registered in cache, Database Questions, Users, Live Threads	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Table space performance metrics: Table space name, table space type, Character set and Collation, table space usage, table space free space, Database engine, Table version, Table Row Format, Table Row Count, Average Row Length, Index File length, Table Create time, Table Update Time	
JDBC	None	Database audit trail: Successful and failed database log on, Database CREATE/DELETE/MODIFY operations, Table CREATE/DELETE/MODIFY/INSERT operations	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "mysql" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "mysql" in the main content panel **Search...** field to see the rules associated with this application or device.

Reports

In **RESOURCES > Reports**, search for ""mysql" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- [SNMP](#)
- [JDBC for Database Auditing - MySQL Server](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

JDBC for Database Auditing - MySQL Server

You must configure your MySQL Server to write audit logs to a database table. [This topic in the MySQL documentation](#) explains more about how to set the destination tables for log outputs.

Take the following steps based on your version of Linux:

1. If the binary `bin/mysqld_safe` exists in your version of Linux, run the following command and proceed to step 2:

```
bin/mysqld_safe --user=mysql --log-output=TABLE &
```

If the binary `bin/mysqld_safe` does not exist in your version of Linux, then take the following step based on the version of MySQL being used, then proceed to step 2.

Note: Some Linux variants that use `systemd`, for example, CentOS, do not contain `bin/mysqld_safe`.

For MySQL 5.7 and earlier, add the following into `/etc/my.cnf`.

```
log-output=TABLE
```

For MySQL 8.0 and later, add the following into `/etc/my.cnf.d/mysql-server.cnf`.

```
log-output=TABLE
```

2. Login to MySQL, and run the following SQL commands to enable `general.log` in MyISAM.

```
SET @old_log_state = @@global.general_log;
SET GLOBAL general_log = 'OFF';
ALTER TABLE mysql.general_log ENGINE = MyISAM;
SET GLOBAL general_log = @old_log_state;
SET GLOBAL general_log = 'ON';
```

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#). Use the settings in [Settings for MySQL Server JDBC Access Credentials for Database Auditing](#) to set up MySQL Audit.

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Settings for MySQL Server JDBC Access Credentials for Performance Monitoring](#)
- [Settings for MySQL Server JDBC Access Credentials for Database Auditing](#)
- [Settings for MySQL Server JDBC Access Credentials for Synthetic Transaction Monitoring, Short Audit, McAfee VulnMgr](#)

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP

Setting	Value
Community String	<your own>

Settings for MySQL Server JDBC Access Credentials for Performance Monitoring

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your MySQL Server over JDBC for performance monitoring:

Setting	Value
Name	MySQL-Performance-Monitoring
Device Type	Oracle MySQL
Access Protocol	JDBC
Used For	Performance Monitoring
Pull Interval (minutes)	5
Port	3306
User Name	The administrative user for the database server
Password	The password associated with the administrative user

Settings for MySQL Server JDBC Access Credentials for Database Auditing

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your MySQL Server over JDBC for database auditing:

Setting	Value
Name	MySQL-Audit
Device Type	Oracle MySQL
Access Protocol	JDBC
Used For	Audit
Pull Interval (minutes)	5
Port	3306
Database Name	<database name> (MySQL)
Audit Table	general_log

Setting	Value
User Name	The administrative user for the database server
Password	The password associated with the administrative user

Settings for MySQL Server JDBC Access Credentials for Synthetic Transaction Monitoring, Snort Audit, McAfee VulnMgr

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your MySQL Server over JDBC for Synthetic Transaction Monitoring, Snort Audit, or McAfee VulnMgr:

Setting	Value
Name	<name>
Device Type	Oracle MySQL
Access Protocol	JDBC
Used For	Synthetic Transaction Monitoring, Snort Audit, or McAfee VulnMgr
Pull Interval (minutes)	5
Port	3306
Database Name	<database name>
User Name	The administrative user for the database server
Password	The password associated with the administrative user

Sample Events

- [System Level Performance Metrics](#)
- [Table Space Performance Metrics](#)
- [Logon/Logoff Events](#)
- [Database CREATE/DELETE/MODIFY Events](#)
- [Table CREATE/DELETE/MODIFY Events](#)

System Level Performance Metrics

```
<134>Apr 21 19:06:07 10.1.2.8 java: [PH_DEV_MON_PERF_MYSQLDB]: [eventSeverity]=PHL_INFO, [hostIpAddr]=172.16.22.227, [hostName]=MYSQL, [appGroupName]=MySQL Database Server, [appVersion]=MySQL 5.6.11, [charSetting]=utf8, [dbConnections]=24, [dbComUpdate]=0,
```



```
[dbComSelect]=1, [dbComInsert]=0,
[dbComDelete]=0, [dbCreatedTmpTables]=0, [dbSlowQueries]=0, [dbQcacheHits]=0,
[dbQcacheQueriesInCache]=0,
[dbQuestions]=7, [dbThreadsConnected]=1, [dbThreadsRunning]=1
```

Table Space Performance Metrics

```
<134>Apr 29 10:06:07 172.16.22.227 java: [PH_DEV_MON_PERF_MYSQLDB_TABLESPACE]:
[eventSeverity]=PHL_INFO, [appGroupName]=MySQL Database Server,
[instanceName]=mysql, [tablespaceName]=general_log, [tablespaceType]=PERMANENT,
[tablespaceUsage]=0.01, [tablespaceFreeSpace]=4193886,
[dbEngine]=MyISAM, [tableVersion]=10, [tableRowFormat]=dynamic, [tableRows]=124,
[tableAvgRowLength]=80, [tableIndexLength]=1024,
[tableCreateTime]=2013-04-29 15:12:30, [tableUpdateTime]=2013-04-29 12:35:46,
[tableCollation]=utf8_general_ci
```

Logon/Logoff Events

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Logon_Success]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [logonTime]=2013-04-29 15:14:54, [logoffTime]=,
[actionName]=Connect, [msg]=admin@172.16.22.227 on
```

```
<134>Apr 10 14:29:22 abc-desktop java: [MYSQL_Logoff]: [eventSeverity]=PHL_INFO, [eventTime]=2013-
04-10 14:29:22, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [logonTime]=, [logoffTime]=2014-04-10 14:29:22,
[actionName]=quit, [msg]=
```

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Logon_Fail]: [eventSeverity]=PHL_WARN,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [logonTime]=2013-04-29 15:14:54, [logoffTime]=,
[actionName]=Connect,
[msg]=Access denied for user 'admin'@'172.16.22.227' (using password: YES)
```

Database CREATE/DELETE/MODIFY Events

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Create_database]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=create database sliutest
```

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Drop_database]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=drop database sliutest
```

Table CREATE/DELETE/MODIFY Events

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Create_table]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
```

```
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=CREATE TABLE tutorials_tbl(  
tutorial_id INT NOT NULL AUTO_INCREMENT,  
tutorial_title VARCHAR(100) NOT NULL,      tutorial_author VARCHAR(40) NOT NULL,      submission_  
date DATE,      PRIMARY KEY ( tutorial_id )      )
```

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Delete_table]: [eventSeverity]=PHL_INFO,  
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,  
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=DELETE FROM tutorials_tbl WHERE  
tutorial_id=2NOT NULL,  
tutorial_author VARCHAR(40) NOT NULL,      submission_date DATE,      PRIMARY KEY ( tutorial_id )
```

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Insert_table]: [eventSeverity]=PHL_INFO,  
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,  
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=INSERT INTO tutorials_tbl  
(tutorial_title, tutorial_author, submission_date)  
VALUES      ("Learn Java", "John Smith", NOW())
```

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Drop_table]: [eventSeverity]=PHL_INFO,  
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,  
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=DROP table sliutable
```

Oracle Database Server

Support Added: 4.7.2

Last Modification: 7.3.0

Vendor: Oracle

Product Information: <https://www.oracle.com/database/technologies/>

Supported Versions

- Oracle Database 21c
- Oracle Database 18/19c

Note: FortiSIEM does not support Oracle 12.1 or earlier versions through JDBC discovery.

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring
Agent or OMI	Application type, service mappings	Process level metrics: uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
JDBC		Generic database information: version, Character Setting, Archive Enabled, Listener Status, Instance Status, Last backup date	
JDBC		Database performance metrics: Buffer cache hit ratio, Row cache hit ratio, Library cache hit ratio, Shared pool free ratio, Wait time ratio, Memory Sorts ratio, Host CPU Util ratio, CPU Time ratio, Disk Read/Write rates (operations and MBps), Network I/O Rate, Enqueue Deadlock rate, Database Request rate, User Transaction rate, User count, Logged on user count, Session Count, System table space usage, User table space usage, Temp table space usage, Last backup date, Days since last backup Table space performance metrics: Table space name, table space type, table space usage, table space free space, table space next extent	Performance Monitoring
Syslog		Listener log, Alert log, Audit Log	

Protocol	Information discovered	Metrics collected	Used for
JDBC	None	Database audit trail: Successful and failed database logon, Various database operation audit trail including CREATE/ALTER/DROP/TRUNCATE operations on tables, table spaces, databases, clusters, users, roles, views, table indices, triggers etc.	Security Monitoring

Configuring SNMP for Database Process Performance Monitoring

Configuration

For Microsoft Windows: See [Microsoft Windows Server via SNMP, WMI, OMI - SNMP Configuration](#)

For Linux: See these references:

- [Linux Server - SNMP v1 and v2c Configuration](#)
- [Linux Server - SNMP v3 Configuration](#)

Important Events

Type	Event Type	Description
Database Process Performance Monitoring	PH_DEV_MON_PROC_RESOURCE_UTIL	Process CPU and Memory Utilization stats including database processes

Configuring Agent or OMI for Database Process Performance Monitoring

Configuration

For Windows Agent Based Deployments: See [Microsoft Windows Server via Agent - Configuring Discovery and Performance Monitoring](#)

For Agentless Deployments: See [Microsoft Windows Server via SNMP, WMI, OMI - SNMP Configuration](#)

Important Events

Type	Event Type	Description
Database Process Performance Monitoring	PH_DEV_MON_PROC_RESOURCE_UTIL	Process CPU and Memory Utilization stats including database processes

Configuring JDBC for Database Performance Monitoring

Configuring Oracle

To configure your Oracle Database Server for performance monitoring by FortiSIEM, you must create a read-only user who has select permissions for the database. This is the user you will use to create the access credentials in FortiSIEM to communicate with your database server.

Note: FortiSIEM does not support Oracle 12.1 or earlier versions through JDBC discovery.

1. Open the SQLPlus application.
2. Log in with a system-level account.
3. Connect to your instance as sysdba.

```
SQL> conn / as sysdba;
```

4. Create a non-admin user account. (**Note:** If you already created the phoenix_agent user, you can skip this step.)

```
SQL> create user phoenix_agent identified by "fortisiem";
```

5. Assign permissions to the user.

```
grant select on dba_objects to phoenix_agent;
grant select on dba_tablespace_usage_metrics to phoenix_agent;
grant select on dba_tablespaces to phoenix_agent;
grant select on nls_database_parameters to phoenix_agent;
grant select on v_$backup_set to phoenix_agent;
grant select on v_$instance to phoenix_agent;
grant select on v_$parameter to phoenix_agent;
grant select on v_$session to phoenix_agent;
grant select on v_$sql to phoenix_agent;
grant select on v_$sysmetric to phoenix_agent;
grant select on v_$version to phoenix_agent;
grant select on gv_$session to phoenix_agent;
grant select on gv_$service_stats to phoenix_agent;
```

6. Verify that the permissions were successfully assigned to the user.

```
select count(*) from dba_objects;
select count(*) from dba_tablespace_usage_metrics;
select count(*) from dba_tablespaces;
select count(*) from gv$service_stats;
select count(*) from nls_database_parameters;
select count(*) from v$backup_set order by start_time desc;
select count(*) from v$instance;
select count(*) from v$parameter;
select count(*) from v$session;
select count(*) from v$sql;
select count(*) from v$sysmetric;
select count(*) from v$version;
```

Configuring FortiSIEM

Follow these steps:

1. Go to **Admin > Setup > Credentials**.
2. Under **Step 1: Enter Credentials**, create a credential by taking the following steps.
 - a. Click **New**.
 - b. In the **Name** field, enter the name for this credential.
 - c. From the **Device Type** drop-down list, select **Oracle Database Server**.
 - d. From the **Access Protocol** drop-down list, select **JDBC**.
 - e. Set **Pull Interval**. The default and recommended interval is 5 minutes.
 - f. From the **Used For** drop-down list, select **Performance Monitoring**.
 - g. In the **Port** field, enter the JDBC port number on Oracle (default 1521).
 - h. In the **Instance Name** field, enter the Oracle instance name.
 - i. In the **User Name** field, enter the username used to connect to the Oracle instance using JDBC.
 - j. In the **Password** and **Confirm Password** fields, enter the password associated with the username.
 - k. (Optional) In the **Description** field, enter any information about the credential.
 - l. Click **Save**.
3. Under **Step 2: IP Range to Credential Association**, create an association for the newly created credential by taking the following steps:
 - a. Click **New**.
 - b. In the **IP/IP Range** field, enter the IP address of the Oracle database instance.
 - c. From the **Credentials** drop-down list, select the Credential created earlier (the Credential name was configured in Step 2b).
 - d. Click **Save**.
4. Start Test Connectivity by taking the following steps.
 - a. Select the association entry you created under **Step 2: IP Range to Credential Association**.
 - b. Click the **Test** drop-down list, and select **Test Connectivity**.
 - c. If Test Connectivity fails, then fix the credential and run Test Connectivity again. If Test Connectivity succeeds, then move to next step.
5. Start Discovery
 - a. Go to **Admin > Setup > Discovery**.
 - b. If there is an entry for the Oracle Database Server IP, then select the entry and click **Discover**.
 - c. Once Discovery succeeds
 - i. A CMDB entry for the server will be created in **CMDB > Devices**.
 - ii. A database performance monitoring job will be created in **Admin > Setup > Monitor Performance**.
6. Performance monitoring will now begin.

Important Events

Type	Event Type	Description
Database Process Performance Monitoring	PH_DEV_MON_PERF_ORADB	Oracle database performance metrics
	PH_DEV_MON_PERF_ORADB_TABLESPACE	Oracle tablespace metrics

Type	Event Type	Description
	PH_DEV_MON_PERF_ORADB_TOP_QUERIES	Top queries against Oracle database

System Reports

- Performance: Top Oracle Databases by buffer ratios
- Performance: Top Oracle Databases by database I/O
- Performance: Top Oracle Databases by network I/O
- Performance: Top Oracle Databases by table space usage
- Performance: Top Oracle Databases by users and sessions
- Performance: Top Oracle Databases by user transactions
- Performance: Top Oracle Databases by wait times
- Performance: Top Oracle Queries by completion time

Configuring JDBC for Database Audit Trail

This section covers Oracle database audit log (unified audit trail) collection via JDBC.

Configuring Oracle

Follow these steps

1. Make sure that these environment variables are set.
ORACLE_BASE= C:\oracle
2. Enable auditing by modifying the Oracle instance initialization file `init.ora.$ID`. This is typically located in `$ORACLE_BASE/admin/<service_name>/pfile` where `service_name` is the Oracle service name:
AUDIT_TRAIL = DB
or
AUDIT_TRAIL = true
3. Create a user account (`phoenix_agent`) and grant select privileges to that user.
su - oracle
sqlplus /nolog
conn / as sysdba
create user phoenix_agent identified by "phoenix_agent_pwd";
4. If you encounter the error "ORA-65096: invalid common user or role name in oracle", then create phoenix_agent user using the following alternative steps:
su - oracle
sqlplus /nolog
conn / as sysdba
alter session set "_ORACLE_SCRIPT"=true;
create user phoenix_agent identified by "phoenix_agent_pwd";
5. Assign permissions to the phoenix_agent user by running the following commands.

```
grant connect to phoenix_agent;  
grant create session to phoenix_agent;  
grant select on unified_audit_trail to phoenix_agent;  
grant select on gv_$session to phoenix_agent;
```

6. Turn on auditing by running the following commands.

```
su - oracle  
sqlplus /nolog  
conn / as sysdba;  
audit session;  
quit;
```

7. Fetch the audit data to make sure the configuration was successful.

```
su - oracle;  
sqlplus phoenix_agent/phoenix_agent_pwd;  
select count (*) from unified_audit_trail;
```

You should see the count changing after logging on a few times.

Configuring FortiSIEM

Follow these steps:

1. Go to **Admin > Setup > Credentials**.
2. Under **Step 1: Enter Credentials**, create a credential by taking the following steps.
 - a. Click **New**.
 - b. In the **Name** field, enter the name for this credential.
 - c. From the **Device Type** drop-down list, select **Oracle Database Server**.
 - d. From the **Access Protocol** drop-down list, select **JDBC**.
 - e. Set **Pull Interval**. The default and recommended interval is 5 minutes.
 - f. From the **Used For** drop-down list, select **Audit**.
 - g. In the **Port** field, enter the JDBC port number on Oracle (default 1521).
 - h. In the **Instance Name** field, enter the Oracle instance name.
 - i. In the **Audit Trail Table** field, enter "unified_audit_trail".
 - j. In the **User Name** field, enter "phoenix_agent" (This user was created earlier in [Configuring Oracle](#) (created in step 3 or step 4).
 - k. In the **Password** and **Confirm Password** fields, enter the password associated with the user phoenix_agent created earlier in [Configuring Oracle](#) (created in step 3 or step 4).
 - l. (Optional) In the **Description** field, enter any information about the credential.
 - m. Click **Save**.
3. Under **Step 2: IP Range to Credential Association**, create an association for the newly created credential by taking the following steps:
 - a. Click **New**.
 - b. In the **IP/IP Range** field, enter the IP address of the Oracle database instance.
 - c. From the **Credentials** drop-down list, select the Credential created earlier (the Credential name was configured in step 2b).
 - d. Click **Save**.

4. Start Test Connectivity by taking the following steps.
 - a. Select the association entry created under **Step 2: IP Range to Credential Association**.
 - b. Click the **Test** drop-down list, and select **Test Connectivity**.
 - c. If Test Connectivity fails, then fix the credential and run Test Connectivity again. If Test Connectivity succeeds, then move to next step.
5. Start Discovery
 - a. Go to **Admin > Setup > Discovery**.
 - b. If there is an entry for the Oracle Database Server IP, then select the entry and click **Discover**.
 - c. Once Discovery succeeds
 - i. A CMDB entry for the server will be created in **CMDB > Devices**.
 - ii. A database event pulling job will be created in **Admin > Setup > Pull Events**.
6. Performance monitoring will now begin.

Important Events

Type	Event Type	Description
Database Audit	ORADB_Logon_Success	Oracle database logon successful
	ORADB_Logon_Failure	Oracle database logon failure
	ORADB_Create_table	Oracle Database table created
	ORADB_Alter_table	Oracle Database table altered
	ORADB_Drop_table	Oracle Database table dropped
	ORADB_Truncate_table	Oracle Database table truncated
	ORADB_Create_tablespace	Oracle Database table space created
	ORADB_Alter_tablespace	Oracle Database table space altered
	ORADB_Drop_tablespace	Oracle Database table space dropped
	ORADB_Create_database	Oracle Database created
	ORADB_Alter_database	Oracle Database altered
	ORADB_Create_user	Oracle Database user created
	ORADB_Drop_user	Oracle Database user dropped
	ORADB_Alter_user	Oracle Database user altered

Other events can be found by searching ORADB_ in **Admin > Device Support > Event Types**.

Collecting Listener Log and Error log via Windows Agent

Configuration

1. Login to FortiSIEM GUI.
2. Navigate to **Admin > Setup**, and click the **Windows Agent** tab.
3. Under **Windows Agent Monitor Templates**, click **New** to create a new template, or click an existing template and click **Edit**.
4. If creating a new template, on the **Generic** tab, in the **Name** field, enter a name for the template.
5. Click the **User Log** tab, and click **New**.
 - a. In the **Full File Name** field, enter the full file name (including path) to be monitored.
 - b. In the **Log Prefix** field, enter a log prefix that needs to be added to the log.
 - c. Click **Save**.
6. Click **Save**.
7. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
8. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
9. From the **Host** drop-down list, select the host(s).
10. At **Template**, attach the template to one or more Oracle Server hosts by selecting its checkbox, then click **Save**.
11. Under **Host to Template Associations**, click **Apply**.

The logs will have a prefix set by **Log Prefix** that can be used to write a Parser for these files.

For details, see [Configuring Windows Agent](#).

Sample Events

- [System Level Database Performance Metrics](#)
- [Table Space Performance Metrics](#)
- [Oracle Audit Trail \(FortiSIEM Generated Events\)](#)
- [Oracle Audit Log](#)
- [Oracle Listener Log](#)
- [Oracle Alert Log](#)

System Level Database Performance Metrics

```
[PH_DEV_MON_PERF_ORADB]:[eventSeverity]=PHL_INFO, [hostIpAddr]=10.1.2.8, [hostName]=Host-10.1.2.8,
[appGroupName]=Oracle Database Server,
[appVersion]=Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - Production,
[instanceName]=orcl, [instanceStatus]=OPEN, [charSetting]=ZHS16GBK, [archiveEnabled]=FALSE,
[lastBackupDate]=1325566287, [listenerStatus]=OPEN,[dbBufferCacheHitRatio]=100,
[dbMemorySortsRatio]=100,[dbUserTransactionPerSec]=0.13,[dbPhysicalReadsPerSec]=0,
```

```
[dbPhysicalWritesPerSec]=0.48,[dbHostCpuUtilRatio]=0,[dbNetworkKBytesPerSec]=0.58,
[dbEnqueueDeadlocksPerSec]=0,[dbCurrentLogonsCount]=32,[dbWaitTimeRatio]=7.13,
[dbCpuTimeRatio]=92.87,
[dbRowCacheHitRatio]=100,[dbLibraryCacheHitRatio]=99.91,[dbSharedPoolFreeRatio]=18.55,
[dbSessionCount]=40,[dbIOKBytesPerSec]=33.26,[dbRequestsPerSec]=3.24,
[dbSystemTablespaceUsage]= 2.88,[dbTempTablespaceUsage]= 0,[dbUsersTablespaceUsage]= 0.01,
[dbUserCount]= 2,[dbInvalidObjectCount]= 4
```

Table Space Performance Metrics

```
[PH_DEV_MON_PERF_ORADB_TABLESPACE]:[eventSeverity]=PHL_INFO, [appGroupName]=Oracle Database
Server, [instanceName]=orcl, [tablespaceName]=UNDOTBS1, [tablespaceType]=UNDO,
[tablespaceUsage]=0.01, [tablespaceFreeSpace]=4193886, [tablespaceNextExtent]=0
```

```
[PH_DEV_MON_PERF_ORADB_TABLESPACE]:[eventSeverity]=PHL_INFO, [appGroupName]=Oracle Database
Server, [instanceName]=orcl, [tablespaceName]=USERS, [tablespaceType]=PERMANENT,
[tablespaceUsage]=0.01, [tablespaceFreeSpace]=4193774, [tablespaceNextExtent]=0
```

Oracle Audit Trail (FortiSIEM Generated Events)

```
<134>Apr 10 12:51:42 abc-desktop java: [ORADB_PH_Logoff]:[eventSeverity]=PHL_INFO, [retCode]=0,
[eventTime]=2009-04-10 14:29:22:111420, [rptIp]=172.16.10.40, [srcIp]=QA-V-CtOS-ora.abc.net,
[user]=DBSNMP, [logonTime]=2009-04-10 14:29:22:111420, [logoffTime]=2009-04-10 14:29:22,
[privUsed]=CREATE_SESSION,
```

Oracle Audit Log

```
<172>Oracle Audit[25487]: LENGTH : '153' ACTION :[004] 'bjn' DATABASE USER:[9] 'user' PRIVILEGE :
[4] 'NONE' CLIENT USER:[9] 'user' CLIENT TERMINAL:[14] 'terminal' STATUS:[1] '0'
```

```
<172>Oracle Audit[6561]: LENGTH : '158' ACTION :[6] 'COMMIT' DATABASE USER:[8] 'user' PRIVILEGE :
[6] 'SYSDBA' CLIENT USER:[6] 'user' CLIENT TERMINAL:[0] '' STATUS:[1] '0' DBID:[9] '200958341'
```

```
<172>Oracle Audit[28061]: LENGTH: 265 SESSIONID:[9] 118110747 ENTRYID:[5] 14188 STATEMENT:[5]
28375 USERID:[8] user ACTION:[3] 100 RETURNCODE:[1] 0 COMMENT$TEXT:[99] Authenticated by:
DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.90.217.247)(PORT=4566)) PRIV$USED:[1] 5
```

Oracle Listener Log

```
<46>Dec 13 06:07:08 WIN03R2E-110929 OracleListenerLog 0 12-OCT-2011 16:17:52 * (CONNECT_
DATA=(CID=(PROGRAM=)(HOST=)(USER=Administrator))(COMMAND=status)(ARGUMENTS=64)(SERVICE=LISTENER)
(VERSION=185599744)) * status * 0
```

Oracle Alert Log

```
<46>Dec 13 06:07:08 WIN03R2E-110929 OracleAlertLog 0 ORA-00312: online log 3 thread 1:  
'C:\APP\ADMINISTRATOR\ORADATA\ORCL\RED003.LOG'
```

DHCP and DNS Server

FortiSIEM supports these DHCP and DNS servers for discovery and monitoring.

- [Infoblox DNS/DHCP](#)
- [ISC BIND DNS](#)
- [Linux DHCP](#)
- [Microsoft DHCP \(2003, 2008\)](#)
- [Microsoft DNS \(2003, 2008\)](#)

Infoblox DNS/DHCP

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host Name, Hardware model, Serial number, Network Interfaces, Running processes, Installed software	System CPU utilization, Memory utilization, Disk usage, Disk I/O	Performance Monitoring
SNMP		Process level CPU utilization, Memory utilization	
SNMP		Zone Transfer metrics: For each zone: DNS Responses Sent, Failed DNS Queries, DNS Referrals, Non-existent DNS Record Queries, DNS Non-existent Domain Queries, Recursive DNS Query Received DNS Cluster Replication metrics: DNS Replication Queue Status, Sent Queue From Master, Last Sent Time From Master, Sent Queue To Master, Last Sent Time To Master DNS Performance metrics: NonAuth DNS Query Count, NonAuth Avg DNS Latency, Auth DNS Query Count, Auth Avg DNS Latency, Invalid DNS Port Response, Invalid DNS TXID Response DHCP Performance metrics: Discovers/sec, Requests/Sec, Releases/Sec, Offers/sec, Acks/sec, Nacks/sec, Declines/sec, Informs/sec DDNS Update metrics: DDNS Update Success, DDNS Update Fail, DDNS Update Reject, DDNS Prereq Update Reject, DDNS Update Latency, DDNS Update Timeout DHCP subnet usage metrics: For each DHCP Subnet (addr, mask) - percent used	Security Monitoring and compliance

Protocol	Information discovered	Metrics collected	Used for
SNMP		Hardware status	Availability monitoring
SNMP Trap		Hardware failures, Software failures	Availability monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "infoblox" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "infoblox" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>

Setting	Value
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

ISC BIND DNS

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials
- Sample BIND DNS Logs

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
Syslog	Application type	DNS name resolution activity: DNS Query Success and Failure by type	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "isc bind" to see the event types associated with this device.

Configuration

- SNMP
- Syslog

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

Configure the ISC BIND DNS Server to Send Syslog

1. Edit `named.conf` and add a new line: `include /var/named/conf/logging.conf;`
2. Edit the `/var/named/conf/logging.conf` file, and in the `channel queries_file { }` section add `syslog local3;`

3. Restart BIND by issuing `/etc/init.d/named restart`.

Configure Syslog to Send to FortiSIEM

1. Edit `syslog.conf` and add a new line: `Local7.* @<IP address of the FortiSIEM server>`.
2. Restart the syslog daemon by issuing `/etc/init.d/syslog restart`.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Sample BIND DNS Logs

```
<158>Jan 28 20:41:46 100.1.1.1 named[3135]: 28-Jan-2010 20:40:28.809 client 192.168.29.18#34065: query: www.google.com IN A +
```

Linux DHCP

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
Syslog	Application type	DHCP address release/renew events that are used by FortiSIEM for Identity and location: attributes include IP Address, MAC address, Host Name	Security and compliance (associate machines to IP addresses)

Event Types

In **ADMIN > Device Support > Event Types**, search for "linux dhcp" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [Syslog](#)
- [Sample Syslog](#)

SNMP

1. Make sure that snmp libraries are installed.
FortiSIEM has been tested to work with net-snmp libraries.
2. Log in to your device with administrator credentials.
3. Modify the `/etc/snmp/snmpd.conf` file:
 - a. Define the community string for FortiSIEM usage and permit snmp access from FortiSIEM IP.
 - b. Allow FortiSIEM to (read-only) view the mib-2 tree.
 - c. Open up the entire tree for read-only view.
4. Restart the snmpd daemon by issuing `/etc/init.d/snmpd restart`.

5. Add the snmpd daemon to start from boot by issuing `chkconfig snmpd on`.
6. Make sure that snmpd is running.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

Configure Linux DHCP to Forward Logs to Syslog Daemon

1. Edit `dhcpd.conf` and insert the line `log-facility local7;`.
2. Restart dhcpd by issuing `/etc/init.d/dhcpd restart`.

Configure Syslog to Forward to FortiSIEM

1. Edit `syslog.conf` and add a new line: `Local7.* @<IP address of FortiSIEM server>`.
2. Restart syslog daemon by issuing `/etc/init.d/syslog restart`.

Sample Syslog

```
<13>Aug 26 19:28:11 DNS-Pri dhcpd: DHCPREQUEST for 172.16.10.200 (172.16.10.8) from  
00:50:56:88:4e:17 (26L2233B1-02)
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Microsoft DHCP

- [Supported OS](#)
- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Settings for Access Controls](#)

Supported OS

- Windows 2003
- Windows 2008 and 2008 R2
- Windows 2012 and 2012 R2
- Windows 2016
- Windows 2019

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Process details	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Process details, process to service mappings	Process level metrics (Win32_Process, Win32_PerfRawData_PerfProc_Process): uptime, CPU utilization, Memory utilization, Read I/O, Write I/O DHCP metrics (Win32_PerfFormattedData_DHCPServer_DHCPServer): DHCP request rate, release rate, decline rate, Duplicate Drop rate, Packet Rate, Active Queue length, DHCP response time, Conflict queue length	Performance Monitoring
Windows Agent	Application type	DHCP address release/renew events that are used by FortiSIEM for Identity and location: attributes include IP Address, MAC address, Host Name	Security and compliance (associate machines to IP addresses)

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft dhcp" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [WMI](#)
- [FortiSIEM Windows Agent](#)

SNMP

See [SNMP Configurations](#) in the *Microsoft Windows Server Configuration* section.

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring DHCP for FortiSIEM Windows Agent, see [Collecting Windows DHCP Logs](#) from Microsoft Windows Server via Agents.

Settings for Access Controls

See [Setting Access Credentials](#) in the *Microsoft Windows Server Configuration* section.

Microsoft DNS

- [Supported OS](#)
- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

Supported OS

- Windows 2003
- Windows 2008 and 2008 R2
- Windows 2012 and 2012 R2
- Windows 2016
- Windows 2019

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics (Win32_Process, Win32_PerfRawData_PerfProc_Process): uptime, CPU utilization, Memory utilization, Read I/O, Write I/O DNS metrics (Win32_PerfFormattedData_DNS_DNS): DNS requests received, DNS responses sent, WINS requests received, WINS responses sent, Recursive DNS queries received, Recursive DNS queries failed, Recursive DNS queries timeout, Dynamic DNS updates received, Dynamic DNS updates failed, Dynamic DNS updates timeout, Secure DNS update received, Secure DNS update failed, Full DNS Zone Transfer requests sent, Full DNS Zone Transfer requests received, Incremental DNS Zone Transfer requests sent, Incremental DNS Zone Transfer requests received	Performance Monitoring
Windows Agent	Application type	DNS name resolution activity: DNS Query Success and Failure by type	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft dns" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [WMI](#)
- [FortiSIEM Windows Agent](#)

SNMP

See [SNMP Configurations](#) in the *Microsoft Windows Server Configuration* section.

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring DNS for FortiSIEM Windows Agent, see [Collecting DNS Logs](#) from Microsoft Windows Server via Agents.

Microsoft recommends that customers enable DNS Analytical logs only to debug DNS traffic or to troubleshoot DNS server issues. Enabling DNS Analytical logs can cause system performance issues (see [Microsoft Logging and Diagnostics](#)).

Settings for Access Credentials

See [Setting Access Credentials](#) in the *Microsoft Windows Server Configuration* section.

Directory Server

FortiSIEM supports this directory server for discovery and monitoring.

- [Microsoft Active Directory](#)

Microsoft Active Directory

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Active Directory User Discovery](#)
- [Validating LDAP Credentials and Permissions](#)
- [Mapping Active Directory User Attributes to FortiSIEM User Attributes](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
LDAP	User details, Password age		Security Monitoring, User meta data for log
WMI		Win32_PerfRawData_NTDS_NTDS class: Directory Search Rate, Read Rate, Write Rate, Browse Rate, LDAP search rate, LDAP Bind Rate, New LDAP Connection Rate, Successful LDAP Bind Rate, LDAP Active Threads, LDAP Bind Time, LDAP Client Sessions	Performance Monitoring
WMI		"dcdiag -e" command output - detect successful and failed domain controller diagnostic tests	Domain Controller Replication status
WMI		"repadmin /replsummary" command output - detect replication statistics	Domain Controller Replication status

Event Types

- PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE (Active Directory account to expire in 2 weeks)
- PH_DISCOV_ADS_ACCT_DISABLED (Accounts Disabled)
- PH_DISCOV_ADS_DORMANT_ACCT (Dormant User Accounts - not log on in last 30 days)
- PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES (Active Directory user password never expires)
- PH_DISCOV_ADS_PASSWORD_NOT_REQD (Active Directory user password not required)

- PH_DISCOV_ADS_PASSWORD_STALE (Active Directory user password stale - more than 90 days)
- PH_DISCOV_ADS_PASSWORD_TO_EXPIRE (Active Directory user password to expire in 2 weeks)
- PH_DEV_MON_DCDIAG (output of "dcdiag -e" command)

```
[PH_DEV_MON_DCDIAG]:[hostIpAddr]=10.1.20.59,[hostName]=WIN-IG0808M5JVT,[errReason]="",
[testResult]="passed",[testSubject]="WIN-IG0808M5JVT",[testName]="NCSecDesc"
```

- PH_DEV_MON_SRC_AD_REPL_STAT (output of "repadmin /replsummary" command)

```
[PH_DEV_MON_SRC_AD_REPL_STAT]:[hostIpAddr]=10.1.20.59,[hostName]=WIN-IG0808M5JVT,
[largestReplDelta]=">60 days",[failureCount]=0.00,[count]=5.00,[failurePct]=0.00,
[srcName]="WIN-IG0808M5JVT",[errReason]=""
```

- PH_DEV_MON_DST_AD_REPL_STAT (output of "repadmin /replsummary" command)

```
[PH_DEV_MON_DST_AD_REPL_STAT]:[hostIpAddr]=10.1.20.59,[hostName]=WIN-IG0808M5JVT,
[largestReplDelta]=">60 days",[failureCount]=0.00,[count]=5.00,[failurePct]=0.00,
[destName]="WIN-IG0808M5JVT",[errReason]=""
```

Rules

- Failed Windows DC Diagnostic Test

Reports

- Successful Windows Domain Controller Diagnostic Tests
- Failed Windows Domain Controller Diagnostic Tests
- Source Domain Controller Replication Status
- Destination Domain Controller Replication Status

Configuration

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

Active Directory User Discovery

If you want to add Active Directory users to FortiSIEM, follow these steps in the FortiSIEM UI.

1. Add the login credentials for Active Directory server and associate them to an IP range.
2. Discover the Active Directory server.

If the Active Directory server is discovered successfully, then all of the users and their properties will be added to FortiSIEM.

After the users have been added to FortiSIEM, you can re-run discovery to get new changes from Active Directory. You cannot make changes in FortiSIEM as this will inevitably make FortiSIEM out of synch with Active Directory.

Since Active Directory can contain many users, it is possible to choose a sub-tree by specifying a base DN (see below).

Adding Active Directory Login Credentials to FortiSIEM

1. Log in to your Supervisor UI.
2. Go to **ADMIN > Setup > Credentials**.
3. Click **New** to create an LDAP discovery credential by entering the following in the Access Method Definition dialog box:
 - a. **Name**: a name for the credential.
 - b. **Device Type**: select **Microsoft Windows**.
 - c. **Access Protocol**:
 - i. By default, **LDAP** servers listen on TCP port 3268.
 - ii. **LDAPS** (LDAP with SSL) defaults to port 3269.
 - iii. **LDAP** Start TLS defaults to port 3268.
Note: Global catalog ports LDAP - TCP/3268 and LDAPS - TCP/3269 when used are much more performant versus the LDAP port TCP/389 and LDAPS port TCP/636, but not all LDAP attributes may be present by default in Global Catalog service.

For single AD servers, or if you do not need to integrate with Microsoft Active Directory cross-domain queries via Global Catalog, you can use the following ports:

 - LDAP servers listen on TCP port 389.
 - LDAPS (LDAP with SSL) defaults to port 636.
 - LDAP Start TLS defaults to port 389.
 - d. **Used For**: select **Microsoft Active Directory**.
 - e. Enter the root of the **LDAP** user tree that you want to discover. For example, `dc=companyABC,dc=com` or `ou=Org1,dc=companyABC,dc=com`
 - f. **NetBIOS/Domain**: enter the NetBIOS/Domain value.
 - g. **User Name**: enter the user name for your LDAP directory.
The user should be a member of the **Domain Users** group in Active Directory. See the [Validating LDAP Credentials and Permissions](#) for information on how to validate this membership.
 - h. Enter and confirm the **Password** for your User.
 - i. Click **Save**. Your LDAP credentials will be added to the list of credentials.- 4. Under **Enter IP Range to Credential Associations**, click **Add**.
- 5. Select your **LDAP** credentials from the list of **Credentials**. Click **+** to add more.
- 6. Enter the **IP/IP Range** or **host name** for your Active Directory server.
- 7. Click **Save**. Your LDAP credentials will appear in the list of credential/IP address associations.
- 8. Click **Test > Test Connectivity** to make sure you can connect to the Active Directory server.

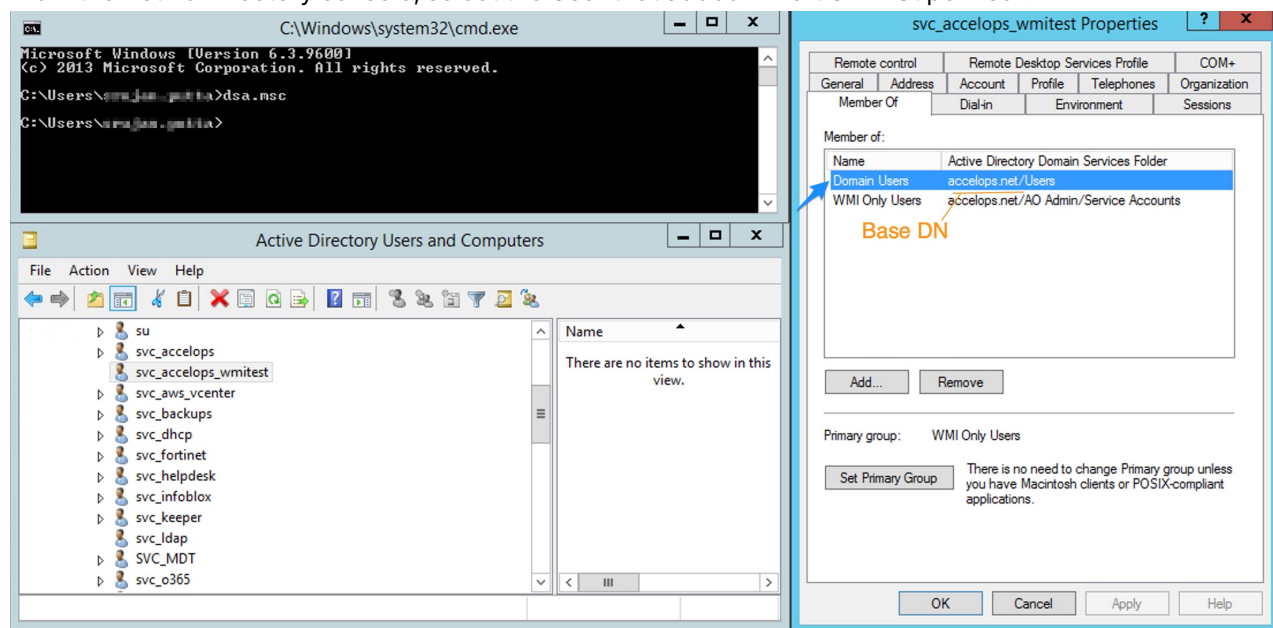
Discovering Users in FortiSIEM

1. Go to **ADMIN > Setup > Discovery** and click **New**.
2. For **Name**, enter **Active Directory**.
3. For **Include**, enter the IP address or host name for your Active Directory server.
4. Click **Save**. Active Directory will be added to the list of discoverable devices.
5. Select the **Active Directory** device and click **Discover**.
6. After discovery completes, go to **CMDB > Users** to view the discovered users. You may need to click the **Refresh** icon to load the user tree hierarchy.

To get user updates in Active Directory, simply re-run discovery.

Validating LDAP Credentials and Permissions

1. Log in to your Active Directory server.
2. Open the Active Directory console from the command prompt and execute the `dsa.msc` command.
3. From the Active Directory console, select the User that added in FortiSIEM Supervisor.



4. Right click the selected User and check **Properties**.
5. The User should be a member of **Domain Users**.
6. On FortiSIEM **Base DN** should match, example: `DC=accelops,DC=net`.

Mapping Active Directory User Attributes to FortiSIEM User Attributes

The following table shows how user attributes in Microsoft Active Directory are shown in the FortiSIEM UI. To find Active Directory user attributes, take the following steps:

1. Log in to Active Directory.
2. Go to Active Directory Users and Computers.
3. Click **View > Enable Advanced Features**.
4. Find a user, and take the following steps:
 - a. Double click user.
 - b. Click Attribute Editor.
You will see a set of attributes and the values they are set to.

In FortiSIEM, user details can be found in **CMDB > Users**. First, click the tree node on the left that you have discovered, then locate the user in the right pane. Attributes are displayed on the main page and under Summary, Contact, and Member Of.

Microsoft Active Directory User Attribute	FortiSIEM User Attribute
sAMAccountName	User Name
name	Full Name
userPrincipalName	<Not shown>
mail	Email
telephoneNumber	Work Phone
mobile	Mobile Phone
title	Job Title
company	Company
department	<Not shown>
employeeID	Employee ID
manager	Manager
l	<Not shown>
postalCode	ZIP
streetAddress	Address
homePostalAddress	<Not shown>
c	City
st	State
co	Country
memberOf	Member Of

Document Management Server

FortiSIEM supports this document management server for discovery and monitoring.

- [Microsoft SharePoint](#)

Microsoft SharePoint

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
LOGbinder Agent		SharePoint logs - Audit trail integrity, Access control changes, Document updates, List updates, Container object updates, Object changes, Object Import/Exports, Document views, Information Management Policy changes	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "sharepoint" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "sharepoint" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

Microsoft SharePoint logs are supported via LOGbinder SP agent from Monterey Technology group. The agent must be installed on the SharePoint server. **Configure the agent to write logs to Windows Security log.** FortiSIEM simply reads the logs from windows security logs via WMI and categorizes the SharePoint specific events and parses SharePoint specific attributes.

Installing and Configuring LOGbinder SP Agent

- [LOGbinder Install Web Link](#)
- [LOGbinder Configuration Web Link](#) - Remember to configure LOGbinder SP agent to write to Windows security log.
- [LOGbinder SP Getting Started Document](#) - Remember to configure LOGbinder SP agent to write to Windows security log.

Healthcare IT

FortiSIEM supports the discovery and monitoring of these healthcare applications.

- [Epic EMR/EHR System](#)

Epic EMR/EHR System

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Authentication Query, Client login Query	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Epic-SecuritySIEM" to see the event types associated with this device. There are two events that are parsed:

- Epic-SecuritySIEM-AUTHENTICATION-Query
- Epic-SecuritySIEM-LOGIN-Query

Rules

No specific rules are written for Epic-SecuritySIEM.

Reports

No specific reports are written for Epic-SecuritySIEM.

Configuration

Configure the Epic-SecuritySIEM system to send logs to FortiSIEM in the supported format (see [Sample Events](#)).

Settings for Access Credentials

None required.

Sample Events

```
Oct 19 05:32:16 10.25.8.111 CEF:0|Epic|Security-SIEM|8.3.0|LOGIN|LOGIN|4|cnt=1
suser=3227^DOE, JOHN L^JOHN-DOE shost=PRD workstationID=WS7946 act=Query
end=Oct 19 00:30:00 flag=^^Workflow Logging CLIENTNAME=dom1/WS7946
DEP=100000010^RMC ICU MAIN IP=10.25.6.59/10.170.10.66 LOGINLDAPID=JOHN-DOE
LOGINREASON= OSUSR=WS7946 ROLE=MODEL IP NURSE SOURCE=1-Hyperspace
USERJOB=304401^RMC INPATIENT NURSE TEMPLATE#011
```

```
Oct 19 05:32:16 10.25.8.111 CEF:0|Epic|Security-SIEM|8.3.0|AUTHENTICATION|AUTHENTICATION|4|cnt=1
suser=3055^DOE, JOHN^JOHN-DOE shost=PRD workstationID=WS7610 act=Query end=Oct 19 00:30:00
flag=Access History^^Workflow Logging LOGINCONTEXT=0-Login
LOGINDEVICE=10001-ImprivataAuthMultiApp LOGINLDAPID=JOHN-DOE LOGINREVAL= 011
```

Mail Server

FortiSIEM supports this mail server for discovery and monitoring.

- [Microsoft Exchange](#)

Microsoft Exchange

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Collecting Microsoft Exchange Message Track Logs
- Settings for Access Credentials
- Sample Logs

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization for the various exchange server processes	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec for the various exchange server processes Exchange performance metrics (: VM Largest Block size, VM Large Free Block Size, VM Total Free Blocks, RPC Requests, RPC Request Peak, RPC Average Latency, RPC Operations/sec, User count, Active user Count, Peak User Count, Active Connection Count, Max Connection Count Exchange error metrics (obtained from Win32_PerfRawData_MSExchangeIS_MSExchangeIS WMI class): RPC Success, RPC Failed, RPC Denied, RPC Failed - Server Busy, RPC Failed - Server Unavailable, Foreground RPC Failed, Background RPC Failed Exchange mailbox metrics (obtained from Win32_PerfRawData_MSExchangeIS_MSExchangeISMailbox and Win32_PerfRawData_MSExchangeIS_MSExchangeISPublic WMI classes): Per Mailbox: Send Queue, Receive Queue, Sent Message, Submitted Message, Delivered Message, Active User, Peak User	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Exchange SMTP metrics (obtained from Win32_PerfRawData_SMTSPVC_SMTPServer WMI class): Categorization Queue, Local Queue, Remote Queue, Inbound Connections, Outbound Connections, Sent Bytes/sec, Received Bytes/sec, Retry Count, Local Retry Queue, Remote Retry Queue Exchange ESE Database (Win32_PerfFormattedData_ESE_MSEExchangeDatabase): Exchange Database Instances (Win32_PerfFormattedData_ESE_MSEExchangeDatabaseInstances):	
		Exchange Mail Submission Metrics (Win32_PerfFormattedData_MSEExchangeMailSubmission_MSEExchangeMailSubmission): Exchange Replication Metrics (Win32_PerfFormattedData_MSEExchangeReplication_MSEExchangeReplication): Exchange Store Interface Metrics (Win32_PerfFormattedData_MSEExchangeStoreInterface_MSEExchangeStoreInterface): Exchange Transport Queue Metrics (Win32_PerfFormattedData_MSEExchangeTransportQueues_MSEExchangeTransportQueues):	
Windows Agent		Application Logs, Microsoft Exchange Message Tracking Logs	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft exchange" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "microsoft exchange" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- [SNMP](#)
- [WMI](#)

SNMP

See [SNMP Configurations](#) in the *Microsoft Windows Server Configuration* section.

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

Settings for Access Credentials

See [Setting Access Credentials](#) in the *Microsoft Windows Server Configuration* section.

Collecting Microsoft Exchange Message Track Logs

To configure Microsoft Exchange to log message tracking on a Microsoft Exchange Server, take the following steps.

Note: General Windows Agent configuration information can be found [here](#).

1. Locate where your Microsoft Exchange log files reside. Typically, this path is:
C:\Program Files\Microsoft\Exchange
Server\V15\TransportRoles\Logs\MessageTracking\MSGTRKM*.log
2. Install the FortiSIEM Windows Server Agent on the Microsoft Exchange Server.
3. Configure a new Windows Agent Monitor Template by taking the following steps in FortiSIEM.
 - a. Navigate to **Admin > Setup > Windows Agent**.
 - b. Under **Windows Agent Monitor Templates**, click **New**.
 - c. In the **Generic** tab, in the **Name** field, enter a name for the Windows Agent Monitor Template.
 - d. Select the **User Log** tab, then and click **New**.
 - e. In the **Full File Name** field, enter the path to your Microsoft Exchange Server logs. For example, for a typical Exchange Server, the path would be:
C:\Program Files\Microsoft\Exchange
Server\V15\TransportRoles\Logs\MessageTracking\MSGTRKM*.log
 - f. In the **Log Prefix** field, enter "ExchTrackLog".
 - g. Click **Save** to save the configuration.
 - h. Click **Save** to save the Windows Agent Monitor Template.
4. Configure a Host to Template Association to associate the template with the Exchange Server agent by taking the following steps.
 - a. Under **Hosts To Template Associations**, click **New**.
 - b. In the **Name** field, enter the name for the Hosts to Template Associations.
 - c. Select an Organization with a collector.
 - d. Select a Host.
 - e. Select the Windows Agent Monitor Template you created earlier.
 - f. Select a Collector or **Select All**.
 - g. Click **Save**.

- h. Under **Hosts to Template Associations**, click **Apply**.

Sample Logs

```
2017-10-05T12:06:00Z EXCH99.foo.com 192.0.2.0 AccelOps-WUA-UserFile-ExchangeTrackLog
[monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="d78e4bd5-bc3f-4950-bcdf-926947ee1db7"
[timeZone]="+0300" [fileName]="C:\\Program Files\\Microsoft\\Exchange
Server\\V15\\TransportRoles\\Logs\\MessageTracking\\MSGTRKMS2017100512-1.LOG" [msg]="2017-10-
05T12:05:56.564Z,ffff::eeee:aaaa:bbbb:cccc:ddd%13,EXCH99,,EXCH99.foo.com,\"MDB:d72c63cf-290e-
456e-86e5-85dedb1f56de, Mailbox:d7c8c416-c1a7-4225-a17f-552d5274703d, Event:4419662,
MessageClass:IPM.Note.ProbeMessage.MBTSubmissionServiceHeartbeatProbe, CreationTime:2017-10-
05T12:05:56.267Z, ClientType:Monitoring,
SubmissionAssistant:MailboxTransportSubmissionEmailAssistant\",,,STOREDRIVER,SUBMIT,,<e545b612256a4
c14a563f78a8999fafd@user.example.com>,0a21180c-5932-4c7e-3888-
08d50be96f34,HealthMailbox66dd83eddb9b4ee69dbd3fa82c925a3b@user.example.com,,,1,,,00000052-0000-
0000-0000-0000ea5a2141-
MBTSubmissionServiceHeartbeatProbe,HealthMailbox66dd83eddb9b4ee69dbd3fa82c925a3b@user.example.com,
,2017-10-05T12:05:56.267Z;LSRV=EXCH99.foo.com:TOTAL-SUB=0.296|SA=0.078|MTSS=0.209(MTSSD=0.209
(MTSSDA=0.005|MTSSDC=0.005|SDSS0=0.161(SMSC=0.020|SMS=0.140)|X-MTSSDPL=0.004|X-
MTSSDSS=0.008|MTSSDS=0.001)),Originating,,,,S:ItemEntryId=00-00-00-00-ED-99-60-31-E3-76-3C-4B-
BE-FE-5B-27-F0-88-3D-0A-07-00-25-D5-0C-8E-46-5A-51-46-A4-18-7D-65-F7-DF-52-1C-00-00-00-00-01-0B-
00-00-25-D5-0C-8E-46-5A-51-46-A4-18-7D-65-F7-DF-52-1C-00-00-30-88-0D-FF-00-00,Email,92e0d0ab-4670-
41e9-d453-08d50be96f50,15.01.0845.034"
```


Management Server/Appliance

FortiSIEM supports these web servers for discovery and monitoring.

- [Cisco Application Centric Infrastructure \(ACI\)](#)
- [Fortinet FortiManager](#)
- [HPE Integrated Lights-Out \(iLO\)](#)
- [SolarWinds Orion](#)
- [VMware NSX for vSphere](#)

Cisco Application Centric Infrastructure (ACI)

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- FortiSIEM Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Cisco APIC API (REST)		Overall Health, Tenant Health, Node Health, Cluster Health, Application Health, EPG health, Fault Record, Event record, Log Record, Configuration Change	Availability and Performance Monitoring

Event Types

Go to **ADMIN > Device Support > Event Types** and search for "Cisco_ACI".

Rules

Go to **RESOURCES > Rules** and search for "Cisco ACI" in the main content panel **Search...** field.

Reports

Go to **RESOURCES > Reports** and search for "Cisco ACI" in the main content panel **Search...** field.

Configuration

- Cisco ACI Configuration
- FortiSIEM Configuration

Cisco ACI Configuration

Please configure Cisco ACI Appliance so that FortiSIEM can access it via APIC API.

FortiSIEM Configuration

1. Go to **ADMIN > Setup > Credentials**.
2. In **Step 1: Enter Credentials**, click **New** and create a credential.

Settings	Description
Name	Enter a name for the credential.
Device Type	CISCO CISCO ACI
Access Protocol	Cisco APIC API
Pull Interval	5 minutes
Port	443
Password config	See Password Configuration
User Name	User name for device access
Password	Password for the various REST APIs
Description	Password for the various REST APIs

3. In **Step 2: Enter IP Range to Credential Associations** click **New** and create the association.
 - a. **IP** - specify the IP address of the ACI Controller
 - b. **Credential** - specify the Name as in 2a
4. **Test Connectivity** - Click the **Test** drop-down list, and select **Test Connectivity** with or without ping and make sure the test succeeds
5. Check **Pull Events**, located by navigating to **ADMIN > Setup > Pull Events**, to make sure that a event pulling entry is created

Sample Events

- [Overall Health Event](#)
- [Tenant Health Event](#)
- [Nodes Health Event](#)
- [Cluster Health Event](#)
- [Application Health Event](#)
- [EPG Health Event](#)
- [Fault Record Event](#)
- [Event Record Event](#)
- [Log Record Event](#)
- [Configuration Change Event](#)

Overall Health Event

```
[Cisco_ACI_Overall_Health]: {"attributes":
{"childAction":"","cnt":"29","dn":"topology/HDfabricOverallHealth5min0","healthAvg":"82","healthMax":"89",
```

```
"healthMin":"0","healthSpct":"0","healthThr":"","healthTr":"1","index":"0","lastCollOffset":"290",
"repIntvEnd":"2016-09-05T08:13:53.232+00:00","repIntvStart":"2016-09-
05T08:09:03.128+00:00","status":""}}
```

Tenant Health Event

```
[Cisco_ACI_Tenant_Health]: {"attributes":{"childAction":"","descr":"","dn":"uni/tn-
CliQr","lcOwn":"local","modTs":"2016-09-05T07:56:27.164+00:00","monPolDn":"uni/tn-common/monepg-
default","name":"CliQr","ownerKey":"","ownerTag":"","status":"","uid":"15374"},"children":
[{"healthInst":{"attributes":
{"childAction":"","chng":"0","cur":"100","maxSev":"cleared","prev":"100","rn":"health","statu
s":"","
```

```
"twScore":"100","updTs":"2016-09-05T08:27:03.584+00:00"}}}]
```

Nodes Health Event

```
[Cisco_ACI_Node_Health]: {"attributes":
{"address":"10.0.208.95","childAction":"","configIssues":"","currentTime":"2016-09-
05T08:15:51.794+00:00","dn":"topology/pod-1/node-
101/sys","fabricId":"1","fabricMAC":"00:22:BD:F8:19:FF","id":"101","inbMgmtAddr":"0.0.0.0",
```

```
"inbMgmtAddr6":"0.0.0.0","lcOwn":"local","modTs":"2016-09-05T07:57:29.435+00:00",
```

```
"mode":"unspecified","monPolDn":"uni/fabric/monfab-
default","name":"Leaf1","oobMgmtAddr":"0.0.0.0","oobMgmtAddr6":"0.0.0.0","podId":"1","role"
```

```
:"leaf","serial":"TEP-1-101","state":"in-
service","status":"","systemUpTime":"00:00:27:05.000"},"children":[{"healthInst":{"attributes":
{"childAction":"","chng":"-
10","cur":"90","maxSev":"cleared","prev":"100","rn":"health","status":"","twScore":"90","updTs":"2
016-09-05T07:50:08.415+00:00"}}}]
```

Cluster Health Event

```
[Cisco_ACI_Cluster_Health]: {"attributes":{"addr":"10.0.0.1","adminSt":"in-
service","chassis":"10220833-ea00-3bb3-93b2-
ef1e7e645889","childAction":"","cntrlSbstState":"approved","dn":"topology/pod-1/node-1/av/node-
1","health":"fully-fit","id":"1","lcOwn":"local","mbSn":"TEP-1-1","modTs":"2016-09-
05T08:00:46.797+00:00","monPolDn":"","mutnTs":"2016-09-
05T07:50:19.570+00:00","name":"","nodeName":"apic1","operSt":"available","status":"","uid":"0"}
```

Application Health Event

```
[Cisco_ACI_Application_Health]: {"attributes":{"childAction":"","descr":"","dn":"uni/tn-infra/ap-access","lcOwn":"local","modTs":"2016-09-07T08:17:20.503+00:00","monPolDn":"uni/tn-common/monepg-default","name":"access","ownerKey":"","ownerTag":"","prio":"unspecified","status":"","uid":"0"},
```

```
"children":[{"healthInst":{"attributes":{"childAction":"","chng":"0","cur":"100","maxSev":"cleared","prev":"100","rn":"health","status":"","twScore":
```

```
"100","updTs":"2016-09-07T08:39:35.531+00:00"}}]}}
```

EPG Health Event

```
[Cisco_ACI_EPG_Health]: {"attributes":{"childAction":"","configIssues":"","configSt":"applied","descr":"","dn":"uni/tn-infra/ap-access/epg-default","isAttrBasedEPg":"no","lcOwn":"local","matchT":"AtleastOne","modTs":"2016-09-07T08:17:20.503+00:00","monPolDn":"uni/tn-common/monepg-default","name":"default","pcEnfPref":"unenforced","pcTag":"16386","prio":"unspecified",
```

```
"scope":"16777199","status":"","triggerSt":"triggerable","txId":"5764607523034234882","uid":"0"},"children":[{"healthInst":{"attributes":{"childAction":"","chng":"0","cur":"100","maxSev":"cleared","prev":"100","rn":"health","status":"","
```

```
"twScore":"100","updTs":"2016-09-07T08:39:35.549+00:00"}}]}}
```

Fault Record Event

```
[Cisco_ACI_Fault_Record]: {"created":"2016-09-05T08:00:41.313+00:00","delegated":"no","delegatedFrom":"","descr":
```

```
"Controller3isunhealthybecause:DataLayerPartiallyDegradedLeadership","dn":"subj-[topology/pod-1/node-1/av/node-3]/fr-4294967583","domain":"infra","highestSeverity":"critical","id":"4294967583","ind":"modification",
```

```
"lc":"soaking","modTs":"never","occur":"1","origSeverity":"critical","prevSeverity":"critical",
```

```
"rule":"infra-wi-node-health","severity":"critical","status":"","subject":"controller","type":"operational"}
```

Event Record Event

```
[Cisco_ACI_Event_Record]: {"attributes":{"affected":"topology/pod-1/node-2/lon/svc-ifc_dhcpd","cause":"state-change","changeSet":{"id:ifc_dhcpd,leCnnct:undefined,leNonOptCnt:undefined,leNotCnnct:undefined,name:ifc_dhcpd","childAction":"","code":"E4204979","created":"2016-09-
```

```
05T07:57:37.024+00:00","descr":"Allshardsofserviceifc_
dhcpdhaveconnectivitytotheleaderreplicaintheCluster.","dn":"subj-[topology/pod-1/node-2/lon/svc-
ifc_dhcpd]/rec-8589934722","id":"8589934722","ind":"state-
transition","modTs":"never","severity":"info","status":"","trig":"oper","txId":
```

```
"18374686479671623682","user":"internal"}
```

Log Record Event

```
[Cisco_ACI_Log_Record]: {"attributes":{"affected":"uni/userext/user-
admin","cause":"unknown","changeSet":"","childAction":"","clientTag":"","code":"generic","created"
```

```
:"2016-09-05T07:56:25.825+00:00","descr":"From-198.18.134.150-client-type-REST-
```

```
Success","dn":"subj-[uni/userext/user-admin]/sess-
4294967297","id":"4294967297","ind":"special","modTs":"never","severity":"info","status":"","syste
mId":"1","trig":
```

```
"login,session","txId":"0","user":"admin"}
```

Configuration Change Event

```
[Cisco_ACI_Configuration_Chang]: {"attributes":{"affected":"uni/tn-CliQr/out-CliQr-Prod-
L3Out/instP-CliQr-Prod-L3Out-
EPG/rscustQosPol","cause":"transition","changeSet":"","childAction":"","clientTag":"","code":"E420
6266",
```

```
"created":"2016-09-05T07:56:27.099+00:00","descr":"RsCustQosPolcreated","dn":"subj-[uni/tn-
CliQr/out-CliQr-Prod-L3Out/instP-CliQr-Prod-L3Out-EPG/rscustQosPol]/mod-
4294967308","id":"4294967308","ind":"creation","modTs":"never","severity":"info","status":"","trig
":"config","txId":
```

```
"7493989779944505526","user":"admin"}}}
```

Fortinet FortiManager

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring

Event Types

Regular monitoring events

- PH_DEV_MON_SYS_CPU_UTIL
- PH_DEV_MON_SYS_MEM_UTIL
- PH_DEV_MON_SYS_DISK_UTIL
- PH_DEV_MON_NET_INTF_UTIL

Rules

Regular monitoring rules

Reports

Regular monitoring reports

Configuration

Configuring FortiManager to send Local Logs to Syslog Server

To configure FortiManager to send local logs to the syslog server, take the following steps:

1. Go to *System Settings > Advanced > Syslog Server* to configure syslog server settings.
2. Double-click on a server, right-click on a server, and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Syslog Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

Configuring FortiManager for Security and Compliance and Perf Logs

To configure FortiManager for Security and Compliance and Perf Logs, take the following steps:

1. Go to *System Settings > Advanced > SNMP* to configure the SNMP agent.
2. Select an SNMP Agent to enable/Select the *Enable* checkbox.
3. Configure the SNMP Agent.

Configure an SNMPv3 User

1. Go to *System Settings > Advanced > SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v3* section, click *Create New* in the toolbar. The *New SNMP User* pane opens. Enter the following:
 - a. In the *User Name* field, enter "fortisiem".
 - b. In *Security Level*, select *Authentication, Privacy*.
 - c. Select *Authentication Algorithm (SHA1, MD5)* the *Private Algorithm (AES, DES)*.
 - d. Select *SHA1* and enter the password.
 - e. Select *AES* and enter the password.
 - f. Select *Queries* to enable, and leave the default port UDP to 161.
 - g. In the *Notification Hosts* field, enter the FortiSIEM collector IP address.
 - h. In *SNMP Event*, select all events.
 - i. Click *Save*.

You can now configure FortiSIEM to communicate with FortiManager. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#). For **Device Type** Fortinet FortiManager, see [Access Credentials](#).

HPE Integrated Lights-Out (iLO)

- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "hp-" and look for HPE iLO in the Device Type column to see the event types associated with this device. In FortiSIEM 6.3.0, there are 25 new event types and 500+ generic HP SNMP trap event types.

Rules

No specific rules are available.

Reports

No specific reports are available.

Configuration

For the latest HP iLO documentation, see https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-a00026111en_us#N1050D.

SNMPv1 Traps Configuration

Configure SNMP Settings

To configure SNMP, take the following steps:

1. In the navigation tree, click **Management**.
2. In the SNMP Settings section, enter the following values:
 - System Location
 - System Contact
 - System Role
 - System Role Detail
 - Read Community 1
 - Read Community 2

- Read Community 3

3. Click **Apply**.

Note: More information is available [here](#).

Add SNMP Alert Destinations

1. In the navigation tree, click **Management**.
2. In the **SNMP Alert Destinations** section, click **New**, and enter the following values.
 - SNMP Alert Destination
 - Trap Community
 - SNMP Protocol
 - SNMPv3 User

3. Click **Add**.

Note: More information is available [here](#).

Configure SNMP Alerts

1. In the navigation tree, click **Management**.
2. In the **SNMP Alerts** section, configure **Trap Source Identifier** by selecting **iLO Hostname** or **OS Hostname**.
3. Configure the following values:
 - iLO SNMP Alerts
 - SNMPv1
 - Cold Start Trap Broadcast
 - Periodic HSA Trap Configuration

Click **Apply** to save.

Note: More information is available [here](#).

ManageEngine Endpoint Central

Vendor: ManageEngine

Product: Endpoint Central

Support Added: 7.4.x, 7.3.x, 7.2.x, 7.1.x

Product Information: <https://www.manageengine.com/products/desktop-central/>

Information Collected

ManageEngine Endpoint Central provides automated patching, asset intelligence, remote troubleshooting, digital employee experience, data security, attack surface management, ransomware protection, and more.

FortiSIEM collects Informational and Security related events from ManageEngine Endpoint Central via Syslog. The following log types are collected:

ManageEngine Endpoint Central Log Type	Event Type Prefix for corresponding FortiSIEM Events	Collection Method
Informational	ManageEngine-EndpointCentral (5 event types)	Syslog
Security	ManageEngine-PAM360 (7 event types)	Syslog

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

Configure ManageEngine Endpoint Central to send syslogs to FortiSIEM. Unless TLS Enabled is required for FIPS operation, no configuration is required in FortiSIEM.

Configure ManageEngine Endpoint Central to send Syslogs

Reference: <https://www.manageengine.com/products/desktop-central/help/ec-op-syslog-integration.html>

Follow these steps:

1. From Endpoint Central server web console, navigate to **Admin > Integrations > Syslog**.
2. In the **Syslog Server Address** field, enter the FortiSIEM IP address or hostname.
3. From the **Protocol** drop-down, select **UDP**.
4. Select **TLS Enabled** if secure communication is required. To configure FortiSIEM to receive syslog over TLS, see [here](#).
5. In the **Server Port** field, enter the port number for UDP communication, typically 514 for UDP.
6. Click **Save**.

Sample Events

```
<110>1 2025-10-03T15:35:24.049+04:00 -- EndpointCentral - - - [Category=EventLog] [EventID=403]
[EventName=AuditLogReports] [UserName=myusername] [UserIPAddress=] [Module=Remote Control]
[Reason=.] [StartTime=1759491324049] [EndTime=1759491324049] [TimeDuration=0]
[ViewerIP=10.10.200.1] [Type=Information] [EndpointName=LAB-123-XYZ] [DomainName=TESTDOMAIN]
[CustomerID=1] [UserEmail=][message=Remote Control Viewer connected successfully for
myuser.mylastname]
```

```
<110>1 2025-10-03T11:12:28.419+04:00 -- EndpointCentral - - - [Category=EventLog] [EventID=402]
[EventName=AuditLogReports] [UserName=testuser] [UserIPAddress=10.10.200.10] [Module=Remote
Control] [Reason=d] [StartTime=1759475548419] [EndTime=1759475548419] [TimeDuration=0] [ViewerIP=]
[Type=Information] [EndpointName=LAB-123-XYZ] [DomainName=TESTDOMAIN] [CustomerID=1] [UserEmail=]
[message=Remote Control with LAB2-DEST-DEV has been initiated by myuser]
```

SolarWinds Orion

This section describes how to configure FortiSIEM to receive SNMP Traps from SolarWinds Orion.

Support Added: FortiSIEM 6.x onwards

Vendor: SolarWinds

Product Information: <https://www.solarwinds.com/orion-platform>

Configuring SolarWinds Orion

SolarWinds Orion configuration is comprised of two main steps.

- [Step 1: Configure SolarWinds Orion](#)
- [Step 2: Configure FortiSIEM](#)

Step 1: Configure SolarWinds Orion

This section describes how to configure SolarWinds Orion to send SNMP Traps to FortiSIEM.

1. Login to SolarWinds Orion Alert Manager.
2. Go to the Alert Manager by taking the following path: **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
3. From the Alert Manager Quick Start window, click **Configure Alerts**.
4. From the Manage Alerts window, select an existing alert and click **Edit**.
5. Click **Triggered Actions**.
6. Click **Add New Action**.
7. Click **Send an SNMP Trap**, then click **OK**.
8. In the **SNMP Trap Destinations** field, enter the FortiSIEM Supervisor or Collector IP address.
9. From the **Trap Template** drop-down list, select **ForwardSyslog**.
10. From the **SNMP Version** drop-down list, select **SNMPv2c** or **SNMP3**.
If you selected **SNMPv2c**, in the **SNMP Community String** field, enter the SNMP Community String for SNMPv2c authentication.
If you selected **SNMPv3**, take the following steps:
 - a. In the **SNMPv3 Credentials Username** field, enter the SNMPv3 username.
 - b. Under **SNMPv3 Authentication**, from the **Method** drop-down list, select an SNMPv3 Authentication Method and enter the associated Password.
 - c. Under **SNMPv3 Privacy/Encryption**, from the **Method** drop-down list, select an SNMPv3 Privacy/Encryption method and enter the associated password.
11. When done, click **OK**.

Step 2: Configure FortiSIEM

To receive SNMP V1/V2 Traps, no configuration is required. To receive SNMP V3 Traps, follow the steps [here](#).

VMware NSX for vSphere

Support Added: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: VMware

Product: VMware NSX for vSphere

Product Information: <https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/index.html>

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOGs collected	Used for
Syslog		security logs	Security and Compliance monitoring

Configuration

Configure VMware NSX for vSphere to send logs to FortiSIEM. FortiSIEM will automatically parse the logs. No configuration is required in FortiSIEM.

Sample Events

```
<182>1 2021-11-12T07:00:00.084Z nsxmgr03-ars.company.local NSXV 5956 - [nsxv@6876 comp="nsx-manager" level="INFO" subcomp="manager"] The task core.services.fabric.stateUpdaterTaskName [id:task-994995] is added to the SchedulerQueue
```

```
<182>1 2021-11-12T06:59:49.339Z nsxmgr03-ars.company.local NSXV 5420 - [nsxv@6876 comp="nsx-manager" level="INFO" subcomp="manager"] [AuditLog] UserName:'admin', Originated IP:'192.0.2.33', ModuleName:'ACCESS_CONTROL', Operation:'LOGIN', Resource Name:'NSX Appliance Manager', Time:'Fri Nov 12 06:59:49.338 WET 2021', Status:'SUCCESS'
```

```
<182>1 2021-11-12T07:00:00.103Z nsxmgr03-ars.company.local NSXV 5956 - [nsxv@6876 comp="nsx-manager" level="INFO" subcomp="manager"] [SystemEvent] Time:'Fri Nov 12 07:00:00.101 WET 2021', Severity:'Critical', Event Source:'null', Code:'30051', Event Message:'Missing or deleted resources: [datastore-339487] found used in NSX Edge(s): [edge-142]. Please reconfigure these NSX Edges to use existing resources. Please refer to NSX Manager logs for the complete list of missing resources.', Module:'NSX Edge Appliance', Universal Object:'false'
```

Remote Desktop

FortiSIEM supports this remote desktop application for discovery and monitoring.

- [Citrix Receiver \(ICA\)](#)

Citrix Receiver (ICA)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
WMI		From PH_DEV_MON_APP_ICA_SESS_MET: • ICA Latency Last Recorded • ICA Latency Session Average • ICA Latency Session Deviation • ICA Input Session Bandwidth • ICA Input Session Line Speed • ICA Input Session Compression • ICA Input Drive Bandwidth • ICA Input Text Echo Bandwidth • ICA Input SpeedScreen Data Bandwidth • Input Audio Bandwidth • ICA Input VideoFrame Bandwidth • ICA Output Session Bandwidth • ICA Output Session Line Speed • ICA Output Session Compression • ICA Output Drive Bandwidth • ICA Output Text Echo Bandwidth • ICA Output SpeedScreen Data Bandwidth • ICA Output Audio Bandwidth • ICA Output VideoFrame Bandwidth	

Event Types

In **ADMIN > Device Support > Event Types**, search for "citrix ICA" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "citrix ICA" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- WMI

WMI

Required WMI Class

Make sure the WMI class `Win32_PerfRawData_CitrixICA_ICASession` is available on the host machine for Citrix ICA.

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- [Creating a Generic User Who Does Not Belong to the Local Administrator Group](#)
- [Creating a User Who Belongs to the Domain Administrator Group](#)

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add**.
6. Find the user you created, and then click **OK**.
This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **EditDefault**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.

10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Enable remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2**.
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced**.
8. Select the user you created for the monitoring account, and then click **Edit**.
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add  
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and then click **OK**.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Source Code Control

FortiSIEM supports the [GitHub](#) and [GitLab](#) Source Code Control tools for log collection via an API, and through webhook.

- [GitHub](#)
- [GitLab](#)
- [GitLab API](#)
- [GitLab CLI](#)

GitHub

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration Through API](#)
- [Configuration Through Webhook](#)

Integration Points

Protocol	Information collected	Used for
GitHub API	Logs from the GitHub Service	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "GitHub" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "GitHub" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "GitHub" in the main content panel **Search...** field to see the reports associated with this device.

Configuration Through API

- [Configuring GitHub Server](#)
- [Configuring FortiSIEM](#)

Configuring GitHub Server

Create an account to be used for FortiSIEM communication, followed by the creation of an access token (instructions for creating an access token follow).

Create Access Token

Take the following steps to create an Access Token.

Reference: Instructions for creating a token come from GitHub Docs. See [here](#) for more information.

1. In the upper right corner of any page, click your profile picture.
2. Click **Settings**.
3. In the left panel, click **Developer settings**, then click **Personal access tokens**.
4. Click **Generate new token**.
5. Click **Generate new token (classic)**.

6. In the **Note** field, enter a descriptive name for your token.
7. To give your token an expiration, select **Expiration**, then choose a default option or click **Custom** to enter a date, or choose **No Expiration**.
8. Select the scopes to grant this token. To use your token to access repositories from the command line, select **repo**. A token with no assigned scopes can only access public information. For more information, see [Scopes for OAuth apps](#). At a minimum, you must select **User scope** for FortiSIEM.
9. Click **Generate token**.
10. (Optional) To copy the new token to your clipboard, click the copy icon.

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access.

1. Login to FortiSIEM.
2. Go to **ADMIN > Setup > Credentials**.
3. In **Step 1: Enter Credentials**, click **New** to create a GitHub credential.
4. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	GitHub.com GitHub
Access Protocol	GitHub API
Pull Interval	The interval in which FortiSIEM will pull events. Default is 5 minutes.
Password Config	See Password Configuration
GitHub Token	Provide the GitHub token.
Organization	Choose the Organization if it is an MSP deployment and the same credential has to be used for multiple customers.
Description	Description of the device

5. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Set **IP/Host Name** to the IP address of the GitHub Server.
 - b. Select the **Credential** created in steps 3 and 4.
 - c. Click **Save**.
6. Select the entry in step 3 above and click the **Test** drop-down list, and select **Test Connectivity**.
7. After **Test Connectivity** succeeds, an entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from GitHub server using the API.

To test for received GitHub events:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the GitHub entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from GitHub in the last 15 minutes. You can modify the time interval to get more events.

Configuration Through Webhook

- [Prerequisite](#)
- [FortiSIEM Setup](#)
- [GitHub Setup](#)
- [Checking for Events](#)
- [Sample Event Type](#)

Prerequisite

Most applications using webhook push notifications do server TLS certificate validation, which means the target collector must be configured with a public CA signed TLS certificate.

See [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#) for configuration information.

FortiSIEM Setup

To configure webhook integration, you will need to take the following general steps.

- [Create Credential](#)

Create Credential

Take the following steps to configure a credential for FortiSIEM.

1. Login to FortiSIEM as an administrator.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the **Access Method Definition** window, input the following:
 - a. In the **Name** field, enter the name of the credential. This serves as the basis of the target endpoint created.
 - b. From the **Device Type** drop-down list, select **GitHub.com GitHub**.
 - c. From the **Access Protocol** drop-down list, select **Webhook**.
 - d. In the **Separator** field, leave the default as "\n" to separate the payload. The "\n" is the newline linefeed and means that each line in the response is treated as a new log.
 - e. In the **Receiver FQDN** field, enter the FQDN of the FortiSIEM node. This field expects the FQDN or IP address of the FortiSIEM collector that will be receiving the webhook traffic. This is used to help dynamically generate an endpoint configuration for you. This should ideally be the FQDN of the collector from the sending application's perspective. For example, if this is a SaaS application on the public internet, this will be a public FQDN, e.g. collector01.example.com.
 - f. In the **Reporting Host Name** field, enter "GitHub.com". This field expects the source hostname of the sending application. It is used to uniquely identify the logs as it will be in the header of every log. You can use something like example.com if example.com was the vendor's domain.
 - g. **Endpoint** is the dynamically generated webhook endpoint based on the receiver FQDN. This makes it easier to paste this URL as the target of your webhooks in the client application.
 - h. From the **Auth Type** drop-down list, select **HMAC**. HMAC uses a shared secret to create a hash signature with each payload from the HTTP request and then compares the value of the header/parameter in the HTTP request. It is client application dependent on whether they pass the hash in a specific HTTP header value, or an HTTP url parameter. After selecting HMAC, take the following steps.
 - i. From the **Algorithm** drop-down list, select **SHA-256**.
 - j. In the **Shared Secret** field, enter the shared secret.

- k. From the **Auth Part** drop-down list, select **Header**.
- l. In the **Header Name** field, enter "X-Hub-Signature-256".
- m. Click **Save and Deploy**.
- n. Click **Edit** to return to the webhook configuration you just saved. From the **Endpoint** row, copy the URL. This URL will be needed to configure webhook in [GitHub Setup](#).

Access Method Definition [X]

Name: github-webhook

Device Type: GitHub.com GitHub ▾

Access Protocol: Webhook ▾

Separator: \n

Receiver FQDN: 192.0.20.0

Reporting Host Name: GitHub.com

Endpoint: **https://192.0.20.0/webhook/github-webhook**

Auth Type: HMAC ▾

Algorithm: SHA-256 ▾

Shared Secret: [Copy]

Auth Part: Header ▾

Header Name: X-Hub-Signature-256

Description:

[Save and Deploy] [Cancel]

GitHub Setup

Documentation Reference: <https://docs.github.com/en/webhooks/using-webhooks/creating-webhooks>

First, ensure the [Prerequisite](#) is complete. Take the following steps to configure webhook for GitHub.

1. On [GitHub.com](#), navigate to your repository, click **Settings** and from the left sidebar, click **Webhooks**.

2. Click **Add webhook**.

3. Under **Payload URL**, enter/paste the URL of the webhook endpoint. You should have this information from your FortiSIEM configuration when you copied the URL from the **Endpoint** row.

It will be in the following format:

`https://<FortiSIEM_Node_IP>/webhook/<FortiSIEM_Credential_NAME>`

4. From the **Content type** drop-down list, select **application/json**.

5. Under **Secret**, enter a string to use as a secret. This secret token should be the same as the shared secret in your FortiSIEM configuration.

6. (Optional) Clear the Enable SSL verification checkbox to disable [SSL verification](#).

If you would like to leave SSL verification enabled, you must ensure the target FortiSIEM collector, or target device terminating the TLS connection is using a public CA signed TLS/SSL certificate.

Note: If **Enable SSL verification** is enabled, ensure the collector is setup with a valid TLS certificate. See the [Prerequisite](#) for more information.

7. Under "Which events would you like to trigger this webhook?", select the webhook events that you want to receive. You should only subscribe to the webhook events that you need. If you choose **Let me select individual events**, select the events that you want to trigger the webhook.

8. To make the webhook active immediately after adding the configuration, select **Active**.

9. Click **Add webhook**.

Checking for Events

Events can be queried from the **Analytics** page, using `github-` as part of a Raw Event Log search. Make sure [GitHub Setup](#) is completed before proceeding with your check for events.

From the FortiSIEM GUI, take the following steps.

1. Navigate to **Analytics > Search**.

2. Click **Edit Filters and Time Range.....**

3. In **Filter By**, select the **Event Attribute** tab.

4. Enter/select the following:

Attribute = Raw Event Log, Operator = CONTAIN, Value = `github-`

5. Click **Apply & Run**.

Sample Event Type

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=GitHub.com,[reptModel]=GitHub,[reptDevName]=GitHub.com,
[reptDevIpAddr]=1.1.1.1,[keyword]=push,[json]=
{"ref":"refs/heads/main","before":"dbfa142e611116231117ec45255c79d53e53929e","after":"ee67c6b5447
07af0d94f4111c1cf2d748729fb8","repository":{"id":768823079,"node_id":"R_kgDOLdNPJw","name":"DH_
TESTER","full_name":"Org1/DH_TESTER","private":true,"owner":
{"name":"Org1","email":null,"login":"Org1","id":23552948,"node_
id":"MDEyOk9xx2FuaXphdGlvbJlZNTUyOTQ4","avatar_
url":"https://avatars.githubusercontent.com/u/23552948?v=4","gravatar_
id":"","url":"https://api.github.com/users/Org1","html_url":"https://github.com/Org1","followers_
url":"https://api.github.com/users/Org1/followers","following_
```



```

url": "https://api.github.com/users/Org1/following{/other_user}", "gists_
url": "https://api.github.com/users/Org1/gists{/gist_id}", "starred_
url": "https://api.github.com/users/Org1/starred{/owner}/{/repo}", "subscriptions_
url": "https://api.github.com/users/Org1/subscriptions", "organizations_
url": "https://api.github.com/users/Org1/orgs", "repos_
url": "https://api.github.com/users/Org1/repos", "events_
url": "https://api.github.com/users/Org1/events{/privacy}", "received_events_
url": "https://api.github.com/users/Org1/received_events", "type": "Organization", "site_
admin": false, "html_url": "https://github.com/Org1/DH_TESTER", "description": "DH_
TEsTER", "fork": false, "url": "https://github.com/Org1/DH_TESTER", "forks_
url": "https://api.github.com/repos/Org1/DH_TESTER/forks", "keys_
url": "https://api.github.com/repos/Org1/DH_TESTER/keys{/key_id}", "collaborators_
url": "https://api.github.com/repos/Org1/DH_TESTER/collaborators{/collaborator}", "teams_
url": "https://api.github.com/repos/Org1/DH_TESTER/teams", "hooks_
url": "https://api.github.com/repos/Org1/DH_TESTER/hooks", "issue_events_
url": "https://api.github.com/repos/Org1/DH_TESTER/issues/events{/number}", "events_
url": "https://api.github.com/repos/Org1/DH_TESTER/events", "assignees_
url": "https://api.github.com/repos/Org1/DH_TESTER/assignees{/user}", "branches_
url": "https://api.github.com/repos/Org1/DH_TESTER/branches{/branch}", "tags_
url": "https://api.github.com/repos/Org1/DH_TESTER/tags", "blobs_
url": "https://api.github.com/repos/Org1/DH_TESTER/git/blobs{/sha}", "git_tags_
url": "https://api.github.com/repos/Org1/DH_TESTER/git/tags{/sha}", "git_refs_
url": "https://api.github.com/repos/Org1/DH_TESTER/git/refs{/sha}", "trees_
url": "https://api.github.com/repos/Org1/DH_TESTER/git/trees{/sha}", "statuses_
url": "https://api.github.com/repos/Org1/DH_TESTER/statuses/{sha}", "languages_
url": "https://api.github.com/repos/Org1/DH_TESTER/languages", "stargazers_
url": "https://api.github.com/repos/Org1/DH_TESTER/stargazers", "contributors_
url": "https://api.github.com/repos/Org1/DH_TESTER/contributors", "subscribers_
url": "https://api.github.com/repos/Org1/DH_TESTER/subscribers", "subscription_
url": "https://api.github.com/repos/Org1/DH_TESTER/subscription", "commits_
url": "https://api.github.com/repos/Org1/DH_TESTER/commits{/sha}", "git_commits_
url": "https://api.github.com/repos/Org1/DH_TESTER/git/commits{/sha}", "comments_
url": "https://api.github.com/repos/Org1/DH_TESTER/comments{/number}", "issue_comment_
url": "https://api.github.com/repos/Org1/DH_TESTER/issues/comments{/number}", "contents_
url": "https://api.github.com/repos/Org1/DH_TESTER/contents/{+path}", "compare_
url": "https://api.github.com/repos/Org1/DH_TESTER/compare/{base}...{head}", "merges_
url": "https://api.github.com/repos/Org1/DH_TESTER/merges", "archive_
url": "https://api.github.com/repos/Org1/DH_TESTER/{archive_format}/{/ref}", "downloads_
url": "https://api.github.com/repos/Org1/DH_TESTER/downloads", "issues_
url": "https://api.github.com/repos/Org1/DH_TESTER/issues{/number}", "pulls_
url": "https://api.github.com/repos/Org1/DH_TESTER/pulls{/number}", "milestones_
url": "https://api.github.com/repos/Org1/DH_TESTER/milestones{/number}", "notifications_
url": "https://api.github.com/repos/Org1/DH_TESTER/notifications
{?since,all,participating}", "labels_url": "https://api.github.com/repos/Org1/DH_TESTER/labels
{/name}", "releases_url": "https://api.github.com/repos/Org1/DH_TESTER/releases{/id}", "deployments_
url": "https://api.github.com/repos/Org1/DH_TESTER/deployments", "created_at": 1709841354, "updated_
at": "2024-03-08T17:54:58Z", "pushed_at": 1709946519, "git_url": "git://github.com/Org1/DH_
TESTER.git", "ssh_url": "git@github.com:Org1/DH_TESTER.git", "clone_
url": "https://github.com/Org1/DH_TESTER.git", "svn_url": "https://github.com/Org1/DH_
TESTER", "homepage": null, "size": 18, "stargazers_count": 0, "watchers_
count": 0, "language": "Python", "has_issues": true, "has_projects": true, "has_downloads": true, "has_
wiki": false, "has_pages": false, "has_discussions": false, "forks_count": 0, "mirror_

```

```

url":null,"archived":false,"disabled":false,"open_issues_count":1,"license":null,"allow_
forking":false,"is_template":false,"web_commit_signoff_required":false,"topics":
[],"visibility":"private","forks":0,"open_issues":1,"watchers":0,"default_
branch":"main","stargazers":0,"master_branch":"main","organization":"Org1","custom_properties":
{},"pusher":{"name":"ExampleUser1","email":"User1@fortinet.com"},"organization":
{"login":"Org1","id":23552948,"node_
id":"MDEyOk9yZ2FuaXphdGlvbWJlZnUyOTQ4","url":"https://api.github.com/orgs/Org1","repos_
url":"https://api.github.com/orgs/Org1/repos","events_
url":"https://api.github.com/orgs/Org1/events","hooks_
url":"https://api.github.com/orgs/Org1/hooks","issues_
url":"https://api.github.com/orgs/Org1/issues","members_
url":"https://api.github.com/orgs/Org1/members{/member}","public_members_
url":"https://api.github.com/orgs/Org1/public_members{/member}","avatar_
url":"https://avatars.githubusercontent.com/u/23552948?v=4","description":null},"enterprise":
{"id":132685,"slug":"dh-mei-enterprise","name":"dh-mei-enterprise","node_id":"E_
kgDOAAIGTQ","avatar_
url":"https://avatars.githubusercontent.com/b/132685?v=4","description":null,"website_
url":null,"html_url":"https://github.com/enterprises/dh-mei-enterprise","created_at":"2024-03-
07T20:52:55Z","updated_at":"2024-03-07T20:52:57Z"},"sender":
{"login":"ExampleUser1","id":23548610,"node_id":"MDQ6VXNlcjZlZnUyOTQ4NjEw","avatar_
url":"https://avatars.githubusercontent.com/u/23548610?v=4","gravatar_
id":"","url":"https://api.github.com/users/ExampleUser1","html_
url":"https://github.com/ExampleUser1","followers_
url":"https://api.github.com/users/ExampleUser1/followers","following_
url":"https://api.github.com/users/ExampleUser1/following{/other_user}","gists_
url":"https://api.github.com/users/ExampleUser1/gists{/gist_id}","starred_
url":"https://api.github.com/users/ExampleUser1/starred{/owner}/{repo}","subscriptions_
url":"https://api.github.com/users/ExampleUser1/subscriptions","organizations_
url":"https://api.github.com/users/ExampleUser1/orgs","repos_
url":"https://api.github.com/users/ExampleUser1/repos","events_
url":"https://api.github.com/users/ExampleUser1/events{/privacy}","received_events_
url":"https://api.github.com/users/ExampleUser1/received_events","type":"User","site_
admin":false},"created":false,"deleted":false,"forced":false,"base_
ref":null,"compare":"https://github.com/Org1/DH_
TESTER/compare/dbfa142e6111...ee67c6b54470","commits":
[{"id":"ee67c6b544707af0d22f4f901c1cf2d748729fb8","tree_
id":"631ce064279a99204114fedab7c40678285e596","distinct":true,"message":"Update new_file_
1","timestamp":"2024-03-08T17:08:39-08:00","url":"https://github.com/Org1/DH_
TESTER/commit/ee67c6b544707af0d94f4f901c1cf2d748729fb8","author":
{"name":"ExampleUser1","email":"User1@fortinet.com","username":"ExampleUser1"},"committer":
{"name":"GitHub","email":"noreply@github.com","username":"web-flow"},"added":[],"removed":
[],"modified":["new_file_1"]},"head_commit":
{"id":"ee67c6b544707af0d94f4f901c1cf2d748729fb8","tree_
id":"631ce064279a989204774fedab7c40678285e596","distinct":true,"message":"Update new_file_
1","timestamp":"2024-03-08T17:08:39-08:00","url":"https://github.com/Org1/DH_
TESTER/commit/ee67c6b544707af0d94f4f901c1cf2d748729fb8","author":
{"name":"ExampleUser1","email":"User1@fortinet.com","username":"ExampleUser1"},"committer":
{"name":"GitHub","email":"noreply@github.com","username":"web-flow"},"added":[],"removed":
[],"modified":["new_file_1"]}]

```

GitLab

Support Added: FortiSIEM 7.2.0

Vendor Version Tested: Not Provided

Vendor: GitLab

Product Information: <https://about.gitlab.com/platform/>

Comprehensive AI-powered DevSecOps platform.

- [Configuration](#)
- [Checking for Events](#)
- [Event Type](#)

Configuration

- [Prerequisite](#)
- [FortiSIEM Setup](#)
- [GitLab Setup](#)

Prerequisite

Most applications using webhook push notifications do server TLS certificate validation, which means the target collector must be configured with a public CA signed TLS certificate.

See [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#) for configuration information.

FortiSIEM Setup

To configure webhook integration, you will need to take the following general steps.

- [Create Credential](#)

Create Credential

Take the following steps to configure a credential for FortiSIEM.

1. Login to FortiSIEM as an administrator.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the **Access Method Definition** window, input the following:
 - a. In the **Name** field, enter the name of the credential. This serves as the basis of the target endpoint created.

- b. From the **Device Type** drop-down list, select **GitLab GitLab**.
- c. From the **Access Protocol** drop-down list, select **Webhook**.
- d. In the **Separator** field, leave the default as "\n" to separate the payload. The "\n" is the newline linefeed and means that each line in the response is treated as a new log.
- e. In the **Receiver FQDN** field, enter the FQDN of the FortiSIEM node. This field expects the FQDN or IP address of the FortiSIEM collector that will be receiving the webhook traffic. This is used to help dynamically generate an endpoint configuration for you. This should ideally be the FQDN of the collector from the sending application's perspective. For example, if this is a SaaS application on the public internet, this will be a public FQDN, e.g. collector01.example.com.
- f. In the **Reporting Host Name** field, enter "GitLab.com". This field expects the source hostname of the sending application. It is used to uniquely identify the logs as it will be in the header of every log. You can use something like example.com if example.com was the vendor's domain.
- g. **Endpoint** is the dynamically generated webhook endpoint based on the receiver FQDN. This makes it easier to paste this URL as the target of your webhooks in the client application.
- h. From the **Auth Type** drop-down list, select **Simple Secret**. Simple Secret compares the secret with the value of header/ parameter in HTTP request directly.
 - i. In the **Shared Secret** field, enter the shared secret.
 - j. From the **Auth Part** drop-down list, select **Header**.
 - k. In the **Header Name** field, enter "X-Gitlab-Token".
 - l. Click **Save and Deploy**.
- m. Click **Edit** to return to the Webhook configuration you just saved. From the **Endpoint** row, copy the URL. This URL will be needed to configure webhook in [GitLab Setup](#).

Access Method Definition

Name: GitLab-webhook

Device Type: GitLab GitLab

Access Protocol: Webhook

Separator: \n

Receiver FQDN: 192.0.20.0

Reporting Host Name: GitLab.com

Endpoint: https://192.0.20.0/webhook/GitLab-webhook

Auth Type: Simple Secret

Shared Secret:

Auth Part: Header

Header Name: X-Gitlab-Token

Description:

Save and Deploy

Cancel

GitLab Setup

Reference Documentation: <https://docs.gitlab.com/ee/user/project/integrations/webhooks.html>

1. From your project or group, on the left sidebar, navigate to **Settings > Webhooks**.
2. Click **Add new webhook**.
3. In the **URL** field, enter/paste the URL of the webhook endpoint. You should have this information from your FortiSIEM configuration when you copied the URL from the **Endpoint** row.

It will be in the following format:

`https://<FortiSIEM_Node_IP>/webhook/<FortiSIEM_Credential_NAME>`

4. Check **Show full URL.**

5. In the **Secret token field, enter the secret token to validate payloads. This secret token should be the same as the shared secret in your FortiSIEM configuration.**

6. In the **Trigger section, select the events that will trigger the webhook.**

7. (Optional) Clear the Enable SSL verification checkbox to disable [SSL verification](#).

If you would like to leave SSL verification enabled, you must ensure the target FortiSIEM collector, or target device terminating the TLS connection is using a public CA signed TLS/SSL certificate.

Note: If **Enable SSL verification** is enabled, ensure the collector is setup with a valid TLS certificate. See the [Prerequisite](#) for more information.

8. Click **Add webhook.**

Checking for Events

Events can be queried from the **Analytics** page, using gitlab- as part of a Raw Event Log search. Make sure [GitLab Setup](#) is completed before proceeding with your check for events.

1. Navigate to **Analytics > Search.**

2. Click **Edit Filters and Time Range....**

3. In **Filter By, select the **Event Attribute** tab.**

4. Enter/select the following:

Attribute = Raw Event Log, Operator = CONTAIN, Value = gitlab-

5. Click **Apply & Run.**

Event Type

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=GitLab,[reptModel]=GitLab,[reptDevName]=Gitlab.com,
[reptDevIpAddr]=192.0.20.1,[json]={ "object_kind": "push", "event_
name": "push", "before": "f6b6bc1d9fb2bb191c61e934031f10931e198088", "after": "f6b6bc1d9fb2bb191c61e934
031f10931e198088", "ref": "refs/heads/main", "ref_protected": true, "checkout_
sha": "f6b6bc1d9fb2bb191c61e934031f10931e198088", "message": null, "user_id": 20685255, "user_
name": "user1", "user_username": "user1", "user_email": null, "user_
avatar": "https://secure.gravatar.com/avatar/b28999676eb9a776197e27504358c0bfce1d1ebf9771c550bd51a2
fde1702833?s=80&d=identicon", "project_id": 56310484, "project":
{ "id": 56310484, "name": "testProject2", "description": null, "web_
url": "https://gitlab.com/testgroup432113/testproject2", "avatar_url": null, "git_ssh_
url": "git@gitlab.com:testgroup432113/testproject2.git", "git_http_
url": "https://gitlab.com/testgroup432113/testproject2.git", "namespace": "testGroup", "visibility_
level": 20, "path_with_namespace": "testgroup432113/testproject2", "default_branch": "main", "ci_config_
path": "", "homepage": "https://gitlab.com/testgroup432113/testproject2", "url": "git@gitlab.com:testgr
oup432113/testproject2.git", "ssh_url": "git@gitlab.com:testgroup432113/testproject2.git", "http_
url": "https://gitlab.com/testgroup432113/testproject2.git"}, "commits":
[ { "id": "f6b6bc1d9fb2bb191c61e934031f10931e198088", "message": "Initial commit", "title": "Initial
commit", "timestamp": "2024-03-
28T22:44:51+00:00", "url": "https://gitlab.com/testgroup432113/testproject2/-
```

```
/commit/f6b6bc1d9fb2bb191c61e934031f10931e198088","author":  
{ "name": "user1", "email": "user1@abc.com"}, "added": [ "README.md", "modified": [], "removed":  
[] }, "total_commits_count": 1, "push_options": {}, "repository":  
{ "name": "testProject2", "url": "git@gitlab.com:testgroup432113/testproject2.git", "description": null,  
"homepage": "https://gitlab.com/testgroup432113/testproject2", "git_http_  
url": "https://gitlab.com/testgroup432113/testproject2.git", "git_ssh_  
url": "git@gitlab.com:testgroup432113/testproject2.git", "visibility_level": 20 }
```

GitLab API

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Syslog Integration](#)
- [API Integration](#)
- [Configuring GitLab Server](#)
- [Configuring FortiSIEM for GitLab API](#)
- [Sample Event](#)

Integration Points

Protocol	Information collected	Used For
syslog	15 Log files including production.log and application.log – over 130 event types pre-fixed with 'GitLab-'	Security and Compliance
API	Code commit, Changes to Projects, Branches, Tag, DiscussionNoted, Tag, Issues, Snippets, Repositories, User created, deleted, modified.	Security and Compliance

Event Types

In **RESOURCES > Event Types**, enter "GitLab" in the main content panel **Search...** field to see the events associated with this device.

Rules

No defined rules.

Reports

In **RESOURCES > Reports**, enter "GitLab" in the main content panel **Search...** field to see the reports associated with this device.

Syslog Integration

In FortiSIEM 7.x, there are two methods to send GitLab syslogs. Of the two methods, Fortinet recommends sending syslog via rsyslog forwarding.

- [Syslog via Rsyslog Forwarding](#)
- [Syslog via GitLab remote_syslog](#)

Syslog via Rsyslog Forwarding

To use rsyslog to collect and send GitLab logs via syslog, take the following steps:

Note: For detailed information on GitLab logs, see <https://docs.gitlab.com/ee/administration/logs/>.

1. Locate where your GitLab installation is writing log files, such as error or access logs. The typical location is provided here:

```
/var/log/gitlab/gitlab-rails/
/home/git/gitlab/log/
```

2. Locate the rsyslog.conf file on your GitLab server. The typical location is provided here:

```
/etc/rsyslog.conf
```

3. Add the imfile module to your rsyslog.conf file in the modules section.

```
module(load="imfile" PollingInterval="10")
```

4. Insert the following lines for GitLab logs in your rsyslog.conf file.

```
input(type="imfile" File="/path/to/application_json.log"
Tag=" GitLab_Application:"
Severity="info"
Facility="local6")
```

Notes:

- The Tag= line is critical as this string is matched in the FortiSIEM parser, do NOT modify it from the example above.
- The Tag= line is case sensitive.
- In addition to application_json.log in this step, you can also add the following suggested log files

- production_json.log
- api_json.log
- git_json.log
- Integrations_json.log
- audit_json.log
- gitlab-shell.log
- auth_json.log
- exceptions_json.log

by inserting the following lines for each additional log you wish to add.

```
input(type="imfile" File="/path/to/<suggested_Log>"
Tag=" <Log type>:"
```

Example: To add git_json.log, you would make the following changes:

```
input(type="imfile" File="/path/to/git_json.log"
Tag=" GitLab_GitRepo:"
```

5. Place the following in the rules section in your rsyslog.conf file.

```
local6.* @<FortiSIEM collector IP or hostname>:514
```

Note: Replace <FortiSIEM collector IP or hostname> with the IP address or hostname of your actual FortiSIEM collector.

6. Restart rsyslog by running the following command.

```
systemctl restart rsyslog
```

7. Confirm that logs are arriving. Ensure that your firewall(s) allow UDP 514 inbound to target IP.

Example Log

```
<13>Feb 21 13:07:48 gitlab-test.example.com GitLab_Application: {"severity":"INFO","time":"2024-02-21T21:07:48.922Z","correlation_id":"01HQ6QXZPDZARVY2F2TJCHNJC1","meta.caller_id":"PipelineProcessWorker","meta.remote_ip":"192.0.2.0","meta.feature_category":"continuous_integration","meta.root_namespace":"devops","meta.client_id":"client/1122","meta.root_caller_id":"POST /api/:version/jobs/request","message":"Enqueuing hooks for Pipeline 772217: running","class":"Ci::Pipeline","pipeline_id":772217,"project_id":2642,"pipeline_status":"running"}
```

How It Works: The bolded section in the example log matches the Tag= definition in the rsyslog.conf file. This unique string is matched in the FortiSIEM GitLabLogParser.

Syslog via GitLab remote_syslog

Configure GitLab to send syslog to FortiSIEM via UDP on port 514. See [here](#) for details.

FortiSIEM will automatically detect GitHubLab log patterns and parse the logs. Currently, the following log files are parsed: api_json.log, application.log, gitaly, gitlab-monitor, gitlab-shell.log, gitlab-workhorse.log, gitlab_access.log, production.log, production_json.log, Prometheus, Redis, remote-syslog, sidekiq, sidekiq_exporter.log, unicorn_stderr.log.

Currently, over 134 GitLab event types are parsed. To see the event types:

1. Login to FortiSIEM.
2. Go to **RESOURCES > Event Types**.
3. Search for "GitLab".

Use cases covered via syslog:

- Failed and Successful Login
- Git command execution
- Git API requests

To test for received GitLab events received via syslog:

1. Login to FortiSIEM.
2. Go to **ANALYTICS**.
3. Click the **Edit Filters and Time Range...** field:
 - a. Choose the **Event Attribute** option.
 - b. Create the Search condition
Attribute: Event Type
Operator: CONTAIN
Value: GitLab
 - c. Change **Time Range** to be Last 1 Hour
 - d. Click **Apply & Run**.
4. See the GitLab events on the GUI.

API Integration

FortiSIEM can also pull logs from GitLab using GitLab API.

Currently, over 134 GitLab event types are parsed. To see the event types:

1. Login to FortiSIEM.
2. Go to **RESOURCES > Event Types**.
3. Search for "GitLab".

Use cases covered via API:

- Code commit – note that the current API does not capture committed files.
- Changes to Projects, Branches, Tag, DiscussionNoted, Tag, Issues, Snippets, Repositories etc
- User created, deleted, modified

For more details, see [here](#).

Configuring GitLab Server

Create a personal access token to be used for FortiSIEM communication.

1. Login to your GitLab account.
2. Go to your **Profile settings**.
3. Go to **Access tokens**.
4. Choose a name and optionally an expiry date for the token.
5. Choose the desired scopes: **api** is required.
6. Click **Create Personal Access Token**. Save the personal access token in your local system. Note that once you leave or refresh the page, you won't be able to access it again.

For more details, see [here](#).

Configuring FortiSIEM for GitLab API

Use the Personal Access Token in [Configuring GitLab Server](#) to enable FortiSIEM access.

1. Login to FortiSIEM.
2. Go to **ADMIN > Setup > Credentials**.
3. In **Step 1: Enter Credentials**, click **New** to create a GitLab credential.
4. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	GitLab GitLab (Vendor = GitLab, Model = Gitlab)
Access Protocol	GitLab API
Pull Interval	The interval in which FortiSIEM will pull events from GitLab. Default is 5 minutes.
Password Config	Manual
Account Name	Enter an account name.
Personal Access	Enter the token you obtained in

Settings	Description
Token	Configuring GitLab Server.
Description	Description of the device

5. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. In **IP/Host Name**, enter the **IP** of GitLab Server.
 - b. Select the **Credential** created in step 4 above.
 - c. Click **Save**.
6. Select the entry in step 3 above, click the **Test** drop-down list and select **Test Connectivity**. Once successful, an entry will be created in **ADMIN > Setup > Pull Events**. FortiSIEM will start to pull events from GitLab using the API.

To test for received GitLab events:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the GitLab entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from GitLab in the last 15 minutes. You can modify the time interval to get more events.

Sample Event

```
[GITLAB_EVENT_DATA] = {"action_name":"pushed to","author":{"avatar_url":"https://abc.cda.com/avatar/62e30f8b2d3cbc60ed22c217c5fa4e57?s=80&d=identicon","id":185,"name":"user1","state":"active","username":" user1","web_url":"https://dac.com/gitmirror"},"author_id":185,"author_username":" user1","created_at":"2018-11-13T22:30:30.340Z","project_id":553,"push_data":{"action":"pushed","commit_count":2,"commit_from":"da5a4fd97fd1f6b7c5a8611c12592eb5e9ff9e2b","commit_title":"Merge \Fix bizservice popup display issue and switching org in bizz...","commit_to":"30d863ece3957aacc95ec45c7663c426c73f38f2","ref":"releases/FCS5_2_1","ref_type":"branch"},"serverIp":"192.0.2.0","serverName":"abc.com","target_id":null,"target_iid":null,"target_title":null,"target_type":null}
```

GitLab CLI

Events that are obtained with the GitLab REST API do not contain up-to-date information. To avoid this limitation, FortiSIEM uses the GitLab CLI to obtain events from the GitLab server in real time.

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Generate an SSH Key in FortiSIEM](#)
- [Configure an SSH Key in GitLab](#)
- [Configuration in FortiSIEM](#)
- [Sample Events](#)

Integration Points

Protocol	Information collected	Used for
GIT CLI	Git commit history	Security and Compliance

Event Types

In **RESOURCES > Event Types**, enter "GitLab" in the main content panel **Search...** field to see the events associated with this device.

Rules

No defined rules.

Reports

In **RESOURCES > Reports**, enter "GitLab" in the main content panel **Search...** field to see the reports associated with this device.

Generate an SSH Key in FortiSIEM

Generate an SSH key for FortiSIEM. The key will allow you to access the GitLab by using Git commands. Use the following command to generate the public key file and the private key file in the `/opt/phoenix/bin/.ssh/` directory.

```
ssh-keygen -t rsa -b 4096 -C "root@localhost"
```

Configure an SSH Key in GitLab

Complete these steps to install the SSH key in the GitLab server:

1. Login to your GitLab account.
2. Select **Settings** from your account drop-down list.
3. Select the **SSH Keys** tab.
4. Add the public part of the key, for example:
`/opt/phoenix/bin/.ssh/id_rsa.pub`
5. Click **Add Key**.
6. Install Git, for example:
`yum install git`

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	GitLab GitLab
Access Protocol	GIT CLI
Pull Interval	The interval in which FortiSIEM will pull events from GitLab. Default is 5 minutes.
Local Path to Clone	The path to the location on your system where the repository will be downloaded. In the case of very large repositories, this gives users the opportunity to specify a location on an external device.
Repositories	The address of the repository in Git. You can enter multiple repositories, separated by whitespaces.
Description	Description of the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter an IP or an IP range in the **IP/Host Name** field.
 - b. Select the name of your GitLab credential from the **Credentials** drop-down list.

- c. Click **Save**.
4. With your Credentials entry selected from Step 3, click the **Test** drop-down list and select **Test Connectivity** to test the connection to GitLab CLI.
5. To see the jobs associated with GitLab, select **ADMIN > Setup > Pull Events**.
6. To see the received events, select **ANALYTICS**, then enter "GitLab" in the search box.

Sample Events

```
[PH_DEV_MON_GIT_COMMIT]: [deviceTime]=1547013028,[user]="abc",  
[exchMboxName]="abc@fortinet.com",[hashCode]="fa408380aa4296d13aeb24418164994eea2c2737",  
[preHashCode]="d9cd6e31346611a4f75dc7fe768f6202a46dd7e6",[title]="Add new file",[details]="",  
[updateCount]="1",[deleteCount]="0",[filePath]="testfile2",[fileType]="testfile2",  
[repoURL]="git@dops-git.fortinet-us.com:abc/testproject_willremove.git"
```

Unified Communication Server Configuration

FortiSIEM supports these VoIP servers for discovery and monitoring.

- [Avaya Call Manager](#)
- [Cisco Call Manager](#)
- [Cisco Contact Center](#)
- [Cisco Presence Server](#)
- [Cisco Tandberg Telepresence Video Communication Server \(VCS\)](#)
- [Cisco Telepresence Multipoint Control Unit \(MCU\)](#)
- [Cisco Telepresence Video Communication Server](#)
- [Cisco Unity Connection](#)

Avaya Call Manager

- What is Discovered and Monitored
- Event Types
- Configuration
- Configure FortiSIEM to Receive CDR Records from Avaya Call Manager
- Configure Avaya Call Manager to Send CDR Records to FortiSIEM
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	System metrics: Uptime, Interface utilization	Performance Monitoring
SFTP		Call Description Records (CDR): Calling Phone IP, Called Phone IP, Call Duration	Performance and Availability Monitoring

Event Types

Avaya-CM-CDR: Avaya CDR Records

Configuration

- SNMP
- SFTP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

SFTP

SFTP is used to send Call Description Records (CDRs) to FortiSIEM.

Configure FortiSIEM to Receive CDR Records from Avaya Call Manager

1. Log in to your FortiSIEM virtual appliance as root over SSH.
2. Change the directory.
`cd /opt/phoenix/bin`
3. Create an FTP account for user **ftpuser** with the home directory `/opt/phoenix/cache/avayaCM/<call-manager-ip>`. If this is the first time you have created a Call Manager definition, you will be prompted for the ftpuser password. When you create subsequent Call Manager definitions, the same password will be used, and you will see a Success message when the definition is created.
4. The CDR records do not have field definitions, but only values. Field definitions are needed to properly interpret the values. Make sure that the CDR fields definitions matches the default one supplied by FortiSIEM in `/opt/phoenix/config/AvayaCDRConfig.csv`.

FortiSIEM will interpret the CDR record fields according to the field definitions specified in: `/opt/phoenix/config/AvayaCDRConfig.csv` and generate events like the following:

```
Wed Feb 4 14:37:41 2015 1.2.3.4 FortiSIEM-FileLog-AvayaCM [Time of day-hours]="11" [Time of
day-minutes]="36" [Duration-hours]="0" [Duration-minutes]="00" [Duration-tenths of
minutes]="5" [Condition code]="9" [Diald number]="5908" [Calling number]="5555550001"
[FRL]="5" [Incoming circuit ID]="001" [Feature flag]="0" [Attendant console]="8" [Incoming
TAC]="01 1" [INS]="0" [IXC]="00" [Packet count]="12" [TSC flag]="1"
```

Configure Avaya Call Manager to Send CDR Records to FortiSIEM

1. Log in to Avaya Call Manager.
2. Send CDR records to FortiSIEM by using this information

Field	Value
Host Name/IP Address	<FortiSIEM IP Address>
User Name	ftpuser
Password	<The password you created for ftpuser>
Protocol	SFTP
Directory Path	/opt/phoenix/cache/ avayaCM/<call-manager-ip>

Settings for Access Credentials in FortiSIEM

See [Access Credentials](#) to set access and protocol for SMTP, SSH, and Telnet.

Cisco Call Manager

- What is Discovered and Monitored
- Event Types
- Rules
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	System metrics: Uptime, CPU utilization, Memory utilization, Disk utilization, Interface utilization, Process count, Per process: CPU utilization, Memory utilization	Performance Monitoring
SNMP	VoIP phones and registration status	Call Manager metrics: Global Info: VoIP phone count, Gateway count, Media Device count, Voice mail server count and SIP Trunks count broken down by Registered/Unregistered/Rejected status (FortiSIEM Event Type: PH_DEV_MON_CCM_GLOBAL_INFO) SIP Trunk Info: Trunk end point, description, status (FortiSIEM Event Type: PH_DEV_MON_CCM_SIP_TRUNK_STAT) SIP Trunk Addition, Deletion: FortiSIEM Event Type: PH_DEV_MON_CCM_NEW_SIP_TRUNK, PH_DEV_MON_CCM_DEL_SIP_TRUNK Gateway Status Info: Gateway name, Gateway IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_GW_STAT) Gateway Status Change, Addition, Deletion: FortiSIEM Event Type: PH_DEV_MON_CCM_GW_STAT_CHANGE, PH_DEV_MON_CCM_NEW_GW, PH_DEV_MON_CCM_DEL_GW H323 Device Info: H323 Device name, H323 Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_H323_STAT) Gateway Status Change, Addition, Deletion: FortiSIEM Event Type: PH_DEV_MON_CCM_H323_STAT_CHANGE, PH_DEV_MON_CCM_NEW_H323, PH_DEV_MON_CCM_DEL_H323 Voice Mail Device Info: Voice Mail Device name, Voice Mail Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_VM_STAT)	Availability Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Voice Mail Device Status Change, Addition, Deletion: FortiSIEM Event Type: PH_DEV_MON_CCM_VM_STAT_CHANGE, PH_DEV_MON_CCM_NEW_VM, PH_DEV_MON_CCM_DEL_VM Media Device Info: Media Device name, Media Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_MEDIA_STAT) Media Device Status Change, Addition, Deletion: FortiSIEM Event Type: PH_DEV_MON_CCM_MEDIA_STAT_CHANGE, PH_DEV_MON_CCM_NEW_MEDIA, PH_DEV_MON_CCM_DEL_MEDIA Computer Telephony Integration (CTI) Device Info: CTI Device name, CTI Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_CTI_STAT) CTI Device Status Change, Addition, Deletion: FortiSIEM Event Type: PH_DEV_MON_CCM_CTI_STAT_CHANGE, PH_DEV_MON_CCM_NEW_CTI, PH_DEV_MON_CCM_DEL_CTI	
WMI (for Windows based Call Managers)	Application type, service mappings	Process level metrics: Per process: Uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
SFTP		Call Description Records (CDR): Calling Phone IP, Called Phone IP, Calling Party Number, Original Called Party Number, Final Called Party Number, Call Connect Time, Call Disconnect Time, Call Duration Call Management Records (CMR): Latency, Jitter, Mos Score - current, average, min, max for each call in CDR	Performance and Availability Monitoring
Syslog		Syslog messages from Cisco Call Manager as well as Cisco Unified Real Time Monitoring Tool (RTMT)	

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco_uc" and "cisco_uc_rtmt" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "cisco call manager" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

- SNMP
- WMI (for Call Manager installed under Windows)
- SFTP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

WMI (for Call Manager installed under Windows)

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- [Creating a Generic User Who Does Not Belong to the Local Administrator Group](#)
- [Creating a User Who Belongs to the Domain Administrator Group](#)

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add**.
6. Find the user you created, and then click **OK**.
This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **EditDefault**.

7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Enable remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2**.
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced**.
8. Select the user you created for the monitoring account, and then click **Edit**.
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and then click **OK**.

SFTP

SFTP is used to send Call Description Records (CDRs) to FortiSIEM.

- [Configure FortiSIEM to Receive CDR Records from Cisco Call Manager](#)
- [Configure Cisco Call Manager to Send CDR Records to FortiSIEM](#)

Configure FortiSIEM to Receive CDR Records from Cisco Call Manager

1. Log in to your FortiSIEM virtual appliance as root over SSH.
2. Change the directory.

```
cd /opt/phoenix/bin
```

3. Run `./phCreateCdrDestDir <call-manager-ip>`.
This creates an FTP account for user **ftpuser** with the home directory `/opt/phoenix/cache/ccm/<call-manager-ip>`. If this is the first time you have created a Call Manager definition, you will be prompted for the ftpuser password. When you create subsequent Call Manager definitions, the same password will be used, and you will see a Success message when the definition is created.
4. Switch user to admin by issuing "su - admin"
5. Modify phoenix_config.txt entry

```
ccm_ftp_directory=/opt/phoenix/cache/ccm
```

6. Restart phParser by issuing "killall -9 phParser"

Configure Cisco Call Manager to Send CDR Records to FortiSIEM

1. Log in to Cisco Call Manager.
2. Go to **Tools > CDR Management Configuration**.
The CDR Management Configuration window will open.
3. Click **Add New**.
4. Enter this information.

5.

Field	Value
Host Name/IP Address	<FortiSIEM IP Address>
User Name	ftpuser
Password	<The password you created for ftpuser>
Protocol	SFTP
Directory Path	/opt/phoenix/cache/ccm/<call-manager-ip>

6. Click **Save**.

Settings for Access Credentials

See [Access Credentials](#) to set access and protocol for SMTP, SSH, and Telnet.

Cisco Contact Center

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Configuration](#)
- [Setting Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	System metrics: CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization, Install software change	Performance Monitoring
SSH		Disk I/O monitoring	

Event Types

There are no event types defined specifically for this device.

Rules

In **RESOURCES > Rules**, search for "cisco contact center" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

- [SNMP](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Setting Access Credentials

See [Access Credentials](#) to set access and protocol for SMTP, SSH, and Telnet.

Cisco Presence Server

- What is Discovered and Monitored
- Event Types
- Configuration
- Setting Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	System metrics: CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization, Install software change	Performance Monitoring
SSH		Disk I/O monitoring	

Event Types

There are no event types defined specifically for this device.

Configuration

- [SNMP](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Setting Access Credentials

See [Access Credentials](#) to set access and protocol for SMTP, SSH, and Telnet.

Cisco Tandberg Telepresence Video Communication Server (VCS)

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	System metrics: CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization, Install software change	Performance Monitoring
SSH		Disk I/O monitoring	

Event Types

There are no event types defined specifically for this device.

Configuration

- SNMP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#)

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Cisco Telepresence Multipoint Control Unit (MCU)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Setting Access Credentials](#)

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Cisco Tandberg VCS

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	System metrics: Uptime, Interface utilization	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco telepresence" to see the event types associated with this device.

Configuration

- [SNMP](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#)

Setting Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Cisco Telepresence Video Communication Server

- What is Discovered and Monitored
- Event Types

What is Discovered and Monitored

Protocol	Logs parsed	Used for
Syslog	Call attempts, Call rejects, Media stats, Request, response, Search	Log Analysis

Event Types

In **Admin > Device Support > Event Types**, search for "Cisco-TVCS" to see the event types associated with this device.

Cisco Unity Connection

- What is Discovered and Monitored
- Event Types
- Rules
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	System metrics: CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco unity" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "cisco unity" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

- SNMP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

See [Access Credentials](#) to set access and protocol for SMTP, SSH, and Telnet.

Web Server

FortiSIEM supports these web servers for discovery and monitoring.

- [Apache Web Server](#)
- [Microsoft IIS for Windows 2000 and 2003](#)
- [Microsoft IIS for Windows 2008](#)
- [NGINX Web Server](#)

Apache Web Server

Support Added: FortiSIEM 4.8.1

Last Modification: FortiSIEM 7.2.3

Vendor Version Tested: Not Provided

Vendor: The Apache Software Foundation and the Apache HTTP Server Project

Product: Web Server

Product Information: <https://httpd.apache.org/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)
- [Define the Apache Log Format](#)
- [Apache Syslog Log Format](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level metrics: CPU utilization, Memory utilization	Performance Monitoring
HTTP(S) via the mod-status module		Apachemetrics: Uptime, CPU load, Total Accesses, Total Bytes Connections, Requests/sec, Bytes/sec, Bytes/req, Busy Workers, Idle Workers	Performance Monitoring
Syslog	Application type	W3C access logs: attributes include Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "apache" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "apache" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

The Apache Web Server Configuration instructions utilizes a reference point for where Apache installs by default. Based on your own configuration, Apache may be installed in the following locations:

```
/etc
/etc/httpd
/usr/local
```

Adjust your configuration according to your installed Apache directory.

- [Syslog via Rsyslog](#)
- [SNMP](#)
- [HTTPS](#)
- [Syslog via FortiSIEM Windows Agent or Linux Agent](#)

Syslog via Rsyslog

To use rsyslog to collect and send Apache logs via syslog, take the following steps:

Notes:

- Rsyslog Tag= is case sensitive, so ensure it is entered properly.
 - For steps 4 and 5, change the path as required to direct it to your *ssl_access.log* and *ssl_error.log* files.
 - For step 6, replace *<FortiSIEM collector IP or hostname>* with your actual FortiSIEM collector IP or hostname.
1. Locate where your Apache installation is writing log files, such as error or access logs. Here is a typical location:


```
/var/log/httpd/ssl_access_log
/var/log/httpd/ssl_error_log
```
 2. Locate rsyslog.conf. Here is a typical location:


```
/etc/rsyslog.conf
```
 3. Add imfile module to your rsyslog.conf file in the modules section.


```
module(load="imfile" PollingInterval="10")
```
 4. Place the following inputs below the modules section for Apache access log in your rsyslog.conf file.


```
input(type="imfile" File="/var/log/httpd/ssl_access_log"
Tag="Apache_AccessLog:"
Severity="error"
Facility="local6")
```
 5. Place the following inputs below for Apache error log in your rsyslog.conf file.


```
input(type="imfile" File="/var/log/httpd/ssl_error_log"
```

```
Tag="Apache_ErrorLog:"
Severity="info"
Facility="local6")
```

6. Place the following in the rules section in your `rsyslog.conf` file.
`local6.* @<FortiSIEM collector IP or hostname>:514`
7. Restart rsyslog by running the following command.
`systemctl restart rsyslog`
8. Confirm that logs are arriving. Ensure that your firewall(s) allow UDP 514 inbound to target IP.

Example Log

```
<179>Mar 22 00:41:50 lab1.example.com Apache_AccessLog: 192.0.20.0 - - [22/Mar/2022:00:41:48
+0000] "POST
/phoenix/rest/h5/rt/start2?t=t1647909924028&s=333078424F54496950533135435470487275415A597470545138
7635564B39496D4949717865776A HTTP/1.1" 200 36
```

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

HTTPS

To communicate with FortiSIEM over HTTPS, you must configure the `mod_status` module in your Apache web server.

1. Log in to your web server as an administrator.
2. Open the configuration file `/etc/Httpd.conf`.
3. Modify the file as shown in these code blocks, depending on whether you are connecting over HTTP without authentication, or over HTTPS with authentication.

Without Authentication

```
LoadModule status_module modules/mod_status.so
...
ExtendedStatus on
...
#Configuration without authentication
<Location /server-status>      SetHandler server-status
    Order Deny,Allow
    Deny from all
    Allow from .foo.com
</Location>
```

With Authentication

```
LoadModule status_module modules/mod_status.so
...
ExtendedStatus on
```

```

...
#Configuration with authentication
<Location /server-status>      SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from all
    AuthType Basic
    AuthUserFile /etc/httpd/account/users
    AuthGroupFile /etc/httpd/account/groups
    AuthName "Admin"      Require group admin
    Satisfy all
</Location>

```

4. If you are using authentication, you will have to add user authentication credentials.
 - a. Go to /etc/httpd, and if necessary, create an account directory.
 - b. In the account directory, create two files, users and groups.
 - c. In the groups file, enter admin:admin.
 - d. Create a password for the admin user.

```
htpasswd --c users admin
```

5. Reload Apache.

```
/etc/init.d/httpd reload
```

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog via FortiSIEM Windows Agent or Linux Agent

- [Configuring Windows Agent](#)
- [Configuring Linux Agent](#)

For Windows Agent, take the following steps:

1. Login to FortiSIEM GUI.
2. Navigate to **Admin > Setup**, and click the **Windows Agent** tab.
3. Under **Windows Agent Monitor Templates**, click **New** to create a new template, or click an existing template and click **Edit**.
4. If creating a new template, on the **Generic** tab, in the **Name** field, enter a name for the template.
5. Click the **User Log** tab, and click **New**.
 - a. In the **Full File Name** field, enter the full file name (including path) to be monitored.
 - b. In the **Log Prefix** field, enter a log prefix that needs to be added to the log.
 - c. Click **Save**.
6. Click **Save**.
7. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
8. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.

9. From the **Host** drop-down list, select the host(s).
10. At **Template**, attach the template to one or more server hosts by selecting its checkbox, then click **Save**.
11. Under **Host to Template Associations**, click **Apply**.
The logs will have a prefix set by **Log Prefix** that can be used to write a Parser for these files.
For details, see [Configuring Windows Agent](#).

For Linux Agent, take the following steps:

1. Login to FortiSIEM GUI.
2. Navigate to **Admin > Setup**, and click the **Linux Agent** tab.
3. Under **Linux Agent Monitor Templates**, click **New** to create a new template, or click an existing template and click **Edit**.
4. If creating a new template, on the **Generic** tab, in the **Name** field, enter a name for the template.
5. Click the **Log File** tab, and click **New**.
 - a. In the **Full File Name** field, enter the full file name (including path) to be monitored.
 - b. In the **Log Prefix** field, enter a log prefix that needs to be added to the log.
 - c. Click **Save**.
6. Click **Save**.
7. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
8. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
9. From the **Host** drop-down list, select the host(s).
10. At **Template**, attach the template to one or more server hosts by selecting its checkbox, then click **Save**.
11. Under **Host to Template Associations**, click **Apply**.
The logs will have a prefix set by **Log Prefix** that can be used to write a Parser for these files.
For details, see [Configuring Linux Agent](#).

Define the Apache Log Format

You must define the format of the logs that Apache will send to FortiSIEM.

1. Open the file `/etc/httpd/conf.d/ssl.conf` for editing.
2. Add the following line to the file.

```
CustomLog logs/ssl_request_log combined
```

3. Uncomment the following line in the file.

```
#CustomLog logs/access_log common
```

4. Add the following line to the file.

```
CustomLog logs/access_log combined
```

5. Reload Apache.

```
/etc/init.d/httpd reload
```

Apache Syslog Log Format

```
2024-10-28T22:55:22Z USER-WIN2016.gettest.com 192.0.20.0 AccelOps-WUA-UserFile-apach_log
[phCustId]="2000" [customer]="org1" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="4a2804f4-e1b6-4e01-ac76-de5aa103d253" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [fileName]="C:\\Apache24\\logs\\access.log" [msg]="::1 - -
[28/Oct/2024:15:55:16 -0700] \"GET / HTTP/1.1\" 304 -"
```

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Settings for Apache Web Server HTTPS Access Credentials](#)

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Settings for Apache Web Server HTTPS Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your Apache web server over https.

Setting	Value
Name	Apache-https
Device Type	generic
Access Protocol	HTTP or HTTPS
Port	80 (HTTP) or 443 (HTTPS)
URL	server-status?auto

Setting	Value
User Name	The admin account you created when configuring HTTPS
Password	The password associated with the admin account

Microsoft IIS for Windows 2000 and 2003

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level metrics: CPU utilization, memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O IIS metrics: Current Connections, Max Connections, Sent Files, Received Files, Sent Bytes, Received Bytes, ISAPI Requests, Not Found Errors	Performance Monitoring
Windows Agent	Application type	W3C access logs: attributes include IIS Service Instance, Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft iis" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [WMI](#)
- [FortiSIEM Windows Agent](#)

SNMP

See [SNMP Configurations](#) in the *Microsoft Windows Server Configuration* section.

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring IIS for FortiSIEM Windows Agent, see [Collecting Windows IIS Logs](#) from Microsoft Windows Server via Agents.

Settings for Access Credentials

See [Setting Access Credentials](#) in the *Microsoft Windows Server Configuration* section.

Microsoft IIS for Windows 2008

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Setting Access Credentials](#)
- [Sample IIS Syslog](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level metrics: CPU utilization, memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O IIS metrics: Current Connections, Max Connections, Sent Files, Received Files, Sent Bytes, Received Bytes, ISAPI Requests, Not Found Errors	Performance Monitoring
Windows Agent	Application type	W3C access logs: attributes include IIS Service Instance, Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft iis" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [WMI](#)
- [FortiSIEM Windows Agent](#)

SNMP

See [SNMP Configurations](#) in the *Microsoft Windows Server Configuration* section.

WMI

See [WMI Configurations](#) in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring IIS for FortiSIEM Windows Agent, see [Collecting Windows IIS Logs](#) from Microsoft Windows Server via Agents.

Setting Access Credentials

See [Setting Access Credentials](#) in the *Microsoft Windows Server Configuration* section.

Sample IIS Syslog

```
<13>Oct  9 12:19:05 ADS-Pri.ACME.net IISWebLog          0          2008-10-09 19:18:43
W3SVC1 ADS-PRI 192.168.0.10 GET /iisstart.htm - 80 - 192.168.20.80 HTTP/1.1 Mozilla/5.0+
(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.3)+Gecko/2008092417+Firefox/3.0.3 - - 192.168.0.10
200 0 0 2158 368 156
<46>Mar 29 12:21:03 192.168.0.40 FTPSvcLog          0          2010-03-29 19:20:32 127.0.0.1 - MSFTPSVC1 FILER
127.0.0.1 21 [1]PASS IEUser@ - 530 1326 0 0 0 FTP - - - -
```

NGINX Web Server

Support Added: FortiSIEM 4.7.2

Last Modification: FortiSIEM 6.4.0

Vendor Version Tested: Not Provided

Vendor: NGINX

Product: Web Server

Product Information: <https://www.nginx.com/products/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

The following protocols are used to discover and monitor various aspects of the NGINX webserver.

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level metrics: CPU utilization, Memory utilization	Performance Monitoring
Syslog		W3C access logs: attributes include Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "nginx" to see the event types associated with this device.

Configuration

- [Syslog via Rsyslog](#)
- [SNMP](#)
- [Syslog via NGINX Config File](#)
- [Sample Directives for Syslog Configuration](#)

- [Example NGINX Syslog](#)

Syslog via Rsyslog

To use rsyslog to collect and send NGINX logs via syslog, take the following steps:

Notes:

- Rsyslog Tag= is case sensitive, so ensure it is entered properly.
 - For steps 4 and 5, change the path as required to direct it to your *access.log* and *error.log* files.
 - For step 6, replace *<FortiSIEM collector IP or hostname>* with your actual FortiSIEM collector IP or hostname.
1. Locate the NGINX error and access log files. Here is a typical location:
`/var/log/nginx/access.log`
`/var/log/nginx/error.log`
 2. Locate `rsyslog.conf` file. Here is the typical location:
`/etc/rsyslog.conf`
 3. Add the `imfile` module to `rsyslog.conf` file.
Note: If `imfile` is already loaded, do not add it again.
`module(load="imfile" PollingInterval="10")`
 4. Add the following to your `rsyslog.conf` file for NGINX access log.
`input(type="imfile" File="/var/log/nginx/access.log"`
`Tag="nginx_AccessLog:"`
`Severity="info"`
`Facility="local6")`
 5. Add the following to your `rsyslog.conf` file for NGINX error log.
`input(type="imfile" File="/var/log/nginx/error.log"`
`Tag="nginx_ErrorLog:"`
`Severity="error"`
`Facility="local6")`
 6. Send local6 to SIEM by adding the following to your `rsyslog.conf` file.
`local6.* @<FortiSIEM collector IP or hostname>`
 7. Restart rsyslog by running the following command.
`systemctl restart rsyslog`
 8. Confirm that logs are arriving. Ensure your firewall(s) allows UDP 514 inbound to target IP.

NGINX Sample Log

```
<179>Mar 22 00:41:50 lab1.example.com Apache_AccessLog: 192.0.20.0 - - [22/Mar/2022:00:41:48
+0000] "POST
/phoenix/rest/h5/rt/start2?t=t1647909924028&s=333078424F54496950533135435470487275415A597470545138
7635564B39496D4949717865776A HTTP/1.1" 200 36
```

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting](#)

[Credentials](#)" in the [User Guide](#).

Syslog via NGINX Config File

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Reference the NGINX guide here: <http://nginx.org/en/docs/syslog.html>

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Sample Directives for Syslog Configuration

```
error_log syslog:server=192.0.2.0:514 debug;
access_log syslog:server=192.0.2.0:514,facility=local6,tag=nginx,severity=info combined;
```

Example NGINX Syslog

```
<29>Jun 15 07:59:03 ny-n1-p2 nginx: "192.0.2.0","-","Mozilla/5.0 (Windows NT 5.1 WOW64; rv:9.0.1)
Gecko/20100178 Firefox/9.0.1","/images/design/header-2-
logo.jpg","GET","http://example.com/images/design/header-2-logo.jpg","200","0","/ypf-cookie_
auth/index.html","0.000","877","-","198.51.100.0","80","example.com","no-cache, no-store, must-
revalidate","-","1.64","_","-","-"
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Blade Servers

FortiSIEM supports these blade servers for discovery and monitoring.

- [Cisco UCS Server](#)
- [HP BladeSystem](#)

Cisco UCS Server

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Cisco UCS Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Cisco UCS API	Host name, Access IP, Hardware components - processors, chassis, blades, board, cpu, memory, storage, power supply unit, fan unit	Chassis status: Input Power, Input Avg Power, Input Max Power, Input Min Power, Output Power, Output Avg Power, Output Max Power, Output Min Power Memory status: Temp (C), Avg Temp (C), Max Temp (C), Min Temp (C) Processor status: Input Current, Input Avg Current, Input Max Current, Input Min Current, Temp (C), Avg Temp (C), Max Temp (C), Min Temp (C) Power supply status: Temp (C), Max Temp (C), Avg Temp (C), Min Temp (C), Input 210Volt, Avg Input 210Volt, Max Input 210Volt, Min Input 210Volt, Output 12Volt, Avg Output 12Volt, Max Output 12Volt, Min Output 12Volt, Output 3V3Volt, Avg Output 3V3Volt, Max Output 3V3Volt, Min Output 3V3Volt, Output Current, Avg Output Current, Max Output Current, Min Output Current, Output Power, Avg Output Power, Max Output Power, Min Output Power Fan status: Fan Speed, Average Fan Speed, Max Fan Speed, Min Fan Speed	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco ucs" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "cisco ucs" to see the reports associated with this application or device.

Configuration

UCS XML API

FortiSIEM uses Cisco the Cisco UCS XML API to discover Cisco UCS and to collect hardware statistics. See the Cisco UCS documentation for information on how to configure your device to connect to FortiSIEM over the API.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	ucs
Device Type	Cisco UCS
Access Protocol	UCS API
Pull Interval (minutes)	5
Port	5988
User Name	The user name you set up in your UCS server to communicate with FortiSIEM
Password	The password associated with user name

Sample Cisco UCS Events

- [Power Supply Status Event](#)
- [Processor Status Event](#)
- [Chassis Status Event](#)
- [Memory Status Event](#)
- [Fan Status Event](#)

Power Supply Status Event

```
[PH_DEV_MON_UCS_HW_PSU_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,[hostIpAddr]=192.0.2.36,  
[hwComponentName]=sys/chassis-1/psu-2,  
[envTempdDegC]=47.764706,[envTempAvgDegC]=36.176472,[envTempMaxDegC]=47.764706,  
[envTempMinDegC]=25.529411,[input210Volt]=214.294113,  
[input210AvgVolt]=210.784317,[input210MaxVolt]=214.294113,[input210MinVolt]=207.823532,
```

```
[output12Volt]=12.188235,[output12AvgVolt]=12.109803,
[output12MaxVolt]=12.376471,[output12MinVolt]=11.905882,[output3V3Volt]=3.141176,
[output3V3AvgVolt]=3.374510,[output3V3MaxVolt]=3.458823,
[output3V3MinVolt]=3.141176,[outputCurrentAmp]=15.686275,[outputCurrentAvgAmp]=20.261436,
[outputCurrentMaxAmp]=24.509804,
[outputCurrentMinAmp]=15.686275,[outputPowerWatt]=191.188004,[outputPowerAvgWatt]=245.736252,
[outputPowerMaxWatt]=303.344879,
[outputPowerMinWatt]=191.188004
```

Processor Status Event

```
[PH_DEV_MON_UCS_HW_PROCESSOR_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,
[hostIpAddr]=192.0.2.36,
[hwComponentName]=sys/chassis-1/blade-3/board/cpu-2,
[inputCurrentAmp]=101.101959,[inputCurrentAvgAmp]=63.420914,[inputCurrentMaxAmp]=101.101959,
[inputCurrentMinAmp]=44.580391,
[envTempdDegC]=5.788235,[envTempAvgDegC]=6.216993,[envTempMaxDegC]=6.431373,
[envTempMinDegC]=5.788235,
```

Chassis Status Event

```
[PH_DEV_MON_UCS_HW_CHASSIS_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,
[hostIpAddr]=192.0.2.36,[hwComponentName]=sys/chassis-1,
[inputPowerWatt]=7.843137,[inputPowerAvgWatt]=7.843137,[inputPowerMaxWatt]=7.843137,
[inputPowerMinWatt]=7.843137,
[outputPowerWatt]=0.000000,[outputPowerAvgWatt]=0.000000,[outputPowerMaxWatt]=0.000000,
[outputPowerMinWatt]=0.000000
```

Memory Status Event

```
[PH_DEV_MON_UCS_HW_MEMORY_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,
[hostIpAddr]=192.0.2.36,
[hwComponentName]=sys/chassis-1/blade-1/board/memarray-1/mem-9,[envTempdDegC]=51.000000,
[envTempAvgDegC]=50.128208,
[envTempMaxDegC]=51.000000,[envTempMinDegC]=48.000000
```

Fan Status Event

```
[PH_DEV_MON_UCS_HW_FAN_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,[hostIpAddr]=192.0.2.36,
[hwComponentName]=sys/chassis-1/fan-module-1-5/fan-2,[fanSpeed]=7800.000000,
[fanSpeedAvg]=7049.000000,
[fanSpeedMax]=8550.000000,[fanSpeedMin]=2550.000000
```

HP BladeSystem

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Access IP, Hardware components - processors, chassis, blades, board, cpu, memory, storage, power supply unit, fan unit	Hardware status: Fan status, Power supply status, power enclosure status, Overall status	Availability and Performance Monitoring

Configuration

SNMP

FortiSIEM uses SNMP to discover the HP BladeSystem and collect hardware statistics. See the instructions on configuring SNMP in your Bladesystem documentation to enable communications with FortiSIEM.

After you have configured SNMP on your BladeSystem blade server, you can configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials in FortiSIEM

See [Access Credentials](#) to set access and protocol for SSH, and Telnet.

Cloud Access Security Broker

FortiSIEM supports the following cloud access security broker (CASB).

- [FortiCASB](#)
- [Oracle CASB](#)

Fortinet FortiCASB

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
API				Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, and search for "FortiCASB" to see the event types associated with this device.

Rules

No specific rules are written for FortiCASB but generic end point rules apply.

Reports

No specific reports are written for FortiCASB but generic end point rules apply.

Configuration

Configure FortiCASB to send logs to FortiSIEM in the supported format (see Sample event below)

Setup in FortiCASB

Take the following steps in FortiCASB.

1. Login to FortiCASB with your account.
2. At the top right corner, click on the Switch Company icon.
3. Click **Manage Company** to access the company setting.
4. Select the **API Setting** tab.
5. Click **Generate New** to generate a new API credential.
6. In the Credential field, enter a credential name and click **Generate Credential**.
7. Copy the credential information to be used later to call the FortiCASB API.
Note: The credential will only be shown once, so keep it in a private and secured place.
The generated credential can be used repeatedly as long as it is not revoked on FortiCASB.

Setup in FortiSIEM

FortiSIEM processes events from this via the Fortinet FortiCASB API. Make sure to complete [Setup in FortiCASB](#) before proceeding here.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Fortinet FortiCASB
Access Protocol	FortiCASB_API
Pull Interval	5 minutes
Token	Provide the authorization token from your account.
Confirm Token	Provide the authorization token from your account to confirm.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Select the name of your credential from the **Credentials** drop-down list. The **IP/Host Name** field will auto populate with "www.forticasb.com".
 - b. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiCASB.
5. To see the jobs associated with FortiCASB, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "FortiCASB" in the search box.

Sample Events

```
[FortiCASB-EVENT] = {
  "alertType": "Data Analysis",

  "applicationId": "Y2lzY29zcGFyazovL3VzL09SR0F0SVpBVElPTi84NGI0NDZlMi0xYTU5LTQyZjQtOGVhMy05YmY4MjdiN2ZlMjg",
  "buId": 84,
  "companyId": "62598",
  "contextName": "DLP Birthdate Policy",
  "createTime": 162125006181,
  "defineType": "Predefined",
  "displayOperation": "Upload File",
  "eventId": "62598-Webex-58cb1d3b6f30326cfca5e64d2f96fa5d",
  "eventIdList": [
    "62598-Webex-58cb1d3b6f30326cfca5e64d2f96fa5d"
  ],

  "fileId": "Y2lzY29zcGFyazovL3VybjpURUFN0nVzLXd1c3QtMl9yL0NPTlRFTlQvOWI2YjUzNzAtYjZmZi0xMWViLWE0NjAtMDE0ZTAzYTk3NmI3LzA",
  "id": "d6e52513ee1069437704271f1144d981",
  "matches": 1,
  "object": "01-ssn-usercollaborator.doc",

  "objectId": "Y2lzY29zcGFyazovL3VybjpURUFN0nVzLXd1c3QtMl9yL0NPTlRFTlQvOWI2YjUzNzAtYjZmZi0xMWViLWE0NjAtMDE0ZTAzYTk3NmI3LzA",
  "objectType": "DOCUMENT",
  "phCustId": 1,
  "policyCode": "FC-ACT-018",
  "policyId": "13285945",
  "policyName": "DLP Birthdate Policy",
  "resultDesc": "File \" 01-ssn-usercollaborator.doc \"Matches the DLP Birthdate 1 time(s), the matched content are: \\n(1) *****1972 \\n\\n\\n null\\n \",
  "serverHostName": "www.forticasb.com",
  "serverIp": "34.212.75.194",
  "service": "Webex",
  "severity": "Alert",
  "timestampUUID": "d6e52513ee1069437704271f1144d981",
  "updateTime": 162125006000,
  "user": "testadmin1@forticasb.com",
  "userId": "Y2lzY29zcGFyazovL3VzL1BFT1BMRS8zZGVmNDBhNC1kYTI1LTQ0ODctODFlOS0zNWJjYzZk5MTA2YTA",
  "userName": "Test admin",
  "violationActivity": "WEBEX_CREATED_MESSAGES"
}
```

Oracle Cloud Access Security Broker (CASB)

- [What is Discovered and Monitored](#)
- [Event Types](#)

- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Log](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
API		Risk Events, Risk Alerts and Policy Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Oracle-CASB-" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 3 event types defined.

Rules

There are no specific rules available for Oracle CASB.

Reports

There are no specific reports available for Oracle CASB. You can view all Oracle events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Oracle-CASB-".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Setup in FortiSIEM

FortiSIEM processes events from this via the Oracle CASB API. Configure and obtain from the Oracle CASB Portal, the access key and secret from the API before proceeding.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Oracle CASB
Access Protocol	Oracle CASB API
Pull Interval	5 minutes
Access Key	The access key for your Oracle CASB instance.
Secret Key	The secret key for Oracle CASB instance.
Confirm Secret Key	Input the same secret key as above for verification.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Oracle CASB.
5. To see the jobs associated with Oracle CASB, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "CASB" in the search box.

Sample Log

```
<![CDATA[[FSM-OracleCASB-riskevent] [1] {"id":"aa1nhj35-6d84-3f5a-a9b5-3e1509bad324","uri":"/v1/events/riskevent?eventId=aa1eab35-6d84-3f5a-a9b5-3e1509bad324&applicationInstanceId=5786ed4c-3527-413d-8j19-da93d0f065c8","appname":"AWS","appinstance":"awse2e_01","appinstanceid":"64909d3d-3855-5de1-49ed-6452ae9f6365","snapdate":"2017-10-25","title":"DeleteSecurityGroup action in EC2 SecurityGroup \SecurityGroup\","additionalDetails":[{"Details":[{"name":"Actor","value":"funct_test_nonservice"}, {"name":"Resource type","value":"EC2 SecurityGroup"}, {"name":"Group","value":"SecurityGroup"}, {"name":"Resource name","value":"JKSecurityGroup"}], {"name":"Action","value":"DeleteSecurityGroup"}, {"name":"Policy alert name","value":"EC2 - Instances Network Routes Network ACL VPN and Security Group changes"}, {"name":"Occurred","value":"2017-10-25T17:17:29Z"}, {"name":"recommendationkey","value":"AWS~PolicyAlert~ec2deletesecuritygroup"}], "Logdata":{"requestParameters":{"groupname":"SecurityGroup"},"responseElements":{"_return":true},"eventVersion":"1.05","eventTime":"2017-10-25T17:17:29Z","eventSource":"ec2.amazonaws.com","eventName":"DeleteSecurityGroup","awsRegion":"us-east-1","sourceIPAddress":"54.191.225.186","userAgent":"aws-sdk-java/1.10.54 Linux/3.13.0-35-
```

```
generic Java_HotSpot(TM)_64-Bit_Server_VM/25.60-b23/1.8.0_60\", \"userIdentity\" : { \"type\" : \"IAMUser\", \"principalId\" : \"BGHAJVECQI6K0IYZMM42A\", \"arn\" : \"arn:aws:iam::141111463221:user/func_test_nonservice\", \"accountId\" : \"141111462111\", \"accessKeyId\" : \"BJKFJ4J60YTZDBHN3KA\", \"userName\" : \"func_test_nonservice\" }, \"requestID\" : \"bc44cd99-fac7-4e6c-8868-382c26fc95ee\", \"eventID\" : \"664d6fa8-8bdf-4bda-af5c-55d447620a78\" } } ], \"category\": \"Policy alert\", \"priority\": \"High\", \"status\": \"Open\", \"createdon\": \"2017-10-25T17:33:55.000Z\", \"realeventtime\": \"2017-10-25T17:17:29.000Z\" } ] ] >
```

Cloud Applications

FortiSIEM supports these cloud applications for monitoring.

- [Akamai Connected Cloud](#)
- [Alcide.io KAudit](#)
- [Atlassian Beacon](#)
- [AWS Access Key IAM Permissions and IAM Policies](#)
- [AWS CloudTrail API](#)
- [AWS EC2](#)
- [AWS EC2 CloudWatch API](#)
- [AWS ELB](#)
- [AWS Kinesis](#)
- [AWS RDS](#)
- [AWS Security Hub](#)
- [AWS Simple Queue Service \(SQS\)](#)
- [AWS Simple Storage Service](#)
- [Box.com](#)
- [Cisco Umbrella](#)
- [G42 Cloud](#)
- [Google Cloud Platform - Pub/Sub Integration](#)
- [Google Workspace \(Formerly G Suite and Google Apps\)](#)
- [Microsoft Azure Audit](#)
- [Microsoft Azure Compute](#)
- [Microsoft Azure Event Hub](#)
- [Microsoft Cloud App Security](#)
- [Microsoft Defender for Identity/Microsoft Azure ATP](#)
- [Microsoft Entra Identity Protection](#)
- [Microsoft Office365 Audit](#)
- [Okta](#)
- [Oracle Cloud Infrastructure](#)
- [Salesforce CRM Audit](#)

Akamai Connected Cloud

Akamai Connected Cloud provides a massively distributed edge and cloud platform where developers can build, run, and secure applications across a continuum of computing power.

Support Added: FortiSIEM 7.2.0

Vendor Version Tested: Not Provided

Vendor: Akamai

Product: Akamai Connected Cloud

Product Information: <https://www.akamai.com/>

[Configuration](#)

[Sample Event](#)

Configuration

Akamai documentation can be found here: <https://techdocs.akamai.com/siem-integration/docs/welcome-siem-integration>

Take the following steps from the FortiSIEM GUI.

1. Navigate to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Akamai Connected Cloud
Access Protocol	Akamai SIEM API
Client ID	Enter the Client ID associated with Akamai Connected Cloud account.
Client Secret/Confirm Client Secret	Enter/paste the client secret into the Client Secret field and Confirm Client Secret field. More information can be found here .
Access Token	Enter/paste the access token associated with the Client ID.
Configuration ID	Enter/paste your configuration ID. More information can be found here .
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your Akamai Connected Cloud credential from the **Credentials** drop-down list if it is not already selected.
 - c. Click **Save**.

4. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection to the server.
5. Navigate to **ADMIN > Setup > Pull Events** to see the new job.

Events can be queried from the **ANALYTICS** page.

Sample Event

```
[Akamai] = {"attackData":{"clientIP":"192.0.20.0","configId":"14227","policyId":"qik1_26545","ruleActions":"alert;alert;deny","ruleData":"telnet.exe;telnet.exe;Vector Score: 10, DENY threshold: 9, Alert Rules: 950002:950006, Deny Rule: , Last Matched Message: System Command Injection","ruleMessages":"System Command Access;System Command Injection;Anomaly Score Exceeded for Command Injection","ruleSelectors":"ARGS:option;ARGS:option","ruleTags":"OWASP_CRS/WEB_ATTACK/FILE_INJECTION;OWASP_CRS/WEB_ATTACK/CMD_INJECTION;AKAMAI/POLICY/CMD_INJECTION_ANOMALY","ruleVersions":"4;4;1","rules":"950002;950006;CMD-INJECTION-ANOMALY"},"botData":{"botScore":"100","responseSegment":"3"},"clientData":{"appBundleId":"com.mydomain.myapp","appVersion":"1.23","sdkVersion":"4.7.1","telemetryType":"2"},"format":"json","geo":{"asn":"14618","city":"ASHBURN","continent":"288","country":"US","regionCode":"VA"},"httpMessage":{"bytes":"266","host":"www.hmapi.com","method":"GET","path":"/","port":"80","protocol":"HTTP/1.1","query":"option=com_jce%20telnet.exe","requestHeaders":"User-Agent%3a%20BOT%2f0.1%20(BOT%20for%20JCE)%0d%0aAccept%3a%20text%2fhtml,application%2fxhtml+xml,application%2fxml%3bq%3d0.9,*%2f*%3bq%3d0.8%0d%0auniqueID%3a%20CR_H8%0d%0aAccept-Language%3a%20en-US,en%3bq%3d0.5%0d%0aAccept-Encoding%3a%20gzip,%20deflate%0d%0aConnection%3a%20keep-alive%0d%0aHost%3a%20www.hmapi.com%0d%0aContent-Length%3a%200%0d%0a","requestId":"1158db1758e37bfe67b7c09","responseHeaders":"Server%3a%20AkamaiGHost%0d%0aMime-Version%3a%201.0%0d%0aContent-Type%3a%20text%2fhtml%0d%0aContent-Length%3a%20266%0d%0aExpires%3a%20Tue,%2004%20Apr%202017%2010%3a57%3a02%20GMT%0d%0aDate%3a%20Tue,%2004%20Apr%202017%2010%3a57%3a02%20GMT%0d%0aConnection%3a%20close%0d%0aSet-Cookie%3a%20ak_bmsc%3dAFE4B6D8CEEDBD286FB10F37AC7B256617DB580D417F0000FE7BE3580429E23D%7epLuPrgNmaBdJqQLZFwxqQLSkGGMy4zGMNXrpRIc1Md4qtsDfgjLCojg1hs2HC8JqaaB97QwQRR3YS1ulk+6e9Dbto0YASJAM909Ujbo6Qfyh1XpG0MniBzVbPMUV8oKhBLLPVSNCP0xXMnH8iXGZUHLUsHqWONT3+EGSbWUU320h4GKiGCJkig5r+hc6V1pi3tt7u3LglG3DloEilchdo8D7iu4lrvvAEzyYQI8Hao8M0%3d%3b%20expires%3dTue,%2004%20Apr%202017%2012%3a57%3a02%20GMT%3b%20max-age%3d7200%3b%20path%3d%2f%3b%20domain%3d.hmapi.com%3b%20HttpOnly%0d%0a","start":"1491303422","status":"200"},"type":"akamai_siem","userRiskData":{"allow":"0","general":"duc_1h:10|duc_1d:30","originUserId":"jsmith007","risk":"udfp:1325gdg4g4343g/M|unp:74256/H","score":"75","status":"0","trust":"ugp:US","username":"jsmith@example.com","uuid":"964d54b7-0821-413a-a4d6-8131770ec8d5"},"version":"1.0"}
```

Alcide.io KAudit

- [Integration Points](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Log](#)

Integration Points

Protocol	Information Collected	Used For
Syslog	Audit logs	Security and Compliance Monitoring

Event Types

Go to **RESOURCES > Event Types** and search "AlcideKAudit" in the main content panel **Search...** field.

Configuration

- [Configuring Alcide.io to Send Logs](#)
- [Configuring FortiSIEM to Receive Logs](#)

Configuring Alcide.io to Send Logs

Follow the steps listed [here](#) to send syslog to FortiSIEM.

1. In the **target** section of the ConfigMap, set the following:
 - a. Target-type = **syslog**
 - b. Syslog host = **<fortisiem.host.com>**
 - c. Syslog port = **514**
 - d. Syslog-tcp = **false**

Configuring FortiSIEM to Receive Logs

No configuration is needed. FortiSIEM can automatically detect and parse Alcide.io logs based on the built in parser.

Sample Log

```
<109>Feb 28 07:09:18 AlcideKAudit:
{"category":"anomaly","cluster":"devel","etype":"cluster","reasons":[{"values":{"high":
```

```
[1]], "doc": "change in count of unique unusual URIs in read access attempts", "period": 180000, "direction": "read"}], "time": 1582873380000, "short-doc": "change in targets of access attempts", "project": "alcide-rnd", "context": {"unusual-uri": ["LHUt"]}, "period": 180000, "eid": "cluster", "confidence": "high", "doc": "unusual change in count of unique unusual URIs in access attempts", "direction": "read"}
```

Atlassian Beacon

Support Added: FortiSIEM 7.2.0

Vendor: Atlassian

Vendor Version Tested: Not Provided

Product Information: <https://www.atlassian.com/software/beacon>

Intelligent threat detection, built for Atlassian cloud products.

- [Configuration](#)
- [Checking for Events](#)
- [Event Type](#)

Configuration

- [Prerequisite](#)
- [FortiSIEM Setup](#)
- [Atlassian Beacon Setup](#)

Prerequisite

Most applications using webhook push notifications do server TLS certificate validation, which means the target collector must be configured with a public CA signed TLS certificate.

See [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#) for configuration information.

FortiSIEM Setup

To configure webhook integration, you will need to take the following general steps.

- [Create Credential](#)

Create Credential

Take the following steps to configure a credential for FortiSIEM.

1. Login to FortiSIEM as an administrator.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.

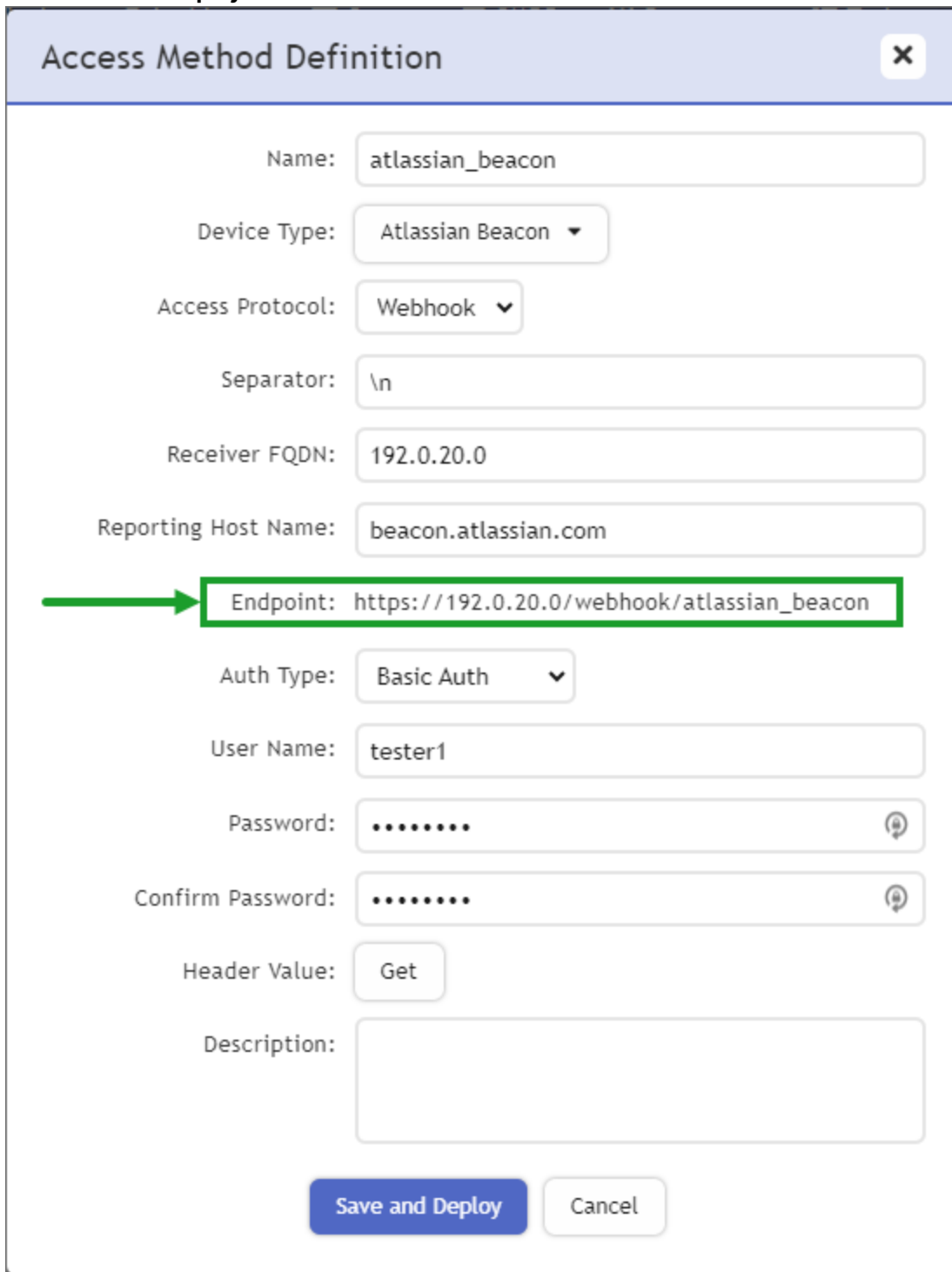
4. In the **Access Method Definition** window, input the following:
- a. In the **Name** field, enter the name of the credential. This serves as the basis of the target endpoint created.
 - b. From the **Device Type** drop-down list, select **Atlassian Beacon**.
 - c. In the **Separator** field, leave the default as "\n" to separate the payload. The "\n" is the newline linefeed and means that each line in the response is treated as a new log.
 - d. In the **Receiver FQDN** field, enter the FQDN of the FortiSIEM node. This field expects the FQDN or IP address of the FortiSIEM collector that will be receiving the webhook traffic. This is used to help dynamically generate an endpoint configuration for you. This should ideally be the FQDN of the collector from the sending application's perspective.
 - e. In the **Reporting Host Name** field, enter "beacon.atlassian.com". This field expects the source hostname of the sending application. It is used to uniquely identify the logs as it will be in the header of every log.
 - f. **Endpoint** is the dynamically generated webhook endpoint based on the receiver FQDN. This makes it easier to paste this URL as the target of your webhooks in the client application.
 - g. From the **Auth Type** drop-down list, select **Basic Auth**. Basic authorization compares the base64 (name:password) with the value of the authorization header (authorization: basic xxxx) in an HTTP request.

There is an optional helpful UI feature if you'd like to get the exact string the client application should send in the authorization header (if for some reason they don't compute the basic auth themselves). You can get the expected Authorization header value by clicking **Get** from **Header Value** after you have entered the User Name, and associated password in the **User Name** field and **Password/Confirm Password** fields respectively. This should rarely be needed, as most client applications sending webhooks with basic auth will only require the same username/password and compute this for you.
 - h. In the **User Name** field, enter the username.
 - i. In the **Password** and **Confirm Password** fields, enter the password associated with the username.
 - j. (Optional) You can get the expected Authorization header value by clicking **Get Header Value**. You will need to enter the username, and associated password in the **User Name** field and **Password/Confirm Password** fields respectively first.

Note: This is only useful if you need to see the preformatted header value (in this case 'Bearer base64 (username:password)'). In most cases this is not even needed, and purely a convenience function for testing.

The client application sending the webhooks using Basic authentication, in this case Atlassian, will generally take the username/password, and generate the Authorization header for you using the base64 value.

k. Click **Save and Deploy**.



The image shows a dialog box titled "Access Method Definition" with a close button (X) in the top right corner. The dialog contains several input fields and buttons. A green arrow points to the "Endpoint" field, which is highlighted with a green border. The fields are as follows:

- Name: atlassian_beacon
- Device Type: Atlassian Beacon (dropdown)
- Access Protocol: Webhook (dropdown)
- Separator: \n
- Receiver FQDN: 192.0.20.0
- Reporting Host Name: beacon.atlassian.com
- Endpoint: https://192.0.20.0/webhook/atlassian_beacon (highlighted with a green arrow and border)
- Auth Type: Basic Auth (dropdown)
- User Name: tester1
- Password: (with an eye icon for toggling visibility)
- Confirm Password: (with an eye icon for toggling visibility)
- Header Value: Get
- Description: (empty text area)

At the bottom of the dialog are two buttons: "Save and Deploy" (in blue) and "Cancel" (in white).

Atlassian Beacon Setup

Reference Documentation: https://intercom.help/atlassian-beacon/en/articles/6558090-send-alerts-to-a-siem-slack-teams-splunk-or-other-tools#h_198d466bb5.

Ensure the [Prerequisite](#) is completed before proceeding.

Set up webhook to get events from Atlassian Beacon through SSL verification by updating the httpd server configuration.

1. In Beacon, navigate to **Integrations > SIEM forwarding**.
2. Click **Add webhook**.
3. In the **Webhook URL** field, enter the Webhook URL. The structure should be:
`https://<FortiSIEM_Node_IP>/webhook/<FortiSIEM_Credential_NAME>`
 You can get the **Webhook URL** by accessing a completed FortiSIEM Create Credential configuration from the FortiSIEM GUI and copying the information in [Endpoint](#).
4. Click **Save**.
5. Click **Authorization**. Input the Authentication Header. The format is "Basic <string of base64 username:password>". To get this content, from a completed FortiSIEM **Create Credential** configuration, click **Get** in **Header Value**, and click the copy icon, then paste the information here.

The screenshot displays two overlapping windows from the FortiSIEM configuration interface. The primary window, titled 'Access Method Definition', contains the following fields: Name (atlassian_beacon), Device Type (Atlassian Beacon), Access Protocol (Webhook), Separator (\n), Receiver FQDN (192.0.20.0), Reporting Host Name (beacon.atlassian.com), Endpoint (https://192.0.20.0/webhook/atlassian_beacon), Auth Type (Basic Auth), User Name (tester1), Password (masked), Confirm Password (masked), Header Value (Get), and Description. A green box highlights the 'Get' button in the Header Value field. A secondary window, titled 'Authentication Header', is open to the right, showing the generated header value 'Basic dGVzdGVyMTQKioKioKg==' and a 'Click to copy' button, which is also highlighted with a green box. A green arrow points from the 'Get' button in the first window to the header value in the second window.

Example: For User Name: tester1, Password: tester:Tester123!, the Authentication Header would be Basic dGVzdGVyMTQKioKioKg==

6. Click **Test**.

Checking for Events

Events can be queried from the **Analytics** page, using atlassian-beacon as part of a Raw Event Log search. Make sure [Atlassian Beacon Setup](#) is completed before proceeding with your check for events.

From the FortiSIEM GUI, take the following steps.

1. Navigate to **Analytics > Search**.
2. Click **Edit Filters and Time Range.....**
3. In **Filter By**, select the **Event Attribute** tab.
4. Enter/select the following:
Attribute = Raw Event Log, Operator = CONTAIN, Value = atlassian-beacon
5. Click **Apply & Run**.

Event Type

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=Atlassian,[reptModel]=Beacon,[reptDevName]=test.com,
[reptDevIpAddr]=11.11.11.11,[json]={
  "alertDetailURL":"https://beacon.atlassian.com/w/11111111-1111-1111-1111-111111111111/alerts/c111e111a11bfd11d1111c1d?atlOrigin=eyJpIjoiODUwMmU1NmFkMTMzNDYxZGJjODk1NmY1MGVmNDkzN1IiLCJwIjoiYmVhY11uIn1",
  "alertId":"c111e111a11bfd11d1111c1d",
  "alertTitle":"Sensitive data detected: Atlassian API token",
  "detectionTime":1711493273898,
  "activity":{
    "action":"READ",
    "subject":{"ari":"ari:cloud:confluence::site/a1111a1d-11f1-1c11-a111-11111c111111",
      "containerAri":"ari:cloud:platform::org/j1111j1b-11d1-1a11-j111-11111a111111",
      "ati":"ati:cloud:confluence:space"},
    "time":{"start":"2023-11-11T11:11:11.111Z",
      "end":"2023-11-11T11:11:11.111Z"}},
    "actor":{"accountId":"111111:db1a1a1e-1c11-111a-11dd-1e1c11111111",
      "name":"Mei Liu",
      "sessions":[{
        "ipAddress":"11.11.11.11",
        "userAgent":"Mozilla/1.1 (Macintosh; Intel Mac OS X 11_11_1) AppleWebKit/111.1.11 (KHTML, like Gecko) Version/11.1.1 Safari/111.1.11",
        "loginTime":"2023-11-11T11:11:11.111Z",
        "lastActiveTime":"2023-11-11T11:11:11.111Z"}]},
    "url":"https://beacon.atlassian.com/w/11111111-1111-1111-1111-111111111111/users/111111:db1a1a1e-1c11-111a-11dd-1e1c11111111?atlOrigin=eyJpIjoiODUwMmU1NmFkMTMzNDYxZGJjODk1NmY1MGVmNDkzN1IiLCJwIjoiYmVhY11uIn1"},
    "alert":{"created":"2023-11-11T11:11:11.111Z",
      "id":"c111e111a11bfd11d1111c1d",
      "product":"CONFLUENCE",
      "site":"https://fortisiem.atlassian.net?atlOrigin=eyJpIjoiODUwMmU1NmFkMTMzNDYxZGJjODk1NmY1MGVmNDkzN1IiLCJwIjoiYmVhY11uIn1",
      "title":"Sensitive data detected: Atlassian API token",
      "url":"https://beacon.atlassian.com/w/11111111-1111-1111-1111-111111111111/alerts/c111e111a11bfd11d1111c1d?atlOrigin=eyJpIjoiODUwMmU1NmFkMTMzNDYxZGJjODk1NmY1MGVmNDkzN1IiLCJwIjoiYmVhY11uIn1"},
      "id":"c111e111a11bfd11d1111c1d",
      "timestamp":1711493273898,
      "type":"beacon:create:test",
      "workspace":{"cloudId":"a1111a1d-11f1-1c11-a111-11111c111111",
        "id":"11111111-1111-1111-1111-111111111111",
        "orgId":"j1111j1b-11d1-1a11-j111-11111a111111"}}}
```

AWS Access Key IAM Permissions and IAM Policies

To monitor AWS resources in FortiSIEM, an access key and a corresponding secret access key is needed. Prior to the availability of AWS IAM users, the recommendation was to create an access key at the level of root AWS account. This practice has been deprecated since the availability of AWS IAM users as you can read from the [AWS Security Credentials best practice guide](#). If you were monitoring AWS using such access keys, the first step is to delete such keys and create keys based on a standalone IAM user dedicated for monitoring purposes in FortiSIEM. This document explains how to create such a user, and what permissions and policies to add to allow FortiSIEM to monitor your AWS environment.

- [Create IAM User for FortiSIEM Monitoring](#)
- [Change Permissions for IAM User](#)
- [S3 Bucket Read-only Policy](#)

Create IAM User for FortiSIEM Monitoring

1. Login to the [IAM Console - Users Tab](#).
2. Click **Create Users**.
3. Type in a username, e.g. aomonitoring under **Enter User Names**.
4. Leave the checkbox **Generate an access key for each user** selected or select it if it is not selected.
5. Click **Download Credentials** and click on **Close** button.
6. The downloaded CSV file contains the Access Key ID and Secret Access Key that you can use in FortiSIEM to monitor various AWS services. You must add permissions before you can actually add them in FortiSIEM.

Change Permissions for IAM User

1. Select the user you are monitoring.
2. Switch to tab **Permissions**.
3. Click **Attach Policy**.
4. Select *AmazonEC2ReadOnlyAccess*, *AWSCloudTrailReadOnlyAccess*, *AmazonRDSReadOnlyAccess*, *CloudWatchReadOnlyAccess*, *AmazonSQSFullAccess* and click **Attach Policy**. You can choose to skip attaching some policies if you do not use that service or plan on monitoring that service. For instance, if you do not use RDS, then you do not need to attach *AmazonRDSReadOnlyAccess*.
5. You can choose to provide blanket read-only access to all S3 buckets by attaching the policy *AmazonS3ReadOnlyAccess*. Alternatively, you can specify a more restricted policy as described in the next step.
6. Identify the set of S3 bucket(s) that you have configured to store Cloudtrail logs for each region. You can create an **inline policy**, choose **custom policy**, then paste the sample policy below. Make sure you replace the actual S3 bucket names below *aocloudtrail1*, *aocloudtrail2* with the ones you have configured.

S3 Bucket Read-only Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": [
        "arn:aws:s3:::aocloudtrail1",
        "arn:aws:s3:::aocloudtrail2"
      ]
    }
  ]
}
```

AWS CloudTrail

Understanding AWS CloudTrail Configuration

While there are essentially two ways to forward CloudTrail logs to FortiSIEM, the FortiSIEM CloudTrail integration is designed for only one method.

Event Path

CloudTrail Generates Events -> Publish to SNS Topic -> SQS Queue is Subscribed to Topic -> FortiSIEM polls message queue (Follow this guide in its entirety, see [Configuration](#).)

When FortiSIEM gets a message from the queue, it will be in this format (if sent direct from CloudTrail service).

```
{
  "Type" : "Notification",
  "MessageId" : "658da72b-684e-5965-bc3a-f123456005a",
  "TopicArn" : "arn:aws:sns:us-east-1:111111:testCloudTrail",
  "Message" : "{\"s3Bucket\":\"testS3Bucket\", \"s3ObjectKey\":[\"AWSLogs/111111/CloudTrail/us-west-2/2022/05/27/111111_CloudTrail_us-west-2_20220527T1540Z_ILkwe2zAtDS.json.gz\"]}",
  "Timestamp" : "2022-05-27T16:35:35.746Z",
  "SignatureVersion" : "1",
  "Signature" :
    "hS79T2w30bfMRBIUt3qJ8D0v4fAq912345I7IHZTulkme+iEjg+mWgiQV3cikFXSAwzfYVUMGwpXx+Qr7m16uW5SRikMRb05L/5ioNrhM+DcRwjSmAEUm3ZzIFrFMaFeSy0hGD/vJEcPmVcs3ExVbz1NL1ZQcBU3LHMkrnwKKi6xFubkJWAj8nPZPUPFio7iqEHWUGHdvjqDVPkX+M7Kpwshze5q2cF6W7oPeXsUjTaV+iqFxlxi7P7TZRXsRw502wVSUYl8uVSsMKB3JdEkAJaEm3Ro/wcwxl8gbuWGwrFYwrXQoipJqv4xtrAp1ebIk/wcfMJur3mfJQ8A==",
  "SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-7ff5318522adbaddaa2a969abfda.pem",
  "UnsubscribeURL" : "https://sns.us-east-1.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:111111:dwfewefa12323:testCloudTrail:2947799d-3c02-4863-8cd6-36123523fd1"
}
```

FortiSIEM parses the s3ObjectKey and retrieves the given file from the configured S3 bucket, and processes the log message.

Unsupported Message Event Path for Cloud Trail Integration

There is another way to get a notification when a log object is written to an S3 bucket, using "S3 Bucket Event Notification". This flow involves configuring an S3 bucket to publish a message event to an SNS topic when a file is placed in the bucket (or some other operation). This message is similar to the events direct from CloudTrail, but the message format is different.

Event Path for Unsupported Method

S3 Bucket creates Event notification on ObjectCreated:PUT -> S3 Publishes to SNS Topic -> SQS Queue is Subscribed to Topic.

The format of this message is not understood.

Our FortiSIEM integration for Cloud Trail does not support S3 Bucket Event Notifications

FAQ

Why doesn't FortiSIEM support this method for CloudTrail logging?

For the FortiSIEM CloudTrail integration, FortiSIEM expects an SQS queue dedicated to CloudTrail message ingest. Using the CloudTrail service to publish to SNS->Queue ensures the integration only gets CloudTrail logs to process. Using S3 event notification will send messages for non-CloudTrail objects and cause an error.

Generic AWS S3 Log Ingestion for Anything other than CloudTrail

Starting in 6.5.0, for generic log ingestion via S3 bucket event notifications, see [Amazon Simple Storage Service \(AWS S3\)](#).

AWS CloudTrail Topics

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)
- [Configure Simple Queue Service \(SQS\) Delivery](#)
- [Set Up Simple Notification Service \(SNS\)](#)
- [Give Permission for Amazon SNS to Send Messages to SQS](#)
- [Settings for Access Credentials](#)
- [Sample Events for AWS CloudTrail](#)
- [Performance Tuning for High EPS CloudTrail Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
CloudTrail API	None	None	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Cloudtrail" to see the event types associated with this device. See the [Amazon API reference](#) for more information about the event types available for CloudTrail monitoring.

Reports

In **RESOURCES > Reports**, search for "cloudtrail" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in [AWS Access Key IAM Permissions and IAM Policies](#).

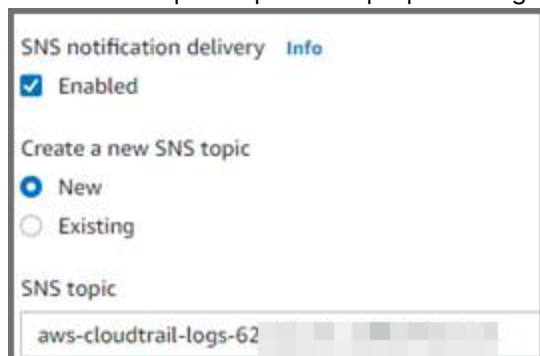
FortiSIEM receives information about AWS events through the CloudTrail API. After creating an S3 bucket for the storage of log files on AWS, you then configure the Simple Notification Service (SNS) and Simple Queue Service (SQS) to create a notification for the log file and have it delivered by SQS. In your FortiSIEM virtual appliance you then enter access credentials so FortiSIEM can communicate with CloudTrail as it would any other device.

Note: Do not add any extra SNS notifications in the SQS queue. The queue should only have one SNS subscription, otherwise pulling logs will not function.

Create a New CloudTrail

1. Log in to <https://console.aws.amazon.com/cloudtrail>.
2. Switch to the **region** for which you want to generate cloud trail logs.
3. Click **Trails**.
4. Click on **Add New Trail**.
5. Enter a **Trail name** such as aocloudtrail.
6. Select **Yes** for **Apply Trail to all regions**.
FortiSIEM can pull trails from all regions via a single credential.
7. Select **Yes** for **Create a new S3 bucket**.
8. For S3 bucket, enter a name like s3aocloudtrail.
9. Click **Advanced**.
10. Select **Yes** for **Create a new SNS topic**.

Note: This step is required for proper configuration. Do not skip.



11. For **SNS topic**, enter a name like snscloudtrail.
12. Leave the rest of advanced settings to the default values.

13. Click **Create**.
A dialog will confirm that logging is turned on.

Configure Simple Queue Service (SQS) Delivery

1. Log in to <https://console.aws.amazon.com/sqs>.
2. Switch to the **region** in which you created a new cloudtrail above.
3. Click **Create New Queue**.
4. Enter a **Queue Name** such as sqsaocloudtrail.

Setting	Value
Default Visibility Timeout	0 seconds
Message Retention Period	10 minutes
This must be set for between 5 and 50 minutes. A lower value is recommended for high event rates to avoid event loss.	
Maximum Message Size	256 KB
Delivery Delay	0 seconds
Receive Message Wait Time	5 seconds

5. Click **Create Queue**.
6. When the queue is created, click the **Details** tab and make note of the **ARN** (Amazon Resource Name), as you will need this when configuring the Simple Notification Service below and when configuring the access credentials for FortiSIEM.

Set Up Simple Notification Service (SNS)

1. Log in to <https://console.aws.amazon.com/sns>.
2. Switch to the **region** where you created the trail and SQS.
3. Select **Topics**.
4. Select the SNS topic `snsaocloudtrail` that you specified when creating a cloudtrail.
5. Click **Actions > Subscribe to topic** from the menu to launch the popup **Create Subscription**.
6. For **Protocol**, select **Amazon SQS**.
7. For **Endpoint**, enter the **ARN** of the queue that you created when setting up SQS.
8. Click **Create Subscription**.

Give Permission for Amazon SNS to Send Messages to SQS

1. Log in to <https://console.aws.amazon.com/sqs>.
2. Select the queue you created, `sqsaocloudtrail`.
3. In the **Queue Actions** menu, select **Subscribe Queue to SNS Topic**.

4. From the **Choose a Topic** dropdown, select the SNS topic `snsaocloudtrail` that you created earlier.
5. The **Topic ARN** will be automatically filled.
6. Click **Subscribe**.

Note: Ensure that SQS, SNS, S3 bucket and CloudTrail are in the same region.

You do not need to initiate discovery of AWS Cloud Trail, but should check that FortiSIEM is pulling events for AWS by checking for an **amazon.com** entry in **ADMIN > Setup > Pull Events**.

You can configure FortiSIEM to communicate with your device by following the instructions in "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with the CloudTrail API.

Setting	Value
Name	aocloudtrail
Device Type	Amazon AWS CloudTrail
Access Protocol	Amazon AWS CloudTrail
Region	Region where you created the trail.
Bucket	The name of the S3 bucket you created (s3aocloudtrail)
SQS Queue URL	Enter the URL of the SQS queue without the <code>http://</code> prefix. For example: <code>sqs.<region>.amazonaws.com/<account-id>/<queue-name></code>
Password Config	See Password Configuration .
Access Key ID	The access key for your AWS instance.
Secret Key	The secret key for your AWS instance.
Organization	Select an organization from the drop-down list.

Sample Events for AWS CloudTrail

```
Fri Oct 10 14:44:23 2014 FortiSIEM-CloudTrail
[additionalEventData/LoginTo]=https://console.aws.amazon.com/console/home?state=
hashArgs%23&isauthcode=true
```

```
[additionalEventData/MFAUsed]=No [additionalEventData/MobileVersion]=No [awsRegion]=us-east-1
[eventID]=fdf8f837-7e75-46a0-ac95-b6d15993ebf7 [eventName]=ConsoleLogin [eventSource]=SIGNIN
[eventTime]=2014-10-10T06:38:11Z [eventVersion]=1.01 [requestParameters]=null
[responseElements/ConsoleLogin]=Success [sourceIPAddress]=211.144.207.10 [userAgent]=Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.120 Safari/537.36
[userIdentity/accountId]=623885071509 [userIdentity/arn]=arn:aws:iam::623885071509:user/John.Doe
[userIdentity/principalId]=AIDAIUSNMEIUYBS7AN4UW [userIdentity/type]=IAMUser
[userIdentity/userName]=John.Doe
```

```
Fri Oct 10 14:19:45 2014 FortiSIEM-CloudTrail [awsRegion]=us-east-1 [eventID]=351bda80-39d4-41ed-
9e4d-86d6470c2436 [eventName]=DescribeInstances [eventSource]=EC2 [eventTime]=2014-10-10T06:12:24Z
[eventVersion]=1.01 [requestID]=2d835ae2-176d-4ea2-8523-b1a09585e803
[requestParameters/filterSet/items/0/name]=private-ip-address
[requestParameters/filterSet/items/0/valueSet/items/0/value]=10.0.0.233 [responseElements]=null
[sourceIPAddress]=211.144.207.10 [userAgent]=aws-sdk-php2/2.4.7 Guzzle/3.7.1 curl/7.19.7 PHP/5.3.3
[userIdentity/accessKeyId]=AKIAI2MUUCROHFSLLT3A [userIdentity/accountId]=623885071509
[userIdentity/arn]=arn:aws:iam::623885071509:root [userIdentity/principalId]=623885071509
[userIdentity/type]=Root [userIdentity/userName]=example
```

Performance Tuning for High EPS CloudTrail Events

AWS CloudTrail can generate a lot of events. Follow these recommendations to enable FortiSIEM to keep up with high EPS CloudTrail events.

1. In the AWS configuration, change the **Message retention period** of SQS to 1 day.
2. Adjust the CloudTrail event pulling parameters as follows. Go to the Collector that pulls AWS CloudTrail events. You will find these three relevant parameters in the `/opt/phoenix/config/phoenix_config.txt` file:
 - `cloudtrail_msg_pull_interval` (default 30 seconds, minimum recommended 10 seconds) - how often CloudTrail events are pulled.
 - `cloudtrail_msg_pull_thread_num` (default 1, maximum recommended 60) - how many threads are used to pull CloudTrail events.
 - `cloudtrail_file_parse_thread_num` (default 3, maximum recommended 60) - how many threads are used to parse CloudTrail events.

Since each API call returns maximum 10 files, set the parameters to satisfy the following two constraints. If the thread count is high, then you must increase the number of vCPUs in the Collector.

- Set `(SQSInputEventRate times cloudtrail_msg_pull_interval)` to be smaller than `(cloudtrail_msg_pull_thread_num times 10)`
- Set `cloudtrail_msg_pull_thread_num` to be equal to `cloudtrail_file_parse_thread_num`

Amazon AWS EC2

- [AWS Access Key IAM Permissions and IAM Policies](#)
- [Configuration](#)

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New**.
 - a. Enter the following settings from the table into the Access Method Definition dialog box:
Note: For more information, see "[Setting Credentials](#)" in the User's Guide to create a new credential.

Settings	Description
Name	<set name>
Device Type	Amazon AWS EC2
Access Protocol	AWS SDK
Region	[Required] Region in which your AWS instance is located
Access Key ID	[Required] Access key for your AWS instance
Secret Key	[Required] Secret key for your AWS instance
Description	Description about the device

- b. Click **Save**.
3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter "amazon.com" in the **IP/Host Name** field, if it does not already appear.
 - b. Select the name of your AWS EC2 credential from the **Credentials** drop-down list if it is not already selected.
 - c. Click **Save**.
 4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Amazon AWS EC2.
 5. Navigate to **Admin > Setup > Discovery**, and click **New**.
 - a. In the **Name** field, enter a name, such as "AWS_EC2".
 - b. From the **Discovery Type** drop-down list, select **AWS Scan**.
 - c. From the **Credential** drop-down list, select the credential you created, if it is not already selected.
 - d. Click **Save**.

6. To see the jobs associated with AWS, select **ADMIN > Setup > Pull Events**.
7. To see the received events select **ANALYTICS**, then enter "AWS" in the search box.

AWS EC2 CloudWatch API

FortiSIEM Support Added: 4.7.2

FortiSIEM Last Modification: 6.3.1

Vendor Version Tested: Not Provided

Vendor: Amazon

Product Information: <https://aws.amazon.com/cloudwatch/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
CloudWatch API	• Machine name • Internal Access IP • Instance ID • Image ID • Availability Zone • Instance Type • Volume ID • Status • Attach Time • Event Logs	• CPU Utilization • Received Bits/sec • Sent Bits/sec • Disk reads (Instance Store) • Disk writes (Instance Store) • Disk reads/sec (Instance Store) • Disk writes/sec (Instance Store) • Packet loss • Read Bytes (EBS) • Write Bytes (EBS) • Read Ops (EBS) • Write Ops (EBS) • Disk Queue (EBS) • AWS or Custom event logs stored in AWS CloudWatch	Performance Monitoring CloudWatch Events Monitoring

Event Types

- PH_DEV_MON_EBS_METRIC captures EBS metrics

In **ADMIN > Device Support > Event Types**, search for "AWS-CloudTrail" to see the event types associated with this device. CloudWatch allows for different AWS event sources and custom event sources to store events in AWS CloudTrail.

To search for these event types, from **ANALYTICS**, click in the **Edit Filters and Time Range...** field, and take the following steps:

1. In Filter, select the **Event Attribute** radio button.
2. In the **Attribute** field, enter "Event Type".
3. In the **Operator** field, select "CONTAIN".
4. In the **Value** field, enter "AWS_VPC_FLOW".
5. Under **Row**, click **+** to add another row.
6. In the new row, in the **Attribute** field, enter "Raw Event Log".
7. In the new row, in the **Operator** field, select "CONTAIN".
8. In the new row, in the **Value** field, enter "AWS_CLOUDWATCH_EVENT_DATA".
9. Configure your Time Range and click **Apply & Run**.

Configuration

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in [AWS Access Key IAM Permissions and IAM Policies](#).

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#). You should also be sure to read the topic "Discovering Amazon Web Services (AWS) Infrastructure".

VPC Flow logs are supported. For more information, see [HOW TO - Integrate Amazon VPC Flows](#).

The purpose of this discovery is to poll a list of EC2 instances in a given region so FortiSIEM knows that they are part of your AWS infrastructure. No logs are collected, but a CMDB entry for each EC2 instance is categorized under the "AWS" group in CMDB. This is important for certain reports that only look at AWS resources. It is still required to configure individual VMs with appropriate logging configurations, such as installable Agents (Linux, Windows) or Agentless (Syslog or WMI). Follow the instructions for the type of guest VM in this guide.

If you only want CloudWatch integration, you can create your AWS user and configure that user's policy by taking these steps.

Note: For the latest AWS documentation, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, choose **Users** and then choose **Add user**.
3. Type the user name for the new user. This is the sign-in name for AWS.
4. Select **Programmatic access** for the type of access this user will have.
5. Choose **Next: Permissions**.
6. Select **Attach existing policies directly**.
7. Select the policy **CloudwatchReadOnlyAccess**.
8. Choose **Next: Tags**.
9. Choose **Next: Review**.

10. Choose **Create user**.
11. Choose **Show** and record the Access key ID.
Note: To save the access keys, choose **Download .csv** and then save the file to a safe location.
This is your only opportunity to view or download the secret access keys. You will not have access to the secret keys again after this step.
12. Choose **Show** and record the secret key.
Note: To save the access keys, choose **Download .csv** and then save the file to a safe location.
This is your only opportunity to view or download the secret access keys. You will not have access to the secret keys again after this step.
13. Click **Close**.

Settings for Access Credentials

FortiSIEM Configuration Setup

Complete these steps in the FortiSIEM UI:

1. Navigate to **ADMIN > Setup** and click the **Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Setting	Value
Name	ec2
Device Type	Amazon AWS CloudWatch
Access Protocol	AWS CloudWatch
Region	The region in which your AWS instance is located
AWS Account	The name of your AWS account.
Log Group Name	Name of the log group.
Log Stream Name	Name of the log stream.
Password Config	See Password Configuration .
Access Key ID	The access key for your EC2 instance
Secret Key	The secret key for your EC2 instance

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Select the ec2 credential you created earlier from the **Credentials** drop-down list. It should autofill **IP/Host Name** as destination "amazon.com".
 - b. Click **Save**.

4. Select the new mapping and click the **Test** drop-down list and select **Test Connectivity without Ping** to start pulling.

Sample Events

```
[PH_DEV_MON_EC2_METRIC]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
```

```
[lineNumber]=6571,[hostName]=ec2-54-81-216-218.compute-1.amazonaws.com,[hostIpAddr]=192.0.2.131,  
[cpuUtil]=0.334000,[diskReadKBytesPerSec]=0.000000,[diskWriteKBytesPerSec]=0.000000,  
[diskReadReqPerSec]=0.000000,[diskWriteReqPerSec]=0.000000,[sentBytes]=131,[recvBytes]=165,  
[sentBitsPerSec]=17.493333,[recvBitsPerSec]=22.026667,[phLogDetail]=
```

```
[PH_DEV_MON_EBS_METRIC]:[eventSeverity]=PHL_INFO,[fileName]=deviceAws.cpp,
```

```
[lineNumber]=133,[hostName]=ec2-52-69-215-178.ap-northeast-1.compute.amazonaws.com,  
[hostIpAddr]=198.51.100.50,[diskName]=/dev/sda1,[volumeId]=vol-63287d9f,  
[diskReadKBytesPerSec]=7.395556,[diskWriteKBytesPerSec]=7.395556,[ioReadsPerSec]=0.000000,  
[ioWritesPerSec]=0.010000,[diskQLen]=0,[phLogDetail]=
```

AWS Elastic Load Balancer (ELB)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Event](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
AWS API		Permitted traffic	Log analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "aws elb" to see the event types associated with this device.

Rules

There are no specific rules available for AWS ELB.

Reports

In **RESOURCES > Reports**, search for "aws elb" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- [Setup in AWS](#)
- [Setup in FortiSIEM](#)

Setup in AWS

Follow the steps here to complete your setup in AWS.

- [Enable Elastic Load Balancing Access Logs](#)
- [Enable Event Notifications](#)
- [Generate a New Access Key](#)

Enable Elastic Load Balancing Access Logs

Take the following steps to enable Elastic Load Balancing Access Logs.

1. Go to the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. On the navigation pane, under **LOAD BALANCING**, select **Load Balancers**.
3. Select your load balancer.
4. On the **Description** tab, select **Configure Access Logs**.
5. On the **Configure Access Logs** page, take the following steps:
 - a. Select **Enable access logs**.
 - b. Leave **Interval** as the default (60 minutes).
 - c. At **S3 location**, enter the name of your S3 bucket, including the prefix, for example, `my-loadbalancer-logs/my-app`. You can specify the name of an existing bucket or a name for a new bucket.
 - d. (Optional) If the bucket does not exist, select **Create this location for me**. You must specify a name that is unique across all existing bucket names in Amazon S3 and follows the DNS naming conventions. For more information, see [Bucket naming rules](#) in the Amazon Simple Storage Service Guide.
 - e. Click **Save**.

Enable Event Notifications

Take the following steps to enable Event Notifications.

1. Go to the Amazon S3 console at <https://s3.console.aws.amazon.com/s3/>.
2. Select your bucket.
3. Click **Properties**.
4. Click **Event notifications > Create event notification**.
 - a. Input **Event name** and **Prefix**.
 - b. Select **All object create events for Event Types**.
 - c. Select **SQS queue** for **Destination**.
 - d. Select your SQS.
 - e. Click **Save changes**.

Notes:

- There are no other servers to use with SQS. This is because the format of the message in SQS coming from other servers may not be the same as that coming from S3 used by the ELB server. For example, a message coming from the Cloudtrail server may not be the same.
- Ensure the **Message retention period** property for SQS is 12 hours.
- Ensure the **Default visibility timeout** property for SQS is 1 day.

Generate a New Access Key

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, select **Users**.
3. Click **Add user**.
4. In the **User Name** field, enter a user name.
5. For **AWS access type**, select **Programmatic access**.
6. Click **Next: Permissions**.
7. Select the **Attach existing policies directly** tab.
8. Select **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess**.
9. Click **Next: Tags**, then click **Next: Review**.
10. Click **Create user**.
11. Click **Download Credentials**. The downloaded CSV file contains the Access Key ID and Secret Access Key that will be used in FortiSIEM.
12. Click **Close**.

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in [AWS Access Key IAM Permissions and IAM Policies](#).

You can now configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#). You should also be sure to read the topic [Discovering Amazon Web Services \(AWS\) Infrastructure](#).

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:
Note: Make sure no other devices use the same credential, otherwise events may appear missing.

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS ELB
Access Protocol	AWS_ELB
Region	The region in which your AWS instance is located
Bucket	The AWS S3 bucket

Settings	Description
SQS Queue URL	Provide the full URL, for example: <code>https://sqs.us-west-2.amazonaws.com/623885071509/sqsforloadblancer</code>
Password Config	See Password Configuration .
Access Key ID	The access key for your EC2 instance
Secret Key	The secret key for your EC2 instance
Confirm Secret Key	Enter the secret key for validation.
Session Token	If you provided an access key, you can leave this field blank.
Organization	Select an organization from the drop-down list.
Description	Description about the device

- In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - Select the name of your credential from the **Credentials** drop-down list.
 - Click **Save**.
- Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS ELB.
- To see the jobs associated with AWS ELB, select **ADMIN > Setup > Pull Events**.
- To see the received events select **ANALYTICS**, then enter "ELB" in the search box.

Sample Event

```
AWS-ELB:phCustId=1,reptDevIpAddr=10.10.103.205,reptDevName=amazon.com,msg=http 2021-02-11T01:56:06.000372Z app/shashi-elb/061d492a88a60fb1 10.10.168.108:46938 - -1 -1 -1 503 - 500 337 "POST http://10.10.29.144:80/boaform/admin/formLogin HTTP/1.1" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0" - - arn:aws:elasticloadbalancing:us-west-2:623885071509:targetgroup/user-tg/974fbb8764192573 "Root=1-60248eb5-01950dcf187ac3c244ab2231" "-" "-" 0 2021-02-11T01:56:05.999000Z "forward" "-" "-" "-" "-" "-" "-"
```

AWS Kinesis

Amazon Kinesis is an Amazon Web Service (AWS) for processing big data in real time. Kinesis is capable of processing hundreds of terabytes per hour from high volumes of streaming data from sources such as operating logs, financial transactions and social media feeds.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuring AWS Kinesis](#)
- [Configuring FortiSIEM](#)
- [Configuring AWS CloudTrail Logs through Kinesis Streams](#)
- [Configuring VPC Flow Logs through Kinesis Streams](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information collected	Used for
Amazon AWS Client Library	Streaming data	Collect, process, and analyze real-time streaming data.

Event Types

In **RESOURCES > Event Types**, enter "Kinesis" in the main content panel **Search...** field to see the event types associated with this device.

Rules

No defined rules.

Reports

No defined reports.

Configuring AWS Kinesis

1. Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the [IAM console](#).
2. In the navigation bar on the upper right, choose your user name, and then choose My Security Credentials.
3. On the AWS **IAM Credentials** tab, in the Access keys for CLI, SDK, and API access section, do any of the following:
 - To create an access key, choose **Create access key**. Then choose **Download .csv** file to save the access key ID and secret access key to a .csv file on your computer. Store the file in a secure location. You will not have access to the secret access key again after this dialog box closes. After you have downloaded the .csv file, choose **Close**. When you create an access key, the key pair is active by default, and you can use the pair right away.
 - To disable an active access key, choose **Make inactive**.
 - To reenable an inactive access key, choose **Make active**.
 - To delete an access key, choose its **X** button at the far right of the row. Then choose **Delete** to confirm. When you delete an access key, it's gone forever and cannot be retrieved. However, you can always create new keys.

Configuring FortiSIEM

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in “[Setting Credentials](#)” in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS Kinesis
Access Protocol	AWS Kinesis Client Library
Region	You can enter one or more regions separated by a space, for example, “us-east-1 us-west-2”. See Supported Regions in AWS for a list of valid regions.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration . For CyberArk REST API, see CyberArk REST API Password Configuration . For RAX_Janus, see RAX_

Settings	Description
	Janus Password Configuration.
Access Key	Access key for your AWS Kinesis instance. See Configuring AWS Kinesis .
Secret Key	Secret key for your AWS Security Hub instance
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your AWS Kinesis credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS Kinesis.
5. To see the jobs associated with AWS Kinesis, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "AWS Kinesis" in the search box.

Configuring AWS CloudTrail Logs through Kinesis Streams

The data flow for this setup is AWS CloudTrail -> AWS CloudWatch -> AWS Kinesis Data Streams.

Taking the following steps to configure.

Prerequisite

- Obtain your access key and secret for a user account with administrator privileges.
 - Ensure the AWS CLI is installed. For more information on AWS CLI, see [here](#).
1. Run from cmd:


```
aws configure
```

 Enter your access key, secret and default region.
 Example:
 Account ID: 111111111111
 Access Key ID: aaaaaaaaaaaaaaaaaaaaaa
 Access Secret: 13452322222222222222
 Region: us-west-1
 Kinesis Role: SIEMKinesisRole
Note: This will be created in a later portion of this guide.
 2. Create log group by entering the following:


```
aws logs create-log-group --log-group-name "cloudwatch-group"
```

```
aws logs describe-log-groups
```
 3. Create a cloudtrail role that permits sending logs to the CloudWatch log group by putting the following JSON into a file, and save it as a JSON file on your desktop.


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Use the AWS CLI to run the following command, referencing the file path where you saved the JSON file. In this command example, the file above was saved as `cloudtrail-role.json`.

```
aws iam create-role --role-name CTRole --assume-role-policy-document file://cloudtrail-
role.json
```

5. Create the CloudTrail policy-document by saving the following JSON into a file, saving it to your desktop.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-west-1:111111111111:log-group:CloudTrail:log-stream:1111111111_
CloudTrail_us-west-1*"
      ]
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-west-1:111111111111:log-group:CloudTrail:log-stream:1111111111_
CloudTrail_us-west-1*"
      ]
    }
  ]
}
```

6. Use the AWS CLI to run the following command, referencing the file path where you saved the JSON file. In this command example, the file above was saved as `cloudtrail-policy.json`. **Note:** What we're doing

here is creating a role called "CTRole" and applying a policy to it.

```
aws iam put-role-policy --role-name CTRole --policy-name cloudtrail-policy --policy-document file://cloudtrail-policy.json
```

Kinesis Configuration Setup

Take the following steps to configure Kinesis. **Note:** The latest instructions can be found [here](#).

1. Create an AWS Kinesis stream (if it does not exist). In this example, we'll create one called "fortisiem".

```
aws kinesis create-stream --stream-name "fortisiem"
```

2. Create a file called "TrustPolicyForCWL.json" using the following code.

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "logs.us-west-1.amazonaws.com" },
    "Action": "sts:AssumeRole"
  }
}
```

3. Create an iam role with the defined policy, called "CWLtoKinesisRole" by running the following command.

```
aws iam create-role --role-name CWLtoKinesisRole --assume-role-policy-document file://~/TrustPolicyForCWL.json
```

4. Create a permission file called "PermissionsForCWL.json" using the following code.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kinesis:PutRecord",
      "Resource": "arn:aws:kinesis:us-west-1: 111111111111:stream/fortisiem"
    }
  ]
}
```

5. Associate the above policy file with the role we created, by running the following command.

```
aws iam put-role-policy --role-name CWLtoKinesisRole --policy-name Permissions-Policy-For-CWL --policy-document
```

6. Create the subscription to forward cloudwatch logs.

Note: The following multiline command is for Windows, as ^ indicates the command continues on the next line. If using Linux, use the multiline command for Linux, which replaces the ^ with \. Paste all of it in as one command.

Windows:

```
//Create CloudWatch Log Subscription filter:
aws logs put-subscription-filter ^
  --log-group-name "cloudwatch-group" ^
  --filter-name "fortisiem" ^
```

```
--filter-pattern "" ^
--destination-arn "arn:aws:kinesis:us-west-1:111111111111:stream/fortisiem" ^
--role-arn "arn:aws:iam::111111111111:role/CWLtoKinesisRole"
```

Linux:

```
//Create CloudWatch Log Subscription filter:
aws logs put-subscription-filter \
  --log-group-name "cloudwatch-group" \
  --filter-name "fortisiem" \
  --filter-pattern "" \
  --destination-arn "arn:aws:kinesis:us-west-1:111111111111:stream/fortisiem" \
  --role-arn "arn:aws:iam::111111111111:role/CWLtoKinesisRole"
```

7. Create an IAM user account that FortiSIEM can use to ingest Kinesis Data Streams. When assigning permissions for the IAM user, the following must be allowed.

Consumer		
Actions	Resource	Purpose
DescribeStream	Kinesis data stream	Before attempting to read records, the consumer checks if the stream exists and is active, and if the shards are contained in the stream.
Get Records, Get ShardIterator	Kinesis data stream	Read records from a Kinesis Data Streams shard.
CreateTable, DescribeTable, GetItem, PutItem, Scan, Update Item	Amazon DynamoDB table	If the consumer is developed using the Kinesis Client Library (KCL), it needs permissions to a DynamoDB table to track the processing state of the application. The first consumer started creates the table.
Delete Item	Amazon DynamoDB table	For when the consumer performs split/merge operations on Kinesis Data Stream shards.
PutMetricData	Amazon CloudWatch log	The KCL also uploads metrics to

Consumer		
Actions	Resource	Purpose
		CloudWatch, which are useful for monitoring the application.

8. Navigate to IAM -> Users -> Add user
Access Type: Programmatic Access
Next Permission:
9. Under permissions, select Attach existing policies directly
AmazonKinesisReadOnlyAccess
AmazonDynamoDBFullAccess
CloudWatchLogsFullAccess
Note: If step 11 is followed, it replaces the more generic access policy set here in step 9, which would no longer be needed.
10. Click Next -> Review.
You should see that under Permissions summary, the following policies attached to the user.

Type	Name
Managed policy	CloudWatchLogsFullAccess
Managed policy	AmazonDynamoDBFullAccess
Managed policy	AmazonKinesisReadOnlyAccess

11. Once the user is created, generate an access key and secret for this user. The following reference link demonstrates how to implement restrictive, minimum access policies to FortiSIEM (which is the consumer as referenced in the guide). - <https://docs.aws.amazon.com/streams/latest/dev/tutorial-stock-data-kplkcl-iam.html>
Note: For advanced users, you can customize permissions policies to allow only access to a specific CloudWatch log group, specific Kinesis Stream, etc....

FortiSIEM Configuration Setup

Go to the **ADMIN > Setup > Credentials** tab.

In Step 1: Enter Credentials:

1. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
2. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, such as

Settings	Description
	KinesisStreamIntegration
Device Type	Amazon AWS Kinesis
Access Protocol	AWS Kinesis Client Library
Region	You can enter one or more regions separated by a space, for example, "us-east-2 us-west-1". See Supported Regions in AWS for a list of valid regions.
Log Stream Name	Enter "fortisiem" or the name of your stream.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration . For CyberArk REST API, see CyberArk REST API Password Configuration . For RAX_Janus, see RAX_Janus Password Configuration .
Access Key	Access key for your AWS Kinesis instance. See Configuring AWS Kinesis .
Secret Key	Your Secret key.
Organization	The organization the device belongs to.
Description	Description of the device.

- In **Step 2: Enter IP Range to Credential Associations**, to the right of the **Search...** field, select the desired collector that will poll CloudTrail logs from the drop-down list if you have more than one collector. If only one collector is available, the drop-down list will not be available.
- Click **New**.
 - Select the CloudTrail credential you created earlier from the **Credentials** drop-down list. It should autofill **IP/Host Name** as destination "amazon.com". FortiSIEM will handle communication to the appropriate API.
 - Click **Save**.
- Select the new mapping and click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling.
- To see the jobs associated with AWS Kinesis, select **ADMIN > Setup > Pull Events**.
- To see the received events select **ANALYTICS**, then enter "AWS Kinesis" in the search box.

Configuring VPC Flow Logs through Kinesis Streams

The data flow for this setup is AWS VPC Flow Logs -> AWS CloudWatch -> AWS Kinesis Data Streams. Taking the following steps to configure.

Prerequisite

- Obtain your access key and secret for a user account with administrator privileges.
 - Ensure the AWS CLI is installed. For more information on AWS CLI, see [here](#).
1. Run from cmd:
`aws configure`
 Enter your access key, secret and default region.
 Example:
 Account ID: 111111111111
 Access Key ID: aaaaaaaaaaaaaaaaaaaaaa
 Access Secret: 13452322222222222222
 Region: us-west-1
 2. Configure AWS VPC flow logs to send to CloudWatch logs by following similar steps documented [here](#).

Kinesis Configuration Setup

Take the following steps to configure Kinesis. **Note:** The latest instructions can be found [here](#).

1. Create an AWS Kinesis stream (if it does not exist). In this example, we'll create one called "fortisiem".
`aws kinesis create-stream --stream-name "fortisiem"`
2. Create a file called "TrustPolicyForCWL.json" using the following code.

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "logs.us-west-1.amazonaws.com" },
    "Action": "sts:AssumeRole"
  }
}
```

3. Create an iam role with the defined policy, called "CWLtoKinesisRole" by running the following command.
`aws iam create-role --role-name CWLtoKinesisRole --assume-role-policy-document file://~/TrustPolicyForCWL.json`
4. Create a permission file called "PermissionsForCWL.json" using the following code.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kinesis:PutRecord",
      "Resource": "arn:aws:kinesis:us-west-1: 111111111111:stream/fortisiem"
    }
  ]
}
```

5. Associate the above policy file with the role we created, by running the following command.
`aws iam put-role-policy --role-name CWLtoKinesisRole --policy-name Permissions-Policy-For-CWL --policy-document`

6. Create the subscription to forward cloudwatch logs.

Note: The following multiline command is for Windows, as ^ indicates the command continues on the next line. If using Linux, use the multiline command for Linux, which replaces the ^ with \. Paste all of it in as one command.

Windows:

```
//Create CloudWatch Log Subscription filter:
aws logs put-subscription-filter ^
  --log-group-name "cloudwatch-group" ^
  --filter-name "fortisiem" ^
  --filter-pattern "" ^
  --destination-arn "arn:aws:kinesis:us-west-1:111111111111:stream/fortisiem " ^
  --role-arn "arn:aws:iam::111111111111:role/CWLtoKinesisRole "
```

Linux:

```
//Create CloudWatch Log Subscription filter:
aws logs put-subscription-filter \
  --log-group-name "cloudwatch-group" \
  --filter-name "fortisiem" \
  --filter-pattern "" \
  --destination-arn "arn:aws:kinesis:us-west-1:111111111111:stream/fortisiem " \
  --role-arn "arn:aws:iam::111111111111:role/CWLtoKinesisRole "
```

7. Create an IAM user account that FortiSIEM can use to ingest Kinesis Data Streams. When assigning permissions for the IAM user, the following must be allowed.

Consumer		
Actions	Resource	Purpose
DescribeStream	Kinesis data stream	Before attempting to read records, the consumer checks if the stream exists and is active, and if the shards are contained in the stream.
Get Records, Get ShardIterator	Kinesis data stream	Read records from a Kinesis Data Streams shard.
CreateTable, DescribeTable, GetItem, PutItem, Scan, Update Item	Amazon DynamoDB table	If the consumer is developed using the Kinesis Client Library (KCL), it needs permissions to a DynamoDB table to track the processing state of the application. The first

Consumer		
Actions	Resource	Purpose
		consumer started creates the table.
Delete Item	Amazon DynamoDB table	For when the consumer performs split/merge operations on Kinesis Data Stream shards.
PutMetricData	Amazon CloudWatch log	The KCL also uploads metrics to CloudWatch, which are useful for monitoring the application.

8. Navigate to IAM -> Users -> Add user
Access Type: Programmatic Access
Next Permission:
9. Under permissions, select Attach existing policies directly
AmazonKinesisReadOnlyAccess
AmazonDynamoDBFullAccess
CloudWatchLogsFullAccess
Note: If step 11 is followed, it replaces the more generic access policy set here in step 9, which would no longer be needed.
10. Click Next -> Review.
You should see that under Permissions summary, the following policies attached to the user.

Type	Name
Managed policy	CloudWatchLogsFullAccess
Managed policy	AmazonDynamoDBFullAccess
Managed policy	AmazonKinesisReadOnlyAccess

11. Once the user is created, generate an access key and secret for this user. The following reference link demonstrates how to implement restrictive, minimum access policies to FortiSIEM (which is the consumer as referenced in the guide). - <https://docs.aws.amazon.com/streams/latest/dev/tutorial-stock-data-kplkcl-iam.html>
Note: For advanced users, you can customize permissions policies to allow only access to a specific CloudWatch log group, specific Kinesis Stream, etc....

FortiSIEM Configuration Setup

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:

- a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
- b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, such as KinesisStreamIntegration
Device Type	Amazon AWS Kinesis
Access Protocol	AWS Kinesis Client Library
Region	You can enter one or more regions separated by a space, for example, "us-east-2 us-west-1". See Supported Regions in AWS for a list of valid regions.
Log Stream Name	Enter "fortisiem" or the name of your stream.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration . For CyberArk REST API, see CyberArk REST API Password Configuration . For RAX_Janus, see RAX_Janus Password Configuration .
Access Key	Access key for your AWS Kinesis instance. See Configuring AWS Kinesis .
Secret Key	Your Secret key.
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, to the right of the **Search...** field, select the desired collector that will poll CloudTrail logs from the drop-down list if you have more than one collector. If only one collector is available, the drop-down list will not be available.
4. Click **New**.
 - a. Select the CloudTrail credential you created earlier from the **Credentials** drop-down list. It should autofill the **IP/Host Name** field as destination "amazon.com". FortiSIEM will handle communication to the appropriate API.
 - b. Click **Save**.
5. Click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling.
6. To see the jobs associated with AWS Kinesis, select **ADMIN > Setup > Pull Events**.
7. To see the received events select **ANALYTICS**, then enter "AWS Kinesis" in the search box.

Sample Events

VPC Log Example

```
2021-04-27T08:40:50.00Z [FSM-AWSKinesis] 2 311111777194 eni-054c755e644dcf32d 103.114.104.68
172.31.9.216 22898 22717 6 1 40 1619538050 1619538102 REJECT OK

2021-04-27T09:14:45.00Z [FSM-AWSKinesis] 2 311111777194 eni-054c755e644dcf32d 172.31.9.216
222.187.239.109 22 43638 6 3 3996 1619540085 1619540142 ACCEPT OK
```

CloudTrail Log Example

```
2021-04-28T14:29:51.783Z [FSM-AWSKinesis] {"eventVersion":"1.08","userIdentity":
{"type":"Root","principalId":"921045424829","arn":"arn:aws:iam::1234567890AB:root","accountId":"11
1115424829","accessKeyId":"ASIA1234567890ABCDEF","sessionContext":{"sessionIssuer":
{},"webIdFederationData":{},"attributes":{"mfaAuthenticated":"false","creationDate":"2021-04-
28T20:37:47Z"}}},"eventTime":"2021-04-
28T21:13:07Z","eventSource":"health.amazonaws.com","eventName":"DescribeEventAggregates","awsRegion":
"us-east-1","sourceIPAddress":"10.20.30.40","userAgent":"console.amazonaws.com","requestParameters":
{"aggregateField":"eventTypeCategory","filter":{"eventStatusCodes":
["open","upcoming"],"startTimes":[{"from":"Apr 21, 2021 9:13:07
PM"]}}},"responseElements":null,"requestID":"1a712381-62d1-4485-8ce5-
109930945c62","eventID":"eb8c077f-321d-471a-b207-
849f5089a428","readOnly":true,"eventType":"AwsApiCall","managementEvent":true,"eventCategory":"Man
agement","recipientAccountId":"921045424829"}
```

AWS RDS

- What is Discovered and Monitored
- Event Types
- Configuration
- Sample Events

What is Discovered and Monitored

Type	Protocol	Information Discovered	Metrics Collected	Used For
Relational Database Storage (RDS)	CloudWatch API		• CPU Utilization • User Connections • Free Memory • Free Storage • Used Swap • Read Latency • Write Latency • Read Ops • Write Ops	Performance Monitoring

Event Types

- PH_DEV_MON_RDS_METRIC captures RDS metrics

Configuration

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in [AWS Access Key IAM Permissions and IAM Policies](#).

Discovering AWS RDS

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential

Settings	Description
Device Type	Amazon AWS RDS
Access Protocol	AWS SDK
Region	Set Region as the region in which your AWS instance is located.
Password Config	See Password Configuration .
Access Key ID	Access key for your EC2 instance.
Secret Key	Secret key for your EC2 instance
Organization	Select an Organization from the drop-down list.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Set **IP/Host Name** to amazon.com.
 - b. Select the name of your AWS RDS credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS RDS.
5. Go to **ADMIN > Setup > Discovery**.
6. Click **New**.
7. Fill out the information in the Discovery Definition window, ensuring you set **Discovery Type** as AWS Scan.
8. When done, click **Save**.
9. Select the entry and click **Discover**.
10. After Discovery finishes, check **CMDB > Devices > Amazon Web Services > AWS Database**.

Sample Events

```
[PH_DEV_MON_RDS_METRIC]:[eventSeverity]=PHL_INFO,[fileName]=deviceAwsRDS.cpp,[lineNumber]=104,[hostName]=mysql11.cmdzvce07ar.ap-northeast-1.rds.amazonaws.com,[hostIpAddress]=54.64.131.93,[dbCpuTimeRatio]=1.207500,[dbUserConn]=0,[dbEnqueueDeadlocksPerSec]=0.000587,[freeMemKB]=489,[freeDiskMB]=4555,[swapMemUtil]=0.000000,[ioReadsPerSec]=0.219985,[ioWritesPerSec]=0.213329,[devDiskRdLatency]=0.08,[devDiskWrLatency]=0.4029,[phLogDetail]=
```

AWS Security Hub

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Requirements](#)
- [Configuring AWS Security Hub](#)
- [To Create, Modify, or Delete Your Own IAM User Access Keys \(Console\)](#)
- [Configuring FortiSIEM for AWS Security Hub Access](#)
- [Sample Events](#)

Security Hub collects security data from across AWS accounts, services, and supported third-party partner products. Configure FortiSIEM to gather this data collected by Security Hub, so FortiSIEM can analyze this data to identify the highest priority security issues.

What is Discovered and Monitored

Protocol	Information collected	Used for
AWS Security Hub SDK	Security data	Security and compliance

Event Types

In **RESOURCES > Event Types**, enter "AWS Sechub" in the main content panel **Search...** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, enter "AWS Sechub" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, enter "AWS Security Hub" in the main content panel **Search...** field to see the reports associated with this device.

Requirements

FortiSIEM uses PHP V3 SDK to integrate data from the security hub to perform comprehensive security analytics.

Configuring AWS Security Hub

Supported Regions in AWS

Security Hub only collects events from the region where you enabled Security Hub. If you don't enable the Security Hub for other regions, then you won't get events from those regions. FortiSIEM allows you to specify multiple regions when you create a new credential. In the regions you specify, the Security Hub will be enabled. These regions should use the following AWS region codes:

Region Name	Region Code
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
EU (Stockholm)	eu-north-1
South America (São Paulo)	sa-east-1

Step 1: Enable Security Hub

Permissions required to [enable Security Hub](#)

1. The IAM identity (user, role, or group) that you use to enable Security Hub must have the required permissions. To grant the permissions required to enable Security Hub, attach the following policy to an IAM user, group, or role.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

2. Use the credentials of the IAM identity from step 1 to sign in to the Security Hub console. When you open the Security Hub console for the first time, choose **Get Started** and then choose **Enable Security Hub**.

Step 2: Get an Access Key

This feature supports [long-term access keys](#). Access keys consist of two parts: an access key ID and a secret access key.

Permissions Required

To [create access keys for your own IAM user](#), you must have the permissions from the following policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateOwnAccessKeys",
```

```
"Effect": "Allow",
"Action": [
  "iam:CreateAccessKey",
  "iam:GetUser",
  "iam:ListAccessKeys"
],
"Resource": "arn:aws:iam::*:user/${aws:username}"
}
```

To Create, Modify, or Delete Your Own IAM User Access Keys (Console)

1. Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the [IAM console](#).
2. In the navigation bar on the upper right, choose your user name, and then choose My Security Credentials.
3. On the AWS IAM Credentials tab, in the Access keys for CLI, SDK, and API access section, do any of the following:
 - To create an access key, choose Create access key. Then choose Download .csv file to save the access key ID and secret access key to a .csv file on your computer. Store the file in a secure location. You will not have access to the secret access key again after this dialog box closes. After you have downloaded the .csv file, choose Close. When you create an access key, the key pair is active by default, and you can use the pair right away.
 - To disable an active access key, choose Make inactive.
 - To reenable an inactive access key, choose Make active.
 - To delete an access key, choose its X button at the far right of the row. Then choose Delete to confirm. When you delete an access key, it's gone forever and cannot be retrieved. However, you can always create new keys.

Configuring FortiSIEM for AWS Security Hub Access

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS Security Hub
Access Protocol	AWS Security Hub SDK
Region	You can enter one or more regions separated by a space, for example, "us-east-1 us-west-2". See Supported Regions in AWS for a list of valid regions.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration . For CyberArk REST API, see CyberArk REST API Password Configuration . For RAX_Janus, see RAX_Janus Password Configuration .
Access Key	Access key for your AWS Security Hub instance. See Step 2: Get an Access Key .
Secret Key	Secret key for your AWS Security Hub instance
Session Token	The session token is used by credentials from Rax Scan. If you obtained an access key as described in Step 2: Get an Access Key , then leave this field empty.
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Select the name of your AWS Security Hub credential from the **Credentials** drop-down list. The **IP/Host Name** field/destination should auto populate to "amazon.com".
 - b. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS Security Hub.
5. To see the jobs associated with AWS Security Hub, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "AWS Security Hub" in the search box.

Sample Events

```
[AWS_SECURITY_HUB_EVENT_DATA] ={
  "AwsAccountId": "111111111111",
  "CreatedAt": "2019-08-06T04:56:44.894Z",
```

```

    "Description": "10.10.10.72 is performing SSH brute force attacks against i-0100ee1e110c011c1. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.",
    "FirstObservedAt": "2019-08-06T04:51:14Z",
    "GeneratorId": "arn:aws:guardduty:us-west-2:111111111111:detector/50b2ea07131dbe1530c23facb594b1fa",
    "Id": "arn:aws:guardduty:us-west-2:111111111111:detector/50b2ea07131dbe1530c23facb594b1fa/finding/8cb632a4b32f7c3b854d9f5347bf07a4",
    "LastObservedAt": "2019-08-06T05:22:54Z",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
    "ProductFields": {
      "action/actionType": "NETWORK_CONNECTION",
      "action/networkConnectionAction/blocked": "false",
      "action/networkConnectionAction/connectionDirection": "INBOUND",
      "action/networkConnectionAction/localPortDetails/port": "22",
      "action/networkConnectionAction/localPortDetails/portName": "SSH",
      "action/networkConnectionAction/protocol": "TCP",
      "action/networkConnectionAction/remoteIpDetails/country/countryName": "Ruritania",
      "action/networkConnectionAction/remoteIpDetails/geoLocation/lat": "12.7265",
      "action/networkConnectionAction/remoteIpDetails/geoLocation/lon": "132.7756",
      "action/networkConnectionAction/remoteIpDetails/ipAddressV4": "10.10.10.72",
      "action/networkConnectionAction/remoteIpDetails/organization/asn": "56047",
      "action/networkConnectionAction/remoteIpDetails/organization/asnOrg": "Ruritania Mobile communications corporation",
      "action/networkConnectionAction/remoteIpDetails/organization/isp": "Ruritania Mobile Yourtown",
      "action/networkConnectionAction/remoteIpDetails/organization/org": "Ruritania Mobile",
      "action/networkConnectionAction/remotePortDetails/port": "33242",
      "action/networkConnectionAction/remotePortDetails/portName": "Unknown",
      "archived": "false",
      "aws/securityhub/CompanyName": "Amazon",
      "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/guardduty/arn:aws:guardduty:us-west-2:111111111111:detector/50b2ea07131dbe1530c23facb594b1fa/finding/8cb632a4b32f7c3b854d9f5347bf07a4",
      "aws/securityhub/ProductName": "GuardDuty",
      "aws/securityhub/SeverityLabel": "MEDIUM",
      "count": "7",
      "detectorId": "50b2ea07131dbe1530c23facb594b1fa",
      "resourceRole": "TARGET"
    },
    "RecordState": "ACTIVE",
    "Resources": [
      {
        "Details": {
          "AwsEc2Instance": {
            "ImageId": "ami-f2c2408a",
            "IPv4Addresses": [

```

```

        "10.10.10.20",
        "10.0.0.137"
    ],
    "LaunchedAt": "2019-08-05T17:10:47.000Z",
    "SubnetId": "subnet-931605f1",
    "Type": "m5.4xlarge",
    "VpcId": "vpc-c66576a4"
}
},
"Id": "arn:aws:ec2:us-west-2:111111111111:instance/i-0799ee6e490c078c5",
"Partition": "aws",
"Region": "us-west-2",
"Tags": {
    "Name": "elasticsearch-node-coordinator"
},
"Type": "AwsEc2Instance"
}
],
"SchemaVersion": "2018-10-08",
"Severity": {
    "Normalized": 40,
    "Product": 2
},
"Title": "310.10.10.72 is performing SSH brute force attacks against i-0799ee6e490c078c5. ",
"Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
],
"UpdatedAt": "2019-08-06T05:28:24.425Z",
"WorkflowState": "NEW",
"phCustId": 1,
"serverIp": "10.10.10.22",
"serverName": "amzon.com"
}

```

AWS Simple Queue Service (SQS)

Support Added: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: Amazon

Product: Amazon Simple Queue Service (SQS)

Product Information: <https://aws.amazon.com/sqs/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
AWS SQS		service logs	Log analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "aws sqs" to see the event types associated with this device.

Rules

There are no specific rules available for AWS SQS.

Reports

There are no specific reports available for AWS SQS.

Configuration

- [Setup in FortiSIEM](#)

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:
Note: Make sure no other devices use the same credential, otherwise events may appear missing.

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS SQS
Access Protocol	AWS SQS
Region	The region in which your AWS instance is located .
SQS Queue URL	Provide the full URL, for example: <code>https://sqs.us-west-2.amazonaws.com/623885071509/sqsforloadblancer</code>
Pull Interval	The interval in which FortiSIEM will pull events from AWS SQS. Default is 5 minutes.
Password Config	See Password Configuration .
Access Key ID	The access key for your EC2 instance
Secret Key	The secret key for your EC2 instance
Confirm Secret Key	Enter the secret key for validation.
Session Token	If you provided an access key, you can leave this field blank.
Organization	Select an organization from the drop-down list.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS SQS.
5. To see the jobs associated with AWS SQS, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "AWS" in the search box.

Amazon Simple Storage Service (AWS S3)

Amazon Simple Storage Service (AWS S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use it to store and protect

any amount of data.

Support Added: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: Amazon

Product: AWS S3

Product Information: <https://aws.amazon.com/s3/>

- [Configuration](#)
- [Sample Events](#)

Configuration

- [Setup in AWS S3](#)
- [Setup in FortiSIEM](#)

Setup in AWS S3

Complete these steps from AWS S3.

Generate a New Access Key

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>
2. In the navigation pane, choose **Users**.
3. Click **Create Users**.
4. In the **User name** field, enter a user name.
5. For **AWS access type**, select **Programmatic access - with an access key**.
6. Click **Next: Permissions**.
7. Select the **Attach existing policies directly** tab.
8. Select **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess**.
9. Click **Next: Tag**.
10. Click **Next: review**.
11. Click **Create user**.
12. Click **Download Credentials**.
13. Click on the **Close** button.

The downloaded CSV file contains the Access Key ID (User Name) and Secret Access Key (Password) that will be used in the FortiSIEM configuration.

Enable Event Notifications

1. Open the Amazon S3 console at <https://s3.console.aws.amazon.com/s3/>
2. Select your bucket.
3. Click **Properties**.
4. Click **Event notifications > Create event notification**.
 - a. In the **Event name** field, enter a event name.
 - b. In the **Prefix** field, enter a prefix.

Note: Leave this field blank to generate an event for all objects created in an S3 bucket. If you only want a specific subfolder (terminology defined as prefix in S3 bucket) to generate events, then you can define it.

Example: A prefix for /logs will only generate events when files are added under this prefix of the S3 bucket, but logs on the root prefix '/' will not generate events.

/logs/vpc_logs – Would generate an event when file created.

/logs/my_custom_logs – Would generate an event when file created.

/log1.gz – Would **NOT** generate an event when file created.

/cloudtraillog.json.gz – Would **NOT** generate an event when file created.
 - c. Under Event types, select **All object create events**.
 - d. For **Destination**, select **SQS queue**.
 - e. Select your SQS.
 - f. Click **Save changes**.

For your configuration, make sure of the following.

 - Ensure that there are no other servers that use this SQS.
 - Make sure the property **Message retention period** of SQS is set to 1 Days.
 - Make sure the property Default **visibility timeout** of SQS is set to 12 Hours.

Setup in FortiSIEM

Start a Pulling Job by taking the following steps.

1. Login to FortiSIEM.
2. Navigate to **ADMIN > Device Support > Devices/Apps**.
3. Click **New** to create a new device type.
4. In the **Category** drop-down list, select **Device**.

In the **Vendor** field, enter the vendor name, e.g. "Amazon".
5. In the **Model** field, enter the device model, e.g. "AWS S3".
6. In the **Version** field, enter the version device.
7. In the **Device/App Group** drop-down list, expand **Devices**, and select a value, e.g. "Generic".
8. From the **Access Protocol** drop-down list, select **AWS_S3_WITH_SQS**.
9. Click **Save**.

Create a new Access Method Credential by taking the following steps.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Select the device type you created earlier.
Access Protocol	AWS_S3_WITH_SQS
Bucket	Enter your AWS bucket.
SQS Queue URL	Enter your SQS queue URL. You must enter the entire URL, for example: <code>https://sqs.us-west-2.amazonaws.com/111111111111/sqsforloadblancer</code> .
User Name	Enter the username for your AWS S3 account. This will be the Access Key ID when you generated your access key. Note: Make sure no other devices uses the credential. Otherwise, events may be missed in this device.
Password	Enter the password associated with your username. This will be the Secret Access Key when you generated your access key.
Session Token	This can be left blank. It is not required for S3 integration.
Log Keyword	By default, a log keyword is provided. Feel free to change this and enter a keyword that can be easily matched by a custom parser. This will simplify the creation of a parser for the logs collected from the AWS S3 bucket.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the server.
5. Navigate to **ADMIN > Setup > Pull Events** to see the new job.

Events can be queried from the **ANALYTICS** page.

Forwarding Logs to S3

Customers can forward any services logs to S3 if those services allow it to do so. Examples include AWS Elastic Load Balancing, Cisco Umbrella. Customer also can upload any logs file to S3 manually.

Forward ELB Access Logs to AWS S3

Please refer to “Setup in AWS” at <https://docs.fortinet.com/document/fortisiem/7.2.7/external-systems-configuration-guide/470868/aws-elastic-load-balancer#AWS>

Forward Cisco Umbrella Log to AWS S3

Please refer to <https://docs.umbrella.com/deployment-umbrella/docs/setting-up-an-amazon-s3-bucket>.

Upload Log File to AWS S3

Note: The file format currently can be any extension. (e.g. no extension, .txt, .log, .json, .log.gz, etc). The filetype is checked if it is zipped using gzip (regardless of extension .gz). If it is zipped using gzip, FortiSIEM will unzip the log.

Logs are processed as 1 line per log in the file. The entirety of a single log entry must exist on one line. Multiline JSON (JSON log entries spanning multiple lines in the log file) logs will be supported in an upcoming release.

e.g.

file1.txt contents:

```
{"Name" : "log1"}
```

```
{"Name" : "log2"}
```

```
{"Name" : "log3"}
```

Log4 text

Sample Logs

Note that in Credential Definition, you can change the text (Log Keyword = AWS_S3_LOG_KEYWORD_1) e.g. VPCFLOWLOGS if S3 bucket contains VPC flow logs. This is important for parsing the logs later in FortiSIEM.

```
AWS_S3_LOG_KEYWORD_1:phCustId=1,reptDevIpAddr=192.0.2.20,reptDevName=amazon.com,msg={"Name" : "log1"}
```

```
AWS_S3_LOG_KEYWORD_1:phCustId=1,reptDevIpAddr=192.0.2.20,reptDevName=amazon.com,msg={"Name" : "log2"}
```

```
AWS_S3_LOG_KEYWORD_1:phCustId=1,reptDevIpAddr=192.0.2.20,reptDevName=amazon.com,msg={"Name" : "log3"}
```

```
AWS_S3_LOG_KEYWORD_1:phCustId=1,reptDevIpAddr=192.0.2.20,reptDevName=amazon.com,msg=Log4 text
```

Take the following steps.

1. Open the Amazon S3 console at <https://s3.console.aws.amazon.com/s3/>.
2. Select your bucket.
3. Click **Upload** and then click **Add files**.
4. Select log files and click **Upload**.

Notes: FortiSIEM only supports:

- gz compression file, and uncompressed files (e.g. no extension, .txt, .log, .json, etc...)
- "Single event per line" in log file

Sample Events

Logs from AWS ELB

```
AWS_S3_LOG_KEYWORD_1:phCustId=1,reptDevIpAddr=192.0.2.20,reptDevName=amazon.com,msg=http 2021-02-11T01:56:06.000372Z app/shashi-elb/061d492a88a60fb1 192.0.2.108:46938 - -1 -1 -1 503 - 500 337
"POST http://192.0.2.144:80/form/admin/formLogin HTTP/1.1" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0" - - arn:aws:elasticloadbalancing:us-west-2:623885071509:targetgroup/shashi-tg/974fbb8764192573 "Root=1-60248eb5-01950dcf187ac3c244ab2231"
"- " "- " 0 2021-02-11T01:56:05.999000Z "forward" "- " "- " "- " "- " "- " "- "
```

Logs from AWS Cloudtrail

```
AWS_S3_LOG_KEYWORD_1:phCustId=1,reptDevIpAddr=10.10.103.205,reptDevName=amazon.com,msg=
{"Records":[{"eventVersion":"1.05","userIdentity":
{"type":"IAMUser","principalId":"AIDAZCQTSWSKVN6P266F6","arn":"arn:aws:iam::623885071509:user/dusan",
"accountId":"623885071509","accessKeyId":"ASIAZCQTSWSKZ5NL340B","userName":"dusan","sessionContext":{"sessionIssuer":{"webIdFederationData":{"attributes":
{"mfaAuthenticated":"false","creationDate":"2019-09-05T09:05:25Z"}},
"invokedBy":"signin.amazonaws.com"},"eventTime":"2019-09-05T11:16:21Z",
"eventSource":"lambda.amazonaws.com","eventName":"ListFunctions20150331","awsRegion":"us-west-1",
"sourceIPAddress":"85.241.114.212","userAgent":"signin.amazonaws.com","requestParameters":null,
"responseElements":null,"requestID":"26057495-d109-4366-9961-77955807e508","eventID":"321c137a-8999-48a3-89f6-7168e4107ecb","eventType":"AwsApiCall","recipientAccountId":"623885071509"}]}
```

Box/Box.com

FortiSIEM Support Added: 4.7.2

FortiSIEM Last Modification: 6.4.0

Vendor Version Tested: Not Provided

Vendor:Box

Product Information: <https://www.box.com/overview>

- [Integration Points](#)
- [Box API Integration](#)
- [Configuration](#)

Integration Points

Protocol	Information Discovered	Used For
Box API		Security and Compliance

Box API Integration

FortiSIEM can pull audit events from Box.com Cloud Service via Box API.

Configuration

- [Configuring Box.com Service](#)
- [Configuring FortiSIEM](#)

Configuring Box.com Service

Create an account to be used for FortiSIEM communication, taking note of the following:

- A general account can pull user events
- An Admin account can pull enterprise events
- A unique **Client ID** and **Client Secret** can only start one job. It cannot be used to start multiple jobs.

Take the following steps:

1. Login to the Box developer's console at <https://app.box.com/developers/console>.
2. Navigate to **My Apps > Create New APP**.
3. Click **Custom App**.

4. Select **User Authentication (OAuth 2.0)**.
5. In the **App Name** field, enter the application name.
6. Click **Create App**.
7. Under **Configuration**, make a record of the **Client ID** and **Client Secret** of the new application. This will be used when creating a credential in [Configuring FortiSIEM](#).
8. In the Redirect URI field, enter the URI in the following format:
`https://<supervisor_ip_address>:443/phoenix/boxAuth?custId=<ID>`
 Example:
`https://10.10.10.10:443/phoenix/boxAuth?custId=2112`
9. Click **Save Changes**.

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Box.com Box
Access Protocol	Box API
Client ID	Provide the Client ID obtained in step 7 of Configuring Box.com Service . Note: A unique Client ID and Client Secret can only start one job. It cannot be used to start multiple jobs.
Client Secret	Provide the Client Secret obtained in step 7 of Configuring Box.com Service .
Account	Choose Account as the email address for the account created while Configuring Box.com Service .
Organization	Choose the Organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

3. After clicking **Save**, you will be redirected to the Box.com website. Enter the credentials for Box.com and click **Authorize**.
4. Click **Grant Access to Box**. You should see that the authorization for FortiSIEM to access your Box account was successful.

5. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Select the Credential created in step 2a from the **Credentials** drop-down list.
 - b. The **IP/Host Name** should automatically be set to api.box.com.
 - c. Click **Save**.
6. Select the entry from step 5, click the **Test** drop-down list and select **Test Connectivity** and make sure it succeeds, which implies that the credential is correct.
7. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Box.com Cloud Service using the Box.com API.
8. To see the received events, go to **ADMIN > Setup > Pull Events**, select the Box.com entry and click **Report**. The system will take you to the **ANALYTICS** tab and run a query to display the events received from Box in the last 15 minutes. You can modify the time interval to get more events.

Cisco Umbrella

FortiSIEM Support Added: 6.3.2

FortiSIEM Last Modification: 7.3.1

Vendor: Cisco

Product Information: <https://umbrella.cisco.com/>

There are two methods to ingest Cisco Umbrella audit log data:

- (Recommended) Cisco Umbrella publishing logs to an S3 bucket (either Cisco Managed or Customer managed), and FortiSIEM ingests that data using AWS S3 integration.
- FortiSIEM collecting the data via Cisco Umbrella Reporting and Management API.

The method for ingestion via S3 buckets is recommended for high EPS environments.

You can follow the Generic Log API Poller (HTTPS Advanced) Integration documentation [here](#) on creating your own logging API integrations for other endpoints that provide interesting data to ingest for auditing purposes.

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Cisco Umbrella.

Protocol	Metrics Collected	Used For
AWS S3 Integration	DNS logs, Proxy logs, IP logs (Traffic logs), Admin Audit logs	Security Monitoring

Protocol	Metrics Collected	Used For
Umbrella Reporting and Management API via Generic HTTPS Poller	DNS, Proxy, Firewall, Intrusion logs via Activity API; List users and other information using Reporting API	Security Monitoring

Configuration

The following configuration options are available:

- [Configuration via AWS S3 Integration](#)
- [Configuring Cisco Umbrella API using Generic HTTPS Poller](#)

Configuration via AWS S3 Integration

- [Setup in Cisco Umbrella](#)
- [Setup in FortiSIEM](#)

Setup in Cisco Umbrella

Complete these steps from the Cisco Umbrella Portal.

1. Login to dashboard.umbrella.com.
2. Navigate to **Admin > Log Management**.
3. Navigate to Amazon S3.
4. Select the **Use Cisco-Managed S3 storage** radio button.
5. Select the closest geographically region to the FortiSIEM instance that will poll the logs.
6. Select the desired retention duration.
Note: Since this will be ingested by FortiSIEM, it is recommended to select the shortest duration.
7. Click **Save**.
8. Click **Continue**.
9. On the final screen, record these values for [Setup in FortiSIEM](#).
 - Data Path: This is the S3 bucket URL
 - Access Key
 - Secret Key
10. Click **Got It**.
11. Click **Continue**.
Cisco Umbrella setup is now complete. However, it may take some time to activate.

Note: You can select company-managed s3 bucket, but you must provide an access key and secret with appropriate permissions. Cisco managed takes away the difficulty with IAM permissions for S3 bucket access.

Setup in FortiSIEM

FortiSIEM processes events from Cisco Umbrella via the AWS S3 bucket API. Obtain your Access Key, Secret Key, and S3 bucket URL from the Cisco Umbrella Portal before proceeding.

Complete these steps in the FortiSIEM UI:

1. For Multi-tenant users, change the scope to the appropriate FortiSIEM organization.
2. Go to the **ADMIN > Setup > Credentials** tab.
3. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box, and click **Save** when done.

Settings	Description
Name	Enter a name for the credential.
Device Type	Cisco Umbrella
Access Protocol	AWS_S3
Region	Enter the AWS region for the bucket that was created, which can be found by looking at the data path name. For example, <code>cisco-managed-us-east-1</code>, means "us-east-1", so you would input <code>us-east-1</code> in the Region field. If you know your region, you can use the region information from the link below. For example, for the region Europe (Frankfort), input <code>eu-central-1</code> in the Region field. Region information can be found here: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html
Bucket	Use the Data Path field from Amazon S3 (available by going to https://dashboard.umbrella.com/ and navigating to Admin > Log Management) to get the Bucket value. Enter the Bucket value that appears before the forward slash, e.g. <code>cisco-managed-us-east-1</code>.

Settings

Description

If there is no prefix specified in the S3 data path section, e.g. `s3://umbrella-managed-1105020-07c11114f2bd1366f0cef0db1048d111`, the bucket should be `umbrella-managed-1105020-07c11114f2bd1366f0cef0db1048d111`.

Example:

Bucket: `umbrella-managed-1105020-07c11114f2bd1366f0cef0db1048d111`

Amazon S3

Status

Last Sync

● Active (Managed)

Jan 31, 2025 at 4:22 AM

✓

We're sending data to your Cisco-managed S3 storage.

Storage Region

US East (N. Virginia)

Retention Duration

30 days [Edit](#)

Admin Audit Log

Include Admin Audit Log in S3

☒

Log Https Query

Log Query Parameters for HTTPS transaction

☒

Data Path

s3://cisco-managed-us-east-1/538[REDACTED]1253

Last Sync

Jan 31, 2025 at 4:22 AM

Schema Version

v11 [View Details](#)

Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#).

Forget your keys?

You can regenerate them below. Note that this will invalidate any existing keys.

STOP LOGGING

REGENERATE KEYS

Prefix

Use the **Data Path** field from Amazon S3 (available by going to <https://dashboard.umbrella.com/> and navigating to **Admin > Log Management**) to get the **Prefix** value. Provide the prefix; This is the part with the forward slash from the **Data Path** field.

Example:

Note: This example provides an obfuscated version of the Data Path value. The actual Prefix value would be made up of alpha and numeric characters instead of "@" and "#".

If the **Data Path** is: s3://cisco-managed-us-east-1/538####

@#@@##@#####@#@#@#@#@#@#@#@#@#@#@#@#253

then the Prefix value is:

538#### @#@@##@#####@#@@@#@@@#@@@#@@@#@@@#@@@#@###@#253

The prefix may be entered in any of the following ways:

/XXXX/

XXXX

/xxxx

xxxx/

Examples:

/538#### @#@#@#@#####@#@#@#@#@#@#@#@#@#@#@#@#@#@#@#@#253/

538#### @#@@##@#####@#@@@@#@@@#@@@@#@@@#@@@##@@#253

Settings	Description
	/538####_#@########@#@#@#@#@#@#@#@#@#@#@#@#253 538####_#@########@#@#@#@#@#@#@#@#@#@#@#@#253/ If there is no prefix specified in the S3 data path section, e.g. s3://umbrella-managed-something, enter only a forward slash, "/". Example: Prefix: /
Access Key ID	Enter/paste the access key you acquired during the Cisco Umbrella setup .
Secret Key	Enter/paste the secret key you acquired during the Cisco Umbrella setup .
Log Keyword	Leave the default option, which is Cisco_Umbrella_Log.
Description	Description about the device

4. In **Step 2: Enter IP Range to Credential Associations**, if you have more than one FortiSIEM collector, select the collector that will do the polling from the drop-down list.
Note: A drop-down list will not appear if you only have one collector.
5. Click **New**.
 - a. Select the credential name you created (during step 3a) from the **Credentials** drop-down list. The **IP/Host Name** field should auto populate the URL (api.umbrella.com).
 - b. Click **Save**.
6. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection.
7. Wait for approximately 5 minutes.
8. Navigate to **Analytics**, and confirm that events appear.

Configuring Cisco Umbrella API using Generic HTTPS Poller

This is not needed if you have already configured AWS S3 integration.

This integration uses pre-built definition files for specific Cisco Umbrella API endpoints using the HTTPS Advanced credential type. There are two examples provided. One with the Cisco Umbrella Reporting API, and another with the Cisco Umbrella Management API.

Configure Cisco Umbrella Reporting API

Take the following steps.

Set up Cisco Umbrella Reporting API Credentials

1. Login to <https://login.umbrella.com/>.
2. Navigate to **Admin > API Keys**.
3. Select **Umbrella Reporting** or click **New API Key**.

- a. Under **Key Scope**: Ensure both Admin (Roles and Users) and all Reports scopes are selected. For each scope, ensure it is set to Read-Only.
 - b. Set optional expiry date: Never expire OR a defined interval that you will have to re-create and re-enter the key into the SIEM.
4. Click **Generate**.

The generated values will be an OAuth2.0 client ID and client secret. Copy these values as well as the OAuth2.0 endpoint for later use.

Note: The unified Umbrella API doesn't have a region specific API endpoint so this step can be skipped.

Configuring FortiSIEM

This credential configuration implements the following API endpoint:

<https://developer.cisco.com/docs/cloud-security/#!get-activities-all>

Take the following steps.

1. Navigate to **ADMIN > Setup > Credentials**.
2. In **Step 1: Enter Credentials**, take the following steps.
 - a. In the **Name** field, enter "CiscoUmbrellaActivity".
 - b. In the **Device Type** field, enter "Cisco Umbrella".
 - c. From the **Access Protocol** drop-down list, select/enter **HTTPS Advanced**.
 - d. Download the following file: [Umbrella_Report_All_Activity_https_advanced_definition.json](#)
 - e. Click **Import Definition**, and select the file Umbrella_Report_All_Activity_https_advanced_definition.json downloaded from step d.
 - f. Click **Yes** to overwrite.
 - g. Only for Multi-Org and Managed Child Organizations:

Note: If you do not do this, the data returned will be for whichever organization the API key was generated for.

Using this method, you can generate one API key in the parent organization, and simply update the child ID in each FortiSIEM organization.

Ensure you configure the credential in the target FortiSIEM organization so that data is not mixed.

i.e. FortiSIEM Organization ABC -> Create Credential for Umbrella Child Organization 12345

FortiSIEM Organization XYZ -> Create Credential for Umbrella Child Organization 9876

Click the **Authentication Parameters** icon, and take the following steps.

 - i. Click the **Header** tab, then **New**.
 - ii. For header **Key Name**, enter "X-Umbrella-OrgId".
 - iii. For header **Key Value**, enter the target child organization ID you'd like to poll events for.
 - iv. Click **OK**.
 - v. Click **Save**.
 - h. Click the **Authentication Parameters** icon, and take the following steps.
 - i. In the **Client ID** field, enter the Client ID you generated earlier for Cisco Umbrella Reporting API.

Note: Several Umbrella APIs each use different authentication. This one is for reporting API.
 - ii. For **Client Secret**, enter the client secret that was generated earlier.
 - iii. Click **OK**.
 - i. Click **Save** to save the entire credential.

3. In **Step 2: Enter IP Range to Credential Associations**, if you have more than one FortiSIEM collector, select the collector that will do the polling from the drop-down list.
Note: A drop-down list will not appear if you only have one collector.
4. Click **New**.
 - a. In the **IP/Host Name** field, enter "api.umbrella.com".
 - b. Click **+**, and add all relevant Cisco Umbrella credentials that each represent an API call to get data.
 - c. Click **Save**.
 - d. Select the Step 2 mapping that was just saved/created.
5. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection. If you encounter an error, refer to [Common Errors](#) for additional information that may help you resolve the issue.
6. Observe that the test connectivity and confirm that it is successful.
7. Wait for approximately 5 minutes for the first set of events to get pulled in.
8. Navigate to **Analytics**, and confirm that events appear by searching for event type containing "CiscoUmbrella".

Configure Cisco Umbrella Management API

Take the following steps.

Set up Cisco Umbrella Management API Credentials

1. Login to <https://login.umbrella.com/>.
2. Navigate to **Admin > API Keys**.
3. Select **Umbrella Management** or click **New API Key**.
 - a. Under **Key Scope**: Ensure both Admin (Roles and Users) and all Management scopes are selected. For each scope, ensure it is set to Read-Only.
 - b. Set optional expiry date: Never expire OR a defined interval that you will have to re-create and re-enter the key into the SIEM.
4. Click **Generate**.
Copy the API Key and Secret Keys for authentication use later.

Configuring FortiSIEM

You can pull various endpoints using the management API. We only provide an example for Listing Users API (<https://api.umbrella.com/admin/v2/users>). This API endpoint continually polls a list of users in the Cisco Umbrella portal, and packages each into a log message in the following format:

Event Type: CiscoUmbrella-User-<status> Active/Inactive etc.

Take the following steps.

1. Navigate to **ADMIN > Setup > Credentials**.
2. In **Step 1: Enter Credentials**, take the following steps.
 - a. In the **Name** field, enter "CiscoUmbrellaListUsers".
 - b. In the **Device Type** field, enter "Cisco Umbrella".
 - c. From the **Access Protocol** drop-down list, select/enter **HTTPS Advanced**.
 - d. Download the following file: [Umbrella_List_Users_https_advanced_definition.json](#)

- e. Click **Import Definition**, and select the file Umbrella_List_Users_https_advanced_definition.json downloaded from step d.

- f. Click **Yes** to overwrite.

- g. Only for Multi-Org and Managed Child Organizations:

Note: If you do not do this, the data returned will be for whichever organization the API key was generated for.

Using this method, you can generate one API key in the parent organization, and simply update the child ID in each FortiSIEM organization.

Ensure you configure the credential in the target FortiSIEM organization so that data is not mixed.

i.e. FortiSIEM Organization ABC -> Create Credential for Umbrella Child Organization 12345

FortiSIEM Organization XYZ -> Create Credential for Umbrella Child Organization 9876

Click the **Authentication Parameters** icon, and take the following steps.

- i. Click the **Header** tab, then **New**.
- ii. For header **Key Name**, enter "X-Umbrella-OrgId".
- iii. For header **Key Value**, enter the target child organization ID you'd like to poll events for.
- iv. Click **OK**.
- v. Click **Save**.

- h. Click the **Authentication Parameters** icon, and take the following steps.

- i. In the **Username** field, enter the API Key generated earlier for Cisco Umbrella Management API.

Note: Several Umbrella APIs each use different authentication. This one is for management API.

- ii. In the **Password** field, enter the Secret Key that was generated earlier.

- iii. Click **OK**.

- i. Click **Save** to save the entire credential.

- 3. In **Step 2: Enter IP Range to Credential Associations**, if you have more than one FortiSIEM collector, select the collector that will do the polling from the drop-down list.

Note: A drop-down list will not appear if you only have one collector.

- 4. Click **New**.

- a. In the **IP/Host Name** field, enter "api.umbrella.com".

- b. Click **+**, and add all relevant Cisco Umbrella credentials that each represent an API call to get data.

- c. Click **Save**.

- d. Select the Step 2 mapping that was just saved/created.

- 5. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection.

If you encounter an error, refer to [Common Errors](#) for additional information that may help you resolve the issue.

- 6. Observe that the test connectivity and confirm that it is successful.

- 7. Wait for approximately 5 minutes for the first set of events to get pulled in.

- 8. Navigate to **Analytics**, and confirm that events appear by searching for event type containing "CiscoUmbrella".

Sample Events

```
//CiscoUmbrella-DNS-A-Query-Success
1 146.112.59.20 reports.api.umbrella.com Cisco_Umbrella_Log 5381234_
```

```

b617173610f6e6a12340410126fdb516751f0/dnslogs/2021-08-25/2021-08-25-21-20-ade8.csv.gz : "2021-08-25 21:19:36","LAB-MACHINE","LAB-MACHINE","192.168.10.218","99.99.99.25","Allowed","1(A)","NOERROR","static-asm.secure.skypeassets.com.,"Chat,Instant Messaging,Software/Technology,Infrastructure,Internet Telephony,Application","Roaming Computers","Roaming Computers",""

//CiscoUmbrella-DNS-A-Query-Blocked
1 146.112.59.20 reports.api.umbrella.com Cisco_Umbrella_Log 5381234_
b617173610f6e6a12340410126fdb516751f0/dnslogs/2021-08-26/2021-08-26-19-00-44ea.csv.gz : "2021-08-26 19:03:13","LAB-MACHINE","LAB-MACHINE","192.168.10.218","99.99.99.25","Blocked","1(A)","NOERROR","www.facebook.com.,"Social Networking,Application,Application Block","Roaming Computers","Roaming Computers","Application,Application Block"

```

G42 Cloud

G42 is a cloud server platform that provides various services to its users.

Object Storage Service (OBS) is a G42 object-based storage service. It allows users to store and manage unstructured data, including log files, in a cost-effective and secure manner. All logs in G42 can be transferred to OBS.

Cloud Trace Service (CTS) is a log audit service for security. It allows you to collect, store, and query resource operation records. It can collect operations (Create/Upload/Delete log files) in OBS.

FortiSIEM can use the G42 REST API to get traces in CTS and download these log files in OBS according to traces.

Support Added: FortiSIEM 7.1.0

Vendor Version Tested: Not Provided

Vendor: G42 Cloud

Product: Cloud Services

Product Information: <https://www.g42cloud.com/#/>

- [Configuration](#)

Configuration

- [Setup in G42](#)
- [Setup in FortiSIEM](#)

Setup in G42

Complete these steps from G42 Console.

- [Generate a New Access Key](#)
- [Create a Bucket in OBS](#)
- [Create a Tracker to Trace a Bucket](#)

Generate a New Access Key

1. Log in to the management console, point to the username in the upper right corner, and select **My Credentials** from the drop-down list.
2. On the **My Credentials** page, you can find your **Account Name** and **Project ID**. The two attribute values will be used in FortiSIEM.
3. On the **My Credentials** page, click the **Access Keys** tab.
4. Click **Create Access Key**. In the dialog box that is displayed, enter the login password and verification code sent to your email or mobile phone.
5. Make sure it has permission to access OBS.
6. Click **OK** and download the generated Access Key/Secret Key (AK/SK) pair.
7. Retain this information as the Access Key and Secret Key will be used in FortiSIEM setup later.

Create a Bucket in OBS

1. Open the G42 OBS console.
2. Click **Create Bucket**.
3. Fill in the information on this page. Refer to the G42 document [here](#) for more details.
4. Click **Create Now**.

Create a Tracker to Trace a Bucket

1. Open the G42 CTS console.
2. Navigate to/click **Tracker List**.
3. Click **Create Tracker**.
 - a. For **OBS Bucket**, select the OBS bucket created in [Create a Bucket in OB](#), and select **Trace**.
 - b. For **Operation**, select **Write**.
 - c. For the other pages, fill in as necessary. Refer to the G42 document [here](#) for more information.
4. Click **Create**.

Setup in FortiSIEM

Start a Pulling Job by taking the following steps.

1. Login to FortiSIEM.
2. Navigate to **ADMIN > Device Support > Devices/Apps**.
3. Click **New** to create a new device type.
4. In the **Category** drop-down list, select **Device**.

In the **Vendor** field, enter the vendor name, e.g. "G42 Cloud".
5. In the **Model** field, enter the device model, e.g. "G42 Cloud".

6. In the **Version** field, enter the version device.
7. In the **Device/App Group** drop-down list, expand **Devices**, and select a value, e.g. "Generic".
8. From the **Access Protocol** drop-down list, select **G42_OBS_WITH_CTS**.
9. Click **Save**.

Create a new Access Method Credential by taking the following steps.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Select the device type you created earlier.
Access Protocol	G42_OBS_WITH_CTS
Region (optional)	Enter the region where your G42 resides.
Account Name	Enter/paste the Account Name used when you generated your Access Key .
Project Id	Enter/paste the Project Id used when you generated your Access Key .
Access Key	Enter/paste your Access Key.
Secret Key/Confirm Secret Key	Enter/paste your Secret Key.
Tracker Name	Enter the tracker name.
Split JSON Log	Check the Split JSON Log checkbox to enable.
JSON Log Array Key Path	Leave this field empty.
Log Keyword	By default, a log keyword is provided, which is G42_AUDIT_LOG.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the server.

5. Navigate to **ADMIN > Setup > Pull Events** to see the new job.
Events can be queried from the **ANALYTICS** page.

Forwarding Logs to OBS

- [Forward G42 Audit Logs to OBS](#)
- [Upload Log File to OBS](#)

Forward G42 Audit Logs to OBS

G42 uses CTS to record operations on cloud service resources, enabling you to query, audit, and backtrack operations. CTS records the following:

- Operations performed on the management console.
- Operations performed by calling supported APIs.
- Operations triggered by connected cloud services.

A tracker is automatically created when you enable CTS. This tracker identifies and associates with all cloud services your tenant account is using and records all operations of your tenant account.

The following steps allow you to forward logs to OBS.

1. Open the CTS console.
2. Navigate to **Tracker List**.
3. Select tracker **System**.
4. Click **Configure**.
5. On the **Configure Transfer** page, select the bucket you want to keep logs.
6. Click **Next > Configure**.

Upload Log File to OBS

Customer can upload log files manually.

1. Open the G42 OBS console.
2. Select your bucket.
3. Click **Upload** and then click **Add files**.
4. Select log files and click **Upload**.
Note: The log files in OBS must be in gz or txt format.

Google Cloud Platform (GCP)- Pub/Sub Integration

FortiSIEM Support Added: 6.3.1

FortiSIEM Last Modification: 6.3.1

Vendor Version Tested: Not Provided

Vendor: Google

Product Information: <https://cloud.google.com/>

What is Discovered and Monitored

- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Dashboard](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Logs Collected	Used For
Google Cloud Pub/Sub SDK	Admin Activity audit logs, Data Access Audit logs, System Event audit logs, Policy Denied audit logs. Arbitrary custom log ingestion via Pub/Sub topic.	GCP Audit Log ingestion, or Custom Log Ingestion

Event Types

In **ADMIN > Device Support > Event Types**, search for "GCP_A" in the **Search** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "GCP:" in the main content panel **Search...** field to see the rules associated with this application or device.

In 6.3.1 the following rules are available:

- GCP: Firewall Rule Created
- GCP: Firewall Rule Deleted
- GCP: Firewall Rule Patched
- GCP: IAM Custom Role Created
- GCP: IAM Custom Role Deleted
- GCP: IAM Member assigned role of type admin or owner
- GCP: Logging Sink Deleted, GCP: Logging Sink Updated
- GCP: Pub/Sub Subscription Created
- GCP: Pub/Sub Subscription Deleted
- GCP: Pub/Sub Topic Created
- GCP: Pub/Sub Topic Deleted
- GCP: Service Account Access Key Created

- GCP: Service Account Access Key Deleted
- GCP: Service Account Created
- GCP: Service Account Deleted
- GCP: Service Account Disabled
- GCP: Storage Bucket IAM Permissions Modified
- GCP: Storage Bucket Updated
- GCP: Storage or Logging Bucket Deleted
- GCP: VPC Network Deleted
- GCP: VPC Route Added
- GCP: VPC Route Deleted

Reports

There are many reports defined in **RESOURCES > Reports**. Search for "GCP:" in the main content panel **Search...** field.

In 6.3.1, the following reports are available:

- GCP: Firewall Rule Created, Deleted, or Changed
- GCP: IAM Custom Roles Created or Deleted
- GCP: IAM Policy Change Audit Report
- GCP: Logging Sinks Created, Updated, or Deleted
- GCP: Pub/Sub Subscriptions Created or Deleted
- GCP: Pub/Sub Topic Created or Deleted
- GCP: Service Account Access Keys Created or Deleted
- GCP: Service Accounts Created, Deleted, or Disabled
- GCP: Storage Bucket IAM Permissions Modified
- GCP: Storage Buckets Updated
- GCP: Storage or Logging Bucket Deleted
- GCP: Top Admin Activity Events by Principal
- GCP: Top Admin Activity Events by Source IP
- GCP: Top Data Access Events by Principal
- GCP: Top Data Access Events by Source IP
- GCP: Top Event Types by Count
- GCP: Top Traffic by Country
- GCP: VPC Network Created or Deleted
- GCP: VPC Routes Created or Deleted

Dashboard

A standard GCP Audit Dashboard can be found by navigating to **DASHBOARD**, and selecting **GCP Dashboard** from the Dashboard drop-down list.

Configuration

- [Google Cloud Platform Pub/Sub Setup](#)
- [FortiSIEM Service Account Setup](#)
- [FortiSIEM Configuration](#)
- [Custom Log Integration](#)

Google Cloud Platform Pub/Sub Setup

Google Cloud Platform (GCP) Log Flow: GCP audit logs sink -> Pub/Sub topic for FortiSIEM -> FortiSIEM ingest with standard log header appended

To set up GCP Pub/Sub:

1. Create a topic by taking the following steps:
 - a. Go to Pub/Sub Service in GCP console.
 - b. Select the project where the topic should reside.
 - c. In the Create Topic dialog boxes, enter the following options:
 - i. In the **Topic id** field, enter "fortisiem-topic", or a desired name for the topic.
 - ii. For **Leave option**, make sure the checkbox next to "**Add a default subscription**" is checked.
 - iii. When done, click **CREATE TOPIC**.
 - iv. Notate the topic name. Example: projects/fortisiem-integration-1111/topics/fortisiem-topic
 - v. Click on **Subscriptions** and notate the subscription name. Example: projects/fortisiem-integration-1111/subscriptions/fortisiem-topic-sub
2. Turn on audit logs for all services by taking the following steps:

Note: Not all auditing is on by default, so this configuration is necessary.

 - a. Go to **IAM & Admin**.
 - b. Select **Audit Logs** on the left hand toolbar.
 - c. Click the **Default Audit Config** button at the top of the screen.
 - d. Select all desired log options.
 For the most verbose log information, make sure to select the following 4 boxes: **Admin Read, Admin Write, Data Read, and Data Write**.
 For minimal logging, only select **Admin Read** and **Admin Write**.
Note: Optionally, VPC flows and Firewall Rule logs can be configured through the VPC network menu by taking the following steps:
 For Firewall rules, you must select each one you would like to enable with logs, edit, and then select the Logs radio button to turn on. Repeat for each desired Firewall rule.
 - i. Go to **VPC networks**.
 - ii. Select your desired Subnet.
 - iii. Click the **Flow logs** drop-down list.
 - iv. Set sampling interval to 5 seconds, and leave the rest as default.
 - e. Click **Done**.
3. Create an aggregated sink with the topic in pub/sub as the destination. The destination topic can be created in any Cloud project in any organization if the service account from the log sink has permission to write to the destination.

The serviceAccount entry is returned from the create sink command that shows which identity must be added to the particular Pub/Sub topic as a role Pub/Sub Publisher.

This identity represents a Google Cloud service account that has been created for the log export. Until you grant this identity, publisher permissions to the destination topic and log entry exports from this sink will fail. For more information, see step 4 for granting access for a resource.

Take the following steps:

- a. Select the Gcloud console (>) button on top right hand of your browser.
- b. Enter the following command:


```
gcloud organizations list
```
- c. You may be prompted to authorize the command. If so, select **yes**.
- d. Notate the Organization ID. Example: 87732091111
- e. Format your sink destination as `pubsub.googleapis.com/<pubsubtopic>`
- f. Run the following command if your project is tied to, or part of an organization; This command creates an organization wide sink called **fortisiem_sink** for all projects and folders, and sends all logs to the Pub/Sub topic specified.

```
gcloud logging sinks create fortisiem_sink \
pubsub.googleapis.com/projects/fortisiem-integration-1111/topics/fortisiem-topic --
include-children \
--organization=<organization_id>
```

If your project is not tied to, or has no organization, use the project id instead. It will create a sink of this project only, meaning only the logs from this project will go into the topic.

You can repeat this command for each sink you'd like to create per project. You can modify the sink name for each to ensure uniqueness.

```
gcloud logging sinks create fortisiem_sink \
pubsub.googleapis.com/projects/fortisiem-integration-1111/topics/fortisiem-topic --
include-children \
--project=<project_id>
```

- g. **!IMPORTANT!** Copy the output, and notate the service account created. It is required to permit the service to write to the pub/sub topic. Must be Pub/Sub Publisher.

Example:

Created [https://logging.googleapis.com/v2/organizations/87732091111/sinks/fortisiem_sink].

Grant **serviceAccount**:o111110938575-661167@gcp-sa-logging.iam.gserviceaccount.com the **Pub/Sub Publisher role** on the topic.

More information about sinks can be found at

https://cloud.google.com/logging/docs/export/configure_export

4. Configure aggregated sink service account for the given organization (from step 3) to publish to the created topic (created in step 1) by taking the following steps:
 - a. Go to the **Pub/Sub topics** service page.
 - b. Select the project where the topic was created.
 - c. Click on the topic (fortisiem-topic, or the topic name entered) from step 1.
 - d. Click **Show Info Panel** on the right hand toolbar to show the **Permissions** tab.
 - e. Click the **Add Member** button.
 - f. Paste the service account created with the aggregated sink that you created earlier here.
 - g. Apply role of Pub/Sub Publisher.

- h. Click **Add**.
Pub/Sub is now set up.

FortiSIEM Service Account Setup

A service account for FortiSIEM is required to ingest logs from the Pub/Sub topic. To create this account, take the following steps:

1. Go to the **Service accounts** page.
2. Click **Create Service Account**.
3. Select the project in the drop-down list where the Pub/Sub topic exists.
4. In the **Service Account Name** field, enter "fortisiem-pubsub", or a desired name for the service account.
5. Click **Create**.
6. Click **Continue**.
7. Select **Role Pub/Sub Subscriber**.
8. Click **Continue**.
9. Click **Done**.

Now, a service account key is needed. To create a service account key, take the following steps:

1. Select your new service account.
2. Click on the **Keys** tab.
3. Click the **Add key** drop-down list, and select **Create new key**.
4. Select **JSON** as the Key type, and click **Create**.

A file download will be created with service account data. This file is required for FortiSIEM configuration. Store a secure copy.

FortiSIEM Configuration

The following items are required for FortiSIEM integration.

- The subscription name created under the Pub/Sub topic: e.g. **projects/fortisiem-integration-1111/subscriptions/fortisiem-topic-sub**
 - Locate the subscription name by going to the topic you created, selecting subscriptions, and clicking on the subscription name.
Note: The subscription name will need to be entered into the Subscription Path field configuration for FortiSIEM.
- The Service Account JSON Key file.

Make sure you have completed these instructions if you do not have these items.

- [Google Cloud Platform Pub/Sub Setup](#)
- [FortiSIEM Service Account Setup](#)

To configure FortiSIEM, take the following steps:

1. Login to the FortiSIEM GUI.
Note: If this SIEM has multiple organizations, change the scope to the desired organization level for ingesting logs.
2. Navigate to **ADMIN > Setup > Credentials**.
3. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in “[Setting Credentials](#)” in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Google Google Cloud Platform
Access Protocol	GOOGLE_Pub_Sub
Pull Interval	5 minutes (leave at default)
Subscription Path	Enter the subscription name from Google Cloud Platform. Example: projects/fortisiem-integration-111/subscriptions/fortisiem-topic-sub
Service Account Key	Click Upload and upload the JSON Service Account Key.
Log Keyword	Leave the default value of “GCP_AUDIT_LOG”. Changing this will break the parser. This uniquely identifies that every log in this Pub/Sub topic is from Google Cloud Audit logging.
Description	(Optional) Description about the instance.

- c. Click **Save**.
4. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
Note: If your SIEM organization has multiple FortiSIEM collectors, be sure to select which collector will do the polling. A drop-down list will appear to the right of the **Test** button if you have multiple collectors. If you only have 1 collector, or in Super only environments, no collectors, no drop-down list will appear.
 - a. Select the name of your credential from the **Credentials** drop-down list.
 - b. The **IP/Host Name** field will auto populate with google.com. This is normal, do not change it.
 - c. Click **Save**.
5. To start polling, select the new mapping, click the **Test** drop-down list, and select **Test Connectivity without Ping**. It will take approximately 5 minutes for the initial poll job to kick off.
6. Once 5 minutes have passed, click **ANALYTICS**.
7. Click the **Edit Filters and Time Range...** field to run a query to see any Google Audit Logs.
 - a. Select **Event Attribute**.
 - b. Under **Attribute**, enter/select **Event Type**.

- c. Under **Operator**, select **CONTAIN**.
- d. Under **Value**, enter **GCP_AUDIT**.
- e. Click **Apply & Run** to execute.

Custom Log Integration

This integration is only needed if you are publishing custom logs to a Google Pub/Sub topic, and would like FortiSIEM to ingest those logs. Note that once the logs are ingested, you will still need to create a FortiSIEM parser for the log to be parsed and analyzed once ingested.

Log Flow: Custom logs from customer applications and systems -> Pub/Sub custom topic -> FortiSIEM ingest with custom log header appended

To integrate custom logs, take the following steps:

Note: In this process, the setup for a Pub/Sub topic is the same as normal integration, but instead of sinking GCP logs to the topic, you instead ingest your custom logs to the topic on your own.

1. Create a Pub/Sub topic.
2. Publish your custom logs to your topic. Your team will create a service account for your custom applications to send logs to this topic.
3. Create a service account with subscriber permissions to the topic for FortiSIEM. See [FortiSIEM Service Account Setup](#).
4. Configure FortiSIEM with service account credential and subscription name, and enter the custom log header format. This step follows the exact instructions in [FortiSIEM Configuration](#) except for the need to change **Log Keyword** in the **Access Method Definition** dialog box. See [Log Keyword Information](#) for more information.

Log Keyword Information

Log Keyword is a critical component for the parsing of logs. If you are ingesting custom logs, FortiSIEM will prepend the string to the log. This is supposed to be a unique identifier to know what the custom logs are for parsing.

Example:

We publish the log file {"attackName":"REvil Compromise","hostname":"host1"} into a Pub/Sub topic. This is a log from Custom Application A for our example.

When we set up the FortiSIEM integration, we'll do something to specify a log keyword to uniquely identify what type of logs these are.

When FortiSIEM ingests the log, it will appear in this format:

```
1 192.168.1.20 google.com CUSTOM_APP_A {"attackName":"REvil Compromise","hostname":"host1"}
```

This is important for log parsing, as we can write a parser that matches this log header, to process these logs. Any log in this Pub/Sub topic gets this header. This helps us write parsing in a simplified manner, as not all logs are cleanly structured and helps identify what or where the logs are from originally.

For custom log parsing, see the [NSE training documentation](#) on the topic, or consult [FortiCare Professional Services](#).

Google Workspace (Formerly G Suite and Google Apps)

FortiSIEM Support added: 4.8.1 (as Google Apps Audit)

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Google

Product: Workspace (Formerly G Suite / Google Apps)

Product Information: <https://workspace.google.com/>

Note: Older rules and reports use "Google Apps" to reference "Google Workspace".

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Dashboard](#)
- [Activity Auditing Collected Services](#)
- [Configuration](#)
- [Sample Events for Google Workspace Audit](#)

What is Discovered and Monitored

Protocol	Logs Collected	Used For
Google Apps Admin SDK	Account Create/Delete/Modify Account Group Create/Delete/Modify Configuration Change Device Compromise Document Create/Delete/Modify/Download Document Permission Change Logon Failure Logon Success	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Google_Apps" and "Google Workspace" in the **Search** field to see the event types associated with this device.

Rules

There are many rules defined in **RESOURCES > Rules**. Search for "Google Workspace" in the main content panel **Search...** field.

Some examples are provided:

- Google Workspace: 2FA Enforcement Disabled for Organization
- Google Workspace: 2FA Verification Disabled for Organization
- Google Workspace: API Access Permitted for OAUTH Client
- Google Workspace: Application Added to Domain
- Google Workspace: Domain added to Trusted Domains List
- Google Workspace: Password Management Policy Changed
- Google Workspace: Role Assigned to User
- Google Workspace: Role Created by User
- Google Workspace: Role Deleted by User
- Google Workspace: Role Modified by User
- Uncommon GSuite Login

Reports

There are many reports defined in **RESOURCES > Reports > Device > Application > Document Mgmt.** Search for "Google Apps" and "Google Workspace" in the main content panel **Search...** field.

Some examples are provided:

- Google Workspace: Top Event Types by Count
- Google Workspace: Top Events by User
- Google Workspace: Top Events by Source IP
- Google Workspace: Top Events by Source Country
- Google Workspace: Password Management Policy Changed Audit Report
- Top GSuite Login

Dashboard

A standard Google Apps Dashboard can be found by navigating to **DASHBOARD**, and selecting **Google Apps Dashboard** from the Dashboard drop-down list.

Activity Auditing Collected Services

The following services have Activity Auditing collected:

- Access Transparency
- Admin

- Chrome
- Context-Aware Access
- Currents
- Data Studio
- Enterprise Groups
- Google Calendar
- Google Chat
- Google Cloud Platform
- Google Drive
- Google Groups
- Google Keep
- Google Meet
- Jamboard
- Login
- Mobile
- OAuth Token
- Rules
- SAML
- User Accounts

Configuration

- [Google Workspace API Setup](#)
- [Configure FortiSIEM](#)

Google Workspace API Setup

FortiSIEM Supports Querying Google Workspace (formerly Gsuite) APIs to monitor activity in the organization.

Prerequisites

Ensure you are or have an admin of your Google Workspace environment available.

Step 1: Create a Project in Google Cloud Console

To use Cloud APIs, a Google project is required. A project is equivalent to a developer account. It serves as a resource container for your Google Cloud resources. It also provides an isolation boundary for your usage of Google Cloud services, so you can manage quota limits and billing independently at the project level.

Reference: <https://developers.google.com/workspace/guides/create-project>

1. Navigate to <https://console.cloud.google.com/>
The following should appear: "You're working in <domain> > My First Project"
2. On the top left of the screen next to the Google Cloud logo, click "My First Project" > New Project if you want to create a new project for this specific configuration, then take the following steps:

- a. In the **Project Name** field, enter a project name, such as "FortiSIEM".
 - b. If you have more than one organization, for Organization, select the appropriate organization.
 - c. In the **Location** field, click **Browse** to update, and click **Select** when one is chosen, or leave as default.
Note: Typically the Parent Org <domain> or your specific sub org appears as default.
 - d. When done, click **Create**.
3. Before proceeding, ensure your Project is selected on top left of screen.

Step 2: Enable Required APIs for Your Project

Some Cloud APIs are enabled by default. To use a Cloud API that is not enabled by default, you must enable it for your project. Depending on which services and which projects are involved from your application, including the client project and resource projects, you may need to enable an API for multiple projects. When you enable an API that depends on other APIs, those APIs are also enabled at the same time.

FortiSIEM currently only needs the following APIs at this time:

- Admin SDK API

To enable an API for a project using the console:

1. Go to the Google Cloud console API Library: https://console.cloud.google.com/apis/library?project=_
2. From the projects list, select the project you want to enable APIs for.
3. In the API Library page, select the API you want to enable.
4. Under the "Google Workspace" category of APIs, select **Admin SDK API**.
5. On the API page, click **Enable**.

Step 3: Enable Billing (Optional - For other APIs)

Some Cloud APIs charge for usage. You must enable billing for your project before you can start using these specific APIs in your project. The API usage in a project is charged to the billing account associated with the project.

Step 4: Create a Service Account

Reference: <https://developers.google.com/workspace/guides/create-credentials>

The service account will have a limited API scope, but will be capable of impersonating any user in your domain using domain wide delegation.

1. Login to <https://console.cloud.google.com/>
2. From the left pane, select **API & Services > Credentials**.
Note: You can use the search bar, and enter "APIs & Services" to locate this page.
3. Ensure your project is selected.
4. Click **APIs & Services** and then **Credentials**.
Note: You might have to click **Menu** first.
5. Click **Create Credentials**.
 - a. From the drop-down, select **Service account**.
 - b. In the **Service account name** field, enter a name such as "FortiSIEM".
 - c. (Optional) In the **Service account description** field, enter a description of the service account.

- d. Click **Create and Continue**.
 - e. Under **Step 2** - Grant this service account access to project, select Role: Viewer
 - f. Under **Step 3** - Grant users access to this service account, skip as this is optional.
 - g. Click **Done**.
6. Generate a key for the service account by taking the following steps.
 - a. Select the service account you created, and click the Edit (pencil) icon on the far right.
 - b. Select the **Keys** tab > **Add Key** > **Create New Key**.
 - c. For **Key Type**, select **JSON**.

You will get a message that the service account's private key JSON file was downloaded to your computer. Make a note of the file name and where your browser saved it. By default, the downloaded credential should be located in your downloads folder. This will be needed for the FortiSIEM configuration shortly.
7. Find the Client ID for the generated credential by taking the following steps.
 - a. Refresh the page on the **Keys** tab under this service account.
 - b. The key status should now appear as active. There should be a long identifier (the Client ID) such as 227b19d71c4cb88cdxxxxxxc65d0c5c. Copy this Client ID as it will be needed later.
8. Click **Close**.

Step 5: Enable Domain Wide Delegation for your Service Account

Your service account cannot directly access the API until it impersonates a licensed user in your Google Workspace domain. This can be any domain admin. Since the scope of what APIs the service account can access is limited, security can be locked down to minimal requirements.

Prerequisites

You need the "Client ID" of the service account's credential you created earlier

1. Login to <https://admin.google.com/>
2. Go to **Security > Access and Data Controls > API controls > Manage Domain Wide Delegation**.
3. Under **API clients**, click **Add New**.

A popup will appear prompting for the following:

Client ID: Enter/paste this from the downloaded JSON credential saved earlier (and also appears in the Google console for service accounts).

OAuth Scopes: Enter "https://www.googleapis.com/auth/admin.reports.audit.readonly"
4. Click **Authorize**.

Configure FortiSIEM

Step 1: Create the Credential

1. Login to the FortiSIEM GUI.
2. Navigate to **Admin > Setup**.
3. Click the **Credentials** tab.
4. Under **Step 1: Enter Credentials**, click **New** to create a new credential.

- a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential. Enter/select these settings in the Access Method Definition dialog box and click **Save** when done:

Settings	Description
Name	GoogleWorkspace
Device Type	Google Google Apps
Access Protocol	Google Apps Admin SDK
Account Name	someDomainAdmin@yourdomain.com Note: This is any licensed domain admin user in Google Workspace that the service account will impersonate. You must select one to impersonate, it does not matter which account. It can be any Google Workspace domain admin user, since Auth Scopes limit to read only, permissions are limited on what the service account can do. This is not the service accounts email address, as it must impersonate a licensed user to access Admin Reports.
Service Account Key	Upload the JSON credential for the service account that you downloaded earlier.
Organization	(Optional for MSSP FortiSIEM versions in Global View). Select the FortiSIEM organization this applies to. Note: Enterprise users will not see this option.
Description	Description of the function, example: Google Workspace Monitoring.

Step 2: Create the Credential Association

Under **Step 2: Enter IP Range to Credential Associations**, take the following steps.

1. Select the collector that will make the API calls from the drop-down.
Note: If you have only 1 collector for an organization, or no collectors, this drop-down does not exist.
2. Click **New** to create a mapping.
 - a. From the **Credentials** drop-down list, select the Google Workspace credential.
 - b. The **IP/Host Name** field should auto-populate with "google.com".
 - c. Click **Save**.

Step 3: Start the Event Pulling Job

Select the Credential Association entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. This will start an event pulling job.

Step 4: Check Event Pulling Job Status

Navigate to **Admin > Setup**, and click the **Pull Events** tab.

You will see a job added for Google Workspace. Under the **Method** column, if a Yellow Star appears, it means the job is pending first execution. Wait about 5 minutes and you should see a Green Checkmark indicating the first job has kicked off.

Step 5: Check for Events

1. Navigate to **Analytics**, and select **Search** tab, if not already selected.
2. Click inside the **Edit Filters and Time Range...** search field.
3. From the **Filter By** window, take the following steps to create the following query: Event Type CONTAIN "Google_Apps"
 - a. Make sure the **Event Attribute** tab is selected.
 - b. In the **attribute...** field, select/enter **Event Type**.
 - c. From the **Operator** drop-down list, select **CONTAIN**.
 - d. In the **value...** field, enter **Google_Apps**.
 - e. Click **Apply & Run**.
 Event types with "Google_Apps" will start to appear.

Sample Events for Google Workspace Audit

- Logon Success
- Logon Failure
- Create User
- Delete User
- Move User Settings

Logon Success

```
<134>Jan 21 19:29:21 google.com java: [Google_Apps_login_login_success]:[eventSeverity]=PHL_INFO,
[actor.profileId]=117858279951236905887,[id.time]=2016-09-09T06:53:58.000Z,
[id.applicationName]=login,[kind]=admin#reports#activity,[id.customerId]=C01lzy8ye,
[id.uniqueQualifier]=8830301951515521023,[event.parameters.login_type]=google_password,
[event.type]=login,[ipAddress]=192.0.2.103,[actor.email]=api1@example.net,[event.name]=login_
success,[etag]=""6KGrH_UY2JDZNpgjPKUOF8yJF1A/Nfmg2SFjlC2gR6pJtpP2scVidmc"",Google_Apps_login_
login_success,login_success,1,192.0.2.103,
```

Logon Failure

```
<134>Jan 21 19:29:21 google.com java: [Google_Apps_login_login_failure]:
[eventSeverity]=PHL_INFO,[actor.profileId]=117858279951236905887,
[id.applicationName]=login,[kind]=admin#reports#activity,[event.parameters.login_
type]=google_password,[ipAddress]=192.0.2.103,[event.name]=login_failure,[id.time]=2016-
09-19T09:27:51.000Z,[id.customerId]=C01lzy8ye,[id.uniqueQualifier]=4795688196368428241,
[event.type]=login,[actor.email]=api1@example.net,[etag]=""6KGrH_
UY2JDZNpgjPKUOF8yJF1A/v5zsUPNoEdXLLK79zQpBcuxNbQU"",[event.parameters.login_failure_
type]=login_failure_invalid_password",Google_Apps_login_login_failure,login_
failure,1,192.0.2.103,
```

Create User

```
<134>Jan 21 19:29:20 google.com java: [Google_Apps_USER_SETTINGS_CREATE_USER]:
[eventSeverity]=PHL_INFO,[actor.callerType]=USER,[actor.profileId]=117858279951236905887,
[id.applicationName]=admin,[kind]=admin#reports#activity,[ipAddress]=192.0.2.103,
[event.name]=CREATE_USER,[id.time]=2016-09-19T09:22:44.646Z,[id.customerId]=C01lzy8ye,
[id.uniqueQualifier]=-8133102622954793216,[event.type]=USER_SETTINGS,
[event.parameters.USER_EMAIL]=test-user@example.org,[actor.email]=api1@example.net,
[etag]=""6KGrH_UY2JDZNpgjPKUOF8yJF1A/R5GJyWG9YHSiGRvo3-8ZBM0Z1L0"",Google_Apps_USER_
SETTINGS_CREATE_USER,CREATE_USER,1,192.0.2.103,
```

Delete User

```
<134>Jan 21 19:29:20 google.com java: [Google_Apps_USER_SETTINGS_DELETE_USER]:[eventSeverity]=PHL_
INFO,[actor.callerType]=USER,[actor.profileId]=117858279951236905887,[id.applicationName]=admin,
[kind]=admin#reports#activity,[ipAddress]=192.0.2.103,[event.name]=DELETE_USER,[id.time]=2016-09-
19T09:22:28.582Z,[id.customerId]=C01lzy8ye,[id.uniqueQualifier]=-4630441819990099585,
[event.type]=USER_SETTINGS,[event.parameters.USER_EMAIL]=test-user@example.org,
[actor.email]=api1@example.net,[etag]=""6KGrH_
UY2JDZNpgjPKUOF8yJF1A/08MaodxPU6Zv7s6vJtuUQW9ugx0"",Google_Apps_USER_SETTINGS_DELETE_USER,DELETE_
USER,1,192.0.2.103,
```

Move User Settings

```
<134>Jan 21 19:29:20 google.com java: [Google_Apps_USER_SETTINGS_MOVE_USER_TO_ORG_UNIT]:
[eventSeverity]=PHL_INFO,[actor.callerType]=USER,[actor.profileId]=117858279951236905887,
[event.parameters.ORG_UNIT_NAME]=/test,[id.applicationName]=admin,[kind]=admin#reports#activity,
[ipAddress]=192.0.2.103,[event.name]=MOVE_USER_TO_ORG_UNIT,[id.time]=2016-09-19T09:24:25.285Z,
[id.customerId]=C01lzy8ye,[id.uniqueQualifier]=-6704816947489240452,[event.type]=USER_SETTINGS,
[event.parameters.USER_EMAIL]=test-user@example.org,[actor.email]=api1@example.net,
[event.parameters.NEW_VALUE]=/, [etag]=""6KGrH_
UY2JDZNpgjPKUOF8yJF1A/r1v9DiPZbL06fXFFjJlRwf2s3qI"",Google_Apps_USER_SETTINGS_MOVE_USER_TO_ORG_
UNIT,MOVE_USER_TO_ORG_UNIT,1,192.0.2.103,,
```


Microsoft Azure Audit

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Events for Microsoft Azure Audit](#)

What is Discovered and Monitored

Protocol	Information Discovered	Information Collected	Used For
Azure CLI	None	Audit Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Azure Audit" in the **Search** field to see the event types associated with this device.

Configuration

- [Configuration in Azure](#)
- [Configuration in FortiSIEM](#)

Configuration in Azure

You must define a user account in Azure for use by FortiSIEM to pull Audit logs. Use any of the following roles:

- Owner
- Reader
- Monitoring Reader
- Monitoring Contributor
- Contributor

Notes:

- These roles are only defined at the subscription level, and are not visible under the Users tab in Entra ID (Formerly Azure AD).
- FortiSIEM recommends using the 'Monitoring Reader' role, which is the least privileged to do the job.

Take the following steps to create and assign a role.

1. Login to the [Azure portal](#).
2. Navigate to **Home > Subscriptions > Access control (IAM)**.

3. Click on **Add role assignment**.
4. Search for, and apply Monitoring Reader or Monitoring Contributor.

For more information on roles, see:

<https://docs.microsoft.com/en-us/azure/azure-monitor/roles-permissions-security>

and

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current>

Configuration in FortiSIEM

Take the following steps for configuration.

- [Create Microsoft Azure Audit Credential in FortiSIEM](#)
- [Create IP Range to Credential Association and Test Connectivity in FortiSIEM](#)

Create Microsoft Azure Audit Credential in FortiSIEM

Complete these steps in the FortiSIEM UI after logging into the FortiSIEM supervisor node:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Azure Audit
Access Protocol	Azure CLI
Password Config	Choose Manual, CyberArk, or RAX_MSCloud from the drop down list. For Manual credential method, enter the username and credentials for an Azure account. FortiSIEM recommends using 'Monitoring Reader' role for this account. For CyberArk or RAX_MSCloud, see Password Configuration .
Azure Subscription ID	Enter the 32-digit GUID associated with your Azure subscription. In 6.3.0, to enter multiple subscription IDs, separate each ID by a space. Examples: Entering one subscription ID: a0123bcd-e456-6f78-9112-gh3i4j56k789

Settings	Description
	Entering two subscription IDs: a0123bcd-e456-6f78-9112-gh3i4j56k789 z9876yxv-u543-2t10-9876-sr5q4p32o109
Account Env	In 6.3.0, you can choose AzureCloud , AzureChinaCloud , AzureGermanCloud , or AzureUSGovernmentCloud . Selecting AzureUSGovernmentCloud applies a GCC High environment. Note: Prior to 6.3.0, the Azure CLI Agent only supported Global Azure, and did not support Azure China Cloud, Azure German Cloud, nor Azure US Government Cloud.
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity in FortiSIEM

When logged in to the FortiSIEM Supervisor node, take the following steps.

1. Go to **ADMIN > Setup > Credentials**.
2. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. From the **Credentials** drop-down list, select the name of the credential created in the "[Create Microsoft Azure Audit Credential](#)" step.
The **IP/Host Name** field will auto populate to azure.com
 - b. Click **Save**.
3. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection.
4. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Microsoft Audit Log Collection.

Sample Events for Microsoft Azure Audit

```
2016-02-26 15:19:10 FortiSIEM-Azure,
[action]=Microsoft.ClassicCompute/virtualmachines/shutdown/action,[caller]=Doe.John@example.com,
[level]=Error,[resourceId]=/subscriptions/3ed4ee1c-1a83-4e02-a928-7ff5e0008e8a/resourcegroups/china/providers/Microsoft.ClassicCompute/virtualmachines/china,
[resourceGroupName]=china,[eventTimestamp]=2016-02-14T06:12:18.5539709Z,[status]=Failed,
[subStatus]=Conflict,[resourceType]=Microsoft.ClassicCompute/virtualmachines,
[category]=Administrative
```

Microsoft Azure Compute

- [Configuration](#)

The purpose of this integration is to discover Virtual Machines (VMs) running in Azure. It does not collect events or performance statistics. Many Azure specific reports rely on properly categorizing which VMs exist in Azure Cloud. Please follow the appropriate integration guide for each instance in Azure you would like to ingest logs and monitor.

Configuration

- [Setup in Azure](#)
- [Setup in FortiSIEM](#)

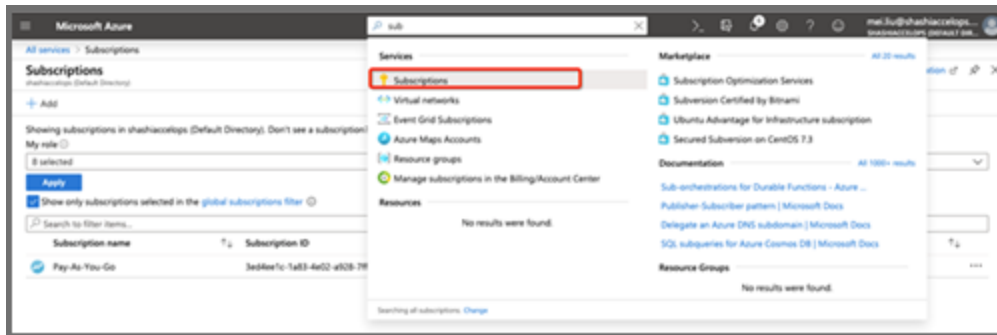
Setup in Azure

1. Log in to the Azure Portal
2. Create an Azure Active Directory application
 - Sign in to your Azure Account through the Azure portal.
 - Select **Azure Active Directory**.
 - Select **App registrations**.
 - Select **New registration**.

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The breadcrumb trail is 'All services > shashiaccelops (Default Directory) > App registrations > Register an application'. The page title is 'Register an application'. The 'Name' field is required and contains 'discover-by-Azure-Resource-SDK' with a green checkmark. Below it, the 'Supported account types' section asks 'Who can use this application or access this API?' and has three radio button options: 'Accounts in this organizational directory only (shashiaccelops (Default Directory) only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', and 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)'. There is a 'Help me choose...' link. The 'Redirect URI (optional)' section explains that it's for returning authentication responses and has a dropdown set to 'Web' and a text box containing 'https://myapp.com/auth'. At the bottom, there is a link to 'Microsoft Platform Policies' and a blue 'Register' button.

3. Assign the application to a role:

- Select **Subscriptions** on the Home page.

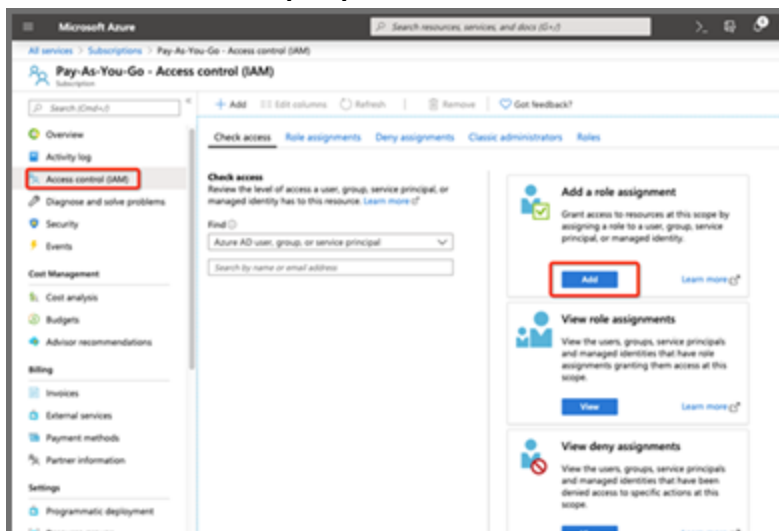


- Select the particular subscription to assign your application to. In here, it uses Pay-As-You-GO as the example.

Click Pay-AS-You-GO to open it. Save the **Subscription ID** for FortiSIEM credential.

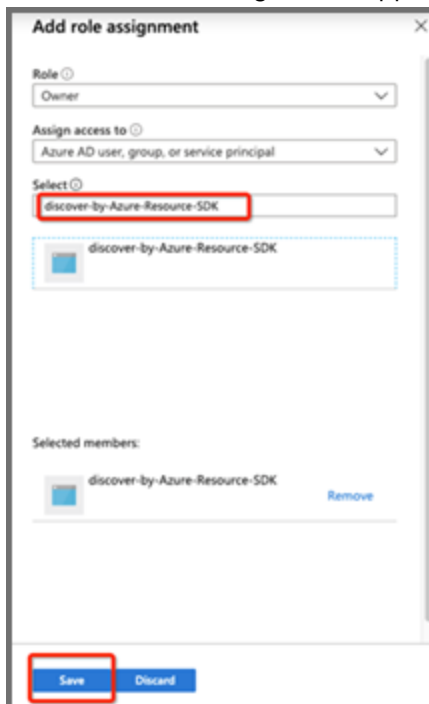


- Copy the **Subscription ID**, it will be needed when defining the credential in FortiSIEM.
- Select **Access control (IAM)**.



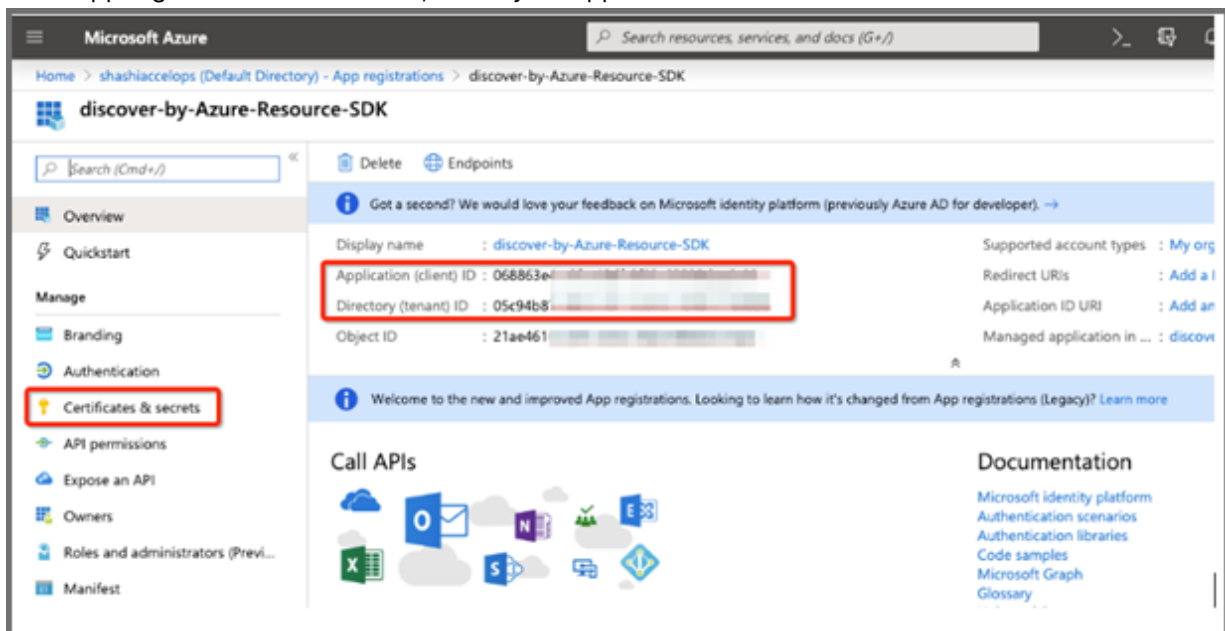
- Select **Add role assignment**.

- Select **Owner** to assign to the application and select the app that you created. And then click **Save**.



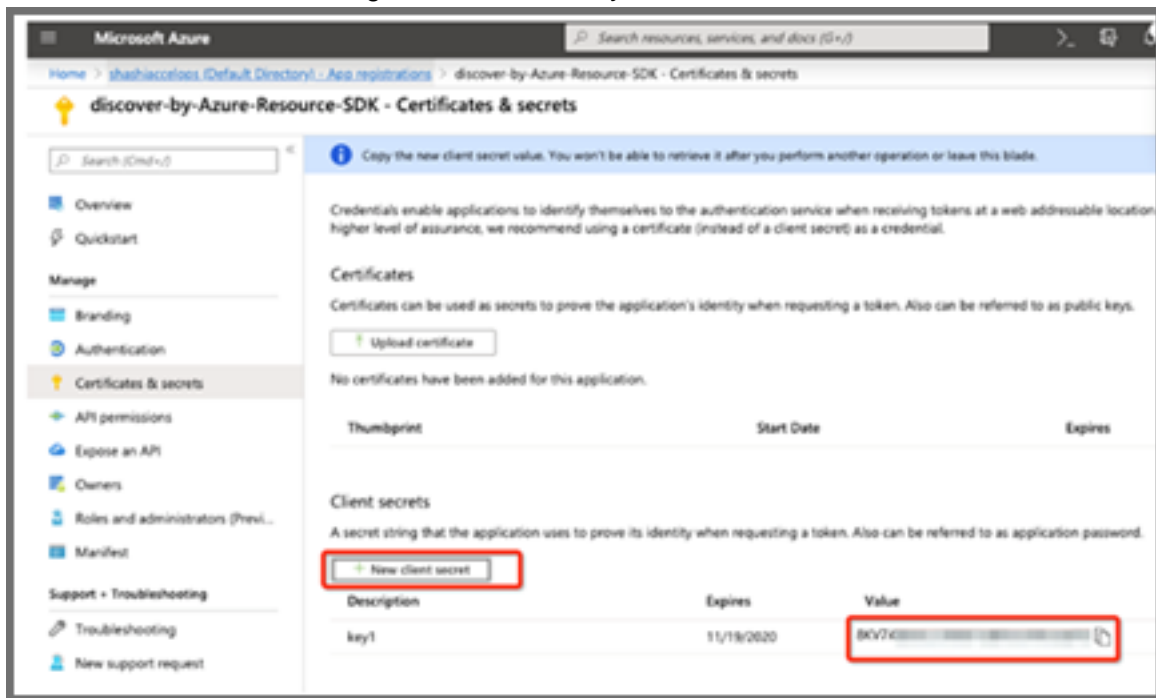
4. Get value for FortiSIEM credential

- Select **Azure Active Directory**.
- From App registrations in Azure AD, select your application.



- Copy the **Application (client) ID** and **Directory (tenant) ID**, it will be needed when defining the credential in FortiSIEM.

- Select Certificate & secrets to generate a secret key.



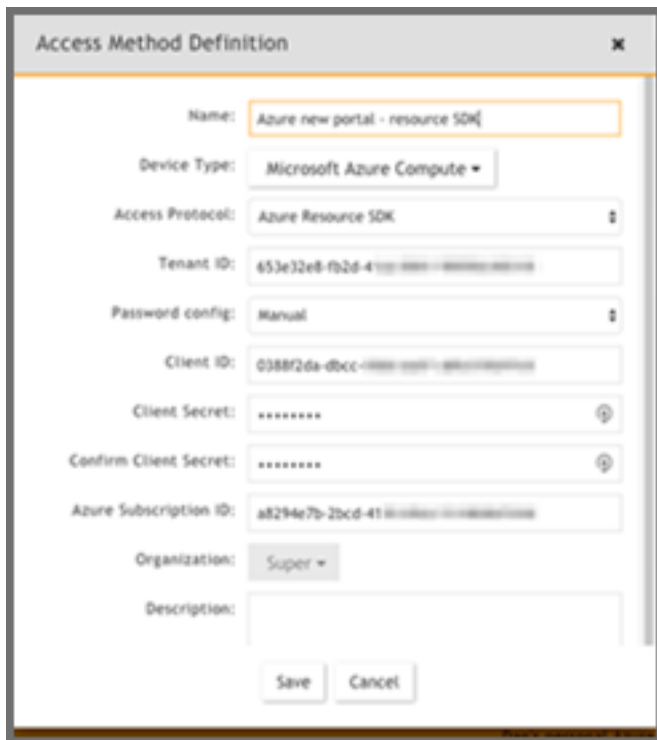
5. Test

- Command:
`/opt/phoenix/bin/getAzureResourceVM.py {subscriptionId} {tenantId} {clientId} {client secret}.`
- Example:
`/opt/phoenix/bin/getAzureResourceVM.py 7327432-1a83-4e02-a928-9032489032898a 05c94b87-da0c-4e11-be1d-789234789432 068863e4-c2fa-48df-8f33-79823478932 jh23hjkb324ugih32hujdsdsvqeP]]'`

Setup in FortiSIEM

Follow these steps in the FortiSIEM UI:

1. Create a new credential. Make sure to select **Azure Resource SDK** as the **Access Protocol**.

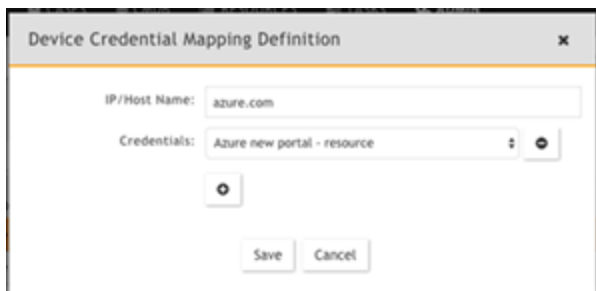


The **Access Method Definition** dialog box is used to configure a new access method. It contains the following fields:

- Name:** Azure new portal - resource SDK
- Device Type:** Microsoft Azure Compute
- Access Protocol:** Azure Resource SDK
- Tenant ID:** 653e32e8-fb2d-4100-8000-000000000000
- Password config:** Manual
- Client ID:** 0388f2da-dbcc-4000-8000-000000000000
- Client Secret:** (masked with asterisks)
- Confirm Client Secret:** (masked with asterisks)
- Azure Subscription ID:** a8294e7b-2bcd-4100-8000-000000000000
- Organization:** Super
- Description:** (empty)

Buttons: Save, Cancel

2. Define a credential.

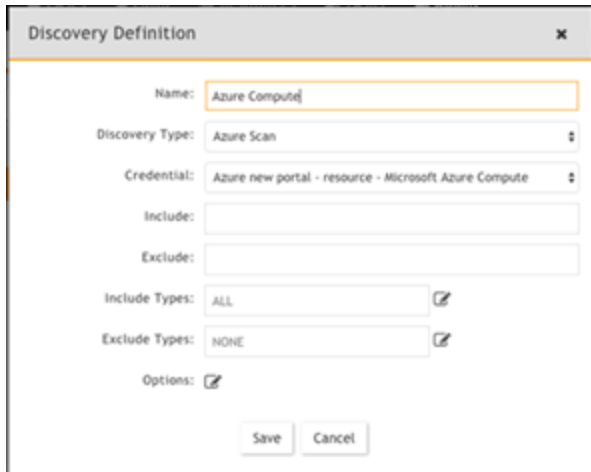


The **Device Credential Mapping Definition** dialog box is used to map a credential to a device. It contains the following fields:

- IP/Host Name:** azure.com
- Credentials:** Azure new portal - resource

Buttons: Save, Cancel

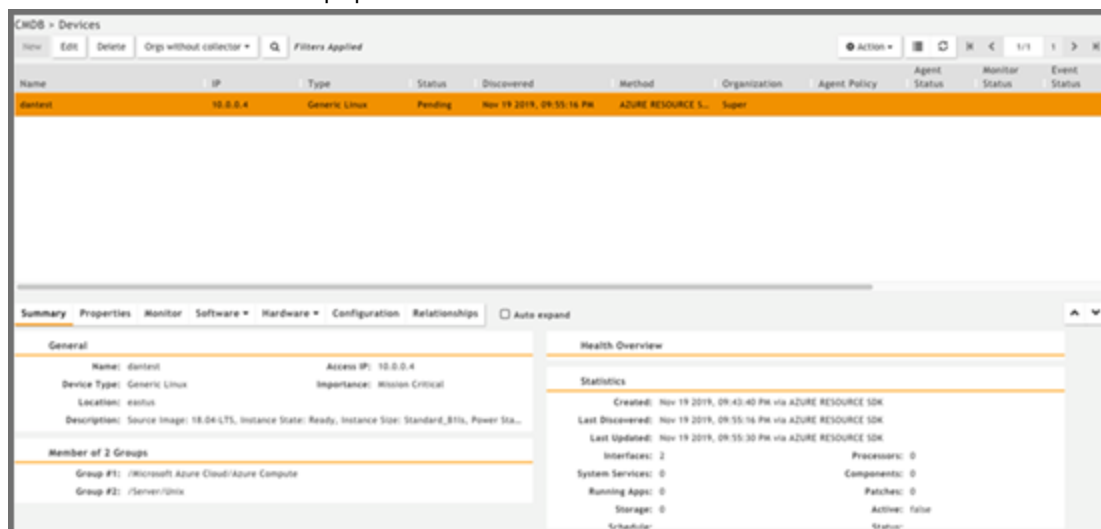
3. Create a **Discovery Definition**.



The **Discovery Definition** dialog box is used to define a discovery method. It contains the following fields:

- Name:** Azure Compute
- Discovery Type:** Azure Scan
- Credential:** Azure new portal - resource - Microsoft Azure Compute
- Include:** (empty)
- Exclude:** (empty)
- Include Types:** ALL
- Exclude Types:** NONE
- Options:** (checked)

Buttons: Save, Cancel

4. The CMDB should then be populated.

Microsoft Azure Event Hub

Support Added: FortiSIEM 5.2.5

Last Modification: FortiSIEM 7.3.2

Vendor: Microsoft

Product Information: <https://azure.microsoft.com/en-us/products/event-hubs>

Event Hubs is a fully managed, real-time data ingestion service that is simple, trusted, and scalable. Stream millions of events per second from any source to build dynamic data pipelines and immediately respond to business challenges.

Overview

1. Create an Azure Event Hub (only 1 Event Hub is needed for all log forwarding, although multiple hubs can be configured for different event sources).
2. Configure various Microsoft cloud services to forward audit logs to this Azure Event Hub.
3. Configure FortiSIEM to ingest events from the created Event Hub.

This document covers the following topics.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Rules](#)
- [Configuration in Azure](#)
- [Configuration in FortiSIEM](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Information Collected	Used For
Azure Python SDK	None	Audit Logs	Security Monitoring

- Microsoft Entra ID (Formerly Azure AD) Audit Logs
- Microsoft Azure Monitor Events
- Microsoft Defender XDR (formerly MS365 Defender)
- Any other Microsoft Cloud service that supports forwarding events to Azure Event Hubs
- Custom applications events sent to the ingested Event Hub

Event Types

In **Admin > Device Support > Event Types**, search for "azure-" and "evt-hub" to see the event types associated with this integration.

Reports

In **Resources > Reports**, search for "azure" to see reports associated with this integration.

Rules

In **Resources > Rules**, search for "azure" to see rules associated with this integration.

Configuration in Azure

Create an Event Hub Namespace and Event Hub

Complete these steps in the Azure Portal.

Step 1: Create a Resource Group in Azure

A resource group is a logical collection of Azure resources. All resources are deployed and managed in a resource group.

Note: If you already have a resource group where you would like this event hub to reside, you can skip this step.

To create a resource group:

1. Login to the Azure portal: <https://portal.azure.com/>
2. Click **Resource groups** in the left navigation pane.
3. Click **Add**.
4. For **Subscription**, select the name of the Azure subscription in which you want to create the resource group.
5. Enter a unique name for the resource group, The system immediately checks to see if the name is available in the currently selected Azure subscription.
6. Select a **Region** for the resource group.
7. Click **Review + Create**.
8. Click **Create** on the **Review + Create** page.

Note: In the example used in step 2, a **Resource Group** called fsm1 was created.

Step 2: Create an Event Hub Namespace

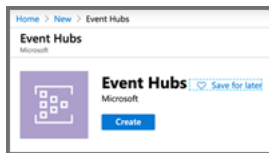
An Event Hub namespace provides a unique scoping container, referenced by its fully-qualified domain name, in which you create one or more event hubs. To create a namespace in your resource group using the portal, complete the following steps:

1. In the Azure portal, click **Create a resource** at the top left of the screen. If you do not see this option, you can search for "Event Hubs" at the top of the page.

Azure services



2. In the **Search the Market** text box, enter **Select All services** in the left menu, select star (*) next to **Event Hubs**, and then click the **Create** button in the **ANALYTICS** category.



3. On the **Create namespace** page, complete the following steps:
 - a. Enter a name for the namespace. The system immediately checks to see if the name is available.
 - b. Choose the pricing tier (**Basic** or **Standard**). **Standard** is recommended for options like auto inflate (performance auto scaling for the event hub)



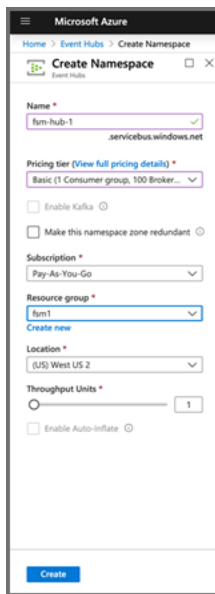
Note: The default behavior of event hubs is that they are created as public endpoints. For standard and premium tier event hubs, you have the option to create private endpoints. While outside of the scope of this document, should you decide to set up a FortiSIEM collector in a private subnet in Azure, you can set up a private endpoint for the endpoint not exposed to the public internet. This is provided your FortiSIEM collector has network reachability to the private Azure endpoint should you go this route.

- c. Select the billing subscription in which you want to create the namespace.
- d. Select a region location for the namespace. Ideally, this is geographically closest to the FortiSIEM collector completing the polling.
- e. Select the number of throughput units - default 1. This determines the size of the event hub backing infrastructure, and should be scaled based on the volume of logs ingested. You can view this at any time in the Event Hub stats page later.

Note: You can scale this up later at any time.
- f. **Enable Auto Inflate:** Check this box to have the event hub auto scale as performance needs require up to a configured limit.

Set to 10: This option is only available to **Standard** Tier or higher (not **Basic**) Event Hubs.
- g. Leave other options as default.

- h. Click **Create**. You may have to wait a few minutes for the system to fully provision the resources.

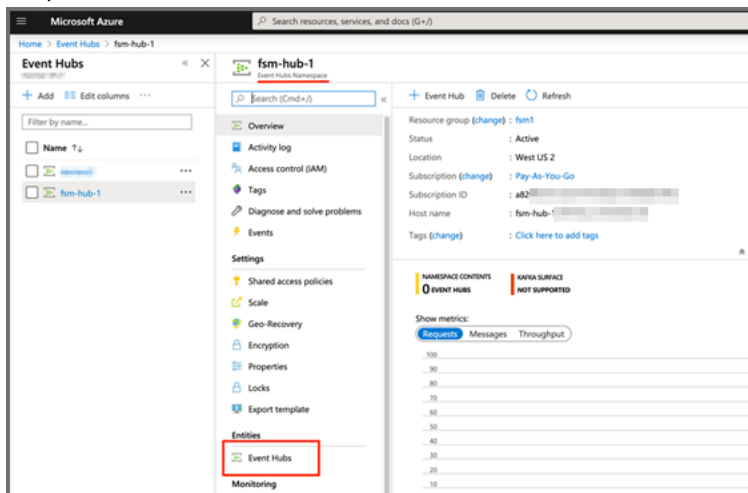


4. Refresh the **Event Hubs** page to see the event hub namespace. You can check the status of the event hub creation in the alerts.
5. Select the namespace. You will see the home page for your **Event Hubs Namespace** in the portal.

Step 3: Create an Event Hub

To create an event hub within the namespace, follow these steps:

1. In the **Event Hubs Namespace** page, click **Event Hubs** in the left menu. This is found under the "Entities" drop-down > **Event Hubs**.

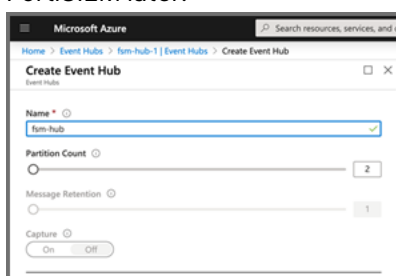


2. At the top of the window, click **+ Event Hub**.
3. **Enter a Name:** Provide a name, such as "fsm-eventhub".
4. **Partition count:** This defaults to 1, which equates to about 1MB/s of logs.



Note: The rule of thumb for calculating the number of partitions would be to divide the maximum expected throughput by 1 MB/s. For example, if your use case requires 20 MB/s, Fortinet recommends that you choose at least 20 partitions to achieve the optimal throughput. Many times, you won't know this until you initially set up. **In most cases, you can set this value to 5, but if you need more, you'll have to re-create an event hub in this namespace with a larger partition count. You can do this at any time.**

5. **Retention:** This option specifies how long data is retained in the event hub before it is purged. This data only needs to be retained until FortiSIEM can poll it, so it is advisable to set this to the lowest option, such as 1-2 days. For this example configuration, it will be set to 24 hours.
6. **Cleanup policy:** Delete
7. **Retention Time:** 24 (hours)
8. Click **Create**. It may take a few minutes to create. You'll need the event hub name when configuring FortiSIEM later.



9. You can check the status of the event hub creation in alerts. After the event hub is created, you will see it in the list of event hubs.

Step 4: Configure an Event Hub Namespace Shared Access Policy

FortiSIEM needs an API Key to access the event hub. Take the following steps to create it.

1. Select an event hub namespace and go to **Shared access policies**, and then click **+ Add**.
2. Enter the **Policy name**, such as "FSMAccess". You will need this later for FortiSIEM configuration.
3. **Permission** checkbox: Check the **Listen** box, and then click **Create**.

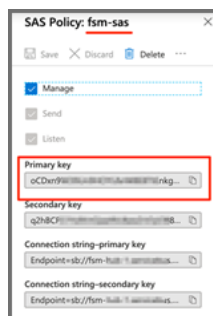


Step 5: Obtain the FSMAccess SAS Policy Primary Key

From the Shared Access Policy, get the Primary key.

1. Select the **Shared Access** policy you just created and a popup on right side will display the **"Primary key"**. Copy this value.

Note: When the event hub namespace is created, Azure will also create a default Shared Access Policy named **RootManageSharedAccessKey**. That is normal.



Step 6: Define an Event Hub Consumer Group

1. Select the event hub created earlier, and select the "consumer group" option.

Note: You can click **+Consumer group** or use default group name **\$default**.

2. Go to the new EventHub and click **Entities > Consumer Groups**.
3. Click create consumer group.
 - a. **Name:** Enter a name, such as "fsmgroup".
 - b. **Location:** Select your region

Note: If you have selected **Basic (1 Consumer Group)**, then there will be no option to add a another consumer group. You will use the "\$default" consumer group in your configuration.

Configuration in FortiSIEM

FortiSIEM needs the following items from your prior setup of an Azure Event Hub:

- **Event Hub Namespace Name:** e.g. "companyname-fsm-eventhub-ns"
 - Use the short name, not the FQDN.
- **Event Hub Name:** Enter the hub name as seen under the created namespace created earlier.
- **SAS Policy Name:** This is the policy you created earlier, e.g. FSMAccess.
- **Primary Key:** The API key generated from the SAS policy created earlier.
- **Consumer Group Name:** If you create a custom consumer group (recommended) for the event hub, enter its name here. If you did not, use the \$default consumer group.
- **Account Env:** This is information about your Azure Tenant. In most cases, you can leave this default "AzureCloud", meaning the Azure Enterprise public cloud. If you are a government customer, you can select the appropriate cloud which has different endpoints.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Azure Event Hub
Access Protocol	AZURE PYTHON SDK
Pull Interval	The interval in which FortiSIEM will pull events from Azure Event Hub. Default is 5 minutes.
Event Hub Name Space	The name of the Azure event hub namespace
Event Hub Name	The name of the Azure event hub
SAS Policy Name	Shared Access (SAS) Policy Name
Primary Key	The primary key value (API key)
Account Env	In most cases, you can leave this default "AzureCloud", meaning the Azure Enterprise public cloud. If you are a government customer, you can select the appropriate cloud which has different endpoints.
Consumer Group	The name of the consumer group
Description	Description of the device

Based on the example screenshots, this is the configuration in FortiSIEM:

Access Method Definition

Name:

FSM Azure Hub

Device Type:

Microsoft Azure Event Hub ▾

Access Protocol:

AZURE PYTHON SDK ▾

Pull Interval:

5

Minute(s)

Event Hub Name Space:

fsm-hub-1

Event Hub Name:

fsm-hub

SAS Policy Name:

fsm-sas

Primary Key

.....

Confirm Primary Key

.....

Account Env:

AzureCloud

Consumer Groups:

Sdefault

Organization:

Super ▾

Description:

Save

Cancel

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.

- Enter a host name, an IP, or an IP range in the **IP/Host Name** field. For this integration, **leave the default of "azure.com"**. FortiSIEM internal integration handles making the correct API call. This is just a placeholder.
- Select the credential name of your Azure event hub credential from the **Credentials** drop-down list.

- c. Click **Save**.

4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Azure event hub.

5. To see the jobs associated with Azure, select **Admin > Setup > Pull Events**.

6. To see the received events select **Analytics**, then enter "Azure" in the search box.

Note: Azure services must be configured to write to the Event Hub before there are any events to be collected.

Next, we'll set up various Microsoft Cloud Services to send events to this event hub.

Set up Azure Entra ID Audit Log Forwarding to Azure Event Hub

Prerequisites:

- You have previously followed all prior instructions in this guide to create an Azure Event Hub and configured FortiSIEM to pull from this event hub.
1. Login to Azure Portal.
 2. Search for "Microsoft Entra ID".
 3. On the left hand toolbar, towards the bottom, locate the **Monitoring** section > **Diagnostic settings**.
 - a. Click **Add diagnostic setting**.
 - b. **Diagnostic setting name:** Enter a name for the diagnostic setting, such as "FortiSIEM-Forwarding".
 - c. **Logs:** Configure as needed. For example, select all options, or to omit certain logs, leave those unchecked.
 - d. Under **Destination details:**
 - Check the **Stream to an event hub** checkbox.
 - From the **Subscription** drop-down, select the subscription we created the event hub under.
 - From the **Event hub namespace** drop-down, select your event hub namespace.
 - From the **Event hub name** drop-down, select the target event hub.
 - From the Event hub policy name drop-down, select the event hub policy name (default is RootManageSharedAccessKey).
 - e. Click **Save**.

Home > Fortinet AzureStore | Diagnostic settings > Diagnostic settings | General >

Diagnostic setting ...

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name * FortiSIEM-forwarding ✓

Logs

Categories

- ☒ AuditLogs
- ☒ SignInLogs
- ☒ NonInteractiveUserSignInLogs
- ☒ ServicePrincipalSignInLogs
- ☒ ManagedIdentitySignInLogs
- ☒ ProvisioningLogs
- ☒ ADFSSignInLogs
- ☒ RiskyUsers
- ☒ UserRiskEvents
- ☒ NetworkAccessTrafficLogs
- ☒ RiskyServicePrincipals
- ☒ ServicePrincipalRiskEvents
- ☒ EnrichedOffice365AuditLogs
- ☒ MicrosoftGraphActivityLogs
- ☒ RemoteNetworkHealthLogs
- ☒ NetworkAccessAlerts
- ☒ NetworkAccessConnectionEvents

Destination details

- ☐ Send to Log Analytics workspace
- ☐ Archive to a storage account
- ☒ Stream to an event hub

For potential partner integrations, [click to learn more about event hub integration](#).

Subscription

Event hub namespace *

Event hub name (optional) ⓘ

Event hub policy name

- ☐ Send to partner solution

i In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

- f. After saving, wait for a period of time, approximately 15 minutes, for the first events to generate. The Azure logging subsystems may take up to 24 hours to forward events, but should be generally seen within 15 minutes.

Sample Events

Note: The schema of events changes depending on the log sources forwarding to Event Hub. FortiSIEM may have more than one parser for different log sources. If you identify any events coming in as "Unknown_

EventType", please file a support request with those log samples.

General Log Format FortiSIEM 7.3.x and Earlier

```
<raw event identically as seen in event hub>
```

Example EntraID ServicePrincipalSignInLog – Truncated for brevity.

```
MS_EVENT_HUB eventHubName=myeventhubname event=
{"Level":4,"callerIpAddress":"1.1.1.1","category":"ServicePrincipalSignInLogs","correlationId":"f5
4111d5-11111-4136-8948-84e11111eda","durationMs":0,"location":"US","operationName":"Sign-in
activity","operationVersion":"1.0","phCustId":1 }
```

Microsoft Cloud App Security

- [Integration Points](#)
- [Event Types](#)
- [Configuring a SIEM Agent](#)
- [Connecting Office 365 to Cloud App Security](#)
- [Sample Events](#)

Integration Points

Protocol	Information Discovered	Used For
SIEM Agent	Logon, User creation/deletion and other Audit activity for Azure Applications including Office 365, SharePoint, OneDrive, Teams, PowerBI , Exchange	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "MS-Azure-CloudAppSec" in the **Search** field to see the event types associated with Microsoft Cloud App Security.

Configuring a SIEM Agent

FortiSIEM integrates with Microsoft Cloud App Security to collect alerts and activities from apps to Microsoft Cloud. As new activities and events are supported by connected apps, they become available to FortiSIEM via Microsoft Cloud App Security integration.

The integration is done via the Microsoft Cloud App Security SIEM agent. It can run on any server (including FortiSIEM). It pulls alerts and activities from Microsoft Cloud App Security and then streams them into FortiSIEM.

For details, see [here](#).

FortiSIEM integration is accomplished in three steps:

1. Set up a SIEM Agent in the Microsoft Cloud App Security portal.
2. Download the SIEM agent (JAR file) and run it on a server. The agent would connect to the portal, collect logs and forward to FortiSIEM. The server could be a FortiSIEM node such as Collector.
3. Validate that the SIEM agent is working correctly.
4. Configure an application to connect to Microsoft Cloud App Security portal. See those events in FortiSIEM.

Step 1: Set Up a SIEM Agent in the Microsoft Cloud App Security Portal

1. In the Cloud App Security portal, under the Settings cog, click **Security extensions** and then click on the **SIEM agents** tab.
2. Click the plus icon to start the **Add SIEM agent** wizard.

3. In the wizard:
 - a. Click **Start Wizard**.
 - b. Fill in a name.
 - c. **Select your SIEM format** as 'Generic CEF'.
 - d. In **Advanced settings**:
 - i. Set **Time Format** to 'RFC 5424'.
 - ii. Check **Include PRI**.
 - iii. Check **Include system name**.
 - e. Click **Next**.
 - f. Type in the IP address or hostname Forti**SIEM** node receiving the events and port **514**. Select TCP or UDP as the **SIEM** protocol. In most common situations, you would choose a FortiSIEM Collector. Click **Next**.
 - g. Select which data types, **Alerts** and **Activities** you want to export to your **FortiSIEM**. **We recommend choosing All Alerts and All Activities**. You can use the Apply to drop-down to set filters to send only specific alerts and activities. You can click **Edit and preview results** to check that the filter works as expected. Click **Next**.
 - h. The wizard will say that SIEM agent configuration is finished. Copy the token and save it for later.
 - i. After you click **Finish** and leave the Wizard, back in the SIEM page, you can see the SIEM agent you added in the table. It will show that it's **Created** until it's connected later.

Step 2: Download the SIEM agent (JAR file) and Run it on a Server

1. In the Microsoft Download Center, after accepting the software license terms, download the .zip file and unzip it.
2. Run the following command:

```
java -jar mcas-siemagent-0.87.20-signed.jar --logsDirectory <DIRNAME> --token <TOKEN> &
```

where:
 - DIRNAME (optional) is the path to the directory for agent to write debug log.
 - TOKEN is the SIEM agent token you copied in the previous [Step 1](#) Sub-step 3.h.

Step 3: Validate that the SIEM Agent is Working Correctly

Make sure the status of the SIEM agent in the Cloud App Security portal is 'Connected'.

If the connection is down for more than two hours, then the status may show 'Connection error'. The status will be 'Disconnected' if down for more than 12 hours.

Step 4: Configure an Application to Connect to Microsoft Cloud App Security Portal

Cloud App Security currently supports the following Office 365 apps:

- [Office 365](#)
- Dynamics 365 CRM
- Exchange (only appears after activities from Exchange are detected in the portal and requires you to turn on auditing)
- OneDrive
- PowerBI (only appears after activities from PowerBI are detected in the portal, and requires you to turn on auditing)
- SharePoint
- Teams (only appears after activities from Teams are detected in the portal)

See the [Microsoft documentation](#) to setup these applications.

Connecting Office 365 to Cloud App Security

Use the app connector API to connect Microsoft Cloud App Security to your existing Microsoft Office 365 account. The Microsoft Cloud App Security connection gives you visibility into and control over Office 365 use.

For information on how Cloud App Security helps protect your Office 365 environment, see [here](#).

For information on the prerequisites and steps to connect Microsoft Cloud App Security to your existing Microsoft Office 365 account, see [How to connect Office 365 to Cloud App Security](#).

Sample Events

```
<109>2018-05-22T04:17:28.340Z SP204 CEF:0|MCAS|SIEM_Agent|0.123.162|EVENT_CATEGORY_LOGIN|Log
on|0|externalId=70e988af3b82e19b872d12a91860d300d968f47e0bb245a0e765d9dbfddb02ce
rt=1526962648340 start=1526962648340 end=1526962648340 msg=Log on
suser=user1@userexample.onmicrosoft.com destinationServiceName=Microsoft Azure
dvc=43.254.220.13 requestClientApplication=;Windows 10;Edge 17.17134; cs1Label=portalURL
cs1=https://userexample.us2.portal.cloudappsecurity.com/#/audits?activity.id\=eq
(70e988af3b82e19b872d12a91860d300d968f47e0bb245a0e765d9dbfddb02ce,)
cs2Label=uniqueServiceAppIds cs2=APPID_AZURE cs3Label=targetObjects cs3=Azure
Portal,user1,user1 cs4Label=policyIDs cs4= c6a1Label="Device IPv6 Address" c6a1=
```

Microsoft Defender for Identity (Previously Microsoft Azure Advanced Threat Protection (ATP))

- [Integration Points](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Event](#)

Integration Points

Protocol	Information Discovered	Used For
Syslog (CEF)	Suspicious alerts occurring on Windows machine in Azure	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "MS-AzureATP" in the **Search** field to see the event types associated with Microsoft Azure Advanced Threat Protection (ATP).

Configuration

FortiSIEM receives alerts via CEF formatted syslog. See [here](#) for details.

Sample Event

```
02-21-2018 16:20:21 Auth.Warning 192.168.0.220 1 2018-02-21T14:20:06.156238+00:00 CENTER CEF
6076 LdapBruteForceSecurityAlert 0|Microsoft|Azure
ATP|2.22.4228.22540|LdapBruteForceSecurityAlert|Brute force attack using LDAP simple
bind|5|start=2018-02-21T14:19:41.7422810Z app=Ldap suser=John Doe shost=CLIENT1 msg=A brute
force attack using the Ldap protocol was attempted on John Doe (Software Engineer) from
CLIENT1 (100 guess attempts). cnt=100 externalId=2004 cs1Label=url cs1=https://contoso-
corp.atp.azure.com/securityAlert/57b8ac96-7907-4971-9b27-ec77ad8c029a
```

Microsoft Entra Identity Protection

Microsoft Entra ID Protection uses advanced machine learning to identify sign-in risks and unusual user behavior to block, challenge, limit, or allow access. For more information, see [here](#).

Support Added: FortiSIEM 6.6.0

Vendor Version Tested: Not Provided

Vendor: Microsoft

Product: Entra Identity Protection

Product Information: <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id-protection>

FortiSIEM supports ingesting data from the Microsoft Graph List Risky Users API using the FortiSIEM "HTTPS Advanced" credential type, also known as the Generic Log API Poller feature from FortiSIEM 6.6.0 and later. See [Configuring Microsoft Graph List Risky Users API using Generic HTTPS Poller](#) for details.

Configuration

- [Configuring Microsoft Graph List Risky Users API using Generic HTTPS Poller](#)

Configuring Microsoft Graph List Risky Users API using Generic HTTPS Poller

To configure Microsoft Graph List riskyUsers API, you will need to perform setup in Entra and in FortiSIEM by taking the following steps.

- [Setup in Entra](#)
- [Setup FortiSIEM Credential to call the List riskyUsers API Endpoint](#)

Notes:

- Using the riskyUsers API requires a Microsoft Entra ID P2 license.
- The availability of risky user data is governed by the Microsoft Entra data retention policies.

References:

[What is Microsoft Entra Identity Protection](#)

[Overview of Graph List riskyUsers API](#)

[Overview of the FortiSIEM HTTPS Advanced \(Generic Log API Poller\) no-code feature for ingesting third party JSON APIs](#)

Setup in Entra

- [Configuring Microsoft Entra ID \(Formerly Azure AD\) Application for access to Graph APIs](#)
- [Create Office 365 Credential](#)
- [Generate Secret Key](#)
- [Configure API Permissions for Application Registration](#)
- [Administrator Consent](#)

Configuring Microsoft Entra ID (Formerly Azure AD) Application for access to Graph APIs

1. Follow the guide for the Office 365 integration [here](#), which also includes the necessary permissions for accessing the List Risky Users API.

Note: Most Entra ID (Formerly Azure AD) customers are also users of Office 365. If so, follow the entire guide [here](#) and you can use the same credential for both Office 365 and List Risky Users API integrations.

If you do not need the Office 365 integration, you can instead just create the below credential with the necessary Graph API permissions.

Note: Information for Microsoft configuration here is taken from <https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-aad?tabs=workforce-tenant>.

Create Office 365 Credential

1. Login to the Azure portal.
2. From the portal menu, select **Microsoft Entra ID** (Formerly Azure AD).
3. From the left navigation, select **App registrations > New registration**.
4. In the **Name** field, enter "FortiSIEM App".
5. From **Supported Account Types**, select **Accounts in this organizational directory only (<domain> only – single tenant)**.
6. Leave **Redirect URI** (optional) blank.
7. Click **Register**.
8. On the redirected page showing your registration details, record the following for later.
 - Application (client) ID
 - Directory (tenant) ID

Generate Secret Key

To generate a secret key, take the following steps:

1. From the left navigation, select **Certificates & secrets > Client secrets > New client secret**.
2. In the right side panel, enter the following information:
3. In the **Description** field, enter "FortiSIEM Secret Key".
4. From the **Expires** drop-down list, select **730 days (24 months)**, or your desired expiration.
Note: You must update the key in FortiSIEM configuration BEFORE it expires by creating a new key before retiring the old one.
5. Click **Add**.
6. Record the new API Key secret value at the bottom of the page. You can only view this once, so store the information in a secure location for configuration later.

Configure API Permissions for Application Registration

1. From the left navigation, select **API permissions > Add a permission**.
2. Select **Microsoft Graph**.
3. Select **Application permissions**.
4. Select the following permissions:
 - IdentityRiskyUser.Read.All
 - IdentityRiskEvent.Read.All
 - IdentityRiskyServicePrincipal.Read.All
 - IdentityRiskyUser.Read.All
5. Save your configuration.

Administrator Consent

1. Click the **Grant admin consent for <tenant>** after saving.
2. When prompted with: **Do you want to grant consent for the requested permissions for all accounts in your_organization?** alert, select **Yes**. This will update any existing admin consent records this application already has to match what has been configured.

Setup FortiSIEM Credential to call the List riskyUsers API Endpoint

Setup in FortiSIEM for a new integration using the Generic Log API Poller can be broken down into the following general steps:

- [Create a New Device/Application](#)
- [Create the Credentials Configuration](#)
- [Create the Credentials Mapping](#)
- [Test the Credential](#)

After testing the credential, you can [search for Risky User events](#). More information on parsing of new events is [here](#).

To configure the Microsoft List riskyUsers API to FortiSIEM, take the following steps.

Create a New Device/Application

Note: If this device type already exists, you can skip this step, and proceed to [Create the Credentials Configuration](#).

1. Navigate to **ADMIN > Device Support > Devices/Apps**.
2. Click **New**.
3. From the Device/Application Type Definition dialog box, take the following steps.
 - a. From the **Category** drop-down list, select **Application**.
 - b. In the **Vendor** field, enter "Microsoft".
 - c. In the **Model** field, enter "Graph API Platform".
 - d. In the **Version** field, enter "ANY".
 - e. From the **Device/App Group** drop-down list, select
Applications > Infrastructure App > **Security Mgmt Server**
Applications > Infrastructure App > **Cloud Mgmt**
 - f. Leave **Biz Service Group** blank.
 - g. From the **Access Protocol** drop-down list, remove **SSH**, **SNMP**, and **TELNET**.
 - h. From the **Access Protocol** drop-down list, select **HTTPS Advanced**.
 - i. Leave **App Package Group** blank.
 - j. Click **Save**.

Create the Credentials Configuration

1. Navigate to **ADMIN > Setup > Credentials**.
2. Under **Step 1: Enter Credentials**, click **New**.
3. In the **Name** field, enter a name, for example "Graph_Risky_Users".
4. From the **Device Type** drop-down list, select **Microsoft Graph**.
5. From the **Access Protocol** drop-down list, select **HTTPS Advanced**.
6. Download the following file: [Microsoft_Graph_List_Risky_Users.json](#)
7. Click **Import Definition**.
8. Select the file you just downloaded from step 6, and click **Import**.
9. Click **Yes** to overwrite.
10. Click the Authentication Parameters icon, and take the following steps.
 - a. With the **General** tab selected, take the following steps.
 - i. In the **Access Token URL** field, replace "xxxxx" with your Directory (tenant) ID that you recorded earlier.
`https://login.microsoftonline.com/<your-tenant-id>/oauth2/v2.0/token`
 - ii. In the **Client Id** field, enter the Application (client) ID you recorded earlier.
 - iii. In the **Client Secret** field, enter the client secret you recorded earlier.
 - iv. Click **OK**.
 - b. Click **Save**.

Create the Credentials Mapping

1. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
2. From the Device Credential Mapping Definition dialog box, take the following steps.
 - a. From the **Credentials** drop-down list, select the credential you just created (Graph_Risky_Users).
 - b. Click **Save**.

Test the Credential

1. Ensure the credentials mapping you just created is selected. If not, select it.
2. Under **Step 2: Enter IP Range to Credentials Association**, click the **Test** drop-down list, and select **Test Connectivity without Ping**.

If successful, it should take about 5 minute before the first pull job is complete. Click the **Pull Events** tab to view the status.

Icon	Description
Yellow Star	Job is queued, has not started yet. Typically, a job takes 5 minutes to complete.
Green Check	Most recent event pull of the pull job succeeded.
Yellow Triangle with Exclamation Point	Error occurred during the most recent event pull. Hover over the icon to get more information.

If you encounter an error, refer to [Common Errors](#) for additional information that may help you resolve the issue.

Searching for List riskyUsers Graph API events

Navigate to **Analytics**, click on the **Edit Filters and Time Range...** search field, and run the following query, by first selecting Filter By: **Event Attribute**, then entering/selecting the following:

Attribute	Operator	Value
Raw Event Log	CONTAIN	graph_risky_users

When done, click **Apply & Run**.

Sample Event

```
Nov 02 12:38:10 2023 graph.microsoft.com 192.0.20.0 graph_risky_users: {"id": "123456", "isDeleted": false, "isProcessing": false, "riskLevel": "none", "riskState": "dismissed", "riskDetail": "adminDismissedAllRiskForUser", "riskLastUpdatedDateTime": "2023-11-01T15:57:37.5356848Z", "userDisplayName": "example user", "userPrincipalName": "exampleUser"}
```

Parsing of New Events

For new integrations, a parser will not exist for these events. All events will come in as unknown until a custom parser is created. See [Creating a Custom Parser](#) for more information. For this particular integration, the parser is pre-defined.

Microsoft Office 365 Audit

FortiSIEM Support added: 4.8.1

FortiSIEM last modification: 7.1.0

Vendor: Microsoft

Vendor version tested: Not Provided

Product Information: <https://www.microsoft.com/en-us/microsoft-365/business>

- [What is Monitored](#)
- [Configuring Office365 Auditing](#)
- [Office365 Auditing Rules](#)
- [Office365 Auditing Reports](#)
- [Office365 Auditing Dashboard](#)
- [Sample Events for Office 365 Audit Activity](#)
- [Enabling Mailbox Auditing](#)

What is Monitored

Office 365 Management Activity API (manage.office.com) – The Office 365 Management Activity API aggregates actions and events into tenant-specific content blobs, which are classified by the type and source of the content they contain. Currently, the following content types are supported:

- Audit.AzureActiveDirectory
- Audit.Exchange
- Audit.SharePoint
- Audit.General (includes all other workloads not included in the previous content types)
- DLP.All (DLP events only for all workloads)

For details about the events and properties associated with these content types, see [Office 365 Management Activity API schema](#). An extensive list of Office 365 services are audited via this method, and service names can be seen by inspecting the “AuditLogRecordType” of this link: <https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema>

The following activities are monitored:

- File and folder activities
- Sharing and access request activities
- Site administration activities
- Exchange mailbox activities
- User administration activities
- Group administration activities
- Application administration activities
- Role administration activities

Microsoft Graph API (graph.microsoft.com) – This API is used to obtain Office 365 Mail Statistics. The following activity report is run: [https://graph.microsoft.com/v1.0/reports/getEmailActivityCounts\(period='D30'\)](https://graph.microsoft.com/v1.0/reports/getEmailActivityCounts(period='D30'))

Office 365 Reporting Web Service (reports.office365.com) – This API is used to obtain Office 365 Mail Statistics. The following reporting web service reports are run:

- <https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MailDetailATP>
- <https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MailTrafficSummary> (TopMailSender, TopMailRecipient, and TopMalwareRecipient categories)

The following information is obtained:

- Email Activity Reports
- Top Mail Senders
- Top Mail Receivers
- Top Malware Recipients
- All Mail sent/received statistics

Configuring Office365 Auditing

Office365 Auditing configuration is comprised of three main steps. Before proceeding, ensure you have a good understanding of mailbox auditing. Supplemental information is provided in [Enabling Mailbox Auditing](#).

- [Step 1: Configure Office365 Mailboxes for Auditing](#)
- [Step 2: Configure Office365 for Auditing by FortiSIEM](#)
- [Step 3: Configure FortiSIEM](#)

Step 1: Configure Office365 Mailboxes for Auditing

To set up mailbox auditing in Office 365, take the following steps.

1. Login to Exchange Online (**Note:** Instructions differ slightly for GCC High and other gov cloud Organizations)
2. Powershell Command:
`Connect-ExchangeOnline -UserPrincipalName navin@contoso.onmicrosoft.com`
3. For each mailbox you'd like to turn on auditing, run the following command:
`Set-Mailbox -Identity <MailboxIdentity> -AuditEnabled $true`
 - To bulk set for every mailbox run:
`Get-Mailbox -ResultSize Unlimited -Filter{RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -AuditEnabled $true`

Important Notes

- Although mailbox audit logging is on by default for all organizations, only users with licenses that include Audit (Premium) (collectively referred to in this article as E5/A5/G5 licenses) return mailbox audit log events in audit log searches in the Microsoft Purview compliance portal or via the Office 365 Management Activity API by default.
- Mailbox Operations that require premium licenses: (Available only for users with E5/A5/G5 licenses.)

Mailbox action	Description
SearchQueryInitiated	A person uses Outlook (Windows, Mac, iOS, Android, or Outlook on the web) or the Mail app for Windows 10 to search for items in a mailbox.
MailItemsAccessed	Occurs when mail data is accessed by mail protocols and clients.
MessageBind	A message was viewed in the preview pane or opened by an admin.
***Send	The user sends an email message, replies to an email message, or forwards an email message.

Note: Remember, an admin with Full Access permission to a mailbox is considered a delegate.

- Mailbox Audit Operations that do not have auditing turned on by default:

Mailbox action	Description
Copy (Admin only)	A message was copied to another folder.
FolderBind (Admin and Delegate)	A mailbox folder was accessed. This action is also logged when the admin or delegate opens the mailbox.
MailboxLogin (Owner only)	The user signed into their mailbox.
MessageBind (Admin only)	A message was viewed in the preview pane or opened by an admin. (not applicable to E5/A5/G5 licenses)
Move	A message was moved to another folder.
RecordDelete	An item that's labeled as a record was soft-deleted (moved to the Recoverable Items folder). Items labeled as records can't be permanently deleted (purged from the Recoverable Items folder).
SearchQueryInitiated (Owner only)	A person uses Outlook (Windows, Mac, iOS, Android, or Outlook on the web) or the Mail app for Windows 10 to search for items in a mailbox.
UpdateComplianceTag	A retention label was updated.

Step 2: Configure Office365 for Auditing by FortiSIEM

Take the following steps to configure Office365 for Auditing by FortiSIEM.

- [Create Office 365 Credential](#)
- [Create New App Registration](#)
- [Generate Secret Key](#)
- [Configure API Permissions for Application Registration](#)
- [Grant Sharepoint Permissions](#)
- [Grant Graph API Permissions](#)
- [Grant Reports API Permissions](#)

Create Office 365 Credential

1. Login to the Azure Portal.
2. Go to Microsoft Entra ID (Formerly Azure AD).

3. On the left hand toolbar, select **App registrations**.

Create New App Registration

1. Click **New registration**.
2. In the Name field, enter "FortiSIEM App".
3. From Supported Account Types, select **Accounts in this organizational directory only (<domain> only – single tenant)**.
4. Leave the **Redirect URI** (optional) field blank.
5. Click **Register**.

After clicking Register, on the redirected page showing your registration details, note the following:

- Application (Client) ID
- Directory (Tenant) ID

Generate Secret Key

To generate a secret key, take the following steps:

1. On the left hand toolbar, click **Certificates and Secrets**.
2. Click **New client secret**.
3. In the right side popup, enter the following information:
 - In the **Description** field, enter "FortiSIEM Secret Key".
 - From the **Expires** drop-down list, select 730 days (24 months) or your desired expiration.

Note: You must update the key in FortiSIEM configuration BEFORE it expires by creating a new key before retiring the old one.
4. Click **Add**.
5. Record the new API Key secret **value** at the bottom of the page. You can only view this once and will need it later for configuring FortiSIEM, so store the information in a secure location for configuration later.

Configure API Permissions for Application Registration

1. In the left pane, navigate to **API permissions**.
2. Click **Add a permission**.
3. Select **Office 365 Management APIs**.
4. Click **Application permissions** and expand all.
5. Select all permissions with "Read" access. (There is no reason to write).
6. Click **Add permissions**.

You will see a warning: "Permissions have changed." Users and/or admins will have to consent even if they have already done so previously.

Grant Sharepoint Permissions

For Sharepoint Permissions, take the following step:

Add permission > Sharepoint > Application Permissions > Sites.Read.All

Grant Graph API Permissions

For Graph API Permissions, take the following steps:

1. Login to Azure Portal.
2. Go to Microsoft Entra ID (Formerly Azure AD).
3. On the left hand toolbar, select **App registrations**.
4. Select your app from the list if it is already defined.
5. On the left hand toolbar, select **API permissions**.
6. Select Microsoft Graph > Application permissions.
7. Select the following permissions:
 - Reports.Read.All
 - IdentityRiskEvent.Read.All
 - IdentityRiskyServicePrincipal.Read.All
 - IdentityRiskyUser.Read.All
 - SecurityEvents.Read.All
 - SecurityIncident.Read.All (Microsoft365 Defender APIs)
 - ThreatIndicators.Read.All
 - ThreatIntelligence.Read.All
 - User.Read.All

Grant Reports API Permissions

For Office 365 Reports API Permissions, take the following steps:

1. Login to Azure Portal.
2. Go to Microsoft Entra ID (Formerly Azure AD).
3. On the left hand toolbar, select **App registrations**.
4. Select your app from the list if it is already defined.
5. On the left hand toolbar, select **API permissions**.
6. Click **Add a permission**.
7. Select the middle tab at the top labeled **APIs my organization uses**.
8. In the search bar, enter "Office 365 Exchange Online" and select it (**Note:** It does not appear by default).
9. Select **Application Permissions**.
10. Locate the **ReportingWebService** drop-down list and select the permission **ReportingWebService.Read.All**.
11. Make sure to click the **Grant admin consent for <tenant>** after saving. Click **grant admin consent** and select **Yes** when you see the prompt: Do you want to grant consent for the requested permissions for all accounts in your_organization? alert. This will update any existing admin consent records this application already has to match what has been configured.

Step 3: Configure FortiSIEM

FortiSIEM configuration is comprised of two main steps.

- [Define Office 365 Management Credential](#)
- [Create IP Range to Credential Association and Test Connectivity](#)

Define Office 365 Management Credential

Log in to the FortiSIEM Supervisor node, and take the following steps.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Office365
Access Protocol	Office 365 Mgmt Activity API
Tenant ID	Use the ID from Azure Login URL. See Step 5 in Create Office 365 API Credential .
Password config	If you select Manual, take the following steps: 1. For Client ID, use the value obtained from the Create New App Registration step in Create Office 365 Credential. 2. For Client Secret, use the value obtained from the Generate Secret Key step in Create Office 365 Credential. For CyberArk SDK credential method, see CyberArk SDK Password Configuration. For CyberARK REST API credential method, see CyberArk REST API Password Configuration.
Authentication Endpoint	Enter the authentication endpoint. The Authentication Endpoint depends on the type of Office 365 environment you have: • Enterprise plan: login.windows.net • GCC government plan: login.microsoftonline.com • GCC High government plan: login.microsoftonline.us • DoD government plan: login.microsoftonline.us Note: Do NOT include "https://" in the Authentication Endpoint URL field.

Settings	Description
Authentication Protocol	Enter the token location. For example, /oauth2/token.
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps.

1. In **Step 2: Enter IP Range to Credential Associations**, if the organization has more than 1 collector, select the collector from the drop-down list that will do the API polling. If the organization has 1 or no collectors, there is no drop-down and you can proceed to the next step.
2. Click **New** to create a new association.
 - a. Select the name of the credential created in the **Define Office 365 Management Credential** from the **Credentials** drop-down list.
 - b. In the **IP/Host Name** field, enter the API Endpoint based off your Office 365 plan type. Your options are:
 - Enterprise plan: manage.office.com
 - GCC government plan: manage-gcc.office.com
 - GCC High government plan: manage.office365.us
 - DoD government plan: manage.protection.apps.mil
 - c. Click **Save**.
3. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling. A pop up will appear and show the Test Connectivity results.
4. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Office 365 Log Collection.

Office365 Auditing Rules

The following are rules all generated via datasource : Office365 Mgmt Activity API. Note that the following are examples, and non-exhaustive. Navigate to **Resources > Rules** and search for "Office365:" in the main **Search...** field to see available rules.

- Office365: Abnormal Logon Detected
- Office365: Admin or Delegated User Created Mailbox Forwarding Rule for another User
- Office365: Brute Force Login Attempts - Same Source
- Office365: Brute Force Login Attempts - Same User
- Office365: Brute Force Logon Success
- Office365: Delete Message Inbox Rule Created
- Office365: Identity Protection Detected a Risky User or SignIn Activity
- Office365: Mailbox Login from Outside My Country
- Office365: Mailbox SendAs or SendOnBehalf has occurred
- Office365: Mailbox User Created Mail Forwarding Rule
- Office365: Move To Folder Inbox Rule Created
- Office365: Set-Mailbox Forwarding Action Created

- Office365: Strong Authentication Disabled for a User
- Office365: Suspicious File Type Uploaded

Office365 Auditing Reports

The following are reports all generated via datasource : Office365 Mgmt Activity API. Note that the following are examples, and non-exhaustive. Navigate to **Resources > Reports** and search for "Office365:" in the main **Search...** field to see available reports.

- Office365: Top Entra ID Logons by Source
- Office365: Top Entra ID Failed User Logon
- Office365: Top Mailbox Logins by Source Country
- Office365: Top Mailbox Logins by Source IP
- Office365: Top Mail Senders
- Office365: Top Mail Recipients
- Office365: Top SendAs or SendOnBehalf Activity by Originating User
- Office365: Top Sharepoint Links Used
- Office365: Top Sharepoint Secure Links Used by Source
- Office365: Top Sharepoint Company Links Used by Source
- Office365: Top Sharepoint Anonymous Links Used by Source

Office365 Auditing Dashboard

The Office 365 Dashboard contains 4 tabs:

- [Logon Audit](#)
- [Sharepoint Audit](#)
- [Sensitivity Label Audit](#)
- [Mail Statistics](#)

Logon Audit

Object	Description
Data Source	Microsoft Office365 Management Activity API - Collects both Entra ID (formerly Azure AD) logon events as well as Exchange mailbox logons.
Widgets	Various mailbox and Entra ID logon success/failure activity reports.
Troubleshooting	Ensure that mailbox auditing is enabled for every mailbox in your organization.

Sharepoint Audit

Object	Description
Data	Microsoft Office365 Management Activity API

Object	Description
Source	
Widgets	These are reports based on Sharepoint shared link activity primarily, others may be added in the future. Other Sharepoint reports are available.

Sensitivity Label Audit

This is only populated if you are using Microsoft MIP for Exchange to assign sensitivity labels to emails.

Object	Description
Data Source	Microsoft Office365 Management Activity API
Reference Documents	https://support.microsoft.com/en-us/office/apply-sensitivity-labels-to-your-files-and-email-2f96e7cd-d5a4-403b-8bd7-4cc636bae0f9 https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-new-microsoft-information-protection-capabilities-to/ba-p/1999692

Mail Statistics

This is mail statistical data such as top senders / receivers collected from primarily the Office365 Reporting Web Service and Graph APIs.

Object	Description
Data Source	Office365 Reporting Web Service and Microsoft Graph Reporting API

Sample Events for Office 365 Audit Activity

```
[MS_OFFICE365_MessageTrace] = {"EndDate":"/Date
(1694294532249)/","FromIP":"10.10.10.19","Index":3,"MessageId":"<11111111-855c-44ff-8edb-
ffaffae245dd@example.com>","MessageTraceId":"11111111-e22c-485e-be92-
08dbb082b92e","Organization":"example.onmicrosoft.com","Received":"/Date
(1694187970214)/","RecipientAddress":"example@azurestorefortinet.onmicrosoft.com","SenderAddress":
"example@microsoft.com","ServerHostName":"reports.office365.com","Size":193926,"StartDate":"/Date
(1694121732249)/","Status":"Resolved","Subject":"We detected synchronization errors in your
directory","TenantId":"11111111-1b14-42a1-8dcf-4b21dece61ba","ToIP":null,"__metadata":
{"id":"https://reports.office365.com/ecp/ReportingWebService/Reporting.svc/MessageTrace
(3)","type":"TenantReporting.MessageTrace","uri":"https://reports.office365.com/ecp/ReportingWebSe
rvice/Reporting.svc/MessageTrace(3)"},"phCustId":1}
```

```
[MS_OFFICE365_MailTrafficSummary_TopMalwareRecipient] =
{"ServerHostName":"reports.office365.com","ServerIpAddr":"10.10.10.10","TenantId":"0000-0000-
00000-0000-00000","TopMalwareRecipient":"","count":"0","phCustId":1}
```

```
[MS_OFFICE365_MailTrafficSummary_Count] = {"Meeting Created":"41","Meeting
Interacted":"57","Read":"12458","Report Date":"2023-08-25","Report
```

```
Period":"30","ServerHostName":"reports.office365.com","ServerIpAddr":"10.10.10.10","TenantId":"0000-00000-00000-00000","count":"1911","direction":"outbound","phCustId":1,"\uffffReport Refresh Date":"2023-09-23"}
```

```
[MS_OFFICE365_MessageTrace] = {"Action":"Hosted Mailbox:
Inbox","BulkComplaintLevel":null,"Date":"/Date(
(1695940243000)/","Direction":"Inbound","Domain":"example1.com","EndDate":"/Date(-
621355968000000)/","EventType":"Message
passed","FileHash":null,"FileName":null,"Index":4,"MalwareName":null,"MessageId":"<9DB1A48827764D1
783C1CD22F9BC8D5B@MUMTILLPCMS>","MessageTraceId":"125227f2-a7fe-42ec-b748-
08dbc0728a18","Organization":".com","RecipientAddress":"user@example.com","SenderAddress":"user1@e
xample1.com","ServerHostName":"reports.office365.com","ServerIpAddr":"10.10.10.10","StartDate":"/D
ate(-621355968000000)/","Subject":"Compliance under Maharashtra State Tax On Professions, Trades,
Callings And Employments Act,1975 - ","TenantId":"0000-0000-00000-0000-
00000","VerdictSource":"NotSpam","__metadata":
{"id":"https://reports.office365.com/ecp/ReportingWebService/Reporting.svc/MailDetailATP
(4)","type":"TenantReporting.MailDetailATPReport","uri":"https://reports.office365.com/ecp/Reporti
ngWebService/Reporting.svc/MailDetailATP(4)"},"phCustId":1}
```

Enabling Mailbox Auditing

Note: The following is an excerpt of the Microsoft Manage mailbox auditing article [here](#).

Mailbox audit logging is turned on by default in all organizations. This effort started in January 2019, and means that certain actions performed by mailbox owners, delegates, and admins are automatically logged.

Here are some benefits of mailbox auditing on by default:

- Auditing is automatically turned on when you create a new mailbox. You don't need to manually turn on mailbox auditing for new users.
- You don't need to manage the mailbox actions that are audited. A predefined set of mailbox actions are audited by default for each sign-in type (Admin, Delegate, and Owner).
- When Microsoft releases a new mailbox action, the action might be added automatically to the list of mailbox actions that are audited by default (subject to the user having the appropriate license). This result means you don't need to add new actions on mailboxes as they're released.
- You have a consistent mailbox auditing policy across your organization (because you're auditing the same actions for all mailboxes).

Key Note:

By default, only mailbox audit events for users with licenses that include Microsoft Purview Audit (Premium) are available in audit log searches in the Microsoft Purview compliance portal or via the Office 365 Management Activity API. These licenses are described [here](#). For brevity, this article will collectively refer to licenses that include Audit (Premium) as E5/A5/G5 licenses.

To verify that mailbox auditing on by default is turned on for your organization, run the following command in [Exchange Online PowerShell](#):

```
Get-OrganizationConfig | Format-List AuditDisabled
```

The value **False** indicates that mailbox auditing on by default is turned on for the organization. Mailbox auditing on by default in the organization overrides the mailbox auditing settings on individual mailboxes.

Supported Mailbox Types

Mailbox types that are supported by mailbox auditing on by default are described in the following table:

Mailbox type	Supported
User mailboxes	✓
Shared mailboxes	✓
Microsoft 365 Group mailboxes	✓
Resource mailboxes	
Public folder mailboxes	

Sign-in Types Information

- **Owner:** The mailbox owner (the account that's associated with the mailbox).
- **Delegate:**
 - A user who's been assigned the SendAs, SendOnBehalf, or FullAccess permission to another mailbox.
 - An admin who's been assigned the FullAccess permission to a user's mailbox.
- **Admin:**
 - The mailbox is searched with one of the following Microsoft eDiscovery tools:
 - Content Search in the compliance portal.
 - eDiscovery or eDiscovery (Premium) in the compliance portal.
 - In-Place eDiscovery in Exchange Online.
 - The mailbox is accessed by using the Microsoft Exchange Server MAPI Editor.

Mailbox Actions

Mailbox action	Description
Create	An item was created in the Calendar, Contacts, Draft, Notes, or Tasks folder in the mailbox (for example, a new meeting request is created). Creating, sending, or receiving a message isn't audited. Also, creating a mailbox folder isn't audited.
FolderBind	A mailbox folder was accessed. This action is also logged when the admin or delegate opens the mailbox. (24 hour delay)
HardDelete	A message was purged from the Recoverable Items folder.
MailboxLogin	The user signed into their mailbox. (owner only login)
MailItemsAccessed	Note: This value is available only for users with E5/A5/G5 licenses. For more information, see Set up Microsoft Purview Audit (Premium). Occurs when mail data is accessed by mail protocols and clients.

Mailbox action	Description
MessageBind	Note: This value is available only for users without E5/A5/G5 licenses. A message was viewed in the preview pane or opened by an admin. (admin only activity, not delegate or owner)
Move	A message was moved to another folder.
MoveToDeletedItems	A message was deleted and moved to the Deleted Items folder.
RecordDelete	An item that's labeled as a record was soft-deleted (moved to the Recoverable Items folder). Items labeled as records can't be permanently deleted (purged from the Recoverable Items folder).
SearchQueryInitiated	Note: This value is available only for users with E5/A5/G5 licenses. For more information, see Set up Microsoft Purview Audit (Premium). A person uses Outlook (Windows, Mac, iOS, Android, or Outlook on the web) or the Mail app for Windows 10 to search for items in a mailbox.
Send	Note: This value is available only for users with E5/A5/G5 licenses. For more information, see Set up Microsoft Purview Audit (Premium). The user sends an email message, replies to an email message, or forwards an email message. (Owner or Admin only not delegate)
SendAs	A message was sent using the SendAs permission. This permission allows another user to send the message as though it came from the mailbox owner. (Admin or Delegate, Owner n/a)
SendOnBehalf - (admin and delegate only)	A message was sent using the SendOnBehalf permission. This permission allows another user to send the message on behalf of the mailbox owner. The message indicates to the recipient who the message was sent on behalf of and who actually sent the message.
SoftDelete	A message was permanently deleted or deleted from the Deleted Items folder. Soft-deleted items are moved to the Recoverable Items folder.
Update	A message or any of its properties was changed.
UpdateCalendarDelegation	A calendar delegation was assigned to a mailbox. Calendar delegation gives someone else in the same organization permissions to manage the mailbox owner's calendar.
UpdateComplianceTag	A retention label was updated.
UpdateFolderPermissions	A folder permission was changed. Folder permissions control which users in your organization can access folders in a mailbox and the messages located in those folders.
UpdateInboxRules	An inbox rule was added, removed, or changed. Inbox rules process messages in the user's Inbox based on conditions. Actions specify what to do to messages that match the conditions of the rule. For example, move the message to a specified folder or delete the message.

Differences between SendAs and SendOnBehalf

SendAs - Recipient does not know who actually sent the message, appears to be from impersonated mailbox

SendOnBehalf - Recipient sees the sender, and who actually sent the message.

Important:

If you customized the mailbox actions to audit before mailbox auditing on by default was turned on in your organization, the customized mailbox auditing settings are preserved on the mailbox and aren't overwritten by the default mailbox actions as described in this section. To revert the audit mailbox actions to their default values (which you can do at any time), see the Restore the default mailbox actions section later in this article.

Okta

FortiSIEM can integrate with Okta as a single sign-on service for FortiSIEM users, discover Okta users and import them into the CMDB, and collect audit logs from Okta. See [Setting Up External Authentication](#) for information on configuring Okta to use as a single sign-on service, and [Adding Users from Okta](#) for discovering users and associating them with the Okta authentication profile. Once you have discovered Okta users, FortiSIEM will begin to monitor Okta events.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Access Credentials in FortiSIEM](#)
- [Sample Okta Event](#)
- [Adding Users from Okta](#)
- [Configuring Okta Authentication](#)
- [Logging In to Okta](#)
- [Setting Up External Authentication](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Okta API			

Event Types

In **ADMIN > Device Support > Event Types**, search for "okta" to see the event types associated with this device.

Configuration

- In Okta **Administration -> Security -> API**, [create a token](#). Note, tokens generated by this mechanism will have the permissions of the user who generated them.
- Tokens are valid for 30 days and automatically refresh with each API call. Tokens that are not used for 30 days will expire. The token lifetime is currently fixed and cannot be changed.

Access Credentials in FortiSIEM

Setting	Value
Name	<name>
Device Type	OKTA.com OKTA
Access Protocol	OKTA API
Pull Interval	5
Domain	The name of your OKTA domain
Security Token	The token that has been created in Okta
Organization	Select an organization from the drop-down list.

Sample Okta Event

```
Mon Jul 21 15:50:26 2014 FortiSIEM-Okta [action/message]=Sign-in successful
[action/objectType]=core.user_auth.login_success [action/requestUri]=/login/do-login
[actors/0/displayName]=CHROME [actors/0/id]=Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36 [actors/0/ipAddress]=211.144.207.10
[actors/0/login]=firstname.lastname@example.com [actors/0/objectType]=Client [eventId]=tev-
UlpTnWJRI2vXNRKTJHE4A1405928963000 [eventName]=USER-AUTH-LOGIN-SUCCESS [published]=2014-07-
21T07:49:23.000Z [requestId]=U8zGA0zxVNXabfCeka9oGAAAA [sessionId]=s024bi4GpUkRaegPXuA1IFEDQ
[targets/0/displayName]=a_name [targets/0/id]=00uudkhrxcPNGYWISAGK [targets/0/login]=a_
name@doamin.com [targets/0/objectType]=User
```

Adding Users from Okta

- [Create an Okta API Token](#)
- [Define Okta Credential and Associate It with an IP Address](#)
- [Discover Okta Users](#)

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.

Define Okta Credential and Associate It with an IP Address

Take the following steps from these sections:

- [Define Okta Credential in FortiSIEM](#)
- [Create IP Range to Credential Association and Test Connectivity](#)

Define Okta Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**. Your LDAP credentials will be added after clicking **Save**.

Settings	Description
Name	Enter a name for the credential
Device Type	OKTA.com OKTA
Access Protocol	OKTA API
Pull Interval	Enter how often, in minutes, you want FortiSIEM to pull information from Okta.
Domain	Enter the NetBIOS/Domain associated with your Okta account. For example, FortiSIEM.okta.com
Security Token	Enter the security token information.
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps.

1. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter the IP range or host name for your Okta account in the **IP/Host Name** field.
 - b. Select your Okta credentials from the **Credentials** drop-down list created in [Define Okta Credential in FortiSIEM](#) step 2a.
 - c. Click **Save**. Your Okta credentials will appear in the list of credential/IP address associations in **Step 2: Enter IP Range to Credential Associations**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity** to make sure you can connect to the Okta server. A pop up will appear and show the Test Connectivity results.

Discover Okta Users

If the number of users are less than 200, then Test Connectivity will discover all the users.

Okta API has some restrictions that does not allow FortiSIEM to pull more than 200 users. In this case, follow these steps:

1. Login to **Okta**.
2. Download user list CSV file (OktaPasswordHealth.csv) from **Admin > Reports > Okta Password Health**.
3. Rename the CSV file to `all_user_list_%s.csv` (where %s is the placeholder of token obtained in [Create an Okta API Token](#) - Step 3, for example, `all_user_list_00UbCrgrU9b1Uab0cHCuup-5h-6Hi9ItokVDH8nRRT.csv`).
4. Login 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**, and in **Step 2: Enter IP Range to Credential Associations**, select the Okta entry, click on the **Test** drop-down list and select **Test Connectivity** to import all users.

Configuring Okta 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 in to 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	<code>https://<FortiSIEMIP>/phoenix/okta</code>
Name ID Format	EmailAddress
Recipient	FortiSIEM
Audience Restriction	Super
authnContextClassRef	PasswordProtectedTransport
Response	Signed
Assertion	Signed
Request	Uncompressed
Destination	<code>https://<FortiSIEMIP>/phoenix/okta</code>

4. Click **Save**.
5. In the **Sign On** tab, click **View Setup Instructions**.

6. Click **Download Certificate**.
7. Enter the downloaded certificate for Okta authentication.

Logging In to Okta

Follow these steps to log in to Okta from the Okta domain <https://fortinetfsm.okta.com>. You cannot log into Okta from the FortiSIEM UI.

1. Create a new Okta account from <https://www.okta.com/> or log in to an existing account, using the domain fortinetfsm.okta.com.
2. Configure users for the account, for example, testone@fortinet.com, testtwo@fortinet.com, and so on. See [Adding Users From Okta](#) and [Create Login Credentials and Associate Them with an IP Address](#).
3. Discover the Okta users to ensure that you have users to test. See [Discover Okta Users](#).
4. Create a SAML authentication configuration from Okta based on the OKTA SAML 2.0 template. See [Configuring Okta Authentication](#).
5. Associate the users (for example, testone@fortinet.com and testtwo@fortinet.com) to the external profile in **CMDB > Users**.
6. Log in to the Okta domain <https://fortinetfsm.okta.com> as one of the users you defined in [Step 2](#).
7. Click the SAML configuration application in Okta (see [Configuring Okta Authentication](#)). You can now log in to Okta.

Setting Up External Authentication

You have three options for setting up external authentication for your FortiSIEM deployment: LDAP, RADIUS, and Okta.

Multiple Authentication Profiles

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.

1. Log in to your Supervisor node.
2. Go to **ADMIN > Settings > General > External Authentication**.
3. Click **New**.
4. If you are setting up authentication for an organization within a multi-tenant deployment, select the **Organization**.
5. Select the **Protocol**.
6. Complete the protocol settings.

Protocol	User-Defined Settings
LDAP	Access IP Select Set DN Pattern to open a text field in which you can enter the DN pattern if you want to override the discovered pattern, or you want

Protocol	User-Defined Settings
	to add a specific LDAP user.
RADIUS	Access IP Shared Secret Select CHAP if you are using encrypted authentication to your RADIUS server. See also Juniper Networks Steel-Belted RADIUS .
Okta	Certificate See Configuring Okta Authentication for more information.

7. Click **Test**, and then enter credentials associated with the protocol you selected to make sure users can authenticate to your deployment.

Oracle Cloud Infrastructure

FortiSIEM Support Added: 6.4.0

Vendor: Oracle

Product Information: <https://www.oracle.com/cloud/>

- [Configuration](#)
- [Streams Log Ingestion Information](#)
- [Sample Event](#)

Configuration

- [Setup in Oracle](#)
- [Setup in FortiSIEM](#)

Setup in Oracle

Complete these steps from the Oracle Cloud Portal.

Create a User for FortiSIEM Integration

1. Login to Oracle Cloud.
2. In the Search Bar, enter "users".
3. Select **Services > Users**.
4. Click **Create User**.
5. Select **IAM User** and take the following steps.

- a. In the **Name** field, enter a name, such as "fortisiem-user".
- b. In the **Description** field, enter a description, such as "Used by FortiSIEM to ingest logs using Streams integration".
- c. Leave the other options as default.
- d. Click **Create**.

Generate an API Key for the User

1. On the Users page, from the left panel, select **Resources > API Keys**.
Note: You should be re-directed to the Users page after creating a user.
2. Click **Add API Key**.
3. At the Pop Up, generate a key pair or upload an existing public key by taking the following steps.
 - a. Select **Generate API Key Pair**. If you already have an RSA Key Pair, you can select or paste your public key instead.
 - b. Click **Download Private Key**. You'll need this to upload to FortiSIEM later.
 - c. Click **Add**.
 - d. The next page outputs your API Key **Config File**. Copy this and save the entire config file to a text file. You'll need these items to upload to FortiSIEM.
 - e. Click **Close**.

Create a Stream for Audit Logs

1. From Oracle Cloud, in the search bar, search for **Services > Streaming**.
2. Click **Create Stream**, and take the following steps.
 - a. In the **Stream Name** field, enter a name, such as "fortisiem-stream".
 - b. In the **Compartment** drop-down, select **Root Compartment**.
 - c. Select **Existing > Stream Pool: DefaultPool** or **Create Stream Pool**.
Note: A pool is a logical grouping of resources, not necessarily required to create a new one from default.
 - d. In Define Stream Settings, enter the following:
Retention: **24**
Number of Partitions: **5**
Note: You will scale this based on number of logs. 5 partitions provides 5MB/s write, and 10MB/s read. Increase this number if you believe the audit log volume will be significant. If you encounter a tenancy limit, open a case with Oracle to increase the limit and change it to a higher number. 1 may not be enough throughput if the volume of logs written exceeds 1MB/s.
 - e. Click **Create**.
 - f. Click on the created Streams **Stream Information** section.
 - g. Select **OCID**. Record the ID for later use.
 - h. In the same **Stream Information** section, record the **Messages Endpoint** URL for later use.

Create a Service Connector

A Service Connector is required to tell Oracle to ship logs from its logging service to a Stream.

1. Search for Service Connectors.
2. Click **Service Connectors**, and take the following steps.
 - a. In the **Connector Name** field, enter a name, such as "fortisiem-connector".
 - b. In the **Description** field, enter a description, such as "Connector to ship audit logs to fortisiem-stream".
 - c. For **Compartment**, select **Root compartment**.
 - d. For **Source**, select **Logging**.
 - e. For **Target**, select **Streaming**.
 - f. For **Configure Source**, take the following steps.
 - i. In the **Compartment Name** field, enter a name, such as "root compartment".
 - ii. For **Log Group:_Audit**, select checkbox for **Include_Audit in subcompartments**.
 - g. For **Configure Target**, take the following steps.
 - i. For **Compartment**, select **Root Compartment**.
 - ii. For **Stream**, select fortisiem-stream.
 - h. Click **Create**. If the system prompts you to create a default publishing policy to allow Connector to publish logs to stream, click **Create**.

Create a User Group and Add User to the Group

1. Login to Oracle Cloud.
2. Go to **Services > Groups**.
3. Click **Create Group** and take the following steps.
 - a. In the **Name** field, enter a name, such as "fortisiem-group".
 - b. In the **Description** field, enter a description, such as "Group for fortisiem user."
 - c. Click **Create**.
4. Once the group is created, click **Add User to Group**.
5. Select User fortisiem-user, and click **Add**.

Create Policy to Allow User to Consume FortiSIEM-stream

1. Search for **Services > Policies**.
Note: This is done to look for Identity policies.
2. Under **List Scope**, select **Root compartment**.
3. Click **Create Policy**, and take the following steps.
 - a. In the **Name** field, enter a name, such as "fortisiem-policy".
 - b. In the **Description** field, enter a description, such as "Policy for permitting fortisiem-group and fortisiem-user access to pull streams".
 - c. In the **Policy Builder**, select **Show manual editor**.
 - d. Paste this policy, replacing the OCID with the OCID of the Stream that was created earlier.

```
#Template: Allow group <group_name> to use stream-pull in tenancy where target.stream.id =
'<stream_ocid>'
Allow group fortisiem-group to use stream-pull in tenancy where target.stream.id =
'ocid1.stream.oc1.iad.xxxxx'
```

Setup in FortiSIEM

FortiSIEM processes events from Oracle Cloud Infrastructure.

Complete these steps in the FortiSIEM UI:

1. For Multi-tenant users, change the scope to the appropriate FortiSIEM organization you want to configure Oracle OCI for.
2. Go to the **ADMIN > Setup > Credentials** tab.
3. In **Step 1: Enter Credentials**, click **New**.
 - a. Follow the instructions in “[Setting Credentials](#)” in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box, and click **Save** when done.

Settings	Description
Name	Enter a name for the credential.
Device Type	Oracle Cloud Infrastructure
Access Protocol	Streams
Pull Interval	Leave the default.
Message Endpoint	Enter the streams URL you recorded earlier.
Stream OCID	Enter the OCID of the stream created earlier.
User Config File	Upload the config file.
User Private Key	Upload the key.
Log Keyword	Leave the default option, which is OCI_AUDIT_LOG.

4. In **Step 2: Enter IP Range to Credential Associations**, if you have more than one FortiSIEM collector, select the collector that will do the polling from the drop-down list. **Note:** A drop-down list will not appear if you only have one collector.
5. Click **New**.
 - a. Select the credential name you created (during step 3a) from the **Credentials** drop-down list. The **IP/Host Name** field should auto populate the URL.
 - b. Click **Save**.
6. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection.
7. Wait for approximately 5 minutes.
8. Navigate to **ADMIN > Setup > Pull Events** table to check for the new job.
9. Navigate to **ANALYTICS**, and confirm that events appear.


```
optimizer","tenantId":"ocid1.tenancy.oc1..aaaaaaa64d4rod2cgrqleyskgao4wkbeosylqellmeqbvxxkybhonlrbgka","userAgent":"Oracle-JavaSDK/1.33.1 (Linux/4.14.35-2047.507.7.6.el7uek.x86_64; Java/1.8.0_301; Java HotSpot(TM) 64-Bit Server VM GraalVM EE 20.3.3/25.301-b09-jvmci-20.3-b18)","message":"ListAutonomousDatabases succeeded","request":{"action":"GET","headers":{},"id":"ED35F1B2C831403C8FA1B1500476B546/E0454F83ACADEDC84F994F64A6DB8A2C/D8DDC2DE2394258B8964E3C5D2334ECA","parameters":{},"path":"/20160918/autonomousDatabases"},"resourceId":null,"response":{"headers":{},"message":null,"payload":null,"responseTime":"2021-10-14T19:32:02.519Z","status":"200"},"stateChange":{"current":null,"previous":null}},"dataschema":"2.0","id":"125d76e1-3064-4b86-a3f3-ef24fd36b504","oracle":{"compartmentid":"ocid1.tenancy.oc1..aaaaaaaegzp63kezjhyhycdzpmknqs5augg6r7qcgqy5am4lt3h6j3koxkq","ingestedtime":"2021-10-14T19:32:06.259Z","loggroupid":"_Audit","tenantid":"ocid1.tenancy.oc1..aaaaaaa64d4rod2cgrqleyskgao4wkbeosylqellmeqbvxxkybhonlrbgka"},"source":"","specversion":"1.0","time":"2021-10-14T19:32:02.218Z","type":"com.oraclecloud.DatabaseService.ListAutonomousDatabases"}
```

Salesforce CRM Audit

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events for Salesforce Audit](#)

What is Discovered and Monitored

Protocol	Logs Collected	Used For
Salesforce API	Successful/Failed Login, API Query Activity, Dashboard Activity, Opportunity Activity, Report Export Activity, Report Activity, Document Download Activity	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Salesforce Audit" in the **Search** field to see the event types associated with this device.

Reports

There are many reports defined in **RESOURCES > Reports > Device > Application > CRM**

- Salesforce Failed Logon Activity
- Salesforce Successful Logon Activity
- Top Browsers By Failed Login Count
- Top Browsers By Successful Login Count
- Top Salesforce Users By Failed Login Count
- Top Salesforce Users By Successful Login Count
- Top Successful Salesforce REST API Queries By Count, Run Time
- Top Failed Salesforce REST API Queries By Count, Run Time
- Top Salesforce API Queries By Count, Run Time
- Top Salesforce Apex Executions By Count, Run Time
- Top Salesforce Dashboards Views By Count
- Top Salesforce Document Downloads By Count
- Top Salesforce Opportunity Reports By Count
- Top Salesforce Report Exports By Count
- Top Salesforce Reports By Count, Run Time
- Top Salesforce Events

Configuration

- [Salesforce Configuration](#)
- [Define Salesforce Audit Credential in FortiSIEM](#)
- [Create IP Range to Credential Association and Test Connectivity](#)

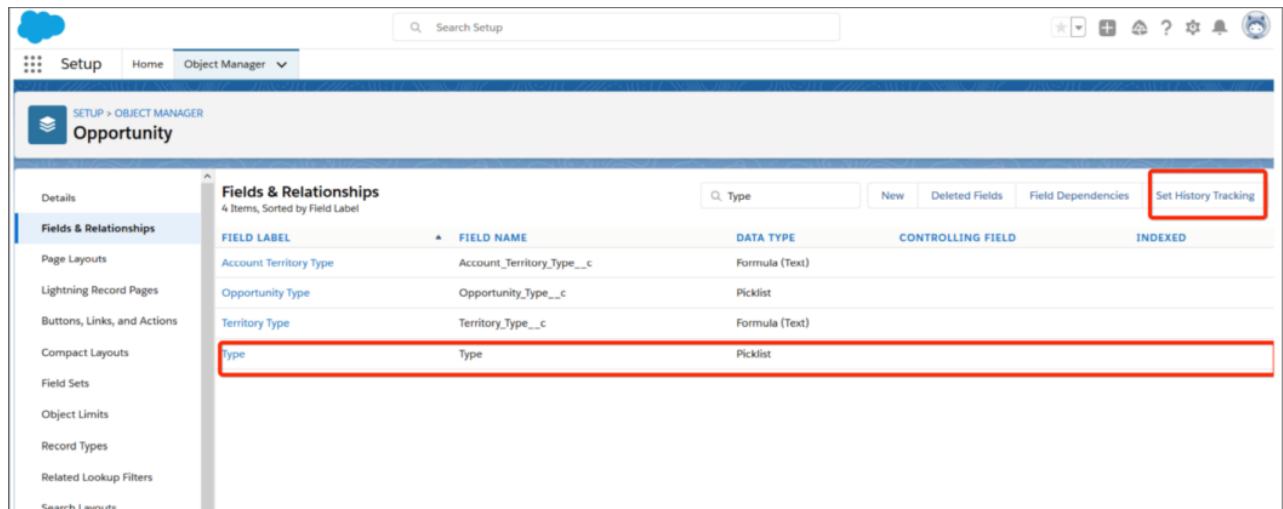
Salesforce Configuration

Note:

1. Salesforce requires the purchase of the Event Monitoring add-on in order to access all event types. See [here](#) for more information.
2. To get to **Object Manager** (Object Management Settings), click **Lightning Experience**. See [here](#) for more information.
3. For more information on how to enable Set History Tracking, please refer to https://help.salesforce.com/articleView?id=sf.updating_picklists.htm&type=5
4. Salesforce saves events in a SQL Database, where FortiSIEM will pull the following events from tables: **EventLogFile, LoginHistory, User, Dashboard, Opportunity, Report** through SQL commands. If you get an error about missing columns, please make sure your administrator has enabled **Set History Tracking** for the missing columns in the tables. The required columns are listed in this table.

Event	Required Columns
EventLogFile	Id, EventType, LogFile, LogDate, LogFileLength, LastModifiedDate, LastModifiedDate
LoginHistory	Id, UserId, LoginTime, Browser, Platform, Status, SourceIp, LoginTime , LoginTime
Dashboard	Id, Description, DeveloperName, FolderName, Title, LastModifiedDate, LastModifiedDate LastModifiedDate
Opportunity	Id, Amount, CloseDate, Name, OwnerId, Type, LastModifiedDate, LastModifiedDate, LastModifiedDate
Report	Id, Name
User	Id, Username

For example, if Type in Opportunity is not enabled in Set History Tracking, FortiSIEM will fail to get events in Opportunity.



Define Salesforce Audit Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

- Go to the **ADMIN > Setup > Credentials** tab.
- In **Step 1: Enter Credentials**:
 - Follow the instructions in “[Setting Credentials](#)” in the User's Guide to create a new credential.
 - Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Salesforce Salesforce Audit
Access Protocol	Salesforce API
Pull Interval	5 minutes
Timeout	30 seconds
Password config	See Password Configuration
User Name	User name for device access
Password	Password for device access
Security Token	Security token
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (From **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter "login.salesforce.com" in the **IP/Host Name** field.
 - b. Select the name of the credential created in the "[Define Salesforce Audit Credential in FortiSIEM](#)" from the **Credentials** drop-down list.
 - c. Click **Save**.
2. 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.
3. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Salesforce Audit Log Collection.

Sample Events for Salesforce Audit

```
[Salesforce_Activity_Perf]:[activityType]=API,[activityName]=get_user_info,  
[srcIpAddr]=23.23.13.166,[user]=user1.my@example.com,[deviceTime]=1458112097,[isSuccess]=false,  
[runTime]=31,[cpuTime]=9,[dbTime]=19434051,[infoURL]=Api
```

Cloud Email Security

FortiSIEM supports the following cloud email security.

- [Fortinet FortiMail Workspace Security](#)
- [Mimecast Cloud](#)

Fortinet FortiMail Workspace Security

Vendor: Fortinet

Product: FortiMail Workspace Security

Support Added: 7.4.x, 7.3.x, 7.2.x, 7.1.x

Product Information: <https://www.fortinet.com/products/fortimail-workspace-security>

Information Collected

FortiMail Workspace Security is a featured cloud-based email defense platform that provides real-time scanning of email, browser security, and collaboration security solutions.

FortiSIEM collects Scans and Audit Log events from FortiMail Workspace Security using **HTTPS_ADVANCED**. The following log types are collected:

FortiMail Workspace API Used	Event Type Prefix for corresponding FortiSIEM Events	Collection Method
Scans API	FortiMail-Workspace-Scan (45 event types)	HTTPS_ADVANCED
Audit Log API	FortiMail-Workspace-Audit (2 event types)	HTTPS_ADVANCED

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

Four steps are involved.

1. Create API Key for FortiMail Workspace Security.
2. Generate Credentials for the Audit Log API and Scans API .
3. Enter the API Credentials in FortiSIEM.
4. Test Credentials in FortiSIEM and Start Event Collection.

Step 1: Create API Key for FortiMail Workspace Security

Follow these steps:

1. Login to FortiMail Workspace portal as a user with at least the Cyber analyst role.
2. Navigate to **Settings > Profile > Security**, and click **Regenerate/Create API Key**.
3. Copy the API key to a secure location. This will be required in [Step 2: Enter API Credentials in FortiSIEM](#).

Step 2: Enter API Credentials in FortiSIEM

Follow these steps:

1. Logon to FortiSIEM via GUI.
2. Navigate to **Admin > Setup > Credentials**.
3. Create a Credential for **Audit Log API** by following the next step.
4. Under **Step 1: Enter Credentials**, click **+**.
 - a. In the **Name** field, enter a name.
 - b. From the **Device Type** drop-down list, select **Fortinet FortiMail Workspace Security**.
 - c. From the **Access Protocol** drop-down list, select **HTTPS Advanced**.
 - d. Download the file [FML_Workspace_Audit_https_advanced_definition.json](#).
 - e. Click **Import Definition**.
 - f. Select the file you just downloaded from step d and click **Import**. Click **Yes** to overwrite.
 - g. Click the **Authentication Parameters** Edit (✎) icon and take the following steps.
 - i. In the **API Key Value** field, enter "Token <Your_API_Key>".
Example: Token 12345abc05cxxx1f4bdc3exxxxxx
 - ii. Click **OK**.
 - h. Click the **General Parameters** Edit (✎) icon, and take the following steps.
 - i. Confirm that Host Name matches the API endpoint as specified in FortiMail Workspace portal. By default, it is `api.perception-point.io`.
 - ii. Click **OK**.
 - i. Click **Save**.
5. Create a Credential for **Scans API** by repeating step 4 with these differences:
 - a. In step 4d, download the following file:
[FML_Workspace_Scans_https_advanced_definition.json](#)

Step 3: Test above Credentials in FortiSIEM and Start Event Collection

1. Create an association for **Audit Log API** by following steps 2-6.
2. Under **Step 2: Enter IP Range to Credential Associations**, click **+**.
3. From the **Device Credential Mapping Definition** dialog box:
 - a. From the **Credentials** drop-down list, select the Audit Log API Credential.
 - b. Confirm that "api.perception-point.io" appears in the **IP/Host Name** field.
 - c. Click **Save**.
4. Select the credential just created.
5. Click the **Test** drop-down and select **Test Connectivity without Ping**.

6. If successful, the new job will appear in the **Admin > Setup Pull Events** table.
Events can then be queried in **Analytics** by filtering: Event Type CONTAIN "FortiMail-Workspace-Audit".
7. Create an association for **Scans API** by following steps 2-6 with the following changes.
 - a. In step 3a, choose the Scans API Credential.
 - b. In Step 6, use the query filter Event Type CONTAIN "FortiMail-Workspace-Scan"

Mimecast Cloud

FortiSIEM Support added: 7.2.0

Vendor: Mimecast

Vendor version tested: Mimecast API 2.0

Product Information: <https://www.mimecast.com/>

- [Overview](#)
- [Configuring Mimecast](#)
- [Checking for Events](#)
- [Rules](#)
- [Reports](#)
- [Dashboard](#)
- [Appendix](#)

Overview

Mimecast provides cloud-based services for email security, archiving, and continuity.

FortiSIEM supports ingesting various logs relating to email activity, and activity within the Mimecast portal such as archive, search, and view logging. For details on how FortiSIEM uses Mimecast API, see [Appendix - Mimecast API Information](#).

Configuring Mimecast

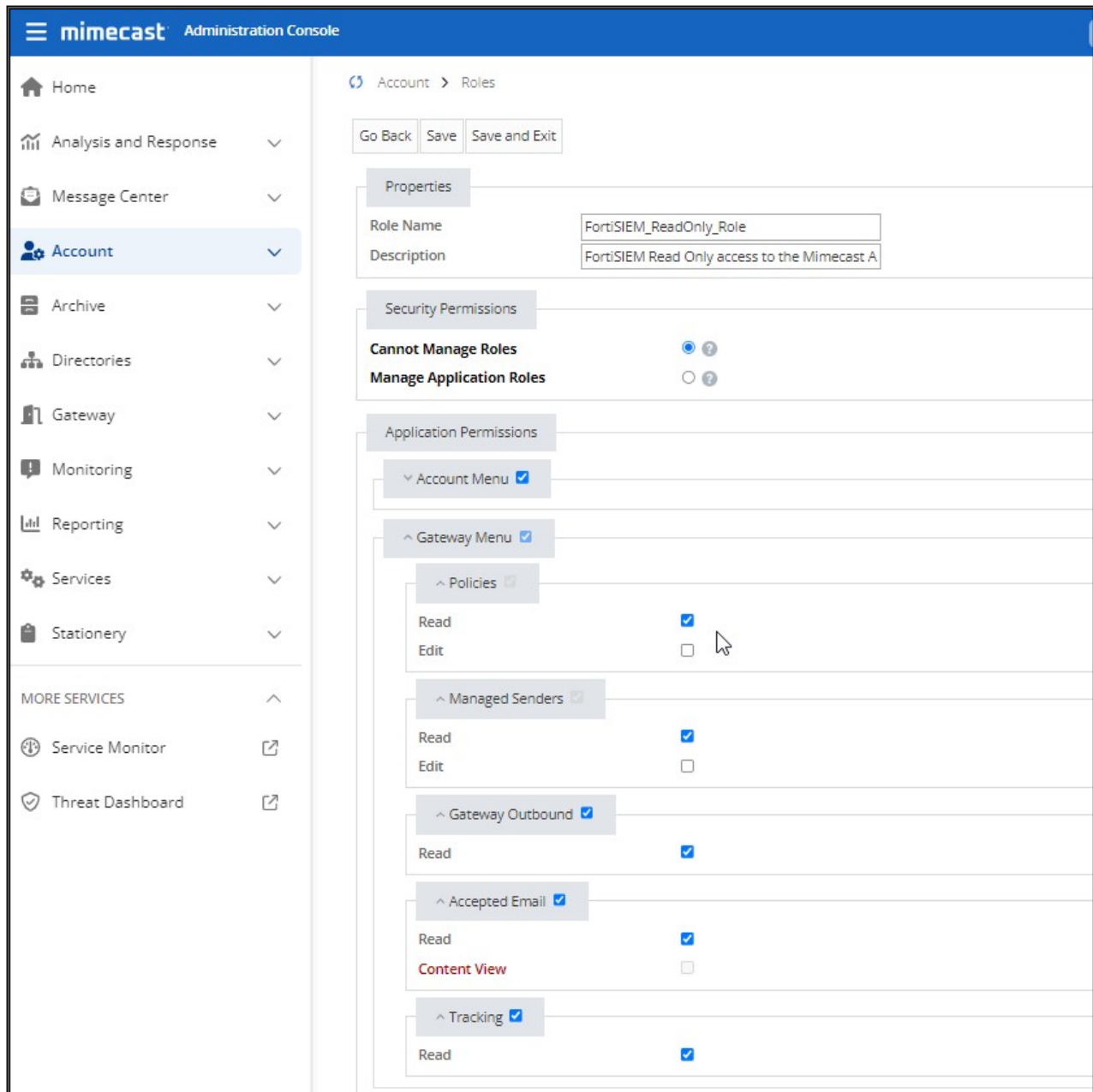
- [Step 1 - Define a Role with Necessary Permissions](#)
- [Step 2 - Define a New API Application Integration](#)
- [Step 3 - Configure FortiSIEM](#)

To configure Mimecast, you must create an application with appropriate permissions and subsequently generate an oauth2.0 client ID and client secret. After these steps are completed, you can then configure FortiSIEM.

Note: In the future, FortiSIEM will have a predefined API2.0 application tile in Mimecast portal, but in the interim, you must manually define the role and application here.

Step 1 - Define a Role with Necessary Permissions

1. Login to Mimecast Administration Console.
2. Navigate to **Account > Roles**.
3. Click **New Role**.
4. In the **Role Name** field, enter a name, such as "FortiSIEM_ReadOnly_Role".
5. In the **Description** field, enter a description, such as "FortiSIEM Read Only access to the Mimecast API".
6. For **Security Permissions**, select the **Cannot Manage Roles** button.
7. Under **Application Permissions**, for every single application permission drop-down, modify the permission so only **Read** is enabled.
8. When every single permission is set with "Read only", at the very top of the list, click the **Save and Exit** button.



Reference: <https://community.mimecast.com/s/article/api-integrations-managing-api-2-0-for-cloud-gateway>

Step 2 - Define a New API Application Integration

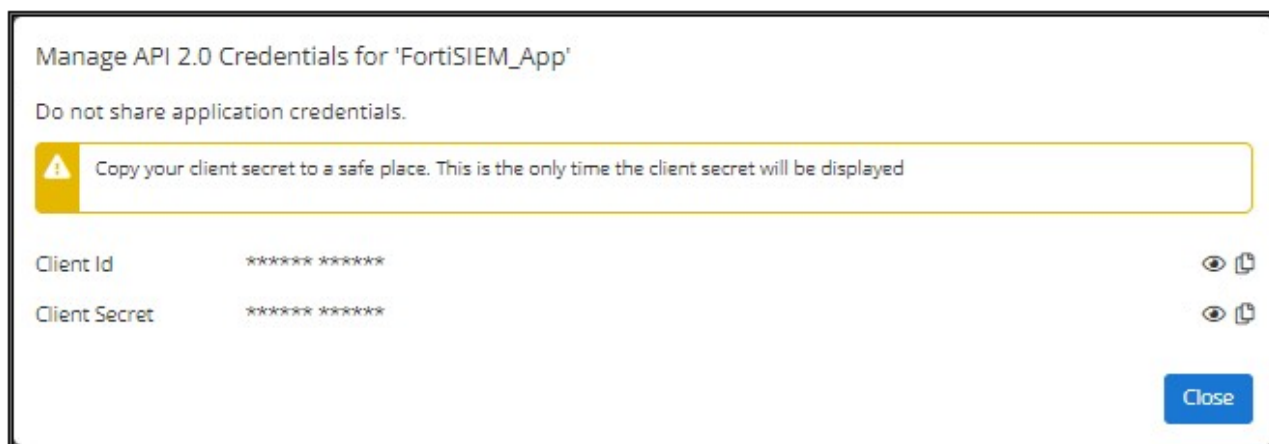
1. Login to the Mimecast Administration Console.
2. Navigate to **Services > API and Platform Integrations**.
3. Select the tile **Mimecast API 2.0** at the top of the list.
4. On the next page, read and accept the disclaimer, and click **Next**.
5. On the Application Details page, set up the following:

- a. In the **Application Name** field, enter a names, such as "FortiSIEM_App".
- b. From the **Category** drop-down list, select **SIEM Integration**.
- c. From the **Products** drop-down list, select all of them.
- d. From the **Application Role** drop-down list, select the role you created earlier. If you used the example suggestion, it should be "FortiSIEM_ReadOnly_Role".
- e. In the **Description** field, enter a description, such as "FortiSIEM integration with Mimecast 2.0 API".

The screenshot shows the Mimecast Administration Console interface. On the left is a navigation menu with options like Home, Analysis and Response, Message Center, Account, Archive, Directories, Gateway, Monitoring, Reporting, Services (selected), Stationery, and MORE SERVICES. The main content area is titled 'Add Mimecast API 2.0 Application' and shows a progress bar with four steps: 1. Disclaimer (completed), 2. Details (current step), 3. Notifications, and 4. Summary. The 'Details' step contains the following fields:

- Application Name ***: Text input field containing 'FortiSIEM_App'.
- Category ***: Dropdown menu showing 'SIEM Integration'.
- Products ***: Dropdown menu showing 'Threats, Security Events and Data for CG, Email Security Clou...'.
- Application Role ***: Dropdown menu showing 'FortiSIEM_ReadOnly_Role'.
- Description ***: Text area containing 'FortiSIEM integration with Mimecast 2.0 api'.

- f. At the bottom right corner, click **Next**.
6. On the next page, enter the Notification Settings.
 - a. In the **Technical Point of Contact** field, enter the name of the primary technical point of contact. You can provide a group contact instead of an individual.
7. In the **Email** field, enter the email address of the primary technical point of contact.
8. On bottom right corner, click **Next**.
9. On the last page click **Add and Generate Keys**.
A pop up will appear with the Client ID and Client Secret for the application.



The pop up will only appear once.

10. Store the Client ID and Client Secret securely in a password management utility. These will be needed to configure FortiSIEM shortly.
11. Click **Close** to navigate away from the credentials.

Reference: <https://community.mimecast.com/s/article/api-integrations-managing-api-2-0-for-cloud-gateway>

Step 3 - Configure FortiSIEM

Prerequisites: A valid Mimecast application created with the necessary permissions, and associated Client ID and Client Secret.

FortiSIEM configuration is comprised of two main steps.

- [Define Mimecast Credential](#)
- [Create IP Range to Credential Association and Test Connectivity](#)

Define Mimecast Credential

Log in to the FortiSIEM Supervisor node, and take the following steps.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, such as "Mimecast_CG".
Device Type	Mimecast Cloud Gateway
Access Protocol	MIMECAST_API
Pull Interval	5 Minutes is the default. Leave as is unless there is a specific reason to change.

Settings	Description
Client ID	Enter/paste the Client ID from the Mimecast application credential.
Client Secret/Confirm Client Secret	Enter/paste the Client Secret associated with the client ID from the Mimecast application credential.
Description	Description of the device, such as "Mimecast FortiSIEM credential".

Access Method Definition ✕

Name:

Device Type:

Access Protocol:

Pull Interval: Minute(s)

Client ID:

Client Secret:

Confirm Client Secret:

Description:

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps.

1. In **Step 2: Enter IP Range to Credential Associations**, if the organization has more than 1 collector, select the collector from the drop-down list that will do the API polling. If the organization has 1 or no collectors, there is no drop-down and you can proceed to the next step.

2. Click **New** to create a new association.
 - a. Select the name of the credential created in the **Define Mimecast Credential** from the **Credentials** drop-down list. If you used the example, it would be "Mimecast_CG".
 - b. The **IP/Host Name** field will auto-populate. If you would like to use a region specific base URL, you can change the **IP/Host Name** field. For more information, see [Appendix - Regional Endpoints](#) for specific URLs.
 - c. Click **Save**.

Device Credential Mapping Definition

IP/Host Name:

Credentials:

3. Select the entry just created, click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling. A pop up will appear and show the Test Connectivity results.

Step 2: Enter IP Range to Credential Associations

New Edit Delete Test Search...

Test Connectivity
Test Connectivity without Ping

Name/IP/IP Range	Credential Name
api.services.mimecast.com	Mimecast_CG

You should expect a success response here. Afterward, the initial event pulling job will be scheduled. It should take approximately 5 minutes for the first job to kick off.

4. Go to **ADMIN > Setup > Pull Events** to observe the job progress.

Storage Organizations Credentials Discovery **Pull Events** Monitor Performance STM Maintenance Windows Agent Linux Agent FortiSIEM Manager

☒ All ☐ Errors Edit Apply Export Report Search... Org without collector

Enabled	Device Name	Access IP	Device Type	Organization	Method
☒	api.services.mimecast.com			Super	★ Mimecast_CG (MIMECAST_API)

- A yellow star means a job is scheduled for the first time and has not yet kicked off.
- A green checkbox means a successful poll (as of the last attempt)
- A yellow exclamation or other symbol next to the job indicates an error.

Checking for Events

To check for events, take the following steps.

1. Navigate to **Analytics > Search**.
2. Click in the **Edit Filters and Time Range...** field.
 - a. In the **Attribute** field, enter/select **Event Type**.
 - b. From the **Operator** drop-down list, select **CONTAIN**.
 - c. In the **Value** field, enter "Mimecast".
 - d. Under **Time Range**, in the Last field, enter "1".
 - e. Under **Time Range**, from the time unit drop-down list, select **Hour**.
 - f. Click **Apply & Run**.

The screenshot shows the FortiSIEM Search interface. At the top, there are tabs for 'Search', 'Machine Learning', and 'Investigation'. Below these, there's a search bar and a filter section. The 'Edit Filters and Time Range...' dialog box is open, showing a filter rule: 'Event Type' (Attribute) 'CONTAIN' (Operator) 'Mimecast' (Value). The 'Time Range' section is set to 'Relative' with 'Last 1 Hour'. The 'Trend Interval' is set to 'Auto'. The 'Result Limit' is set to '100 K rows'. The 'Apply & Run' button is highlighted in blue.

Rules

Note that the following is an example, and non-exhaustive. Navigate to **Resources > Rules** and search for "mimecast" in the main **Search...** field to see available rules.

- Mimecast: User clicked malicious link in email

Reports

Note that the following are examples, and non-exhaustive. Navigate to **Resources > Reports** and search for "mimecast" in the main **Search...** field to see available reports.

- Mimecast: Clicked Malicious or Unsafe URL Details
- Mimecast: External Email Count
- Mimecast: Inbound Email Count
- Mimecast: Internal Email Count
- Mimecast: Outbound Email Count
- Mimecast: Top Clicked Malicious or Unsafe URLs

- Mimecast: Top delivery errors by code
- Mimecast: Top delivery errors by reason
- Mimecast: Top Inbound Mail Senders
- Mimecast: Top internal mail senders without TLS encryption
- Mimecast: Top malware found in emails
- Mimecast: Top malware receivers
- Mimecast: Top malware senders
- Mimecast: Top Message Held Reasons
- Mimecast: Top Outbound Mail Senders
- Mimecast: Top Recipients Clicking on Malicious or Unsafe URLs
- Mimecast: Top Senders and Receivers
- Mimecast: Top Senders with Held Messages
- Mimecast: Top Spam Recipients
- Mimecast: Top Spam Senders
- Mimecast: Top Spam Senders by Source IP
- Mimecast: Top Spam Types by Count
- Mimecast: Top TLS versions used

Dashboard

From the FortiSIEM GUI, navigate to **Dashboard**, and from the Dashboard drop-down list, select **Mimecast**. An **Overview** and **Threats** dashboard are available by clicking on the appropriate tab.

Note: Only visible under **Admin View - Local** or Organization Scope.

Appendix

- [Mimecast API Information](#)
- [Notes on Monitoring with Mimecast](#)
- [Regional Endpoints](#)

Mimecast API Information

FortiSIEM utilizes the MimeCast 2.0 APIs to provide ingestion of common auditing data points.

Default Base URL: api.services.mimecast.com

OAUTH2.0 Token Endpoint: - /oauth/token

API	Associated Permissions
/api/email/get-email-queues	Account Dashboard Read
/api/archive/get-archive-search-logs	Archive Search Logs Read

API	Associated Permissions
/api/archive/get-search-logs	Archive Search Logs Read
/api/archive/get-view-logs	Archive View Logs Read
/api/dlp/get-logs	Monitoring Data Leak Prevention Read
/api/ttp/attachment/get-logs	Monitoring Attachment Protection Read
/api/ttp/impersonation/get-logs	Monitoring Impersonation Protection Read
/api/ttp/url/get-logs	Monitoring URL Protection Read
/api/audit/get-audit-events	Account Logs Read
/siem/v1/batch/events/cg	Security Events and Data Retrieval Threat and Security Events (SIEM) Read permission
/threats/v1/stats/attachment-scans	
/threats/v1/stats/url-clicks	
/threats/v1/stats/impersonations	Security Events and Data Retrieval Threat and Security Events (SIEM) Read permission

Notes on Monitoring with Mimecast

While the default polling interval from FortiSIEM is every 5 minutes, the Mimecast SIEM batch API can only be called every 15 minutes. This is enforced by Mimecast, so be aware that there is an intentional delay from the time some events occur and when they are available in FortiSIEM.

Regional Endpoints

Base URL Region	Host
Europe (EU) [Excluding Germany]	https://eu-api.mimecast.com
Germany (DE)	https://de-api.mimecast.com
United States of America (US)	https://us-api.mimecast.com
United States of America (USB)	https://usb-api.mimecast.com
USPCOM	https://uspcom-api.mimecast-pscom-us.com
Canada (CA)	https://ca-api.mimecast.com
South Africa (ZA)	https://za-api.mimecast.com
Australia (AU)	https://au-api.mimecast.com
Offshore	https://je-api.mimecast.com

Console Access Devices

FortiSIEM supports this console access device for discovery and monitoring.

- [Lantronix SLC Console Manager](#)

Lantronix SLC Console Manager

- What is Discovered and Monitored
- Event Types
- Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Admin access, Updates, Commands run	Log analysis and compliance

Event Types

The complete list of Lantronix SLC log event types can be found in **ADMIN > Device Support > Event Types** by searching for "Lantronix-SLC". Some important ones are:

- Lantronix-SLC-RunCmd
- Lantronix-SLC-Update
- Lantronix-SLC-User-Logon-Success

Configuration

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example Syslog

```
<174>xmsd: gen/info-Syslog server changed to 10.4.3.37
<38>xwsd[32415]: auth/info-Web Authentication Success for user andbr003
```

Customer Relationship Management

FortiSIEM supports the following customer relationship management.

- Workday Enterprise Suite (Workday Report API via Generic HTTPS Poller)

Workday Enterprise Suite (Workday Report API via Generic HTTPS Poller)

Workday has a flexible reports service that lets Workday users define columns and details around report parameters. These reports can then be executed against data in the Workday UI. These reports are also available using a REST API web service in the following format:

```
https://wd2-impl-services1.workday.com/ccx/service/customreport2/<tenantId_here>/<username_here>/<report_name_here>
```

For example:

```
https://wd2-impl-services1.workday.com/ccx/service/customreport2/MyCustomTenant/ExampleReportUser/UserListReport
```

URL Component	Description
wd2-impl-services1.workday.com	Hostname of report API
MyCustomTenant	The workday tenant name
ExampleReportUser	The Workday username of the user who owns the custom reports
UserListReport	The report name as defined in Workday UI

Note: The reports exposed via API being discussed here are from the Workday UI, and should not be confused with FortiSIEM reports.

When Workday users have crafted reports, these reports can be exported in Excel representations of that reports setup, so it can be recreated in other tenants. The FortiSIEM team has generated a set of Excel representations of common Workday reports that can be properly parsed by FortiSIEM.

Please download the following Excel spreadsheets and repeat the input options in your Workday tenant to create your reports. Also, ensure that the authorized user

account FortiSIEM needs to retrieve the report is either the owner of the report, or authorized to execute/view it.

- [BusinessProcesses.xlsx](#)
 - [Domain_SecurableItems.xlsx](#)
 - [Domains.xlsx](#)
 - [FunctionalAreas.xlsx](#)
 - [Organizations.xlsx](#)
 - [SecurityGroup_Details.xlsx](#)
 - [SecurityGroups.xlsx](#)
 - [SystemAccountSignons.xlsx](#)
 - [Users.xlsx](#)
-
- [All Workday Excel files in one zip file](#)

Contact your Workday solutions support team if you have issues generating the Workday reports. Workday customers have access to detailed documentation on setting up a

report and exposing it via API. The defined excel documents here represent all the GUI options prompted for the setup of each standard report.

FortiSIEM makes use of the "Generic HTTPS Poller" in FortiSIEM 6.6.0 and later to integrate with the Workday Reports API.

For more information on this type of integration, see [Generic Log API Poller \(HTTPS Advanced\) Integration](#) in the [Appendix](#).

General Steps

For this integration, you will be taking the following general steps.

1. Define Workday user account with basic authentication for your tenant.
2. Define Reports in Workday UI and enable them as a web service (allow them to be retrieved via API). Follow the excel representations of each report linked in this guide.
3. Configure FortiSIEM's Generic Log API Poller (Credential type HTTPS ADVANCED under Access Protocols in FortiSIEM Credential configuration).
4. Test connectivity to Reports API and confirm events are ingested.
5. Define any Rules or Reports as desired.

Configuration

- [Setup in Workday](#)
- [Setup in FortiSIEM](#)
 - [Walkthrough Example using SystemAccountSignons](#)
 - [Walkthrough Example using Users \(Workday Report\)](#)

Setup in Workday

Take the following steps from Workday

Creating a Workday User Account

1. Login to Workday.
2. Create a Workday user account.
 - a. In the **Label** field, enter the unique name of the account.
 - b. In the **Username** field, enter the username of the account.
 - c. In the **Password** field, enter the password associated with the username.
 - d. In the **Tenant** field, enter the Workday tenant.
 - e. In the **Host** field, enter the hostname.
 - f. In the **Version** field, enter the Workday version.
3. Use the Excel spreadsheets to re-create the settings from your own Workday tenant.
 - [BusinessProcesses.xlsx](#)
 - [Domain_SecurableItems.xlsx](#)
 - [Domains.xlsx](#)
 - [FunctionalAreas.xlsx](#)
 - [Organizations.xlsx](#)
 - [SecurityGroup_Details.xlsx](#)
 - [SecurityGroups.xlsx](#)
 - [SystemAccountSignons.xlsx](#)
 - [Users.xlsx](#)
 - [Download of all above Workday Excel spreadsheets via zip file](#)

Setup in FortiSIEM

To configure a FortiSIEM credential, take the following steps.

Note: A unique credential is required for each report endpoint. So in this situation, 9 credentials (one for each report) will need to be created.

FortiSIEM provides support by default for the following standard reports:

Report	Description
BusinessProcesses	List of all business processes (not time series data)
Domain_SecurableItems	List of domain securable items
Domains	List of all domains (not time series data)
FunctionalAreas	List of all functional areas (not time series data)

Report	Description
Organizations	List of all organizations in a tenant (not time series data)
SecurityGroups	List of all security groups (not time series data)
SecurityGroup_Details	List of details for security groups (not time series data)
SystemAccountSignons	Audit logon history for a given time interval (This is time series audit log data)
Users	List of users and their status of active/inactive (not time series data)

You can define any number of custom reports, but you will have to extend the WorkdayParser to handle new fields and eventTypes. Consult the [parser training course/documentation](#) or [professional services](#) for more information.

1. Login to FortiSIEM GUI.
2. Navigate to **ADMIN > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the Access Method Definition window, take the following steps.
 - a. In the **Name** field, enter a name for the credential representing the API endpoint, for example, "Workday_<Workday_Report>".
 - b. From the **Device Type** drop-down list, select **Workday Enterprise Suite**.
 - c. Ensure the **Access Protocol** drop-down list has **HTTPS Advanced** selected. If it does not, select it from the drop-down list.
 - d. In the **Pull Interval** field, set the pull interval. The default is 5 minutes.
 - e. Click the Edit icon in the **General Parameters** row.
 - i. In the **Host Name** field, enter the Workday report API hostname. This will likely be "wd2-impl-services1.workday.com".
 - ii. In the **URI Stem** field, replace the "<XXXX_here>" information with your report API endpoint information, following this format.
/ccx/service/customreport2/<tenantId_here>/<username_here>/<report_name>
 - iii. From the **HTTP Method** drop-down list, select **GET**.
 - iv. In the **Log Header** field, enter "Workday_HTTP_API <Report_Entry>:"
 - v. Click **OK**.
Note: The other options in **General Parameters** do not need to be checked.
 - f. Click on the Edit icon in the **Authentication Parameters** row.
 - i. In the **User Name** field, enter the Workday user's username that owns the reports, or has access to the reports.
 - ii. In the **Password** field, enter the password associated with the Workday username.
 - iii. In the **Confirm Password** field, re-enter the password associated with the Workday username.
 - iv. Click **OK**.
 - g. Click on the Edit icon in the **Log API Parameters** row.
 - i. Configure the Log API. For information, see [Log API Configuration](#) in [Generic Log API Poller \(HTTPS Advanced\) Integration](#).
Note: A full walkthrough example using SystemAccountSignons is available to view to see how the API parameters from_Moment and to_Moment should be configured.

- h. Click **Save**.
5. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
6. From the **Credentials** drop-down list, select the Credentials you just created. The **IP/Host Name** field will auto-populate.
7. Verify that the **IP/Host Name** field information is correct.
8. Click **Save**.
9. Select the Workday credential, click the **Test** drop-down list, and select **Test Connectivity without Ping** to start the polling job.
10. From the top horizontal tab selection, click **Pull Events** to verify job. You should see a yellow star symbol next to the new polling job. If the pull interval was left at its 5 minutes default, it should take approximately 5 minutes for the first job to execute. Afterwards, a green checkbox will appear instead of a yellow star.
11. Click **ANALYTICS**, and run a query such as EventType CONTAIN Workday-.
 - a. Select the **Edit Filters and Time Range...** field
 - b. Under **Filter**, select **Event Attribute**.
 - c. Under **Attribute**, select/enter **Event Type**.
 - d. From the **Operator** drop-down list, select **CONTAIN**.
 - e. Under **VALUE**, enter "Workday-".
 - f. Click **Apply & Run**.

Walkthrough Example using SystemAccountSignons

There are two major categories of logging APIs:

- Those with time-series data, where we have to specify a time range in the API Query
- Non time-series reporting data, e.g. a list of users

In the case of SystemAccountSignons, although it offers a complete list of signons since the beginning of time of the initial poll interval, we can configure it so it only provides the signons from the given poll interval.

To configure this, you need to understand that in the standard report defined in Workday called SystemAccountSignons, it has time range arguments called from_Moment and to_Moment. These are populated by FortiSIEM using the following template, called Workday-SystemAccountSignongs_https_advanced_definition.json, which is available for download [here](#).

We will use this JSON config template shortly. Take the following steps:

1. Login to FortiSIEM GUI.
2. Navigate to **ADMIN > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the Access Method Definition window, take the following steps.
 - a. In the **Name** field, enter a name for the credential representing the API endpoint, for example, "Workday_SystemAccountSignons".
 - b. From the **Device Type** drop-down list, select **Workday Enterprise Suite**.
 - c. Ensure the **Access Protocol** drop-down list has **HTTPS Advanced** selected. If it does not, select it from the drop-down list.
 - d. In the **Pull Interval** field, set the pull interval. The default is 5 minutes.
 - e. Click **Import Definition** in the lower left part of the Access Method Definition window.

- f. Select the file Workday-SystemAccountSignons_https_advanced_definition.json, and when prompted with the message "Definition will be overwritten, continue?", click **Yes**.
At this point, several parameters will be auto-filled, but some additional configuration is required.
 - g. Click the Edit icon in the **General Parameters** row.
 - i. In the **Host Name** field, enter the Workday report API hostname if it is different than wd2-impl-services1.workday.com.
 - ii. In the **URI Stem** field, replace the "<XXXX_here>" information with your report API endpoint information, following this format.
`/ccx/service/customreport2/<tenantId_here>/<username_here>/FN_SystemAccountSignons`
 - iii. Click **OK**.
Note: The other options in **General Parameters** do not need to be checked.
 - h. Click on the Edit icon in the **Authentication Parameters** row.
 - i. In the **User Name** field, enter the Workday user's username that owns the reports, or has access to the reports.
 - ii. In the **Password** field, enter the password associated with the Workday username.
 - iii. In the **Confirm Password** field, re-enter the password associated with the Workday username.
 - iv. Click **OK**.
 - i. Click **Save**.
Note: The log API parameters have already been auto-filled for time series polling using the API parameters from_Moment and to_Moment for SystemAccountSignons API report in **Log API Parameters**.
5. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
6. From the **Credentials** drop-down list, select the Credentials you just created. The **IP/Host Name** field will auto-populate.
7. Verify that the **IP/Host Name** field information is correct.
8. Click **Save**.
9. Select the Workday credential, click the **Test** drop-down list, and select **Test Connectivity without Ping** to start the polling job.
10. From the top horizontal tab selection, click **Pull Events** to verify job. You should see a yellow star symbol next to the new polling job. If the pull interval was left at its 5 minutes default, it should take approximately 5 minutes for the first job to execute. Afterwards, a green checkbox will appear instead of a yellow star.
11. Click **ANALYTICS**, and run a query such as EventType CONTAIN Workday-.
 - a. Select the **Edit Filters and Time Range...** field
 - b. Under **Filter**, select **Event Attribute**.
 - c. Under **Attribute**, select/enter **Event Type**.
 - d. From the **Operator** drop-down list, select **CONTAIN**.
 - e. Under **VALUE**, enter "Workday-".
 - f. Click **Apply & Run**.

Walkthrough Example using Users (Workday Report)

Users uses the exact same process for setting up a credential that SystemAccountSignons does, except the template does not need any time-series configuration (There are no API arguments for time, a full list of attributes is pulled each time).

Download the Workday Users Report Excel definition [here](#).

Download the FortiSIEM Credential Definition json file for Workday Users, WorkdaySystem-Users_https_advanced_definition.json, [here](#).

1. Login to FortiSIEM GUI.
2. Navigate to **ADMIN > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the Access Method Definition window, take the following steps.
 - a. In the **Name** field, enter a name for the credential representing the API endpoint, for example, "Workday_System-Users".
 - b. From the **Device Type** drop-down list, select **Workday Enterprise Suite**.
 - c. Ensure the **Access Protocol** drop-down list has **HTTPS Advanced** selected. If it does not, select it from the drop-down list.
 - d. In the **Pull Interval** field, set the pull interval. The default is 5 minutes.
 - e. Click **Import Definition** in the lower left part of the Access Method Definition window.
 - f. Select the file WorkdaySystem-Users_https_advanced_definition.json, and when prompted with the message "Definition will be overwritten, continue?", click **Yes**.
At this point, several parameters will be auto-filled, but some additional configuration is required.
 - g. Click the Edit icon in the **General Parameters** row.
 - i. In the **Host Name** field, enter the Workday report API hostname if it is different than wd2-impl-services1.workday.com.
 - ii. In the **URI Stem** field, replace the "<XXXX_here>" information with your report API endpoint information, following this format.
/ccx/service/customreport2/<tenantId_here>/<username_here>/FN_Users
 - iii. Click **OK**.
Note: The other options in **General Parameters** do not need to be checked.
 - h. Click on the Edit icon in the **Authentication Parameters** row.
 - i. In the **User Name** field, enter the Workday user's username that owns the reports, or has access to the reports.
 - ii. In the **Password** field, enter the password associated with the Workday username.
 - iii. In the **Confirm Password** field, re-enter the password associated with the Workday username.
 - iv. Click **OK**.
 - i. Click **Save**.
5. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
6. From the **Credentials** drop-down list, select the Credentials you just created. The **IP/Host Name** field will auto-populate.
7. Verify that the **IP/Host Name** field information is correct.
8. Click **Save**.
9. Select the Workday credential, click the **Test** drop-down list, and select **Test Connectivity without Ping** to start the polling job.
10. From the top horizontal tab selection, click **Pull Events** to verify job. You should see a yellow star symbol next to the new polling job. If the pull interval was left at its 5 minutes default, it should take approximately 5 minutes for the first job to execute. Afterwards, a green checkbox will appear instead of a yellow star.

11. Click **ANALYTICS**, and run a query such as EventType CONTAIN Workday-.
 - a. Select the **Edit Filters and Time Range...** field
 - b. Under **Filter**, select **Event Attribute**.
 - c. Under **Attribute**, select/enter **Event Type**.
 - d. From the **Operator** drop-down list, select **CONTAIN**.
 - e. Under **VALUE**, enter "Workday-".
 - f. Click **Apply & Run**.

Digital Risk Protection

FortiSIEM supports the following digital risk protection (DRP).

- [Fortinet FortiRecon](#)

Fortinet FortiRecon

Support Added: FortiSIEM 7.1.0

Vendor Version Tested: FortiRecon 23.3

Vendor: Fortinet

Product Information: <https://www.fortinet.com/products/fortirecon>

- [Configuring Generic Poller for FortiRecon API Events](#)
- [Sample Events](#)

Configuring Generic Poller for FortiRecon API Events

FortiSIEM uses the integration type (HTTPS Advanced), otherwise known as the "Generic Log API Poller," to ingest data from FortiRecon API on a recurring interval.

To configure, you will define an HTTPS Advanced credential for each API endpoint to collect data from that endpoint.

FortiSIEM out of the box provides parsing for the following FortiRecon APIs.

- `/aci/<org_id>/iocs` - Displays any indicators of compromise.
- `/aci/<org_id>/leaked_cards` - Displays any detected leaked credit or debit cards for your organization.
- `/aci/<org_id>/reports` - Displays latest breach/attack/campaigns/data leaks seen on web using a variety of intelligence sources - general information not specific to your org.
- `/bp/<org_id>/rogue_apps` - Publicly known Rogue or Malicious app list, and the number of known downloads of that application, not specific to your org.
- `/bp/<org_id>/domain_threats` - Domain threat list for the monitored organization.
- `/easm/<org_id>/exposed_services` - Information on services exposed to the public internet for the monitored organization.
- `/easm/<org_id>/issues` - Detected issues for scanned externally visible assets in your organization.
- `/easm/<org_id>/leaked_creds` - Displays any detected leaked credentials for your organization.
- `/easm/<org_id>/scan_statistics` - Statistical information on the EASM scan for the monitored organization.

Definitions:

ACI - Adversary Centric Intelligence

BP - Brand Protection

EASM - External Attack Surface Management

<org_id> - Placeholder to be replaced by actual FortiRecon organization ID

Additional details:

<https://fndn.fortinet.net/index.php?/fortiapi/2232-fortirecon/>

<https://docs.fortinet.com/product/fortirecon/>

- [Preparation](#)
- [Setup in FortiSIEM](#)
- [Starting the Event Pulling](#)

Preparation

1. Login to FortiRecon and generate an API Key, which will be needed for your HTTPS Advanced credential definitions.
2. Obtain your FortiRecon Tenant/Organization ID, which is used in the URL path of many API calls for FortiRecon.
3. Confirm the base API hostname. As of this writing, it is: api.fortirecon.forticloud.com.

Setup in FortiSIEM

The following showcases two methods to set up a single API endpoint (Leaked Cards). This process must be repeated for each API endpoint. After following the Easy or Manual Method, proceed to [Starting the Event Pulling](#).

- [Easy Method](#)
- [Manual Method \(Defining the API Components\) - Leaked Cards Walkthrough](#)

Easy Method

1. Download the following JSON file: [FortiRecon_Generic_Poller_Templates.zip](#) and unzip to your local computer.

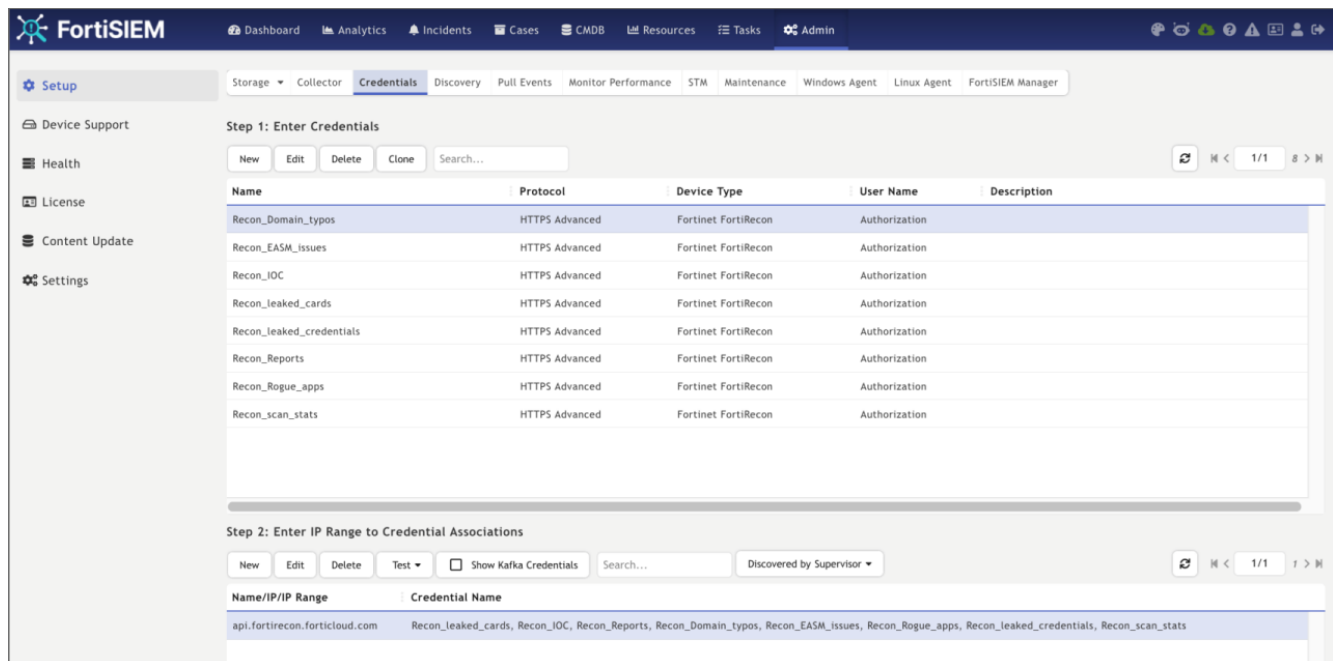
The file should contain the templates files:

- FORTIRECON_ACI_IOC.json
- FORTIRECON_ACI_LEAKED_CARDS.json
- FORTIRECON_ACI_REPORTS.json
- FORTIRECON_BP_ROGUE_APPS.json
- FORTIRECON_BP_DOMAIN_THREATS.json
- FORTIRECON_EASM_EXPOSED_SERVICES.json
- FORTIRECON_EASM_ISSUES.json
- FORTIRECON_EASM_LEAKED_CREDS.json
- FORTIRECON_EASM_SCAN_STATS.json

2. Navigate to **Admin > Setup > Credentials**, and under **Step 1: Enter Credentials**, click **New**.
 - a. In the **Name** field, enter the name of the FortiRecon API endpoint you wish to add. For example, for FORTIRECON_ACI_LEAKED_CARDS.json, you might enter the name "FortiRecon_LeakedCards".
 - b. In **Device Type**, enter/select "Fortinet FortiRecon".

- c. Click **Import Definition** in the bottom window and select the appropriate json file. For example, for "Leaked cards" you would select the FORTIRECON_ACI_LEAKED_CARDS.json file, and click **Import**.
 - d. When prompted to overwrite the definition, click **Yes** to overwrite the config.
 - e. In the **General Parameters** row, click the Pencil icon.
 - i. In the **URI Stem** field, replace *<yourOrgID>* with your FortiRecon organization ID.
 - ii. Click **OK**.
 - f. In the **Authentication Parameters** row, click the Pencil icon.
 - i. In the **API Key Name** field, ensure it is "Authorization".
 - ii. In the **API Key Value** field, enter/paste your FortiRecon API key.
 - iii. Click **OK**.
 - g. Click **Save** at bottom of the Access Method Definition window.
3. Repeat the instructions from [step 2](#) for the remaining JSON files, as each of the FortiRecon API endpoints requires a separate credential to be defined. Also, make sure to change the **Name** field to reflect each of the FortiRecon credentials. For example, use the name "FortiRecon_IOC" for the FORTIRECON_ACI_IOC.json file.

When complete, your FortiRecon credentials should look similar to the following:



Manual Method (Defining the API Components) - Leaked Cards Walkthrough

After logging in to FortiSIEM, take the following steps.

1. Navigate to **Admin > Setup > Credentials**, and under **Step 1: Enter Credentials**, click **New**.
2. In the **Name** field, enter "FortiRecon_LeakedCards".
3. In **Device Type**, enter/select "Fortinet FortiRecon".
4. For **Pull Interval**, leave at default, or change as desired e.g. every 30 minutes.
5. For **Authentication Type**, select **API Key**.
6. In the **General Parameters** row, click the Pencil icon and configure the following fields:

- a. **Host Name:** api.fortirecon.forticloud.com
 - b. **URI Stem:** /aci/<yourOrgID>/leaked_cards
Note: You must replace <yourOrgID> with your FortiRecon organization ID
 - c. **JSON Response Log Key:** hits
 - d. **Log Header:** FORTIRECON_ACI_LEAKED_CARDS
 - e. Click **OK**.
Note: Leave other fields default
7. In the **Authentication Parameters** row, click the Pencil icon and configure the following fields.
- a. **API Key Name:** Authorization
 - b. **API Key Value:** <Enter/paste your FortiRecon API key>
 - c. **Send Method:** Send As Header
 - d. Click **OK**.
8. In the **Log API Parameters** row, click the Pencil icon and configure the following fields.
- a. Click the **Header** tab, click **New**, and configure the following fields.
 - i. **Key Type:** String
 - ii. **Key Name** (header name): Content-Type
 - iii. **Key Value:** application/json
 - b. Click **OK**.
 - c. Under **Header**, click **New** again, and configure the following fields.
 - i. **Key Type:** string
 - ii. **Key Name** (header name): accept
 - iii. **Key Value:** application/json
 - d. Click **OK**.
 - e. Click the **Pagination** tab, and configure the following fields.
 - i. **Pagination Method:** Offset and Limit
 - ii. **Limit Key Name:** size
 - iii. **Limit Value:** 100
 - iv. **Offset Key Name:** page
 - v. **Offset Start Value:** 1
 - vi. **Offset Increment Value:** 1
 - vii. **Offset Max Value:** 100
 - f. Click **OK**.
9. Click **Save** for Credential.

Setup for all other API endpoints are the same. You can import the same credential above, except, under **General Parameters**, update the URI Stem to the correct API call for each new credential.

URI Stem	Log Header	Template file
/aci/<yourOrgID>/iocs	FORTIRECON_ACI_IOC	FORTIRECON_ACI_IOC.json
/aci/<yourOrgID>/leaked_cards	FORTIRECON_ACI_LEAKED_CARDS	FORTIRECON_ACI_LEAKED_CARDS.json

URI Stem	Log Header	Template file
/easm/<yourOrgID>/leaked_creds	FORTIRECON_EASM_LEAKED_CREDS	FORTIRECON_EASM_LEAKED_CREDS.json
/bp/<yourOrgID>/rogue_apps	FORTIRECON_BP_ROGUE_APPS	FORTIRECON_BP_ROGUE_APPS.json
/bp/<yourOrgID>/stats/domain_threats	FORTIRECON_BP_DOMAIN_THREATS	FORTIRECON_BP_DOMAIN_THREATS.json
/easm/<yourOrgID>/issues	FORTIRECON_EASM_ISSUES	FORTIRECON_EASM_ISSUES.json
/aci/<yourOrgID>/reports	FORTIRECON_ACI_REPORTS	FORTIRECON_ACI_REPORTS.json
/easm/<yourOrgID>/exposed_services	FORTIRECON_EASM_EXPOSED_SERVICES	FORTIRECON_EASM_EXPOSED_SERVICES.json
/easm/<yourOrgID>/scan_statistics	FORTIRECON_EASM_SCAN_STATS	FORTIRECON_EASM_SCAN_STATS.json

Starting the Event Pulling

1. Under **Step 2: Enter IP Range to Credential Associations**, Click **New**.
2. In **Credentials**, select the credential created prior for the API endpoint.
3. Click **Save**.
4. Select the credential you created in step 2, and click **Test > Test Connectivity without Ping**.
5. Click **Pull Events** in the top navigation bar, and wait 5 minutes for first event pull to start. A green checkbox should eventually appear.
6. Navigate to **Analytics**.
7. Search for events with: Event Type CONTAIN FortiRecon-

Sample Events

```
Jan 13 14:55:09 2023 api.fortirecon.forticloud.com 192.0.2.0 FORTIRECON_ACI_LEAKED_CARDS: {"org_id": "xxxx1234-xx12-33c5-a7a6-97134501723", "bin": "437551", "bank_name": "Example Bank", "base_name": "DEC 14 USA MAGENTO SSN DOB EMAIL IP", "category": "VISA", "type": "CREDIT", "shop_name": "findsome", "city": "Sunnyvale", "holder_name": "Example User", "expiry": "January/2024", "country": "UNITED STATES", "price": "15.00", "state": "ca", "unique_id": "4961534989", "zip": "90210", "brand_name": "VISA", "bg_code": 2, "index_ts": "2022-12-15T15:20:40Z"}
Jan 13 12:29:25 2023 api.fortirecon.forticloud.com 192.0.2.0 FORTIRECON_EASM_ISSUES: {"id": "6284d0f7dbb73af1cab5aa40", "issue_name": "Exposed HTTP Service", "asset": "1.1.1.1", "severity": "low", "port": null, "bucket": "Exposed Insecure Service", "status": "active", "user_name": null, "issue_name_identifier": "exposed_http_service", "bucket_id": "exposed_insecure_service"}
Jan 13 14:36:16 2023 api.fortirecon.forticloud.com 192.0.2.0 FORTIRECON_BP_ROGUE_APPS: {"id": "a9db3f42-edb6-461e-ba97-5c098b276b73", "name": "Best Ringtones 1.5 by Excellente Ringtones Sounds", "size": "6.54", "download_count": "0", "index_ts": "2022-11-10T04:13:13Z", "first_seen": "2022-11-10T08:52:56Z", "source_name": "apk-watch", "ticket_id": null, "keyword": "zoom", "developer_name": "Excellente Ringtones Sounds", "status": "Unofficial"}
Jan 13 15:04:06 2023 api.fortirecon.forticloud.com 192.0.2.0 FORTIRECON_ACI_REPORTS: {"report_id": "2022080476177", "motivation": "Cyber Crime", "relevance_rating": "Medium", "status": "Published",
```

```
"geography": ["south asia"], "tlp": "Amber", "source_name": "Breached aka BreachForums", "source_reliability": "B-Usually reliable", "information_reliability": "2-Probably true", "information_date": "2022-08-04T00:00:00Z", "adversary": ["leakbase"], "summary": "FortiGuard Threat Research identified two posts on the English language cybercrime forum 'Breached', where an actor who operates by the handle 'LeakBase' shared the database claiming to be from an Indian payment facilitator SecurePe, and an Indian DTH and mobile recharge service provider Click On Recharge.", "industry_tags": ["consumer services", "financial services"], "source_category": "Darknet", "report_title": "Actor 'LeakBase' shared databases claimed to be from Indian payment facilitator 'SecurePe', and Indian TV and mobile recharge service provider 'Click On Recharge'", "report_type": "Threat Alert", "threat": ["data breach", "personal information identification (pii)", "account(s) compromised", "database"], "publish_date": "2022-08-04T00:00:00Z"}
```

End Point Security Software

The following anti-virus and host security (HIPS) applications are supported for discovery and monitoring by FortiSIEM.

- Bit9 Security Platform
- Bitdefender GravityZone
- Carbon Black Security Platform
- Cisco AMP for Endpoints API V0 - Previously Cisco AMP Cloud V0
- Cisco AMP for Endpoints API V1 - Previously Cisco AMP Cloud V1
- Cisco Security Agent (CSA)
- CloudPassage Halo
- CrowdStrike Endpoint Security
- Cybereason
- Digital Guardian Code Green DLP
- ESET NOD32 Anti-Virus
- FortiClient
- FortiClient EMS
- FortinetFortiEDR
- Kaspersky
- Malwarebytes Breach Remediation
- MalwareBytes Endpoint Protection
- McAfee ePolicy Orchestrator (ePO)
- Microsoft Defender for Endpoint/Microsoft Windows Defender ATP
- MobileIron Sentry and Connector
- Netwrix Auditor
- Palo Alto Traps Endpoint Security Manager
- SentinelOne Singularity
- Sophos Central
- Sophos Endpoint Security and Control
- Symantec Endpoint Protection
- Symantec SEPM
- Tanium Connect
- Trend Micro Interscan Web Filter
- Trend Micro Intrusion Defense Firewall (IDF)
- Trend Micro OfficeScan
- Trend Vision One

Bit9 Security Platform

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Bit9 Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Bit9" to see the event types associated with this device.

Rules

- Bit9 Agent Uninstalled or File Tracking Disabled
- Bit9 Fatal Errors
- Blocked File Execution
- Unapproved File Execution

Reports

- Bit9 Account Group Changes
- Bit9 Fatal and Warnings Issues
- Bit9 Functionality Stopped
- Bit9 Security Configuration Downgrades

Bit9 Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<14>1 2015-04-06T16:24:02Z server1.foo.com - - - Bit9 event: text="Server discovered new file  
'c:\users\acct\appdata\local\temp\3cziegdd.dll'  
[361aa7fbd5d00aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f]." type="Discovery" subtype="New  
file on network" hostname="SVR123" username="SVR123\acct" date="4/6/2015 4:22:52 PM" ip_  
address="10.168.1.1" process="c:\abc\infrastructure\bin\scannerreset.exe" file_  
path="c:\users\acct\appdata\local\temp\3cziegdd.dll" file_name="3cziegdd.dll" file_  
hash="361aa7fbd5d00aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f" installer_name="csc.exe"  
policy="High Enforce" process_key="00000000-0000-1258-01d0-7085edb50080" server_  
version="7.2.0.1395" file_trust="-2" file_threat="-2" process_trust="-1" process_threat="-1"
```

Bitdefender GravityZone

Vendor: Bitdefender

Product Information: <https://www.bitdefender.com/>

Support Added: FortiSIEM 7.0.0

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Configuration](#)

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Bitdefender GravityZone.

Protocol	Metrics Collected	Used For
HTTP POST	Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Bitdefender-GravityZone-" to see the event types associated with this device.

Rules

There are no specific rules for Bitdefender GravityZone, however events are categorized and normalized for use by generic FortiSIEM detection rules.

Configuration

- [Bitdefender GravityZone Configuration](#)
- [FortiSIEM Configuration](#)
- [Sending a Test Event via GravityZone](#)

Bitdefender GravityZone Configuration

Create a GravityZone API Key by taking the following steps.

1. Sign in to GravityZone Control Center at <https://gravityzone.bitdefender.com>.
2. Click your username in the upper-right corner of the console and choose **My Account**.
3. Go to the Control Center **API section** to get the **Access URL** field.
The base URL for all API is: `Access_url/v1.0/jsonrpc/`
The base URL will be used in the feature.
4. Go to the **API keys** section and click the **Add** button at the upper side of the table.
5. Select the **Integrations APIs**.
6. Click **Save**. An **API key** will be generated for the selected APIs.

FortiSIEM Configuration

Enable FortiSIEM HTTP Post Feature

Take the following steps to enable the FortiSIEM HTTP Post feature.

1. Login to FortiSIEM Collector/Supervisor via SSH.
Note: The following IP addresses must be whitelisted to ensure end-to-end communication between the GravityZone Event Push Service and FortiSIEM Collector/Supervisor:
 - 34.159.83.241
 - 34.159.47.15
 - 34.159.150.228
 - 34.85.152.87
 - 34.85.155.173

2. Run the following command to create a HTTP account.
`htpasswd -bs /etc/httpd/accounts/passwds <http user name> <http password>`
3. Save the <http user name> <http password> information, as it will be used later on in the configuration.

Enable GravityZone to Forward Events to FortiSIEM

Take the following steps to enable Bitdefender GravityZone to forward events to FortiSIEM

1. Login to FortiSIEM Collector/Supervisor via SSH.
2. Run script `enableBitDefenderForwardEventsToFortiSIEM.py` to enable GravityZone forward events to FortiSIEM.

Usage:

```
enableBitDefenderForwardEventsToFortiSIEM.py [API base url] [API key] [FSIEM
Collector/Supervisor IP] [FSIEM HTTP user] [FSIEM HTTP password]
```

Example:

```
/opt/phoenix/bin/enableBitDefenderForwardEventsToFortiSIEM.py
https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/push/
71ba6cb43f87389b11fb5e64b7811e4fb3f8cd111454a9cb23ae483c75cea3d3 10.10.10.10 test test*1
```

GravityZone will start sending events to FortiSIEM after the Event Push Service settings are reloaded. This happens every 10 minutes.

Sending a Test Event via GravityZone

To force Bitdefender GravityZone to send a test event, take the following steps.

1. Encode API key
`echo -n '<API key>:' | base64 -w 0`
2. Post command to make Gravity to send test event.

```
curl -k -X POST \
  https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/push/ \
  -H 'authorization: Basic <API Key base64 string>' \
  -H 'cache-control: no-cache' \
  -H 'content-type: application/json' \
  -d '{"params": {"eventType": "av"}, "jsonrpc": "2.0", "method": "sendTestPushEvent",
    "id": "3"}'
```

3. Find the REST API GravityZone used to send test event to FortiSIEM. And the HTTP status code is 200.
`tail -1000f /etc/httpd/logs/ssl_access_log |grep GravityZone`
4. Events can be queried from the **Analytics** page.

Example Walkthrough:

1. `echo -n '71ba6cb43f87389b95cb5e64b7811e4fb3f8cd111454a9cb23ae483c75cea3d3:' | base64 -w 0`

API Key:

NzAAYTZjYjQzZjg3Mzg5Yjk1Y2I1ZTY0Yjc4MTF1NGZiM2Y4Y2QxMTE0NTRhOWNiMjNhZTQ4M2M3NWNlYTNkMzo=

2. `curl -k -X POST https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/push/ -H 'authorization: Basic NzAAYTZjYjQzZjg3Mzg5Yjk1Y2I1ZTY0Yjc4MTF1NGZiM2Y4Y2QxMTE0NTRhOWNiMjNhZTQ4M2M3NWNlYTNkMzo=' -H 'cache-control: no-cache' -H 'content-type: application/json' -d '{"params": {"eventType": "av"}, "jsonrpc": "2.0", "method": "sendTestPushEvent", "id": "3"}'`
3. `tail -1000f /etc/httpd/logs/ssl_access_log |grep GravityZone 34.85.155.173 - test [19/Aug/2022:10:37:35 -0500] "POST /rawupload?vendor=Bitdefender&model=GravityZone&reptIp=104.17.52.22&reptName=cloud.gravityzone.bitdefender.com&separator=%0A HTTP/1.1" 200 -`
4. Log onto FortiSIEM GUI, navigate to **Analytics** page and query for event.

Carbon Black Security Platform

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Carbon Black Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Carbon Black" to see the event types associated with this device.

Rules

- Carbon Black Agent Uninstalled or File Tracking Disabled
- Carbon Black Fatal Errors
- Blocked File Execution
- Unapproved File Execution

Reports

- Carbon Black Account Group Changes
- Carbon Black Fatal and Warnings Issues
- Carbon Black Functionality Stopped
- Carbon Black Security Configuration Downgrades

Carbon Black Configuration

Syslog

The following guide should be used to install the python Carbon Black Cloud Syslog Connector on your FortiSIEM collector.

<https://developer.carbonblack.com/reference/carbon-black-cloud/integrations/syslog-connector/>

Note: You may need your Carbon Black account to view the Unix instructions.

An install guide with a sample configuration file is available here:

<https://pypi.org/project/cbc-syslog/>

Notes:

- If you haven't done so already, create a symbolic link to pip for easier execution.
Example: `ln -sf /usr/bin/pip<#.#> /usr/bin/pip`
- From the GitHub Installation instructions "Install python package", make sure to include the period.
`pip install .`

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514. CEF formatted logs are also supported.

Sample Syslog

Standard Syslog:

```
<14>1 2015-04-06T16:24:02Z server1.foo.com - - - Carbon Black event: text="Server discovered
new file 'c:\users\acct\appdata\local\temp\3cziegdd.dll'
[361aa7fbd5d0aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f]." type="Discovery" subtype="New
file on network" hostname="SVR123" username="SVR123\acct" date="4/6/2015 4:22:52 PM" ip_
address="10.168.1.1" process="c:\abc\infrastructure\bin\scannerreset.exe" file_
path="c:\users\acct\appdata\local\temp\3cziegdd.dll" file_name="3cziegdd.dll" file_
hash="361aa7fbd5d0aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f" installer_name="csc.exe"
policy="High Enforce" process_key="00000000-0000-1258-01d0-7085edb50080" server_
version="7.2.0.1395" file_trust="-2" file_threat="-2" process_trust="-1" process_threat="-1"
```

CEF Formatted Syslog:

```
<14>May 06 13:28:09 host1 CEF:0|Carbon Black|Protection|8.0.0.2562|809|Report write (custom
rule)|4|externalId=649219 cat=Policy Enforcement start=May 06 13:27:41 UTC rt=May 06 13:28:02 UTC
filePath=c:\\windows\\system32\\perfdisk.dll fname=perfdisk.dll
fileHash=60b8a55c0f3228b18d918a3fd6684c401442f6447f2cec5dad9860a8c1d6462c fileId=39126
deviceProcessName="C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\4.14.17639.18041-
0\\MsMDEV.exe" dst=172.30.31.13 dhost=EXAMPLE\\DC01 duser=NT AUTHORITY\\SYSTEM
dvchost=cbprotection msg='c:\\windows\\system32\\perfdisk.dll' was created by 'NT
```

```
AUTHORITY\\SYSTEM'. sproc=00000000-0000-15b8-01d3-dd191e70c6d3 cs1Label=rootHash  
cs1=e1c32fca51d86aad28c2dd13ec427eccd03f9d6900f8f1fe90b99f85550a8a98 cs2Label=installerFilename  
cs2=msi669d.tmp cs3Label=Policy cs3=Domain Controllers cs5Label=ruleName cs5=[File Integrity  
Monitoring] Changes to system files cfp1Label=fileTrust cfp1=10 flexString1Label=fileThreat  
flexString1=0 - Clean cfp2Label=processTrust cfp2=10 flexString2Label=processThreat flexString2=0  
- Clean
```

Cisco AMP for Endpoints API V0 - Previously Cisco AMP Cloud V0

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Logs Collected	Used For
CloudAMP API	End point malware activity	Security Monitoring

Event Types

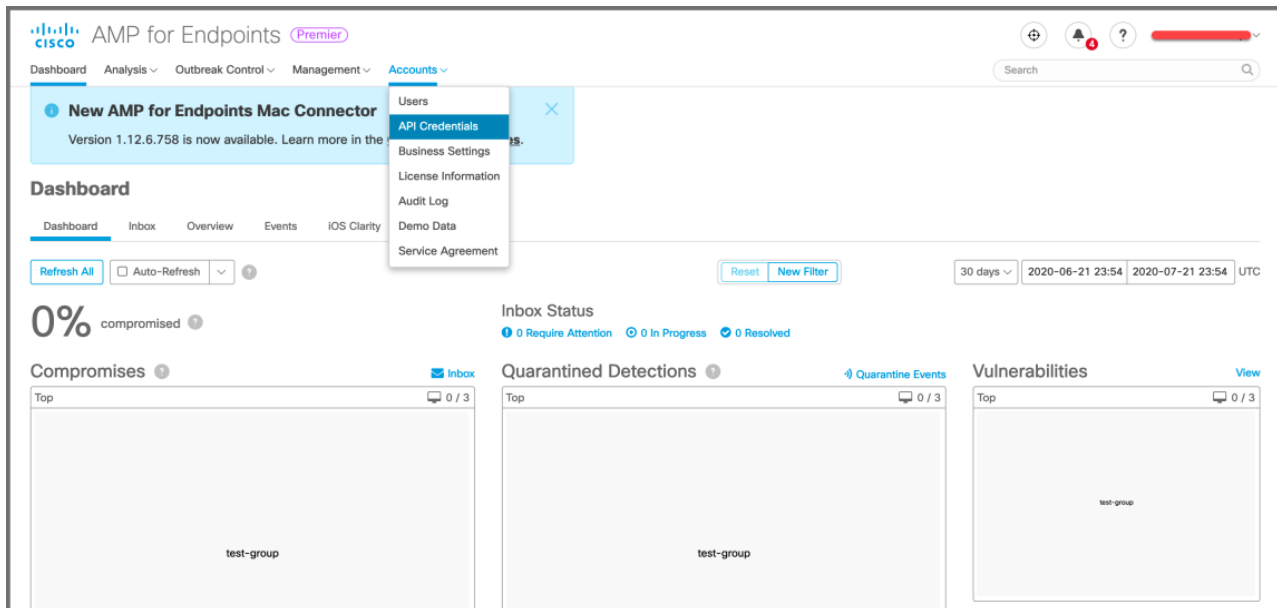
In **ADMIN > Device Support > Event Types**, search for "FireAMP Cloud" in the **Search** field to see the event types associated with this device.

Configuration

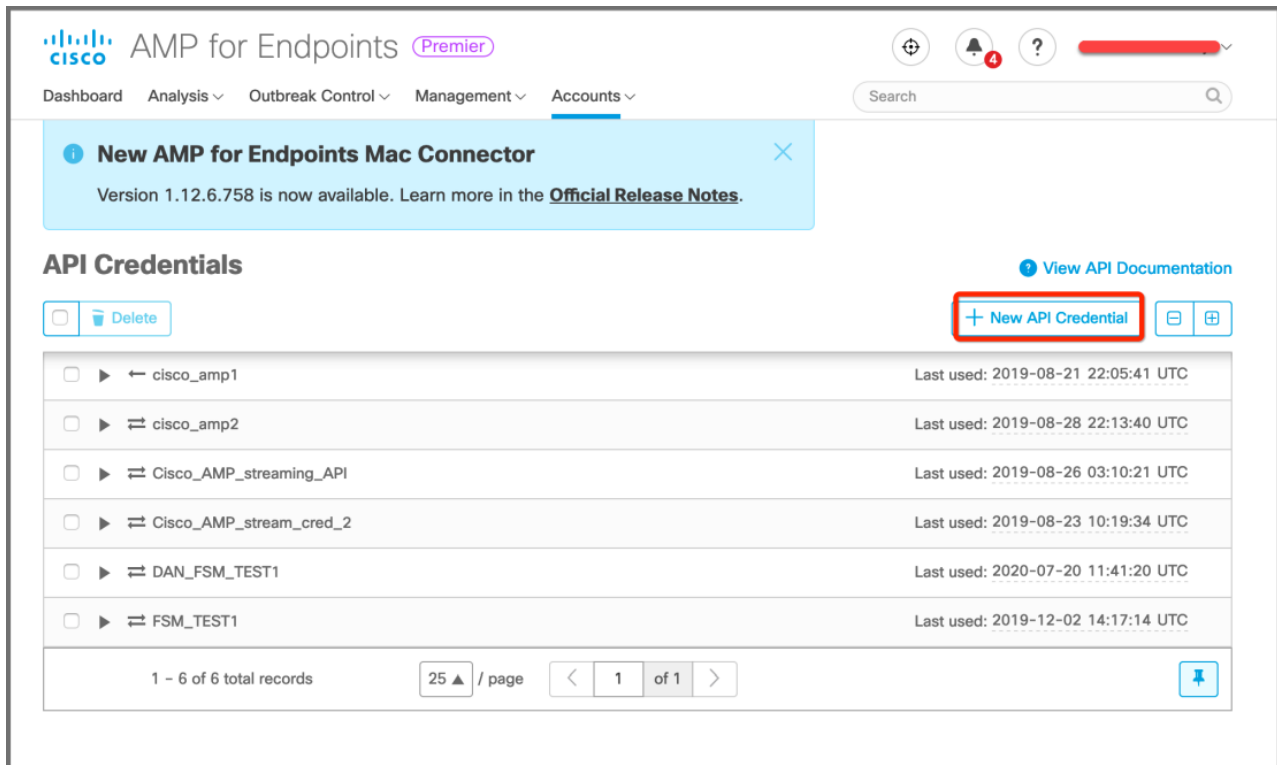
- [Configure Cisco AMP Cloud V0](#)
- [Define Cisco FireAMP Cloud Credential in FortiSIEM](#)
- [Create IP Range to Credential Association, Test Connectivity, and Event Pulling](#)

Configure Cisco AMP Cloud V0

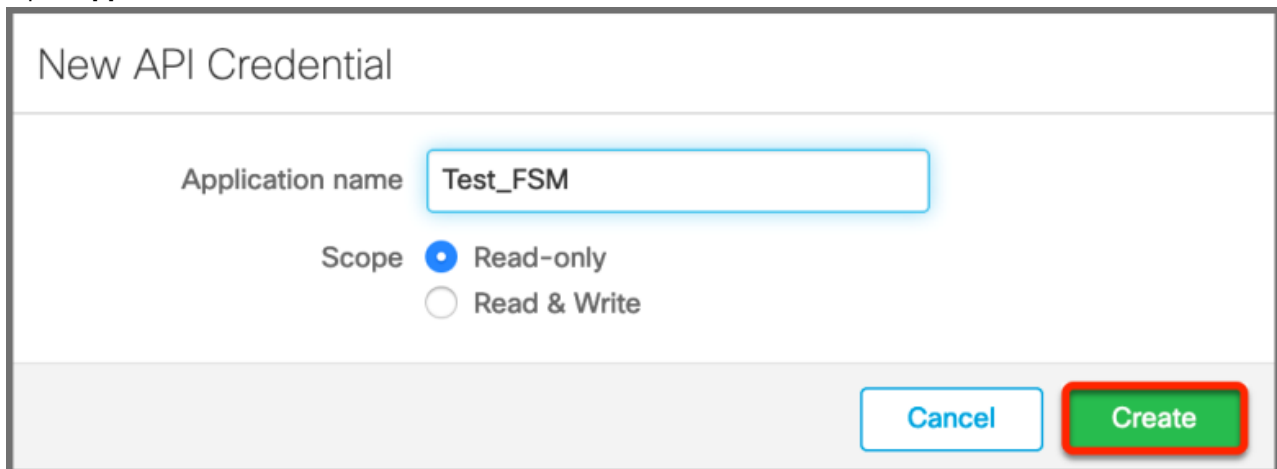
1. Login in <https://auth.amp.cisco.com/>.
2. Click **Accounts-> API Credentials**.



3. Click **New API Credential**.



4. Input **Application name** and click **Create**.

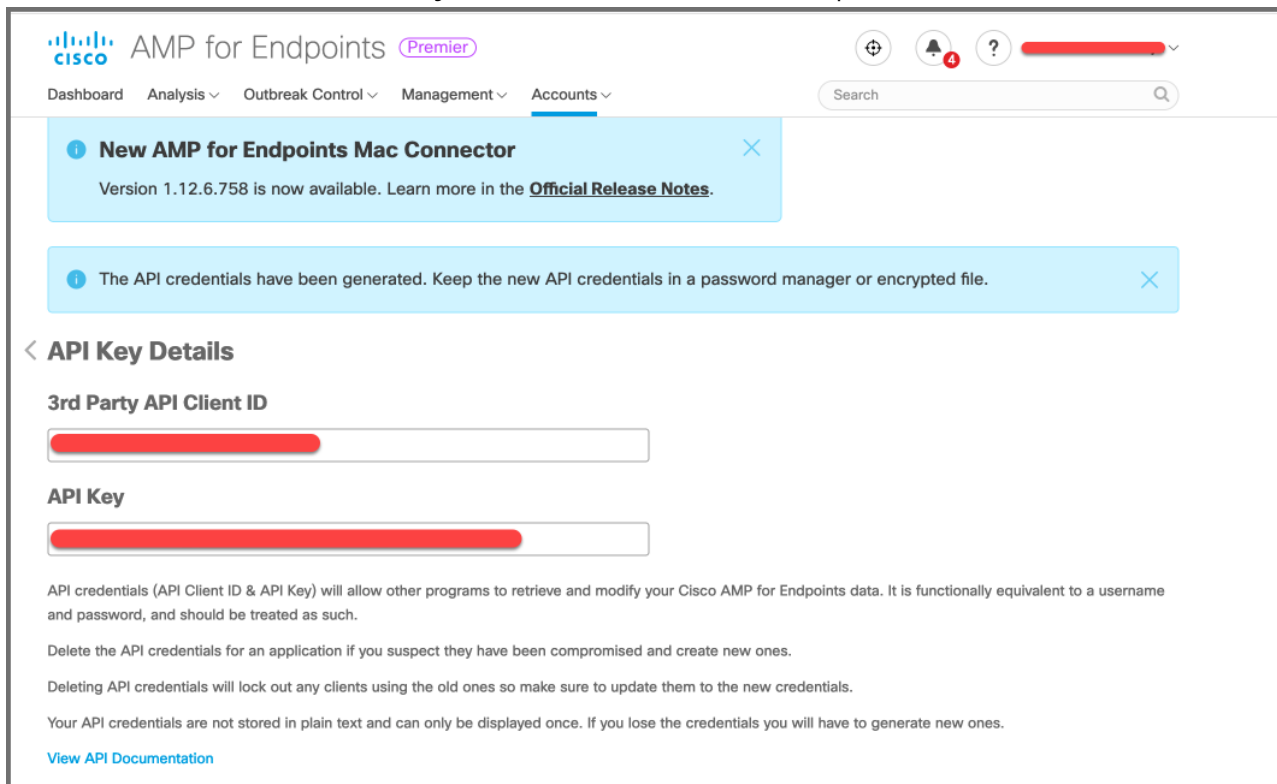


New API Credential

Application name

Scope ☒ Read-only ☐ Read & Write

5. Record the **API Client ID** and **API key**. You will need them in a later step.



API Key Details

3rd Party API Client ID

API Key

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

[View API Documentation](#)

New AMP for Endpoints Mac Connector
Version 1.12.6.758 is now available. Learn more in the [Official Release Notes](#).

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

Define Cisco FireAMP Cloud Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in “[Setting Credentials](#)” in the User's Guide to create a new credential.
 1. b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, for example "FireAMP Cloud"
Device Type	Cisco FireAMP Cloud
Access Protocol	FireAMP Cloud API
Password config	Manual
Client ID	CiscoAMP Client ID
Client Secret	CiscoAMP API Key
Organization	The organization the device belongs to.
Description	Description of the device.

Access Method Definition ✕

Name:

FireAMP Cloud

Device Type:

Cisco FireAMP Cloud ▾

Access Protocol:

FireAMP Cloud API ▾

Pull Interval:

5

Minute(s)

Timeout:

30

Second(s)

Password config:

Manual ▾

Client ID:

ff35299e906cb0ca4597

Client Secret:

.....

Confirm Client Secret:

.....

Organization:

Super ▾

Description:

Save

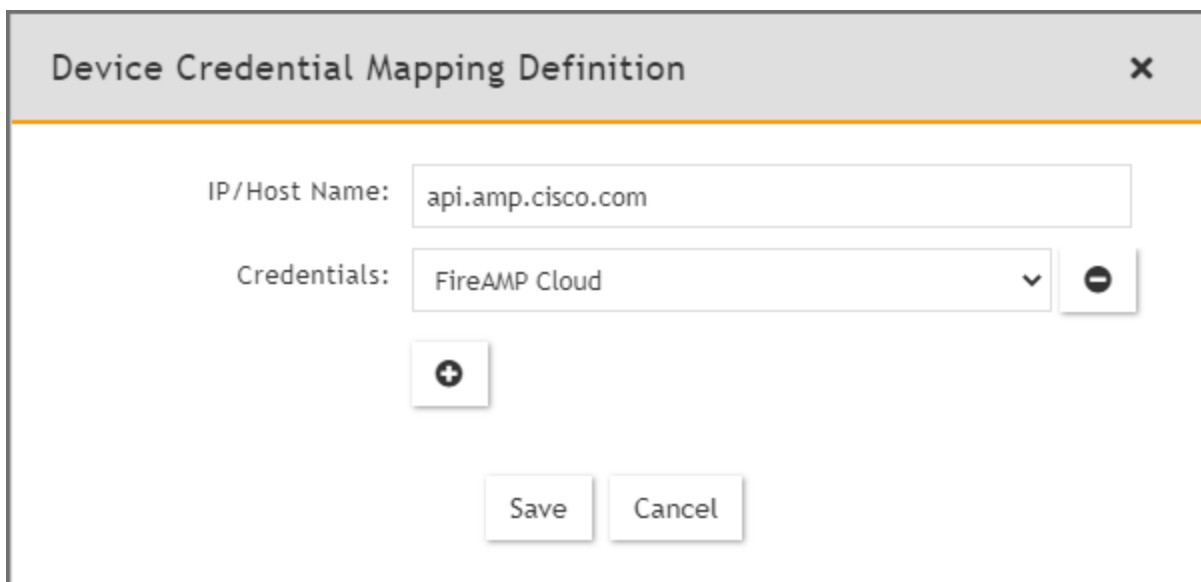
Cancel

Create IP Range to Credential Association, Test Connectivity, and Event Pulling

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter "api.amp.cisco.com" in the **IP/Host Name** field.
 - b. Select the name of the credential created in [Define Cisco FireAMP Cloud Credential in FortiSIEM](#) from the **Credentials** drop-down list.

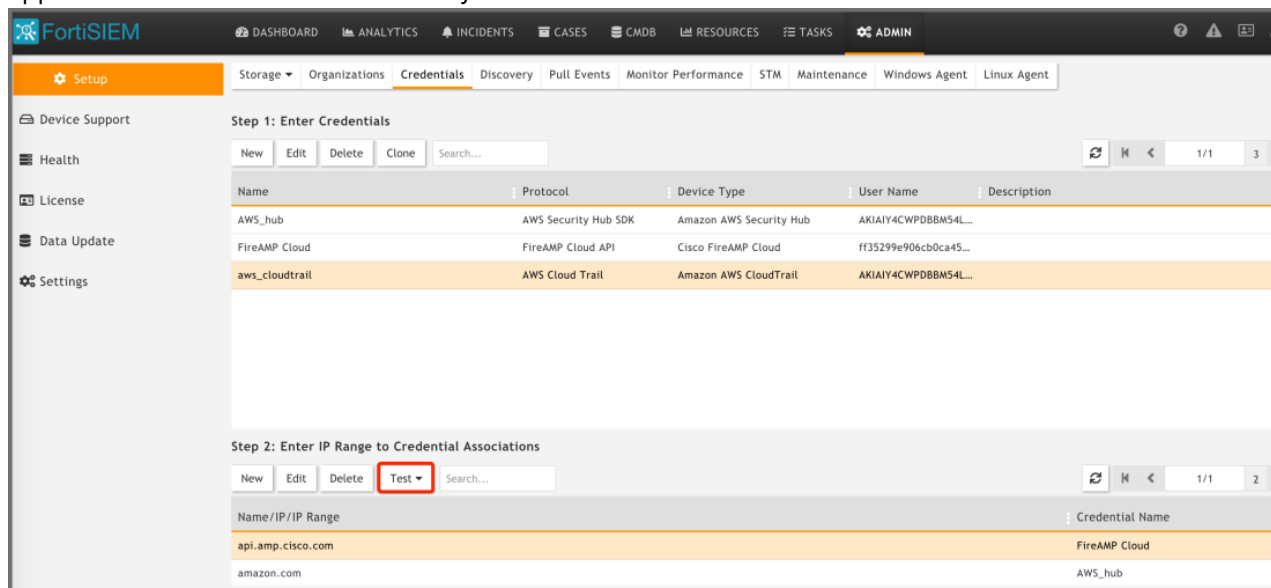
- c. Click **Save**.



The dialog box titled "Device Credential Mapping Definition" contains the following fields and controls:

- IP/Host Name:** A text input field containing "api.amp.cisco.com".
- Credentials:** A dropdown menu showing "FireAMP Cloud". To the right of the dropdown is a minus sign icon.
- A plus sign icon is located below the Credentials dropdown.
- At the bottom are two buttons: "Save" and "Cancel".

2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity**. A pop up will appear and show the Test Connectivity results.



The screenshot shows the FortiSIEM interface with the "Credentials" tab selected. It displays two steps for credential management:

Step 1: Enter Credentials

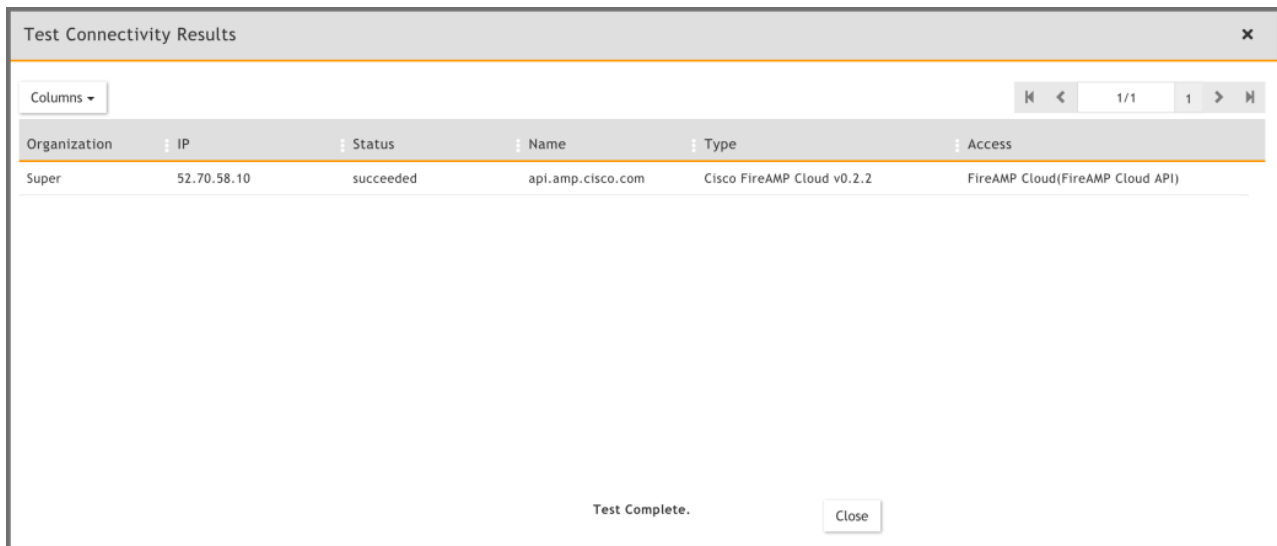
Name	Protocol	Device Type	User Name	Description
AWS_hub	AWS Security Hub SDK	Amazon AWS Security Hub	AKIAIY4CWPDBBM54L...	
FireAMP Cloud	FireAMP Cloud API	Cisco FireAMP Cloud	ff35299e906cb0ca45...	
aws_cloudtrail	AWS Cloud Trail	Amazon AWS CloudTrail	AKIAIY4CWPDBBM54L...	

Step 2: Enter IP Range to Credential Associations

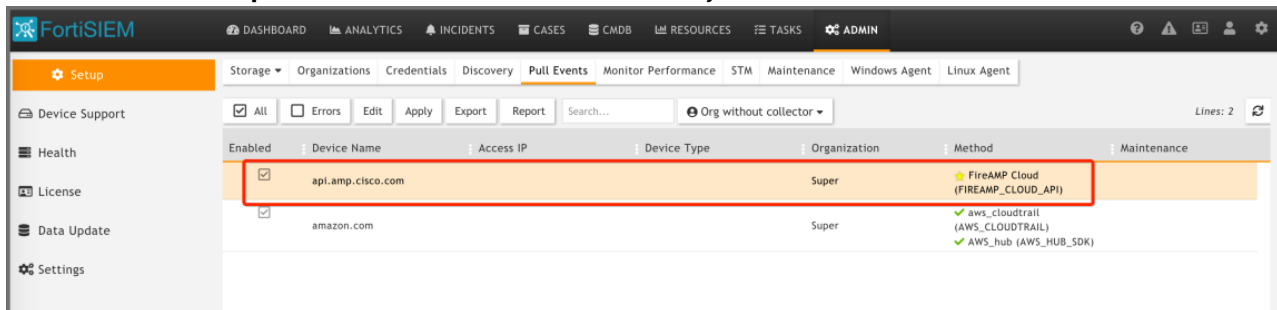
Name/IP/ IP Range	Credential Name
api.amp.cisco.com	FireAMP Cloud
amazon.com	AWS_hub

In the "Test" dropdown menu in Step 2, the "Test" option is highlighted with a red box.

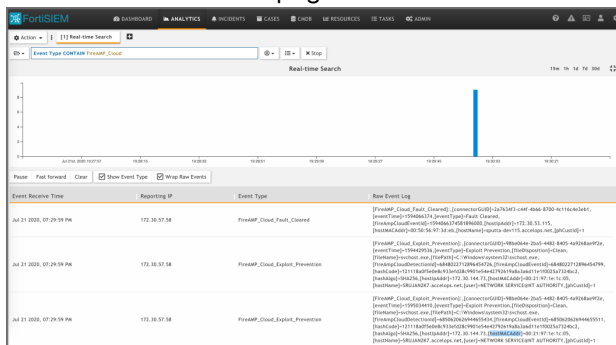
The result is a success.



3. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Cisco FireAMP Cloud.



4. Go to the **ANALYTICS** page to see the events.



Sample Events

```
[FireAMP_Cloud_Threat_Detected]:[eventSeverity]=PHL_CRITICAL,[connectorGUID]=12345,[date]=2015-11-25T19:17:39:00:00,[detection]=W32.DFC.MalParent,[detectionId]=6159251516445163587,[eventId]=6159251516445163587,[eventType]=Threat Detected,[eventTypeid]=1090519054,[fileDisposition]=Malicious,[fileName]=rjtsbks.exe,[fileSHA256]=3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370,
```

Cisco AMP for Endpoints API V1 - Previously Cisco AMP Cloud V1

Cisco Advanced Malware Protection (AMP) for Endpoints API V1 is a lightweight connector that can use the public cloud or be deployed as a private cloud, relying on AMQP Event Streams.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configure Cisco AMP Cloud V1](#)
- [Configure FortiSIEM](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information collected	Used for
AMQP	Global threat intelligence, advanced sand boxing, and real-time malware blocking.	Intrusion protection system

Event Types

In **RESOURCES > Event Types**, enter "Cisco AMP" in the **Search** field to see the event types associated with this device.

Rules

No defined rules.

Reports

No defined reports.

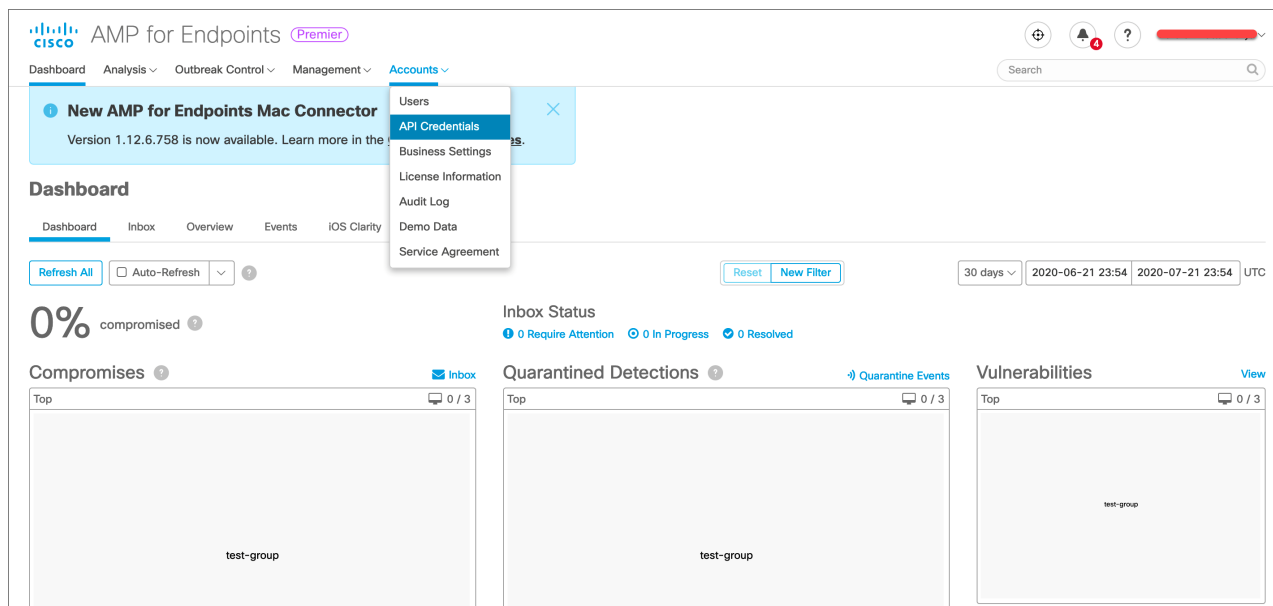
Configuration

- [Configure Cisco AMP Cloud V1](#)
- [Define Cisco CloudAMP Credential in FortiSIEM](#)

- Create IP Range to Credential Association, Test Connectivity, and Event Pulling Check

Configure Cisco AMP Cloud V1

1. Log in to the Cisco AMP for Endpoints Portal as an administrator.
2. Click **Accounts > API Credentials**.



3. In the API Credentials pane, click **New API Credential**.
4. In the **Application name** field, enter a name, and then select **Read & Write**.
Note: you must have Read & Write access to manage event streams on your Cisco AMP for Endpoints platform.

New API Credential

Application name

Test_AMQP_FSM|

Scope

☐ Read-only

☒ Read & Write

 An API credential with read and write scope can make changes to your AMP for Endpoints configuration that may cause significant problems with your endpoints.

Some of the input protections built into the AMP Console do not apply to the API.

Cancel

Create

5. Click **Create**.
6. In the **API Key Details** section, make note of the values for the **3rd Party API Client ID** and the **API Key**. You will need these values to manage queues.
7. Click **Management > Group**.
8. In the Groups pane, click **Create Group**.

9. Enter the group name and click **Save**.

The screenshot displays the 'New Group' configuration interface in the Cisco AMP for Endpoints console. The top navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Management' (selected), and 'Accounts'. A notification banner at the top left indicates a new version of the Mac Connector is available. The main form area is titled 'New Group' and contains the following fields:

- Name:** A text input field containing 'Audit'.
- Description:** A large text area for additional details.
- Parent Group:** A dropdown menu.
- Windows Policy:** A dropdown menu set to 'Default Policy (Audit)'.
- Android Policy:** A dropdown menu set to 'Default Policy (Protect)'.
- Mac Policy:** A dropdown menu set to 'Default Policy (Audit)'.
- Linux Policy:** A dropdown menu set to 'Default Policy (Audit)'.
- iOS Policy:** A dropdown menu set to 'Default Policy (Audit)'.

Buttons for 'Cancel' and 'Save' are located below the policy fields. To the right, a 'Computers' sidebar contains the text: 'Assign computers from the Computers page after you have saved the new group'. At the bottom, the 'Child Groups' section shows a list of available groups: Audit, Domain Controller, Protect, Server, and test-group. There are 'Select All' and 'Deselect All' buttons for both the 'Child Groups' and 'Add Child Groups' sections.

10. Enter the following `curl` command to get the `group_guid` of the group that is created in the previous step.

```
curl -X GET -H 'accept: application/json' \
  -H 'content-type: application/json' --compressed \
  -H 'Accept-Encoding: gzip, deflate' \
  -u <CLIENTID:APIKEY>\
  'https://api.amp.cisco.com/v1/groups'
```

where:

- `<CLIENTID:APIKEY>` is the Client ID and the API key that you created in [Step 6](#).
- If you are in the Asia Pacific Japan and China (APJC) region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.apjc.amp.cisco.com/v1/event_streams`.
- If you are in the European region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.eu.amp.cisco.com/v1/event_streams`.

11. Enter the following `curl` command to create a Cisco AMP event stream:

```
curl -X POST -H 'accept: application/json' \
```

```
-H 'content-type: application/json' --compressed \
-H 'Accept-Encoding: gzip, deflate' \
-d '{"name": "<STREAM_NAME>"}' \
-u <CLIENTID:APIKEY> \
'https://api.amp.cisco.com/v1/event_streams'
```

where:

- <STREAM_NAME> is the name of your choice for the event stream.
 - <CLIENTID:APIKEY> is the Client ID and the API key that you created in [Step 6](#).
 - If you are in the Asia Pacific Japan and China (APJC) region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.apjc.amp.cisco.com/v1/event_streams`.
 - If you are in the European region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.eu.amp.cisco.com/v1/event_streams`.
- Note:** Only the event stream name is required. In the absence of event_type or group_guid, the stream will collect events from all groups and all event types.

- 12.** Enter the following curl command to get a summary of the information you need to get a CloudAMP V1 credential in FortiSIEM:

```
curl -X POST -H 'accept: application/json' \
-H 'content-type: application/json' --compressed \
-H 'Accept-Encoding: gzip, deflate' \
-d '{"name": "meistream", "group_guid": ["34e483f4-85a8-412f-9997-07dd3f0c29ea"]}' \
-u a54c0f4c589d72e0c73e:14713974-eb93-420b-ad76-6e13943f87d4 \
'https://api.amp.cisco.com/v1/event_streams'
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "https://api.amp.cisco.com/v1/event_streams"
    }
  },
  "data": {
    "id": 8849,
    "name": "meistream",
    "group_guids": [
      "34e483f4-85a8-412f-9997-07dd3f0c29ea"
    ],
    "amqp_credentials": {
      "user_name": "8849-a54c0f4c589d72e0c73e",
      "queue_name": "event_stream_8849",
      "password": "e3298163b3c57e5e4e11ea1b571e85cc2ac45b55",
      "host": "export-streaming.amp.cisco.com",
      "port": "443",
      "proto": "https"
    }
  }
}
```

Define Cisco CloudAMP Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New**.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
1.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, for example, "AMQP".
Device Type	Cisco AMP
Access Protocol	AMQP
Queue Name	Use the queue-name in Step 12 of the previous section.
User Name	Use the user_name in Step 12 of the previous section.
Password	Use the password in Step 12 of the previous section.
Description	Description of the device.

Access Method Definition

Name:

AMQP

Device Type:

Cisco AMP ▾

Access Protocol:

AMQP ▾

Port:

443

Queue Name:

event_stream_8849

User Name:

88490a54c0f4c589d72e0c73e

Password:

.....

Confirm Password:

.....

Description:

e3298163b3c57e5e4e11ea1b571e85cc2ac45b55

Save

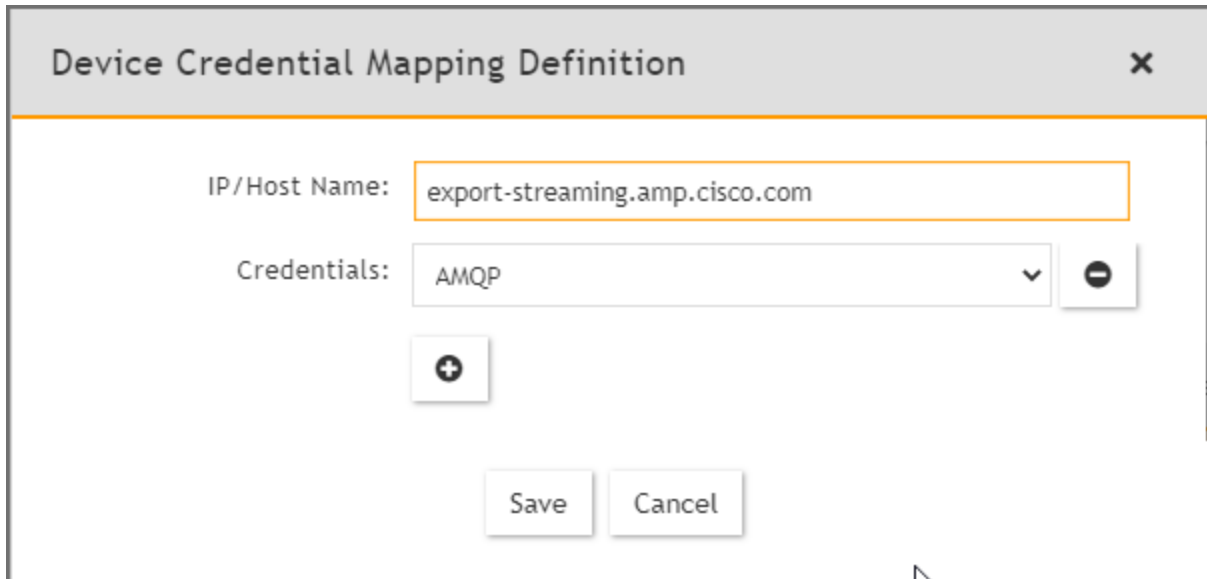
Cancel

Create IP Range to Credential Association, Test Connectivity, and Event Pulling Check

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create your mapping.
 - a. Enter the host in [Step 12](#) of previous section into the **IP/Host Name** field.
 - b. Select the name of the credential created in [Define Cisco CloudAMP Credential in FortiSIEM](#) from the **Credentials** drop-down list.

- c. Click **Save**.



The screenshot shows a dialog box titled "Device Credential Mapping Definition". It has a close button (X) in the top right corner. Inside the dialog, there is a text field for "IP/Host Name" containing the value "export-streaming.amp.cisco.com". Below this is a "Credentials" dropdown menu currently showing "AMQP". To the right of the dropdown is a minus sign button (-). Below the dropdown is a plus sign button (+). At the bottom of the dialog are "Save" and "Cancel" buttons.

2. Select the entry just created, click the **Test** drop-down list, and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. If connectivity is successful, go to **ADMIN > Setup > Pull Events**. An entry will appear in the **Event Pulling** table. That means events are being pulled.

Sample Events

Events are in JSON format.

```
[CiscoAMP-Update-Policy-Failure>{"id":6723137944535695384,"timestamp":1565352535,"timestamp_
nanoseconds":82000000,"date":"2019-08-09T12:08:55+00:00","event_type":"Policy Update
Failure","event_type_id":2164260866,"connector_guid":"98be064e-2ba5-4482-8405-
4a9268ae9f2e","group_guids":["3c025f05-a2c4-4613-9186-343365f53853"],"error":{"error_
code":3242196993,"description":"Unknown Error"},"computer":{"connector_guid":"98be064e-2ba5-
4482-8405-4a9268ae9f2e","hostname":"host1","external_ip":"1.2.3.4","active":true,"network_
addresses":[{"ip":"1.2.3.5","mac":"00:21:97:1e:1c:05"}],"links":
{"computer":"https://api.amp.cisco.com/v1/computers/98be064e-2ba5-4482-8405-
4a9268ae9f2e","trajectory":"https://api.amp.cisco.com/v1/computers/98be064e-2ba5-4482-8405-
4a9268ae9f2e/trajectory","group":"https://api.amp.cisco.com/v1/groups/3c025f05-a2c4-4613-9186-
343365f53853"}}}]
```

Cisco Security Agent (CSA)

- [What is Discovered and Monitored](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Example SNMP Trap](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Rules

FortiSIEM uses these rules to monitor events for this device:

Rule	Description
Agent service control	Attempts to modify agent configuration
Agent UI control	Attempts to modify agent UI default settings, security settings, configuration, contact information
Application control	Attempts to invoke processes in certain application classes
Buffer overflow attacks	
Clipboard access control	Attempts to access clipboard data written by sensitive data applications
COM component access control	Unusual attempts to access certain COM sets including Email objects
Connection rate limit	Excessive connections to web servers or from email clients
Data access control	Unusual attempts to access restricted data sets such as configuration files, password etc. by suspect applications
File access	Unusual attempts to read or write restricted

Rule	Description
control	files sets such as system executables, boot files etc. by suspect applications
Kernel protection	Unusual attempts to modify kernel functionality by suspect applications
Network access control	Attempts to connect to local network services
Network interface control	Attempts by local applications to open a stream connection to the NIC driver
Network shield	Attacks based on bad IP/TCP/UDP/ICMP headers, port and host scans etc
Windows event log	
Registry access control	Attempts to write certain registry entries
Resource access control	Symbolic link protection
Rootkit/kernel protection	Unusual attempts to load files after boot
Service restart	Service restarts
Sniffer and protocol detection	Attempts by packet/protocol sniffer to receive packets
Syslog control	Syslog events
System API control	Attempts to access Windows Security Access Manager (SAM)

Reports

There are no predefined reports for Cisco Security Agent.

Configuration

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example SNMP Trap

```
2008-05-13 11:00:36 192.168.1.39 [192.168.1.39]:SNMPv2-MIB::sysUpTime.0 = Timeticks: (52695748) 6
days, 2:22:37.48 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.8590.3.1 SNMPv2-
SMI::enterprises.8590.2.1 = INTEGER: 619 SNMPv2-SMI::enterprises.8590.2.2 = INTEGER: 261
SNMPv2-SMI::enterprises.8590.2.3 = STRING: "sjdevVwindb06.ProspectHills.net"SNMPv2-
SMI::enterprises.8590.2.4 = STRING: "2008-05-13 19:03:21.157" SNMPv2-SMI::enterprises.8590.2.5
= INTEGER: 5 SNMPv2-SMI::enterprises.8590.2.6 = INTEGER: 452 SNMPv2-SMI::enterprises.8590.2.7
= STRING: "C:\\Program Files\\RealVNC\\VNC4\\winvnc4.exe"SNMPv2-SMI::enterprises.8590.2.8 =
NULL SNMPv2-SMI::enterprises.8590.2.9 = STRING: "192.168.20.38"SNMPv2-
SMI::enterprises.8590.2.10 = STRING: "192.168.1.39"SNMPv2-SMI::enterprises.8590.2.11 = STRING:
"The process 'C:\\Program Files\\RealVNC\\VNC4\\winvnc4.exe' (as user NT AUTHORITY\\SYSTEM)
attempted to accept a connection as a server on TCP port 5900 from 192.168.20.38 using
interface Wired\\VMware Accelerated AMD PCNet Adapter. The operation was denied." SNMPv2-
SMI::enterprises.8590.2.12 = INTEGER: 109 SNMPv2-SMI::enterprises.8590.2.13 = STRING:
"192.168.1.39" SNMPv2-SMI::enterprises.8590.2.14 = STRING: "w"SNMPv2-
SMI::enterprises.8590.2.15 = INTEGER: 3959 SNMPv2-SMI::enterprises.8590.2.16 = INTEGER: 5900
SNMPv2-SMI::enterprises.8590.2.17 = STRING: "Network access control"SNMPv2-
SMI::enterprises.8590.2.18 = STRING: "Non CSA applications, server for TCP or UDP
services"SNMPv2-SMI::enterprises.8590.2.19 = INTEGER: 33 SNMPv2-SMI::enterprises.8590.2.20 =
STRING: "CSA MC Security Module"SNMPv2-SMI::enterprises.8590.2.21 = NULL SNMPv2-
SMI::enterprises.8590.2.22 = STRING: "NT AUTHORITY\\SYSTEM"SNMPv2-SMI::enterprises.8590.2.23 =
INTEGER: 2
```


CloudPassage Halo

- [Integration Points](#)
- [CloudPassage REST API Integration](#)
- [Event Types](#)
- [Configuration](#)

Integration Points

Protocol	Information collected	Used For
CloudPassage REST API	Halo– over 110 event types including User login and account activity, server compliance and vulnerability status, server FIM and firewall policy modification etc.	Security and Compliance

CloudPassage REST API Integration

FortiSIEM can pull logs from CloudPassage Halo via the CloudPassage REST API. Currently, over 110 CloudPassage event types are parsed.

Use cases covered via API:

- User login to Halo and user account creation/deletion/modification activity
- Vulnerable software package found and Compromised host detection
- Server FIM, Firewall policy modification
- Server account creation
- Server login via ghostport

Event Types

In **RESOURCES > Event Types**, search for "CloudPassage-Halo" in the main content panel **Search...** field to see the various event types for CloudPassage Halo.

Configuration

Take the following steps to configure CloudPassage Halo for FortiSIEM.

- [Configuring CloudPassage Portal](#)
- [Define CloudPassage Halo Credential in FortiSIEM](#)
- [Create IP Range to Credential Association, Test Connectivity, and Event Checking](#)

Configuring CloudPassage Portal

Create an API Key to be used for FortiSIEM communication.

1. Log in to your CloudPassage Halo portal.
2. Create an API Key and API Secret for use in FortiSIEM.

Define CloudPassage Halo Credential in FortiSIEM

Use the API Key and Secret in the previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 1. b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	CloudPassage Halo
Access Protocol	Halo REST API
Pull Interval	5 minutes
Password config	For CyberArk and RAX_CustomerService, see Password Configuration. For Manual, see the following: 1. Set API Key ID to API Key obtained from the CloudPassage portal in Configuring CloudPassage Portal. 2. Set API Key Secret to API Secret obtained from the CloudPassage portal in Configuring CloudPassage Portal.
Organization	Choose the organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association, Test Connectivity, and Event Checking

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter "api.cloudpassage.com" in the **IP/Host Name** field.
 - b. Select the name of the credential created in [Define CloudPassage Halo Credential in FortiSIEM](#) from the **Credentials** drop-down list.
 - c. Click **Save**.
2. 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.
3. Go to **ADMIN > Setup > Pull Events**. FortiSIEM will start to pull events from CloudPassage portal using the API.

4. Test for received CloudPassage Halo events by navigating to **ADMIN > Setup > Pull Events**, selecting a CloudPassage Halo event and clicking **Report**. The system will take you to the **ANALYTICS** tab and run a query to display the events received from CloudPassage in the last 15 minutes. You can modify the time interval to get more events.

CrowdStrike Endpoint Security

Support Added: FortiSIEM 5.2.1

Last Modification: FortiSIEM 6.2.0

Vendor Version Tested: Not Provided

Vendor: CrowdStrike

Product: Endpoint Security

Product Information: <https://www.crowdstrike.com/endpoint-security-products/>

Configuration

- [CrowdStrike Server Configuration](#)
- [FortiSIEM Configuration](#)

CrowdStrike Server Configuration

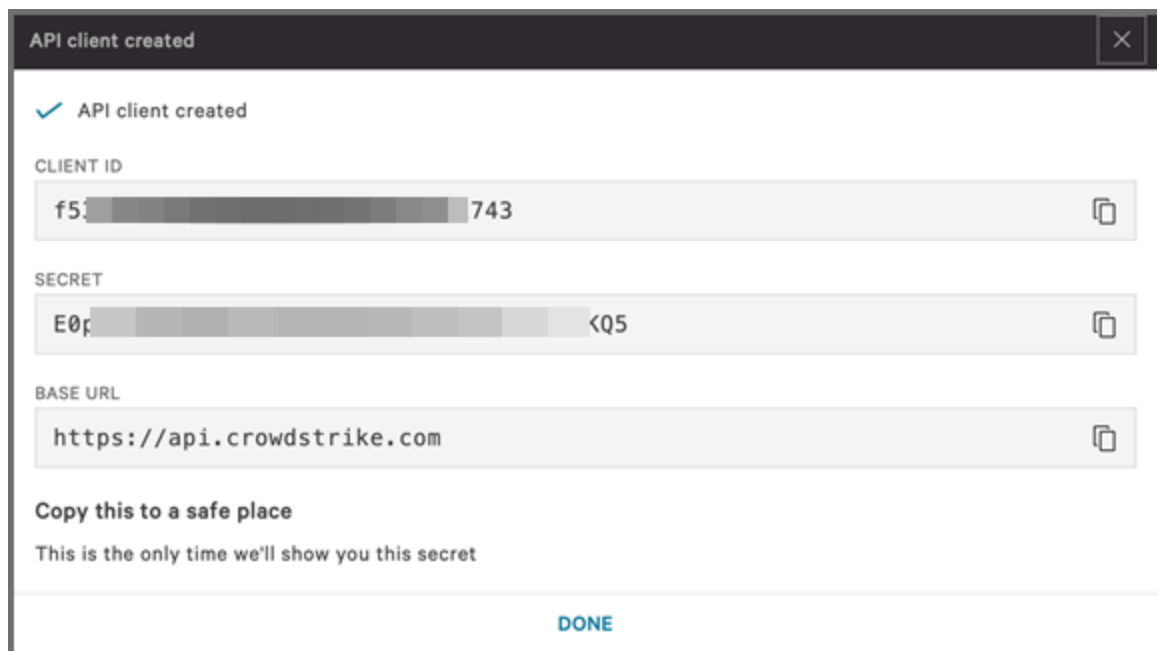
To configure the CrowdStrike server, take the following steps:



For CrowdStrike GovCloud Customers Only - If the CrowdStrike tenant is in one of the GovCloud regions, you must open a support ticket so CrowdStrike Support can enable the streaming API. See CrowdStrike reference article [here](#) for more information.

1. Sign in to the Falcon console.
2. Navigate to **Support > API Clients and Keys > OAuth2 API Clients**.
3. Click **Add new API client**.
4. In the **Client name** field, enter a descriptive client name.
5. For **API SCOPES**, select **Event streams**.
6. Click **Add**.

Keep a record of your API client secret. For security purposes, it is only shown when you create or reset the API client. If you lose your secret, you must reset it, which cuts off access for any integrations that still use the previous secret.



FortiSIEM Configuration

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a CrowdStrike Falcon Credential:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

c.

Settings	Description
Name	Enter a name for the credential
Device Type	CrowdStrike Falcon
Access Protocol	Falcon Streaming API
UUID	Enter the Client ID from the CrowdStrike Server Configuration for the UUID .
API Secret Key	Enter the Secret from the CrowdStrike Server Configuration for the API Secret Key .
Organization	Choose the organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter the host name in base URL from the [CrowdStrike Server Configuration](#) in the **IP/Host Name** field.
For example, `https://api.crowdstrike.com`.
 - b. Select the name of the credential created in step 2 from the **Credentials** drop-down list.
 - c. Click **Save**.
4. 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 5 when connectivity succeeds.
5. An entry is created in **ADMIN > Setup > Pull Events** corresponding to the event pull job. FortiSIEM will start to pull events from the CrowdStrike Cloud service using the Falcon Streaming API.

To test for events received via CrowdStrike:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the CrowdStrike entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from CrowdStrike Cloud Service in the last 15 minutes. You can modify the time interval to get more events.

Protocol	Information Discovered	Used For
Falcon Streaming API	Detection Summary, Authentication Log, Detection Status Update, Indicators of Compromise, Containment Audit Events, IP White-listing events, Sensor Grouping Events.	Security and Compliance
Falcon Data Replicator	Detection Summary, User Activity, Authentication Activity.	Security and Compliance

Cybereason

Support Added: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: Cybereason

Product: Cybereason

Product Information: <https://www.cybereason.com/>

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOGs collected	Used for
Syslog (CEF formatted)		security logs	Security and Compliance monitoring

Configuration

Configure the Cybereason platform to send CEF formatted logs to FortiSIEM. FortiSIEM will automatically parse the logs. No configuration is required in FortiSIEM.

Sample Events

```
Feb 10 13:06:43 xxxx syslogLogger CEF:0|Cybereason|Cybereason||Malop|Malop
Created|10|cs1Label=malopId cs1=11.-1587922454714582908 cs2Label=malopDetectionType cs2=CNC
cs3Label=malopActivityType cs3=MALICIOUS_INFECTION cs4Label=malopSuspect cs4=powershell.exe
cs5Label=malopKeySuspicion cs5=Malicious use of PowerShell / .NET
deviceCustomDate1Label=malopCreationTime deviceCustomDate1=Feb 10 2021, 13:06:43 UTC
deviceCustomDate2Label=malopUpdateTime deviceCustomDate2=Feb 10 2021, 13:06:43 UTC
cn1Label=affectedMachinesCount cn1=1 cn2Label=affectedUsers cn2=1 cs6Label=linkToMalop
cs6=https://cripya.cybereason.net:443/#/malop/11.-1587922454714582908
```

```
Feb 9 08:55:48 XXXX syslogLogger CEF:0|Cybereason|Cybereason||Malop|Malop Machine
Information|10|cs1Label=malopId cs1=11.7905079038751140000 cs2Label=affectedMachine cs2=MACHINE1
deviceCustomDate1Label=malopUpdateTime deviceCustomDate1=Feb 09 2021, 08:55:48 UTC
cn1Label=affectedMachinesCount cn1=6
```

```
Feb 10 13:46:29 XXX auditSyslogLogger
CEF:0|Cybereason|Cybereason||UserAction|Investigation/Query|0|cs1Label=username
cs1=/user@company.com cn1Label=actionSuccess cn1=1 deviceCustomDate1Label=userActionTime
deviceCustomDate1=Feb 10 2021, 13:46:29 UTC cs2Label=QueryDetails cs2=User > Process > Connection
```

Digital Guardian Code Green DLP

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Event](#)

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	1 event type	Security and Compliance

Event Types

In **RESOURCES > Event Types**, Search for "CodeGreen-" in the main content panel **Search...** field to see event types.

Rules

There are no specific rules, but generic rules for Data Leak Protection apply.

Reports

There are no specific reports, but generic rules for Data Leak Protection and Generic Servers apply.

Configuration

Configure Digital Guardian Code Green DLP to send syslog on port 514 to FortiSIEM.

Sample Event

```
<10>1 2017-05-11T12:08:06.380Z ABC-Manager DLP - INCADD incident_id="1.12815.1" managed_device_id="1" number_of_incidents="1" incident_status="New,Audit Only" matched_policies_by_severity="High:C_PHI_MRN / C_MRN_>25;" action_taken="NET_NS_H" matches="55" protocol="SMTP" http_url="" inspected_document="Milla_9.16-4.17__UPDATED.XLSX" source="abc@cda.org" source_ip="1.1.1.1"
```



```
source_port="21752" destination="abc@bcd.edu" destination_ip="2.2.2.2" destination_port="25"  
email_subject="RE: Open Encounters" email_sender="abc@cde.org" email_recipients="abc@bcd.edu;"  
timestamp="2017-05-11 12:06:09 PDT" incidents_  
url=https://aaa.lpch.net/LoadIncidentManagement.do?m=1&id=1,27372
```

ESET NOD32 Anti-Virus

- [What is Discovered and Monitored](#)
- [ESET NOD32 Configuration](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

ESET NOD32 Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in [the device's product documentation](#), and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM Supervisor.
- For **Port**, enter **514**.
- The syslog format should be the same as that shown in the example.

Example Syslog

```
<35313912>Jul 26 18:06:12 HOST01 ERA Server: [2011-07-26 13:06:12.784] V5 [4e2f02148110]
[00000e9c] <SESSION_INFO> Kernel connection from 10.0.52.25:48071 accepted

<35313864>Jul 26 18:06:13 HOST01 ERA Server: [2011-07-26 13:06:13.221] V5 [4e2f02148110]
[00000e9c] <SESSION_INFO> Kernel connection from
10.0.52.25:48071 closed (code 0,took 438ms, name 'HostExample01', mac '00-1E-4F-E8-49-03', product
'ESET NOD32 Antivirus BUSINESS EDITION',
product version '04.00002.00071', virus signature db version '63(20110726)')
```

FortiClient

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Access Credentials for FortiSIEM](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog via FortiAnalyzer (FortiClient > FortiAnalyzer -> FortiSIEM)		Traffic logs (IPSec, VPN, File Cleaning/Blocking) Event logs (Antivirus, Web Filter, Vulnerability Scan, Application Firewall, VPN, WAN Optimization, Update logs)	Security Monitoring and Log analysis

Note: FortiSIEM collects logs from FortiAnalyzer (FAZ).

Event Types

Search for "FortiClient" in the main content panel **Search...** field to see the event types associated with this device under **RESOURCES > Event Types**.

Rules

There are generic rules that trigger for this device as event types are mapped to specific event type groups.

Reports

Generic reports are written for this device as event types are mapped to specific event type groups.

Configuration

Configuring FortiClient to send events to FortiAnalyzer (FAZ).

1. Configure FortiClient to send events to FAZ by following the steps in the knowledge base article [How to integrate EMS in the FortiAnalyzer](#).

2. Configure FAZ to send events to FortiSIEM:

- a. Login to FAZ.
- b. Go to **System Settings > Advanced > Syslog Server**.
- c. Click **Create New**.
- d. Enter the **Name**. It is recommended to use the name of the FortiSIEM Supervisor node.
- e. Set the **IP address (or FQDN)** field to the IP or a fully qualified name of the FortiSIEM node that would parse the log (most likely Collector or Worker/Supervisor).
- f. Retain the **Syslog Server Port** default value '514'.
- g. Click **OK** to save your entries.
- h. Go to **System Settings > Dashboard > CLI Console**.
- i. Type the following in the CLI Console for:

- FAZ 5.1 and older:

```
config system aggregation-client
  edit 1 (or the number for your FSM syslog entry)
    set fwd-log-source-ip original_ip
  end
```

- FAZ 5.6 and newer:

```
config system log-forward
  edit 1 (or the number for your FSM syslog entry)
    set fwd-log-source-ip original_ip
  end
```

- j. Go to **System Settings > Log Forwarding**.
 - k. Click **Create New**.
 - l. Enter the **Name**.
 - m. Select 'Syslog' as **Remote Server Type**.
 - n. Enter the **Server IP** with the IP of the FortiSIEM Server/Collector.
 - o. Retain the **Server Port** default value '514'.
 - p. Set **Reliable Connection** to the default value 'Off'.
Note: Setting this to 'On' will make every log sent from FAZ appear with FAZ's IP and NOT that of the firewall(s). In addition, your network must allow UDP connection between FAZ and FortiSIEM Collector. Otherwise, the logs will not reach the Collector.
 - q. Optional – Use **Log Forwarding Filters** to select specific devices you want to forward log for.
- 3. Follow the steps below to validate that logs are properly flowing from FAZ to FortiSIEM:**
- a. Login to FortiSIEM.
 - b. Click **ANALYTICS** tab and use the filter to perform a real-time search:
 - i. Click on the **Attribute** field to select 'Reporting IP' from the list or enter the same in the field to search.
 - ii. Select '=' **Operator**.
 - iii. In the **Value** field, enter the name of the Fortinet devices from where logs are expected.
Note: This is NOT the IP address of the FAZ but of an original source device, like a FortiGate Firewall. To ensure that everything is being sent/received correctly, you can use multiple IPs.

You will now see events from one, to numerous, source device(s), even though they are all forwarded from a single FAZ device. You can also check **CMDB > Devices** to see whether the devices are appearing within CMDB.

Note: The Relaying IP value in FortiSIEM will not show the IP address of the FAZ but that of the original device which sent the logs to FAZ.

All the device logs appear within FortiSIEM without configuring numerous devices individually.

Access Credentials for FortiSIEM

Setting	Value
Name	<name>
Device Type	Fortinet FortiClient
Access Protocol	WMI
Pull Interval	1 minute
NetBIOS/Domain	The NetBIOS name of servers or domain name
Password config	See Password Configuration

Sample Events

- [Traffic Log](#)
- [Event Log](#)

Traffic Log

```
<116> device=FCTEMS0000000001 severity=medium from=FAZVM64(FAZ-VM0000000001) trigger=EVT2SIEM
log="itime=1489562233 date=2017-03-15 time=00:17:13 logver=2 type=traffic sessionid=N/A
hostname=hostname.local uid=1000000000 devid=FCT8000000000008 fgtserial=FCTEMS0000000005
level=warning regip=10.1.1.1 srcname="Opera" srcproduct=N/A srcip=10.1.1.3 srcport=18398
direction=outbound dstip=10.0.0.4 remotename="aa.com" dstport=20480 user="bb.lee" service=http
proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=webfilter threat="Gambling"
vd=root fctver=1.2.1.1 os="Mac OS X 1.1.1" usingpolicy=N/A url=/ userinitiated=0
browsetime=N/A" ET---> FortiClient-traffic-blocked
```

Event Log

```
<116> device=FCTEMS0036759495 severity=medium from=FAZVM64(FAZ-VM0000000001) trigger=EVT2SIEM1
log="itime=1490237155 date=2017-03-22 time=19:45:55 logver=2 level=info
uid=C4C4E56CE7B04762B053E8F88B8ECF47 vd=root fctver=5.4.2.0862 os="Microsoft Windows Server
2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy=AOFCT fgtserial=N/A
emsserial=FCTEMS0036759495 devid=FCT8003883203338 hostname=sjcitvwfct01 pcdomain=example.net
clientfeature=endpoint deviceip=deviceip=N/A type=event user=N/A id=96953 msg="Endpoint
Control Status changed - Offline""
```

Fortinet FortiClient EMS

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoints (computers). FortiClient EMS provides efficient and effective administration of endpoints running FortiClient. It can control FortiClient to scan devices to find vulnerabilities and collect all vulnerabilities which all FortiClient scans.

For information on FortiEMS Endpoint Tagging, see the FortiSIEM Appendix topic - [FortiEMS Endpoint Tagging](#).

Support Added: FortiSIEM 7.0.0

Vendor Version Tested: FortiClient EMS 7.2.0

Vendor: Fortinet

Product Information: <https://www.fortinet.com/products/endpoint-security/forticlient>

- [Event Types](#)
- [Configuration](#)
- [Sample Events](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortiems" to see the event types associated with this device.

Configuration

- [FortiEMS Configuration](#)
- [FortiSIEM Configuration](#)

FortiEMS Configuration

See the current FortiClient EMS Administration Guide for the latest configuration information. The instructions provided here are based off the [7.2.0 EMS Administration Guide](#).

1. Login to FortiClient EMS.
2. Navigate to **Administration > Administrators**.
3. Click **Add**.
4. Under User source, select **Create a new user**, **Choose from Windows users** or **Choose from LDAP**.
Note: If you selected **Choose from LDAP**, select the desired server from the Authentication Server dropdown list. You must have already configured an authentication server.
5. Click **Next**.
6. In the **Username** field, enter a user name.
7. From the **Role** drop-down list, select **Super administrator**, **Standard administrator**, or **Endpoint administrator**.
8. Click **Next**.

9. In the **Password** field, enter a password.
10. Click **Save**.

FortiSIEM Configuration

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a FortiClient EMS Credential:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

c.

Settings	Description
Name	Enter a name for the credential
Device Type	Fortinet FortiClient EMS
Access Protocol	FORTIEMS_API
Pull Interval	Default is 5 minutes.
Port	Ensure that 443 is entered here.
Serial Number	On your FortiEMS server, navigate to Dashboard > Status to locate your serial number, and enter it in the Serial Number field.
User Name	Enter the FortiClient EMS username created in FortiEMS Configuration .
Password / Confirm Password	Enter the FortiClient EMS user's password in the Password field, and re-enter in the Confirm Password field.
Description (optional)	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Select the name of the credential created in step 2 from the **Credentials** drop-down list.
 - b. Enter the FortiEMS IP address in the **IP/Host Name** field.
 - c. Click **Save**.
4. 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 5 when connectivity succeeds.
5. Navigate to **ADMIN > Setup > Discovery**, and click **New**.
 - a. Enter 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**.
6. Select the identified discovery, and click **Discover**.

7. After discovery succeeds, an entry is created in **ADMIN > Setup > Pull Events** corresponding to the event pull job. FortiSIEM will start to pull events from FortiClient EMS. Events can be queried on the **ANALYTICS** page.

Sample Events

```
[FortiEMS-Vuln-Detected] = {"avatar":0,"client_id":1001,"critical":1,"device_id":"1463","dont_patch":1,"fct_version":"7.0.2.0090","high":4,"host":"John Smith Laptop","ip":"192.0.2.0","last_vuln_scan":1675748166,"low":1,"medium":8,"os_version":"Linux LUBUNTU 16.0.4","patch_status":0,"scan_status":"vulnerable","serverName":"evansr-fsm-lab-321.fortidemo.fortinet.com","serverIp":"198.51.100.0","total":14,"username":"ExampleUser","vblt_running":false}
```

```
[FortiEMS-Vuln-Scan] = {"category":"Applications","client_id":"1770","cve_list":"CVE-2016-7426","cvss":0.0,"device_id":"1353","dont_patch":true,"fct_version":"7.0.2.0090","host":"Jane Doe Desktop","ip":"192.0.2.0","last_scan_time":1676314038,"os_version":"Linux LUBUNTU 14.0.4","patch_status":0,"product_name":null,"reference_page":"http://support.ntp.org/bin/view/Main/NtpSec3071","serverName":"evansr-fsm-lab-321.fortidemo.fortinet.com","serverIp":"198.51.100.0","severity":"Medium","title":"Client rate limiting and server responses","vulnerability_id":38942}
```


Fortinet FortiEDR

Support Added: FortiSIEM 5.3.0

Vendor Version Tested: 7.2.0

Vendor: Fortinet

Product: FortiEDR

Product Information: <https://www.fortinet.com/products/endpoint-security/fortiedr>

- [Integration Points](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	System and Security Events (e.g., file blocked)	Security monitoring

Event Types

In **Admin > Device Support > Event Types**, and search for "FortiEDR" to see the event types associated with this device.

Configuration

Configure FortiEDR system to send logs to FortiSIEM in the supported format (see [Sample Events](#) below)

Step 1 - FortiEDR Syslog Configuration

To configure syslog for FortiEDR, take the following steps:

Note: It is recommended you refer to the latest FortiEDR Administration Guide for the most current information. The latest FortiEDR Admin Guide can be found [here](#).

1. Login to the FortiEDR Central Manager.
2. Navigate to **Administration > Export Settings > Syslog**.
3. Click **Define New Syslog** and fill in the following fields.

Note: If logs must pass across an unprotected medium, see the FortiEDR guide for Configuring Syslog over TLS on FortiSIEM collectors, and set port to 6514, protocol TCP, with Use SSL checked.

Field	Input
Name	Input "FortiSIEM".
Host	Enter the IP address or FQDN of the FortiSIEM Collector.
Port	Input "514".
Protocol	Select UDP.
Use SSL	Make sure the checkbox is unchecked.

- Click the save icon to complete the configuration.

Step 2 - FortiEDR API Configuration

Take the following steps in FortiEDR.

- Login to your FortiEDR device and to go **ADMINISTRATION > LICENSING > <Name>**.
- Give REST API permission to a new or existing user in **ADMINISTRATION > USERS**, and ensure the user has Local Admin permissions.
- Remember the user name and password for your setup in FortiSIEM.

Step 3 - FortiSIEM Configuration

FortiSIEM processes events from this via the Fortinet FortiEDR API. Configure and obtain the user name and password from the API before proceeding.

Complete these steps in the FortiSIEM UI:

- Go to the **ADMIN > Setup > Credentials** tab.
- In **Step 1: Enter Credentials**:
 - Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Fortinet FortiEDR
Access Protocol	FortiEDR_API
Pull Interval	5 minutes
Tenant ID	The FortiEDR tenant ID.
User Name	The user name for your FortiEDR account.
Password	The password for your FortiEDR account.
Confirm Password	Input the same password as above for verification.

Settings	Description
Description	Description about the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
If running FortiEDR v6.2 Cloud or earlier, the deployment URL can be found in the FortiEDR GUI under the **Administration > Tools > "Deployment URL"** section.
If running FortiEDR v7.2 Cloud or later, the deployment URL can be found in the FortiEDR GUI under the **Administration > Settings > "Deployment URL"** section.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiEDR.
5. To see the jobs associated with FortiEDR, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **Analytics**, then enter "FortiEDR" in the search box.

For a video example of FortiSIEM investigation of a FortiEDR Alert, see [here](#).

Sample Events

```
<133>1 2019-09-18T06:42:18.000Z 1.1.1.1 enSilo - - - Organization: Demo;Organization ID:
156646;Event ID: 458478;
Raw Data ID: 1270886879;Device Name: WIN10-VICTIM;Operating System: Windows 10 Pro N;
Process Name: svchost.exe;Process Path: \Device\HarddiskVolume4\Windows\System32\svchost.exe;
Process Type: 64bit;Severity: Critical;Classification: Suspicious;Destination: File Creation;
First Seen: 18-Sep-2019, 02:42:18;Last Seen: 18-Sep-2019, 02:42:18;Action: Blocked;Count: 1;
Certificate: yes;Rules List: File Encryptor - Suspicious file modification;Users: WIN10-VICTIM\U;
MAC Address: 00-0C-29-D4-75-EC;Script: N/A;Script Path: N/A;Autonomous System: N/A;Country: N/A
```

Kaspersy

Vendor: Kaspersy

Product Information: <https://usa.kaspersky.com/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Kaspersky.

Protocol	Metrics Collected	Used For
Syslog	Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Kaspersky-" to see the event types associated with this device.

Rules

There are no specific rules for Kaspersky, however events are categorized and normalized for use by generic FortiSIEM detection rules.

Malwarebytes Breach Remediation

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Malware detection log	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "malwarebytesbreach" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 10 event types defined.

Rules

In **RESOURCES > Rules**, search for "Malware found but not remediated" in the main content panel **Search...** field.

Reports

In **RESOURCES > Reports**, search for "malware found" to see the reports associated with this device.

Examples include:

- Top Computers with Malware Found By Antivirus and Security Gateways
- Top IPs with Malware Found By Antivirus and Security Gateways
- Top IPs with Malware Found By Security Gateways

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
2020-11-25T17:18:46Z 0009NIT-KLUEY CEF:0|Malwarebytes|Malwarebytes Breach Remediation|Version:
4.1.1.84 [eng:Version: 3.0.0.1090 rul:2020.11.25.17 act:Version: 3.2.0.266 sws:Version:
4.3.0.279]|1000|Scan Started|1|cs3=46837c42-2f42-11eb-9c15-025041000001 cs3Label=SessionId
cs5=mbbr scan -full -remove -noreboot cs5Label=CmdLine dvchost=0009NIT-KLUEY
deviceMacAddress=DC:FB:48:92:E9:10 suser=TEST outcome=succeeded
```

Malwarebytes Endpoint Protection

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Malware detection log	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "malwarebytes-" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "Malware found but not remediated" in the main content panel **Search...** field.

Reports

In **RESOURCES > Reports**, search for "malware found" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<45>1 2016-09-23T14:40:35.82-06:00 reportDeviceName Malwarebytes-Endpoint-Security 1552 -  
- {"security_log":{"client_id":"ef5f8fc8-ad0e-46f8-b6d7-1a85d5f73e64","host_name":"Abc-  
cbd","domain":"abc.com","mac_address":"FF-FF-FF-FF-FF","ip_
```

```
address":"10.1.1.1","time":"2016-09-23T14:40:14","threat_level":"Moderate","object_
type":"FileSystem","object":"HKLM\\SOFTWARE\\POLICIES\\GOOGLE\\UPDATE","threat_
name":"PUM.Optional.DisableChromeUpdates","action":"Quarantine","operation":"QUARANTINE","
resolved":true,"logon_user":"dsamuels","data":"data","description":"No
description","source":"MBAM","payload":null,"payload_url":null,"payload_
process":null,"application_path":null,"application":null}}
```

McAfee ePolicy Orchestrator (ePO)

- What is Discovered and Monitored
- Event Types
- Configuration
- Sample Access Protection Violation detected SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Traps			

Event Types

In **ADMIN > Device Support > Event Types**, search for "mcafee epolicy" to see the event types associated with this application or device.

Configuration

FortiSIEM processes events via SNMP traps sent by the device.

Follow the below procedures to configure McAfee ePO to send Threat based SNMP traps to FortiSIEM.

Step 1: Configuring SNMP Server to send Traps from McAfee ePO.

FortiSIEM processes events from a device via SNMP traps sent by the device.

1. Log in to the McAfee ePO web console.
2. Go to **Main Menu > Configuration > Registered Servers**, and click **New Server**.
The **Registered Server Builder** opens.

Configuration

Registered Servers

Registered Server Builder

1 Description 2 Details

Address: IPV4 192.168.100.160

SNMP Version: SNMPv1

Security: Community: fortisiem

SNMPv3 Security

Authoritative Engine ID: 0x800013700465504f5f536572766572

Security Name:

Authentication Protocol: None

Authentication Passphrase:

Confirm Authentication Passphrase:

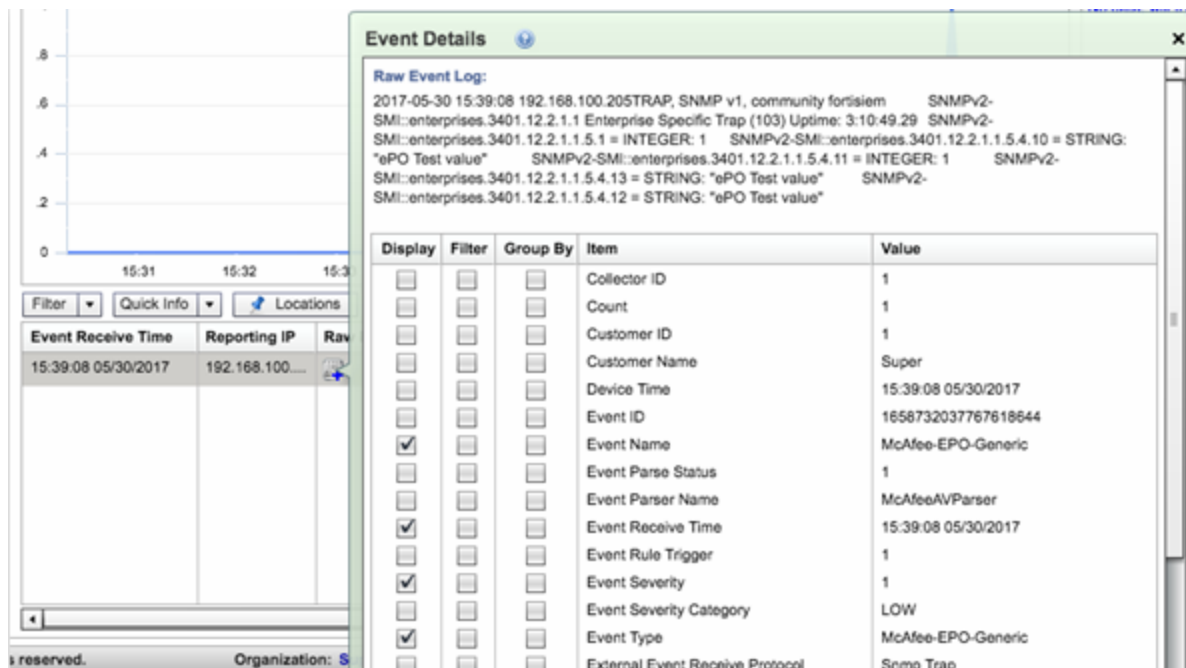
Privacy Protocol: None (AES192/256 requires JCE unlimited strength jurisdiction policy)

Privacy Passphrase:

Confirm Privacy Passphrase:

Test SNMP Traps: Send Test Trap

3. For **Server type**, select **SNMP Server**.
4. For **Name**, enter the IP address of your SNMP server.
5. Enter any **Notes**, and click **Next** to go to the **Details** page.
6. For **Address**, select IP4 from the drop-down and enter the IP/DNS Name for the FortiSIEM virtual appliance and SNMP that will receive the SNMP trap.
7. For **SNMP Version**, select **SNMPv1**.
Note: Only SNMPV1 has been tested and verified on FortiSIEM.
8. For **Community**, enter **public**.
Note: The community string entered here would not be used in FortiSIEM as FortiSIEM accepts traps from McAfee ePO without any configuration.
9. Click **Send Test Trap**, and then click **Save**.
10. Log in to your Supervisor node and use Real Time Search to see if FortiSIEM received the trap. Without any configuration on FortiSIEM, the traps are received under Real time/Historical Analytics. (Search using 'Reporting IP' as McAfee ePO's IP.)



Step 2: Configuring "Automatic Response"

By default, McAfee ePO does not send SNMP Trap alerts for the events that occur. This must be configured.

1. Go to **Main Menu > Automation > Automatic Response**.
2. By default, there are a few Automatic Response configured, but are in a disabled state.
3. Click on **New Response** button.
4. Enter a **Name** for the 'Response'.
5. Set **Status** as 'Enabled' and click **Next**.
6. Click the Ellipsis icon and select the top level under **Select System Tree Group** and click **OK**.
7. On the left side of the same screen, select Threat Handled.

Sample Access Protection Violation detected SNMP Trap

```
2017-05-30 16:24:27 192.168.100.205TRAP, SNMP v1, community fortisiem SNMPv2-
SMI::enterprises.3401.12.2.1.1 Enterprise Specific Trap (101) Uptime: 3:56:08.15 SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.7 = STRING: "Threat_Trigger_Rule"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.30 = STRING: "58F5DD64- 43C5-11E7-0584-000C29219964" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.360 = STRING: "My Organization" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.20 = STRING: "05/30/17 13:20:24 UTC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.50 = STRING: "ENDP_AM_1050" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.510 = "" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.510 =
STRING: "Access Protection" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.520 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.70 = STRING: "WIN2012- SKULLC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.90 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.80 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.500 = STRING: "000c29219964" SNMPv2-
```

```

SMI::enterprises.3401.12.2.1.1.5.2.50 = STRING: "McAfee Endpoint Security"SNMPv2-
SMI::enterprises.3401.12.2.1.1.6.0.00 = STRING: "10.5.0" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.370 = STRING: "Access Protection rule violation detected and
NOT blocked" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.6 = STRING: "Threat" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.1 = INTEGER: 1 SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.390 =
STRING: "Server" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.380 = STRING: "Windows Server 2012
R2" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.50 = STRING: "05/30/17 13:24:05 UTC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.530 = "" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.550 =
STRING: "192.168.100.205" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.540 = STRING:
"192.168.100.205" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.560 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.580 = STRING: "FIREFOX.EXE" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.590 = "" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.570 =
STRING: "WIN2012-SKULLC\Administrator" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.500 = STRING:
"GlobalRoot\Directory\My Group"SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.280 = STRING:
"C:\USERS\ADMINISTRATOR\DOWNLOADS\V3_2994DAT.EXE" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.200 = STRING: "WIN2012- SkullC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.220 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.210 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.230 = "" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.250 =
STRING: "0" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.270 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.260 = "" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.240 =
STRING: "SYSTEM" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.340 = STRING: "IDS_ACTION_WOULD_
BLOCK" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.290 = STRING: "'File' class or access"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.300 = STRING: "1095"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.350 = STRING: "True"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.320 = STRING: "Browsers launching files from the Downloaded
Program Files folder"SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.310 = STRING: "Critical"
SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.330 = STRING: "Access Protection"

```

Microsoft Defender for Endpoint (Previously Microsoft Windows Defender Advanced Threat Protection (ATP))

There are two methods to ingest Microsoft Defender for Endpoint audit log data.

The existing method makes use of Azure Event Hub, see Configuration - [Setup in Azure](#).

FortiSIEM also offers a new ingest method using the Microsoft Graph API, utilizing the Generic HTTPS Polling feature in FortiSIEM 6.6.0 and later.

This integration uses the Microsoft Graph APIs as of this writing. See [Configuring Microsoft Graph Incident API using Generic HTTPS Poller](#) and [Configuring Microsoft Graph Alert API using Generic HTTPS Poller](#).

Configuring Microsoft Graph Incident API using Generic HTTPS Poller or Configuring Microsoft Graph Alert API using Generic HTTPS Poller

The MSDefender 365 Graph Incidents and Alerts APIs for MS365 Defender report data for all Defender services in Azure:

- Microsoft Defender for Endpoint
- Microsoft Defender Vulnerability Management

- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps

You may need to enable the API to work in your tenant.

Using the Generic HTTPS Poller feature, we have two pre-built integrations for the MS365 Defender API endpoints:

- <https://graph.microsoft.com/v1.0/security/incidents>
Reference: <https://learn.microsoft.com/en-us/graph/api/security-list-incidents?view=graph-rest-1.0&tabs=http>
- https://graph.microsoft.com/v1.0/security/alerts_v2
Reference: https://learn.microsoft.com/en-us/graph/api/security-list-alerts_v2?view=graph-rest-1.0&tabs=http

You will create two credentials using the "HTTPS Advanced" protocol, each representing the API call to each endpoint. There are two pre-defined definition files that you can import from this documentation. Use the following links for complete setup instructions.

- [Setup FortiSIEM credential to call the MS365 Defender Graph Incidents API Endpoint](#)
- [Setup FortiSIEM to call the MS365 Defender Graph Alerts_v2 API Endpoint](#)

Main Topics:

- [Configuration](#)
- [Sample Events](#)
- [Legacy Configuration](#)

Configuration

The following Configuration Options are available:

- [Configuring Microsoft Graph Incident API using Generic HTTPS Poller](#)
Note: For general information on Generic HTTPS Poller, see [Generic Log API Poller \(HTTPS Advanced\) Integration](#).
 - [Setup in Azure](#)
 - [Setup FortiSIEM Credential to call the MS365 Defender Graph Incidents API Endpoint](#)
- [Configuring Microsoft Graph Alert API using Generic HTTPS Poller](#)
Note: For general information on Generic HTTPS Poller, see [Generic Log API Poller \(HTTPS Advanced\) Integration](#).
 - [Setup in Azure](#)
 - [Setup FortiSIEM to call the MS365 Defender Graph Alerts_v2 API Endpoint](#)
- [Configuration via Azure Event Hub](#)

- [Azure Event Hub Configuration](#)
- [Configuration in FortiSIEM](#)
- [Microsoft Defender for Endpoint Configuration](#)

Configuring Microsoft Graph Incident API using Generic HTTPS Poller

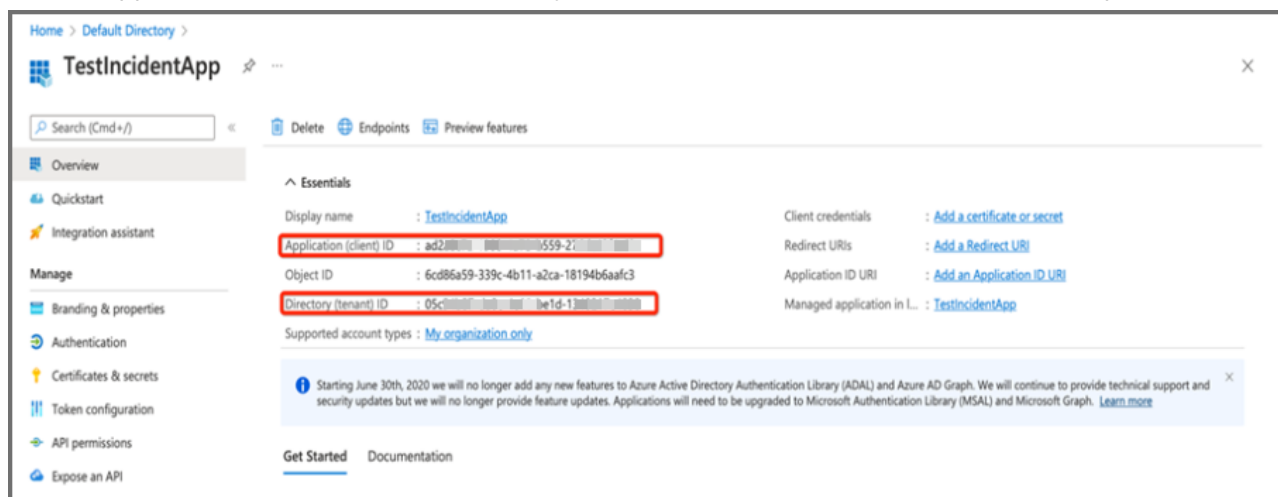
To configure Microsoft Graph Incident API, you will need to perform setup in Azure and in FortiSIEM by taking the following steps.

- [Setup in Azure](#)
- [FortiSIEM credential to call the MS365 Defender Graph Incidents API endpoint](#)

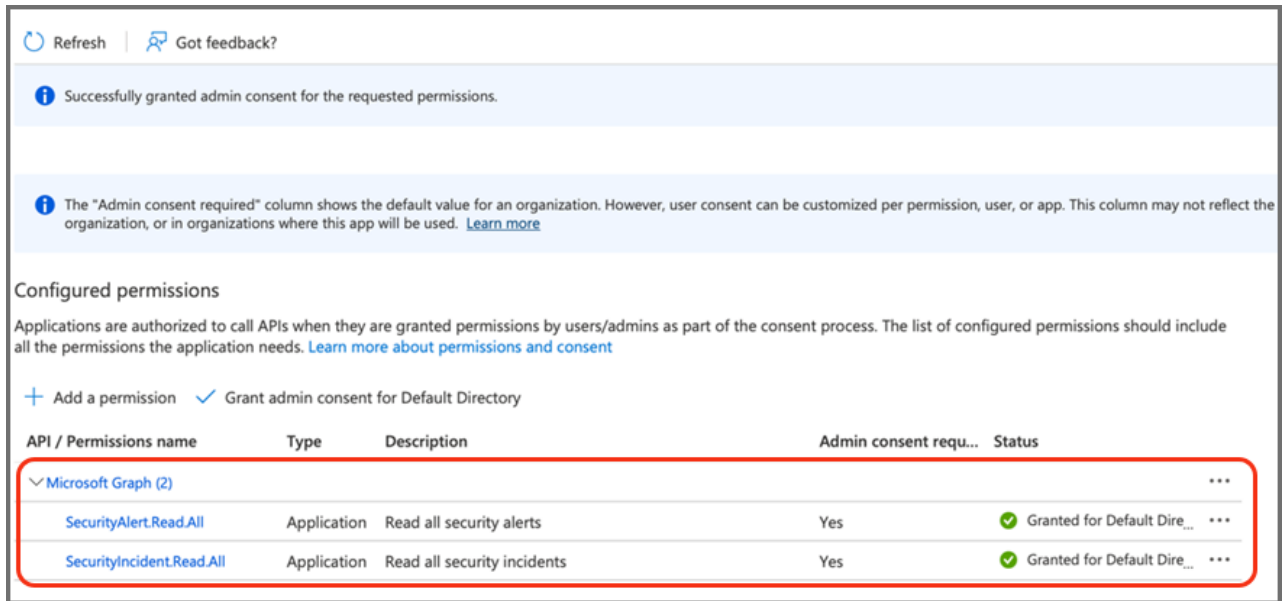
Setup in Azure

Take the following steps to generate credential for the API. This process is the same for the Incident API and Alert API. If this setup was completed for either API, it does not need to be repeated again. In this situation, go to Setup in FortiSIEM for the respective API ([Incident](#), [Alert](#)).

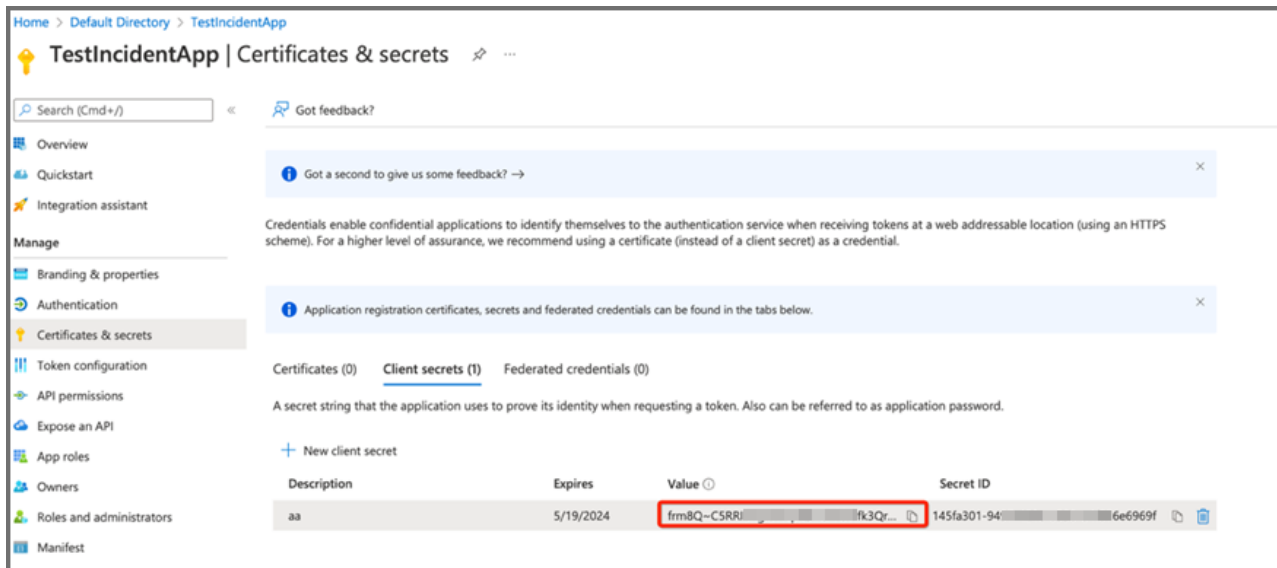
1. Sign in to the [Azure Portal](#).
2. Navigate to **Azure Active Directory > App registrations**.
3. Click **New registration**.
4. Select the new App, and select the **Overview** tab.
5. Get the Application (client) ID and the Directory (tenant) ID, and save it. It will be used in Setup in FortiSIEM.



6. Click **API permissions > Add a permission**, and select **Microsoft Graph**. This adds permission of Microsoft Threat Protection > Application Permission > **SecurityAlert.Read.All** and **SecurityIncident.Read.All** to allow this App to access incident/alert API.



- Click **API permissions > Grant admin consent for Default Directory**, and click **Yes** to granted admin consent for the requested permissions.
- Navigate to **Certificates & secrets > Client secrets**, and click **New client secret** to generate a new client secret.



- Record the value for Setup in FortiSIEM.
Proceed with [Setup FortiSIEM Credential](#) to call the MS365 Defender Graph Incidents API Endpoint or [Setup FortiSIEM](#) to call the MS365 Defender Graph Alerts_v2 API Endpoint.

Setup FortiSIEM Credential to call the MS365 Defender Graph Incidents API Endpoint

To configure the Microsoft Incident API to FortiSIEM, take the following steps.

Create a New Device/Application

1. Navigate to **ADMIN > Device Support > Devices/Apps**.
2. Click **New**.
3. From the Device/Application Type Definition dialog box, take the following steps.
 - a. From the **Category** drop-down list, select **Device**.
 - b. In the **Vendor** field, enter "WindowsDefenderIncident".
 - c. In the **Model** field, enter "Windows Defender".
 - d. In the **Version** field, enter the version number, for example, "1".
 - e. From the **Device/App Group** drop-down list, select **Server**.
 - f. From the **Access Protocol** drop-down list, remove **SSH**, **SNMP**, and **TELNET**.
 - g. From the **Access Protocol** drop-down list, select **HTTPS Advanced**.
 - h. Click **Save**.

Create the Credentials Configuration

1. Navigate to **ADMIN > Setup > Credentials**.
2. Under **Step 1: Enter Credentials**, click **New**.
3. In the **Name** field, enter a name, for example "Windows Defender Incident".
4. From the **Device Type** drop-down list, select the device type you just created in **Create a New Device/Application**.
5. From the Authentication drop-down list, select **Oauth2.0**.
6. Download the following file: [MicrosoftWindowsDefenderIncidentAPI_http_advanced_definition.json](#).
7. Click **Import Definition**.
8. Select the file you just downloaded from step 6, and click **Import**.
9. Click **Yes** to overwrite.
10. Click on the General Parameters icon, and take the following steps.
 - a. In the **Host Name** field, confirm the information is "https://graph.microsoft.com".
 - b. In the **URI Stem** field, confirm the input is "/v1.0/security/incidents".
 - c. From the **HTTP Method** drop-down list, the selection should be **GET**.
 - d. The **Disable SSL Certificate Check** check box should be unchecked.
 - e. The **JSON Response Log Key** field should be "value".
 - f. The **Log Header** field should be "Microsoft 365 Defender Incident".
 - g. Click **OK**.
11. Click the Authentication Parameters icon, and take the following steps.
 - a. With the **General** tab selected, take the following steps.
 - i. In the **Access Token URL** field, enter "https://login.microsoftonline.com/{Tenant ID}/oauth2/v2.0/token" where {Tenant ID} is the tenant ID you recorded from Setup in Azure.
 - ii. In the **Client Id** field, enter the Client ID you recorded from Setup in Azure.
 - iii. In the **Client Secret** field, enter the client secret you recorded from Setup in Azure.
 - iv. Click **OK**.
 - b. Click **Save**.

Create the Credentials Mapping

1. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
2. From the Device Credential Mapping Definition dialog box, take the following steps.
 - a. In the **IP/Host Name** field, enter "graph.microsoft.com".
 - b. From the **Credentials** drop-down list, select the credential you just created.
 - c. Click **Save**.

Test the Credential

1. Ensure the credentials mapping you just created is selected. If not, select it.
2. Under **Step 2: Enter IP Range to Credentials Association**, click the **Test** drop-down list, and select **Test Connectivity without Ping**.

If successful, the new job will appear in the **ADMIN > Setup Pull Events** table. Events can then be queried in **ANALYTICS**.

If you encounter an error, refer to [Common Errors](#) for additional information that may help you resolve the issue.

Configuring Microsoft Graph Alert API using Generic HTTPS Poller

To configure Microsoft Graph Alert API, you will need to perform setup in Azure and in FortiSIEM by taking the following steps. If you have already done the setup in Azure for the Incident API, you can skip **Setup in Azure**, and proceed immediately to [Setup FortiSIEM to call the MS365 Defender Graph Alerts_v2 API Endpoint](#).

- [Setup in Azure](#)
- [Setup FortiSIEM to call the MS365 Defender Graph Alerts_v2 API Endpoint](#)

Setup FortiSIEM to call the MS365 Defender Graph Alerts_v2 API Endpoint

To configure the Microsoft Alert API to FortiSIEM, take the following steps.

Create a New Device/Application

1. Navigate to **ADMIN > Device Support > Devices/Apps**.
2. Click **New**.
3. From the Device/Application Type Definition dialog box, take the following steps.
 - a. From the **Category** drop-down list, select **Device**.
 - b. In the **Vendor** field, enter "WindowsDefenderAlert".
 - c. In the **Model** field, enter "Windows Defender".
 - d. In the **Version** field, enter the version number, for example, "1".
 - e. From the **Device/App Group** drop-down list, select **Server**.
 - f. From the **Access Protocol** drop-down list, remove **SSH**, **SNMP**, and **TELNET**.
 - g. From the **Access Protocol** drop-down list, select **HTTPS Advanced**.
 - h. Click **Save**.

Create the Credentials Configuration

1. Navigate to **ADMIN > Setup > Credentials**.
2. Under **Step 1: Enter Credentials**, click **New**.
3. In the **Name** field, enter a name, for example "Windows Defender Alert".
4. From the **Device Type** drop-down list, select the device type you just created in **Create a New Device/Application**.
5. From the Authentication drop-down list, select **Oauth2.0**.
6. Download the following file: [MicrosoftWindowsDefenderAlertAPI_http_advanced_definition.json](#).
7. Click **Import Definition**.
8. Select the file you just downloaded from step 6, and click **Import**.
9. Click **Yes** to overwrite.
10. Click on the General Parameters icon, and take the following steps.
 - a. In the **Host Name** field, confirm the information is "https://graph.microsoft.com".
 - b. In the **URI Stem** field, confirm the input is "/v1.0/security/alerts_v2".
 - c. From the **HTTP Method** drop-down list, the selection should be **GET**.
 - d. The **Disable SSL Certificate Check** check box should be unchecked.
 - e. The **JSON Response Log Key** field should be "value".
 - f. The **Log Header** field should be "Microsoft 365 Defender Alert".
 - g. Click **OK**.
11. Click the Authentication Parameters icon, and take the following steps.
 - a. With the **General** tab selected, take the following steps.
 - i. In the **Access Token URL** field, enter "https://login.microsoftonline.com/{*Tenant ID*}/oauth2/v2.0/token" where {*Tenant ID*} is the tenant ID you recorded from Setup in Azure.
 - ii. In the **Client Id** field, enter the Client ID you recorded from Setup in Azure.
 - iii. In the **Client Secret** field, enter the client secret you recorded from Setup in Azure.
 - iv. Click **OK**.
 - b. Click **Save**.

Create the Credentials Mapping

1. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
2. From the Device Credential Mapping Definition dialog box, take the following steps.
 - a. In the **IP/Host Name** field, enter "graph.microsoft.com".
 - b. From the **Credentials** drop-down list, select the credential you just created.
 - c. Click **Save**.

Test the Credential

1. Ensure the credentials mapping you just created is selected. If not, select it.
2. Under **Step 2: Enter IP Range to Credentials Association**, click the **Test** drop-down list, and select **Test Connectivity without Ping**.

If successful, the new job will appear in the **ADMIN > Setup Pull Events** table. Events can then be queried in **ANALYTICS**.

If you encounter an error, refer to [Common Errors](#) for additional information that may help you resolve the issue.

Configuration via Azure Event Hub

To configure Microsoft Defender for Endpoint event forwarding to Azure event hub, you will be taking the following general actions.

1. Create an Event Hub Namespace and Event Hub if one does not already exist.
2. Create SAS Policy and generate primary SAS key for authentication.
3. Record the Event Hub Name Space, Event Hub Name, SAS Policy Name, Primary Key, and consumer group for FortiSIEM configuration/authentication.
4. Configure FortiSIEM for Azure Event hub integration and do test Pull.
5. Configure Microsoft Defender for Endpoint raw data streaming to allow event forwarding to Azure Event Hub created earlier.
6. Confirm Raw events are parsed.

Take the steps here to configure Microsoft Defender for Endpoint.

- [Azure Event Hub Configuration](#)
- [Configuration in FortiSIEM](#)
- [Microsoft Defender for Endpoint Configuration](#)

Azure Event Hub Configuration

Create an Event Hub Namespace and Event Hub

Complete these steps in the Azure Portal:

Step 1: Create a Resource Group in Azure

Note: If you already have a Resource Group to use, skip this section

A resource group is a logical collection of Azure resources. All resources are deployed and managed in a resource group. To create a resource group:

1. Login to the Azure portal: <https://portal.azure.com/>
2. Click **Resource groups** in the left navigation pane.
3. Click **Add**.
4. For **Subscription**, select the name of the Azure subscription in which you want to create the resource group.
5. Enter a unique name for the resource group, The system immediately checks to see if the name is available in the currently selected Azure subscription.
6. Select a **Region** for the resource group.
7. Click **Review + Create**.
8. Click **Create** on the **Review + Create** page.

Note: In the example used in **Step 2**, a **Resource Group** called fsm1 was created.

Step 2: Create an Event Hub Namespace

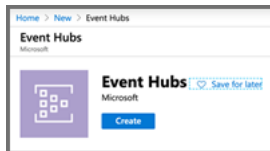
An Event Hub namespace provides a unique scoping container, referenced by its fully-qualified domain name, in which you create one or more event hubs. To create a namespace in your resource group using the portal, complete the following steps:

1. In the Azure portal, click **Create a resource** at the top left of the screen.

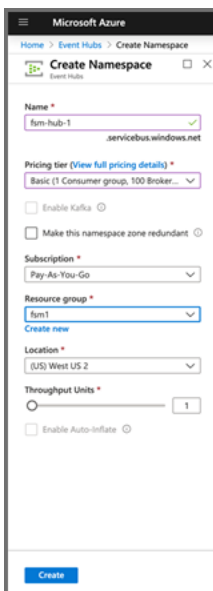
Azure services



2. In the “**Search the Market**” text box, enter **Select All services** in the left menu, select star (*) next to **Event Hubs**, and then click the **Create** button in the **ANALYTICS** category.



3. On the **Create namespace** page, complete the following steps:
 - a. Enter a name for the namespace. The system immediately checks to see if the name is available.
 - b. Choose the pricing tier (**Basic** or **Standard**).
 - c. Select the subscription in which you want to create the namespace.
 - d. Select a location for the namespace.
 - e. Click **Create**. You may have to wait a few minutes for the system to fully provision the resources.



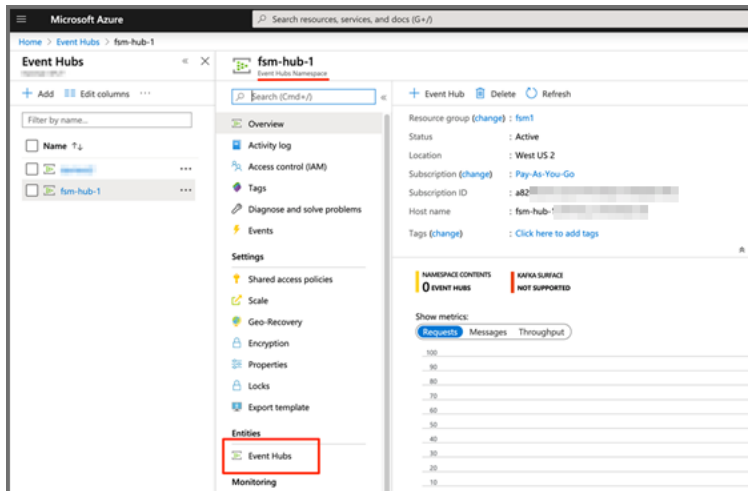
4. Refresh the **Event Hubs** page to see the event hub namespace. You can check the status of the event hub creation in the alerts.

5. Select the namespace. You see the home page for your **Event Hubs Namespace** in the portal.

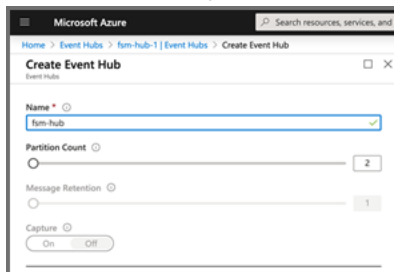
Step 3: Create an Event Hub

To create an event hub within the namespace, follow these steps:

1. In the **Event Hubs Namespace** page, click **Event Hubs** in the left menu.



2. At the top of the window, click **+ Event Hub**.
3. Enter a name for your event hub, then click **Create**.



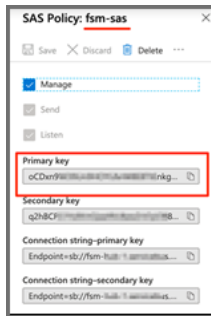
4. You can check the status of the event hub creation in alerts. After the event hub is created, you see it in the list of event hubs.

Step 4: Configure an Event Hub Namespace

1. Select an event hub namespace and go to **Shared access policies**, and then click **+Add**. Enter the **Policy name**, check the **Manage** box, and then click **Create**.



2. Select one of the **Shared Access** policies just created.
3. The Azure Python SDK needs the SAS **Policy name** (defined in step 4.1) and the **Primary key** when creating the credential in FortiSIEM. Copy the primary key and policy name to a text editor for later use.



Note: When the event hub namespace is created, Azure will also create a default Shared Access Policy named **RootManageSharedAccessKey**.

4. Select an event hub namespace and go to **Event Hubs**.
5. Select an event hub and go to **Consumer** group. You can click **+Consumer group** or use default group name **\$default**.

Note: If you have selected **Basic (1 Consumer Group)**, then there will be no option to add a another Consumer group.

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Azure Event Hub
Access Protocol	AZURE PYTHON SDK
Pull Interval	The interval in which FortiSIEM will pull events from Azure Event Hub. Default is 5 minutes.
Event Hub Namespace	The name of the Azure event hub namespace
Event Hub Name	The name of the Azure event hub.
SAS Policy Name	Shared Access (SAS) Policy Name
Primary Key	The name of the primary key
Consumer Group	The name of the consumer group
Description	Description of the device

Based on the example screenshots, this is the configuration in FortiSIEM:

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field. For this integration, enter "azure.com".
 - b. Select the name of your Azure event hub credential from the **Credentials** drop-down list.
 - c. Click **Save**.

4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Azure event hub.
5. To see the jobs associated with Azure, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Azure" in the search box.

Note: Azure services must be configured to write to the Event Hub before there are any events to be collected.

Microsoft Defender for Endpoint Configuration

For the latest Microsoft Defender for Endpoint information, see <https://docs.microsoft.com/en-us/microsoft-365/security/defender/streaming-api-event-hub?view=o365-worldwide>.

Ensure the following steps have been taken before proceeding.

1. An [event hub](#) has been created in your tenant.
2. Your contributor permissions has been configured.
Note: If it hasn't, log in to your [Azure tenant](#), navigate to **Subscriptions > Your subscription > Resource Providers > Register to Microsoft.insights**, and configure your contributor permissions.

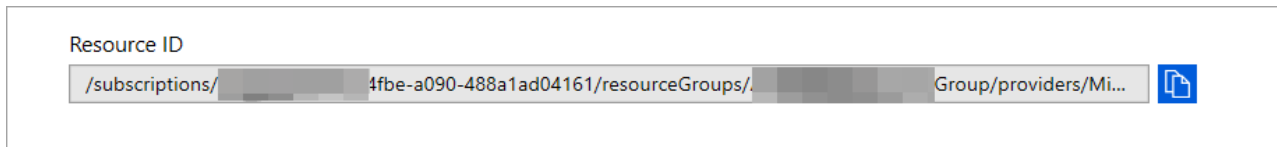
After your event hub namespace has been created, take the following actions.

1. Define the user who will be logging into Microsoft 365 Defender as Contributor.
2. If you are connecting to an application, add the App Registration Service Principal as Reader, Azure Event Hub Data Receiver (this can also be done at Resource Group or Subscription level) by navigating to **Event hubs namespace > Access control (IAM) > Add** and verifying under **Role assignments**.

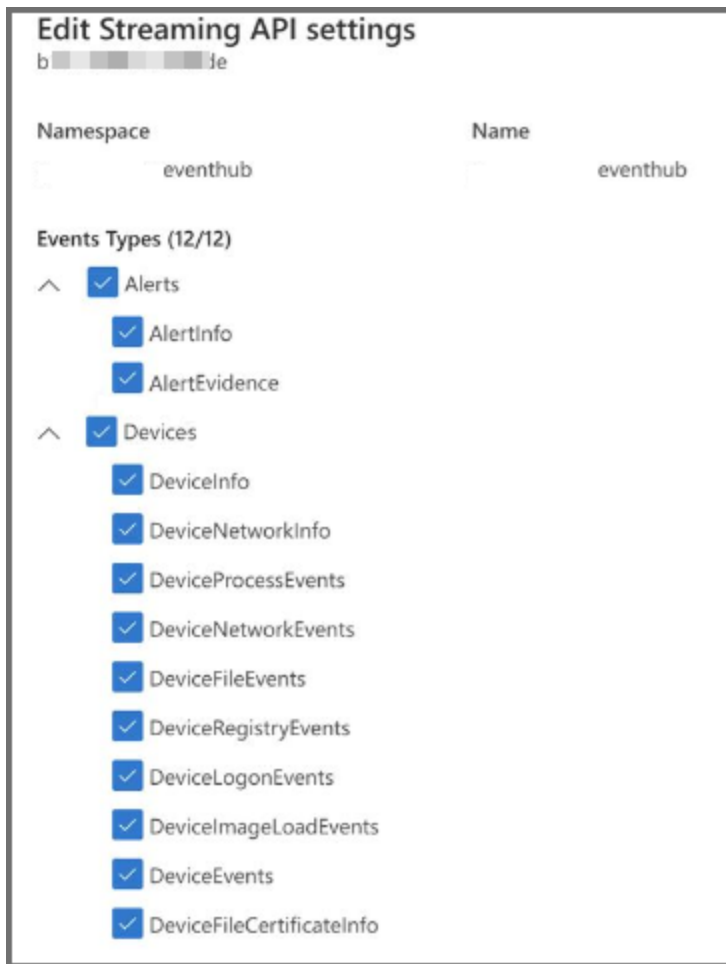
Enable raw data streaming by taking the following steps.

1. Log in to the [Microsoft 365 Defender](#) as a **Global Administrator** or **Security Administrator**.
2. Go to the [Data export settings page](#) in the Microsoft Defender portal.
3. Click on **Add data export settings**.
4. Choose a name for your new settings.
5. Choose **Forward events to Azure Event Hubs**.
6. Type your **Event Hubs** name and your **Event Hubs resource ID**.

To get your **Event Hubs resource ID**, go to your Azure Event Hubs namespace page on [Azure](#) > properties tab > copy the text under **Resource ID**.



7. Choose the events you want to stream and click **Save**.



On the next pull interval, you should see ingested Defender for Endpoint data.

Sample Events

```
{
  "category": "AdvancedHunting-AlertInfo",
  "operationName": "Publish",
  "properties": {
    "AlertId": "da637801291442337370_2831234",
    "AttackTechniques": [
      "\Ingress Tool Transfer (T1105)",
      "\Deobfuscate/Decode Files or Information (T1140)",
      "\Signed Script Proxy Execution (T1216)",
      "\Signed Binary Proxy Execution (T1218)",
      "\CMSTP (T1218.003)",
      "\InstallUtil (T1218.004)",
      "\Mshta (T1218.005)",
      "\Regsvr32 (T1218.010)",
      "\Rundll32 (T1218.011)",
      "\XSL Script Processing (T1220)"
    ],
    "Category": "Execution",
    "DetectionSource": "EDR",
    "MachineGroup": null,
    "ServiceSource": "Microsoft Defender for Endpoint",
    "Severity": "Low",
    "Timestamp": "2022-02-10T22:29:51.4127262Z",
    "Title": "Use of living-off-the-land binary to run malicious code",
    "tenantId": "cdf65b83-41f2-4c0e-97ee-111111111111",
    "time": "2022-02-10T22:32:24.5796030Z"
  }
}
```


[Legacy] Microsoft Defender for Endpoint (Previously Microsoft Windows Defender Advanced Threat Protection (ATP))

Note: This is a Legacy configuration.

As of November 2021, Microsoft has retired the Microsoft Defender ATP SIEM APIs. Defender ATP has also been relabeled as "Microsoft Defender for Endpoint". All integrations using the SIEM APIs will cease to function after the Microsoft Defender for Endpoint SIEM API Deprecation date of April 1st, 2022.

Please follow the [configuration](#) guide to configure Defender for Endpoint event forwarding to Azure event hub.

LEGACY

- [Integration Points](#)
- [Configuring Windows Defender for FortiSIEM REST API Access](#)
- [Configuring FortiSIEM for Windows Defender ATP REST API Access](#)

Integration Points

Protocol	Information Discovered	Used For
Windows Defender API REST API		Security and Compliance

Configuring Windows Defender for FortiSIEM REST API Access

Legacy

Microsoft provides ample documentation [here](#).

Follow the steps specified in 'Enabling SIEM integration', repeated here.

1. Login to Windows Defender Center.
2. Go to **Settings > SIEM**.
3. Select **Enable SIEM integration**.
4. Choose **Generic API**.
5. Click **Save Details to File**.
6. Click **Generate Tokens**.

Configuring FortiSIEM for Windows Defender ATP REST API Access

Legacy

Use the account in the previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

- [Define Windows Defender ATP REST API Access Credential in FortiSIEM](#)
- [Create IP Range to Credential Association and Test Connectivity](#)
- [Viewing Events](#)

Define Windows Defender ATP REST API Access Credential in FortiSIEM

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 1. b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Windows Defender ATP
Access Protocol	Windows Defender ATP Alert REST API
Tenant ID	Enter the Tenant ID for the credential created through the process here .
Password config.	For Manual , enter the Client ID and Client Secret for the credential created here . For CyberArk SDK , see CyberArk SDK Password Configuration . For CyberArk REST API , see CyberArk REST API Password Configuration .
Organization	Choose an organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps.

1. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Select the name of the credential created in step 2 [Configuring FortiSIEM for Windows Defender ATP REST API Access](#) from the **Credentials** drop-down list.
 - b. The **IP/Host Name** field will be automatically filled, but if you wish to change the region, click on the **IP/Host Name** field, and select one of the following:
 - EU: wdatp-alertexporter-eu.windows.com/api/alerts
 - US: wdatp-alertexporter-us.windows.com/api/alerts
 - UK: wdatp-alertexporter-uk.windows.com/api/alerts

If Government Community Cloud (GCC), GCC High, or Department of Defense (DoD) is required, enter the appropriate host name in the **IP/Host Name** field.

GCC: wdatp-alertexporter-us.gcc.securitycenter.windows.us

GCC High and DoD: wdatp-alertexporter-us.securitycenter.windows.us

c. Click **Save**.

2. 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.
3. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Windows Defender Center using the REST API.

Viewing Events

To view events received via Windows Defender ATP REST API, take the following steps:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the Windows Defender ATP entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from Windows Defender Center in the last 15 minutes. You can modify the time interval to get more events.

MobileIron Sentry and Connector

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Syslog	Host name and Device Type from LOG	Over 14 types of security logs	Security and Compliance

Event Types

Go to **ADMIN > Device Support > Event Types** and search for "MobileIron-".

Rules

None

Reports

None

Configuration

Configure MobileIron to send syslog in the supported format to FortiSIEM. No configuration is required in FortiSIEM.

Sample Events

```
Apr  3 04:16:51 mobile-apptunnel.xxxxx.com mi: PRODUCT=Sentry_9.4.0_4,2019 Apr  3 04:16:48 WARN  
(Device=bc7b8d61-b003-49e6-9ef5-76ee5bebd6d9, DeviceIPPort=10.1.1.1:60995, User=Username2,  
Command=POST, Server=25678:domain3.local, Service=Traveler) (AlertOrigin=Sentry, AlertId=HTTP503)
```

Got exception during device-to-server processing, Sentry reporting error to client:java.net.SocketTimeoutException: Read timed out

Netwrix Auditor (via Correlog Windows Agent)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Via Correlog Windows Agent	Host name and Device Type from LOG	2 Security logs	Security and Compliance monitoring

Event Types

Go to **ADMIN > Device Support > Event Types** and search for "Netwrix_Auditor_".

Rules

None

Reports

None

Configuration

Configure Netwrix Auditor to send logs to Correlog Windows Agent. FortiSIEM will automatically parse the logs as long as they appear in the format below.

Sample Events

```
<158>2018 Jul 27 07:20:36 CorreLog_Win_Agent ACME-NETWRIX Netwrix_Auditor_Integration 0: Netwrix_Auditor_Integration_API: DataSource : Windows Server Action : Removed Message: Removed DNS A Where : ACME-DC02 ObjectType : DNS A Who : system What : DNS Server\SAC-DC02\acmegroup.local\ACME-
```

```
TRADE08 IN A 10.150.90.180 1200 When : 2018-07-27T14:15:43Z Details : IP Address: 10.150.90.180,  
TTL: 1200, Container name: acmegroup.local, Owner name: acmegroup.local -
```

Palo Alto Traps Endpoint Security Manager

- What is Discovered and Monitored
- Event Types
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	Over 150 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "PAN-TrapsESM" in the main content panel **Search...** field.

Sample Event Type

```
Sep 28 2016 17:38:48 172.16.183.173 CEF:0|Palo Alto Networks|Traps Agent|3.4.1.16709|Traps Service  
Status Change|Agent|6|rt=Sep 28 2016 17:38:48 dhost=traps-win7x86 duser=Traps msg=Agent Service  
Status Changed: Stopped-> Running
```

```
Sep 28 2016 17:42:04 ESM CEF:0|Palo Alto Networks|Traps ESM|3.4.1.16709|Role  
Edited|Config|3|rt=Sep 28 2016 17:42:04 shost=ESM suser=administrator msg=Role TechWriter was  
added\changed
```

Configuration

Configure Palo Alto Traps Endpoint Security Manager to send syslog on port 514 to FortiSIEM.

SentinelOne Singularity

SentinelOne Singularity can be used to prevent, detect, and respond to cyber attacks.

Support Added: FortiSIEM 7.1.x , 7.2.x, 7.3.x via Content Update, 7.4.1, 7.5.0

Vendor Version Tested: Not Provided

Vendor: SentinelOne

Product: Singularity

Product Information: <https://www.sentinelone.com/platform/>

- [Overview](#)
- [Dashboard](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Log](#)
- [References](#)

Overview

FortiSIEM can use a generic API poller (HTTPS Advanced credential definition) to represent an API endpoint for data ingestion.

This is a low/no code framework where you can define a credential in FortiSIEM of type "HTTPS Advanced". Each credential definition defines a single API endpoint. You can define as many HTTPS advanced credentials as you'd like, with each credential definition defining a single API endpoint.

The generic poller transparently handles tracking the poll intervals (default every 5 minutes) and maintains state to poll each sequential poll interval. If your API is a time series API, you can utilize date parameters to have it generate those at runtime.

Some general guidelines on using the generic poller for custom API integrations:

- This works for JSON APIs only.
- To avoid duplicate events, this method is best used for time series APIs (API supports time range parameters such as "From" and "To" time range to limit the specific window to retrieve data).
- This can be used for status APIs (e.g. get the health of a Firewall) every 5 minutes. Each response object is processed as an individual event.



This requires an understanding of the method of API authentication and the method of pagination of SentinelOne Singularity APIs. Information and template file is provided here to help you create the appropriate SentinelOne Singularity API endpoint configuration(s).

A pre-defined HTTPS Credential Definition for the SentinelOne Singularity activities API template is available [here](#). Or you can choose to manually define/configure the HTTP Advanced Access Protocol with your own customized options.

More information is available in [References](#).

Dashboard

SentinelOne dashboard is available under **Dashboard**.

Rules

Navigate to **Resources > Rules**, and search for "SentinelOne".

Reports

Navigate to **Resources > Reports**, and search for "SentinelOne".

Configuration

Instead of having to manually define all elements of the API for the FortiSIEM credential definition, a pre-defined JSON template is provided. To get this file, click [here](#).

Step 1 - Configuring SentinelOne Singularity

Take the following steps to create a Service User and generate an API Key.

1. Login to your SentinelOne tenant with an Administrator (Admin) user.
2. In the left navigation pane, click **Settings**, select **USERS** from the top screen tabs, and in the menu under **Settings**, choose **Service Users**.
3. From **Actions**, select **Create New Service User**.
4. In the **Name** field, enter a name.
5. (Optional) In the **Description** field, enter any information you wish to include (e.g., Service User for Query Federated Search).
6. From the **Expiration Date** drop-down, select an Expiration Date for your credentials.
Note: SentinelOne recommends setting 1-month or less.
7. From the **Select Scope of Access** menu choose **Account** for the Access Level and ensure that you provide Viewer permissions.
8. Click **Create User**.

After optionally re-authenticating with your MFA code (*only if prompted*), ensure that you copy your API Token or you will have to repeat steps 2-8 again.

Step 2 - Configuring FortiSIEM

Take the following steps to configure a credential for FortiSIEM.

1. Login to FortiSIEM as an administrator.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the **Access Method Definition** window, input the following:
 - a. In the **Name** field, enter the name of the credential. For this example, enter "SentinelOne_Activities".
 - b. From the **Device Type** drop-down list, select **SentinelOne Singularity**.
 - c. **Access Protocol** should have **HTTPS Advanced** pre-selected.
5. Click **Import Definition**.
 - a. Click **Choose File** and select the SentinelOne JSON template file you downloaded, then click **Import**.
 - b. When the prompt "Definition will be overwritten, continue?" appears, click **Yes**.
6. Click the Edit icon next to **General Parameters**.
 - a. In the **Host Name** field, replace the existing name with your Sentinel One Singularity URL: your-domain-here.sentinelone.net
 - b. Click **OK**.
7. Click the Edit icon next to **Authentication Parameters**.
 - a. In the **API Key Value** field, enter the following string **exactly** (minus the double quotation characters):
"APIToken yourapikey"



Key Explanation: SentinelOne sends the API token in the Authorization header, but the value in the header is a hard coded APIToken + your API key separated by a single whitespace. This is functionally equivalent to passing a header in curl with

```
curl -H 'Authorization: APIToken xxxxx'  
https://myexample.sentinelone.net
```

- b. Click **OK**.
8. Click **Save**.

Step 3 - Credential to Device Mapping and Event Pulling

Take the following steps to create the Credential to Device Mapping, and start pulling events.

1. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.

Note: If you have more than one collector, first select the collector from the drop-down prior to clicking **+**. If you have 1 collector or no collectors, this drop-down does not appear.
2. Select the Credential you just defined, "SentinelOne_Activities".

The **IP/Host Name** field is pre-populated.
3. Click **Save**.
4. Select the Credential to Device Mapping and click the **Test** drop-down list and select **Test Connectivity without Ping**.
5. In the next 5 minutes the first events will come in. Click the **Pull Events** tab to monitor.

Step 4 - Checking SentinelOne Events in Analytics

To check events from **Analytics**, take the following steps.

1. Navigate to **Analytics > Search**.
2. Click inside the "Edit Filters and Time Range..." field, then enter the following search query:

Event Type CONTAIN S1-Singularity-Activity

Filter By: Event Keywords Event Attribute CMDB Attribute Clear All Load Save

Paren	Attribute	Operator	Value	Paren	Next	Row
⊖	⊕ Event Type	CONTAIN	S1-Singularity-Activity	⊖	⊕ AND OR ⊕	🗑️

Time Range: Real-time Relative Absolute

Last 10 Minutes

Trend Interval: Auto

Result Limit: 100 K rows

Apply & Run Apply Cancel

3. Click **Apply & Run**, and you should see events coming in.

Sample Log

```
Jul 23 00:33:28 2025 yoursubdomain.sentinelone.net 1.1.1.1 SENTINELONE_ACTIVITIES:
{"accountId": "2082727357056638789", "accountName": "LabAccount", "activityType": 5232,
"activityUuid": "2f9843ee-69c5-4fcb-b00e-257d8d0a44f6", "agentId": "24231111107991",
"agentUpdatedVersion": null, "comments": null, "createdAt": "2025-07-23T00:27:27.233611Z",
"data": {"accountName": "LabAccount", "action": "Block", "application": null,
"applicationType": "any", "computerName": "LAB01", "createdByUsername": test.user@example.com
(test.user@example.com), "direction": "any", "durationOfMeasurement": 60, "fullScopeDetails":
"Group Default Group in Site Default site of Account LabAccount", "fullScopeDetailsPath":
"Global / LabAccount / Default site / Default Group", "groupName": "Default Group",
"ipAddress": "2.2.2.2", "localHost": null, "localHostType": "any", "localPortType": "any",
"localPorts": null, "locationNames": ["Fallback", "Prod2 Ext"], "numberOfEvents": 8, "order":
48, "osTypes": ["windows"], "processId": 1820, "processName":
\\device\\harddiskvolume2\\windows\\system32\\svchost.exe, "protocol": null, "remoteHostTypes":
["range"], "remoteHosts": ["224.0.0.0", "239.255.255.255"], "remotePortType": "any",
"remotePorts": null, "reportedDirection": "outbound", "reportedLocalHost": null,
"reportedLocalPort": "", "reportedProtocol": "", "reportedRemoteHost": "224.0.0.252",
"reportedRemotePort": "", "ruleDescription": null, "ruleId": 2255188848135565064, "ruleName":
"Block broadcast and multicast traffic-external", "ruleScopeLevel": "account", "ruleScopeName":
"LabAccount", "siteName": "Default site", "status": "Enabled", "tagNames": [], "description":
null, "groupId": "2082727358893743954", "groupName": "Default Group", "hash": null, "id":
```

```
"2264937978012492262", "osFamily": null, "primaryDescription": "Firewall Control blocked traffic on the Endpoint LAB01 because of rule Block broadcast and multicast traffic-external in account LabAccount.", "secondaryDescription": "IP address: 1.1.1.1", "siteId": "208272323736", "siteName": "Default site", "threatId": null, "updatedAt": "2025-07-23T00:27:27.233612Z", "userId": null}
```

References

For a complete reference to Generic Log API Poller (HTTPS Advanced) Integration, see [here](#).

API Details

In our reference example, the following API integration is being built.

```
{{baseUrl}}/web/api/v2.1/activities
```

Example:

```
your-domain-here.sentinelone.net/web/api/v2.1/activities
```

Authentication Details

This API uses an API key in the Authorization header in the following format:

```
'Authorization' : 'APIToken <your api key>'
```

For example, a curl would be:

```
curl -H 'Authorization: APIToken xxxxx' https://mydomain.sentinelone.net/web/api/v2.1/activities
```

Time Range Parameters

This API supports a few time range parameters shown in the following table. The generic poller example on this page uses (createdAt__between).

API	Description
createdAt__gt	Activity occurred greater than the given time (ISO 8601 timestamp), e.g. 2018-02-27T04:49:26.257525Z.
createdAt__lt	Activity occurred less than the given time (ISO 8601 timestamp), e.g. 2018-02-27T04:49:26.257525Z.
createdAt__gte	Same as createdAt__gt, but inclusive (from and including the given time range).
createdAt__lte	Same as createdAt__lt, but inclusive (up to and including the given time range).
createdAt__between	Uses the format (inclusive time ranges) in epoch millis "from time" – "to time", e.g. 1514978764288-1514978999999.

As stated in [Overview](#), the selection is arbitrary, as all cases are supported. A date parameter could be defined with `createdAt__gte` (dynamically generated at runtime each poll cycle to represent the "from" time or the last poll time) – each runtime of the script the last poll time is set to this value.

`createdAt__lte` (dynamically generated at runtime each poll cycle to represent the "to" time or current runtime) – each runtime of the script the current execution time minus a standard delay is set to this value.

Both can be used in conjunction with each other, or opt for the single range parameter (`createdAt__between`).

Pagination Details

This particular SentinelOne API (and potentially many others) uses cursor based pagination.

When making the first API call, Fortinet includes the configuration supplied parameters and other filter parameters if supplied, such as `activityTypes`. On that first API response, if there is more than one page of data, you will get a cursor in the "nextCursor" value in the response body of the first API call.

"nextCursor" : "xxxxx"

We can tell the HTTPS Advanced credential to look for this next value, and use it in the next API call with the additional parameter `?cursor=xxxxx`

Note: SentinelOne deviates from most other cursor based pagination implementations. Normally when a cursor is obtained and used, you no longer need to supply the date parameters on subsequent API calls. In SentinelOne's case, the original date and filter parameters must be supplied along with the next page cursor. This type of cursor pagination can be configured by checking the "Include All Parameters in Every Request" checkbox.

The screenshot shows a configuration window titled "Access Method Definition > HTTPS ADVANCED Log API". It has four tabs: "Header", "Parameter", "Body", and "Pagination", with "Pagination" being the active tab. The configuration includes the following fields:

- Pagination Method:** A dropdown menu set to "Custom Next Cursor".
- Cursor Key Name:** A text input field containing "cursor".
- Cursor Type:** A dropdown menu set to "parameter".
- Next Cursor Name:** A text input field containing "nextCursor".
- Include All Parameters in Every Request:** A checkbox that is checked. This checkbox and its label are enclosed in a green rectangular box, with a green arrow pointing to it from the left.

At the bottom of the window are two buttons: "OK" and "Cancel".

Sophos Central

- [Integration Points](#)
- [Event Types](#)
- [Configuring Sophos Central for API Access](#)
- [Configuring FortiSIEM for Sophos Central for API Access](#)

Integration Points

Protocol	Information Discovered	Used For
Sophos Central API	Endpoint suspicious activity detected by Sophos agent	Security and Compliance

Event Types

Over 20 events are parsed. See event types in **RESOURCES > Event Types** by searching for "Sophos-Central" in the main content panel **Search...** field.

Configuring Sophos Central for API Access

Sophos provides ample documentation [here](#).

1. Login to [Sophos Central Website](#).
2. Go to **Global Settings > API Token Management**. Click **Add Token**.
The Token will display.
3. Note the following information for later use:
 - a. Get **Host Name** from **API Access URL** (part after https://).
 - b. Get **Authorization** from **API Access URL + Headers** (part after Authorization:Basic).
 - c. Get **API Key** from Headers (part between **x-api-key:** and **Authorization Basic**).

Configuring FortiSIEM for Sophos Central for API Access

Use the account in the previous step to enable FortiSIEM access. For FortiSIEM configuration, follow the steps [here](#).

- [Define Sophos Central Credential in FortiSIEM](#)
- [Create IP Range to Credential Association and Test Connectivity](#)
- [Viewing Pull Events](#)

Define Sophos Central Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a Sophos Central credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Sophos Central
Access Protocol	Sophos Central API
Authorization	Enter the Authorization created in the previous section - step 3b above.
URI	Fill in the URI field as: gateway/siem/v1/events
API Key	Enter the API Key created in the previous section - step 3c.
Organization	Choose the organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter the **Hostname** created [here](#) - step 3a in the **IP/Host Name** field.
 - b. Select the name of the credential created in step 2 of [Define Sophos Central Credential in FortiSIEM](#) from the **Credentials** drop-down list.
 - c. Click **Save**.
2. 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. If it succeeds, the credential is correct.
3. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Sophos Central using the Sophos Central API.

Viewing Pull Events

To view events received via Sophos Central:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the Windows Defender ATP entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from Sophos Central in the last 15 minutes. You can modify the time interval to get more events.

Sophos Endpoint Security and Control

- What is Discovered and Monitored
- Event Types
- Sophos Configuration
- Sample SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Event Types

In **ADMIN > Device Support > Event Types**, search for "sophos endpoint" to see the event types associated with this application or device.

Sophos Configuration

SNMP Trap

FortiSIEM processes Sophos Endpoint control events via SNMP traps sent from the management console. Configure the management console to send SNMP traps to FortiSIEM, and the system will automatically recognize the messages.

SNMP Traps are configured within the Sophos policies.

1. In the **Policies** pane, double-click the policy you want to change.
2. In the **policy** dialog, in the **Configure** panel, click **Messaging**.
3. In the **Messaging** dialog, go to the **SNMP messaging** tab and select **Enable SNMP messaging**.
4. In the **Messages to send** panel, select the types of event for which you want Sophos Endpoint Security and Control to send SNMP messages.
5. In the **SNMP trap destination** field, enter the IP address of the recipient.
6. In the **SNMP community name** field, enter the SNMP community name.

Sample SNMP Trap

```
2011-05-03 18:22:32 172.15.30.8(via UDP: [172.15.30.8]:1216) TRAP, SNMP v1, community public
SNMPv2-SMI::enterprises.2604.2.1.1.1 Enterprise Specific Trap (1) Uptime: 5:59:55.31
SNMPv2-SMI::enterprises.2604.2.1.1.2.1.1 = STRING: "File \\\"C:\\WINDOWS\\system32\\LDPackage.dll\\\""
```

```
belongs to virus/spyware 'Mal/Generic-S'. "SNMPv2-SMI::enterprises.2604.2.1.1.2.2.2 = STRING:  
"9.5.5"
```

Symantec Endpoint Protection

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Symantec Endpoint Protection Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "symantec endpoint" to see the event types associated with this device.

Symantec Endpoint Protection Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device.

- [Configuring Log Transmission to FortiSIEM](#)
- [Configuring the Types of Logs to Send to FortiSIEM](#)

Configuring Log Transmission to FortiSIEM

1. Log in to Symantec Endpoint Protection Manager.
2. Go to **Admin > Configure External Logging > Servers > General**.
3. Select **Enable Transmission of Logs to a Syslog Server**.
4. For **Syslog Server**, enter the IP address of the FortiSIEM virtual appliance.
5. For **UDP Destination Port**, enter **514**.

Configuring the Types of Logs to Send to FortiSIEM

1. Go to **Admin > Configure External Logging > Servers > Log Filter**.
2. Select the types of logs and events you want to send to FortiSIEM.

Sample Syslog

```
<13>Feb 23 12:36:37 QA-V-Win03-App1.Acme.net SymAntiVirus 0 2701170C2410,3,2,1,QA-V-WIN03-APP1,Administrator,,,,,16777216,"Scan started on selected drives and folders and all extensions.",1235421384,,0,,,,0,,,,,,{C11B44CF-35C9-4342-AB3D-E0E9E3756510},,(IP)-0.0.0.0,,ACME,00:50:56:A3:30:2F,11.0.1000.1112,,,,,,0,,,,
<54>Jun 11 12:24:38 SymantecServer sjdevswinapp05: Site: Site sjdevswinapp05,Server: sjdevswinapp05,Domain: Default,Admin: admin,Administrator log on failed
<54>Jun 11 12:24:51 SymantecServer sjdevswinapp05: Site: Site sjdevswinapp05,Server: sjdevswinapp05,Domain: Default,Admin: admin,Administrator log on succeeded
<54>Feb 23 13:08:29 SymantecServer sjdevswinapp05: Virus found,Computer name: Filer,Source: Real Time Scan,Risk name: EICAR Test String,Occurrences: 1,C:/Documents and Settings/Administrator.ACME/Local Settings/Temp/vpqz3cxj.com,"",Actual action: Cleaned by deletion,Requested action: Cleaned,Secondary action: Quarantined,Event time: 2009-02-23 21:06:51,Inserted: 2009-02-23 21:08:29,End: 2009-02-23 21:06:51,Domain: Default,Group: Global\Acme,Server: sjdevswinapp05,User: Administrator,Source computer: ,Source IP: 0.0.0.0

Mar 16 15:11:06 SymantecServer aschq97: NF77088-PCA,Local: 192.168.128.255,Local: 138,Local: FFFFFFFFFFFFFFFF,Remote: 192.168.128.86,Remote: ,Remote: 138,Remote: 0015C53B9216,UDP,Inbound,Begin: 2009-03-16 15:05:02,End: 2009-03-16 15:05:02,Occurrences: 1,Application: C:/WINDOWS/system32/ntoskrnl.exe,Rule: Allow local file sharing,Location: Default,User: ,Domain: ASC
<54>Feb 24 11:51:19 SymantecServer sjdevswinapp05: QA-V-Win03-App2,[SID: 20352] HTTP Whisker/Libwhisker Scan (1) detected. Traffic has been allowed from this application: C:\WINDOWS\system32\ntoskrnl.exe,Local: 0.0.0.0,Local: 000000000000,Remote: ,Remote: 192.168.1.4,Remote: 000000000000,Inbound,TCP,Intrusion ID: 0,Begin: 2009-02-24 11:50:01,End: 2009-02-24 11:50:01,Occurrences: 1,Application: C:/WINDOWS/system32/ntoskrnl.exe,Location: Default,User: Administrator,Domain: ACME
<54>Jul 28 08:08:52 SymantecServer corpepp01: 6910p-X751008R,Category: 2,Symantec AntiVirus,New virus definition file loaded. Version: 130727ag.
<54>Jul 28 08:09:32 SymantecServer corpepp01: CORPMIO-H4VYWB1,Category: 2,Symantec AntiVirus,Symantec Endpoint Protection services shutdown was successful.
<52>Jul 28 08:10:13 SymantecServer corpepp01: TEMPEXP02,Category: 0,Smc,Failed to disable Windows firewall
<54>Jul 28 08:08:52 SymantecServer corpepp01: 8440p-X0491JYR,Category: 0,Smc,Connected to Symantec Endpoint Protection Manager (10.0.11.17)
<54>Jul 28 08:08:52 SymantecServer corpepp01: 8440p-X0491JYR,Category: 0,Smc,Disconnected from Symantec Endpoint Protection Manager (10.0.11.17)
<54>Jul 28 08:09:52 SymantecServer corpepp01: CORPES-3042,Category: 0,Smc,Connected to Symantec Endpoint Protection Manager (corphqpepp01)
<54>Jul 28 08:09:52 SymantecServer corpepp01: CORPES-3042,Category: 0,Smc,Disconnected from Symantec Endpoint Protection Manager (corpepp01)
<54>Jul 28 08:09:32 SymantecServer corpepp01: CORPMIO-H4VYWB1,Category: 0,Smc,Network Threat Protection - - Engine version: 11.0.480 Windows Version info: Operating System: Windows XP (5.1.2600 Service Pack 3) Network info: No.0 "Local Area Connection 3" 00-15-c5-46-58-1e "Broadcom NetXtreme 57xx Gigabit Controller" 10.0.208.66
<54>Jul 28 07:55:32 SymantecServer corpepp01: tol-user1,Blocked,Unauthorized NT call rejected by
```

```
protection driver.,System,Begin: 2011-07-27 15:29:57,End: 2011-07-27 15:29:57,Rule: Built-in  
rule,6092,AcroRd32.exe,0,None,"FuncID=74H, RetAddr=18005CH",User: user1,Domain: HST
```

Symantec SEPM

- [Configuring Symantec SEPM](#)
- [Receiving Events in FortiSIEM](#)

Configuring Symantec SEPM

follow these steps to configure Symantec SEPM to send logs to FortiSIEM. For more information about Symantec SEPM, see the *SEPM Installation and Administration Guide*:

<https://support.symantec.com/us/en/article.DOC10654.html>

1. In the Symantec SEPM console, go to **Admin > Servers**.
2. Click the local site or remote site that you want to export log data from.
3. Click **Configure External Logging**.
4. On the **General** tab, in the **Update Frequency** list box, select how often to send the log.
5. In the **Master Logging Server** list box, select the management server to send the logs to. If you use SQL Server and connect multiple management servers to the database, then specify only one server as the **Master Logging Server**.
6. Check **Enable Transmission of Logs to a Syslog Server** (FortiSIEM).
7. Provide the following information. Be sure that syslog server IP and Port can be reached from SEPM.
 - a. **Syslog Server**—Enter the IP address or domain name of the Syslog server that will receive the log data (in this case, the IP of FortiSIEM).
 - b. **Destination Port**—Select the protocol to use, and enter the destination port that the Syslog server uses to listen for Syslog messages. (for example, UDP 514 for FortiSIEM).
 - c. **Log Facility**—Enter the number of the log facility that you want to the Syslog configuration file to use, or use the default value. Valid values range from 0 to 23.
8. On the **Log Filter** tab, check which logs to export

Receiving Events in FortiSIEM

1. Check for events in FortiSIEM. Go to the **ANALYTICS** page and search for "Symantec".
2. Check for the device added by log. Go to **CMDB > Devices**.

Tanium Connect

- [Integration Points](#)
- [Event Types](#)
- [Configuring Tanium Connect](#)
- [Configuring FortiSIEM](#)

Integration Points

Protocol	Information Discovered	Used For
syslog	Endpoint security logs	Security and Compliance

Event Types

Currently, 4 events are parsed. See event types in **RESOURCES > Event Types** and search for "TaniumConnect-" in the main content panel **Search...** field. The user can extend the parser to add other events.

Configuring Tanium Connect

Follow [Tanium Connect documentation](#) to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes Tanium Connect syslog as long it follows the following format as shown in the sample syslog:

```
<134>1 2018-09-06T02:50:02.762000+00:00 tanium-server-1 Tanium 7020 - [Comply-  
Deployment-Status---Deployment-5@017472 Installed=true Version=3.0.45 Type=full  
Installed1=true Version1=8u131-e1 Comply---Has-Latest-Tools=true Count=2
```

Trend Micro Interscan Web Filter

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	15 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "TrendMicro-InterscanWeb-" in the main content panel **Search...** field.

Sample Event Type:

```
<130>abc.com: <Mon, 18 Sep 2017 10:00:48,IST> [EVT_URL_BLOCKING|LOG_CRIT] Blocked URL log tk_username=1.1.1.1,tk_date_field=2017-09-18 10:00:48+0530,tk_protocol=https,tk_url=https://google.com:443/,tk_malicious_entity=,tk_file_name=,tk_entity_name=,tk_action=,tk_scan_type=user defined,tk_blocked_by=rule,tk_rule_name=google.com,tk_opp_id=0,tk_group_name=None,tk_category=URL Blocking,tk_uid=0099253425-0ecd0076872a9d0ace16,tk_filter_action=0
```

```
<134>abc.com: <Mon, 18 Sep 2017 10:00:48,IST> [EVT_URL_ACCESS_TRACKING|LOG_INFO] Access tracking log tk_username=1.1.1.1,tk_url=http://aaa.com/pc/SHAREitSubscription.xml,tk_size=0,tk_date_field=2017-09-18 10:00:48+0530,tk_protocol=http,tk_mime_content=unknown/unknown,tk_server=abc.com,tk_client_ip=1.1.1.1,tk_server_ip=2.2.2.2,tk_domain=aaa.com,tk_path=pc/SHAREitSubscription.xml,tk_file_name=SHAREitSubscription.xml,tk_operation=GET,tk_uid=0099253421-bdd7d4ce063b924a2342,tk_category=56,tk_category_type=0
```

```
<134>abc.com: <Mon, 18 Sep 2017 10:00:59,IST> [EVT_PERFORMANCE|LOG_INFO] Performance log tk_server=abc.com,tk_date_field=2017-09-18 10:00:59+0530,tk_metric_id=Number of FTP Processes,tk_metric_value=6,
```

Rules

There are no specific rules, but generic rules for Web Filters and Generic Servers apply.

Reports

There are no specific reports, but generic rules for Web Filters and Generic Servers apply.

Configuration

Configure TrendMicro Interscan Web Filter to send syslog on port 514 to FortiSIEM.

Trend Micro Intrusion Defense Firewall (IDF)

- What is Discovered and Monitored
- Trend Micro Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Trend Micro Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in [the device's product documentation](#), and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog

```
<134>May 31 15:24:34 DSK-FT11XL1 dsa_mpld: REASON=PLD:Disallow_Web_Proxy_Autodiscovery_Protocol  
REV IN= OUT=Local_Area_Connection  
MAC=00:26:B9:80:74:71:2C:6B:F5:35:4E:00:08:00 SRC=192.168.20.2 DST=192.168.13.39 LEN=133 PROTO=UDP  
SPT=53 DPT=58187 CNT=1 act=Reset POS=0  
SPOS=0 NOTE=CVE-2007-5355 FLAGS=0
```

Trend Micro OfficeScan

- What is Discovered and Monitored
- Configuration
- Example SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Configuration

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send SNMP traps to FortiSIEM as directed in [the device's product documentation](#), and FortiSIEM will parse the contents.

Example SNMP Trap

```
2011-04-14 02:17:54 192.168.20.214(via UDP: [192.168.20.214]:45440) TRAP, SNMP v1, community
public      SNMPv2-SMI::enterprises.6101 Enterprise Specific Trap (5) Uptime: 0:00:00.30      SNMPv2-
SMI::enterprises.6101.141 = STRING: "Virus/Malware: Eicar_test_file Computer: SJDEVVWINDB05
Domain: ABC File: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\yc8eayj0.com Date/Time: 4/10/2008 14:23:26
Result: Virus successfully detected, cannot perform the Clean action (Quarantine) "
```

Trend Vision One

Support Added: FortiSIEM 7.1.1

Vendor Version Tested: Not Provided

Vendor: Trend Micro

Product Information: https://www.trendmicro.com/en_us/business.html

Trend Vision One is the solution name for the new Trend Vision One platform that enhances and consolidates detection, investigation and response capabilities across email, endpoints, servers, cloud workloads and networks.

- [Event Types](#)
- [Configuration](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "Trend_Vision" to see the event types associated with this device.

Configuration

- [Required API Permissions for Trend Vision One Integration](#)
- [Acquire Trend Vision One API Token](#)
- [FortiSIEM Setup](#)

Required API Permissions for Trend Vision One Integration

The following APIs are called for the Trend Vision One integration. The required API key role permissions are provided here.

Note: See <https://automation.trendmicro.com/xdr/api-v3> for more information.

API	API Key Role Permissions Required
Audit Logs v3.0/audit/logs	• View, filter, and search • Export And Download
Workbench v3.0/workbench/alerts	• View, filter, and search
Sandbox Analysis v3.0/sandbox/analysisResults	• View, filter, and search • Submit objects
Search v3.0/search/endpointActivities v3.0/search/detections v3.0/search/emailActivities v3.0/search/networkActivities v3.0/search/containerActivities	• View, filter, and search

Acquire Trend Vision One API Token

FortiSIEM requires an API token from Trend Vision One. Take the following steps from your Trend Vision One console.

1. Navigate to **Administration > User Accounts**.
2. Click on your Account Name.
3. Copy the authentication token and place it in a secure location.
Note: By default, an authentication token expires one year after its creation. However, a Master Administrator can delete and re-generate a token at any time.
4. Click **Close**.

FortiSIEM Setup

Take the following steps to configure Trend Vision One with FortiSIEM.

Create Trend Vision One Credential

1. Login to FortiSIEM as an administrator.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the **Access Method Definition** window, input the following:
 - a. In the **Name** field, enter "TrendMicro Trend Vision One".
 - b. From the **Device Type** drop-down list, select **TrendMicro Trend Vision One**.
 - c. In the **Token** field, enter/paste the authentication token information from [Acquire Trend Vision One API Token](#).
 - d. In the **Confirm Token** field, enter/paste the same authentication token information from [Acquire Trend Vision One API Token](#).
 - e. Click **Save**.
 - f. Ensure the Trend Vision One Credential is selected. If it isn't, select it.

Create IP to Credential Mapping

Under **Step 2: Enter IP Range to Credential Associations**, take the following steps.

1. Click **New**.
2. From the **Device Credential Mapping Definition** window, take the following steps.
 - a. From the **Credentials** drop-down list, select the credential you just created in the above steps.
 - b. In the **IP/Host Name** field, enter the host name based on your appropriate region.

Region	Host Name
Australia	api.au.xdr.trendmicro.com
European Union	api.eu.xdr.trendmicro.com
India	api.in.xdr.trendmicro.com
Japan	api.xdr.trendmicro.co.jp
Singapore	api.sg.xdr.trendmicro.com
United States	api.xdr.trendmicro.com

- c. Click **Save**.

Verifying Mapping

To verify your configuration, take the following steps.

1. Under **Step 2: Enter IP Range to Credential Associations**, select the "IP to Credential Mapping" you just created.
2. Click the **Test** drop-down, and select **Test Connectivity without Ping**.
3. Navigate to **Admin > Setup > Pull Events**. The new job will appear in the Pull Events table.
4. Events can be queried from the **Analytics** page by doing a search of Raw Event Log CONTAIN Trend_Vision_One_.

Firewalls

FortiSIEM supports these firewalls for discovery and monitoring.

- [Check Point FireWall-1](#)
- [Check Point Provider-1](#)
 - [CLM for Check Point Provider-1](#)
 - [CMA for Check Point Provider-1](#)
 - [MDS for Check Point Provider-1](#)
 - [MLM for Check Point Provider-1](#)
- [Check Point VSX](#)
- [Cisco Adaptive Security Appliance \(ASA\)](#)
- [Cisco Firepower Threat Defense \(FTD\)](#)
- [Clavister Firewall](#)
- [Cyberoam Firewall](#)
- [Dell SonicWALL](#)
- [Fortinet FortiGate Firewall](#)
- [Hillstone Firewall](#)
- [Imperva SecureSphere Web App Firewall](#)
- [Juniper Networks SSG](#)
- [McAfee Firewall Enterprise \(Sidewinder\)](#)
- [Palo Alto](#)
- [Sophos UTM](#)
- [Stormshield Network Security](#)
- [UserGate UTM Firewall](#)
- [WatchGuard Firebox](#)
- [Zscaler Internet Access \(ZIA\)](#)

Check Point FireWall-1

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Check Point

Product Information: <https://www.checkpoint.com/products/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Firewall model and version, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
LEA		All traffic and system logs	Security and Compliance
Syslog		Traffic and logs sent via the CheckPoint Log Exporter tool via CEF format.	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "firewall-1" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog CEF Format](#)
- [LEA](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog CEF Format

The Syslog CEF format is a more straightforward integration method than LEA, and collects similar information. To configure CheckPoint for syslog event forwarding, use the CheckPoint Log Exporter tool that details on how to configure the CheckPoint Firewall at the following URL:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323.

Configure the tool to send Syslog in CEF format to FortiSIEM.

Example CEF Format Log

```
CEF:0|Check Point|VPN-1 & FireWall-1|Check Point|Log|domain-udp|Unknown|act=Accept
deviceDirection=0 rt=1528095651000 spt=49005 dpt=53 cs2Label=Rule Name cs2=Implicit Cleanup layer_
name=LRSK Security layer_name=LRSK Application layer_uuid=ab166dee-e955-4b8f-a5e7-6234fbaeefde
layer_uuid=5549ebc0-70a4-43d1-8ec6-ca53f2306a62 match_id=34 match_id=33554431 parent_rule=0
parent_rule=0 rule_action=Accept rule_action=Accept rule_uid=78f0ba26-4d36-4352-96dd-0303a2a31cbb
ifname=eth2 logid=0 loguid={0x5b14e3a3,0x0,0xfbffff0a,0xc0000008} origin=1.1.1.1
originsicname=CN\=gate2,0\=pgkeeper.citadele.lrs.lt.wj6ide sequencenum=99 version=5 dst=1.1.1.1
inzone=Internal outzone=Internal product=VPN-1 & FireWall-1 proto=17 service_id=domain-udp
src=1.1.1.1
```

LEA

Sending events from Checkpoint to FortiSIEM in Syslog CEF format can be a more straightforward integration method than using LEA Integration method.

Following the steps here for LEA configuration.

- [Add FortiSIEM as a Managed Node](#)
- [Create an OPSEC Application for FortiSIEM](#)
- [Create a Firewall Policy for FortiSIEM](#)

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host...**
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like FortiSIEMVA.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.
4. Enter a **Name** for your OPSEC application, like OPSEC_FortiSIEMVA.
5. For **Host**, select the FortiSIEM host.
6. Under **Client Entities**, select **LEA** and **CPMI**.
For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like CN=OPSEC_FortiSIEMVA,0=MDS..i6g4zq.
This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In **Servers and Opsec > OPSEC Applications**, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.

9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Checkpoint Firewall-1
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Check Point Provider-1 Firewall

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration Overview](#)
- [Component Configuration for Domain-Level Audit Logs](#)
- [Component Configuration for Firewall Logs](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Firewall model and version, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
LEA		All traffic and system logs	Security and Compliance

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration Overview

The configuration of Check Point Provider-1 depends on the type of log that you want sent to FortiSIEM. There are two options:

- **Domain level audit logs**, which contain information such as domain creation, editing, etc.
- **Firewall logs**, which include both audit log for firewall policy creation, editing, etc., and traffic logs

These logs are generated and stored among four different components:

- **Multi-Domain Server (MDS)**, where domains are configured and certificates have to be generated.
- **Multi-Domain Log Module (MLM)**, where domain logs are stored.
- **Customer Management Add-on (CMA)**, the customer management module.
- **Customer Log Module (CLM)**, which consolidates logs for an individual customer/domain.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Component Configuration for Domain-Level Audit Logs

1. [Configure MDS](#).
2. Use the **Client SIC** obtained while configuring MDS to configure MLM.
3. [Pull logs from MLM](#).

Component Configuration for Firewall Logs

1. [Configure CMA](#).
2. Use the **Client SIC** obtained while configuring CMA to configure CLM.
3. [Pull logs from CLM](#).

If you want to pull firewall logs from a domain, you have to configure CLM for that domain.

See these topics for instructions on how to configure each component for Check Point Provider-1 firewalls.

- [Configuring MDS for Check Point Provider-1 Firewalls](#)
- [Configuring MLM for Check Point Provider-1 Firewalls](#)
- [Configuring CMA for Check Point Provider-1 Firewalls](#)
- [Configuring CLM for Check Point Provider-1 Firewalls](#)

Configuring CMA for Check Point Provider-1 Firewalls

The Check Point Provider-1 Customer Management Add-On (CMA) creates logs that are then consolidated by the Customer Log Module (CLM). If you want the CLM to send logs to FortiSIEM, you must first configure the CMA and obtain the **AO Client SIC** to configure access credentials for communication between the CLM and FortiSIEM.

- [Configuration](#)
- [Settings for Access Credentials](#)

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get CMA Server SIC for Setting Up FortiSIEM Access Credentials

1. Log in to your Check Point SmartDomain Manager.
2. Click the **General** tab.
3. Select **Domain Contents**.
4. Select the **Domain Management Server** and right-click to select **Launch Application > Smart Dashboard**.
5. Select the **Desktop** tab.
6. Select the **Network Objects** icon.
7. Double-click on the **Domain Management Server** to view the **General Properties** dialog.
8. Click **Test SIC Status...**

Note the value for **DN**. You will use this for the **CMA Server SIC** setting when creating the access credentials for FortiSIEM to access your CMA server.

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host...**
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like FortiSIEMVA.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.
4. Enter a **Name** for your OPSEC application, like OPSEC_FortiSIEMVA.
5. For **Host**, select the FortiSIEM host.
6. Under **Client Entities**, select **LEA** and **CPMI**.
For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like CN= OPSEC_FortiSIEMVA,0=MDS..i6g4zq.
This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In Servers and Opsec > OPSEC Applications, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.
9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall CLA SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point Provider-1 Firewall CMA. When you complete the access credentials, click **Generate Certificate** to establish access between your firewall and FortiSIEM.

Setting	Value
Name	CMA
Device Type	Checkpoint Provider-1 CMA
Access Protocol	CheckPoint SSLCA
CMA IP	The IPS address of your server
Checkpoint LEA Port	The port used by LEA on your server
AO Client SIC	The DN number of your FortiSIEM OPSEC application
CMA Server SIC	The DN number of your server
CPMI Port	The port used by CPMI on your server
Activation Key	The password you used in creating your OPSEC application

Configuring CLM for Check Point Provider-1 Firewalls

- [Prerequisites](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

Prerequisites

- You must first configure and discover the Check Point CLA and obtain the **AO Client SIC** before you can configure the Customer Log Module (CLM). The AO Client SIC is generated when you create the FortiSIEM OPSEC application.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get CLM Server SIC for Creating FortiSIEM Access Credentials

1. Log in to your Check Point SmartDomain Manager.
2. Click the **General** tab.
3. Select **Domain Contents**.
4. Select the **Domain Management Server** and right-click to select **Launch Application > Smart Dashboard**.
5. Select the **Desktop** tab.
6. Click the **Network Objects** icon.
7. Under **Check Point**, select the CLM host and double-click to open the **General Properties** dialog.
8. Under Secure Internal Communication, click **Test SIC Status...**
9. In the **SIC Status** dialog, note the value for **DN**.
This is the CLM Server SIC that you will use in setting up access credentials for the CLM in FortiSIEM.
10. Click **Close**.
11. Click **OK**.

Install the Database

1. In the **Actions** menu, select **Policy > Install Database...**
2. Select the MDS Server and the CLM, and then **OK**.
The database will install in both locations.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall CLM SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point Provider-1 Firewall CMA. When you complete the access credentials, click **Generate Certificate** to establish access between your firewall and FortiSIEM.

Setting	Value
Name	CLM
Device Type	Checkpoint Provider-1 CLM
Access Protocol	CheckPoint SSLCA
CLM IP	The IP address of the host where your CLM is located
Checkpoint LEA Port	The port used by LEA on your server
AO Client SIC	The DN number of your FortiSIEM OPSEC application
CLM Server SIC	The DN number of your server
CPMI Port	The port used by CPMI on your server
CMA IP	The IP address of the host where your CMA is located

Configuring MDS for Check Point Provider-1 Firewalls

- [Configuration](#)
- [Settings for Access Credentials](#)

The Check Point Provider-1 firewall Multi-Domain Server (MDS) is where domains are configured and certificates are generated for communicating with FortiSIEM. If you want to have domain logs from the Multi-Domain Log Module (MLM) sent from your firewall to FortiSIEM, you must first configure and discover MDS, then use the AO Client SIC created for your FortiSIEM OPSEC application to configure the access credentials for MLM.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get the MDS Server SIC for FortiSIEM Access Credentials

You will use the MDS Server SIC to create access credentials in FortiSIEM for communicating with your server.

1. Log in to your Check Point SmartDomain Manager.
2. Select **Multi-Domain Server Contents**.
3. Select **MDS**, and then right-click to select **Configure Multi-Domain Server...**
4. In the **General** tab, under **Secure Internet Communication**, note the value for **DN**.

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host...**
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like FortiSIEMVA.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.

4. Enter a **Name** for your OPSEC application, like OPSEC_FortiSIEMVA.
5. For **Host**, select the FortiSIEM host.
6. Under **Client Entities**, select **LEA** and **CPMI**.
For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like CN= OPSEC_FortiSIEMVA,0=MDS..i6g4zq.
This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In Servers and Opsec > OPSEC Applications, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.
9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

Copy Secure Internal Communication (SIC) certificates

Copy Client SIC

1. Go to **Manage > Server and OPSEC Applications**.
2. Select **OPSEC Application** and then right-click to select the FortiSIEM application.
3. Click **Edit**.
4. Enter the **SIC DN** of your application.

Copy Server SIC

1. In the **Firewall** tab, go to **Manage**.
2. Click the **Network Object** icon, and then right-click to select **Check Point Gateway**.
3. Click **Edit**.
4. Enter the **SIC DN**.

5. If there isn't a field to enter the SIC DN, click **Test SIC Status** and a dialog will display the SIC DN.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point Provider-1 Firewall MDS. When you complete the access credentials, click **Generate Certificate** to establish access between your firewall and FortiSIEM.

Setting	Value
Name	MDS
Device Type	Checkpoint Provider-1 MDS
Access Protocol	CheckPoint SSLCA
MDS IP	The IPS address of your server
Checkpoint LEA Port	The port used by LEA on your server
AO Client SIC	The DN number of your FortiSIEM OPSEC application
MDS Server SIC	The DN number of your server
Password	The password associated with the administrative user
CPMI Port	The port used by CPMI on your server
Activation Key	The password you used in creating your OPSEC application

1. Generate a certificate for MDS communication in FortiSIEM.
 - a. Configure Checkpoint Provider-1 MDS credential as shown below.

Activation key was the one-time password you input in [Create an OPSEC Application for FortiSIEM](#)
AO Client SIC was generated in [Create an OPSEC Application for FortiSIEM](#)
MDS Server SIC was generated in [Get the MDS Server SIC for FortiSIEM Access Credentials](#)
 - b. Click **Generate Certificate**. It should be successful. Note that the button will be labeled **Regenerate Certificate** if you have already generated the certificate once.

Configuring MLM for Check Point Provider-1 Firewalls

- [Prerequisites](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

Prerequisites

- You must [configure and discover your Check Point Provider-1 MDS](#) before you configure the Multi-Domain Log Module (MLM). You will need the **AO Client SIC** that was generated when you created your FortiSIEM OPSEC application in the MDS to set up the access credentials for your MLM in FortiSIEM.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get MLM Server SIC for Setting Up FortiSIEM Access Credentials

1. Log in to your Check Point SmartDomain Manager.
2. In the **General** tab, click **Multi-Domain Server Contents**.
3. Right-click **MLM** and select **Configure Multi-Domain Server...**
4. Next to **Communication**, note the value for **DN**.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Settings for Check Point Provider-1 MLM SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point MLM over SSLCA.

Setting	Value
Name	MLM
Device Type	Checkpoint Provider-1 MLM
Access Protocol	CheckPoint SSLCA
MLM IP	The IPS address of your module

Setting	Value
Checkpoint LEA Port	The port used by LEA on your server
AO Client SIC	The DN number of your FortiSIEM OPSEC application
MLM Server SIC	The DN number of your MLM
CPMI Port	The port used by CPMI on your server
MDS IP	The IP address of your MDS server

Check Point VSX Firewall

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

FortiSIEM uses SNMP, LEA to discover the device and to collect logs, configurations and performance metrics.

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Firewall model and version, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
LEA		All traffic and system logs	Security and Compliance

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [LEA](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

LEA

- [Add FortiSIEM as a Managed Node](#)
- [Create an OPSEC Application for FortiSIEM](#)
- [Create a Firewall Policy for FortiSIEM](#)
- [Copy Client SIC](#)
- [Copy Server SIC](#)

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host....**
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like FortiSIEMVA.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.
4. Enter a **Name** for your OPSEC application, like OPSEC_FortiSIEMVA.
5. For **Host**, select the FortiSIEM host.
6. Under **Client Entities**, select **LEA** and **CPMI**.
For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like CN=OPSEC_FortiSIEMVA,0=MDS..i6g4zq.
This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In Servers and Opsec > OPSEC Applications, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.
9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

Copy Client SIC

1. Go to **Manage > Server and OPSEC Applications**.
2. Select **OPSEC Application** and then right-click to select the FortiSIEM application.
3. Click **Edit**.
4. Enter the **SIC DN** of your application.

Copy Server SIC

1. In the **Firewall** tab, go to **Manage**.
2. Click the **Network Object** icon, and then right-click to select **Check Point Gateway**.
3. Click **Edit**.
4. Enter the **SIC DN**.
5. If there isn't a field to enter the SIC DN, click **Test SIC Status** and a dialog will display the SIC DN.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Checkpoint VSX
Access Protocol	See Access Credentials
Port	See Access Credentials

Setting	Value
Password config	See Password Configuration

Cisco Adaptive Security Appliance (ASA)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [NetFlow](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	Host name, Hardware model, Network interfaces, Hardware component details: serial number, model, manufacturer, software and firmware versions of components such as fan, power supply, network cards etc., Operating system version, SSM modules such as IPS	Uptime, CPU and Memory utilization, Free processor and I/O memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
SNMP (V1, V2c, V3)		Hardware health: temperature, fan and power supply status	
SNMP (V1, V2c, V3)	OSPF connectivity, neighbors, state, OSPF Area	OSPF state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)		IPSec VPN Phase 1 tunnel metrics: local and remote Vpn Ip addresses, Tunnel status, Tunnel Uptime,	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
		Received/Sent BitsPerSec, Received/Sent Packets, Received/Sent BitsPerSec, Received/Sent Dropped Packets, Received/Sent Rejected Exchanges, Received/Sent Invalid Exchanges Invalid Received Pkt Dropped, Received Exchanges Rejected, Received Exchanges Invalid IPSec VPN Phase 2 tunnel metrics: local and remote Vpn Ip addresses, Tunnel status, Tunnel Uptime, Received/Sent BitsPerSec, Received/Sent Packets, Received/Sent BitsPerSec, Received/Sent Dropped Packets, Received/Sent Auth Failed, Sent Encrypted Failed, Received Decrypt failed, Received Replay Failed	
Telnet/SSH	Running and startup configuration, Interface security levels, Routing tables, Image file name, Flash memory size	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
Telnet/SSH		Virtual context for multi-context firewalls, ASA interface security levels needed for setting source and destination IP address in syslog based on interface security level comparisons, ASA name mappings from IP addresses to locally unique names needed for converting names in syslog to IP addresses	
Netflow (V9)	Open server ports	Traffic logs (for ASA 8.x and above)	Security and Compliance
Syslog	Device type	All traffic and system logs	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "asa-" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "asa" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "asa" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- Don't configure SNMP Trap.
- Don't configure ASA to send logs via SNMP trap, as FortiSIEM doesn't parse them.

Check Security Levels

Make sure interface security levels are appropriately set in FortiSIEM. In your FortiSIEM Supervisor, go to **CMDB > Devices > Network Device > Firewall** and select your firewall. Click the **Interface** tab, and make sure that the inside security level is 100, outside is 0 and other interfaces are in between. This information can either be discovered via SSH or entered manually after SNMP discovery. Without correct security level information, ASA traffic built and teardown logs can not be parsed correctly (they may not have correct source and destination addresses and ports).

Configuration topics are listed here.

- [SNMP](#)
- [Syslog](#)
- [Sample Cisco ASA Syslog](#)
- [SSH](#)
- [Telnet](#)
- [Commands Used During Telnet/SSH Communication](#)

SNMP

1. Log in to your ASA with administrative privileges.
2. Configure SNMP with this command.

```
snmp-server host <ASA Interface name> <FortiSIEM IP> poll community <community string>
```

Syslog

1. Log in to your ASA with administrative privileges.
2. Enter configuration mode (config terminal).
3. Enter the following commands:
 - no names
 - logging enable
 - logging timestamp
 - logging monitor errors
 - logging buffered errors
 - logging trap debugging

- logging debug-trace
- logging history errors
- logging asdm errors
- logging mail emergencies
- logging facility 16
- logging host <ASA interface name> <FortiSIEM IP>

Example using Cisco ASA + Anyconnect vpn logging / SNMP

Notes regarding example:

Replace content marked with *<italicized_text>* with your actual content.

Replace “inside” with the egress firewall zone that logging traffic is sent

Avoid whitespace in your passwords, group name, and username.

```
logging enable
logging timestamp
no logging hide username
logging host inside <IP_address_of_your_FortiSIEM_collector>
logging class auth trap informational
logging class config trap informational
logging class vpn trap informational
logging class vpnc trap debugging
logging class webvpn trap informational
logging class svc trap informational

snmp-server enable
snmp-server group <SNMP_group_name> v3 priv
snmp-server user <Your_chosen_SNMPv3_username> <SNMP_group_name> v3 auth sha <Your_SHA_password>
priv aes 128 <Your_AES_Password>
snmp-server host inside <IP_address_of_your_FortiSIEM_collector> poll version 3 <Your_chosen_
SNMPv3_username>
```

Sample Cisco ASA Syslog

```
<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)
```

SSH

1. Log in to your ASA with administrative privileges.
2. Configure SSH with this command.

```
ssh <FortiSIEM IP> <FortiSIEM IP netmask> <ASA interface name>
```

Telnet

1. Log in to your ASA with administrative privileges.
2. Configure telnet with this command.

```
telnet <FortiSIEM IP> <FortiSIEM IP netmask> <ASA interface name>
```

Commands Used During Telnet/SSH Communication

The following commands are used for discovery and performance monitoring via SSH. Make sure that the accounts associated with the ASA access credentials you set up in FortiSIEM have permission to execute these commands.

Critical Commands

It is critical to have no `names` and `logging timestamp` commands in the configuration, or logs will not be parsed correctly.

1. `show startup-config`
2. `show running-config`
3. `show version`
4. `show flash`
5. `show context`
6. `show ip route`
7. `enable`
8. `terminal pager 0`
9. `terminal length 0`

NetFlow

NetFlow is an optimized protocol for collecting high volume traffic logs. You should configure NetFlow with ASM, the ASA device manager.

- [Set Up FortiSIEM as a NetFlow Receiver](#)
- [Create a NetFlow Service Policy](#)
- [Configure the Template Refresh Rate](#)

Set Up FortiSIEM as a NetFlow Receiver

1. Login to ASDM.
2. Go to **Configuration > Device Management > Logging > Netflow**.
3. Under Collectors, click **Add**.
4. For **Interface**, select the ASA interface over which NetFlow will be sent to FortiSIEM.
5. For **IP Address or Host Name**, enter the IP address or host name for your FortiSIEM virtual appliance that will receive the NetFlow logs.
6. For **UDP Port**, enter **2055**.
7. Click **OK**.

8. Select **Disable redundant syslog messages**.
This prevents the netflow equivalent events from being also sent via syslog.
9. Click **Apply**.

Create a NetFlow Service Policy

1. Go to **Configuration > Firewall > Service Policy Rules**.
2. Click **Add**.
The **Service Policy Wizard** will launch.
3. Select **Global - apply to all interfaces**, and then click **Next**.
4. For **Traffic Match Criteria**, select **Source and Destination IP Address**, and then click **Next**.
5. For **Source** and **Destination**, select **Any**, and then click **Next**.
6. For **Flow Event Type**, select **All**.
7. For **Collectors**, select the FortiSIEM virtual appliance IP address.
8. Click **OK**.

Configure the Template Refresh Rate

This is an optional step. The template refresh rate is the number of minutes between sending a template record to FortiSIEM. The default is 30 minutes, and in most cases this is sufficient. Since flow templates are dynamic, FortiSIEM cannot process a flow until it knows the details of the corresponding template. This command may not always be needed, but if flows are not showing up in FortiSIEM, even if tcpdump indicates that they are, this is worth trying.

```
flow-export template timeout-rate 1
```

You can find out more about configuring NetFlow in the [Cisco support forum](#).

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community	<your own>

Setting	Value
String	

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Cisco Firepower Threat Defense (FTD)

- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Comparison of Syslog and eStreamer for Security Eventing](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco-ftd" to see the event types associated with this device.

Rules

There are no specific rules available for Cisco Firepower Threat Defense. Matches device agnostic firewall rules.

Reports

There are no specific reports available for Cisco Firepower Threat Defense. Matches device agnostic firewall rules.

Configuration

Before configuring, you may want to see a comparison of [Syslog and eStreamer for Security Eventing](#) first.

FirePower Threat Defense SNMP Configuration through Firepower Management Center

Cisco Firepower Threat Defense (FTD) supports SNMPv1, v2c, and SNMPv3. Take the following steps to configure:

1. Login to the Firepower Management Center (FMC) GUI, and navigate to **Devices > Platform Settings > (Policy) > SNMP**.
2. Check the **Enable SNMP Servers** checkbox, and configure the SNMPv2 settings.
3. Click on the **Hosts** tab.
4. Click on **Add**, and specify your SNMP server settings in the **Add SNMP Management Hosts** window.
5. Deploy the policy.

For the latest configuration instructions and information, see **Configuring SNMP for FTD** at <https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/white-paper-c11-741739.html>.

FirePower Threat Defense Syslog Configuration through Firepower Management Center

To configure Syslog, take the following steps:

1. Login to the Firepower Management Center (FMC) GUI, and navigate to **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.
2. Click **Add** to add a Logging Filter for a specific logging destination.
3. From the **Logging Destination** drop-down list, choose the logging destination.

For the latest configuration instructions and information, see <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200479-Configure-Logging-on-FTD-via-FMC.html>.

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Comparison of Syslog and eStreamer for Security Eventing

The following content is taken from

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/analyze_events_using_external_tools.html#id_102110.

Generally, organizations that do not currently have significant existing investment in eStreamer should use syslog rather than eStreamer to manage security event data externally.

Syslog	eStreamer
No customization required	Significant customization and ongoing maintenance required to accommodate changes in each release
Standard	Proprietary
Sends directly from devices	Sends from FMC, adding processing overhead
Support for file and malware events, connection events (including security intelligence events) and intrusion events.	Support for all event types listed in eStreamer Server Streaming .
Some event data can be sent only from FMC. See Data Sent Only via eStreamer, Not via Syslog .	Includes data that cannot be sent via syslog directly from devices. See Data Sent Only via eStreamer, Not via Syslog .

Clavister Firewall

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
syslog	Host name, Reporting IP	None	Connection – permit and deny, system events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Clavister" to see the event types associated with this device.

Rules

No specific rules are written for Clavister firewall but generic firewall rules will apply.

Reports

No specific reports are written for Clavister firewall but generic firewall rules will apply.

Configuration

Configure Clavister firewall to send logs to FortiSIEM in the supported format (see [Sample Events](#)).

Settings for Access Credentials

None required

Sample Events

```
<134>[2016-04-26 16:10:07] EFW: CONN: prio=1 id=00600005 rev=1 event=conn_close_natsat  
action=close rule=if3_net_nat_out conn=close connipproto=TCP connrecvif=If3  
connsrccip=192.168.99.13 connsrccport=43347 conndestif=If1 conndestip=1.1.1.1 conndestport=443  
connnewsrccip=1.1.1.2 connnewsrccport=65035 connnewdestip=1.1.1.1 connnewdestport=443 origsent=1395  
termsent=5763 conntime=83
```

```
<134>[2016-04-26 16:10:11] EFW: ALG: prio=1 id=00200001 rev=1 event=alg_session_open algmod=ftp  
algsesid=95238 connipproto=TCP connrecvif=If1 connsrccip=1.1.1.3 connsrccport=59576 conndestif=core  
conndestip=1.1.1.4 conndestport=21 origsent=100 termsent=44
```

```
<134>[2016-04-26 16:10:05] EFW: IPSEC: prio=1 id=01800211 rev=2 event=reconfig_IPsec action=ipsec_  
reconfigured
```

Cyberoam Firewall

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Setting for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Connection – permit and deny, system events, malware events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Cyberoam" to see the event types associated with this device.

Rules

No specific rules are written for Cyberoam firewall but generic firewall rules will apply.

Reports

No specific reports are written for Cyberoam firewall but generic firewall rules will apply.

Configuration

Configure Cyberoam firewall to send logs to FortiSIEM in the supported format (see [Sample Events](#)).

Settings for Access Credentials

None required.

Sample Events

```
<30>date=2019-07-10 time=11:06:48 timezone="GMT" device_name="CR50iNG" device_id=C162213098933-
QQ6REI
log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed"
status="Allow" priority=Information duration=0 fw_rule_id=12 user_name="" user_gp="" iap=1
ips_policy_id=0 appfilter_policy_id=1 application="" application_risk=0 application_technology=""
application_category="" in_interface="PortA" out_interface="" src_mac=00: 0:00: 0:10: 0
src_ip=10.0.70.17 src_country_code=AP dst_ip=1.1.1.1 dst_country_code=IRL protocol="TCP"
src_port=61244 dst_port=443 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_
port=0
tran_dst_ip=10.0.0.13 tran_dst_port=8080 srczonetype="LAN" srczone="ZONE1"
dstzonetype="WAN" dstzone="WAN" dir_disp="" connevent="Start" connid="3340934816" vconnid=""
```

Dell SonicWALL Firewall

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Example Syslog](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Hardware model, Network interfaces, Operating system version	CPU Utilization, Memory utilization and Firewall Session Count	Availability and Performance Monitoring
Syslog	Device type	All traffic and system logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "sonicwall" to see the event types associated with Dell SonicWALL firewalls.

Rules

There are no predefined rules for Dell SonicWALL firewalls.

Reports

There are no predefined reports for Dell SonicWALL firewalls.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

- [Dell SonicWALL Firewall Administrator's Guide \(PDF\)](#)

Syslog

1. Log in to your SonicWALL appliance.
2. Go to **Log > Syslog**.
Keep the default settings.
3. Under **Syslog Servers**, click **Add**.
The Syslog Settings wizard will open.
4. Enter the **IP Address** of your FortiSIEM Supervisor or Collector.
Keep the default **Port** setting of **514**.
5. Click **OK**.
6. Go to **Firewall > Access Rules**.
7. Select the rule that you want to use for logging, and then click **Edit**.
8. In the **General** tab, select **Enable Logging**, and then click **OK**.
Repeat for each rule that you want to enable for sending syslog to FortiSIEM.

Your Dell SonicWALL firewall should now send syslog to FortiSIEM.

Example Syslog

```
Jan  3 13:45:36 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:06" fw=1.1.1.1 pri=6
c=262144 m=98
msg="Connection Opened" n=23419 src=2.2.2.2:36701:WAN dst=1.1.1.1:50000:WAN proto=tcp/50000
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic

Setting	Value
Access Protocol	SNMP
Community String	<your own>

Fortinet FortiGate Firewall

Support Added: FortiSIEM 4.7.2

Last Modification: FortiSIEM 7.0.0

Vendor: Fortinet

Product Information: <https://www.fortinet.com/products/next-generation-firewall>

Supported Versions

FortiGate / FortiOS 7.0.0 and later.



Note: Risk Rating not supported for FortiGate / FortiOS 7.6.x.

Integration Overview

FortiSIEM offers multiple ways to monitor FortiGate firewalls using REST API discovery, Syslog, Netflow, SNMP, or SSH. REST API FortiGate Fabric Discovery features are only available if the FortiGate is a standalone fabric root firewall, or is a member of a FortiGate fabric.

Protocol	Information Discovered	Metrics collected	Used for
REST API	Host name, Model, Version, Interfaces, Serial Number, FortiAP and FortiSwitch managed by FortiGate.	Uptime, CPU, Memory and Disk utilization, Network Interface metrics, VPN metrics, Firewall Connection metrics FortiGate Security Fabric Topology - Adjacent firewall Host name, Model, Version, Serial Number. Fortinet Security Fabric - Risk Rating FortiGate User Store Discovery - Discover FortiClient installed hosts passing through Firewalls.	Performance and Availability Monitoring
Syslog	Device type	All traffic, system logs, IPS events	Availability, Security and Compliance
Netflow		Firewall traffic, application detection and application link usage metrics	Security monitoring and compliance, Firewall Link Usage and Application

Protocol	Information Discovered	Metrics collected	Used for
			monitoring
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths). For 5xxx series firewalls, per CPU utilization (event PH_DEV_MON_FORTINET_PROCESSOR_USGE)	Availability and Performance Monitoring
SSH	Running configuration	Configuration Change	Performance Monitoring, Security and Compliance

Recommended Integration

For most use cases and integration needs, using the FortiGate REST API and Syslog integration will collect the necessary performance, configuration and security information.

If a FortiAnalyzer is receiving FortiGate logs, alternatively forward syslog from the FortiAnalyzer to FortiSIEM. Do not forward logs from both FortiGate and FortiAnalyzer to FortiSIEM as this will cause duplicate events to be received by FortiSIEM (one from FortiGate and another from FortiAnalyzer).

This document covers the following topics:

- [Configuring FortiGate REST API Integration](#)
- [Configuring Syslog Integration](#)
- [Configuring Netflow Integration](#)
- [Configuring SNMP Integration](#)
- [Configuring SSH Based Integration](#)
- [Configuring FortiAnalyzer to Send Logs to FortiSIEM](#)

Configuring FortiGate REST API Integration

- [Configuring FortiGate via GUI](#)
- [Configuring FortiGate via CLI](#)
- [Configuring FortiSIEM](#)
- [Important REST API Integration Events](#)
- [Rest API Integration Results](#)

Configuring FortiGate via GUI

- [Step 1: Create Admin Profile \(RBAC Role\)](#)
- [Step 2: Create Rest API User Account and Assign Admin Profile](#)

Note on FortiGate REST API User Permissions: If you just want to collect audit and performance data from a FortiGate, and no configuration backups, you can assign an admin profile with read only for all access controls. If however, you would like configuration backups via the REST API, certain write permissions are needed to accomplish this.

To collect config backups in addition to other data, take the following steps:

Step 1: Create Admin Profile (RBAC Role)

1. Login to FortiGate Firewall GUI.
2. Navigate to **System > Admin Profiles**, and select **Create New**.
 - a. In the Name field, enter the name the new profile, for example: "Read_Plus_Backup".
 - b. In the **Access Permissions** window, for **Access Control**, take the following steps.
 - i. Select **Read** for all **Access Control** except the following:
 - **User & Device:** Set control to **Read/Write**.
 - **System > Administrator Users:** Set control to **Read/Write**.



Note on the two required Write Permissions:

User & Device: Required for remediation scripts to quarantine/ban an IP/User/Device on the firewall.

System > Administrator Users : Required to allow configuration backups via API. This is because FortiOS considers the API user an Administrator if you have the ability to read configurations with password hashes, certificate info, and other sensitive data.

- c. Optionally, if the firewall is a multi-vdom firewall, ensure the **Scope** option is set to "Global".

Note: Config backups per vdom is not supported at this time.

Access Permissions	
Access Control	Permissions Set All ▾
Security Fabric	☐ None ☒ Read ☐ Read/Write
FortiView	☐ None ☒ Read ☐ Read/Write
User & Device	☐ None ☐ Read ☒ Read/Write
Firewall	☐ None ☒ Read ☐ Read/Write ☐ Custom
Log & Report	☐ None ☒ Read ☐ Read/Write ☐ Custom
Network	☐ None ☒ Read ☐ Read/Write ☐ Custom
System	☐ None ☐ Read ☐ Read/Write ☒ Custom
Administrator Users	☐ None ☐ Read ☒ Read/Write
FortiGuard Updates	☐ None ☒ Read ☐ Read/Write
Configuration	☐ None ☒ Read ☐ Read/Write
Maintenance	☐ None ☒ Read ☐ Read/Write
Security Profile	☐ None ☒ Read ☐ Read/Write ☐ Custom
VPN	☐ None ☒ Read ☐ Read/Write
WAN Opt & Cache	☐ None ☒ Read ☐ Read/Write
WiFi & Switch	☐ None ☒ Read ☐ Read/Write

Permit usage of CLI diagnostic commands ☒

Scope Virtual Domain **Global**

d. Click **OK**.

Step 2: Create Rest API User Account and Assign Admin Profile

Now define a REST API User account, and give it this new profile. Set any preferred IP restrictions (preferably restrict the account to the collector Source IP).

1. On the FortiGate GUI, navigate to **System > Administrators > Create New > REST API Admin**.
2. On the **New REST API Admin** dialog, enter the following information.
 - a. In the **Username** field, enter a user name.
 - b. (Optional) In the **Comments** field, enter any additional information about this account.
 - c. In the **Administrator Profile** drop-down list, select the "Read_Plus_Backup" profile.
 - d. Disable **PKI Group**.
 - e. Disable CORS by setting the toggle **CORS Allow Origin** to off.
 - f. In the **Trusted Hosts** field, enter a trusted host based off your source address. The Trusted Host must be specified to ensure that your local host can reach FortiGate. For example, to restrict requests as coming from only 10.20.100.99, enter "10.20.100.99/32". The Trusted Host is created from the Source Address. (From the FortiGate GUI, select the Status dashboard, navigate to <your-userid>, show active administrator sessions and copy the source address of your <your-userid>.

- [illegible]

Configuring FortiGate via CLI

- Step 1: Create Admin Profile (RBAC Role)
- Step 2: Create Rest API User Account and Assign Admin Profile

To configure via the CLI, take the following steps.

Note:

1. It is most ideal to restrict the user to only the source IP of the collector doing the discovery, in our example below our collector IP is 192.168.1.25. This allows the user to only authenticate to the Firewall via this source IP.
2. If you experience connectivity issues, you can temporarily remove the trusted host configuration, and test.
3. Collector -> FortiGate firewall on administrator port must be allowed inbound to Firewall.
4. If multi-vdom, enter "config global" first.

Step 1: Create Admin Profile (RBAC Role)

Create an admin profile using the following:

```
config system accprofile
  edit "Read_Plus_Backup"
    set scope global
    set secfabgrp read
    set ftviewgrp read
    set authgrp read-write
    set sysgrp custom
    set netgrp read
    set loggrp read
    set fwgrp read
    set vpngrp read
    set utmgrp read
    set wanoptgrp read
    set wifi read
    config sysgrp-permission
      set admin read-write
      set upd read
      set cfg read
      set mnt read
    end
  next
end
```

Step 2: Create Rest API User Account and Assign Admin Profile

Now configure the user, using the following:

```

config system api-user
  edit "fortisiem_user"
    set accprofile "Read_Plus_Backup"
    set vdom "root"
    config trusthost
      edit 1
        set ipv4-trusthost 192.168.1.25 255.255.255.255
      next
    end
  next
end

```

Now finally, generate the api key.

```
execute api-user generate-key fortisiem_user
```

Note the output API key and store in password management utility. This will be placed in FortiSIEM credential (Device Type: Fortinet FortiOS, Access Protocol: FORTIOS_REST_API).

Configuring FortiSIEM

Obtain your token from FortiGate (see [Configuring FortiGate via GUI](#) or [Configuring FortiGate via CLI](#)) before proceeding.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Fortinet FortiOS
Access Protocol	FORTIOS_REST_API
Password config	Manual
Token	Input the API token from the REST API User account.
Confirm Token	Input the same API token as above for verification.
Description	Description about the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Enter the FortiGate IP address or IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiGate.
5. Navigate to **ADMIN > Setup > Discover > New**.

6. In the **Discovery Definition** window, take the following steps:
 - a. In the **Name** field, enter a name for this device.
 - b. In the **Discovery** Type drop-down list, select Range Scan.
 - c. In the **Include** field, enter the FortiGate IP address.
 - d. Click **Save**.
7. Navigate to **ADMIN > Setup > Discovery > Discover**. Your devices will be added into CMDB and 3 jobs are added in Monitor Performance.

Important REST API Integration Events

Type	Event Type	Description
Performance Monitoring	PH_DEV_MON_SYS_UPTIME	System uptime for a device
	PH_DEV_MON_SYS_CPU_UTIL	System CPU Utilization for a device
	PH_DEV_MON_SYS_MEM_UTIL	System memory Utilization stats for a device
	PH_DEV_MON_SYS_DISK_UTIL	Disk Utilization stats for a device
	PH_DEV_MON_NET_INTF_UTIL	Network Interface utilization stats for a device
	PH_DEV_MON_VPN_STATUS	VPN Statistics
	PH_DEV_MON_FW_CONN_UTIL	Firewall Connection Statistics
User Discovery	PH_DEV_MON_FGT_USER_INFO	FortiClient User Device Information seen by FortiGate
Security Posture Discovery	PH_DEV_MON_FGT_SEC_POSTURE_DETAILS	Per device audit details done by FortiGate Security Posture Analysis
	PH_DEV_MON_FGT_SEC_POSTURE_PER_DEVICE_STATS	Per Device Stats done by FortiGate Security Posture Analysis
	PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_STATS	Per Category Security Stats done by FortiGate Security Posture Analysis
	PH_DEV_MON_FGT_SEC_POSTURE_PER_CATEGORY_GRADE	Per Category Security Posture Letter Grade done by FortiGate Security Posture Analysis
	PH_DEV_MON_FGT_SEC_POSTURE_FABRIC_GRADE	Overall Security Posture Letter Grade done by FortiGate Security Posture Analysis
	PH_DEV_MON_FGT_SEC_POSTURE_DETECTED_ENDPOINTS	Endpoint OS Types detected by FortiGate Security Posture Analysis

Rest API Integration Results

Once you discover a FortiGate firewall using REST API:

- The discovered firewall is discovered in depth and appears in **CMDB > Devices > Firewalls**.
- Other devices in the Security fabric are discovered partially - including a few parameters like hostname, access IP (usually the management IP of the Firewall), OS version and serial number. These devices include other Firewalls, attached switches and access points. They all appear in **CMDB > Devices** in their respective groups.
- FortiClient enabled user devices passing through the discovered firewall are discovered and they appear in **Dashboard > Identity Location**. Information includes Host name, IP, MAC, User and attached FortiGate device.
- Performance monitoring is done for the discovered firewall.

If you discover the root FortiGate firewall, then the Security Posture information is available and shown in the **Dashboard > Fortinet Security Fabric > Security Posture** Dashboard.

The recommended setting would be to do the REST API based discovery individually for each FortiGate firewall in the Security fabric.

Configuring Syslog Integration

To configure FortiGate to send logs to FortiSIEM over Syslog, take the following steps either via the Web GUI or CLI.

- [Web GUI](#)
- [CLI](#)

With the Web GUI

1. Log in to your firewall as an administrator.
2. Go to **Log & Report > Log Config > syslog**.
3. Enter the following for your FortiSIEM virtual appliance:
 - IP Address
 - Port Number
 - Minimum Log Level and Facility
4. Make sure that CSV format is not selected.

With the CLI

1. Connect to the FortiGate firewall over SSH and log in.
2. To configure your firewall to send syslog over UDP, enter this command, replacing the IP address 192.168.53.2 with the IP address of your FortiSIEM virtual appliance.

```
config log syslogd setting
    set status enable
    set server "192.168.53.2"
    set facility user
    set port 514
end
```

3. Verify the settings.

```

frontend # show log syslogd
setting config log syslogd setting
    set status enable
    set server "192.168.53.2"
    set facility user
end

```

Sending Logs Over VPN

If you are sending these logs across a VPN, FortiGate will try to use the WAN interface for the source of all system traffic. You can change this by setting the source-ip option to the IP used on the FortiGate Internal/LAN interface.

On FortiSIEM, no configuration is needed.

Important Syslog Integration Events

Type	Event Type	Description
Malware	FortiGate-dns-botnet-domain	Domain blocked by DNS botnet C&C (Domain)
	FortiGate-dns-botnet-ip	Domain blocked by DNS botnet C&C (IP)
	FortiGate-antivirus-botnet	FortiGate antivirus botnet
	FortiGate-antivirus-file-blocked	Outbreak prevention blocked an infected file
	FortiGate-antivirus-file-infect	FortiGate antivirus file infect
DNS Traffic	FortiGate-antivirus-file-infect-mime	FortiGate antivirus file infect mime
	FortiGate-dns-query	DNS query message
	FortiGate-dns-resolv-error	DNS resolution error message
	FortiGate-dns-ftgd-cat-allow	Domain is monitored
Web filter	FortiGate-dns-ftgd-cat-block	System CPU Utilization for a device
	FortiGate-webfilter-allow	Web filter traffic allowed
	FortiGate-webfilter-blacklist-urlblock	Blacklisted web traffic blocked
Application Detection	FortiGate-webfilter-block	Web filter traffic blocked
	FortiGate-appctrl-*	FortiGate Application Control detection
Network Traffic		
	FortiGate-traffic-allowed	Permitted traffic
	FortiGate-traffic-denied	Denied traffic

Type	Event Type	Description
Network Admission Control	FortiGate-event-nac-anomaly-quarantine	NAC anomaly quarantine
	FortiGate-event-nac-quarantine	NAC quarantine
	FortiGate-event-nac-quarantined-ban-ip	NAC module quarantined a host by blocking IP
Login	FortiGate-event-admin-login-success	Admin login successful
	FortiGate-event-admin-login-fail	Admin login failed
	FortiGate-event-login-failure	Failed admin logon
	FortiGate-event-login-success	Successful admin logon
DHCP	FortiGate-event-DHCP-response-Offer	DHCP Offer message
	FortiGate-event-device-upgrade-succeeded	Microsoft IIS performance metrics
Wireless	FortiGate-event-wireless-rogue-detect	Rogue AP detected
	FortiGate-event-wireless-rogue-offair	Rogue AP off wire
DLP	FortiGate-dlp-leak-detected	A data leak was detected by a specified DLP sensor rule
System	FortiGate-event-shutdown	Device shutdown
	FortiGate-event-sys-restart	Scheduled daily reboot started
	FortiGate-event-system-start	FortiGate started
	FortiGate-event-temp-too-high	Temperature too high
	FortiGate-event-temp-too-low	Temperature too low
	FortiGate-fnTrapTempHigh	A temperature sensor on the device has exceeded its threshold
	FortiGate-event-fan-anom	Fan anomaly
	FortiGate-event-power-redundancy-degrade	Power Supply Redundancy Degrade
	FortiGate-event-power-redundancy-failure	Power Supply Redundancy Lost

Type	Event Type	Description
	FortiGate-ConfigChange-Interface-Down	FortiGate user changed interface status to down
	FortiGate-ConfigChange-Interface-Up	FortiGate user changed interface status to up
Config Change	FortiGate-event-config-change	Configuration changed in admin session
IPS detections	FortiGate-ips-signature-<id>	FortiGate signatures

Configuring Netflow Integration

- [Step 1: Configure FortiGate via CLI](#)
- [Step 2: Configure FortiGate via GUI](#)

Step 1: Configure FortiGate via CLI

1. Connect to the FortiGate firewall over SSH and log in.
2. To configure your firewall to send Netflow over UDP, enter the following commands:

```
config system netflow
set collector-ip <FortiSIEM IP>
set collector-port 2055
end
```
3. Enable Netflow on the appropriate interfaces, replacing `port1` with your interface name:

```
config system interface
edit port1
set netflow-sampler both
end
```
4. *Optional - Using Netflow with VDOMs*
For VDOM environments, excluding the management VDOM, Netflow must be configured using the following CLI commands:

```
con global
con sys netflow
set collector-ip <FortiSIEM IP>
set collector-port 2055
set source-ip <source-ip>
end

con vdom
edit root (root is an example, change to the required VDOM name.)
con sys interface
edit wan1 (change the interface to the one to use.)
set netflow-sampler both
end
```

end

Step 2: Configure FortiGate via GUI

1. Login to FortiGate.
2. Go to **Policy & Objects > IPv4 Policy**.
3. Click on the Policy IDs you wish to receive application information from.
4. Add SSL inspection and App Control on the policy by clicking the **+** button in the Security Profiles column.

On FortiSIEM side, no configuration is needed.

Important Netflow Integration Events

Type	Event Type	Description
Netflow	FortiGate-NetFlow	FortiGate Netflow traffic

Configuring SNMP Integration

Monitoring of a FortiGate for performance monitoring using SNMP is not typically required if using the FortiGate API for monitoring. If using FortiSIEM to monitor the interface and application usage, helpful for SDWAN monitoring, then a specific SNMP configuration will be required on the FortiGate, detailed in [Interface Usage Dashboard](#) in the FortiSIEM Online Help.

- [Configuring SNMP v1 or v2 on FortiGate](#)
- [Configuring SNMP v3 on FortiGate](#)
- [Configuring FortiSIEM](#)

Configuring SNMP v1 or v2 on FortiGate

Follow these steps to configure SNMPv1 or v2 on FortiGate. For more information on configuring the FortiGate to allow detailed interface monitoring using SNMP, see [Data Source](#) in the [FortiSIEM User's Guide](#).

1. Log in to your firewall as an administrator.
2. Go to **System > Network**.
3. Select the FortiGate interface IP that FortiSIEM will use to communicate with your device, and then click **Edit**.
4. For **Administrative Access**, make sure that **SSH** and **SNMP** are selected.
5. Click **OK**.
6. Go to **System > Config > SNMP v1/v2c**.
7. Click **Create New** to enable the public community.

Configuring SNMP v3 on FortiGate

To configure SNMPv3 on a FortiGate Firewall and integrate it with FortiSIEM, take the following steps:

1. Allow SNMP traffic on inbound interface where FortiSIEM collector will reach FortiGate firewall.
2. Run the show command under the interface, then run "set allowaccess snmp", replacing the options with the preexisting values, adding snmp to the end.

The following example has the FortiSIEM collector polling inbound on interface port 1.

```
config system interface
```

```
edit "port1"
```

```
show
```

```
set allowaccess snmp
```

```
end
```

```
config system snmp sysinfo
```

```
set status enable
```

```
set description "Description of device"
```

```
set contact-info "Optional contact info"
```

```
set location "Optional location info"
```

```
end
```

3. Replace the sha and aes passwords with your own, and for notify-hosts, enter the IP address of your FortiSIEM collector that will be polling the FortiGate unit.

```
config system snmp user
```

```
edit "fortisiem_user"
```

```
set status enable
```

```
set queries enable
```

```
set security-level auth-priv
```

```
set auth-protocol sha
```

```
set auth-pwd "yourShaPassword1"
```

```
set priv-protocol aes
```

```
set priv-pwd "yourAesPassword1"
```

```
set notify-hosts "192.168.1.2"
```

```
next
```

```
end
```

Configuring SNMP on FortiSIEM

Complete these steps in the FortiSIEM GUI:

1. Go to the **Admin > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. For **SNMP v3**, enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Generic
Access Protocol	SNMP v3
Security Level	authPriv
Security Name	fortisiem_user or <your SNMPv3 username here>
Auth Protocol	SHA
Auth Password	<your password>
Priv Protocol	AES
Priv Password	<your password>
Context	You can leave this field blank.
Description	Optional, you can explain which devices this credential is used for.

- c. For **SNMP V1 or V2**, enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Generic
Access Protocol	SNMP
Community String / Confirm Community String	<the community string>
Description	Optional, you can explain which devices this credential is used for.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.

Note: If multiple collectors, use the collector drop-down list to select which collector will do the polling. If you have only 1 collector, no drop-down list will appear.

- a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field. You can add multiple IPs by using a comma as a separator, for example:
192.168.1.1,192.168.2.1,192.168.3.1
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection. If it fails, ensure the firewall is configured correctly, that SNMP is allowed from the collector on UDP 161, and that the correct SNMPv3 user and password is being used.
 5. Click the **Discovery** tab. If there is more than one collector, select from the drop-down list the collector you'd like to do the polling.
 6. In the include list, enter the same comma separated IP list as before.
 7. Optionally, you can disable ICMP alive check by selecting **Options > Do not ping before discovery**.
 8. Click **Save**.
 9. Select the new discovery, and click **Discover**. Wait for it to finish, or click run in background.
 10. Click the **CMDB** tab, and confirm that the devices are discovered via SNMP.

Important SNMP Integration Events

Type	Event Type	Description
Performance Monitoring	PH_DEV_MON_SYS_UPTIME	System uptime for a device
	PH_DEV_MON_SYS_CPU_UTIL	System CPU Utilization for a device
	PH_DEV_MON_SYS_MEM_UTIL	System memory Utilization stats for a device
	PH_DEV_MON_SYS_DISK_UTIL	Disk Utilization stats for a device
	PH_DEV_MON_NET_INTF_UTIL	Network Interface utilization stats for a device
	PH_DEV_MON_FORTINET_QOS	Fortinet QoS metrics
	PH_DEV_MON_FORTIGATE_PERF	FortiGate performance
	PH_DEV_MON_FORTIGATE_INTF_UTIL	FortiGate interface performance
	PH_DEV_MON_AUTH_STATS	FortiGate Authentication statistics

Configuring SSH Based Integration

Configuring SSH on FortiGate

FortiSIEM Collector SSH Client, when communicating to FortiGate via SSH, may use the public key authentication method first. This may fail and create some alerts in FortiGate. To prevent this, modify the per user config file as follows:

1. Log in to the FortiSIEM node that communicates to FortiGate via SSH, as admin.
2. Open `/opt/phoenix/bin/.ssh/config` and create a new file, if necessary.
3. Add these two lines and save:
`PreferredAuthentications password`
`PubkeyAuthentication no`
4. Ensure that the owner is admin:
`chown admin.admin /opt/phoenix/bin/.ssh/config`
`chmod 600 /opt/phoenix/bin/.ssh/config`
5. Verify using the commands:
`su admin`
`ssh -v <fgt host>`



Verification is successful if the following files are found:

```
[admin@gram .ssh]$ ssh -v localhost
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
debug1: Reading configuration data /opt/phoenix/bin/.ssh/config
debug1: Reading configuration data /etc/ssh/ssh_config
```

Alternatively, modify the global `ssh_config` file as below. Since this is a global configuration, all programs will use this setting.

1. Log in to a FortiSIEM node that communicates to FortiGate via SSH, as root.
2. Open `/etc/ssh/ssh_config`
3. Add these two lines:
`PreferredAuthentications password`
`PubkeyAuthentication no`

SSH Credentials are not normally necessary if using the FortiGate API discovery method, as the FortiGate configuration can also be monitored via the API. You may wish to use the SSH credential for some remediation actions such as "Block Source IP FortiOS 7.x via SSH" and "Block Source MAC FortiOS 7.x via SSH". See [Remediations](#) in the FortiSIEM Online Help for more information. FortiGate remediation action "Block Source IP FortiOS 7.x via FortiOS API" can also be performed via API.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

```
show firewall address
```

```
show full-configuration
```

Configuring SSH on FortiSIEM

Complete these steps in the FortiSIEM GUI:

1. Go to the **Admin > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. For **SSH**, enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Generic
Access Protocol	SSH
Security Level	authPriv
User Name	A user who has access credentials for your device over SSH
Password	The password for the user
Description	Optional, you can explain which devices this credential is used for.

Important SSH Integration Events

Type	Event Type	Description
Configuration Collection and Change Detection	PH_DEV_MON_CHANGE_RUN_CONFIG	Running config changed
	PH_DEV_MON_CHANGE_STARTUP_CONFIG	Startup config changed
	PH_DEV_MON_SYS_PER_CPU_UTIL	Per-process CPU Utilization

Configuring FortiAnalyzer to Send Logs to FortiSIEM

If you are already sending FortiGate logs to FortiAnalyzer, then you can forward those logs to FortiSIEM by configuring FortiAnalyzer as follows:

- [Setting Up the Syslog Server](#)
- [Pre-Configuration for Log Forwarding](#)
- [Configuring Log Forwarding](#)
- [Configuring FortiSIEM Collector to Receive Logs from FortiAnalyzer](#)

Setting Up the Syslog Server

1. Login to FortiAnalyzer.
2. Go to **System Settings > Advanced > Syslog Server**.
 - a. Click the **Create New** button.
 - b. Enter the **Name**. (It is recommended to use the name of the FortiSIEM server.)
 - c. Fill in the **IP address** (or **FQDN**) with the IP or a fully qualified name of the FortiSIEM server.
 - d. Leave the **Syslog Server Port** to the default value '514'.
 - e. Click **OK** to save your entries.

Pre-Configuration for Log Forwarding

To configure FortiAnalyzer event forwarding to FortiSIEM, you must first set up the following.

1. Install a FortiSIEM collector in the same subnet as FortiAnalyzer that will be forwarding the events.
Note: The same subnet request is required as FortiAnalyzer will later be configured to spoof packets to the collector. RPF (reverse path forwarding checks) on network equipment would have to be disabled if FortiAnalyzer and collector existed on different subnets.
2. It is recommended that for every 5,000 EPS (events per second) ingested, you add 1 collector that is 8vCPU, 8GB RAM. If you have more than 5,000 EPS forwarding from FortiAnalyzer, please set up a load balancer with multiple collectors behind it, allowing UDP 514 inbound.

Configuring Log Forwarding

Take the following steps to configure log forwarding on FortiAnalyzer.

1. Go to **System Settings > Log Forwarding**.
2. Click the **Create New** button in the toolbar. The **Create New Log Forwarding** pane opens.
3. fill in the information as per the below table, then click **OK** to create the new log forwarding. The FortiAnalyzer device will start forwarding logs to the server.

Field	Input
Name	FortiSIEM-Forwarding
Status	On
Remote Server Type	Syslog
Compression	OFF
Sending Frequency	Real-time
Log Forwarding Filters	Select all desired Administrative Domains (ADOMs) / device logs you'd like to forward

4. Go to the CLI Console and configure the CLI only log forward option by running the following CLI commands.

Notes:

- Logs received by FortiAnalyzer, and then forwarded to FortiSIEM, have the source IP of the log packet overwritten with the IP address of the FortiAnalyzer appliance. This hides the "true" source of the log packet from FortiSIEM. To override this behavior, FortiAnalyzer can spoof the original log sender's IP address when forwarding to FortiSIEM. This allows FortiSIEM collectors to receive all the original information as if it received the logs directly from the originating device.
- For FortiAnalyzer versions 7.6, 7.4, 7.2 and later, use the following CLI:

Notes:

Replace <id> with the actual name of the log forward created earlier.

You can run "set server-name..." or "set server-addr...". Fortinet recommends using set server-addr "a.b.c.d", so you do not require name resolution of the Collector.

```
config system log-forward
  edit <id>
    set mode forwarding
    set fwd-max-delay realtime
    set server-name "<FortiSIEM_Collector>"
    set server-addr "a.b.c.d"
    set fwd-log-source-ip original_ip
    set fwd-server-type syslog
  next
end
```

Configuring FortiSIEM Collector to Receive Logs from FortiAnalyzer

To configure the FortiSIEM collector to receive logs from FortiAnalyzer, you will need to disable RPF checks that would normally cause the collector virtual machine from dropping the log packet as it is spoofed.

```
sysctl -w net.ipv4.conf.all.rp_filter=0
```

To make this change persistent across reboots, add the following code to the /etc/sysctl.conf file.

```
net.ipv4.conf.all.rp_filter=0
```

Hillstone Firewall

Hillstone Networks offers numerous defensive solutions from edge to cloud, protecting against multilayer and multistage cyberattacks.

Support Added: FortiSIEM 6.5.0-7.0.1 via Content Update

Vendor Version Tested: Not Provided

Vendor: Hillstone Networks

Product: Hillstone NG Firewall

Product Information: <https://www.hillstonenet.com/>

- [Event Types](#)
- [Rules](#)

- [Reports](#)
- [Configuration](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "hillstone" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [Configuring Hillstone Firewall to send Logs](#)
- [Configuring FortiSIEM to Receive Logs](#)

Configuring Hillstone Firewall to send Logs

Follow the steps [here](#) to send syslogs to FortiSIEM.

Configuring FortiSIEM to Receive Logs

No configuration is needed. FortiSIEM can automatically detect and parse Hillstone Firewall logs based on the built in parser.

Imperva SecureSphere Web App Firewall

- [Configuration](#)
- [Sample Events](#)

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create Imperva SecureSphere Web App Firewall credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	<set name>
Device Type	Imperva Securesphere Web App Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration
User Name	A user who has access credentials for the device
Password	The password for the user
Super Password	Password for Super

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping for your Imperva SecureSphere Web App Firewall credential.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Imperva SecureSphere Web App Firewall.
5. To see the jobs associated with Imperva, navigate to **ADMIN > Setup > Pull Events**.
6. To see the received events, select **ANALYTICS**, then enter "Imperva" in the search box.

Sample Events

```
<6>CEF:0|Imperva Inc.|SecureSphere|11.5.0|Firewall Policy|Firewall Policy|High|act=None  
dst=1.1.1.1 dpt=123 duser=n/a src=192.0.20.0 spt=123 proto=UDP rt=Sep 30 2016 11:22:54 cat=Alert  
cs1=Firewall Policy cs1Label=Policy cs2=PCI-V2 cs2Label=ServerGroup cs3=ServiceName  
cs3Label=ServiceName cs4=AppName cs4Label=ApplicationName cs5=Distributed Unauthorized Access to  
Service: port UDP:123 cs5Label=Description
```

Juniper Networks SSG Firewall

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
Telnet/SSH	Running configuration	Configuration Change	Performance Monitoring, Security and Compliance
Syslog	Device type	Traffic log, Admin login activity logs, Interface up/down logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Juniper-SSG" and "Juniper_SSG" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP and SSH](#)
- [Syslog](#)
- [Sample Parsed FortiGate Syslog](#)

SNMP and SSH

Enable SNMP, SSH, and Ping

1. Log in to your firewall's device manager as an administrator.
2. Go to **Network > Interfaces > List**.
3. Select the interface and click **Edit**.
4. Under **Service Options**, for **Management Services**, select **SNMP** and **SSH**.
5. For **Other Services**, select **Ping**.

Create SNMP Community String and Management Station IP

1. Go to **Configuration > Report Settings > SNMP**.
2. If the public community is not available, create it and provide it with read-only access.
3. Enter the **Host IP** address and **Netmask** of your FortiSIEM virtual appliance.
4. Select the Source Interface that your firewall will use to communicate with FortiSIEM.
5. Click **OK**.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, see "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

Modify Policies so Traffic Matching a Policy is Sent via Syslog to FortiSIEM

1. Go to **Policies**.
2. Select a policy and click **Options**.
3. Select **Logging**.
4. Click **OK**.

Set FortiSIEM as a Destination Syslog Server

1. Go to **Configuration > Report Settings > Syslog**.
2. Select **Enable syslog messages**.
3. Select the **Source Interface** that your firewall will use to communicate with FortiSIEM.
4. Under **Syslog servers**, enter the **IP/Hostname** of your FortiSIEM virtual appliance.
5. For **Port**, enter **514**.
6. For **Security Facility**, select **LOCALD**.
7. For **Facility**, select **LOCALD**.

8. Select **Event Log** and **Traffic Log**.
9. Select **Enable**.
10. Click **Apply**.

Set the Severity of Syslog to Send to FortiSIEM

1. Go to **Configuration > Report Setting > Log Settings**.
2. Click **Syslog**.
3. Select the **Severity Levels** of the syslog you want sent to FortiSIEM.
4. Click **Apply**.

Sample Parsed FortiGate Syslog

```
<129>Aug 26 11:09:45 213.181.33.233 20090826, 6219282, 2009/08/26 09:09:40, 2009/08/26 08:09:49,
global.CoX, 1363,
CoX-eveTd-fw1, 213.181.41.226, traffic, traffic log, untrust, (NULL), 81.243.104.82, 64618,
81.243.104.82,
64618, dmz, (NULL), 213.181.36.162, 443, 213.181.36.162, 443, tcp, global.CoX, 1363, Workaniser_
cleanup, fw/vpn, 34,
accepted, info, no, (NULL), (NULL), (NULL), (NULL), 3, 858, 1323, 2181, 0, 0, 14, 1, no, 0, Not

<129>Aug 26 11:09:45 213.181.33.233 20090826, 6219282, 2009/08/26 09:09:40, 2009/08/26 08:09:49,
global.CoX, 1363,
CoX-eveTd-fw1, Category, Sub-Category, untrust, (NULL), 81.243.104.82, 64618, 81.243.104.82,
64618, dmz,
(NULL), 213.181.36.162, 443, 213.181.36.162, 443, tcp, global.Randstad, 1363, Workaniser_cleanup,
fw/vpn, 34, accepted,
info, no, (NULL), (NULL), (NULL), (NULL), 3, 858, 1323, 2181, 0, 0, 14, 1, no, 0, Not
```

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic

Setting	Value
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

McAfee Firewall Enterprise (Sidewinder)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Parsed Sidewinder Syslog](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "sidewinder" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Sample Parsed Sidewinder Syslog

```
Jun 18 10:34:08 192.168.2.10 wcrfw1 auditd: date="2011-06-18 14:34:08 +0000",fac=f_http_
proxy,area=a_libproxycommon,
type=t_nettraffic,pri=p_
major,pid=2093,logid=0,cmd=http,hostname=wcrfw1.community.int,event="session end",app_risk=low,
app_categories=infrastructure,netsessid=1adc04dfcb760,src_
geo=US,srcip=74.70.205.191,srcport=3393,srczone=external,protocol=6,
dstip=10.1.1.27,dstport=80,dstzone=dmz1,bytes_written_to_client=572,bytes_written_to_
server=408,rule_name=BTC-inbound,
cache_hit=1,start_time="2011-06-18 14:34:08 +0000",application=HTTP
```

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	McAfee Sidewinder Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Palo Alto Firewall

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Parsed Palo Alto Syslog Message](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
Telnet/SSH	Running configuration	Configuration Change	Performance Monitoring, Security and Compliance
Syslog	Device type	Traffic log, Threat log (URL, Virus, Spyware, Vulnerability, File, Scan, Flood and data subtypes), config and system logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "palo alto" to see the event types associated with this device. In 6.3.0, the Palo Alto parser has been enhanced to handle some firewall generated Palo Alto Wildfire log events.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "palo alto" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- [SNMP, SSH, and Ping](#)
- [Syslog](#)
- [Set the Severity of Logs to Send to FortiSIEM](#)
- [Create a Log Forwarding Profile](#)
- [Use the Log Forwarding Profile in Firewall Policies](#)
- [Logging Permitted Web Traffic](#)

SNMP, SSH, and Ping

1. Log in to the management console for your firewall with administrator privileges.
2. In the **Device** tab, click **Setup**.
3. Click **Edit**.
4. Under **MGMT Interface Services**, make sure **SSH**, **Ping**, and **SNMP** are selected.
5. For **SNMP Community String**, enter `public`.
6. If there are entries in the **Permitted IP** list, **Add** the IP address of your FortiSIEM virtual appliance.
7. Click **OK**.
8. Go to **Setup > Management** and check that SNMP is enabled on the management interface.

Syslog

Set FortiSIEM as a Syslog Destination

1. Log in to the management console for your firewall with administrator privileges.
2. In the **Device** tab, go to **Log Destinations > Syslog**.
3. Click **New**.
4. Enter a **Name** for your FortiSIEM virtual appliance.
5. For **Server**, enter the IP address of your virtual appliance.
6. For **Port**, enter `514`.
7. For **Facility**, select `LOG_USER`.
8. Click **OK**.

Set the Severity of Logs to Send to FortiSIEM

1. In the **Device** tab, go to **Log Settings > System**.
2. Click **Edit....**

3. For each type of log you want sent to FortiSIEM, select the FortiSIEM virtual appliance in the **Syslog** menu.
4. Click **OK**.

Create a Log Forwarding Profile

1. In the **Objects** tab, go to **Log Forwarding > System**.
2. Create a new log forwarding profile by entering a **Name** for the profile, and then setting **Syslog** to the IP address of your FortiSIEM virtual appliance for each type of log you want send to FortiSIEM.
3. Click **OK**.

Use the Log Forwarding Profile in Firewall Policies

1. In the **Policies** tab, go to **Security > System**.
2. For each security rule that you want to send logs to FortiSIEM, click **Options**.
3. For **Log Forwarding Profile**, select the profile you created for FortiSIEM.
4. Click **OK**.
5. Commit changes.

Logging Permitted Web Traffic

By default, Palo Alto firewalls only log web traffic that is blocked by URL filtering policies. If you must log permitted web traffic, follow these steps.

1. In the **Objects** tab, go to **Security Profiles > URL Filtering**.
2. **Edit** an existing profile by clicking on its name, or click **Add** to create a new one.
3. For website categories that you want to log, select **Alert**.
Traffic matching these website category definitions will be logged.
4. Click **OK**.
5. For each security rule that you want to send logs to FortiSIEM, edit the rule and add the new url filter.

Sample Parsed Palo Alto Syslog Message

```
<14>May  6 15:51:04 1,2010/05/06 15:51:04,0006C101167,TRAFFIC,start,1,2010/05/06
15:50:58,192.168.28.21,172.16.255.78,::172.16.255.78,172.16.255.78,rule3,,,icmp,vsys1,untrust,untr
ust,ethernet1/1,ethernet1/1,syslog-172.16.20.152,2010/05/06
15:51:04,600,2,0,0,0,0x40,icmp,allow,196,196,196,2,2010/05/06 15:50:58,0,any,0

<14>May  6 15:51:15 1,2010/05/06 15:51:15,0006C101167,SYSTEM,general,0,2010/05/06
15:51:15,,unknown,,0,0,general,informational,User admin logged in via CLI from 192.168.28.21

<14>May  9 17:55:21 1,2010/05/09 17:55:21,0006C101167,THREAT,url,6,2010/05/09
17:55:20,172.16.2.2,216.163.137.68,::172.16.255.78,216.163.137.68,DynamicDefault,,,web-
browsing,vsys1,trust,untrust,ethernet1/2,ethernet1/1,syslog-172.16.20.152,2010/05/09
17:55:21,976,1,1126,80,38931,80,0x40,tcp,block-url,"www.playboy.com/favicon.ico",(9999),adult-and-
pornography,informational,0
```

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic

Setting	Value
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Sophos UTM

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Syslog Message](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Configuration change, command execution	Log Management, Compliance and SIEM

Event Types

In **ADMIN > Device Support > Event Types**, search for "sophos-utm" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

Sample Syslog Message

```
<30>2016:07:05-16:57:39 c-server-1 httpproxy[15760]: id="0001" severity="info" sys="SecureWeb"
sub="http" name="http access" action="pass" method="GET" srcip="10.10.10.10" dstip="1.1.1.1"
user="" group="" ad_domain="" statuscode="302" cached="0" profile="REF_DefaultHTTPProfile (Default
Web Filter Profile)" filteraction="REF_HttCffCustoConteFilte (Custom_Default content filter
action)" size="0" request="0xdc871600" url="http://a.com" referer="http://foo.com/bar/" error=""
authtime="0" dnstime="1" cattime="24080" avscantime="0" fullreqtime="52627" device="0" auth="0"
ua="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko" exceptions=""
category="154" reputation="unverified" categoryname="Web Ads"
```

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Sophos UTM
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Stormshield Network Security

- [Integration Points](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Logs](#)

Integration Points

Protocol	Information Collected	Used For
Syslog	Firewall logs	Security and Compliance Monitoring

Event Types

Go to **RESOURCES > Event Type** and search "Stormshield-" in the main content panel **Search...** field to see the event types associated with this device.

Configuration

- [Configuring Stormshield to Send Logs](#)
- [Configuring FortiSIEM to Receive Logs](#)

Configuring Stormshield to Send Logs

Follow the steps listed [here](#) under the **Choose where to save logs** section, to save logs.

Configuring FortiSIEM to Receive Logs

No configuration is needed. FortiSIEM can automatically detect and parse Stormshield logs based on the built in parser.

Sample Logs

```
id=firewall time="2019-02-24 16:38:01" fw="SN310A17B0323A7" tz="+0100" starttime="2019-02-24 16:38:00" pri=5 confid=00 slotlevel=2 ruleid=4 rulename="1690fb96019_7" srcif="Ethernet0" srcifname="out" ipproto=udp proto=ssdp src=10.11.11.11 srcport=49907 srcportname=ephemeral_fw_udp srcname=user1 srcmac=11:11:11:11:11:11 dst=10.10.10.10 dstport=1900 dstportname=sdp ipv=4 sent=0 rcvd=0 duration=0.00 action=pass logtype="filter"
```


Tigera Calico

- [Integration Points](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Logs](#)

Integration Points

Protocol	Information Collected	Used For
Syslog	Flow, Audit and DNS logs	Security and Compliance Monitoring

Event Types

Go to **RESOURCES > Event Type** and search "Calico_Enterprise_" in the main content panel **Search...** field to see the event types associated with this device.

Configuration

- [Configuring Tigera Calico to Send Logs](#)
- [Configuring FortiSIEM to Receive Logs](#)

Configuring Tigera Calico to Send Logs

Follow the steps listed [here](#) to send syslog to FortiSIEM.

Configuring FortiSIEM to Receive Logs

No configuration is needed. FortiSIEM can automatically detect and parse Tigera Calico logs based on the built in parser.

Sample Logs

```
<14>May 8 15:49:58 ip-10-0-0-193.ec2.internal tigera_secure: {"start_time":1588952982,"end_time":1588952992,"source_ip":"10.48.98.2","source_name":"elastic-operator-0","source_name_aggr":"elastic-operator-*","source_namespace":"tigera-eck-operator","source_port":null,"source_type":"wep","source_labels":{"labels":["k8s-app=elastic-operator"],"statefulset.kubernetes.io/pod-name=elastic-operator-0","control-plane=elastic-operator","controller-revision-hash=elastic-operator-6fc7545df5"}}, {"dest_ip":"10.48.241.198","dest_name":"tigera-secure-es-es-0","dest_name_aggr":"tigera-secure-es-es-
```

```
*", "dest_namespace": "tigera-elasticsearch", "dest_port": 9200, "dest_type": "wep", "dest_labels":
{"labels": ["statefulset.kubernetes.io/pod-name=tigera-secure-es-es-
0", "elasticsearch.k8s.elastic.co/version=7.3.2", "controller-revision-hash=tigera-secure-es-es-
757895bb98", "elasticsearch.k8s.elastic.co/http-
scheme=https", "elasticsearch.k8s.elastic.co/statefulset-name=tigera-secure-es-
es", "elasticsearch.k8s.elastic.co/node-data=true", "elasticsearch.k8s.elastic.co/config-
hash=1585026949", "elasticsearch.k8s.elastic.co/node-
ml=true", "common.k8s.elastic.co/type=elasticsearch", "elasticsearch.k8s.elastic.co/node-
ingest=true", "elasticsearch.k8s.elastic.co/node-
master=true", "elasticsearch.k8s.elastic.co/cluster-name=tigera-
secure"]}, "proto": "tcp", "action": "allow", "reporter": "dst", "policies": {"all_policies": ["0|allow-
tigera|tigera-elasticsearch/allow-tigera.elasticsearch-access|allow"]}, "bytes_in": 2593, "bytes_
out": 4617, "num_flows": 3, "num_flows_started": 1, "num_flows_completed": 1, "packets_in": 17, "packets_
out": 10, "http_requests_allowed_in": 0, "http_requests_denied_in": 0, "original_source_
ips": null, "num_original_source_ips": 0, "host": "fluentd-node-xzscj"}
```

UserGate UTM Firewall

Support Added: FortiSIEM 6.3.1

Last Modification: FortiSIEM 6.3.1

Vendor Version Tested: Not Provided

Vendor: UserGate

Product: UTM Firewall

Product Information: <https://www.usergate.com/products/enterprise-firewall>

- [Log Information](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "usergate" to see the event types associated with this device. In FortiSIEM 6.3.1, there are 7 event types defined.

Rules

In **RESOURCES > Rules**, search for "usergate" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there is 1 rule available.

- UserGate UTM IDPS Alert Detected

Reports

In **RESOURCES > Reports**, search for "usergate" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 reports available.

- UserGate UTM - IDPS Events
- UserGate UTM - Web Access Logs

WatchGuard Firebox Firewall

SNMP and syslog are supported. Syslog is used for security and compliance purposes.

- [Integration Points](#)
- [Configuring Watchguard Firebox for SNMP Access](#)
- [Configuring FortiSIEM](#)

Integration Points

Protocol	Information Discovered	Used For
SNMP	Performance metrics – CPU, Memory, Uptime, Interface Usage statistics, Connection rate and Policy Statistics	Performance and Availability Monitoring

Configuring Watchguard Firebox for SNMP Access

1. Logon to Watchguard Firebox Management Console.
2. Follow Watchguard Firebox documentation to allow inbound SNMP access (default UDP port 161) to appropriate FortiSIEM node that will communicate to Firebox node.
3. Note the SNMP credentials. FortiSIEM supports versions 1, 2 and 3.

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access:

- [Define WatchGuard Firebox Firewall Credential in FortiSIEM](#)
- [Create IP Range to Credential Association, Test Connectivity, and Monitor Performance](#)

Define WatchGuard Firebox Firewall Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in “[Setting Credentials](#)” in the User’s Guide to create a new credential.
 1. b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential

Settings	Description
Device Type	Generic
Access Protocol	"SNMP" or "SNMP v3"
Port	Choose the SNMP port (default 161)
Password config	Manual or CyberArk . See Password Configuration .
Community String	If "SNMP" was selected for Access Protocol, enter the community string.
Security Level/Security Name/Auth Protocol/Auth Password/Priv Protocol/Priv Password/Context	If "SNMP v3" was selected for Access Protocol, enter the detailed SNMP V3 security configuration and credentials.
Description	Description of the device.

Create IP Range to Credential Association, Test Connectivity, and Monitor Performance

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

- In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - Enter the **IP** or **IP Range** containing the Firebox firewall in the **IP/Host Name** field. Allowed formats are comma separated IP, IP Range formatted as IP1-IP2 or IP range in CIDR notation.
 - Select the name of the credential created in step 2 of [Define WatchGuard Firebox Firewall Credential in FortiSIEM](#) from the **Credentials** drop-down list.
 - Click **Save**.
- 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. If it succeeds, your credentials are correct.
- Go to **ADMIN > Setup > Discovery**.
- Click **New** and create a discovery entry containing the IP Address of the Firebox firewall.
- Click **Save**.
- With the entry selected, click **Discover**. Ensure that the device is discovered.
- When successful, an entry will be created in **ADMIN > Setup > Monitor Performance** corresponding to this firewall. FortiSIEM will start to pull SNMP metrics from this firewall.

Zscaler Internet Access (ZIA)

ZIA provides Internet traffic inspection and firewall services. FortiSIEM can ingest ZIA logs via syslog or webhook. The following topics are covered:

- Information Collected
- ZIA Syslog based Integration
- ZIA Webhooks based Integration
- Recommended Integration
- Sample Event Logs

Information Collected

The following log types are collected

ZIA Event Category	Event Type Prefix for FortiSIEM Events	Collection Method
Firewall Logs	Zscaler-ZIA-Fw (3 event types)	Syslog or Webhook
Web Logs	Zscaler-ZIA-Web (2 event types)	Syslog or Webhook
DNS Logs	Zscaler-ZIA-Dns (2 event types)	Syslog or Webhook
Tunnel Logs	Zscaler-ZIA-Tunnel (11 event types)	Syslog or Webhook
EDLP Logs	Zscaler-ZIA-EDLP (2 event types)	Syslog or Webhook
Audit Logs	Zscaler-ZIA-AUDIT (4 event types)	Syslog or Webhook
SaaS Security Logs	Zscaler-ZIA-CASB-Audit (1 event type)	Syslog or Webhook

You can go to **Resources > Event Types** and search for these event types by using the prefix.

ZIA Syslog based Integration

In this integration, ZIA uses **Nanolog Streaming Service (NSS)** to forward logs to an NSS VM which can then forward to FortiSIEM via **syslog**.

Configuration

Two steps are involved. Also, no configuration is required on FortiSIEM.

1. Deploy NSS Virtual Appliance.
2. Set up NSS Forwarding Feed for each Log Type.

Step 1: Deploy NSS Virtual Appliance

1. Deploy a NSS Virtual Appliance using the information [here](#).
2. Confirm that the new NSS VM has outbound network connectivity to a FortiSIEM collector on TCP port 514.

Step 2: Set up NSS Forwarding Feed for each Log Type

Reference: <https://help.zscaler.com/zia/adding-nss-feeds>

1. Login to Zscaler ZIA portal.
2. Navigate to Administration > Nanolog Streaming Service.
3. From the NSS Feeds tab, take the following steps.
 - a. Click **Add NSS Feed**.
 - b. In the Add NSS Feed window, take the following steps.

Field	Configuration Instructions
Feed Name	FortiSIEM_NSS_FirewallLogs
NSS Type	Firewall
NSS Server	Select the NSS Virtual Appliance from the drop-down.
Status	Enabled
SIEM Destination Type	IP of FortiSIEM collector (If you have a resolvable FQDN for SIEM collector, you can use this.)
SIEM IP Address	###.###.### (The FortiSIEM collector you would like to send the forwarded logs.)
SIEM TCP Port	514
SIEM Rate	Unlimited
Log Type	Firewall Logs
Feed Output Type	JSON
Timezone	Select UTC or GMT time.
Duplicate Logs	Recommendation: Disabled. If enabled, it may result in duplicate logs during the following circumstance: If connection is down, on recovery, Zscaler will resend the logs that were not sent.

- c. Click **Save**.
 - d. Hover over the **Activation** menu near the lower left, and click **Activate**. See [here](#) for more information.
4. Repeat Step 3 for each of the remaining Log Types, excluding **Web Log (DNS Log, Tunnel, SaaS Security, SaaS Security Activity, Sandbox Verdict, Admin Audit)** using the additional instructions here:
 - **Feed Name:** Use a name that easily identifies it with the Log Type being added to the NSS Feed.
 - **NSS Type:** Select the **NSS Type** from the [NSS Feed Table](#) that matches the **Log Type** being configured for NSS Feed, e.g., Log Type Web Log uses NSS Type: Web, and DNS Logs Log Type uses NSS Type: Firewall.
 - **Log Type:** Select the Log Type being configured as part of the NSS Feed, i.e., NSS Type -> Firewall means Log Type ->Firewall Logs (or DNS Logs), using the [NSS Feed Table](#) as reference.

NSS Feed Table

NSS Type	Log Type	Format (Feed Output Type)
Web	Admin Audit	JSON

NSS Type	Log Type	Format (Feed Output Type)
Web	SaaS Security	JSON
Web	SaaS Security Activity	JSON
Web	Sandbox Verdict	JSON
Web	Tunnel	JSON
Firewall	Firewall Logs	JSON
Firewall	DNS Logs	JSON
Web	Web Log	Custom

5. For **Web Log**, use the table below to configure.

Field	Configuration Instructions
Feed Name	FortiSIEM_NSS_WebLogs
NSS Type	Web
NSS Server	Select the NSS Virtual Appliance from the drop-down.
Status	Enabled
SIEM Destination Type	IP of FortiSIEM collector (If you have a resolvable FQDN for SIEM collector, you can use this.)
SIEM IP Address	###.### (The FortiSIEM collector you would like to send the forwarded logs.)
SIEM TCP Port	514
SIEM Rate	Unlimited
Log Type	Web Log
Feed Output Type	Custom.
Feed Escape Character	,\"

Field	Configuration Instructions
Feed Output Format	<pre>\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}", "reason":"%s{reason}", "event_id":"%d{recordid}", "protocol":"%s{proto}", "action":"%s{action}", "transactionsize":"%d{totalsize}", "responsesize":"%d{respsize}", "requestsize":"%d{reqsize}", "urlcategory":"%s{urlcat}", "serverip":"%s{sip}", "requestmethod":"%s{reqmethod}", "refererURL":"%s{ereferer}", "useragent":"%s{eua}", "product":"NSS", "location":"%s{elocation}", "ClientIP":"%s{cip}", "status":"%s{respcode}", "user":"%s{ellogin}", "url":"%s{eurl}", "vendor":"Zscaler", "hostname":"%s{ehost}", "clientpublicIP":"%s{cintip}", "threatcategory":"%s{malwarecat}", "threatname":"%s{threatname}", "filetype":"%s{filetype}", "appname":"%s{appname}", "app_status":"%s{app_status}", "pagerisk":"%d{riskscore}", "threatseverity":"%s{threatseverity}", "department":"%s{edepartment}", "urlsupercategory":"%s{urlsupercat}", "appclass":"%s{appclass}", "dlpengine":"%s{dlpeng}", "urlclass":"%s{urlclass}", "threatclass":"%s{malwareclass}", "dlpdictionaries":"%s{dlpdict}", "fileclass":"%s{fileclass}", "bwthrottle":"%s{bwthrottle}", "contenttype":"%s{contenttype}", "unscannabletype":"%s{unscannabletype}", "deviceowner":"%s{deviceowner}", "devicehostname":"%s{devicehostname}", "keyprotectiontype":"%s{keyprotectiontype}"\}\}</pre>
Timezone	Select UTC or GMT time.
Duplicate Logs	Recommendation: Disabled. If enabled, it may result in duplicate logs during the following circumstance: If connection is down, on recovery, Zscaler will resend the logs that were not sent.

ZIA Webhooks based Integration

In this method, ZIA uses **Nanolog Streaming Service (NSS)** to push logs to FortiSIEM via **Webhooks**.

Configuration

Four steps are involved.

1. Configure a FortiSIEM Webhook Credential.
2. Verify that the FortiSIEM configuration is correct.
3. Set up Cloud NSS Webhooks (HTTPS Post) to forward logs to a FortiSIEM public webhook URL endpoint generated in Step 1.
4. Confirm Logs appear in FortiSIEM.

Step 1: Configure a FortiSIEM Webhook Credential

When configuring your FortiSIEM Credential, your webhook end point will be dynamically created. Zscaler will send logs to this endpoint.

1. Go to the **Admin > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	Zscaler
Access Protocol	Webhook
Separator	\n
Receiver FQDN	Select the FQDN or IP of the FortiSIEM node that will receive the webhook.  - Zscaler does not allow using invalid or untrusted TLS certificates. Your target FortiSIEM node (collector) must have a valid TLS certificate. If your edge firewall is doing SSL/TLS deep inspection. It must present a valid TLS certificate to Zscaler cloud (the client). To test, see Step 2. - Enter a publicly reachable FQDN that will map to your FortiSIEM node that will ingest the events. E.g. collector1.example.com. If you are using FortiSIEM cloud, this can be either the Supervisor FQDN or one of the Worker node FQDNs, but ideally you should dedicate a collector node for this ingestion.
Reporting Host Name	zscalercloudnss
Endpoint	This is auto populated based on Receiver FQDN and Credential Name as <code>https://<Receiver FQDN>/webhook/<Name></code>.  You must ensure that the Zscaler ZIA Cloud is able to call this API on TCP 443 over the public internet. You can lock down access to Zscaler's published source IP blocks. - Write this value down e.g. <code>https://xyzexample.fortisiem.cloud/webhook/zscaler</code> - Double check the URI (/webhook/<credential_name>) and make sure it's the same as defined in FortiSIEM, and as entered in Zscaler.
Auth Type	Select Simple Secret .

Settings	Description
	1. Shared Secret: Enter a complex password. Store this value securely, this is needed for the NSS Cloud configurations on Zscaler admin portal. 2. Auth Part: Select Header. Specifies that Zscaler will authenticate by sending the shared secret in an HTTP header of the webhook POST. 3. Header Name: Enter "Authorization". This is the header name that will contain your shared secret. This means the Authorization header will contain your shared secret value. This value must match the header configured in NSS Cloud.
Description (Optional)	Description of the device.

- The endpoint will be set as `http://<ReceiverFQDN>/webhook/<Name>`
- Click **Save and Deploy**. This will push the endpoint definition to the FortiSIEM node defined in step 2b – "Receiver FQDN" field.

Step 2: Verify that the FortiSIEM Configuration is Correct

You can test your configuration and verify it works by doing the following curl commands.

Replace the endpoint and password with your own

If this command works, you are all set and should follow the guide on setting up Zscaler webhook forwarding

```
curl -H 'Authorization: YourSecretSharedPaswordHere' https://yourSIEM/webhook/zscaler \ -d '{
"sourcetype" : "zscalernss-edlp","log_type": "fake example not expected to parse"}
```

If the above command fails, try this command below that disables certificate verification, if this succeeds, you must follow instructions to configure a proper TLS certificate on the FortiSIEM collector or node receiving the traffic.

Test Webhook post to FortiSIEM node without certificate validation (Testing only)

```
curl -k -H 'Authorization: YourSecretSharedPaswordHere' https://yourSIEM/webhook/zscaler \ -d '{
"sourcetype" : "zscalernss-edlp","log_type": "fake example not expected to parse"}
```

Step 3: Configure Zscaler NSS Cloud (Webhook) Feeds to Point to FortiSIEM Webhook Endpoint

Reference: <https://help.zscaler.com/zia/adding-cloud-nss-feeds>

- Navigate to Administration > Nanolog Streaming Service.
- From the Cloud NSS Feeds tab, take the following steps.
 - Click **Add Cloud NSS Feed**.
 - In the Add Cloud NSS Feed window, take the following steps.

Field	Configuration Instructions
Feed Name	FortiSIEM_NSS_FirewallLogs
NSS Type	NSS for Firewall
SIEM Type	Other
API URL	https://<your_FortiSIEM_URL>/phoenix/webhook/zscaler Note: The HTTPS URL must be configured with a publicly trusted SSL certificate. Self-signed or internally issued certificates do not pass the SIEM connectivity test. Define the HTTP header in the webhook that contains the simple secret verification The value of this header must match on the FortiSIEM Webhook configuration HTTP Headers: • Key1: Authorization • Value1: EnterARandomSecretHere2332 Key Detail: This is the equivalent of Zscaler doing a curl command like this <pre>curl -H 'Authorization: EnterARandomSecretHere2332' https://yourSIEM/webhook/zscaler \ -d '{ "some" : "json"}'</pre>
Log Type	Firewall Logs
Firewall Log Type (Firewall logs only)	Both Session and Aggregate Logs
Feed Output Type	JSON Note: If you see a JSON Array Notation checkbox, leave it unchecked. This is currently not supported in the parsers.
Feed Escape Character	Leave blank.
User obfuscation	Disabled
Timezone	Select UTC or GMT time.
Duplicate Logs	Recommendation: Disabled. If enabled, it may result in duplicate logs during the following circumstance: If connection is down, on recovery, Zscaler will resend the logs that were not sent.

- c. Click **Save**.
 - d. Hover over the **Activation** menu near the lower left, and click **Activate**. See [here](#) for more information.
3. Repeat [Step 3.2.a-b](#) for each of the remaining Log Types (**Web Log**, **DNS Log**, **Tunnel**, **SaaS Security**, **SaaS Security Activity**, **Admin Audit**, **Endpoint DLP**, **Email DLP**) using the additional instructions here:
- **Feed Name:** Use a name that easily identifies it with the Log Type being added to the NSS Feed.
 - **NSS Type:** Select the **NSS Type** from the [NSS Feed Table](#) that matches the **Log Type** being configured for NSS Feed, e.g., Web Log Log Type uses NSS Type: NSS for Web, and DNS Logs Log Type uses NSS Type: NSS For Firewall.
 - **Log Type:** Select the Log Type being configured as part of the NSS Feed ensuring the NSS Type and Log Type match up using the [NSS Feed Table](#).

NSS Feed Table

Log Type	NSS Type	Feed Output Type
Firewall Logs	NSS for Firewall	JSON
Web Log	NSS for Web	JSON
DNS Logs	NSS for Firewall	JSON
Tunnel	NSS for Web	JSON
SaaS Security	NSS for Web	JSON
SaaS Security Activity	NSS for Web	JSON
Admin Audit	NSS for Web	JSON
Endpoint DLP	NSS for Web	JSON
Email DLP	NSS for Web	JSON

Step 4: Confirm Logs appear in FortiSIEM

1. Login to FortiSIEM GUI.
2. Navigate to **Analytics**.
3. Run the following query:
Event Type CONTAIN Zscaler-ZIA
Note: To perform a specific query for a given log type simply change Zscaler-ZIA to Zscaler-ZIA-*<Log type>*
e.g. Zscaler-ZIA-fw for firewall logs.
4. Confirm that Zscaler logs appear.

Recommended Integration

Method	Pros	Cons
ZIA Via Syslog	1. Simpler configuration. 2. No need to expose your collectors TCP 514 port inbound from the public internet.	You need to setup a NSS logging VM in your internal network.
ZIA Via Webhook	No additional VM setup.	Additional firewall configuration to ensure there is a virtual IP/static NAT firewall mapping to a FortiSIEM collector.

Fortinet generally recommends VM-based NSS syslog forwarding to minimize network complexity.

Sample Event Logs

FortiSIEM expects all forwarded NSS logs to be in JSON format. Example formats are below:

Firewall Logs

```
{ "sourcetype" : "zscalernss-fw", "event" : {"datetime":"Fri Sep 29 20:15:04
2023", "user": "testuser@example-
siem.com", "department": "General%20Group", "locationname": "Road%20Warrior", "cdport": "53", "csport": "5
7319", "sdport": "53", "ssport": "36412", "csip": "10.2.3.4", "cdip": "168.63.129.16", "ssip": "165.225.242.
252", "sdip": "128.177.129.156", "tsip": "2.2.2.2", "tunsport": "0", "tuntype": "ZscalerClientConnector", "
action": "Allow", "dnat": "Yes", "stateful": "Yes", "aggregate": "No", "nwsvc": "DNS", "nwapp": "dns", "proto"
: "UDP", "ipcat": "Internet
Services", "destcountry": "Other", "avgduration": "0", "rulelabel": "Allow%20DNS", "inbytes": "190", "outby
tes": "80", "duration": "0", "durationms": "0", "numsessions": "1", "ipsrulelabel": "None", "threatcat": "Non
e", "threatname": "None", "deviceowner": "eparra", "devicehostname": "ws1client1"}}
```

Web Logs

```
{ "sourcetype" : "zscalernss-web", "event" : {"datetime":"2023-09-29
17:52:32", "reason": "Allowed", "event_
id": "7284307277989806081", "protocol": "HTTPS", "action": "Allowed", "transactionsiz": "1039", "response
size": "234", "requestsize": "805", "urlcategory": "Professional
Services", "serverip": "54.84.102.8", "requestmethod": "GET", "referrerURL": "None", "useragent": "Mozilla/
5.0%20(Windows%20NT%2010.0;%20Win64;%20x64)%20AppleWebKit/537.36%20
(KHTML,%20like%20Gecko)%20Chrome/110.0.0.0%20Safari/537.36", "product": "NSS", "location": "Road%20War
rior", "ClientIP": "10.2.3.4", "status": "101", "user": "testuser@example-siem.com", "url": "1456754-
4.chat.api.drift.com/ws/websocket?session_
token=SFMyNTY.g2gDdAAAAVKAAPZG0AAAAVMTQ1Njc1NC0xOTYxNDY5NTM3OS00ZAAGb3JnX2lkQAAAAcxNDU2NzU0ZAAJ
c2NvcGVfc2V0bQAAAAARsZWFKZAAHdXNlc19pZG0AAAAALMTk2MTQ2OTUzNzlkAA11c2VyX3R5cGVkAARsZWFKbgYA6BwS4ooBYg
ABUYA.OUHGFPe2dOYIy0Bmtf3yvb6NTnxvIrHi5MD8U1TJFik&remote_
ip=3.226.111.211&vsN=2.0.0", "vendor": "Zscaler", "hostname": "1456754-
4.chat.api.drift.com", "clientpublicIP": "2.2.2.2", "threatcategory": "None", "threatname": "None", "file
type": "None", "appname": "Drift", "pagerisk": "0", "department": "General%20Group", "urlsupercategory": "B
usiness and Economy", "appclass": "Sales and Marketing", "dlpengine": "None", "urlclass": "Business
Use", "threatclass": "None", "dlpdictionaries": "None", "fileclass": "None", "bwthrottle": "NO", "contentty
pe": "Other", "unscannabletype": "None", "deviceowner": "eparra", "devicehostname": "ws1client1", "keyprot
ectiontype": "Software Protection"}}
```

DNS Logs

```
{ "sourcetype" : "zscalernss-dns", "event" : {"datetime":"Fri Sep 29 17:59:27
2023", "user": "testuser@example-
siem.com", "department": "General%20Group", "location": "Road%20Warrior", "reqaction": "Allow", "resactio
n": "Allow", "reqrulelabel": "Default Firewall DNS Rule", "resrulelabel": "Default Firewall DNS
Rule", "dns_reqtype": "UNKNOWN", "dns_req": "www.bing.com", "dns_resp": "www-
www.bing.com.trafficmanager.net", "srv_dport": "53", "durationms": "1", "clt_sip": "10.2.3.4", "srv_
```

```
dip":"128.177.129.156","category":"Web Search","respipcategory":"Internet Services","deviceowner":"eparra","devicehostname":"ws1client1"}}}
```

Tunnel Logs

```
{ "sourcetype" : "zscalernss-tunnel", "event" : {"datetime":"Thu Apr 11 20:20:00 2024","Recordtype":"Tunnel Samples","tunneltype":"IPSec IKEv2","user":"35.176.50.157","location":"UK1","sourceip":"35.176.50.157","destinationip":"165.225.16.38","sourceport":"4500","txbytes":"0","rxbytes":"920","dpdrec":"0","recordid":"7356706889184378880"}}}
```

EDLP Logs

```
{ "sourcetype" : "zscalernss-edlp", "event" : {"datetime":"2024-04-09-01:39:46-GMT","recordid":"7355676544023068673","login":"testuser@example-siem.com","dept":"General Group","filetypename":"xlsx","filemd5":"9a2d0d62c22994a98f65939ddcd3eb8f","dlpdicnames":"Social Security Number (US): Detect leakage of United States Social Security Numbers|Credit Cards: Detect leakage of credit card information|Aadhaar Card Number (India): Detect Leakage of Indian Aadhaar Card Numbers","dlpdiccount":"1428|141|81","dlpenginenames":"Financial Stuff|cc|PCI|GLBA|HIPAA","channel":"Removable Storage","actiontaken":"Allow","severity":"High Severity","rulename":"Endpoint_DLP_","itemdstname":"Removable Storage"}}}
```

Audit Logs

```
{ "sourcetype" : "zscalernss-audit", "event" : {"time":"Thu Apr 11 19:42:12 2024","recordid":"735296","action":"UPDATE","category":"ACCESS_CONTROL_RESOURCE","subcategory":"URL_CATEGORY","resource":"music","interface":"UI","adminid":"admin@example-siem.com","clientip":"136.226.68.209","result":"SUCCESS","errorcode":"None","auditlogtype":"ZIA","preaction":{"id":{"val":24,"mask":255,"parent":"ENTERTAINMENT_AND_RECREATION","deprecated":false,"backendName":"music","name":"MUSIC","userConfiguredName":""},"superCategory":"ENTERTAINMENT_AND_RECREATION","keywords":[],"keywordsRetainingParentCategory":[],"customUrlsToAdd":[],"customUrlsToDelete":[],"urlsRetainingParentCategoryToAdd":[],"urlsRetainingParentCategoryToDelete":[],"customIpRangesToAdd":[],"customIpRangesToDelete":[],"ipRangesRetainingParentCategoryToAdd":[],"ipRangesRetainingParentCategoryToDelete":[],"customCategory":false,"editable":true,"description":"MUSIC_DESC","type":"URL_CATEGORY","customUrlsCount":1,"urlsRetainingParentCategoryCount":1,"customIpRangesCount":0,"ipRangesRetainingParentCategoryCount":0,"urlsToAdd":[],"urlsToDelete":[],"dbCategorizedUrlsToAdd":[],"dbCategorizedUrlsToDelete":[]},"postaction":{"id":{"val":24,"mask":255,"parent":"ENTERTAINMENT_AND_RECREATION","deprecated":false,"backendName":"music","name":"MUSIC","userConfiguredName":""},"superCategory":"ENTERTAINMENT_AND_RECREATION","customUrlsToAdd":["wefwef.com"],"urlsRetainingParentCategoryToDelete":[],"customIpRangesToAdd":[],"customIpRangesToDelete":[],"ipRangesRetainingParentCategoryToAdd":[],"ipRangesRetainingParentCategoryToDelete":[],"customCategory":false,"editable":true,"description":"MUSIC_DESC","type":"URL_CATEGORY","customUrlsCount":1,"urlsRetainingParentCategoryCount":2,"customIpRangesCount":0,"ipRang
```

```
esRetainingParentCategoryCount":0,"urlsToAdd":[],"urlsToDelete":[],"dbCategorizedUrlsToAdd":  
[],"dbCategorizedUrlsToDelete":[]}]}}
```

SaaS Security Logs (used for both SaaS Security and Activity Logs)

```
{ "sourcetype" : "zscalernss-casb", "event" :{"datetime":"Tue Apr 30 07:49:19  
2024","company":"Paul Lopez-Internal","login":"autopilot@zs-labs.net","tenant":"zs-labs-teams-  
corp","dept":"Default  
Department","applicationname":"MSTEAM","threatname":"None","policy":"None","dlpdictnames":"None","  
dlpdictcount":"None","dlpenginenames":"None"}}
```


Load Balancers and Application Firewalls

FortiSIEM supports these load balancers and application firewalls for discovery and monitoring.

- Barracuda Web Application Firewall
- Brocade ServerIron ADX
- Citrix Netscaler Application Delivery Controller (ADC)
- F5 Networks Application Security Manager
- F5 Networks Local Traffic Manager
- F5 Networks Web Accelerator
- Fortinet FortiADC
- Qualys Web Application Firewall

Barracuda Web Application Firewall

FortiSIEM Support Added: 6.3.2

Vendor: Barracuda

Product Information: <https://www.barracuda.com/products/webapplicationfirewall>

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Barracuda Web Application Firewall (WAF).

Protocol	Metrics Collected	Used For
Syslog	System logs, Web Firewall logs, Access logs, Audit logs and Network Firewall logs	Security and Compliance

Configuration

To configure syslog from your Barracuda WAF, take the following steps:

1. Navigate to **Advanced > Export Logs > Syslog**.
2. Configure the following fields in the table.

Field	Description
Name	Enter the name of the syslog server.
Syslog Server	Enter the IP address of the syslog server.
Log Time Stamp	Select "Yes" to log the date and time of system events.
Log Unit Name	Select "Yes" to log the name of the Barracuda Web Application Firewall unit. The unit name is the same as the Default Host name located on the BASIC > IP Configuration page.
Comment	Enter any comments about the syslog server.
Select appropriate facility	Leave as Local7 or default option.

3. When done, click **Add** to add the settings.

Sample Events

```
<134>Sep 1 13:10:09 nlb_lab 2021-09-01 13:10:09.163 -0600 nlb_lab NF INFO TCP 192.0.2.105 443
ALLOW traffic:allow
<132>Sep 1 13:10:09 nlb_lab 2021-09-01 13:10:09.550 -0600 nlb_lab WF WARN UNRECOGNIZED_COOKIE
98.98.98.22 51415 192.0.2.110 443 global GLOBAL LOG NONE [Cookie\_="_derived_epik" Service-
created\_="1565 days back" Reason\_="No valid encrypted pair"] GET test.example.com/random_page
TLSv1.2 "-" "Mozilla/5.0 (Linux; Android 11; SAMSUNG SM-G991U) AppleWebKit/537.36 (KHTML, like
Gecko) SamsungBrowser/15.0 Chrome/90.0.4430.210 Mobile Safari/537.36" 98.98.98.22 51415 "-"
https://test.example.com/
<134>Sep 1 13:10:11 nlb_lab 2021-09-01 13:10:11.342 -0600 nlb_lab TR 192.0.2.105 443 192.0.2.134
53619 "-" "-" POST TLSv1.2 test.example.com HTTP/1.1 200 736974 439 0 104 10.20.20.102 443 103 "-"
SERVER DEFAULT PASSIVE VALID /json/reply/TicketingEventsGetAvailableByEventTypeName "-" "-" "-"
"ServiceStack .NET Client 5.40" 192.0.2.134 53619 "-" "-" "-" "-"
```

Brocade ServerIron ADX

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
SNMP	Host name, serial number, hardware (CPU, memory, network interface etc)	Uptime, CPU, Memory, Interface Utilization, Hardware status, Real Server Statistics	Performance/Availability Monitoring

Event Types

- PH_DEV_MON_SYS_CPU_UTIL

```
[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceBrocadeServerIron.cpp,
[lineNumber]=434,[cpuName]=CPU,[hostName]=lb1-1008-qts,[hostIpAddr]=192.0.2.15,
[cpuUtil]=55.000000,[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_SYS_MEM_UTIL

```
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceBrocadeServerIron.cpp,
[lineNumber]=456,[memName]=Physical
Memory,[hostName]=lb1-1008-qts,[hostIpAddr]=192.0.2.15,[memUtil]=10.000000,[pollIntv]=176,
[phLogDetail]=
```

- PH_DEV_MON_NET_INTF_UTIL

```
[PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phIntfFilter.cpp,
[lineNumber]=323,[intfName]=GigabitEthernet8,[intfAlias]=,[hostName]=lb1-1008-qts,
[hostIpAddr]=192.0.2.15,[pollIntv]=56,[recvBytes64]=1000000,[recvBitsPerSec]=142857.142857,
```

```
[inIntfUtil]=0.014286,[sentBytes64]=2000000,[sentBitsPerSec]=285714.285714,
[outIntfUtil]=0.028571,[recvPkts64]=0,[sentPkts64]=0,[inIntfPktErr]=0,
[inIntfPktErrPct]=0.000000,[outIntfPktErr]=0,[outIntfPktErrPct]=0.000000,
[inIntfPktDiscarded]=0,[inIntfPktDiscardedPct]=0.000000,[outIntfPktDiscarded]=0,
[outIntfPktDiscardedPct]=0.000000,[outQLen64]=0,[intfInSpeed64]=1000000000,
[intfOutSpeed64]=1000000000,[intfAdminStatus]=up,[intfOperStatus]=up,[daysSinceLastUse]=0,
[totIntfPktErr]=0,[totBitsPerSec]=428571.428571,[phLogDetail]=
```

- PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT

```
[PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT]:[eventSeverity]=PHL_INFO,
[fileName]=deviceBrocadeServerIron.cpp,[lineNumber]=507,[hostName]=lb1-1008-qts,
[hostIpAddr]=192.0.2.15,[realServerIpAddr]=192.0.2.131,[realServerState]=7,
[failedPortExists]=2,[openConnectionsCount]=2,[peakConns]=114,[activeSessions]=4,
[phLogDetail]=
```

- PH_DEV_MON_HW_STATUS

```
[PH_DEV_MON_HW_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=deviceBrocadeServerIron.cpp,
[lineNumber]=359,[hostName]=lb1-1008-qts,[hostIpAddr]=192.0.2.15,[hwStatusCode]=2,
[hwPowerSupplyStatus]=0,[hwTempSensorStatus]=2,[hwFanStatus]=0,[phLogDetail]=
```

```
[PH_DEV_MON_HW_STATUS_TEMP_CRIT]:[eventSeverity]=PHL_CRITICAL,[fileName]=device.cpp,
[lineNumber]=13812,[hostName]=lb1-1008-qts,[hostIpAddr]=192.0.2.15,[hwStatusCode]=2,
[hwComponentName]=1-Temperature
sensor,[hwComponentStatus]=Critical,[phLogDetail]=
```

- PH_DEV_MON_HW_TEMP

```
[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceBrocadeServerIron.cpp,
[lineNumber]=401,[hostName]=lb1-1008-qts,[hostIpAddr]=192.0.2.15,[hwComponentName]=Temp1,
[envTempDegF]=90,[phLogDetail]=
```

Rules

There are no predefined rules for this device other than covered by generic network devices.

Reports

There are no predefined reports for this device other than covered by generic network devices.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Brocade ServerIron ADX
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Citrix Netscaler Application Delivery Controller (ADC)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Example Syslog](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted and Denied traffic	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "netscaler" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "netscaler" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

- The syslog format should be the same as that shown in the example.

Example Syslog

```
<182> 07/25/2012:19:56:41 PPE-0 : UI CMD_EXECUTED 473128 : User nsroot - Remote_ip 10.13.8.75 -  
Command "show ns hostName" - Status "Success"<181> 07/25/2012:19:56:05 NS2-MAIL PPE-0 : EVENT  
DEVICEUP 33376 : Device "server_vip_NSSVC_SSL_172.17.102.108:443(accellion:443)" - State UP  
<181> 07/25/2012:19:55:35 NS2-MAIL PPE-0 : EVENT DEVICEDOWN 33374 : Device "server_vip_NSSVC_  
SSL_172.17.102.108:443(accellion:443)" - State DOWN  
<182> 07/24/2012:15:37:08 PPE-0 : EVENT MONITORDOWN 472795 : Monitor Monitor_http_of_Domapps:80  
(10.50.15.14:80) - State DOWN
```

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Citrix NetScaler
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

F5 Networks Application Security Manager

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Various application level attack scenarios - invalid directory access, SQL injections, cross site exploits.	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "f5-asm" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Example Syslog

```
<134>Jun 26 14:18:56 f5virtual.tdic.ae ASM:CEF:0|F5|ASM|10.2.1|Successful Request|Successful Request|2|dvchost=f5virtual.adic.com dvc=192.168.1.151 cs1=master-key_default cs1Label=policy_name cs2=master-key cs2Label=web_application_name deviceCustomDate1=Jul 13 2011 16:24:25 deviceCustomDate1Label=policy_apply_date externalId=3601068286554428885 act=passed cn1=404 cn1Label=response_code src=10.10.77.54 spt=49399 dst=10.10.175.82 dpt=443 requestMethod=POST app=HTTPS request=/ipp/port1 cs5=N/A cs5Label=x_forwarded_for_header_value rt=Jun 26 2012 14:18:55 deviceExternalId=0 cs4=N/A cs4Label=attack_type cs6=N/A cs6Label=geo_location cs3Label=full_request cs3=POST /ipp/port1 HTTP/1.1\r\nHost: 127.0.0.1:631\r\nCache-Control: no-cache\r\nContent-Type: application/ipp\r\nAccept: application/ipp\r\nUser-Agent: Hewlett-Packard IPP\r\nContent-Length: 9\r\n\r\n\r\n
```

F5 Networks Local Traffic Manager

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
SNMP	Host name, serial number, hardware (CPU, memory, network interface, disk etc) and software information (running and installed software)	Uptime, CPU, Memory, Disk utilization, Interface Utilization, Hardware status, process level CPU and memory utilization	Performance/Availability Monitoring
SNMP Trap		Exception situations including hardware failures, certain security attacks, Policy violations etc	Performance/Availability Monitoring
Syslog		Permitted and Denied traffic	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "f5-LTM" to see the event types associated with this device.

Search for "f5-BigIP" in **ADMIN > Device Support > Event Types** to see event types associated with SNMP traps for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [SNMP Trap](#)
- [Example SNMP Trap](#)
- [Syslog](#)
- [Example Syslog](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example SNMP Trap

```
2012-01-18 14:13:43 0.0.0.0(via UDP: [192.168.20.243]:161) TRAP2, SNMP v2c, community public
. Cold Start Trap (0) Uptime: 0:00:00.00 DISMAN-EVENT-MIB::sysUpTimeInstance =
Timeticks: (33131) 0:05:31.31 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.3375.2.5.0.1
```

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog

```
<133>Oct 20 13:52:46 local/tmm notice tmm[5293]: 01200004:5: Packet rejected remote IP
172.16.128.26 port 137 local IP 172.16.128.255 port 137 proto UDP: Port closed.

<134>Jul 30 15:28:33 tmm1 info tmm1[7562]: 01070417: 134: ICSA: non-session UDP packet accepted,
source: 112.120.125.48 port: 10144, destination: 116.58.240.252 port: 53

<134>Jul 30 15:28:33 tmm1 info tmm1[7562]: 01070417: 134: ICSA: non-session TCP packet accepted,
source: 108.83.156.153 port: 59773, destination: 116.58.240.225 port: 80

<134>Jul 30 15:28:33 tmm2 info tmm2[7563]: 01070417: 134: ICSA: non-session ICMP packet accepted,
source: 10.11.218.10, destination: 10.255.111.2, type code: Echo Reply
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

F5 Networks Web Accelerator

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted traffic	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "f5-web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Example Syslog

```
<182>Oct 20 13:52:56 local/BadReligion1 info logger: [ssl_acc] 1.1.1.2 - admin [20/Oct/2011:13:52:56 -0400] "POST /iControl/iControlPortal.cgi HTTP/1.1" 200 654
```

Fortinet FortiADC

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
syslog	Host name, Reporting IP	None	Event, Security and Traffic logs	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiADC" to see the event types associated with this device.

Rules

No specific rules are written for FortiADC Web application firewall but generic firewall rules will apply.

Reports

No specific reports are written for FortiADC Web application firewall but generic firewall rules will apply.

Configuration

Configure FortiADC Web application firewall to send logs to FortiSIEM in the supported format (see [Sample Events](#)).

To configure a syslog object in FortiADC, take the following steps:

Note: Refer to the FortiADC Handbook for the most recent configuration information. Configuration taken from [6.1.2 FortiADC Handbook](#).

1. Go to **System > Alert > Alert Resource** and select the **Syslog** tab.
2. Click **Create New**.
3. Complete the configuration as described in the following table.

Settings	Guidelines
Name	Enter a name for the syslog message object. No spaces. You will use this name to select the syslog in an Alert Actions profile.
Syslog Server	Enter the IP address of the syslog server that will receive syslog messages.
Port	Enter the port of the syslog server. The default is 514.

4. Click **Save**.

Settings for Access Credentials

None required

Sample Events

```
<6>date=2019-06-12 time=13:05:52 device_id=FAD2KD3114000026 log_id=0000000100 type=event
subtype=config pri=information vd=root msg_id=71118385 user=user1 ui=GUI(1.2.3.4) action=add
cfgpath=log setting remote cfgobj=<No.> cfgattr=1 logdesc=Change the configuration msg="added a
new entry '1' for "log setting remote" on domain "root""
```

```
<1>date=2019-06-12 time=13:06:52 device_id=FAD2KD3114000026 log_id=0003000235 type=event
subtype=system pri=alert vd=root msg_id=71118386 submod=update user=system ui=system action=update
status=none logdesc=License could not be validated msg="Unable to connect to FDS server"
```


Qualys Web Application Firewall

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted and Denied Web traffic	Log analysis and compliance

Event Types

The following event types are generated by parsing Qualys Web Application Firewall traffic logs and analyzing the HTTP error code.

- Qualys-WAF-Web-Request-Success
- Qualys-WAF-Web-Bad-Request
- Qualys-WAF-Web-Client-Access-Denied
- Qualys-WAF-Web-Client-Error
- Qualys-WAF-Web-Forbidden-Access-Denied
- Qualys-WAF-Web-Length-Reqd-Access-Denied
- Qualys-WAF-Web-Request
- Qualys-WAF-Web-Request-Redirect
- Qualys-WAF-Web-Server-Error

Rules

There are no predefined rules for this device.

Reports

Relevant reports are defined in **RESOURCES > Reports > Device > Network > Web Gateway**.

Configuration

FortiSIEM processes events from this device via syslog sent in **JSON format**. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Qualys Web Application Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

Note that each JSON formatted syslog contains many logs.

```
<1350>1 2015-05-15T12:57:30.945000+00:00 localhost qualys_waf - QUALYS_WAF - {"timestamp":"2015-05-15T12:57:30.945-00:00","duration":6011,"id":"487c116c-4908-4ce3-b05c-eda5d5bb7045","clientId":"172.27.80.170","clientPort":9073,"sensorId":"d3acc41f-d1fc-43be-af71-e7e10e9e66e2","siteId":"41db0970-8413-4648-b7e2-c50ed53cf355","connection":{"id":"bc1379fe-317e-4bae-ae30-2a382e310170","clientId":"172.27.80.170","clientPort":9073,"serverIp":"192.168.60.203","serverPort":
```

```
:443},"request":{"method":"POST","uri":"/","protocol":"HTTP/1.1","host":"esers-test.foo.org","bandwidth":0,"headers":[{"name":"Content-Length","value":"645"}, {"name":"Accept","value":"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
```

```
q=0.8"},"name":"User-Agent","value":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36"},"name":"Content-Type","value":"application/x-www-form-urlencoded"}, {"name":"Referer","value":"https://esers-test.ohsers.org/"}, {"name":"Accept-Encoding","value":"gzip, deflate"}, {"name":"Accept-Language","value":"en-US,en;q=0.8"}], "headerOrder": "HILCAUTRELO"}, "response": {"protocol": "HTTP/1.1", "status": "200", "message": "OK", "bandwidth": 0, "headers": [{"name": "Content-Type", "value": "text/html; charset=utf-8"}, {"name": "Server", "value": "Microsoft-IIS/8.5"}, {"name": "Content-Length", "value": "10735"}], "headerOrder": "CTXSDL"}, "security": {"auditLogRef": "b02f96e9-2649-4a83-9459-6a02da1a5f05", "threatLevel": 60, "events": [{"tags":
```

```
[{"qid/226015","cat/XPATHi","cat/SQLi","qid/150003","loc/req/body/txtUserId","cfg/pol/applicationSecurity"},
```

```
"type":"Alert","rule":"main/qrs/sqli/xpathi/condition_escaping/boolean/confidence_high/3","message":"Condition escaping detected (SQL or XPATH injection) - txtUserId.","confidence":80,"severity":60,"id":"262845566"},{"tags":["cat/correlation","qid/226016"],"type":"Observation","rule":"main/correlation/1",
```

```
"message":"Info: Threat level exceeded blocking threshold (60).","confidence":0,"severity":0,"id":"262846018"},{"tags":["cat/correlation","qid/226016"],"type":"Observation","rule":"main/correlation/1",
```

```
"message":"Info: Blocking refused as blocking mode is disabled.","confidence":0,"severity":0,"id":"262846167"},{"tags":["cat/correlation","cat/XPATHi","qid/226015"],"type":"Alert","rule":
```

```
"main/correlation/1","message":"Detected: XPATHi.","confidence":80,"severity":60,"id":"268789851"}]]}]}
```

Log Aggregators

FortiSIEM supports these devices.

- [Fortinet FortiAnalyzer](#)

Fortinet FortiAnalyzer

- [Overview](#)
- [Configuring FortiAnalyzer](#)
- [Configuring FortiSIEM Collectors to Receive Logs from FortiAnalyzer](#)
- [Configuring FortiAnalyzer to Forward its own System Event Logs](#)

Overview

Customers of both FortiAnalyzer and FortiSIEM may want to take already aggregated event data received on FortiAnalyzer and forward those events to FortiSIEM.

Configuring FortiAnalyzer

- [Setting Up the Syslog Server](#)
- [Pre-Configuration for Log Forwarding](#)
- [Configuring Log Forwarding](#)

Setting Up the Syslog Server

1. Login to FortiAnalyzer.
2. Go to **System Settings > Advanced > Syslog Server**.
 - a. Click the **Create New** button.
 - b. Enter the **Name**. (It is recommended to use the name of the FortiSIEM server.)
 - c. Fill in the **IP address** (or **FQDN**) with the IP or a fully qualified name of the FortiSIEM server.
 - d. Leave the **Syslog Server Port** to the default value '514'.
 - e. Click **OK** to save your entries.

Pre-Configuration for Log Forwarding

To configure FortiAnalyzer event forwarding to FortiSIEM, you must first set up the following.

1. Install a FortiSIEM collector in the same subnet as FortiAnalyzer that will be forwarding the events.
Note: The same subnet request is required as FortiAnalyzer will later be configured to spoof packets to the

collector. RPF (reverse path forwarding checks) on network equipment would have to be disabled if FortiAnalyzer and collector existed on different subnets.

2. It is recommended that for every 5,000 EPS (events per second) ingested, you add 1 collector that is 8vCPU, 8GB RAM. If you have more than 5,000 EPS forwarding from FortiAnalyzer, please set up a load balancer with multiple collectors behind it, allowing UDP 514 inbound.

Configuring Log Forwarding

Take the following steps to configure log forwarding on FortiAnalyzer.

1. Go to **System Settings > Log Forwarding**.
2. Click the **Create New** button in the toolbar. The **Create New Log Forwarding** pane opens.
3. fill in the information as per the below table, then click **OK** to create the new log forwarding. The FortiAnalyzer device will start forwarding logs to the server.

Field	Input
Name	FortiSIEM-Forwarding
Status	On
Remote Server Type	Syslog
Compression	OFF
Sending Frequency	Real-time
Log Forwarding Filters	Select all desired Administrative Domains (ADOMs) / device logs you'd like to forward

4. Go to the CLI Console and configure the CLI only log forward option by running the following CLI commands.

Notes:

- Logs received by FortiAnalyzer, and then forwarded to FortiSIEM, have the source IP of the log packet overwritten with the IP address of the FortiAnalyzer appliance. This hides the "true" source of the log packet from FortiSIEM. To override this behavior, FortiAnalyzer can spoof the original log sender's IP address when forwarding to FortiSIEM. This allows FortiSIEM collectors to receive all the original information as if it received the logs directly from the originating device.
- For FortiAnalyzer versions 7.6, 7.4, 7.2 and later, use the following CLI:

Note: Replace *<id>* with the actual name of the log forward created earlier.

```
config system log-forward
  edit <id>
    set mode forwarding
    set fwd-max-delay realtime
    set server-name "<FSM_Collector>"
    set server-addr "a.b.c.d"
    set fwd-log-source-ip original_ip
    set fwd-server-type syslog
  next
end
```

- To configure FortiAnalyzer to forward its own local logs, see [Configuring FortiAnalyzer to Forward its own System Event Logs](#).

Configuring FortiSIEM Collector to Receive Logs from FortiAnalyzer

To configure the FortiSIEM collector to receive logs from FortiAnalyzer, you will need to disable RPF checks that would normally cause the collector virtual machine from dropping the log packet as it is spoofed.

```
sysctl -w net.ipv4.conf.all.rp_filter=0
```

To make this change persistent across reboots, add the following code to the `/etc/sysctl.conf` file.

```
net.ipv4.conf.all.rp_filter=0
```

Configuring FortiAnalyzer to Forward its own System Event Logs

FortiAnalyzer can forward two primary types of logs, each configured differently:

- Events received from other devices (FortiGates, FortiMail, FortiManager, etc)
- Locally generated System events (FortiAnalyzer admin login attempts, config changes, etc)

FortiAnalyzer System Event Logs via Syslog

- 9 event types
- no rules
- no reports
- no dashboards

Configuring FortiAnalyzer System's Local Log

To configure the system's local log, replace the IP with the IP of the FortiSIEM collector.

```
config system syslog
edit "fortisiem"
    set ip "192.168.1.1"
end
config system locallog syslogd setting
set status enable
set syslog-name "fortisiem"
end
```

Network Access Control

FortiSIEM supports these Network Access Control Management applications and devices.

- [Fortinet FortiNAC](#)
- [HPE Aruba Networking ClearPass Policy Manager](#)

Fortinet FortiNAC

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Administrative and User Admission Control events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiNAC" to see the event types associated with this device.

Rules

No specific rules are written for FortiNAC but generic rules for network admission control apply

Reports

No specific reports are written for FortiNAC but generic reports for network admission control apply
Configuration

Configuration

Configure FortiNAC system to send logs to FortiSIEM in the supported format (see [Sample Events](#)).

To configure FortiNAC to send syslog to FortiSIEM, take the following steps:

Note: Refer to the latest FortiNAC Administration Guide for the latest instructions. Steps provided here to configure syslog for FortiSIEM are from the [9.1.0 FortiNAC Administration Guide](#).

1. Click **System > Settings**.
2. In the left navigation tree, select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Enter the configuration parameters from the following table to configure:

Field	Definition
Type	Select Syslog Command Event Format (CEF) for FortiSIEM configuration.
IP address	Provide the IP address of the FortiSIEM Collector that will receive Event and Alarm messages.
Port	The default port for Syslog CEF servers is 514 . Leave as is.
Facility	Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is 4 security/authorization messages . Leave as is.

5. Click **OK**.

Settings for Access Credentials

None required.

Sample Events

```
<37>Jan 08 19:03:45 : CEF:0|Bradford Networks|FortiNAC-VM-Control and Application
Server|8.3.0.79|426|
Adapter Destroyed|1|rt=Jan 08 19:03:45 269 UTC cat=EndStation msg=Adapter 18:5E:0F:AA:56:31
Destroyed.
```

```
<37>Dec 06 10:34:42 : CEF:0|Bradford Networks|FortiNAC-VM-Control and Application Server|
8.3.1.30|447702|Admin User Login Success|1|rt=Dec 06 10:34:42 736 CET
cat= suid=guiadmin msg=Admin user guiadmin logged in.
```

```
<37>Apr 16 11:06:19 : CEF:0|Bradford Networks|FortiNAC-VM-Control and Application
Server|8.3.6.104|605250|
Security Risk Host|1|rt=Apr 16 11:06:19 447 CEST cat=EndStation src=192.168.242.20
smac=00:26:9E:D9:87:12
shost=X100e-1 cs1Label=Physical<space>network<space>location cs1=BA-HPswitch GigabitEthernet1/0/10
{ GigabitEthernet1/0/10 Interface } msg=Host failed Windows-PA-Notepad Tests: Failed :: Custom ::
Notepad
MAC Address: 00:26:9E:D9:87:12 Last Known Adapter IP: 192.168.242.20 Host Location: BA-HPswitch
GigabitEthernet1/0/10 { GigabitEthernet1/0/10 Interface }
```

HPE Aruba Networking ClearPass Policy Manager

HPE Aruba Networking ClearPass Policy Manager (CPPM) provides robust network access control with granular role-based policies for authentication, authorization, continuous monitoring and enforcement with its highly

interoperability feature.

Vendor Version Tested: Not Provided

Vendor: Hewlett Packard Enterprise

Product: Aruba Networking ClearPass Policy Manager

Product Information: <https://www.arubanetworks.com/products/security/network-access-control/secure-access/>

- [Event Types](#)
- [Configuration](#)
- [Sample Events](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "aruba clearpass" to see the event types associated with this device.

Configuration

- [Setup in Aruba ClearPass Policy Manager](#)

Setup in Aruba ClearPass Policy Manager

Complete these steps from your HPE Aruba ClearPass Policy Manager server. No additional configuration is required on FortiSIEM.

Note: The ClearPass Policy Manager User Guide can be found [here](#).

Configure Syslog Target

1. Log in to your Aruba ClearPass Policy Manager server.
2. Navigate to **Administration > External Servers > Syslog Targets**.
3. Click on **Add**.
4. From the **Add Syslog Target** window, enter the following configuration information for your FortiSIEM. See [Syslog Targets](#) for more information.
 - a. In the **Host Address** field, enter your FortiSIEM IP Address.
 - b. For **Protocol**, select **UDP**.
 - c. For **Server Port**, enter "514".
 - d. Click **Save**.

Configure Syslog Export Filter

See [Adding a Syslog Export Filter](#) for more information.

1. Navigate to **Administration > External Servers > Syslog Export Filters**.
2. Click **Add**.
3. Configure as required. Ensure the following is done.
 - a. For **Export Event Format Type**, select **Standard**.
 - b. For **Syslog Servers**, select the FortiSIEM Syslog target you created earlier from the drop-down list.
 - c. Click **Save**.

Sample Events

```
<143>2012-05-30 16:07:55,484 192.168.1.68 A0361 0 1 0 protocol=RADIUS,username=test1,login_
status=REJECT,request_timestamp=2012-05-30 16:06:23-07,connection_dest_ip_
address=192.0.20.0,connection_nad_ip_address=192.0.20.3,
```

```
<143>2015-09-17 15:58:58,474 10.0.0.20 ClearPassAuth 204 1 0
Auth.Username=john,Auth.Service=Aruba-Wireless-Service (xxxxxxx),Auth.Roles=[AirGroup v2][[Guest]]
[User Authenticated],Endpoint.Device-Category=SmartDevice,Endpoint.Device-
Family=Apple,Endpoint.MAC-Address=aabbccddeeff,Endpoint.MAC-Vendor=Apple,Endpoint.IP-
Address=192.0.20.1,Endpoint.Hostname=My_iPhone,Endpoint.Device-Name=Apple iPhone,Auth.Auth-
Status=User
```

Network Compliance Management Applications

FortiSIEM supports these Network Compliance Management applications and monitoring.

- [Cisco Network Compliance Manager](#)
- [PacketFence](#)

Cisco Network Compliance Manager

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Network device software update, configuration analysis for compliance, admin login	Log analysis and compliance

Event Types

Over 40 event types are generated by parsing Cisco Network Configuration Manager logs. The complete list can be found in **ADMIN > Device Support > Event Types** by searching for "Cisco-NCM". Some important ones are

- Cisco-NCM-Device-Software-Change
- Cisco-NCM-Software-Update-Succeeded
- Cisco-NCM-Software-Update-Failed
- Cisco-NCM-Policy-Non-Compliance
- Cisco-NCM-Device-Configuration-Deployment
- Cisco-NCM-Device-Configuration-Deployment-Failure

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example Syslog

Note that each JSON formatted syslog contains many logs.

```
490998571 Mon Mar 03 03:09:31 EST 2014 Savvy Device Command Script Completed Successfully
server01.foo.com 10.4.161.32 Script 'Re-enable EasyTech port for Cisco IOS configuration'
completed. Connect - Succeeded Connected via ssh to 10.170.30.9 [in realm Default Realm] Login
/ Authentication - Succeeded Successfully used: Last successful password (Password rule Retail
TACACS NCM Login) Optional:Script - Succeeded Successfully executed: prepare configuration for
deployment Script - Succeeded Successfully executed: deploy to running configuration via TFTP
through CLI Bypassed: deploy to running configuration via SCP through CLI. (Requires SCP, CLI to
be enabled.) Tried: deploy to running configuration via FTP through CLI (Warning: SSH server
username or password not specified in NA admin settings.) Optional:Script - Succeeded
Successfully executed: determine result of deployment operation Script run: -----
----- ! interface fast0/16 no shut

491354611 Tue Mar 04 03:38:22 EST 2014 FooA Software Update Succeeded server01.foo.com 1.1.1.32
44571 10.173.30.9 $0rignatorEmail$ FooA Update Device Software 2014-03-04 03:30:00.0 usmist_
1699295009 (1.13.3.9) Succeeded
```

PacketFence Network Access Control (NAC)

- [Integration Points](#)
- [Event Types](#)
- [Configuring PacketFence Network Access Control](#)

Integration Points

Protocol	Information Discovered	Used For
Syslog	User network admission control events	Security and Compliance

Event Types

Over 20 events are parsed. See event types in **RESOURCES > Event Types** and search for "PacketFence-NAC-" in the main content panel **Search...** field.

Configuring PacketFence NAC

Follow PacketFence NAC documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes PacketFence NAC syslog as long as it follows the format shown in the sample syslog:

```
Oct 9 11:29:34 10.2.204.81 1 2018-10-09T11:29:34.04189+01:00 example.com packetfence.log - - -
Oct 11 15:42:00 httpd.aaa(4765) WARN: [mac:40:83:1d:12:2a:cb] Calling match with empty/invalid
rule class. Defaulting to 'authentication' (pf::authentication::match)
```

Network Detection and Response

FortiSIEM supports these devices.

- [Fortinet FortiNDR \(Formerly FortiAI\)](#)
- [Fortinet FortiNDR Cloud](#)
- [Zeek Network Security Monitor \(Previously known as Bro\)](#)

Fortinet FortiNDR (Formerly FortiAI)

- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortiai" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortiai" in the main content panel **Search...** field to see related rules associated with this device.

- FortiAI: Attack Chain Blocked
- FortiAI: Attack Chain Permitted

Reports

In **RESOURCES > Reports**, search for "fortiai" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

FortiAI Syslog Configuration

See the current FortiAI Administration Guide for the latest configuration information under Log & Report. The instructions provided here are based off the [1.5.0 FortiAI Administration Guide](#).

1. From the FortiAI GUI, navigate to **Log and Report > Log Settings > Remote Log Server**.
2. Set **Send logs to FortiSIEM** to **Enable**.
3. Set **Type** to **Syslog**.
4. In the **Log Server Address** field, enter the IP address or FQDN of the FortiSIEM Collector.
5. In the Port field, enter "514".
6. Click **OK**.

Fortinet FortiNDR Cloud

Support Added: FortiSIEM 7.1.0

Vendor Version Tested: Not Provided

Vendor: Fortinet

Product Information: <https://www.fortinet.com/products/network-detection-and-response>

FortiNDR Cloud is a cloud-native network detection and response solution built for the rapid detection of threat activity, investigation of suspicious behavior, proactive hunting for potential risks, and directing a fast and effective response to active threats.

- [What is Collected](#)
- [Configuration](#)
- [Rules and Reports](#)
- [Search FortiNDR Cloud Events via Event Type Prefix](#)

What is Collected

Object Collected	Description
Detections – via FortiNDR Cloud API Key integration	FortiNDR Cloud Detections is an alert mechanism that notifies you when events matching a specific criteria appear in your account. Detections allow you to quickly identify and respond to suspicious or known malicious activity in your network.
Signals – via FortiNDR Cloud Metastream S3 bucket integration	Underlying sensor traffic logs that comprise one or more detections.
Devices – via FortiNDR Cloud	This is simply a host IP of a device seen on your network, detected by

Object Collected	Description
Metastream S3 bucket integration	FortiNDR sensor.
Sensor Data – via FortiNDR Cloud Metastream S3 bucket integration	This is verbose sensor data collected in the customer environment. It is generally not recommended to pull this data unless required.

S3 bucket data is optional, and it is generally recommended that only signals data be ingested.

For more information on what a detection is in FortiNDR, see [here](#).

Configuration

- [Setup in FortiNDR](#)
- [Setup in FortiSIEM](#)

Setup in FortiNDR

- Create API Key
- Enable MetaStream for FortiNDR Cloud (S3 bucket data ingestion – optional)

Create API Key

An API key is required so that FortiSIEM can use to query FortiNDR Cloud. To create an API key, take the following steps:

1. Login to FortiNDR Cloud portal.
2. Click the username icon on top right hand corner of FortiNDR Cloud Portal.
3. On the **My Profile** page, in the Token section, click **Create new token**.
4. Store the created token in a password management utility as this will be later used in FortiSIEM. It is strongly recommended to copy it directly into FortiSIEM integration in FortiSIEM Credential Definition, and to not store the key anywhere else.
5. Follow the steps in [Setup in FortiSIEM](#) to continue, or follow the optional steps [Enable MetaStream for FortiNDR Cloud](#).

Enable MetaStream for FortiNDR Cloud (S3 bucket data ingestion – optional)

Take the following steps to enable MetaStream for FortiNDR Cloud.

1. Login to FortiNDR Cloud as an administrator.
2. Go to Account Management.
3. Select an account.
4. Click the **Modules** tab.

5. Find the MetadataStream block.

If the feature is inactivated, click **Contact Support** to get information on how to contact Fortinet Support to license the Meta Stream feature.

If the feature is enabled, you will see a **Retrieve** button. Refer to **Retrieving S3 Credentials** for instructions.

Retrieving S3 Credentials

Note: You must be an "Admin" user to perform these steps.

1. Go to Account Management.
2. Select an account.
3. Click the **Modules** tab.
4. Find the Metadata Stream block.
5. Click **Retrieve** to retrieve the credentials.
6. View Credentials in the dialog that appears.

Note the following:

- Access Key Id
- Secret Access Key
- Bucket
- Prefix

Setup in FortiSIEM

Note: The S3 Bucket configuration is optional, and not required to populate the dashboards. This data is ideally for long term retention of underlying event data that resulted in a detection in FortiNDR Cloud.

Take the following steps:

1. Login to FortiSIEM tenant as an administrator.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the **Access Method Definition** window, input the following:
 - a. In the **Name** field, enter "FortiNDR".
 - b. From the **Device Type** drop-down list, select **Fortinet FortiNDR Cloud**.
 - c. In the **API Key** field, enter/paste the API Key you created earlier.
 - d. In the **S3 Bucket Name** field, enter "fortindr-cloud-metastream".
 - e. In the **S3 Bucket Prefix** field, enter "/v1/customer/cust-xxxx/".
 - f. In the **S3 Access Key** field, enter/paste your S3 Access Key.
 - g. In the **S3 Access Key Secret** and **Confirm S3 Access Key** field, enter/paste the S3 Access Key Secret.
 - h. From the **S3 Data Set Options** drop-down list, select the types of data to ingest.
 - Signals (default)
 - Devices
 - Sensor Data (heavy cost, not recommended unless required)
 - i. When done, click **Save**.

Under **Step 2: Enter IP Range to Credential Associations**, take the following steps.

1. If the organization has more than 1 collector, select the collector from the drop-down list that will do the API polling.

Note: If the organization has 1 or no collectors, there is no drop-down list, so you can proceed to step 2.

2. Click **New**.
3. From the **Device Credential Mapping Definition** window, take the following steps.

- a. In the **IP/Host Name** field:
 - For the US region, enter "detections.icebrg.io"
 - For the EU region, enter "investigation.eu.fortindr.forticloud.com"
- b. From the **Credentials** drop-down list, select the credential you just created in the above steps.
- c. Click **Save**.

Note: As of this writing, the current API endpoint for FortiNDR Cloud is "detections.icebrg.io", but this can change in the future. Reference FortiNDR Cloud API documentation [here](#) for more information.

Verifying Mapping

To verify your configuration, take the following steps.

1. Under **Step 2: Enter IP Range to Credential Associations**, select the "IP to Credential Mapping" you just created.
2. Click the **Test** drop-down, and select **Test Connectivity without Ping**.

After a successful test, it will be approximately 5 minutes before the first pull job starts. You can view this by clicking the **Pull Events** tab at the top of the screen.

 - A yellow star next to a pull job means it has not started yet.
 - A green checkmark means the pull job has completed successfully for the latest interval.
 - Other status implies an error.

Rules and Reports

The following rules and reports are available.

Rules

FortiNDR Cloud: High Severity Detection triggered for a Host

FortiNDR Cloud: Moderate Severity Detection triggered for a Host

FortiNDR Cloud: Low Severity Detection triggered for a Host

Reports

FortiNDR Cloud: Detection Details

FortiNDR Cloud: Top Detection Categories by Count

FortiNDR Cloud: Top Detection Hosts by Count

FortiNDR Cloud: Top Detections and Hosts by Count

FortiNDR Cloud: Top Detections by Count

FortiNDR Cloud: Top Detection Severities by Count

Search FortiNDR Cloud Events via Event Type Prefix

You can locate FortiNDRCloud raw logs by running a search. FortiNDR Cloud event types contain "FortiNDRCloud". Perform a search by taking the following steps:

1. Navigate to **Analytics**.
2. Click inside the **Edit Filters and Time Range...** field.
3. Ensure **Event Attribute** is selected in **Filter By**. If not, select it.
4. In the first row, input the following:
 - a. In the **Attribute** field, enter/select "Event Type".
 - b. From the **Operator** drop-down list, select "=".
 - c. In the **Value** field, enter "FortiNDRCloud".
 - d. Configure any additional parameters, and click **Apply & Run**.

Zeek Network Security Monitor (Previously known as Bro)

FortiSIEM Support added: 5.2.5 (Installed on Security Onion)

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Zeek

Product Information: <https://zeek.org/>

- [Log Information](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

Log Information

Log Collection Method	Log Body Format Accepted	Purpose
Syslog (via Rsyslog)	JSON	Security and Compliance

Event Types

In 6.3.1, there are 29 event types.

Rules

There are no specific rules for Zeek Network Security Monitor.

Reports

There are no specific reports for Zeek Network Security Monitor.

Configuration

To forward logs to FortiSIEM, they must be configured to follow a specific format. Prior to this configuration, you may need to configure Zeek to output logs to JSON format. If you are using Security Onion with Zeek, you can skip the [Configuring Zeek to Output Logs to JSON](#) as Security Onion by default configures Zeek for JSON.

- [Configuring Zeek to Output Logs to JSON](#)
- [FortiSIEM Expected Format](#)
- [Zeek Deployment through Security Onion Rsyslog Configuration](#)
- [Standalone Zeek Deployment Rsyslog Configuration](#)

Configuring Zeek to Output Logs to JSON

To configure Zeek to output logs to JSON, take the following steps:

1. Stop Zeek if it is running by using the following command.
`zeekctl stop`
2. Edit `/opt/zeek/share/zeek/site/local.zeek` by adding the following line.
`@load policy/tuning/json-logs.zeek`
3. Restart Zeek and confirm logs are stored in JSON format by running the follow commands.
`zeekctl deploy`
`cd /opt/zeek/logs/current`
`less conn.logs`

FortiSIEM Expected Format

Rsyslog or Syslog NG configuration is required to pickup the desired logs using FortiSIEM's expected format.

```
Example Format of Log:
<190>Jun 16 17:55:50 host1 zeek_conn: {}
```

The log type is appended to `zeek_<log file name>`. See [here](#) for more information.

Rsyslog or Syslog-ng must be configured to pick up the defined log files and put them in the correct expected header format.

```
<190>Jun 16 17:55:50 host1 zeek_<log_file_name> <log body>
```

Example:

```
<190>Jun 16 17:55:50 co-nuc zeek_conn:
{"ts":1623862540.702791,"uid":"CBeSUC20TqYMeNKaL4","id.orig_h":"192.168.77.115","id.orig_p":58734,"id.resp_h":"1.1.1.1","id.resp_p":443,"proto":"tcp","conn_state":"OTH","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0}
```

This format is achieved in rsyslog if you specify an input file tag when opening the log file as shown here.

\$InputFileTag zeek_conn:

Choose the configuration that matches your environment.

- [Zeek Deployment through Security Onion Rsyslog Configuration](#)
- [Standard Zeek Deployment Rsyslog Configuration](#)

Zeek Deployment through Security Onion Rsyslog Configuration

If your Zeek deployment is through Security Onion, and you are using the Centos 7 + docker ISO download, you can use rsyslog to collect the log files. The path to your logs should be here: /nsm/zeek/logs/current. The default format is already JSON.

Under this folder, you have several defaults, listed here:

```
broker.log
capture_loss.log
cluster.log
conn.log
loaded_scripts.log
notice.log
packet_filter.log
reporter.log
stats.log
stderr.log
stdout.log
weird.log
```

Take the following steps:

1. Open the Rsyslog file using the following command.
`vi /etc/rsyslog.conf`
2. Under the Modules section, add the following line.
`$ModLoad imfile`
3. In between the Global Directives and Rules sections, add the following:

```
$InputFileName /nsm/zeek/logs/current/notice.log
$InputFileTag zeek_notice:
$InputFileStateFile stat-zeek_notice
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/cluster.log
$InputFileTag zeek_cluster:
$InputFileStateFile stat-zeek_cluster
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/loaded_scripts.log
$InputFileTag zeek_loaded_scripts:
$InputFileStateFile stat-zeek_loaded_scripts
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/conn.log
$InputFileTag zeek_conn:
$InputFileStateFile stat-zeek_conn
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dns.log
$InputFileTag zeek_dns:
$InputFileStateFile stat-zeek_dns
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/http.log
$InputFileTag zeek_http:
$InputFileStateFile stat-zeek_http
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
```



```
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dhcp.log
$InputFileTag zeek_dhcp:
$InputFileStateFile stat-zeek_dhcp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ntp.log
$InputFileTag zeek_ntp:
$InputFileStateFile stat-zeek_ntp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dce_rpc.log
$InputFileTag zeek_dce_rpc:
$InputFileStateFile stat-dce_rpc
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/kerberos.log
$InputFileTag zeek_kerberos:
$InputFileStateFile stat-kerberos
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ntlm.log
$InputFileTag zeek_ntlm:
$InputFileStateFile stat-ntlm
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ssl.log
$InputFileTag zeek_ssl:
$InputFileStateFile stat-zeek_ssl
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/files.log
$InputFileTag zeek_files:
$InputFileStateFile stat-zeek_files
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
```

```
$InputFileName /nsm/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/x509.log
$InputFileTag zeek_x509:
$InputFileStateFile stat-zeek_x509
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/pe.log
$InputFileTag zeek_pe:
$InputFileStateFile stat-zeek_pe
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/rdp.log
$InputFileTag zeek_rdp:
$InputFileStateFile stat-zeek_rdp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/traceroute.log
$InputFileTag zeek_irc:
```

```
$InputFileStateFile stat-zeek_traceroute
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dpd.log
$InputFileTag zeek_dpd:
$InputFileStateFile stat-zeek_dpd
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/software.log
$InputFileTag zeek_software:
$InputFileStateFile stat-zeek_software
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/weird.log
$InputFileTag zeek_weird:
$InputFileStateFile stat-zeek_weird
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/known_services.log
$InputFileTag zeek_known_services:
$InputFileStateFile stat-zeek_known_services
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/known_hosts.log
$InputFileTag zeek_known_hosts:
$InputFileStateFile stat-zeek_known_hosts
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/known_certs.log
$InputFileTag zeek_known_certs:
$InputFileStateFile stat-zeek_known_certs
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/capture_loss.log
$InputFileTag zeek_capture_loss:
$InputFileStateFile stat-zeek_capture_loss
$InputFileSeverity info
$InputFileFacility local7
```

```
$InputRunFileMonitor
```

4. at the bottom of the Rules section, add the following check for new lines every second.

```
$InputFilePollingInterval 1
local7.info @<ip or FQDN of the FortiSIEM collector>
```

5. Save the file.
 6. Restart Rsyslog by running the following command.
- ```
systemctl restart rsyslog
```

As events occur for Zeek, these logs will be sent to the location specified under @<ip or FQDN of the FortiSIEM collector>.

## Standalone Zeek Deployment Rsyslog Configuration

For standalone Zeek deployment, log file location is most typically here:

```
/opt/zeek/logs/current
```

If your log file path is neither of these, replace the following commands with your correct path.

Take the following steps:

1. Open the Rsyslog file using the following command.
- ```
vi /etc/rsyslog.conf
```
2. Under the Modules section, add the following line.
- ```
$ModLoad imfile
```
3. In between the Global Directives and Rules sections, add the following:

```
$InputFileName /opt/zeek/logs/current/notice.log
$InputFileTag zeek_notice:
$InputFileStateFile stat-zeek_notice
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/conn.log
$InputFileTag zeek_conn:
$InputFileStateFile stat-zeek_conn
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dns.log
$InputFileTag zeek_dns:
$InputFileStateFile stat-zeek_dns
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/http.log
```

```
$InputFileTag zeek_http:
$InputFileStateFile stat-zeek_http
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dhcp.log
$InputFileTag zeek_dhcp:
$InputFileStateFile stat-zeek_dhcp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ntp.log
$InputFileTag zeek_ntp:
$InputFileStateFile stat-zeek_ntp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dce_rpc.log
$InputFileTag zeek_dce_rpc:
$InputFileStateFile stat-dce_rpc
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/kerberos.log
$InputFileTag zeek_kerberos:
$InputFileStateFile stat-kerberos
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ntlm.log
$InputFileTag zeek_ntlm:
$InputFileStateFile stat-ntlm
$InputFileSeverity info
```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ssl.log
$InputFileTag zeek_ssl:
$InputFileStateFile stat-zeek_ssl
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/files.log
$InputFileTag zeek_files:
$InputFileStateFile stat-zeek_files
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/x509.log
$InputFileTag zeek_x509:
$InputFileStateFile stat-zeek_x509
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/pe.log
$InputFileTag zeek_pe:
$InputFileStateFile stat-zeek_pe
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
```

```
$InputFileName /opt/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/rdp.log
$InputFileTag zeek_rdp:
$InputFileStateFile stat-zeek_rdp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/traceroute.log
$InputFileTag zeek_irc:
$InputFileStateFile stat-zeek_traceroute
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dpd.log
$InputFileTag zeek_dpd:
$InputFileStateFile stat-zeek_dpd
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/software.log
$InputFileTag zeek_software:
$InputFileStateFile stat-zeek_software
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/weird.log
$InputFileTag zeek_weird:
$InputFileStateFile stat-zeek_weird
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/known_services.log
$InputFileTag zeek_known_services:
$InputFileStateFile stat-zeek_known_services
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/known_hosts.log
$InputFileTag zeek_known_hosts:
$InputFileStateFile stat-zeek_known_hosts
```

```
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/known_certs.log
$InputFileTag zeek_known_certs:
$InputFileStateFile stat-zeek_known_certs
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/capture_loss.log
$InputFileTag zeek_capture_loss:
$InputFileStateFile stat-zeek_capture_loss
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
```

4. At the bottom of the Rules section, add the following check for new lines every second.

```
$InputFilePollingInterval 1
local7.info @<ip or FQDN of FortiSIEM collector>
```

5. Save the file.
6. Restart Rsyslog by running the following command.
- ```
systemctl restart rsyslog
```

As events occur for Zeek, these logs will be sent to the location specified under @<ip or FQDN of FortiSIEM collector>.

Network Intrusion Detection System

FortiSIEM supports these devices.

- [Microsoft Advanced Threat Analytics \(ATA\) On Premise Platform](#)

Microsoft Advanced Threat Analytics (ATA) On Premise Platform

FortiSIEM Support added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Microsoft

Product Information: <https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata>

Microsoft Advanced Threat Analytics (ATA) is an on-premises platform that helps protect enterprises from multiple types of advanced targeted cyber attacks and insider threats.

- [Log Information](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft-ata" to see the event types associated with this device.

In 6.3.1, there are 51 event types.

Rules

In **RESOURCES > Rules**, search for "microsoft ata" in the main content panel **Search...** field to see related rules associated with this device.

In FortiSIEM 6.3.1, there is 1 rule available.

- Microsoft ATA Center: Security Alert Triggered

Reports

In **RESOURCES > Reports**, search for "microsoft ata" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 reports available.

- Microsoft ATA (Advanced Threat Analytics) Center - Change Audit Events
- Microsoft ATA (Advanced Threat Analytics) Center - Security Alerts

Network Intrusion Prevention Systems (IPS)

FortiSIEM supports these intrusion prevention systems for discovery and monitoring.

- [3COM TippingPoint UnityOne IPS](#)
- [AirTight Networks SpectraGuard](#)
- [Alert Logic IRIS API](#)
- [Armis Asset Intelligence Platform](#)
- [Claroty Continuous Threat Detection](#)
- [Cisco Firepower Management Center \(FMC\) - Formerly FireSIGHT and FirePower Threat Defense](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco Stealthwatch](#)
- [Corero Smartwall Threat Defense System](#)
- [Cylance Protect Endpoint Protection](#)
- [Cyphort Cortex Endpoint Protection](#)
- [Damballa Failsafe](#)
- [Darktrace CyberIntelligence Platform](#)
- [Dragos Platform](#)
- [FireEye Malware Protection System \(MPS\)](#)
- [FortiDDoS](#)
- [Fortinet FortiDeceptor](#)
- [Fortinet FortiSandbox](#)
- [Fortinet FortiTester](#)
- [IBM Internet Security Series Proventia](#)
- [Indegy Security Platform](#)
- [Juniper DDoS Secure](#)
- [Juniper Networks IDP Series](#)
- [McAfee IntruShield](#)
- [McAfee Stonesoft IPS](#)
- [Motorola AirDefense](#)
- [Palo Alto Cortex XDR](#)
- [Radware DefensePro](#)
- [Snort Intrusion Prevention System](#)
- [Sourcefire 3D and Defense Center](#)
- [Trend Micro Deep Discovery](#)
- [Zeek \(Bro\) Installed on Security Onion](#)

3Com TippingPoint UnityOne IPS

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Sample Parsed Syslog Messages](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP		CPU, memory, Interface utilization	Performance and Availability Monitoring
Syslog		IPS Alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "tippingpoint" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [Syslog](#)

SNMP

1. Log in to the TippingPoint appliance or the SMS Console.
2. Go to **System > Configuration > SMS/NMS**.
3. For **SMS Authorized IP Address/CIDR**, make sure **any** is entered.
4. Select **Enabled** for **SNMP V2**.
5. For **NMS Community String**, enter **public**.
6. Click **Apply**.

Syslog

1. Log in to the TippingPoint appliance or the SMS Console.
2. Go to **System > Configuration > Syslog Servers**.

3. Under **System Log**, enter the **IP Address** of the FortiSIEM virtual appliance.
4. Select **Enable syslog offload for System Log**.
5. Under **Aud Log**, enter the **IP Address** of the FortiSIEM virtual appliance.
6. Select **Enable syslog offload for Audit Log**.
7. Click **Apply**.

Configure the Syslog Forwarding Policy (Filter Notification Forwarding)

The filter log can be configured to generate events related to specific traffic on network segments that must pass through the device. This log includes three categories of events.

Event Category	Description
Alert	Alert events indicate that the IPS has detected suspicious activity in the packet, but still permits the packet to pass through (specific settings are controlled by administrator profile)
Block	Block events are malicious packets not permitted to pass
P2P	Refers to peer-to-peer traffic events

In addition, filter events contain a UUID, which is a unique numerical identifier that correlates with the exact security threat defined by Tipping Point Digital Vaccine Files. The FortiSIEM Virtual Appliance will correlate these with authoritative databases of security threats.

1. Go to **IPS > Action Sets**.
2. Click **Permit + Notify**.
3. Under **Contacts**, click **Remote Syslog**.
4. Under **Remote Syslog Information**, enter the **IP Address** of the FortiSIEM virtual appliance.
5. Make sure the **Port** is set to **514**.
6. Make sure **Delimiter** is set to **tab**, **comma**, or **semicolon**.
7. Click **Add to Table Below**.
You should now see the IP address of the FortiSIEM virtual appliance appear as an entry in the **Remote Syslogs** table.

Sample Parsed Syslog Messages

- [Directly from TippingPoint IPS Device](#)
- [From Tipping Point NMS Device](#)

Directly from TippingPoint IPS Device

```
<36>Oct 28 13:10:45 9.0.0.1 ALT,v4,20091028T131045+0480,"PH-QA-TIP1"/20.30.44.44,835197,1,Permit,Minor,00000002-0002-0002-0002-000000000089, "0089: IP: Short Time To Live (1)","0089: IP: Short Time To Live (1)",ip," ",172.16.10.1:0,224.0.0.5:0,20091028T130945+0480,6," ",0,1A-1B <37>Nov 5 20:16:19 20.30.44.44 BLK,v4,20091105T201619+0480,"PH-QA-TIP1"/20.30.44.44,70,2,Block,Low,00000002-0002-0002-0002-000000004316, "4316: OSPF: OSPF Packet With Time-To-Live of 1","4316: OSPF: OSPF Packet With Time-To-Live of 1",ip," ",172.16.10.1:0,224.0.0.5:0,20091105T201619+0480,1," ",0,1A-1B <37>Jul 12 15:04:01 SOCIPS01 ALT,v5,20110712T150401-0500,SOCIPS01/192.168.10.122,3225227,1,Permit,Low,00000002-0002-0002-0002-000000010960, "10960: IM: Google GMail Chat SSL Connection Attempt","10960: IM: Google GMail Chat SSL Connection Attempt",tcp," ",156.63.133.8,10948,72.14.204.189,443, 20110712T150239-0500,3," ",0,6A-6B
```

From Tipping Point NMS Device

```
<36> 7 2 00000002-0002-0002-0002-000000001919 00000001-0001-0001-0001-000000001919 1919: Backdoor: Psychward 1919 tcp 10.1.1.100 13013 10.1.1.101 1240 3 3 2 207-2400-Jack 33761793 1109876221622
<36> 7 2 00000002-0002-0002-0002-000000001919 00000001-0001-0001-0001-000000001919 1919: Backdoor: Psychward 1919 tcp 10.1.1.100 13013 10.1.1.101 1240 3 3 2 207-2400-Jack 33761793 1109876221622
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	3Com TippingPoint UnityOne IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

AirTight Networks SpectraGuard

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "airtight" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Airtight SpectraGuard
Access Protocol	See Access Credentials

Setting	Value
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<30><2013.09.09 19:45:16>CEF:0|AirTight|SpectraGuard Enterprise|6.7|5.51.515|
Authorized AP operating on non-allowed channel|3|msg=Stop:
Authorized AP [AP2.12.c11d] is operating on non-allowed channel.
rt=Sep 09 2013 19:45:16 UTC dvc=10.255.1.36 externalId=726574
dmac=58:BF:EA:FA:26:EF cs1Label=TargetDeviceName
cs1=AP2.12.c11d cs2Label=SSID cs2=WiFiHiSpeed cs3Label=SecuritySetting
cs3=802.11i cn1Label=RSSI_dBm cn1=-50 cn2Label=Channel cn2=149
cs4Label=Locationcs4=//FB/FBFL2
```

Alert Logic IRIS API

Support for Alert Logic IRIS API allows FortiSIEM to respond to incidents and events in real-time with up-to-date situational awareness and comprehensive security analytics.

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuring AlertLogic IRIS for FortiSIEM API Access](#)
- [Configuring FortiSIEM for AlertLogic IRIS API Access](#)
- [Sample Events](#)

Integration Points

Protocol	Information Discovered	Used For
AlertLogic Iris API	Security Alerts created by AlertLogic	Security and Compliance

Event Types

In **RESOURCES > Event Types**, enter "AlertLogic" in the main content panel **Search...** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, enter "AlertLogic" in the main content panel **Search...** field to see the rules associated with this device.

Reports

No defined reports.

Configuring Alert Logic for FortiSIEM API Access

Get API Key from Alert Logic

1. Login to the Alert Logic user interface.
2. On the left menu, select **Admin >Account**.

3. Click **New API Key**.
4. Enter a descriptive name in the **Generate New API key** dialog box.
5. Click **Save** to generate the API key.
A file containing your API key information (**ID**, **ClientSecret**, and **Name**) will be downloaded. The **ID** and **ClientSecret** will be used by FortiSIEM.

Configuring FortiSIEM for Alert Logic API Access

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Alert Logic IPS
Access Protocol	Alert Logic IPS
Pull Interval	The interval in which FortiSIEM will pull events from Alert Logic. Default is 5 minutes.
Access Key ID	Access key for your Alert Logic instance.
Secret Key	Secret key for your Alert Logic instance
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your Alert Logic credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Alert Logic.
5. To see the jobs associated with Alert Logic, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Alert Logic" in the search box.

Sample Events

Raw events of an incident start with [AlertLogic_Incident]:

```
[AlertLogic_Incident]:[reptDevIpAddr]=10.10.10.10,
[reptDevName]=api.cloudinsight.alertlogic.com,[accountId]=11111111.0,[phCustId]=1,
[inIncidentAcknowledgeStatus]=closed,[inIncidentEventFirstSeen]=1558710055.0,
```

```
[inIncidentClearedTime]=1558710055.0,[inIncidentCreateTime]=1558710161.9708278,
[inIncidentCreatedUserId]=,[inIncidentLastModifiedTime]=0,[inIncidentLastModifiedUser]=,
[inCustomerName]=1074822-INT4 - RMS FAWS Test,[msg]=This is a correlation incident,
[inIncidentId]=e911347e8c1ca0fa,[inIncidentStatus]=closed,[attackType]=suspicious-activity,
[type]=,[count]=0.0,[comment]=Test,[eventSeverity]=5,[eventType]=AlertLogic-Incident-User_Test,
[srcIpAddr]=255.255.255.255,[destIpAddr]=255.255.255.255
```

Raw events of an associated event start with [AlertLogic_Incident_Associated_Event]:

```
AlertLogic_Incident_Associated_Event:[reptDevIpAddr]=10.10.10.10,[phCustId]=,
[reptDevIpAddr]=34.192.118.124,[reptDevName]=api.cloudinsight.alertlogic.com,
[accountId]=100000,[inIncidentId]=e9113683d6815742,[httpContentType]=application/x-alpocket-
megmsgs,[description]=meta,[resourceType]=associated log,[resourceName]=Log,
[uuid]=UVUxSk5BQ2tNS3NBQUFBQVhQQnNkRnp3YkhRQUFiRE1BQUVBBSG1Gd2NHeHBZMkYwYVc5dUwzZ3RZV3h3WVd0clpY
UXRiV1ZuY1h0bmN3QUdURT1IVFZOSDphcHBsawNhdGlvbi94LWFscGFja2V0LW1lZ21zZ3M6ZTkxMTM2ODNkNjg5NTc0Mjo
xMDc2MDM2Mw==,[hostname]=meta,[msg]=ddddddd,[eventSeverity]=5,[procId]=0,[procName]=meta,
[collectorTime]=1559260276,[reptDevName]=user,[eventType]=AlertLogic_e9113683d6815742_
Associated_Event
```

Armis Asset Intelligence Platform

Armis utilizes existing management platforms and passive traffic monitoring to discover and identify every device in any environment enterprise, medical, industrial, and more. Armis then analyzes device behavior and detects vulnerabilities to identify risks and threats.

Support Added: FortiSIEM 6.5.0-7.0.1 via Content Update

Vendor Version Tested: Not Provided

Vendor: Armis

Product: The Asset Intelligence and Security Platform

Product Information: <https://www.armis.com/platform/>

- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Armis Asset Intelligence Platform Configuration](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "Armis" to see the event types associated with this device.

Rules

Go to **RESOURCES > Rules** and search for "Armis" in the main content panel **Search...** field.

Reports

There are no predefined reports for the Armis Asset Intelligence Platform.

Armis Asset Intelligence Platform Configuration

To configure the Armis Asset Intelligence Platform with FortiSIEM, take the following steps.

1. From the ARMIS GUI, navigate to **Integrations > Library > Connect SIEM Integration**.
2. In the **Name** field, enter the name of your FortiSIEM.
3. From the **Connection Type** drop-down list, select **UDP**.
4. In the **Address** field, enter the IP address of your FortiSIEM.
5. In the **Port** field, enter 514.
6. From the **Message Format** drop-down list, select **CEF**.
7. Click **Test connection** to validate.

ARMIS

Search

Integrations > Library > Connect SIEM Integration

Analytics

Assets

Network

Security

AVM

Value Packs

Settings

Before You Start

Provide Access Details

Manage Data

SIEM

Name

FSM@fortinet.com

Before You Start

Prior to configuring this integration, please accomplish the prerequisites described at [Full Documentation](#) > Prerequisites.

Provide Access Details

Connection Type

UDP

Address

Port

514

Message Format

CEF

Include Syslog Header

Send Events From

Cloud

Appliance

Select

Enable TLS

Enable Mutual TLS

Client Root CA Certificate

Download File

Test connection

Manage Data

Alerts Severity Threshold

Low

Message Preview

CEF:0|Armis|Armis Discover|4.1|123|SYSTEM_POLICY_VIOLATION|2|start=Jan 18 11:07:53 act=SYSTEM_POLICY_VIOLATION src=1.2.3.4 spt=-

Copy

Full Documentation

About

FortiSIEM 7.2.7 External Systems Configuration Guide
Fortinet Inc.

706

Cisco Firepower Management Center (FMC) - Formerly FireSIGHT and FirePower Threat Defense

Cisco Firepower Management Center (FMC) provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. It can easily go from managing a firewall to controlling applications to investigating and remediating malware outbreaks.

This section describes how FortiSIEM collects logs from Cisco FireSIGHT console and FirePower Threat Defense via the eStreamer API integration. FortiSIEM provides two integrations options, either through the FortiSIEM built-in eStreamer integration or via the Cisco FirePower eStreamer eNcore client.

The Cisco eNcore client Collects System intrusion, discovery, and connection data from the Firepower Management Center or managed device (also referred to as the eStreamer server) to external client applications, in this case via Syslog to FortiSIEM.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Using Cisco eStreamer Client](#)

What is Discovered and Monitored

Protocol	Information Discovered	Logs Collected	Used For
eStreamer API		Intrusion Events, Malware Events. File Events. Discovery Events, User Activity Events, Impact Flag Events	Security Monitoring

Event Types

FortiSIEM obtains events from Cisco FireSIGHT via eStreamer protocol. Event types follow.

- **Intrusion events:** PH_DEV_MON_FIREAMP_INTRUSION

```
[PH_DEV_MON_FIREAMP_INTRUSION]:[eventSeverity]=PHL_CRITICAL,[fileName]=phFireAMPAgent.cpp,
[lineNumber]=381,[reptDevIpAddr]=10.1.23.177,[envSensorId]=6,[snortEventId]=393258,
[deviceTime]=1430501705,[eventType]=Snort-1,[compEventType]=PH_DEV_MON_FIREAMP_INTRUSION,
[ipsGeneratorId]=137,[ipsSignatureId]=2,[ipsClassificationId]=32,[srcIpAddr]=10.131.10.1,
[destIpAddr]=10.131.10.120,[srcIpPort]=34730,[destIpPort]=443,[ipProto]=6,[iocNum]=0,
[fireAmpImpactFlag]=7,[fireAmpImpact]=2,[eventAction]=1,[mplsLabel]=0,[hostVLAN]=0,
[userId]=3013,[webAppId]=0,[clientAppId]=1296,[appProtoId]=1122,[fwRule]=133,
[ipsPolicyId]=63098,[srcIntfName]=b16c69fc-cd95-11e4-a8b0-b61685955f02,
[destIntfName]=b1a1f900-cd95-11e4-a8b0-b61685955f02,[srcFwZone]=9e34052a-9b4f-11e4-9b83-
```

```
efa88d47586f,[destFwZone]=a7bd89cc-9b4f-11e4-8260-63a98d47586f,[connEventTime]=1430501705,
[connCounter]=371,[srcGeoCountryCode]=0,[destGeoCountryCode]=0,[phLogDetail]=
```

- **Malware events:** PH_DEV_MON_FIREAMP_MALWARE

```
[PH_DEV_MON_FIREAMP_MALWARE]:[eventSeverity]=PHL_INFO,[fileName]=phFireAMPAgent.cpp,
[lineNumber]=487,[reptDevIpAddr]=10.1.23.177,[envSensorId]=6,[deviceTime]=1430502934,
[srcIpAddr]=10.110.10.73,[destIpAddr]=10.0.112.132,[srcIpPort]=21496,[destIpPort]=80,
[ipProto]=6,[fileName]=CplLnk.exe,[filePath]=,[fileSize64]=716325,[fileType]=1,
[fileTimestamp]=0,[hashAlgo]=SHA,
[hashCode]=f1bfab10090541a2c3e58b4b93c504be8b65cdc823209c7f4def24acc38d7fd1,
[fileDirection]=1,[fireAmpFileAction]=3,[parentFileName]=,[parentFileHashCode]=,
[infoURL]=http://wrl/wrl/CplLnk.exe,[threatScore]=0,[fireAmpDisposition]=3,
[fireAmpRetrospectiveDisposition]=3,[iocNum]=1,[accessCtlPolicyId]=125870424,
[srcGeoCountryCode]=0,[destGeoCountryCode]=0,[webAppId]=0,[clientAppId]=638,
[applicationId]=676,[connEventTime]=1430502933,[connCounter]=409,[cloudSecIntelId]=0,
[phLogDetail]=
```

- **File events:** PH_DEV_MON_FIREAMP_FILE

```
[PH_DEV_MON_FIREAMP_FILE]:[eventSeverity]=PHL_INFO,[fileName]=phFireAMPAgent.cpp,
[lineNumber]=541,[reptDevIpAddr]=10.1.23.177,[envSensorId]=6,[deviceTime]=1430497343,
[srcIpAddr]=10.131.15.139,[destIpAddr]=10.0.112.137,[srcIpPort]=1587,[destIpPort]=80,
[ipProto]=6,[fileName]=Locksky.exe,[hashAlgo]=SHA,
[hashCode]=aa999f5d948aa1a731f6717484e1db32abf92fdb5f1e7ed73ad6f5a21b0737c1,
[fileSize64]=60905,[fileDirection]=1,[fireAmpDisposition]=3,[fireAmpSperoDisposition]=4,
[fireAmpFileStorageStatus]=11,[fireAmpFileAnalysisStatus]=0,[threatScore]=0,
[fireAmpFileAction]=3,[fileType]=17,[applicationId]=676,[destUserId]=2991,
[infoURL]=http://wrl/wrl/Locksky.exe,[signatureName]=,[accessCtlPolicyId]=125869976,
[srcGeoCountryCode]=0,[destGeoCountryCode]=0,[webAppId]=0,[clientAppId]=638,[connCounter]=103,
[connEventTime]=1430497343,[phLogDetail]=
```

- **Discovery events:**

- PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL

```
PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL:[eventSeverity]=PHL_INFO,
[fileName]=phFireAMPAgent.cpp,[lineNumber]=815,[reptDevIpAddr]=10.1.23.177,
[destIpPort]=2054,[ipProto]=54,[phLogDetail]=
```

- PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT

```
[PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT]:[eventSeverity]=PHL_INFO,
[fileName]=phFireAMPAgent.cpp,[lineNumber]=737,[reptDevIpAddr]=10.1.23.177,
[fingerprintId]=01f772b2-fceb-4777-8a50-1e1f27426ad0,[osType]=Windows 7,
[hostVendor]=Microsoft,[osVersion]=NULL,[phLogDetail]=
```

- PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP

```
[PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP]:[eventSeverity]=PHL_INFO,
[fileName]=phFireAMPAgent.cpp,[lineNumber]=775,[reptDevIpAddr]=10.1.23.177,
[clientAppId]=638,[appName]=Firefox,[phLogDetail]=
```

- PH_DEV_MON_FIREAMP_DISCOVERY_SERVER


```
[PH_DEV_MON_FIREAMP_DISCOVERY_SERVER]:[eventSeverity]=PHL_INFO,
[fileName]=phFireAMPAgent.cpp,[lineNumber]=853,[reptDevIpAddr]=10.1.23.177,
[applicationId]=676,[appTransportProto]=HTTP,[phLogDetail]=
```

- **User activity events:** PH_DEV_MON_FIREAMP_USER_LOGIN

```
[PH_DEV_MON_FIREAMP_USER_LOGIN]:[eventSeverity]=PHL_INFO,[fileName]=phFireAMPAgent.cpp,
[lineNumber]=672,[reptDevIpAddr]=10.1.23.177,[deviceTime]=1430490441,[user]="User1",
[userId]=0,[ipProto]=710,[emailId]=,[loginType]=0,[destIpAddr]=198.18.133.1,[phLogDetail]=
```

- **Impact Flag events:** PH_DEV_MON_FIREAMP_IMPACT_FLAG

```
[PH_DEV_MON_FIREAMP_IMPACT_FLAG]:[eventSeverity]=PHL_CRITICAL,[fileName]=phFireAMPAgent.cpp,
[lineNumber]=591,[reptDevIpAddr]=10.1.23.177,[envSensorId]=6,[snortEventId]=34,
[deviceTime]=1430491431,[eventType]=Snort-648,[compEventType]=PH_DEV_MON_FIREAMP_IMPACT_FLAG,
[ipsGeneratorId]=1,[ipsSignatureId]=14,[ipsClassificationId]=29,[srcIpAddr]=10.131.12.240,
[destIpAddr]=10.131.11.46,[srcIpPort]=80,[destIpPort]=8964,[ipProto]=6,[fireAmpImpactFlag]=7,
[phLogDetail]=
```

Rules

There are no predefined rules for this device.

Reports

The following reports are provided:

- Top Cisco FireAMP Malware Events
- Top Cisco FireAMP File Analysis Events
- Top Cisco FireAMP Vulnerable Intrusion Events
- Top Cisco FireAMP Discovered Login Events
- Top Cisco FireAMP Discovered Network Protocol
- Top Cisco FireAMP Discovered Client App
- Top Cisco FireAMP Discovered OS

Configuration

- [Cisco FireSIGHT Configuration](#)
- [FortiSIEM Configuration](#)

Cisco FireSIGHT Configuration

1. Login to Cisco FIRESIGHT console.
2. Go to **System > Local > Registration > eStreamer**

3. Click **Create Client**

- a. Enter **IP address** and **Password** for FortiSIEM. The password can only contain alpha (a-z, A-Z) and numeric (0-9) characters. Special characters are not allowed.
- b. Click **Save**.

4. Select the types of events that should be forwarded to FortiSIEM.**5. Click **Download Certificate** and save the certificate to a local file.****FortiSIEM Configuration**

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

- [Define Cisco FireSIGHT console and FirePower Threat Defense Credential in FortiSIEM](#)
- [Create IP Range to Credential Association and Test Connectivity](#)

Define Cisco FireSIGHT console and FirePower Threat Defense Credential in FortiSIEM

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 1. b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Cisco FireAMP
Access Protocol	eStreamer SDK
Password	Enter the Password as in Step 3a from Cisco FireSIGHT Configuration .
Certificate File	Click Upload and enter/select the certificate downloaded in Step 5 from Cisco FireSIGHT Configuration .
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter the IP address of the FireSIGHT console in the **IP/Host Name** field.
 - b. Select the name of the credential created in [Define Cisco FireSIGHT console and FirePower Threat Defense Credential in FortiSIEM](#) from the **Credentials** drop-down list.
 - c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity**. FortiSIEM will start collecting events from the FIRE SIGHT console.

Using Cisco eStreamer Client

Cisco has published a free eStreamer client to pull events from FireAMP server. This client is more up-to-date than FortiSIEM's own eStreamer client.

If you decide to use Cisco's eStreamer client instead of FortiSIEM's eStreamer client, follow these steps.

- [Step 1: Install a New Version of Python with a New User 'estreamer'](#)
- [Step 2: Download and Configure eStreamer Client](#)
- [Step 3: Start eStreamer Client](#)

Step 1: Install a New Version of Python with a New User 'estreamer'

This is required because the python version used by FortiSIEM is compiled with PyUnicodeUCS2, while eStreamer client requires the standard version of python built with PyUnicodeUCS4.

1. Log in to FortiSIEM Collector or the node where eStreamer client is going to be installed.
2. Install openssl-devel and openssl-devel.i686 by running the following command.
`yum install openssl-devel openssl-devel.i686`
3. Create eStreamer user using the following command.
 - a. `useradd estreamer`
4. Download the python library using the following commands.
 - a. `su estreamer`
 - b. `mkdir ~/python`
 - c. `cd ~/python`
 - d. `wget https://www.python.org/ftp/python/3.9.0/Python-3.9.0.tgz`
5. Install python library by using the following commands.
 - a. `tar xzfv Python-3.9.0.tgz`
 - b. `find ~/python -type d | xargs chmod 0755`
 - c. `cd Python-3.9.0`
 - d. `./configure --prefix=$HOME/python --enable-unicode=ucs4`
 - e. `make && make install`
 - f. Add the following two lines to `~/ .bashrc`.
`export PATH=$HOME/python/Python-3.9.0/:$PATH`
`export PYTHONPATH=$HOME/python/Python-3.9.0`
 - g. `source ~/.bashrc`

Step 2: Download and Configure eStreamer Client

1. SSH to FortiSIEM Collector or the node where eStreamer client is going to be installed as estreamer user.
2. Git clone: [git://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight.git](https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight.git)
3. Change directory using the following command.
`cd fp-05-firepower-cef-connector-arcsight`

4. Login to eStreamer server and take the following steps.
 - a. Go to **System > Integration > eStreamer**.
 - b. Create a **New client** and enter the **IP address** of the Supervisor/Collector as the host.
 - c. Download the pkcs12 file and save it to directory.
fp-05-firepower-cef-connector-arcsight
 5. Go back to fp-05-firepower-cef-connector-arcsight directory.
 6. Run `sh encore.sh`, and type 2 for selection of output in CEF as prompted. An `estreamer.conf` file is generated.
 7. Edit `estreamer.conf` with the below settings (in JSON format).
 - `handler.outputters.stream.uri : "udp://VA_IP:514"`
 - `servers.host : eStreamer_Server_IP`
 - `servers.pkcs12Filepath : /path/to/pkcs12`
 8. Run the following two commands.
 - `openssl pkcs12 -in "client.pkcs12" -nocerts -nodes -out "/path/to/fp-05-firepower-cef-connector-arcsight/{eStreamer_Server_IP}-{port}_pkcs.key"`
 - `openssl pkcs12 -in "client.pkcs12" -clcerts -nokeys -out "/path/to/fp-05-firepower-cef-connector-arcsight/{eStreamer_Server_IP}-{port}_pkcs.cert"`
- Notes:**
1. 8302 is the default port.
 2. The public IP of the device must be used to create `client.pkcs12` according to Cisco FireSIGHT Configuration documentation. The command `curl ifconfig.co` can be used to get the public IP of the device.

Step 3: Start eStreamer Client

SSH to FortiSIEM Collector or the node where eStreamer client is installed, as eStreamer user. Start eStreamer client by entering:

```
sh encore.sh start
```

Now eStreamer client is ready for use. FortiSIEM 5.2.5 contains an updated parser for the events generated by Cisco eStreamer client. Trigger a few events in eStreamer server and query from FortiSIEM to verify if everything is working.

Cisco Intrusion Prevention System

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample XML-Formatted Alert](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			Performance and Availability Monitoring
SDEE		Alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco ips" in the **Search...** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "cisco ips" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "cisco ips" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

1. Log in to the device manager for your Cisco IPS.
2. Go to **Configuration > Allowed Hosts/Networks**.

3. Click **Add**.
4. Enter the IP address of your FortiSIEM virtual appliance to add it to the access control list, and then click **OK**.
5. Go to **Configuration > Sensor Management > SNMP > General Configuration**.
6. For **Read-Only Community String**, enter `public`.
7. For **Sensor Contact** and **Sensor Location**, enter **Unknown**.
8. For **Sensor Agent Port**, enter **161**.
9. For **Sensor Agent Protocol**, select **udp**.

If you must create an SDEE account for FortiSIEM to use, go to **Configuration > Users** and **Add** a new administrator.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco IPS
Access Protocol	Cisco SDEE
Pull Interval	5 minutes
Port	443
Password config	See Password Configuration

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Sample XML-Formatted Alert

```
<\!-\ CISCO IPS \--><evAlert eventId="1203541079317487802" severity="low"> <originator>
  <hostId>MainFW-IPS</hostId> <appName>sensorApp</appName> <appInstanceId>376</appInstanceId>
</originator> <time offset="0" timeZone="UTC">1204938398491122000</time> <signature
  sigName="ICMP Network Sweep w/Echo" sigId="2100" subSigId="0" version="S2"></signature>
<interfaceGroup>vs1</interfaceGroup><vlan>0</vlan> <participants> <attack> <attacker> <addr
  locality="OUT">2.2.2.1</addr> </attacker> <victim> <addr locality="OUT">171.64.10.225</addr>
<os idSource="unknown" type="unknown" relevance="relevant"></os> </victim> <victim> <addr
  locality="OUT">171.66.255.87</addr> <os idSource="unknown" type="unknown"
  relevance="relevant"></os> </victim> <victim> <addr locality="OUT">171.66.255.86</addr> <os
  idSource="unknown" type="unknown" relevance="relevant"></os> </victim> <victim> <addr
  locality="OUT">171.66.255.84</addr> <os idSource="unknown" type="unknown"
  relevance="relevant"></os> </victim> <victim> <addr locality="OUT">171.66.255.85</addr> <os
  idSource="unknown" type="unknown" relevance="relevant"></os> </victim> <victim> <addr
  locality="OUT">171.66.255.82</addr> <os idSource="unknown" type="unknown"
  relevance="relevant"></os> </victim> </attack> </participants>
<alertDetails>InterfaceAttributes: context="single_vf" physical="Unknown"
backplane="GigabitEthernet0/1" </alertDetails></evAlert>
```

Cisco Stealthwatch

- [Integration Points](#)
- [Event Types](#)
- [Configuring FortiSIEM](#)

Integration Points

Protocol	Information Discovered	Used For
syslog	Network Anomaly Detection Alerts	Security and Compliance

Event Types

Currently over 150 events are parsed. See event types in **RESOURCES > Event Types**, and search for "Cisco-StealthWatch-" in the main content panel **Search...** field. The user can extend the parser to add other events.

Configuring FortiSIEM

FortiSIEM automatically recognizes Cisco Stealthwatch syslog as long as it follows the format as shown in the sample syslog:

```
<129>Jun 18 14:56:00 ED2ALENTSVRSMC-1 StealthWatch[2699]: LancopelStealthWatch|PRIORITY  
A|time=2018-06-18T14:55:30Z|target_hostname=|alarm_severity_id=5|alarm_type_  
id=60|alarm_type_description=Host may be infected with an SMB
```

Claroty Continuous Threat Detection (CTD) Platform

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Claroty Alert, Baseline and Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "ClarotyCTD" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 20 event types defined.

Rules

There are no specific rules available for Claroty.

Reports

There are no specific reports available for Claroty. You can view all Claroty events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "ClarotyCTD".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<12>Sep 12 15:31:33 localhost.localdomain
CEF:0|Claroty|CTD|2.7.0|Baseline|None|Unapproved|cs1Label=Site cs1=Site cs2Label=Network
cs2=Default cs3Label=Transmission cs3=TCP / 44818 cs4Label=SiteId cs4=1 cs5Label=SrcZone
cs5=Engineering Station: Acme cs6Label=DstZone cs6=PLC: Acme cs7Label=Category cs7=Protocol
cs8Label=CategoryAccess cs8=Read cs9Label=Frequency cs9=NotTimed cs10Label=FirstSeen cs10=Sep 12
```

```
2018 15:31:29 src=10.1.30.40 smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d
dhost=N/A externalId=2365 cat=Create rt=Sep 12 2018 15:31:29 msg=CIP : Service Get Attribute All
called on ExtendedDevice
```

```
<12>Sep 12 15:18:03 localhost.localdomain CEF:0|Claroty|CTD|2.7.0|Alert|Configuration
Download|Critical|cs1Label=Site cs1=Site cs2Label=Network cs2=Default cs3Label=ResolvedAs
cs3=Unresolved cs4Label=SiteId cs4=1 cs5Label=SrcZone cs5=Engineering Station: Acme
cs6Label=DstZone cs6=PLC: Acme cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8=https://10.210.16.2:5000/alert/74-1 src=10.1.30.40 smac=00:50:56:b9:e2:ad shost=N/A
dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d dhost=N/A externalId=74 cat=Create rt=Sep 12 2018 15:18:01
msg=A configuration has been downloaded to controller Chemical_plant by 10.1.30.40
```

Corero Smartwall Threat Defense System

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Security Alerts and Events	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Corero-smart" to see the event types associated with this device. In FortiSIEM 6.2.0, there are approximately 3,452 event types defined.

Rules

There are no specific rules available for Corero.

Reports

There are no specific reports available for Corero. You can view all Corero events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Corero-smart".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Please refer to the Corero documentation for information on configuring the device at the following link.

https://www.juniper.net/documentation/en_US/corero-smartwall9.5.0/information-products/topic-collections/Corero_SmartWall_CMS_UG/Content/cms_connect_swa.htm

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Corero SmartWall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sample Syslog

```
<165>2020-09-22T18:07:28.905+02:00 10.11.12.13
cat=network,type=sflow,v=1,cl=default,device=Defense_10_12_12_
102,profile=default,sc=175,sfn=16,dir=inbound,time=1600790847976000,mp=xe-
1/1,issr=1999,isr=1,px=32,lb=0,ipv=4,dip=1.2.3.4,dprt=61205,iplen=1143,prot=6,tos=0,sip=1.2.3.5,sp
rt=443,ttl=126,bp=0,ep=0,icn=5,scl=0,fp=0,flags=24,flags-
decode=PSH:ACK,plen=1161,ptag=37,pdu=0896ad670b22204e71624fc68100002508004500047762f400007e06f701d
83ad724b9b9757201bbef15d173297cf6bf83c7501810dec0ad00004b10a65f2b244bb73879b0f4346428273ce3582fe59
501013ea113a6bbdc535832cbf1ea85d95ecd7ab906eae299b27f16ee3d74b7fe3d981e33971dad0e03d68f90c03fbfabb
d4fb63d081701603f5893e42ef3311b0d4936e9abd39621f62608de62b4466947feeaf3ca9aca54ba8fb8121dd3b5dfa5a
3adf0ca8c92bb3cf4398b15edb508901db78409a09e3c
```


Cylance Protect Endpoint Protection

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		End point malware alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cylance" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via **CEF formatted syslog** sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cylance Protect
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
CylancePROTECT: Event Type: AppControl, Event Name: pechange, Device Name: WIN-7entSh64, IP  
Address: (192.168.119.128), Action: PEFileChange, Action Type: Deny, File Path:  
C:\Users\admin\AppData\Local\Temp\MyInstaller.exe, SHA256:  
04D4DC02D96673ECA9050FE7201044FDB380E3CFE0D727E93DB35A709B45EDAA
```

Cyphort Cortex Endpoint Protection

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		End point malware alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cyphort" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via **CEF formatted syslog** sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cylance Cortex
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<134>Feb 23 21:58:05 tap54.eng.cyphort.com cyphort: CEF:0|Cyphort|Cortex|3.2.1.16|http|TROJAN_GIPPERS.DC|8|externalId=374 eventId=13348 lastActivityTime=2015-02-24 05:58:05.151123+00 src=172.16.0.1 dst=10.1.1.26 fileHash=acf69d292d2928c5ddfe5e6af562cd482e6812dc fileName=79ea1163c0844a2d2b6884a31fc32cc4.bin fileType=PE32 executable (GUI) Intel 80386, for MS Windows startTime=2015-02-24 05:58:05.151123+00
```


Damballa Failsafe

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, and click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	A name for the device.
Device Type	Damballa Failsafe
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Damballa Failsafe.
5. To see the jobs associated with Damballa, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Damballa" in the search box.

Darktrace CyberIntelligence Platform

Darktrace provides proactive cyber resilience with real-time detection and autonomous response to known and novel threats. FortiSIEM can ingest Darktrace logs via syslog or webhook. The following topics are covered:

- [Information Collected](#)
- [Darktrace CyberIntelligence Syslog based Integration](#)
- [Darktrace CyberIntelligence Webhooks based Integration](#)
- [Sample Event Logs](#)

Information Collected

The following log types are collected

Darktrace Event Category	Event Type Prefix for FortiSIEM Events	Collection Method
Activity, Informational, and Security	DarkTrace (19 event types) Exclude "-DCIP"	Webhook
Informational and Security	DarkTrace-DCIP (101 event types)	Syslog
Security	DarkTrace-Anomalous (5 event types)	
Informational	DarkTrace-Container (1 event type)	
Activity and Security	DarkTrace-IaaS (8 event types)	
Security	DarkTrace-SaaS (1 event type)	
Security	DarkTrace-Unusual (4 event types)	
Informational and Security	DarkTrace-DCIP-Anomalous (24 event types)	
Security	DarkTrace-DCIP-Antigena (8 event types)	
Informational and Security	DarkTrace-DCIP-Compliance (19 event types)	
Security	DarkTrace-DCIP-Compromise (10 event types)	
Security	DarkTrace-DCIP-Connections (1 event type)	
Security	DarkTrace-DCIP-Device (13 event types)	
Security	DarkTrace-DCIP-Drop (2 event types)	

Darktrace Event Category	Event Type Prefix for FortiSIEM Events	Collection Method
Informational	DarkTrace-DCIP-Enforce (2 event types)	
Security	DarkTrace-DCIP-Multiple (2 event types)	
Security	DarkTrace-DCIP-Possible (1 event type)	
Informational and Security	DarkTrace-DCIP-System (3 event types)	
Security	DarkTrace-DCIP-Unusual (13 event types)	
Security	DarkTrace-DCIP-User (3 event types)	

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Darktrace CyberIntelligence Syslog based Integration

Configure Darktrace to send CEF formatted logs to FortiSIEM. FortiSIEM will automatically parse the logs. No configuration is required in FortiSIEM.

Darktrace CyberIntelligence Webhooks based Integration

In this method, Darktrace CyberIntelligence Platform push logs to FortiSIEM via **Webhooks**. This option is required for the Darktrace SaaS portal where syslog is not an option over the public internet.

Three steps are involved.

1. Configure a FortiSIEM Webhook Credential.
2. Configure Darktrace to forward logs to a FortiSIEM public webhook URL endpoint generated in Step 1.
3. Confirm Logs appear in FortiSIEM.

Prerequisite

Most applications using webhook push notifications do server TLS certificate validation, which means the target collector must be configured with a public CA signed TLS certificate. See [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#) for configuration information.

Step 1: Configure a FortiSIEM Webhook Credential

Define the Webhook end point as follows. Darktrace will send logs to the endpoint defined in this step.

1. Go to the **Admin > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential, such as darktrace.
Device Type	DarkTrace Darktrace Cyber Intel Platform Note: If "DarkTrace" does not appear, you can select "Generic".
Access Protocol	Webhook
Separator	\n
Receiver FQDN	Enter the IP or FQDN of the FortiSIEM collector Darktrace has network reachability to, and can resolve and send webhooks on TCP 443 to that destination. (Used to help build the target URL the sender will send webhooks to) Example: fsm-collector01.example.com  This node needs to have a valid public CA signed TLS certificate. Self-signed certificate is not recommended.
Reporting Host Name	darktrace.com Note: This is just used to provide some detail about the sending device in the resulting log headers. The raw event field [reptDevName]=<this field> is set. It can be anything, but sometimes is hard coded.
Endpoint	This is dynamically generated, based on the Receiver FQDN and Credential Name you input. It is the URL Darktrace will point to for webhook sending. E.g. https://fsm-collector01.example.com/webhook/darktrace
Auth Type	Basic Auth
UserName	Enter a username such as fsm_webhook_user
Password/Confirm Password	Enter a strong password. Note: Save this password in your management utility as it is required when setting up Darktrace.
Description (Optional)	Description of the device.

- c. The endpoint will be set as `http://<ReceiverFQDN>/webhook/<Name>`. Save the endpoint URL for your Darktrace configuration.
- d. Click **Save and Deploy**. This will deploy the webhook endpoint to all FortiSIEM nodes.

Step 2 - Darktrace Configuration

Enable Integration for Devices/Subnets

1. Login to Darktrace Threat Visualizer.
2. Navigate to **Modules**.
3. Select **HTTPS**.
4. Click **Workflow Integrations**.
5. Enable the integration and select the devices or subnets you want to monitor.

Configure HTTP/HTTPS Alerts

1. In the **Configuration for HTTP/HTTPS Alerts** section, click **New** to create a new alert configuration.
2. Toggle **Send Alerts** to enabled.
3. In the **URL** field, paste the Webhook URL from the FortiSIEM webhook configuration (`https://<yoursiemfqdn>/webhook/darktrace`).
Note: The FortiSIEM webhook is dynamic and follows the following format: `https://<yoursiemfqdn>/webhook/<FortiSIEM_credential_name>`.
4. Toggle **Show Advanced Options** to expand authentication settings.
5. Set **Authentication** to **Basic**.
6. Enter the same user/password you defined when setting up the FortiSIEM Darktrace webhook on FortiSIEM.
7. Click **Verify alert settings** to test the connection.
8. Save your configuration.

Step 3 - Confirm Logs appear in FortiSIEM

1. Login to FortiSIEM GUI.
2. Navigate to **Analytics**.
3. Run the following query:
Event Type CONTAIN Darktrace-
Note: To perform a specific query for a given log type simply change Darktrace- to Darktrace-<Log type> e.g. Darktrace-Unusual for logs related to unusual activities.
4. Confirm that Darktrace logs appear.

Sample Event Logs

Syslog CEF Event Log

```
CEF:0|Darktrace|DCIP|3.0.8|537|Antigena/Network/Compliance/Antigena RDP Block|Low| eventId=2
externalId=1462565 art=1536856095244 deviceSeverity=1 rt=1536856054000
shost=personalpcd698.abccompany.local src=10.10.1.85 sourceZoneURI=/All Zones/ArcSight
System/Private Address Space Zones/RFC1918: 192.0.2.0-10.255.255.255 smac=1:1:1:1:1:1 dst=1.1.1.1
destinationZoneURI=/All Zones/ArcSight System/Public Address Space Zones/APNIC/1.0.0.0-1.1.1.255
(APNIC) dpt=9999 ahost=personalpc123.abccompany.local agt=10.10.28.38 agentZoneURI=/All
Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.0.2.0-10.255.255.255 av=2.2.2.2.0
```

```
atz=CountryA aid=3mAvC02UBABCAa72iNm4jZA\=\= at=syslog dvc=10.10.10.10 deviceZoneURI=/All
Zones/ArcSight System/Private Address Space Zones/RFC1918: 192.0.2.0-10.255.255.255 dtz=CountryA _
cefVer=0.1 ad.darktraceUrl=https://192.0.2.10/#modelbreach/1462565
```

Webhook Parsed Event Log

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=DarkTrace,[reptModel]=DarkTrace SaaS Platform,
[reptDevName]=example1.cloud.darktrace.com,[reptDevIpAddr]=192.0.2.25,[json]={
  "model":{
    "name":"Anomalous Connection::Unusual Incoming Data
    Volume","pid":500858,"phid":501963,"uuid":"abcd1234-12ab-1111-2222-123412341234","logic":{"data":
    [503757],"type":"componentList","version":1},"throttle":3600,"sharedEndpoints":true,"actions":
    {"alert":true,"antigena":
    {},"breach":true,"model":true,"setPriority":false,"setTag":false,"setType":false,"aianalyst":
    {"hypotheses":["InternalTransferSummary"]},"tags":["AP: Internal Recon","AP: Lateral
    Movement"],"interval":0,"delay":0,"sequenced":false,"active":true,"readOnly":true,"modified":"202
    5-08-11 16:06:26","activeTimes":{"devices":{}},"tags":
    {},"type":"exclusions","version":2},"autoUpdatable":true,"autoUpdate":true,"autoSuppress":true,"de
    scription":"A device is transferring an abnormally large volume of data internally Action: Use the
    breach log and device event log to investigate where the data is being sent to / from and whether
    it could contain sensitive information.","behaviour":"decreasing","defeats":[{"arguments":
    {"value":"artifactory-shared-services"},"comparator":"matches","defeatID":1,"filtertype":"Internal
    destination device name"},[{"defeatID":2,"filtertype":"Internal source device
    name","comparator":"matches regular expression","arguments":{"value":"^sample-.*$"}},
    {"defeatID":"2-1","filtertype":"Internal destination device
    name","comparator":"matches","arguments":{"value":"example-test-web-alb"}}]],"created":
    {},"edited":{},"version":11,"mitre":{"tactics":["collection"],"techniques":
    ["T1074"]},"priority":2,"category":"Informational","compliance":false},"device":
    {"did":"1000000067386","objecttype":"device","ip":"192.0.2.25 [aws:vpc-
    01234567890abcdef]","sid":"100002000100","vlan":-
    1014,"firstSeen":1735834258000,"lastSeen":1755170291000,"typename":"server","typelabel":"Server",
    "tags":[{"tid":28,"thid":108403,"name":"Cloud::AWS","restricted":true,"data":
    {"color":36,"description":"This device is linked to one or more Darktrace cloud
    assets"},"isReferenced":true},{tid":36,"thid":108277,"name":"Network Flow
    Analysis","restricted":false,"data":{"color":100,"description":"For devices monitored with Network
    Flow Analysis"},"isReferenced":true},{tid":42,"thid":108223,"name":"Re-Activated
    Device","restricted":false,"data":{"auto":false,"color":142,"description":"A device that has been
    inactive for at least 4 weeks has re-appeared on the network in the past 48
    hours."},"visibility":"Public"},"isReferenced":true,"expiry":1755343411000}}],"triggeredComponent
    s":
    [{"time":1755170230000,"cbid":389478,"cid":503757,"chid":2000004212,"size":1,"threshold":0,"interv
    al":3600,"logic":{"data":{"left":"A","operator":"AND","right":"B"},"version":"v0.1"},"metric":
    {"mlid":236,"name":"dtmodelbreach","label":"Model"},"triggeredFilters":
    [{"cfid":156499,"id":"A","filterType":"Message","arguments":{"value":"Unusual Incoming Data Volume
    Indicator"},"comparatorType":"contains","trigger":{"value":"Device / Anomaly Indicators / Unusual
    Incoming Data Volume Indicator"}},{cfid":156500,"id":"B","filterType":"Age of
    source","arguments":{"value":604800},"comparatorType":">","trigger":{"value":"19335972"}},
    {"cfid":156501,"id":"d1","filterType":"Destination port","arguments":
    {},"comparatorType":"display","trigger":{"value":"14000"}},
    {"cfid":156502,"id":"d2","filterType":"Application protocol","arguments":
    {},"comparatorType":"display","trigger":{"value":""}}],
```

```
{
  "cfid": 156503,
  "id": "d3",
  "filterType": "Destination IP",
  "arguments": {
    "comparatorType": "display",
    "trigger": {
      "value": "10.6.0.170"
    }
  },
  "cfid": 156504,
  "id": "d4",
  "filterType": "Internal destination device name",
  "arguments": {
    "comparatorType": "display",
    "trigger": {
      "value": ""
    }
  }
}],
"sourceIP": "192.0.2.251 [aws::vpc-01234567890abcdef]",
"percentScore": 57,
"breachUrl": "https://euw2-782-02.cloud.darktrace.com/#modelbreach/1000000322185",
"pbid": "1000000322185",
"score": 0.567,
"commentCount": 0,
"creationTime": 1755170615000,
"time": 1755170231000,
"mitreTechniques": [
  {
    "tactics": ["collection"],
    "technique": "Data Staged",
    "techniqueID": "T1074"
  }
]
```

Dragos Platform

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Dragos Alert logs regarding Modeling, Indicator, Configuration, Threat Behavior	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "dragos" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 5 event types defined.

Rules

There are no specific rules available for Dragos.

Reports

There are no specific reports available for Dragos. You can view all Dragos events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".

4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Dragos".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<13>1 2020-07-02T14:58:31.538019Z dragos dragos_syslog - - system="Dragos Platform"
createdAt="2020-07-02T14:58:31Z" summary="Test Message from Dragos App" severity="{severity}"
content="This test message was created by the Dragos Syslog App" asset_ip="{asset_ip}" asset_
hostname="Test" dst_asset_ip="10.0.0.9" dst_asset_hostname="Test" dst_asset_
mac="83:77:DB:E3:A3:38" dst_asset_domain="ip-10-10-255-1.ec2.test" src_asset_ip="10.0.0.9" src_
asset_hostname="Test" src_asset_mac="89:3A:EE:01:0F:D3" src_asset_domain="ip-10-10-test.ec2.test"
id="1234567" asset_domain="ip-10-10-255-1.ec2.test" asset_id="111111" asset_
mac="06:92:1C:1B:F2:72" detection_quad="Modeling" detectorId="test-detector-1111" dst_asset_
id="333333" matchedRuleId="16" occurredAt="2020-07-02T14:58:31Z" originalSeverity="0"
reviewed="False" src_asset_id="222222" type="Test"
```

```
<8>May 06 21:06:19 dragos dragos_syslog: CEF:0|Dragos|Platform|1.6|notification|Test Message from
Dragos App|5|content=This test message was created by the Dragos Syslog App asset_ip=10.0.0.9
asset_hostname=Test dst_asset_ip=10.0.0.9 dst_asset_hostname=Test dst_asset_mac=9C:B6:TE:ST:4B:95
dst_asset_domain=ip-10-10-255-1.ec2.test src_asset_ip=10.0.0.9 src_asset_hostname=Test src_asset_
mac=TE:ST:D0:F2:4B:95 src_asset_domain=ip-10-10-test.ec2.test id=1234567 asset_domain=ip-10-10-
255-1.ec2.test asset_id=111111 asset_mac=9C:B6:D0:F2:TE:ST createdAt=2020-05-06T21:06:24Z
detection_quad=Indicator detectorId=test-detector-4444 dst_asset_id=333333 matchedRuleId=16
occurredAt=2020-05-06T21:06:24Z originalSeverity=5 reviewed=False src_asset_id=222222 type=Test
```


FireEye Malware Protection System (MPS)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "fireeye" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	FireEye MPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<164>fenotify-45640.alert: CEF:0|FireEye|MPS|6.0.0.62528|MC|malware-callback|9|rt=Apr 16 2012
15:54:41 src=192.168.26.142 spt=0 smac=00:14:f1:90:c8:01 dst=2.2.2.2 dpt=80 dmac=00:10:db:ff:50:00
cn1Label=vlan cn1=202 cn2Label=sid cn2=33335390 cs1Label=sname cs1=Trojan.Gen.MFC cs4Label=link
cs4=https://10.10.10.10/event_stream/events_for_bot?ev_id\=45640 cs5Label=ccName cs5=3.3.3.3
cn3Label=ccPort cn3=80 proto=tcp cs6Label=ccChannel cs6= shost=abc.org <http://abc.org>
dvchost=ALAXFEYE01 dvc=10.10.10.10 externalId=45640
```

FortiDDoS

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog	Host Name, Access IP, Vendor/Model	Over 150 event types to include Protocol Anomaly, Traffic Volume Anomaly, DoS Attacks,	Security Monitoring

Event Types

In **Admin > Device Support > Event Types**, search for "FortiDDoS" to see the event types associated with this device.

Rules

There are many IPS correlation rules for this device under **Resources > Rules > Security > Exploits**.

Reports

There are many reports for this device under **Resources > Reports > Function > Security**.

Configuration

Syslog

FortiSIEM processes FortiDDoS events via syslog. Configure FortiDDoS to send syslog to FortiSIEM as directed in the device's product documentation by taking the following steps:

FortiDDoS Documentation References:

- [Event Log Remote Logging Configuration](#)

- [Attack Log Remote Logging Configuration](#)

Event Log Remote Logging Configuration

To configure remote log settings for event logs, take the following steps.

1. Navigate to **Log & Report > Log Configuration > Event Log Remote**.
2. Click **Add**.
3. Complete the configuration using the following table. Make sure **RFC 5424** is disabled.

Settings	Guidelines
Status	Enable or disable this configuration. Note 1: You must enable to configure via GUI or CLI. After configuration, you can disable, if needed and the configuration will be maintained. Note 2: if disabled, the configuration still counts towards the maximum three allowed.
Address	IP address of FortiSIEM.
Port	Listening port number of FortiSIEM. Usually this is UDP port 514.
Log Level	Select the severity to log from the following choices. Levels below the selected level will not be sent: • Emergency—The system has become unstable. • Alert—Immediate action is required. • Critical—Functionality is affected. • Error—An error condition exists and functionality could be affected. • Warning—Functionality might be affected. • Notification—Information about normal events. • Information—General information about system operations. • Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior.
Format	• Default – Standard syslog format for most syslog servers, modified by the various format options seen in the table below. • CSV - Send logs in CSV format. This format is not supported by most servers. • CEF – Send logs in Common Event Format (UDP, un-encrypted version)
Facility	Identifier that is not used by FortiDDoS but might be useful for the syslog server.
Event Logging	Select to enable event logging.
Event Category	Select the Event Categories that you want included in the event syslogs. Note: All Event Categories are disabled by default. It is safe to enable all.

4. Save the configuration.

Attack Log Remote Logging Configuration

To configure remote log settings for Attack Log Remote, take the following steps:

1. Navigate to **Log & Report > Log Configuration > Attack Log Remote**.
2. Click **Add**.
3. Complete the configuration using the following table. Make sure **RFC 5424** is disabled.

Settings	Guidelines																																															
Name	Configuration name.																																															
Status	Select to enable sending DDoS attack logs to a remote server.																																															
Global ACL	Select to send Global ACL attack logs to the remote server. If this option is enabled, the SPP field is hidden. Configure up to 2 remote servers.																																															
SPP	Select an SPP whose logs are sent to the remote server. Configure up to 2 remote servers for each SPP																																															
Formats	<table><tr><th rowspan="2">SyslogFormat</th><th colspan="5">Options</th></tr><tr><th>FortiAnalyzer</th><th>Encrypt to FortiAnalyzer</th><th>UDP / TCP</th><th>RFC 5424</th><th>Transparent / Octet</th></tr><tr><td>Standard UDP FortiAnalyzer</td><td>Enabled</td><td>Disabled</td><td></td><td></td><td></td></tr><tr><td>UDP FAZ OFTP</td><td>Enabled</td><td>Enabled</td><td></td><td></td><td></td></tr><tr><td>UDP RFC 3164</td><td>Disabled</td><td></td><td>UDP</td><td>Disabled</td><td></td></tr><tr><td>UDP RFC 5424</td><td>Disabled</td><td></td><td>UDP</td><td>Enabled</td><td></td></tr><tr><td>TCP RFC 6587</td><td>Disabled</td><td></td><td>TCP</td><td></td><td>User / Server choice</td></tr><tr><td>CEF (un-encrypted)</td><td>Disabled</td><td></td><td>UDP/TCP</td><td></td><td></td></tr></table>	SyslogFormat	Options					FortiAnalyzer	Encrypt to FortiAnalyzer	UDP / TCP	RFC 5424	Transparent / Octet	Standard UDP FortiAnalyzer	Enabled	Disabled				UDP FAZ OFTP	Enabled	Enabled				UDP RFC 3164	Disabled		UDP	Disabled		UDP RFC 5424	Disabled		UDP	Enabled		TCP RFC 6587	Disabled		TCP		User / Server choice	CEF (un-encrypted)	Disabled		UDP/TCP		
SyslogFormat	Options																																															
	FortiAnalyzer	Encrypt to FortiAnalyzer	UDP / TCP	RFC 5424	Transparent / Octet																																											
Standard UDP FortiAnalyzer	Enabled	Disabled																																														
UDP FAZ OFTP	Enabled	Enabled																																														
UDP RFC 3164	Disabled		UDP	Disabled																																												
UDP RFC 5424	Disabled		UDP	Enabled																																												
TCP RFC 6587	Disabled		TCP		User / Server choice																																											
CEF (un-encrypted)	Disabled		UDP/TCP																																													
Address	IP address of FortiSIEM.																																															
Port	Listening port number of FortiSIEM. Usually this is UDP port 514.																																															

4. Save the configuration.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiDDos
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
Jan 10 16:01:50 172.30.84.114 devid=FI400B3913000032 date=2015-01-23 time=17:42:00
type=attack SPP=1 evecode=1 evesubcode=8 dir=0 protocol=1 sip=0.0.0.0 dip=0.0.0.0
dropCount=312
devid=FI800B3913000055 date=2017-01-27 time=18:24:00 tz=PST type=attack spp=0 evecode=2
```

```
evesubcode=61 description="Excessive Concurrent Connections Per Source flood" dir=1  
sip=24.0.0.2 dip=24.255.0.253 subnet_name=default dropcount=40249 facility=Local0  
level=Notice
```

Fortinet FortiDeceptor

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Authentication logs, Decoy activity	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiDeceptor" to see the event types associated with this device.

Rules

No specific rules are written for FortiDeceptor.

Reports

No specific reports are written for FortiDeceptor.

Configuration

Configure FortiDeceptor system to send logs to FortiSIEM in the supported format (see [Sample Events](#)).

Refer to the latest FortiDeceptor Administration Guide for the latest configuration steps. Instructions here have been taken from the [3.3.1 FortiDeceptor Administration Guide](#).

To configure syslog in FortiDeceptor, take the following steps:

1. From FortiDeceptor, navigate to **Log > Log Servers**.
2. Click **Create New** and enter the following information into the configuration.

Field	Input
Name	FortiSIEM
Server Type	syslog
Server Address	Input the IP address or FQDN of your FortiSIEM collector.
Port	Leave as default (UDP 514)
Status	Enabled
Log Level	Information

3. If applicable, click **OK**.

Settings for Access Credentials

None required.

Sample Events

```
<27>2019-07-29T10:12:44 devhost=FDC-VM0000000262 devid=FDC-VM0000000262 logver=25 tzone=14400 tz=GST
date=2019-07-29
time=10:12:44 logid=0106000001 type=event subtype=system level=error user=system ui=GUI
action=update status=failure
msg="The authentication to FDN server failed"
```

```
<14>2019-07-29T10:40:34 devhost=FDC-VM0000000262 devid=FDC-VM0000000262 logver=25 tzone=14400 tz=GST
date=2019-07-29
time=10:40:34 logid=0106000001 type=event subtype=system level=information user=admin ui=GUI
action=Login
status=success msg="Administrator admin logged into website successfully from 10.0.0.254"
```


Fortinet FortiSandbox

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP	Host Name, OS, version, Hardware	CPU, Memory, Disk, Interface utilization	Performance Monitoring
HTTP(S)	Host Name, OS, version, Hardware		Log Management, Security Compliance, SIEM
Syslog	Threat feed - Malware URL, Malware Hash	Malware found/cleaned, Botnet, Malware URL, System Events	Log Management, Security Compliance, SIEM

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortisandbox-" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortisandbox" in the main content panel **Search...** field to see the rules associated with this device.

Also, basic availability rules in **RESOURCES > Rules > Availability > Network** and performance rules in **RESOURCES > Rules > Performance > Network** also trigger.

Reports

In **RESOURCES > Reports**, search for "fortisandbox" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

For FortiSandbox log server documentation, see

<https://docs.fortinet.com/document/fortisandbox/4.0.0/administration-guide/323679/log-servers>.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog format should be the same as that shown in the [example](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiSandbox
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
Oct 12 14:35:12 172.16.69.142 devname=turnoff-2016-10-11-18-46-05-172.16.69.142 device_
id=FSA3KE3A13000011 logid=0103000001 type=event subtype=system pri=debug user=system
ui=system action= status=success reason=none letype=9 msg="Malware package: urlrel version
2.88897 successfully released, total 1000"
<14>2016-08-19T06:48:51 devhost=turnoff-2016-08-15-19-24-55-172.16.69.55
devid=FSA35D0000000006 tzone=-25200 tz=PDT date=2016-08-19 time=06:48:51 logid=0103000001
type=event subtype=system level=information user=admin ui=GUI action=update status=success
reason=none letype=9 msg="Remote log server was successfully added"
```

Fortinet FortiTester

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Syslog (CEF formatted)	Host name and Device Type from LOG	Over 14 log types	Security and Compliance

Event Types

Go to **ADMIN > Device Support > Event Types**, and search for "FortiTester" to see the event types associated with this device.

Rules

None

Reports

None

Configuration

Configure FortiTester to send CEF formatted syslog to FortiSIEM. No configuration is required on FortiSIEM.

Sample Events

```
CEF:0|Fortinet|FortiTester|3.8|Event|information|category=System deviceExternalId=FTS2KET618000005  
msg=The system is started deviceCustomDate1=2019-11-05-15:12:30 cs1= cs1Label=Description
```

IBM Internet Security Series Proventia

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample SNMP Trap](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected
SNMP Traps		

Event Types

In **ADMIN > Device Support > Event Types**, search for "proventia" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP Trap](#)
- [Define FortiSIEM as a Response Object for SNMP Traps](#)
- [Define a Response Rule to Forward SNMP Traps to FortiSIEM](#)
- [Refining Rules for Specific IP Addresses](#)

SNMP Trap

FortiSIEM receives SNMP traps from IBM/ISS Proventia IPS appliances that are sent by IBM/ISS SiteProtector Management Console. You must first configure IBM/ISS Proventia to send alerts to IBM/ISS SiteProtector, then

configure IBM/ISS SiteProtector to send those alerts as SNMP traps to FortiSIEM.

Configure IBM/ISS Proventia Appliances to Send SNMP Notifications to IBM/ISS SiteProtector Management Console

1. Log in to the IBM Proventia IPS web interface.
2. Click **Manage System Settings > SiteProtector Management**.
3. Click and select **Register with SiteProtector**.
4. Click and select **Local Settings Override SiteProtector Group Settings**.
5. Specify the **Group**, **Heartbeat Interval**, and **Logging Level**.
6. Configure these settings:

Setting	Description
Authentication Level	Use the default first-time trust .
Agent Manager Name	Enter the Agent Manager name exactly as it appears in SiteProtector. This setting is case-sensitive.
Agent Manager Address	Enter the Agent Manager's IP address.
Agent Manager Port	Use the default value 3995 .
User Name	If the appliance has to log into an account access the Agent Manager, enter the user name for that account here.
User Password	Click Set Password, enter and confirm the password, and then click OK .
Use Proxy Settings	If the appliance has to go through a proxy to access the Agent Manager, select the Use Proxy Settings option, and then enter the Proxy Server Address and Proxy Server Port .

Define FortiSIEM as a Response Object for SNMP Traps

1. Log in to IBM SiteProtector console.
2. Go to **Grouping > Site Management > Central Responses > Edit settings**.
3. Select **Response Objects > SNMP**.
4. Click **Add**.
5. Enter a **Name** for your FortiSIEM virtual appliance.
6. For **Manager**, enter the IP address of your virtual appliance.
7. For **Community**, enter `public`.
8. Click **OK**.

Define a Response Rule to Forward SNMP Traps to FortiSIEM

1. Go to **Response Rules**.
2. Click **Add**.
3. Select **Enabled**.
4. Enter a **Name** and **Comment** for the response rule.
5. In the **Responses** tab, select **SNMP**.
6. Select **Enabled** for the response object that represents your FortiSIEM virtual appliance.
7. Click **OK**.

Refining Rules for Specific IP Addresses

By default, a rule matches on any source or destination IP addresses.

1. To refine the rule to match on a specific source IP address, select the rule, click **Edit**, and then select the **Source** tab.
2. Select **Use specific source addresses** to restrict the rule based on IP address of the source.
If you set this option, set the **Mode** to specify that the rule should either be **From** or **Not From** the IP address.
3. Click **Add** to define one or more IP addresses.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	IBM ISS Proventia
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sample SNMP Trap

```
2013-02-07 16:52:18 100.0.0.218(via UDP: [192.168.64.218]:55545) TRAP, SNMP v1, community
public SNMPv2-SMI::enterprises.2499 Enterprise Specific Trap (4) Uptime: 0:00:00.15 SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1 = STRING: "SiteProtector_Central_Response (Response1)"
SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.2 = STRING: "16:52:18 2013-02-07" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.3 = STRING: "6" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.4 = STRING: "100.0.0.216" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.5 = STRING: "100.0.0.218" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.6 = "" SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.7 = ""
```

```
SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.8 = STRING: "48879" SNMPv2-  
SMI::enterprises.2499.1.1.2.1.1.1.1.9 = STRING: "80" SNMPv2-  
SMI::enterprises.2499.1.1.2.1.1.1.1.10 = STRING: "DISPLAY=WithoutRaw:0,BLOCK=Default:0" SNMPv2-  
SMI::enterprises.2499.1.1.2.1.1.1.1.11 = STRING: " SensorName: IBM-IPS ObjectName: 80  
DestinationAddress: 100.0.0.218 AlertName: HTTP_OracleAdmin_Web_Interface AlertTarget:  
100.0.0.218 AlertCount: 1 VulnStatus: Simulated block (blocking not enabled) AlertDateTime:  
16:52:17 2013-02-07 ObjectType: Target Port SourceAddress: 100.0.0.216 SensorAddress:  
192.0.2.15"
```

Indegy Security Platform

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog (CEF formatted)	Host name and Device Type from LOG	Over 14 types of security logs	Security and Compliance

Event Types

Go to **ADMIN > Device Support > Event Types** and search for “Indegy-”.

Rules

None

Reports

None

Configuration

Configure Indegy Security Platform to send syslog in the supported format to FortiSIEM. No configuration is required in FortiSIEM.

Sample Events

```
<12>Nov 17 09:04:06 10.100.20.40 CEF:0|Indegy|Indegy Security Platform|3.0.33|109|Unauthorized Conversation|7|dvchost=indegy rt=Nov 17 2019 09:04:06 duser=AS_01,Comm. Adapter #2 suser=Eng. Station #9 proto=UDP externalId=125 dst=10.100.102.150 src=10.100.20.34 dpt=47808 cs6Label=policy_name cs6=Use of Unauthorized Protocols in Siemens Controllers cat=NetworkEvents
```


Juniper DDoS Secure

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		DDoS Alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "juniper-ddos" to see the event types associated with this device.

- Juniper-DDoS-Secure-WorstOffender
- Juniper-DDoS-Secure-Blacklisted
- Juniper-DDoS-Secure-Generic

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure the device to send syslog to FortiSIEM. Make sure that the event matches the format specified below.

```
<134>Juniper: End : 117.217.141.32 : IND: Worst Offender: Last Defended 66.145.37.254: TCP Attack  
- Port Scan (Peak 55/s, Occurred 554)  
<134>Juniper: End : 78.143.172.52 : IRL: IP Address Temp Black-Listed (Valid IP) Exceeds SYN + RST  
+ F2D Count (Peak 114/s, Dropped 83.5K pkts)
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Juniper DDos Secure
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Juniper Networks IDP Series

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Example Syslog from NSM](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "juniper_idp" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Example Syslog from NSM

```
<25>Oct 11 14:29:27 10.146.68.68 20101011, 58420089, 2010/10/11 18:29:25, 2010/10/11 18:33:12,
global.IDP, 1631, par-real-idp200, 10.146.68.73, traffic, udp port scan in progress, (NULL),
(NULL), 161.178.223.221, 0, 0.0.0.0, 0, (NULL), (NULL), 10.248.8.110, 0, 0.0.0.0, 0, udp,
global.IDP, 1631, Metro IDP IP / Port Scan Policy, traffic anomalies, 2, accepted, info, yes,
'interface=eth3', (NULL), (NULL), (NULL), 0, 0, 0, 0, 0, 0, 0, 0, no, 25, Not
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Juniper Netscreen IDP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

McAfee Network Security Platform (formerly known as McAfee IntruShield)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Settings for Access Credentials](#)
- [Configuration](#)
- [Sample Parsed Syslog Message](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	McAfee Intrushield
Access Protocol	See Access Credentials

Setting	Value
Port	See Access Credentials
Password config	See Password Configuration

Configuration

Syslog

FortiSIEM handles custom syslog messages from McAfee Intrushield.

1. Log in to McAfee Intrushield Manager.
2. Create a customer syslog format with these fields:
 - AttackName
 - AttackTime
 - AttackSeverity
 - SourceIp
 - SourcePort
 - DestinationIp
 - DestinationPort
 - AlertId
 - AlertType
 - AttackId
 - AttackSignature
 - AttackConfidence
 - AdminDomain
 - SensorName:ASDCDCIPS01
 - Interface
 - Category
 - SubCategory
 - Direction
 - ResultStatus
 - DetectionMechanism
 - ApplicationProtocol
 - NetworkProtocol
 - Relevance
3. Set the message format as a sequence of Attribute:Value pairs as in this example.

```
AttackName:$IV_ATTACK_NAME$,AttackTime:$IV_ATTACK_TIME$,AttackSeverity:.$IV_ATTACK_
SEVERITY$,SourceIp:$IV_SOURCE_IP$,SourcePort:$IV_SOURCE_PORT$,
DestinationIp:$IV_DESTINATION_IP$,DestinationPort:$IV_DESTINATION_PORT$,AlertId:$IV_ALERT_
ID$,AlertType:$IV_ALERT_TYPE$,AttackId:$IV_ATTACK_ID$,
AttackSignature:$IV_ATTACK_SIGNATURE$,AttackConfidence:$IV_ATTACK_CONFIDENCE$,AdminDomain:$IV_
ADMIN_DOMAIN$,SensorName:$IV_SENSOR_NAME$,
```

```
Interface:$IV_INTERFACE$,Category:$IV_CATEGORY$,SubCategory:$IV_SUB_CATEGORY$,Direction:$IV_
DIRECTION$,ResultStatus:$IV_RESULT_STATUS$,
DetectionMechanism:$IV_DETECTION_MECHANISM$,ApplicationProtocol:$IV_APPLICATION_
PROTOCOL$,NetworkProtocol:$IV_NETWORK_PROTOCOL$,Relevance:$IV_RELEVANCE$
```

4. Set FortiSIEM as the syslog recipient.

Sample Parsed Syslog Message

```
Mar 24 16:23:18 SyslogAlertForwarder: AttackName:Invalid Packets detected,AttackTime:2009-03-24
16:23:17 EDT,AttackSeverity:Low,SourceIp:127.255.106.236,
```

```
SourcePort:N/A,DestinationIp:192.0.2.252,DestinationPort:N/A,AlertId:5260607647261334188,AlertType
:Signature,AttackId:
```

```
0x00009300,AttackSignature:N/A,
AttackConfidence:N/A,AdminDomain:ASC,SensorName:ASDCDCIPS01,Interface:1A-
1B,Category:Exploit,SubCategory:protocol-violation,Direction:Outbound,
ResultStatus:May be
successful,DetectionMechanism:signature,ApplicationProtocol:N/A,NetworkProtocol:
```

```
N/A,Relevance:N/A,HostIsolationEndTime:N/A
```

McAfee Stonesoft IPS

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Example Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Network IPS alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "stonesoft" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via **CEF formatted syslog** sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	McAfee Stonesoft IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<6>CEF:0|McAfee|IPS|5.4.3|70018|Connection_Allowed|0|spt=123 deviceExternalId=STP-NY-F0001 node 1  
dmac=84:B2:61:DC:E1:31 dst=169.132.200.3 cat=System Situations app=NTP (UDP) rt=Apr 08 2016  
00:26:13 deviceFacility=Inspection act=Allow deviceOutboundInterface=Interface #5  
deviceInboundInterface=Interface #4 proto=17 dpt=123 src=10.64.9.3 dvc=12.17.2.17  
dvchost=12.17.2.17 smac=78:DA:6E:0D:FF:C0 cs1Label=RuleId cs1=2097152.6
```

Motorola AirDefense

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Wireless IDS logs	Security Monitoring

Event Types

About 33 event types covering various Wireless attack scenarios. In **ADMIN > Device Support > Event Types**, search for "Motorola-AirDefense" in the **Search...** field to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure the device to send logs to FortiSIEM. Make sure that the format is as follows.

```
Nov  8 18:48:00 Time=2014-10-29T05:39:00,Category=Rogue
Activity,CriticalityLevel=Severe,Desc=Rogue AP on Wired Network,device=00:22:cf:5d:ee:60
(00:22:cf:5d:ee:60),sensor=fc:0a:81:12:7b:4b(COMP-SENS302EA[a,b,g,n])
Nov 12 13:33:00 Time=2015-11-12T08:47:00,Category=Exploits,CriticalityLevel=Critical,Desc=NAV
Attack - CTS,device=5c:0e:8b:cb:d5:40(5c:0e:8b:cb:d5:40),sensor=fc:0a:81:12:77:3f(COMP-SENS201EA
[a,b,g,n])
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Motorola AirDefense
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Nozomi Central Management Control

Support Added: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: Nozomi Networks

Product: Nozomi Networks Central Management Control (CMC)

Product Information: <https://www.nozominetworks.com/products/overview/>

- [Configuring FortiSIEM for Nozomi](#)

Protocol	Information discovered	Metrics collected	Used for
Syslog	Device type	Node detection, protocol information, network changes	Security and Compliance

Configuring FortiSIEM for Nozomi

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Nozomi Networks CMC
Access Protocol	Nozomi REST API
User Name	Enter the username used to access your Nozomi server.
Password	Enter the password associated with your username.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your Nozomi credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the Nozomi server.
5. Navigate to **ADMIN > Setup > Discovery**.
6. Click **New** to create a Nozomi scan discovery definition.
7. In the **Discovery Definition** dialog box, take the following steps:
 - a. In the **Name** field, enter a name for the Discovery Definition.
 - b. From the **Discovery Type** drop-down list, select **Nozomi Scan**.
 - c. In the **Credential** drop-down list, your Nozomi Access Method Definition should be automatically selected.
 - d. Fill in the other fields as necessary.
 - e. When done, click **Save**.
8. Click **Discover**.
Assets from your Nozomi server will be discovered.

Devices under Nozomi can be discovered via FortiSIEM Device Discovery by selecting Nozomi Scan as Discovery Type. See [Discovering Devices](#) for more information.

Palo Alto Networks Cortex XDR

Support Added: FortiSIEM 6.3.0

Last Modification: FortiSIEM 7.0.0

Vendor: Palo Alto Networks

Product Information: <https://www.paloaltonetworks.com/cortex/cortex-xdr>

- [Cortex XDR Configuration](#)
- [FortiSIEM Configuration](#)

Cortex XDR Configuration

Follow these steps to send Cortex XDR logs to FortiSIEM.

- [Integrate a Syslog Receiver](#)
- [Configure Notification Forwarding](#)

Integrate a Syslog Receiver

Take the following steps to integrate FortiSIEM as a syslog receiver.

Reference: <https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Integrate-a-syslog-receiver>

1. Navigate to **Settings > Configurations > Integrations > External Applications**.
2. In **Syslog Servers**, click **+ New Server**.
3. Configure the following parameters:

Parameter	Description
Name	Enter a name as the identifier, such as "FortiSIEM_Public_Collector".
Destination	Enter the Public IP or FQDN of FortiSIEM Collector.
Port	Enter the port number for sending syslog messages.
Facility	Select one of the syslog standard values. The value maps to how your syslog server uses the facility field to manage messages. Typically Informational, or Default Value.
Protocol	Select the method of communication with FortiSIEM. You can select TCP , UDP , or TCP + SSL .
Certificate	Select if you wish to use TLS for communication between Cortex XDR and FortiSIEM. Note: This will require further configuration via FortiSIEM - See Additional Configuration for Syslog over TLS .

4. Test the parameters, then click **Create**.

Note: Up to five syslog receivers can be defined. Upon success, the table displays the syslog servers and their status.

Configure Notification Forwarding

After integrating FortiSIEM as a syslog server, configuration of notification forwarding is required. Take the following steps.

Reference: <https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Configure-notification-forwarding>

1. Navigate to **Settings > Configurations > General > Notifications**.
2. Click **+ Add Forwarding Configuration**.

3. In the **Name** field, enter a name for the configuration.
4. In the **Description** field, enter a description about the forwarding configuration.
5. Select the log type to forward to FortiSIEM.
 - **Alerts:** Send notifications for specific alert types, such as XDR Agent.
Example: To configure Health alerts, select **Log Type = Alerts** and filter the Alerts table by **Alert Domain = Health**.
 - **Agent Audit Logs:** Send notifications for audit logs reported by your Cortex XDR agents.
 - **Management Audit Logs:** Send notifications for audit logs about events related to your Cortex XDR tenant.
6. Click **Next**.
7. Under **Scope**, use the filter to pass the information you want.
Example: Filter set to Severity = Medium, Alert Source = XDR Agent will send alerts or events matching this filter as a notification.
8. Click **Next**.
9. (Optional) Configure any email requirements.
 - a. In **Distribution List**, enter the email address(es) for notification.
 - b. In **Grouping Timeframe**, define the time frame frequency, in minutes, for notifications. Every 20 alerts or 20 events aggregated within this time frame are sent together in one notification, sorted according to the severity. To send a notification when one alert or event is generated, set the time frame to 0.
 - c. Choose whether you want Cortex XDR to provide an auto-generated subject.
 - d. If you previously used log forwarding and want to continue forwarding logs in the same format, select **Use Legacy Log Format**.
10. Select the syslog receiver for FortiSIEM.
11. Click **Done**.

FortiSIEM Configuration

No special configuration is needed as received syslog is automatically parsed and ingested.

Additional Configuration for Syslog over TLS

If you decide to send Cortex XDR syslog over TLS to FortiSIEM, then follow these steps to generate a certificate (either Public or Self-Signed).

Prerequisites



- Ensure you have a collector that is publicly exposed (has a public IP with port TCP 6514 open).
- Be sure to specify a valid FQDN when registering the collector, and make sure a public DNS A record exists for it.
- Add an allowlist to restrict all traffic only from these destinations based on your region listed in the documentation [here](#).

-
- [Using Public Certificates](#)
 - [Using Self-Signed Certificates](#)

Using Public Certificates

- [FortiSIEM Configuration](#)
- [Cortex XDR Configuration](#)

FortiSIEM Configuration

Take the following steps:

1. Generate a SSL/TLS certificate using a public certificate. A public certificate can be signed by a public certificate authority (CA) such as DigiCert, or GoDaddy.
2. Run the following command on your collector to generate a CSR (Certificate Signing Request)


```
cd /tmp
openssl req -new -newkey rsa:4096 -nodes -keyout /etc/pki/tls/private/tls-collector1.key -
out tls-collector1.csr
```
3. Take the following actions when prompted.
 - a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
 - b. Enter your State or Province. For example, California would be "CA".
 - c. Enter your Locality. For example, a city would be "Sunnyvale".
 - d. Enter your desired org name. For example, "Fortinet".
 - e. Enter Unit Name, which is optional. For example, "IT".
 - f. Enter Common Name. It must match the FQDN of collector. For example, "collector1.myorg.fortinet.com".
 - g. Email Address. This can be left blank. Hit "enter" to continue.
 - h. If prompted for a challenge password, hit "enter" to leave blank and continue.
 - i. Hit enter again to confirm.

A Certificate Signing Request is created in /tmp/tls-collector1.csr.
4. Using WinScp or another SCP utility, download this CSR file to your desktop.
5. Go to your preferred public CA, and upload this CSR when prompted to generate a new SSL certificate file. When you have your new Certificate ZIP file, it will normally contain 2-3 files.
6. WinSCP zip file to /tmp of the Collector.
7. Unzip the file if needed, by using the following command.


```
unzip <filename>.zip
```

The .crt file is your certificate, and is usually a concatenation of all chain certificates.
8. Rename the cert files if needed using similar commands here.


```
cd /tmp
mv 11111111.crt tls-collector1.crt
```
9. Copy the cert to the correct folder using the following command.


```
cp tls-collector1.crt /etc/pki/tls/certs/tls-collector1.crt
```
10. Set permissions using the following command.


```
chmod 644 /etc/pki/tls/certs/tls-collector1.crt
chmod 640 /etc/pki/tls/private/tls-collector1.key
chown root:admin /etc/pki/tls/private/tls-collector1.key
```

11. On the Collector, update the `/opt/phoenix/config/phoenix_config.txt` file to reference the new tls cert using the following command.
`vi /opt/phoenix/config/phoenix_config.txt`
12. Locate the following lines in your `phoenix_config.txt` file.
`listen_tls_port_list=6514`
`tls_certificate_file=/etc/pki/tls/certs/localhost.crt`
`tls_key_file=/etc/pki/tls/private/localhost.key`
and replace the cert and key file with the following:
`listen_tls_port_list=6514`
`tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt`
`tls_key_file=/etc/pki/tls/private/tls-collector1.key`
13. Save the file, and as root, restart phParser using the following command.
`killall -9 phParser`

Cortex XDR Configuration

1. Define the Syslog server parameters (See [Integrate a Syslog Receiver](#) for more information).
 - Name: FortiSIEM_Public_Collector
 - Destination: Public IP or FQDN of FortiSIEM Collector
 - Port: 6514
 - Facility: Informational, or Default Value
 - Protocol: TCP + SSL/TLS
 - Certificate: You do not need to upload as it is a public signed SSL certificate.
2. Click **Create**.

Using Self-Signed Certificates

- [FortiSIEM Configuration](#)
- [Cortex XDR Configuration](#)

FortiSIEM Configuration

Take the following steps:

1. On the Collector, run the following commands as root.
`cd /tmp`
`openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 -keyout /etc/pki/tls/private/tls-collector1.key -out /etc/pki/tls/certs/tls-collector1.crt`
2. Take the following actions when prompted.
 - a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
 - b. Enter your State or Province. For example, California would be "CA".
 - c. Enter your Locality. For example, a city would be "Sunnyvale".
 - d. Enter your desired org name. For example, "Fortinet".
 - e. Enter Unit Name, which is optional. For example, "IT".

- f. Enter Common Name. It must match the FQDN of collector. For example,
"collector1.myorg.fortinet.com".
 - g. Email Address. This can be left blank. Hit "enter" to continue.
 - h. If prompted for a challenge password, hit "enter" to leave blank and continue.
 - i. Hit enter again to confirm.
3. Set the appropriate permissions for the private key and certificate generated, by running the following commands.

```
chmod 640 /etc/pki/tls/private/tls-collector1.key  
chown root:admin /etc/pki/tls/private/tls-collector1.key  
chmod 644 /etc/pki/tls/certs/tls-collector1.crt
```
4. On the collector, update the /opt/phoenix/config/phoenix_config.txt file to reference the new TLS certificate by editing the file, running the following command.

```
vi /opt/phoenix/config/phoenix_config.txt
```
5. Find the following lines in the file.

```
listen_tls_port_list=6514  
tls_certificate_file=/etc/pki/tls/certs/localhost.crt  
tls_key_file=/etc/pki/tls/private/localhost.key
```

and replace the cert and key file with the following:

```
listen_tls_port_list=6514  
tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt  
tls_key_file=/etc/pki/tls/private/tls-collector1.key
```
6. Save the file, and as root, restart phParser using the following command.

```
killall -9 phParser
```
7. Make a copy of the certificate file to /tmp, and using WinSCP or another SCP utility, download the Collector Certificate file. For example, you may run the following command.

```
cp /etc/pki/tls/certs/tls-collector1.crt /tmp
```
8. Download /tmp/tls-collector1.crt to your desktop.

Note: You only need the Certificate file and not the private key. The private key will never leave the collector.

Cortex XDR Configuration

1. Define the Syslog server parameters (See [Integrate a Syslog Receiver](#) for more information).
 - Name: FortiSIEM_Public_Collector
 - Destination: Public IP or FQDN of FortiSIEM Collector
 - Port: 6514
 - Facility: Informational, or Default Value
 - Protocol: TCP + SSL/TLS
 - Certificate: Upload the self-signed SSL certificate.
 - Select Ignore Certificate Error.
2. Click **Create**.

Radware DefensePro

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog		Over 120 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, Search for “Radware-DefensePro” in the main content panel **Search...** field to see the event types associated with this device.

Sample Event Type:

```
<132>DefensePro: 13-09-2017 15:03:21 WARNING 12572 Intrusions "SIP-Scanner-SIPVicious" UDP 1.1.1.1
29992 1.1.1.2 5060 15 Regular "GSN_Web" occur 1 3 N/A 0 N/A high drop FFFFFFFF-FFFF-FFFF-9C94-
000F57F7595F
```

```
<132>DefensePro: 13-09-2017 15:18:45 WARNING 150 HttpFlood "HTTP Page Flood Attack" TCP 1.1.1.3 0
1.1.1.4 80 0 Regular "President-1.1.1.4" ongoing 100 0 N/A 0 N/A medium forward FFFFFFFF-FFFF-
FFFF-9CCF-000F57F7595F
```

```
<132>DefensePro: 13-09-2017 14:37:53 WARNING 200000 SynFlood "SYN Flood HTTP" TCP 0.0.0.0 0
1.1.1.5 80 0 Regular "GSN_Web" ongoing 1 0 N/A 0 N/A medium challenge FFFFFFFF-FFFF-FFFF-9C46-
000F57F7595F
```

```
<134>DefensePro: 13-09-2017 13:56:34 INFO Configuration Auditing manage syslog destinations create
172.16.10.207 -f "Local Use 0", ACTION: Create by user public via SNMP source IP 1.1.1.6
```

Rules

There are no specific rules but generic rules for Network IPS and Generic Servers apply.

Reports

There are no specific reports but generic rules for Network IPS and Generic Servers apply.

Configuration

Configure Radware DefensePro Security Manager to send syslog on port 514 to FortiSIEM.

Snort Intrusion Prevention System

- What is Discovered and Monitored
- Event Types
- Configuration
- JDBC
- SNMP Access to the Database Server
- Debugging Snort Database Connectivity
- Examples of Snort IPS Events Pulled over JDBC
- Viewing Snort Packet Payloads in Reports
- Exporting Snort IPS Packets as a PCAP File
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			
JDBC	Generic information: signature ID, signature name, sensor ID, event occur time, signature priority TCP: packet header, including source IP address, destination IP address, Source Port, Destination Port, TCP Sequence Number, TCP Ack Number, TCP Offset, TCP Reserved, TCP Flags, TCP Window size, TCP Checksum, tTCP Urgent Pointer; and packet payload UDP: packet header, including source IP address, destination IP address, Source Port, Destination Port, UDP Length, checksum; and packet payload ICMP: packet header, including source IP address, destination IP address, ICMP Type, ICMP Code, Checksum, ICMP ID, Sequence Number; and packet payload		
SNMP (for access to the database server hosting the Snort database)			

Event Types

In **ADMIN > Device Support > Event Types**, search for "snort-org" to see the event types associated with this device.

Configuration

Syslog

Collecting event information from Snort via syslog has two drawbacks:

1. It is not reliable because it is sent over UDP.
2. Information content is limited because of UDP packet size limit.

For these reasons, you should consider using JDBC to collect event information from Snort.

These instructions illustrate how to configure Snort on Linux to send syslog to FortiSIEM. For further information, you should consult the [Snort product documentation](#).

1. Log in to your Linux server where Snort is installed.
2. Navigate to and open the file `/etc/snort/snort.conf`.
3. Modify `alert_syslog` to use a local log facility, for example:

```
output alert_syslog: LOG_LOCAL4 LOG_ALERT
```

4. Navigate to and open the file `/etc/syslog.conf`.
5. Add a redirector to send syslog to FortiSIEM.

```
#Snort log to local4
#local4.*
```

```
/var/log/snort.log
#local4.*@192.168.20.41
local4.alert@10.1.2.171
```

6. Restart the Snort daemon.

Example Parsed Snort Syslog

```
<161>snort[2242]: [1:206:9] BACKDOOR DeepThroat 3.1 CD ROM Open Client Request [Classification:
Misc activity] [Priority: 3]: {UDP} 192.168.19.1:6555 -> 172.16.2.5:514
<161>snort[5774]: [1:1560:6] WEB-MISC /doc/ access [Classification: access to a potentially
vulnerable web application] [Priority: 2]: {TCP} 192.168.20.53:41218 -> 192.168.0.26:80
<161>snort[5774]: [1:466:4] ICMP L3retriever Ping [Classification: Attempted Information Leak]
[Priority: 2]: {ICMP} 192.168.20.49 -> 192.168.0.10
<161>snort[5774]: [1:1417:9] SNMP request udp [Classification: Attempted Information Leak]
[Priority: 2]: {UDP} 192.168.20.40:1061 -> 192.168.20.2:161
```

JDBC

Supported Databases and Snort Database Schemas

When using JDBC to collect IPS information from Snort, FortiSIEM can capture a full packet that is detailed enough to recreate the packet via a PCAP file.

FortiSIEM supports collecting Snort event information over JDBC these database types:

- Oracle
- MS SQL
- MySql
- PostgreSQL

FortiSIEM supports Snort database schema 107 or higher.

SNMP Access to the Database Server

You must set up an SNMP access credential for the server that hosts the Snort database. See the topics under [Database Server Configuration](#) for information on setting up SNMP for communication with FortiSIEM for several common types of database servers.

Once you have set up SNMP on your database server, you can now configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Debugging Snort Database Connectivity

Snort IPS alert are pulled over JDBC by a Java agent, which has to join multiple database tables to create the events. An internal log file is created for each pull.

```
2012-08-07T10:02:27.576777+08:00 AO-foo java:[PH_JAVA_AGENT_INFO]:[eventSeverity]=PHL_INFO,
[procName]=phAgentManager,[fileName]=AgentSnort,[phLogDetail]=10.1.20.51:ICMP:Max record
id:17848444 Total records in one round of pulling:20
```

At most 1000 database records (IPS Alerts) are pulled at a time. If FortiSIEM finds more than 1000 new records, then it begins to fall behind and this log is created.

```
2012-08-07T10:02:27.576777+08:00 AO-foo java:[PH_JAVA_AGENT_INFO]:[eventSeverity]=PHL_INFO,
[procName]=phAgentManager,[fileName]=AgentSnort,[phLogDetail]=Event count of snort exceeds the
threshold in one round of pulling, which means there may be more events need to be pulled.
```

Examples of Snort IPS Events Pulled over JDBC

- [UDP Event](#)
- [TCP Event](#)

UDP Event

```
<134>Feb 25 14:27:56 10.1.2.36 java: [Snort-1417]:[eventSeverity]=PHL_INFO,
[relayDevIpAddr]=10.1.2.36,[ipsSensorId]=1,[snortEventId]=10343430,[sensorHostname]=10.1.2.36,
[signatureId]=1417,[eventName]=SNMP request udp,[eventSeverity]=2,[eventTime]=2012-11-07
17:56:51.0,[srcIpAddr]=10.1.2.245,[destIpAddr]=10.1.2.36,[ipVersion]=4,[ipHeaderLength]=5,[tos]=0,
[ipTotalLength]=75,[ipId]=0,[ipFlags]=0,[ipFragOffset]=0,[ipTtl]=64,[ipProto]=17,
[ipChecksum]=8584,[srcIpPort]=35876,[destIpPort]=161,[udpLen]=55,[checksum]=39621,
[dataPayload]=302D02010104067075626C6963A520...
```

TCP Event

```
<134>Aug 08 09:30:59 10.1.20.51
java: [Snort-1000001]:[eventSeverity]=PHL_INFO,[hostIpAddr]=10.1.20.51,[sensorId]=1,
[eventId]=17897184,[signatureId]=1000001,[signatureName]=Snort
Alert [1:1000001:0],[signaturePri]=null,[eventTime]=2012-08-08
09:26:24.0,[srcIpAddr]=10.1.2.99,[destIpAddr]=10.1.20.51,[srcIpPort]=52314,[destIpPort]=80,
[seqNum]=967675661,[tcpAckNum]=3996354107,[tcpOffset]=5,[tcpReserved]=0,[tcpFlags]=24,
[tcpWin]=16695,[checksum]=57367,[tcpUrgentPointer]=0,
[dataPayload]=474554202F66617669636F6E2E69636F204...
```

Viewing Snort Packet Payloads in Reports

FortiSIEM creates an event for each IPS alert in Snort database. You can view the full payload packet associated with a Snort event when you run a report.

1. Set up a structured historical search.
2. Set these conditions, where **Reporting IP** is an IP belonging to the Snort Application group.

Attribute	Operator	Value
Reporting IP	IN	Applications: Network IPS App

3. For **Display Fields**, include **Data Payload**.
When you run the query, Data Payload will be one of the display columns.
4. When the query runs, select an event, and the data payload will display at the bottom of the search results in a byte-by-byte ethereal/wireshark format.

Exporting Snort IPS Packets as a PCAP File

After running a report, click the **Export** button and choose the PCAP option.

Settings for Access Credentials

- [Access Credentials for JDBC](#)
- [Access Credentials for SNMP, Telnet, SSH](#)

Access Credentials for JDBC

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your Snort IPS over JDBC.

Setting	Value
Name	<database type>-snort-BT
Device Type	Select the type of database that you are connecting to for Snort alerts
Access Protocol	JDBC
Used For	Snort Audit
Pull Interval (minutes)	1
Port	3306
Database Name	The name of the database
User Name	The administrative user for the Snort database
Password	The password associated with the administrative user

Access Credentials for SNMP, Telnet, SSH

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP, Telnet, or SSH.

Setting	Value
Name	<set name>
Device Type	Snort-org Snort IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sourcefire 3D and Defense Center

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "sourcefire" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [Syslog](#)
- [Sample Syslog from SourceFire3D IPS](#)
- [Sample Syslog from SourceFire Defense Center](#)

Syslog

FortiSIEM handles SourceFire alerts via syslog either from IPS appliances themselves or from Defense Center. Events are classified as Snort event types.

Simply configure SourceFire appliances or Defense Center to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Sample Syslog from SourceFire3D IPS

```
<188>Jul  4 15:07:01 Sourcefire3D Snort: [119:15:1] http_inspect: OVERSIZE REQUEST-URI DIRECTORY
[Impact: Unknown] From DetectionEngine_IPS_DMZ2/SourcefireIPS at Thu Jul  4 15:07:01 2013 UTC
[Classification: Potentially Bad Traffic] [Priority: 2] {tcp} 10.20.1.12:57689->1.1.1.1:80
```

Sample Syslog from SourceFire Defense Center

```
<46>Jul 17 16:01:54 DefenseCenter SFAppliance: [1:7070:14] "POLICY-OTHER script tag in URI -
likely cross-site scripting attempt" [Impact: Potentially Vulnerable] From "10.134.96.172" at Wed
Jul 17 16:01:52 2013 UTC [Classification: Web Application Attack] [Priority: 1] {tcp}
1.2.3.4:60537->2.3.4.5:80
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Sourcefire Sourcefire3D IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Trend Micro Deep Discovery

- [Integration Points](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Malicious file detection	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Trend-DeepDiscoveryAnalyzer" and "Trend-DeepDiscoveryInspector" to see the event types associated with this device.

Rules

No specific rules are written for Trend Deep Discovery Analyzer and Trend Deep Discovery Inspector, but regular end point rules apply.

Reports

No specific reports are written for Trend Deep Discovery Analyzer and Trend Deep Discovery Inspector, but regular end point reports apply.

Configuration

Configure the Trend Deep Discovery system to send logs to FortiSIEM in the supported format (see [Sample Events](#)).

Settings for Access Credentials

None required.

Sample Events

```
<123>CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1175|20|Malware URL requested - Type 1|6|
dvc=10.0.1.50 dvcmac=00:0C:29:A6:53:0C dvchost=ddi38-143
deviceExternalId=6B593E17AFB7-40FBBB28-A4CE-0462-A536 rt=Mar 09 2015 11:58:25 GMT+08:00
app=HTTP deviceDirection=1 dhost=www.example.com dst=10.10.11.99 dpt=80
dmac=00:1b:21:35:8b:98 shost=10.1.1.97 src=10.1.1.197 spt=12121 smac=fe:ed:be:ef:5a:c6
cs3Label=HostName_Ext cs3=www.example.com fname=setting.doc fileType=0 fsize=0 act=not blocked
cn3Label=Threat Type cn3=1 destinationTranslatedAddress=10.1.1.2
sourceTranslatedAddress=10.1.1.197 cnt=1 cs5Label=CCCA_DetectionSource
cs5=GLOBAL_INTELLIGENCE cn1Label=CCCA_Detection cn1=1 cat=Callback cs6Label=pAttackPhase
cs6=Command and Control Communication
```

Zeek (Bro) Installed on Security Onion

See [Zeek Network Security Monitor \(Previously known as Bro\)](#) for the latest information.

Bro/Zeek is an OpenSource network analysis product that is also installed as part of Security Onion.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog			Event Collection

Event Types

- Bro-dhcp /Regular Traffic/Permit - Traffic A DHCP conversation
- Bro-dns /Regular Traffic/Permit - Traffic DNS activity log
- Bro-conn /Regular Traffic/Permit - Traffic TCP/UDP/ICMP connections
- Bro-app_stats /Info - Statistics about APP
- Bro-radius /Info - RADIUS analysis activity
- Bro-known_devices /Info - Bro known devices

Rules

Generic Rules matching categories.

Reports

Generic Reports matching categories.

Configuration

Complete the following task on Onion Security, as this is crucial to get the headers working in the parser:

Add the following code in the `/etc/syslog-ng/syslog-ng.conf` file, but change `<IP>` to the IP of the FortiSIEM Super/Worker/Collector which will receive the syslog:

```
destination d_fortisiem { tcp("<IP>" port(514));};
log {
  source(s_bro_dns);
  source(s_bro_dhcp);
  log { filter(f_bro_headers); };
  log { destination(d_fortisiem);};
};
```

Sample Events

```
<13>Mar 25 11:02:24 sec-sensor-ps bro_dns: {"ts":"2019-03-
25T11:02:22.485187Z","uid":"CEBf4c2FoLEBtbPLn6","id.orig_h":"10.8.20.21","id.orig_
p":50837,"id.resp_h":"10.8.1.203","id.resp_p":53,"proto":"udp","trans_
id":25959,"rtt":0.000357,"query":"tsomething.my.example.com","qclass":1,"qclass_name":"C_
INTERNET","qtype":1,"qtype_name":"A","rcode":0,"rcode_
name":"NOERROR","AA":false,"TC":false,"RD":true,"RA":true,"Z":0,"answers":["um1.my.
example.com","um1-lo3.my. example.com","um1-lo3.lo3.r.my.
example.com","55.66.8.24","55.66.8.152","55.66.9.24"],"TTLs":
[136.0,5.0,146.0,5.0,5.0,5.0],"rejected":false}
```

Operational Technology

FortiSIEM supports these operational technology applications/devices for discovery and monitoring.

- [APC Netbotz Environmental Monitor](#)
- [APC UPS](#)
- [Claroty Continuous Threat Detection](#)
- [Dragos Platform](#)
- [Generic UPS](#)
- [Hirschmann SCADA Firewalls and Switches](#)
- [Liberty FPC](#)
- [Liberty HVAC](#)
- [Liberty UPS](#)
- [Microsoft Defender for IoT \(Was CyberX OT/IoT Security\)](#)
- [Nozomi Central Management Control \(CMC\)](#)
- [Nozomi SCADAguardian](#)
- [OTORIO RAM2 \(Risk Assessment, Monitoring and Management\)](#)
- [Siemens Simatic PLC](#)

APC Netbotz Environmental Monitor

- [What is Monitored and Collected](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Setting Access Credentials](#)

What is Monitored and Collected

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	Temperature: Sensor Id, Sensor label, Enclosure Id, Temperature Relative Humidity: Sensor Id, Sensor label, Enclosure Id, Relative Humidity Air Flow: Sensor Id, Sensor label, Enclosure Id, Air Flow Dew Point Temperature: Sensor Id, Sensor label, Enclosure Id, Dew Point Temperature Current: Sensor Id, Sensor label, Enclosure Id, Current Audio Sensor Reading: Sensor Id, Sensor label, Enclosure Id, Audio Sensor Reading Dry Contact Sensor Reading: Sensor Id, Sensor label, Enclosure Id, Dry Contact Sensor Reading Door Switch Sensor Reading: Sensor Id, Sensor label, Enclosure Id, Door Switch Sensor Reading (Open/Close) Camera Motion Sensor Reading: Sensor Id, Sensor label, Enclosure Id, Camera Motion Sensor Reading (Motion/No Motion) Hardware Status (for NBRK0200): Contact Status, Output Relay Status, Outlet Status, Alarm Device Status, Memory Sensor Status, Memory Output Status, Memory Outlet Status, memory Beacon Status EMS Status (for NBRK0200): EMS Hardware Status, Connection State Hardware Probe (for NBRK0200): Sensor Id, Temperature, Relative Humidity, Connection State Code Module Sensor (for NBRK0200): Sensor Name, Sensor location, Temperature, Relative Humidity, Connection State Code	Availability and Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
SNMP Trap (V1, V2c)	SNMP Trap	See Event Types for more information about viewing the SNMP traps collected by FortiSIEM for this device.	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "NetBotz" to see the event types associated with this application or device.

Event types for NetBotz NBRK0200

- PH_DEV_MON_HW_STATUS

```
[PH_DEV_MON_HW_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,
[lineNumber]=1642,[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[hwStatusCode]=2,
[hwProbeStatus]=2,[hwInputContactStatus]=2,[hwOutputRelayStatus]=0,[hwOutletStatus]=2,
[hwAlarmDeviceStatus]=0,[hwMemSensorStatus]=0,[hwMemOutputStatus]=2,[hwMemOutletStatus]=2,
[hwMemBeaconStatus]=2,[phLogDetail]=
```

- PH_DEV_MON_HW_EMS_STATUS

```
[PH_DEV_MON_HW_EMS_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,
[lineNumber]=1871,[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[reptDevName]=Unknown,
[emsHwStatus]=0,[phyMachConnectionStateCode]=2,[hwLogStatus]=1,[phLogDetail]=
```

- PH_DEV_MON_HW_PROBE

```
[PH_DEV_MON_HW_PROBE]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,[lineNumber]=2100,
[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[envSensorLabel]=Sensor MM:4,[envTempDegF]=74,
[envTempHighThreshDegF]=138,[envHumidityRel]=51,[envHumidityRelHighThresh]=90,
[envHumidityRelLowThresh]=10,[serialNumber]=L3,[phyMachConnectionStateCode]=3,
[maxTempThresh]=140,[minTempThresh]=32,[maxHumidityThresh]=99,[minHumidityThresh]=0,
[phLogDetail]=
```

- PH_DEV_MON_HW_MODULE_SENSOR

```
[PH_DEV_MON_HW_MODULE_SENSOR]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,
[lineNumber]=2567,[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[moduleNumber]=0,
[envSensorId]=1,[envSensorLabel]=Sensor MM:1,[envSensorLoc]=Orland Park Server,
[envTempDegF]=74,[envHumidityRel]=50,[phyMachConnectionStateCode]=1,[hwAlarmDevicetatus]=1,
[phLogDetail]=
```

Rules

In **RESOURCES > Rules**, search for "NetBotz" in the main content panel **Search...** field to see the rules associated with this application or device.

Reports

In **RESOURCES > Reports**, search for "NetBotz" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Setting Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	APC NetBotz
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

APC UPS

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Setting Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	UPS metrics: Remaining battery charge, Battery status, Replace battery indicator, Time on battery, Output status, Output load, Output voltage, Output frequency	Availability and Performance Monitoring
SNMP Trap			Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "apc" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "apc" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "apc" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Setting Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	APC UPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Claroity Continuous Threat Detection (CTD) Platform

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Claroty Alert, Baseline and Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "ClarotyCTD" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 20 event types defined.

Rules

There are no specific rules available for Claroty.

Reports

There are no specific reports available for Claroty. You can view all Claroty events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "ClarotyCTD".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<12>Sep 12 15:31:33 localhost.localdomain
CEF:0|Claroty|CTD|2.7.0|Baseline|None|Unapproved|cs1Label=Site cs1=Site cs2Label=Network
cs2=Default cs3Label=Transmission cs3=TCP / 44818 cs4Label=SiteId cs4=1 cs5Label=SrcZone
cs5=Engineering Station: Acme cs6Label=DstZone cs6=PLC: Acme cs7Label=Category cs7=Protocol
cs8Label=CategoryAccess cs8=Read cs9Label=Frequency cs9=NotTimed cs10Label=FirstSeen cs10=Sep 12
```

```
2018 15:31:29 src=10.1.30.40 smac=00:50:56:b9:e2:ad shost=N/A dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d
dhost=N/A externalId=2365 cat=Create rt=Sep 12 2018 15:31:29 msg=CIP : Service Get Attribute All
called on ExtendedDevice
```

```
<12>Sep 12 15:18:03 localhost.localdomain CEF:0|Claroty|CTD|2.7.0|Alert|Configuration
Download|Critical|cs1Label=Site cs1=Site cs2Label=Network cs2=Default cs3Label=ResolvedAs
cs3=Unresolved cs4Label=SiteId cs4=1 cs5Label=SrcZone cs5=Engineering Station: Acme
cs6Label=DstZone cs6=PLC: Acme cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8=https://10.210.16.2:5000/alert/74-1 src=10.1.30.40 smac=00:50:56:b9:e2:ad shost=N/A
dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d dhost=N/A externalId=74 cat=Create rt=Sep 12 2018 15:18:01
msg=A configuration has been downloaded to controller Chemical_plant by 10.1.30.40
```

Dragos Platform

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Syslog](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Dragos Alert logs regarding Modeling, Indicator, Configuration, Threat Behavior	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "dragos" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 5 event types defined.

Rules

There are no specific rules available for Dragos.

Reports

There are no specific reports available for Dragos. You can view all Dragos events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Dragos".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<13>1 2020-07-02T14:58:31.538019Z dragos dragos_syslog - - system="Dragos Platform"
createdAt="2020-07-02T14:58:31Z" summary="Test Message from Dragos App" severity="{severity}"
content="This test message was created by the Dragos Syslog App" asset_ip="{asset_ip}" asset_
hostname="Test" dst_asset_ip="10.0.0.9" dst_asset_hostname="Test" dst_asset_
mac="83:77:DB:E3:A3:38" dst_asset_domain="ip-10-10-255-1.ec2.test" src_asset_ip="10.0.0.9" src_
asset_hostname="Test" src_asset_mac="89:3A:EE:01:0F:D3" src_asset_domain="ip-10-10-test.ec2.test"
id="1234567" asset_domain="ip-10-10-255-1.ec2.test" asset_id="111111" asset_
mac="06:92:1C:1B:F2:72" detection_quad="Modeling" detectorId="test-detector-1111" dst_asset_
id="333333" matchedRuleId="16" occurredAt="2020-07-02T14:58:31Z" originalSeverity="0"
reviewed="False" src_asset_id="222222" type="Test"
```

```
<8>May 06 21:06:19 dragos dragos_syslog: CEF:0|Dragos|Platform|1.6|notification|Test Message from
Dragos App|5|content=This test message was created by the Dragos Syslog App asset_ip=10.0.0.9
asset_hostname=Test dst_asset_ip=10.0.0.9 dst_asset_hostname=Test dst_asset_mac=9C:B6:TE:ST:4B:95
dst_asset_domain=ip-10-10-255-1.ec2.test src_asset_ip=10.0.0.9 src_asset_hostname=Test src_asset_
mac=TE:ST:D0:F2:4B:95 src_asset_domain=ip-10-10-test.ec2.test id=1234567 asset_domain=ip-10-10-
255-1.ec2.test asset_id=111111 asset_mac=9C:B6:D0:F2:TE:ST createdAt=2020-05-06T21:06:24Z
detection_quad=Indicator detectorId=test-detector-4444 dst_asset_id=333333 matchedRuleId=16
occurredAt=2020-05-06T21:06:24Z originalSeverity=5 reviewed=False src_asset_id=222222 type=Test
```

Generic UPS

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Setting Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	UPS metrics: Remaining battery charge, Battery status, Time on battery, Estimated Seconds Remaining, Output voltage, Output current, Temperature	Availability and Performance Monitoring

Configuration

SNMP

Note: UPS-MIB Required

Your device must have a UPS-MIB database to communicate with FortiSIEM over SNMP.

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation, then follow the instructions in "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#), to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Setting Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP

Setting	Value
Community String	<your own>

Hirschmann SCADA Firewalls and Switches

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
SNMP	Host Name	SNMP – Uptime, CPU, Memory, Interface utilization, hardware Status, OSPF metrics	Performance Monitoring

Event Types

The following event types are used for performance monitoring:

- PH_DEV_MON_SYS_UPTIME - Uptime monitoring
- PH_DEV_MON_SYS_CPU_UTIL – CPU utilization
- PH_DEV_MON_SYS_MEM_UTIL – Memory utilization
- PH_DEV_MON_NET_INTF_UTIL – Interface utilization
- PH_DEV_MON_HW_STATUS – Hardware status

Rules

All performance monitoring rules apply.

Reports

All performance monitoring reports apply.

Configuration

Configure Hirschmann firewalls and switches for SNMP V1/V2c/V3 discovery and performance monitoring. Define the basic SNMP credentials on FortiSIEM and discover these devices. See [SNMP Access Credentials](#).

Sample Events

The events are standard for all devices.

Liebert FPC

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	Output voltage (X-N, Y-N, Z-N), Output current (X, Y, Z), Neutral Current, Ground current, Output power, Power Factor, Output Frequency, Output Voltage THD (Vx, Vy, Vz), Output Current THD (Lx, Ly, Lz), Output KWh, Output Crest factor (Lx, Ly, Lz), Output K-factor (Lx, Ly, Lz), Output Lx Capacity, output Ly capacity	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Liebert FPC" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "Liebert FPC" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting](#)

[Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Liebert FPC
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Liebert HVAC

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	HVAC metrics: Temperature: current value, upper threshold, lower threshold, Relative Humidity: current value, upper threshold, lower threshold, System state, Cooling state, Heating state, Humidifying state, Dehumidifying state, Economic cycle, Fan state, Heating capacity, Cooling capacity	Availability and Performance Monitoring

FortiSIEM uses SNMP to discover and collector metrics from Generic UPS devices. This requires the presence of UPS-MIB on the UPS device.

See the Liebert HVAC documentation to enable FortiSIEM to poll the device via SNMP.

Event Types

In **ADMIN > Device Support > Event Types**, search for "Liebert HVAC" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "Liebert HVAC" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

Note: UPS-MIB Required

Your device must have a UPS-MIB database to communicate with FortiSIEM.

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Liebert HVAC
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Access Credentials

Liebert UPS

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	UPS metrics: Remaining battery charge, Battery status, Time on battery, Estimated Seconds Remaining, Output voltage, Output current, Temperature	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

Note: UPS-MIB Required

Your device must include a UPS-MIB database to communicate with FortiSIEM.

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Liebert UPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Microsoft Defender for IoT (Was CyberX OT/IoT Security)

- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "cyberx" to see the event types associated with this device. In FortiSIEM 6.3.0, there are 5 event types defined.

Rules

In FortiSIEM 6.3.0, CyberX Security Alerts and CyberX Malware Detected are available.

Reports

In 6.3.0, a CyberX Security Alerts report is available.

Configuration

- [Syslog Configuration](#)

Syslog Configuration

For the latest Microsoft Defender for IoT (CyberX) documentation, see <https://docs.microsoft.com/en-us/azure/defender-for-iot/>

For latest forwarding rules information, see <https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/how-to-forward-alert-information-to-partners>

To configure syslog, take the following steps:

1. Login to the CyberX Platform UI.
2. In the left menu, go to the **Forwarding** menu.
3. Create a new forwarding rule.
4. In the **Name** field, enter "FortiSIEM_Notification" or your desired name.
5. For **Protocols**, select **All**.
6. For **Engines**, select **All**.
7. Select the Informational Severity option for your desired severity level.
8. Under **Actions**, click **Add**.
9. Select **Send to SYSLOG Server (CEF Format)**.
10. In the **Host** field, enter the IP or hostname of your FortiSIEM collector.
11. In the **Port** field, enter "514".
12. In the **Timezone** field, enter your timezone.
13. Click **Submit** when done.

Nozomi Central Management Control

Support Added: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: Nozomi Networks

Product: Nozomi Networks Central Management Control (CMC)

Product Information: <https://www.nozominetworks.com/products/overview/>

- [Configuring FortiSIEM for Nozomi](#)

Protocol	Information discovered	Metrics collected	Used for
Syslog	Device type	Node detection, protocol information, network changes	Security and Compliance

Configuring FortiSIEM for Nozomi

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Nozomi Networks CMC
Access Protocol	Nozomi REST API
User Name	Enter the username used to access your Nozomi server.
Password	Enter the password associated with your username.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your Nozomi credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the Nozomi server.
5. Navigate to **ADMIN > Setup > Discovery**.
6. Click **New** to create a Nozomi scan discovery definition.
7. In the **Discovery Definition** dialog box, take the following steps:
 - a. In the **Name** field, enter a name for the Discovery Definition.
 - b. From the **Discovery Type** drop-down list, select **Nozomi Scan**.
 - c. In the **Credential** drop-down list, your Nozomi Access Method Definition should be automatically selected.
 - d. Fill in the other fields as necessary.
 - e. When done, click **Save**.
8. Click **Discover**.
Assets from your Nozomi server will be discovered.

Devices under Nozomi can be discovered via FortiSIEM Device Discovery by selecting Nozomi Scan as Discovery Type. See [Discovering Devices](#) for more information.

Nozomi SCADAguardian

Support Added: FortiSIEM 5.2.5

Last Modification: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: Nozomi Networks

Product: Nozomi Networks SCADAguardian

Product Information: <https://www.nozominetworks.com/products/guardian/>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuring Syslog on Nozomi](#)
- [Configuring FortiSIEM for Nozomi](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog	Device type	Node detection, protocol information, network changes	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Nozomi" to see the event types associated with this device.

Rules

There are no specific rules for Nozomi, however rules that match the **Event Type Groups** associated with Nozomi Events may trigger.

Reports

There are no specific **Reports** for Nozomi, however reports that match the **Event Type Groups** associated with Nozomi Events may return results.

Configuring Syslog on Nozomi

1. Log in to the Guardian console.
2. Navigate to **Administration->Data Integration**.
3. Press **+Add** on the right side of the screen.
4. Select the **Common Event Format (CEF)** from the drop down.

5. You should see the data entry screen.

New Endpoint

Endpoint Configured as
Common Event Format (CEF) ▼

To URI
tcp://HOST:514

☐ Enable sending Alerts

☐ Send only Alerts following Security Profile

Alert query filter
e.g. 'where risk > 5'

☐ Enable sending Audit Logs

☐ Enable sending Health Logs

New Endpoint Cancel

6. Enter the appropriate host information. For example `udp://<FortiSIEM IP>:514`.
7. Select **Enable sending Alerts** and/or **Enable sending Audit Logs** and/or **Enable sending Health Logs**.
8. Press **New Endpoint**.

Configuring FortiSIEM for Nozomi

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Nozomi Networks SCADAGuardian
Access Protocol	Nozomi REST API
User Name	Enter the username used to access your Nozomi server.
Password	Enter the password associated with your username.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your Nozomi credential from the **Credentials** drop-down list.
 - c. Click **Save**.

4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the Nozomi server.
5. Navigate to **ADMIN > Setup > Discovery**.
6. Click **New** to create a Nozomi scan discovery definition.
7. In the **Discovery Definition** dialog box, take the following steps:
 - a. In the **Name** field, enter a name for the Discovery Definition.
 - b. From the **Discovery Type** drop-down list, select **Nozomi Scan**.
 - c. In the **Credential** drop-down list, your Nozomi Access Method Definition should be automatically selected.
 - d. Fill in the other fields as necessary.
 - e. When done, click **Save**.

OTORIO RAM2 (Risk Assessment, Monitoring and Management)

Supported Added: FortiSIEM 6.3.1

Last Modification: FortiSIEM 6.3.1

Vendor Version Tested: Not Provided

Vendor: Otorio

Product Information: <https://www.otorio.com/resources/ram2-next-generation-ot-soar/>

- [Log Information](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for Otorio" to see the event types associated with this device. In FortiSIEM 6.3.1, there are 12 event types defined.

Rules

In **RESOURCES > Rules**, search for "Otorio" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 rules available.

- Otorio RAM2 Alert has Triggered
- Otorio RAM2 Vulnerability Discovered

Reports

In **RESOURCES > Reports**, search for "Otorio" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 reports available.

- Otorio RAM2 Alerts
- Otorio RAM2 Vulnerabilities Discovered

Siemens Simatic PLC

Vendor: Siemens

Product: Simatic PLC

Support Added: FortiSIEM 7.4.x, 7.3.x, 7.2.x, 7.1.x

Product Information: <https://www.siemens.com/global/en.html>

Information Collected

Siemens Simatic PLC automate as much of the control of industrial plants as possible. FortiSIEM collects Informational and Security related events from Siemens Simatic PLC via Syslog. The following log types are collected:

Siemens Simatic PLC Log Type	Event Type Prefix for corresponding FortiSIEM Events	Collection Method
Security and Activity monitoring	Siemens-Simatic (33 event types)	Syslog

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Configure Siemens Simantic PLC to send Syslogs

1. Obtain the LSsylog Library for your SIMATIC device.
2. From the Totally Integrated Automation (TIA) Portal, configure the PLC to send logs to FortiSIEM by using the following configuration information.
 - a. For the **IP Address**, enter the FortiSIEM IP address.
 - b. For the **Port**, enter your port. Typically, this is 514 for UDP.Logs should now be automatically sent to FortiSIEM.

Sample Event

```
<13>1 2025-01-10T15:36:58.602Z 192.0.20.2 PLC-Program - ID97 [device@4111.6.100.1.1500  
devVendor="Siemens" devProduct="CPU1500 (PLCSIM)" FwVersion="S31.10.65"][session@4111.6.100.1.1500  
protocolType="PG/HMI comm TLS" userName="Anonymous" src="::192.0.1.2:6.0:"]  
[function@4111.6.100.1.1500 fct="new user program" result="start"] SE_USER_PROGRAM_CHANGED
```

Privileged Access Management

FortiSIEM supports the following Privileged Access Management (PAM).

- [Fortinet FortiPAM / FortiSRA](#)
- [ManageEngine PAM360](#)
- [WALLIX Bastion](#)

Fortinet FortiPAM / FortiSRA

Vendor: Fortinet

Product: FortiPAM / FortiSRA

Support Added: 7.4.x, 7.3.x, 7.2.x, 7.1.x

Product Information: <https://www.fortinet.com/products/fortipam>

Information Collected

FortiPAM provides privileged access management, control, and monitoring of elevated and privileged accounts, processes, and critical systems across the entire IT environment. FortiPAM is part of the Fortinet Security Fabric, integrating with products such as FortiClient, FortiAuthenticator, and FortiToken. FortiSRA is an agentless secure remote access solution for OT environments. FortiSRA solutions are an important part of an enterprise network, providing role-based access, auditing, and security options for privileged users (users that have system access beyond that of a regular user).

FortiSIEM collects events via syslog. The following log types are collected:

Log Type	Event Type Prefix for corresponding FortiSIEM Events	Collection Method
Informational and Security related	FortiPAM- (28 event types)	Syslog
Informational and Security related	FortiSRA- (20 event types)	Syslog

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

To configure FortiPAM / FortiSRA to send logs to FortiSIEM, take the following steps.

Note: See the latest [FortiPAM Administration Guide](#) or the latest [FortiSRA Administration Guide](#) for the most recent information.

1. Go to **Log & Report > Log Settings**.
2. In **Additional Information**, select **Edit in CLI**.
The CLI console opens.
3. Use the following parameters in the table below to configure FortiPAM, taking note of the following:

status {enable disable}	Enable/disable remote syslog logging (default = disable).

The following parameters are only available when the status is set as enable.

server <string>	Address of the remote syslog server. <string> must be configured as the FortiSIEM IP address.

mode {legacy-reliable reliable udp}	• The remote syslog logging mode: - legacy-reliable: Legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog). - reliable: Reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP). - udp: syslogging over UDP (default). If you leave the default UDP (most performant), the port will be UDP 514. If you select reliable syslog, ensure your collector has more vCPU and RAM to accommodate the reduced throughput performance.

port <integer>	The server listening port number (default = 514, 0 - 65535). Select 514 if UDP mode, or TCP 1470 if using reliable mode.

facility {kernel user mail daemon auth syslog lpr news uucp cron authpriv ftp ntp audit alert clock local0 local1 local2 local3 local4 local5 local6 local7}	The remote syslog facility (default = local7): • kernel: Kernel messages. • user: Random user-level messages. • mail: Mail system. • daemon: System daemons. • auth: Security/authorization messages. • syslog: Messages generated internally by syslog. • lpr: Line printer subsystem. • news: Network news subsystem. • uucp: Network news subsystem. • cron: Clock daemon. • authpriv: Security/authorization messages (private). • ftp: FTP daemon. • ntp: NTP daemon. • audit: Log audit. • alert: Log alert. • clock: Clock daemon. • local0 ... local7: Reserved for local use. In most cases, you can leave the default option and not set this.

source-ip <string>	The source IP address of syslog.

	(Optional) If you have multiple paths to reach the FortiSIEM collector, the packet log source is set to the egress IP. For a consistent log source, it is recommended to use a loopback address here, so no matter the egress interface, the packet source (reporting IP in the SIEM) is the same. This is especially recommended if the log traffic traverses an IPSEC tunnel to reach the FortiSIEM collector.
format {cef csv default rfc5424}	The log format: • cef: CEF (Common Event Format) format. • csv: CSV (Comma Separated Values) format. • default: Syslog format (default). • rfc5424: Syslog RFC5424 format. Leave as default, the default syslog format.
priority {default low}	The log transmission priority: • default: Set Syslog transmission priority to default (default). • low: Set Syslog transmission priority to low.
max-log-rate <integer>	The syslog maximum log rate in MBps (default = 0, 0 - 100000 where 0 = unlimited).
interface-select-method {auto sdwan specify}	Specify how to select outgoing interface to reach the server: • auto: Set outgoing interface automatically (default). • sdwan: Set outgoing interface by SD-WAN or policy routing rules. • specify: Set outgoing interface manually.

4. After adjusting the parameters, click **x** to close the CLI console.

Sample Events

FortiSRA

```
<189>date=2024-12-12 time=13:47:38 devname="FortiSRA" devid="FRAVULTM12345678"
eventtime=1734007658567988661 tz="+0100" logid="0100022813" type="event" subtype="system"
level="notice" vd="root" logdesc="Scanunit reloaded AV Database" action="update"
msg="scanunit=manager pid=1663 cause='signal' AV database reload requested 1 times by updated
(pid 1665) successful"
```

```
<189>date=2024-12-12 time=13:47:18 devname="FortiSRA" devid="FRAVULTM12345678"
eventtime=1734007638145680402 tz="+0100" logid="0100041000" type="event" subtype="system"
level="notice" vd="root" logdesc="FortiSRA update succeeded" status="update" msg="FortiSRA
scheduled update fcni=yes fdni=yes fsci=yes virdb(92.09472) etdb(92.09472) exdb(1.00000) avai
(3.02149) mmdb(92.09472) cidb(0.00000) from 192.168.1.2:443"
```

```
<187>date=2024-12-12 time=13:44:54 devname="FortiSRA" devid="FRAVULTM12345678"
eventtime=1734007494197529411 tz="+0100" logid="0105048038" type="event" subtype="wad"
level="error" vd="root" logdesc="SSL Fatal Alert received" session_id=745b236f policyid=1
srcip=192.168.1.3 srcport=58489 dstip=192.168.1.4 dstport=443 action="receive" alert="2"
desc="certificate unknown" msg="SSL Alert received"
```

```
<190>date=2024-12-12 time=13:42:26 devname="FortiSRA" devid="FRAVULTM12345678"
eventtime=1734007346793313733 tz="+0100" logid="0112053203" type="event" subtype="connector"
level="information" vd="root" logdesc="Dynamic address updated." addr="FCTEMS_ALL_FORTICLOUD_
SERVERS" msg="Updated tag FCTEMS_ALL_FORTICLOUD_SERVERS"
```

```
<189>date=2024-12-12 time=13:41:57 devname="FortiSRA" devid="FRAVULTM12345678"
eventtime=1734007316924621478 tz="+0100" logid="0100040704" type="event" subtype="system"
level="notice" vd="root" logdesc="System performance statistics" action="perf-stats" cpu=0
mem=20 totalsession=57 disk=4 bandwidth="9/60" setuprate=0 disklograte=0 fazlograte=0
freediskstorage=28488 sysuptime=172542 waninfo="N/A" msg="Performance statistics: average CPU:
0, memory: 20, concurrent sessions: 57, setup-rate: 0"
```

FortiPAM

```
<189>date=2023-12-14 time=12:36:33 devname="FPAVULTM1234567" devid="FPAVULTM1234567"
eventtime=1702557393665511462 tz="+0000" logid="0100040704" type="event" subtype="system"
level="notice" vd="root" logdesc="System performance statistics" action="perf-stats" cpu=0
mem=52 totalsession=107 disk=1 bandwidth="1/0" setuprate=0 disklograte=0 fazlograte=0
freediskstorage=28493 sysuptime=485465 waninfo="N/A" msg="Performance statistics: average CPU:
0, memory: 52, concurrent sessions: 107, setup-rate: 0"
```

```
<187>date=2023-12-14 time=12:38:50 devname="FPAVULTM1234567" devid="FPAVULTM1234567"
eventtime=1702557529389749042 tz="+0000" logid="0105048038" type="event" subtype="wad"
level="error" vd="root" logdesc="SSL Fatal Alert received" session_id=6458ac42 policyid=1
srcip=10.0.5.3 srcport=57291 dstip=10.0.5.45 dstport=443 action="receive" alert="2"
desc="certificate unknown" msg="SSL Alert received"
```

```
date=2023-08-24 time=17:23:03 devname="FPAVULTM1234567" devid="FPAVULTM1234567"
eventtime=1692922983764461604 tz="-0700" logid="2304064604" type="secret" subtype="secret-
request" eventtype="secret-request" action="pass" operation="request" secretid=2820
secret="PC0" account="testUser1" uuid="11111111-1111-1111-1111-111111111111" user="user1"
starttime="2023-08-24 17:23:00" expirytime="2023-08-24 17:53:00" msg="Created secret request."
```

ManageEngine PAM360

Vendor: ManageEngine

Product: PAM 360

Support Added: 7.4.x

Product Information: <https://www.manageengine.com/privileged-access-management/>

Information Collected

ManageEngine PAM360 is a comprehensive, web-based Privileged Access Management (PAM) solution designed for enterprises to secure, manage, and audit critical IT assets. It protects against credential-based attacks through centralized, encrypted password vaulting, session recording, and just-in-time privilege elevation, supporting hybrid IT environments.

The following log types are collected:

PAM360 Logs	Event Type Prefix for corresponding FortiSIEM Events	Collection Method
Informational	ManageEngine-PAM360 (7 event types)	Syslog

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

Configure ManageEngine PAM360 to send syslogs to FortiSIEM. No configuration is required in FortiSIEM.

Reference: <https://www.manageengine.com/privileged-access-management/help/integration-siemtools.html#integration>

1. Navigate to **Admin >> Integrations >> SIEM Integrations**.
2. Click **Add New SIEM** and enter the following details in the page that appears:
 - a. In the **Application Name** field, enter the name of the syslog collector to which PAM360 should send the syslog messages.
 - b. In the **Collector Name** field, enter the hostname of the server where the syslog service is running.
 - c. In the **Port** field, specify the port number at which the syslog collector listens. The default port number is 514 for UDP.
 - d. From the **Protocol** drop-down, select the transport protocol to send the syslog messages to the syslog collector. UDP preferred for performance. Select TCP if reliability is required.
 - e. From **Syslog Standard**, select the desired syslog message format in which PAM360 should send the syslog messages to the syslog collector. Default RFC_3164 is fine.
 - f. In the **Facility Name** field, specify the syslog facility to categorize the messages. Any selection is fine.

Sample Events

```
<134>Sep 2 15:08:45 pam ResourceAudit:testuser123:192.0.2.0 Session_Ended 2025/09/02 15:08:39
Success pam ORG123-TestServerABC:acc123:N/A:RDP_initiated_from_PAM360_to_192.0.2.0_has_stopped
```

```
<134>Sep 2 15:15:04 pam ResourceAudit:testuser123:192.0.2.0 Password_Retrieved 2025/09/02 15:15:03
Success pam ORG123-ExampleServer:acc321:N/A:Retrieved_by_Windows_Remote_Desktop_auto_logon_helper_
Reason_-_To_connect_to_the_machine_192.0.2.0
```

```
<134>Sep 18 16:22:53 pam ResourceAudit:test-user123:192.0.2.2 Session_Ended 2025/09/18 16:22:52
Success pam ORG321:test-admin:N/A:RDP_initiated_from_PAM360_to_192.0.2.3_has_stopped
```

WALLIX Bastion

Vendor: WALLIX

Product: Bastion Privileged Access Management (PAM)

Support Added: FortiSIEM 7.4.x, 7.3.x, 7.2.x, 7.1.x

Product Information: <https://www.wallix.com/products/privileged-access-management/>

Information Collected

WALLIX Bastion is a Privileged Access Management (PAM) solution that secures, controls, and monitors privileged user access to critical IT and OT (Operational Technology) systems. FortiSIEM collects Informational events from WALLIX Bastion via Syslog. The following log types are collected:

Wallix Bastion Log Type	Event Type Prefix for corresponding FortiSIEM Events	Collection Method
Authentication, Vault Activity, Session log export, WALLIX Plugins	Wallix-Bastion (7 event types)	Syslog

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Configure Wallix Bastion to send Syslogs

1. Login to WALLIX.
2. Navigate to **System > SIEM Integration**.
3. Under **Syslog server configuration**, select one entry and enter the following:
 - a. From the **Routing** drop-down, select **Enabled**.
 - b. In the **IP/FQDN** field, enter the FortiSIEM collector IP or FQDN.
 - c. From the **Protocol** drop-down, select **udp**.
 - d. In the **Port** field, enter the port number, typically 514.
 - e. From the **Log Format** drop-down, select **rfc5424**.
 - f. In **Filters**, check all that apply
 - i. Authentication
 - ii. Vault Activity
 - iii. Session log export
 - iv. WALLIX Plugins
 - g. For Configuration changes Filters: Select all.
 - h. SSH proxy events filters: Select all.
 - i. RDP proxy events filters: Select all.
 - j. SSH session filters: Select all.
 - k. Click **Apply**.

Logs should now be automatically sent to FortiSIEM.

Confirm Logs appears in FortiSIEM

1. Login to FortiSIEM GUI.
2. Navigate to **Analytics**.

3. Run the following query:
Event Type CONTAIN Wallix-Bastion
4. Confirm that WALLIX logs appear.

Sample Events

```
<14>1 2024-07-18T12:13:54+01:00 SRV-Wallix-Bastion rdpproxy 4771 - - [RDP Session] session_id="190c55e3d2ea41ce0050568a45c1" client_ip="192.0.2.1" target_ip="192.0.2.16" user="xyzabc" device="SRV-Test-0.16" service="RDP" account="abc" type="DYNAMIC_CHANNEL_CREATION_ALLOWED" channel_name="ABCDE"
```

```
<14>1 2024-07-17T10:31:41+01:00 SRV-Wallix-Bastion rdpproxy 3753 - - [RDP Session] session_id="190bfff6f6fb4b0a0050568a45c1" client_ip="192.0.2.1" target_ip="192.0.2.20" user="test123" device="test-SRV" service="RDP" account="test" type="TITLE_BAR" source="Probe" window="Oracle SQL Developer : SITETest"
```

```
<86>1 2024-07-18T12:02:02+01:00 SRV-Wallix-Bastion CRON 9701 - - pam_unix(cron:session): session closed for user root
```

Routers and Switches

FortiSIEM supports these routers and switches for discovery and monitoring.

- Alcatel TiMOS and AOS Switch
- Arista Router and Switch
- ArubaOS-CX Switching Platform
- Brocade NetIron CER Routers
- Cisco 300 Series Routers
- Cisco IOS Router and Switch
 - How CPU and Memory Utilization is Collected for Cisco IOS
- Cisco Meraki Cloud Controller and Network Devices
- Cisco NX-OS Router and Switch
- Cisco ONS
- Cisco Viptela SDWAN Router
- Dell Force10 Router and Switch
- Dell N-Series Switch
- Dell PowerConnect Switch and Router
- Foundry Networks IronWare Router and Switch
- HP/3Com ComWare Switch
- HP ProCurve Switch
- HP Value Series (19xx) and HP 3Com (29xx) Switch
- Hirschmann SCADA Firewalls and Switches
- Juniper Networks JunOS Switch
- MikroTik Router
- Nortel ERS and Passport Switch

Alcatel TiMOS and AOS Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Software version, Hardware model, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c)		Hardware status: Power Supply, Fan, Temperature	Availability
SNMP (V1, V2c, V3)	Layer 2 port mapping: associating switch ports to directly connected host IP/MAC addresses		Identity and location table; Topology

Event Types

In **ADMIN > Device Support > Event Types**, search for "alcatel" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Arista Router and Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial number, Software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), CPU utilization, Memory utilization, Flash utilization, Hardware Status	Availability and Performance Monitoring
Telnet/SSH	Running and Startup configurations	Startup Configuration Change, Difference between Running and Startup configurations	Change monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [Telnet/SSH](#)
- [SNMP](#)

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

- `show startup-config`
- `show running-config`
- `show version`
- `show ip route`
- `enable`
- `terminal pager 0`

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

ArubaOS-CX Switching Platform

Support Added: FortiSIEM 6.3.2

Vendor: Aruba Networks (a Hewlett Packard Enterprise company)

Product Information: <https://www.arubanetworks.com/products/switches/>

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of ArubaOS-CX switches.

Protocol	Metrics Collected	Used For
Syslog	Audit logs, General Performance and Availability logs	Security and Compliance

Configuration

Logging allows you to add syslog servers where the event log messages related to the AOS-CX switches are saved. For each of the syslog server added, you can configure the severity of the event logs to be saved on these servers. Configuration of the severity level for the debug logs can be done by configuring the severity at the global level. However, a minimum of one syslog server must be added to configure the global severity level.

- [Configuration via CLI](#)
- [Configuration via GUI](#)

Configuration via CLI

To configure syslog for an ArubaOS-CX switch, run the following CLI command.

```
logging <destIP or FQDN of FortiSIEM collector>
```

Example: logging 192.0.2.0

Configuration via GUI

To configure syslog for an ArubaOS-CX switch, take the following steps.

Note: For the latest configuration instructions, see **Configuring Logging Servers for AOS-CX** at https://help.central.arubanetworks.com/latest/documentation/online_help/content/aos-cx/cfg/conf-cx-logging.htm

1. In the **Network Operations** app, select one of the following options:
 - a. To select a group in the filter:
 - i. Set the filter to a group. The dashboard context for the group is displayed.
 - ii. Under **Manage**, click **Devices > Switches**.
 - iii. Click the **AOS-CX** or the **Config** icon to view the AOS-CX switch configuration dashboard.
 - b. To select a switch:
 - i. Set the filter to **Global** or a group containing at least one switch.
 - ii. Under **Manage**, click **Devices > Switches**. A list of switches is displayed in the List view.
 - iii. Click an AOS-CX switch under **Device Name**. The dashboard context for the switch is displayed.
 - iv. Under **Manage**, click **Device**.

The AOS-CX UI configuration page is displayed.

2. Click **System > Logging**. The Logging page is displayed.
3. Select the debug syslog severity level at the global level from the **Level** drop-down list. This severity level is applied to the debug logs that are saved on the syslog servers. You must add a minimum of one event syslog server before configuring the global severity level.
4. In the **Logging Servers** table, click **+** to add a logging server and configure the following parameters in the Add Logging Server page.

Parameters	Description	Value
FQDN or IP address	Fully Qualified Domain Name (FQDN) hostname or IP address of the logging server.	Enter the IPv4 address in the x.x.x.x format or the hostname of the server.
Level	Severity level of the events that the logging server must log.	The following severity levels are supported: • Emergency • Critical • Alert • Error • Warning • Notice • Information • Debug
VRF	VRF on which the logging server is configured.	Default or Management .

5. Click **Apply** and then click **Save**.
6. To edit parameters of a logging server, select the row in the **Logging Servers** table and click the edit icon. The Edit Logging Server page is displayed. You can edit only the event log severity level and the VRF.
7. Click **Apply** and then click **Save**.
8. To delete the syslog server, select the row in the **Logging Servers** table and click the delete icon.
9. Click **OK** in the confirmation pop-up and then click **Save**.

Sample Events

```
<190>1 2021-08-31T12:29:06.148824-06:00 lab-1 hpe-restd 886 - - Event|4604|LOG_INFO|AMM|-|Session
started for user user1, session re07LY123452GW7JlMw==
<190>1 2021-09-01T07:43:56.409226-06:00 lab-1 hpe-restd 886 - - Event|4609|LOG_INFO|AMM|-|User
aruba-admin added newuser-test with role admin-role
```

Brocade NetIron CER Routers

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces	CPU, Memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware Status, Real Server Status	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules specifically for this device.

Reports

There are no predefined reports specifically for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Brocade NetIron CER
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco 300 Series Routers

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces	Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards, and queue lengths)	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules specifically for this device.

Reports

There are no predefined reports specifically for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#)

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Cisco IOS Router and Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

Issue with Generic Serial Numbers in Older Versions of Cisco IOS Routers

FortiSIEM uses serial numbers to uniquely identify a device. For older routers, the serial number is obtained from the OID 1.3.6.1.4.1.9.3.6.3.0. However, this value is often incorrectly set by default to a generic value like MSFC 2A. If multiple routers have a common default value, then these routers will be merged into a single entry in the FortiSIEM CMDB.

You can check the current value for the serial number in a Cisco router by doing a SNMP walk of the OID.

```
snmpwalk -v2c -c <cred> <ip> 1.3.6.1.4.1.9.3.6.3.0
```

If the value is a generic value, then set it to the actual serial number.

```
Router(config)#snmp-server chassis-id
Router(config)#exit
Router#write memory
```

Run the snmpwalk again to verify that the serial number is updated, then perform discovery of your Cisco router.

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	Host name, IOS version, Hardware model, Memory size, Network interface details - name, address, mask and description	Uptime, CPU and Memory utilization, Free processor and I/O memory, Free contiguous processor and I/O memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths),	Availability and Performance Monitoring
SNMP (V1, V2c, V3)	Hardware component details: serial number, model, manufacturer, software firmware versions of hardware	Hardware health: temperature, fan and power supply	Availability

Protocol	Information Discovered	Metrics collected	Used for
	components such as chassis, CPU, fan, power supply, network cards etc.		
SNMP (V1, V2c, V3)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location
SNMP (V1, V2c, V3)	BGP connectivity, neighbors, state, AS number	BGP state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)	OSPF connectivity, neighbors, state, OSPF Area	OSPF state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)		IP SLA and VoIP performance metrics: Max/Min/Avg Delay and Jitter - both overall and Source->Destination and Destination->Source, Packets Lost - both overall and Source->Destination and Destination->Source, Packets Missing in Action, Packets Late, Packets out of sequence, VoIP Mean Opinion Score (MOS), VoIP Calculated Planning Impairment Factor (ICPIF) score	VoIP Performance Monitoring
SNMP (V1, V2c, V3)		Class based QoS metrics (from CISCO-CLASS-BASED-QOS-MIB): For (router interface, policy, class map) tuple: class map metrics including Pre-policy rate, post-policy rate, drop rate and drop pct; police action metrics including conform rate, exceeded rate and violated rate; queue metrics including current queue length, max queue length and discarded packets	QoS performance monitoring
SNMP (V1,		NBAR metrics (from CISCO-NBAR-PROTOCOL-	Performance

Protocol	Information Discovered	Metrics collected	Used for
V2c, V3)		DISCOVERY-MIB): For each interface and application, sent/receive flows, sent/receive bytes, sent/receive bits/sec	Monitoring
Telnet/SSH	Running and startup configuration, Image file name, Flash memory size, Running processes	Startup configuration change, delta between running and startup configuration, Running process CPU and memory utilization	Performance Monitoring, Security and Compliance
Syslog	Device type	System logs and traffic logs matching acl statements	Availability, Security and Compliance

Event Types

In **Admin > Device Support > Event Types**, search for "cisco_ios" to see the event types associated with this device.

Configuration

- [Telnet/SSH](#)
- [SNMP](#)
- [Syslog](#)
- [NetFlow](#)
- [IP SLA](#)
- [Class-Based QoS](#)
- [NBAR](#)

Telnet/SSH

FortiSIEM uses SSH and Telnet to communicate with your device. Follow the instructions in the product documentation for your device to enable SSH and Telnet.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

- `show startup-config`
- `show running-config`
- `show version`
- `show flash`

- show ip route
- show mac-address-table or show mac address-table
- show vlan brief
- show process cpu
- show process mem
- show disk0
- enable
- terminal pager 0

SNMP

SNMP V1/V2c

1. Log in to the Cisco IOS console or telnet to the device.
2. Enter configuration mode.
3. Create an access list for FortiSIEM.

```
access-list 10 permit <FortiSIEM IP>
```

4. Set up community strings and access lists.

```
snmp-server community <community string> ro 10
```

5. Exit configuration mode.

SNMP V3

1. Log in to the Cisco IOS console or telnet to the device.
2. Enter configuration mode.
3. Create an access list for FortiSIEM.

```
access-list 10 permit <FortiSIEM IP>
```

4. Set up SNMP credentials for Authentication only.

```
snmp-server group <grpName> v3 auth
#do this for every VLAN for FortiSIEM to discover per VLAN information such Spanning Tree and
VTP MIBs
snmp-server group <grpName> v3 auth context vlan-<vlanId>snmp-server user <userName> <grpName>
v3 auth md5 <password> access 10
```

5. Set up SNMP credentials for Authentication and Encryption.

```
snmp-server group <grpName> v3 priv
#do this for every VLAN for FortiSIEM to discover per VLAN information such Spanning Tree and
VTP MIBs
snmp-server group <grpName> v3 auth context vlan-<vlanId>snmp-server group <grpName> v3 priv
context vlan-<vlanId>snmp-server user <userName> <grpName> v3 auth md5 <password> priv des56
```

```
<password> access 10
```

6. Exit configuration mode.

Additional IOS SNMPv3 Configuration Examples

IOS

```
enable
```

```
config t
```

```
snmp-server contact "contact info"
```

```
snmp-server location "location info"
```

```
snmp-server group fsiem_group v3 priv
```

#Note, check the context sensitive help in your IOS version to see if aes 128 is supported instead of des56.

```
snmp-server user fortisiem_user fsiem_group 192.168.1.2 v3 auth sha "yourShaPassword" priv  
des56 "yourDesPassword"
```

```
copy running-config startup-config
```

IOS XE

```
enable
```

```
config t
```

```
snmp-server group fsiem_group v3 priv
```

```
snmp-server user fortisiem fsiem_group 192.168.1.2 v3 auth sha "yourShaPassword" priv aes 128  
"yourAesPassword"
```

```
copy running-config startup-config
```

IOS XR

#Note not all models running IOS XR can support aes 128, some may only support des
configure

```
snmp-server contact "contact info"
```

```
snmp-server location "location info"
```

```
snmp-server group fsiem_group v3 priv
```

```
snmp-server user fortisiem fsiem_group v3 auth sha "yourShaPassword" priv aes 128  
"yourDesPassword"
```

```
commit
```

Nexus 9K

```
config t
snmp-server contact "contact info"
snmp-server location "location info"
snmp-server user fortisiem auth sha "yourShaPassword" priv aes-128 "yourAesPassword"
snmp-server user fortisiem enforcePriv
copy running-config startup-config
```

Syslog

1. Login to the Cisco IOS console or telnet to the device.
2. Enter configuration mode.
3. Enable logging with these commands.

```
logging on
logging trap informational
logging <FortiSIEM IP>
```

4. Make sure that the timestamp in syslog message sent to FortiSIEM does not contain milliseconds.

```
no service timestamps log datetime msec
service timestamps log datetime
```

5. To log traffic matching acl statements in stateless firewall scenarios, add the log keyword to the acl statements.

```
access-list 102 deny udp any gt 0 any gt 0 log
```

6. To turn on logging from the IOS Firewall module, use this command.

```
ip inspect audit-trail
```

7. Exit configuration mode.

Sample Cisco IOS Syslog Messages

```
<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)
```

```
<190>263951: 2w6d: %SEC-6-IPACCESSLOGP: list permit-any permitted udp 192.168.20.35(0) ->
192.168.23.255(0), 1 packet
```

```
<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 2010
```



```
<189>217: May 12 13:57:23.720: %SYS-5-CONFIG_I: Configured from console by vty1 (192.168.29.8)

<189>Oct 27 20:18:43.254 UTC: %SNMP-3-AUTHFAIL: Authentication failure for SNMP request from host
192.168.2.98
```

NetFlow

Enable NetFlow on the Router

1. Enter configuration mode.
2. For **every interface**, run this command.

```
interface <interface> <interface_number>ip route-cache flow
exit
```

Set Up NetFlow Export

1. Enter configuration mode.
2. Run these commands.

```
ip flow-export version 5|9
ip flow-export destination <fsiem IP> 2055
ip flow-export source <interface> <interface_number>ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
```

On MLS switches, such as the 6500 or 7200 models, also run these commands.

```
mls netflow
mls nde sender
mls aging long 64
mls flow ip full
Exit configuration mode
```

You can verify that you have set up NetFlow correctly by running these commands.

```
#shows the current NetFlow configuration
show ip flow export
#summarizes the active flows and gives an indication of how much NetFlow data the device is
exporting
show ip cache flow or show ip cache verbose flow
```

Sample Flexible Netflow Configuration in IOS

```
flow exporter e1
! destination is the collector address, default port needs to be changed to 2055
```

```

    destination <fsiemIp>    transport udp 2055
!
flow record r1
    ! record specifies packet fields to collect
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    collect transport tcp flags
    collect interface output
    collect counter bytes
    collect counter packets
!
flow monitor m1
    ! monitor refers record configuration and exporter configuration.
    record r1
    exporter e1
    cache timeout active 60
    cache timeout inactive 30
    cache entries 1000
!
interface GigabitEthernet 2/48
    ip flow monitor m1 input

```

IP SLA

IP SLA is a technology where a pair of routers can run synthetic tests between themselves and report detailed traffic statistics. This enables network administrators to get performance reports between sites without depending on end-host instrumentation.

Cisco provides [detailed documents for configuring IP SLA for both general traffic and VoIP](#).

A variety of IP SLA tests can be run, for example UDP/ICMP Jitter, UDP Jitter for VoIP, UDP/ICMP Echo, TCP Connect, HTTP, etc. You can see the traffic statistics for these tests by routing appropriate Show commands on the router. However, only these IP SLA tests are exported via RTT-MON SNMP MIB.

- UDP Jitter (reported by FortiSIEM event type PH_DEV_MON_IPSLA_MET)
- UDP Jitter for VoIP (reported by FortiSIEM event type PH_DEV_MON_IPSLA_VOIP_MET)
- HTTP performance (reported by FortiSIEM event type PH_DEV_MON_IPSLA_HTTP_MET)
- ICMP Echo (reported by FortiSIEM event type PH_DEV_MON_IPSLA_ICMP_MET)
- UDP Echo (reported by FortiSIEM event type PH_DEV_MON_IPSLA_UDP_MET)

These are the only IP SLA tests monitored by FortiSIEM.

Configuring IP SLA involves choosing and configuring a router to initiate the test and a router to respond. The test statistics are automatically reported by the initiating router via SNMP, so no additional configuration is required. Bi-directional traffic statistics are also reported by the initiating router, so you don't need to set up a

reverse test between the original initiating and responding routers. FortiSIEM automatically detects the presence of the IP SLA SNMP MIB (CISCO-RTTMON-MIB) and starts collecting the statistics.

Configuring IP SLA Initiator for UDP Jitter

```
ipsla-init>enable
ipsla-init#config terminal
ipsla-init(config)#ip sla monitor <operation num>ipsla-init(config-sla-monitor)#type jitter dest-
ipaddr <responder ip> dest-port <dest port>ipsla-init(config-sla-monitor-jitter)#frequency default
ipsla-init(config-sla-monitor-jitter)#exit
ipsla-init(config)# ip sla monitor schedule <operation num> start-time now life forever
```

Configuring IP SLA Initiator for UDP Jitter for VoIP

```
ipsla-init>enable
ipsla-init#config terminal
ipsla-init(config)#ip sla monitor <operation num>ipsla-init(config-sla-monitor)#type jitter dest-
ipaddr <responder ip> dest-port <dest port> codec <codec type> advantage-factor 0
ipsla-init(config-sla-monitor-jitter)#frequency default
ipsla-init(config-sla-monitor-jitter)#exit
ipsla-init(config)# ip sla monitor schedule <operation num> start-time now life forever
```

Configuring IP SLA Initiator for ICMP Echo Operation

```
Router> enable
Router# configure terminal
Router(config)# ip sla monitor 15
Router(config-sla-monitor)# type echo protocol ipIcmpEcho <destination-ip-address>Router(config-
sla-monitor-echo)# frequency 30
Router(config-sla-monitor-echo)# exit
Router(config)# ip sla monitor schedule 10 start-time now life forever
Router(config)# exit
```

Configuring the IP SLA Responder for All Cases

```
ipsla-resp>enable
ipsla-resp#config terminal
ipsla-resp(config)#ip sla monitor responder
```

Class-Based QoS

CBQoS enables routers to enforce traffic dependent Quality of Service policies on router interfaces for to make sure that important traffic such as VoIP and mission critical applications get their allocated network resources.

Cisco provides [detailed documents for configuring IP SLA for both general traffic and VoIP](#).

The CbQoS statistics are automatically reported by the router via SNMP, so no additional configuration is needs. FortiSIEM detects the presence of valid CBQoS MIBs and starts monitoring them.

NBAR

Cisco provides [protocol discovery via NBAR configuration guide](#).

Make sure that the CISCO-NBAR-PROTOCOL-DISCOVERY-MIB is enabled.

Sample event generated by FortiSIEM

```
[PH_DEV_MON_CISCO_NBAR_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceCisco.cpp,  
[lineNumber]=1644,[hostName]=R1.r1.example.com,[hostIpAddr]=10.1.20.59,[intfName]=Ethernet0/0,  
[appTransportProto]=snmp,[totFlows]=4752,[recvFlows]=3168,[sentFlows]=1584,[totBytes64]=510127,  
[recvBytes64]=277614,[sentBytes64]=232513,[totBitsPerSec]=22528.000000,  
[recvBitsPerSec]=12288.000000,[sentBitsPerSec]=10240.000000,[phLogDetail]=
```

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

These are the generic settings for providing SNMP access to your device from FortiSIEM.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet
Device Type	Cisco IOS
Access Protocol	TELNET
Port	23
User Name	A user who has access credentials for your device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	Cisco IOS-SSH
Device Type	Cisco IOS
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password associated with the user
Privileged	If checked/enabled, it means the given SSH user has permissions in Cisco IOS to run the <code>show running-config</code> and <code>show startup-config</code> commands to retrieve and store that data. If unchecked, those two commands will not be run when collecting discovery data via SSH. In general, it is always recommended to have a read-only admin account, or in the case of using remediation script (automation response scripts), a SSH user with write permissions to make config changes such as <code>shun IP</code> commands.

How CPU and Memory Utilization is Collected for Cisco IOS

FortiSIEM follows the process for collecting information about CPU utilization that is [recommended by Cisco](#).

- [Monitoring CPU](#)
- [Monitoring Memory using PROCESS-MIB](#)

Monitoring CPU

The OID is 1.3.6.1.4.1.9.9.109.1.1.1.1.8. The issue there are multiple CPUs – which ones to take? A sample SNMP walk for this OID looks like this

```
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.1 = Gauge32: 46
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.2 = Gauge32: 22
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.3 = Gauge32: 5
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.4 = Gauge32: 4
```

Note that there are 4 CPUs – indexed 1-4. We must identify Control plane CPU and Data plane CPU

The cpu Id -> entity Id mapping from the following SNMP walk

```
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.1 = INTEGER: 3014
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.2 = INTEGER: 3001
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.3 = INTEGER: 1001
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.4 = INTEGER: 7001
```

This provides the following cpu Id -> entity Id mapping

```
1 -> 3014
2 -> 3001
3 -> 1001
4 -> 7001
```

The following SNMP walk provides the names for each entity Id

```
SNMPv2-SMI::mib-2.47.1.1.1.1.7.1001 = STRING: "Chassis 1 CPU of Module 2"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.3001 = STRING: "Chassis 1 CPU of Switching Processor 5"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.3014 = STRING: "Chassis 1 CPU of Routing Processor 5"
SNMPv2-SMI::mib-2.47.1.1.1.1.7.7001 = STRING: "Chassis 2 CPU of Module 2"
```

Combining all this information, we finally obtain the CPU information for each object

```
Chassis 1 CPU of Routing Processor 5 -> 46%
Chassis 1 CPU of Switching Processor 5 -> 22%
Chassis 1 CPU of Module 2 -> 5
Chassis 2 CPU of Module 2 -> 4%
```

FortiSIEM reports utilization per cpu utilization

```
[PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=9596,
[cpuName]=Chassis 1 CPU of Routing Processor
5,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=46.000000,[pollIntv]=176,[phLogDetail]=

[PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=9596,
[cpuName]=Chassis 1 CPU of Switching Processor
5,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=22.000000,[pollIntv]=176,[phLogDetail]=

PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=9596,
[cpuName]=Chassis 1 CPU of Module
2,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=5.000000,[pollIntv]=176,[phLogDetail]=

[PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=9596,
[cpuName]=Chassis 2 CPU of Module
2,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=4.000000,[pollIntv]=176,[phLogDetail]=
```

To get the overall system CPU utilization, we average over "Switching and Routing CPUs"- so CPU Util = $(46+22)/2 = 34\%$

```
PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=9611,
[cpuName]=RoutingCpu,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=34.0000,
[pollIntv]=176,[phLogDetail]=
```

Monitoring Memory using PROCESS-MIB

The relevant OIDs are

Used memory OID = 1.3.6.1.4.1.9.9.48.1.1.1.6

Free memory OID = 1.3.6.1.4.1.9.9.48.1.1.1.5

Memory Util = (Used memory) / (Used memory + Free memory)

```
SNMPv2-SMI::enterprises.9.9.48.1.1.1.5.1 = Gauge32: 87360992 <- Processor Memory Used
SNMPv2-SMI::enterprises.9.9.48.1.1.1.5.2 = Gauge32: 10715440 <- IO Memory Used
SNMPv2-SMI::enterprises.9.9.48.1.1.1.6.1 = Gauge32: 2904976 <- Processor Memory Free
SNMPv2-SMI::enterprises.9.9.48.1.1.1.6.2 = Gauge32: 1342944 <- IO Memory Free
```

Therefore

```
Used Memory = 98,076,432
Total Memory = 102,324,352
Memory Util = 96%
```

Cisco Meraki Cloud Controller and Network Devices

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Cisco Meraki Devices are discoverable in either of the following ways

- SNMP to the Cloud Controller
- SNMP to each Network Device

SNMP Traps can be sent from the Cloud Controller. Cisco Meraki Network Devices can also send logs directly to FortiSIEM.

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c) to Cloud Controller or Devices	Host name, Software version, Hardware model, Network interfaces	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
syslog from Meraki Firewalls		Firewall logs	Security Monitoring
syslog from Meraki Access Points		Air Marshal logs	Security Monitoring
SNMP Traps from Cloud Controller		Health	Availability Monitoring

Event Types

- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL

Rules

- [Availability \(From SNMP Trap\)](#)
- [Performance \(Fixed Threshold\)](#)
- [Performance \(Dynamic Threshold Based on Baselines\)](#)

Availability (From SNMP Trap)

- Meraki Device Cellular Connection Disconnected
- Meraki Device Down
- Meraki Device IP Conflict
- Meraki Device Interface Down
- Meraki Device Port Cable Error
- Meraki Device VPN Connectivity Down
- Meraki Foreign AP Detected
- Meraki New DHCP Server
- Meraki New Splash User
- Meraki No DHCP lease
- Meraki Rogue DHCP Server
- Meraki Unreachable Device
- Meraki Unreachable RADIUS Server
- Meraki VPN Failover

Performance (Fixed Threshold)

- Network Intf Error Warning
- Network Intf Error Critical
- Network Intf Util Warning
- Network Intf Util Critical

Performance (Dynamic Threshold Based on Baselines)

- Sudden Increase in Network Interface Traffic
- Sudden Increase in Network Interface Errors

Reports

None

Configuration

Syslog for Air Marshal Events

The latest instructions can be found at https://documentation.meraki.com/MR/Monitoring_and_Reporting/Air_Marshal to configure syslog for Air Marshal events.

Syslog alerting can be configured by navigating to **Network-wide > General**, and configuring the syslog server IP, port, and specifying "air marshal" events.

Note: For all roles, select each role available. This configuration applies for access points (APs), switches, and firewalls.

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco Meraki Cloud Controller
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco NX-OS Router and Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	Host name, IOS version, Hardware model, Memory size, Network interface details - name, address, mask and description	Uptime, CPU and Memory utilization, Free processor and I/O memory, Free contiguous processor and I/O memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c, V3)	Hardware component details: serial number, model, manufacturer, software and firmware versions of hardware components such as chassis, CPU, fan, power supply, network cards etc.	Hardware health: temperature, fan and power supply	Availability
SNMP (V1, V2c, V3)	Trunk port connectivity between switches and VLANs carried over a trunk port (via CDP MIB), ARP table		Topology and end-host location

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	BGP connectivity, neighbors, state, AS number	BGP state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)	OSPF connectivity, neighbors, state, OSPF Area	OSPF state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)		Class based QoS metrics: For (router interface, policy, class map) tuple: class map metrics including Pre-policy rate, post-police rate, drop rate and drop pct; police action metrics including conform rate, exceeded rate and violated rate; queue metrics including current queue length, max queue length and discarded packets	QoS performance monitoring
Telnet/SSH	Running and startup configuration, Image file name, Flash memory size, Running processes	Startup configuration change, delta between running and startup configuration, Running process CPU and memory utilization	Performance Monitoring, Security and Compliance
Telnet/SSH	End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		
Syslog	Device type>	System logs and traffic logs matching acl statements	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco-nxos" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Telnet/SSH](#)
- [Syslog](#)
- [NetFlow](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

- `show startup-config`
- `show running-config`
- `show version`
- `show flash`
- `show context`
- `show ip route`
- `show cam dynamic`
- `show mac-address-table`
- `show mac address-table (for Nexus 1000v)`
- `show vlan brief`
- `show process cpu`
- `show process mem`
- `show disk0`
- `enable`
- `terminal length 0`

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

NetFlow

- [Enable NetFlow on the Router](#)
- [Create a Flow Template and Define the Fields to Export](#)
- [Set up NetFlow Exporter](#)
- [Associate the Record to the Exporter Using a Flow Monitor](#)
- [Apply the Flow Monitor to Every Interface](#)

Enable NetFlow on the Router

1. Enter configuration mode.
2. Run this command.

```
feature netflow
```

Create a Flow Template and Define the Fields to Export

You can also try using the pre-defined NetFlow template.

```
# show flow record netflow-original
Flow record netflow-original:
  Description: Traditional IPv4 input NetFlow with origin ASs
  No. of users: 1
  Template ID: 261
  Fields:
    match ipv4 source address
    match ipv4 destination address
    match ip protocol
    match ip tos
    match transport source-port
    match transport destination-port
    match interface input
    match interface output
    match flow direction
    collect routing source as
    collect routing destination as
```

```
collect routing next-hop address ipv4
collect transport tcp flags
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

Set up NetFlow Exporter

Run these commands.

```
flow exporter FortiSIEMFlowAnalyzer
description export netflow to FortiSIEM
destination <FortiSIEMIp>export Version 9
transport udp 2055
source vlan613
```

Associate the Record to the Exporter Using a Flow Monitor

In this example the flow monitor is called FortiSIEMMonitoring.

Run these commands.

```
flow monitor FortiSIEMMonitoring
exporter FortiSIEMFlowAnalyzer
record netflow-original
```

Apply the Flow Monitor to Every Interface

Run these commands.

```
interface Vlan612
ip flow monitor Monitortac7000 input
exit
interface Vlan613
ip flow monitor Monitortac7000 input
exit
```

You can now check the configuration using the show commands.

Settings for Access Credentials

For SNMP, Telnet, and SSH access credentials, see [Access Credentials](#).

Cisco ONS

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial Number, software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP Trap		Alerts	Availability and Performance Monitoring

Event Types

Over 1,800 event types defined. In **ADMIN > Device Support > Event Types**, search for "Cisco-ONS" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco ONS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco Viptela SDWAN Router

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Syslog	Host name and Device Type from LOG	Over 280 log types	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "viptela" to see the event types associated with this device.

Rules

None

Reports

None

Configuration

Configure Cisco Viptela to send syslog in the supported format to FortiSIEM. No configuration is required in FortiSIEM.

Sample Events

```
<190>430: *Dec 9 05:41:47.025: %Cisco-SDWAN-Router-OMPD-6-INFO-400005: R0/0: OMPD: Number of vSmarts connected : 2
```

```
CDATA[<187>154: *Aug 23 19:57:51.681: %Cisco-SDWAN-RP_0-OMPD-3-ERR0-400002: R0/0: OMPD: vSmart  
peer 1.1.1.5 state changed to Init
```

Dell Force10 Router and Switch

Support Added: FortiSIEM 4.7.2

Last Modification: FortiSIEM 6.4.0

Vendor Version Tested: Dell Force10 S4048T-ON

Vendor: Dell

Product Information: www.dell.com

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial number, Software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), CPU utilization, Hardware Status	Availability and Performance Monitoring
Syslog			Security and Compliance
Telnet/SSH	Running and Startup configurations	Startup Configuration Change, Difference between Running and Startup configurations	Change monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "force10" to see the event types associated with this device.

The following event types are available:

- Dell-Force10-IFMGR-OSTATE_DN
- Dell-Force10-IFMGR-OSTATE_UP
- Dell-Force10-SEC_LOGIN_SUCCESS

- Dell-Force10-FILEMGR-FILESAVED
- Dell-Force10-SEC_LOGIN_FAILURE
- Dell-Force10-TACACS_ACCESS_ACCEPTED
- Dell-Force10-SSH2-CONF
- Dell-Force10-SYS-CONFIG_I

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Rules**, search for "force10" in the main content panel **Search...** field.

The following reports are available:

- Dell Force10 Interface Extended Performance Metrics
- Dell Force 10 Performance By Component

Configuration

- [SNMP](#)
- [Syslog](#)
- [Telnet/SSH](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

The syslog format should be the same as that shown in the example.

Example Syslog

```
Feb 11 09:50:21: %STKUNIT0-M:CP %IFMGR-5-OSTATE_UP: Changed interface state to up: Te 0/30
190>Jan 6 07:34:34: host1: %STKUNIT0-M:CP %ARPMGR-6-MAC_CHANGE: IP-4-ADDRMOVE: IP address
10.1.48.14 is moved from MAC address 52:54:00:16:5a:74 to MAC address 52:54:00:22:c7:81 .
```

```
<189>Jan 4 08:08:43: host1: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user user1
on line vty0 ( 10.1.48.201 )
>110>1 2017-01-09T15:41:53.191+08:00 p01-ctl-sw2-d5c2f1 - SEC LOGOUT - INFO: Exec session is
terminated for user user2 on line vty0 ( 192.168.128.202 )
Feb 11 08:36:21 utc: %STKUNIT0-M:CP %IFMGR-5-OSTATE_DN: Changed interface state to down: Te 0/31
```

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device. To initiate discovery and monitoring of your device over this protocol, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

- show startup-config
- show running-config
- show version
- show ip route
- enable
- terminal pager 0

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Dell N-Series Switch

Support Added: FortiSIEM 4.7.2

Last Modification: FortiSIEM 6.3.1

Vendor Version Tested: Not Provided

Vendor: Dell

Product Information: www.dell.com

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c)		Hardware Status (Power Supply, Fan)	Availability Monitoring
SSH		Configuration	Change management
Syslog			Security and Compliance

Event Types

- CPU Monitoring: PH_DEV_MON_SYS_CPU_UTIL
- Memory Monitoring: PH_DEV_MON_SYS_MEM_UTIL

- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL
- Hardware Status: PH_DEV_MON_HW_STATUS
- Configuration Change: PH_DEV_MON_CHANGE_STARTUP_CONFIG
- Dell-NSeries-Generic
- Dell-NSeries-Success
- Dell-NSeries-Failed
- Dell-NSeries-Link-Up
- Dell-NSeries-Link-Down
- Dell-NSeries-Logout
- Dell-NSeries-Session-Created
- Dell-NSeries-Temp-Warning
- Dell-NSeries-Temp-Normal
- Dell-NSeries-User-Command
- Dell-NSeries-Invalid-Packet
- Dell-NSeries-SpanningTree-Change
- Dell-NSeries-SpanningTree-Learning-To-Forwarding
- Dell-NSeries-SpanningTree-Learning-To-Blocking
- Dell-NSeries-SpanningTree-Forwarding-To-Blocking
- Dell-NSeries-SpanningTree-Blocking-To-Forwarding

Rules

- [Availability](#)
- [Performance \(Fixed Threshold\)](#)
- [Performance \(Dynamic Threshold Based on Baselines\)](#)
- [Change](#)

Availability

- Network Device Degraded - Lossy Ping Response
- Network Device Down - no ping response
- Network Device Interface Flapping
- Critical Network Device Interface Staying Down
- Non-critical Network Device Interface Staying Down
- Network Device Hardware Warning
- Network Device Hardware Critical

Performance (Fixed Threshold)

- Network CPU Warning
- Network CPU Critical
- Network Memory Warning
- Network Memory Critical

- Network Intf Error Warning
- Network Intf Error Critical
- Network Intf Util Warning
- Network Intf Util Critical

Performance (Dynamic Threshold Based on Baselines)

- Sudden Increase In System CPU Usage
- Sudden Increase in System Memory Usage
- Sudden Increase in Network Interface Traffic
- Sudden Increase in Network Interface Errors

Change

- Startup Config Change

Reports

- [Availability](#)
- [Performance](#)
- [Change](#)

Availability

- Availability: Router/Switch Ping Monitor Statistics

Performance

- Performance: Top Routers Ranked By CPU Utilization
- Performance: Top Routers By Memory Utilization
- Performance: Top Router Network Intf By Util, Error, Discards
- Top Routers/Switches by Business Hours Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by Business Hours System Uptime Pct (Achieved System SLA)
- Top Routers/Switches by Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by System Uptime Pct (Achieved System SLA)
- Top Router Interfaces by Days-since-last-use

Change

- Change: Router Config Changes Detected Via Login

Configuration

- [SNMP](#)
- [Syslog](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

The syslog format should be the same as that shown in the example.

Example Syslog

```
<187> Sep 24 13:17:56 Ashley N3048P Switch Stack 1-1 IPV6[dtlTask]: ip6map.c(3787) 89904 %%  
Received invalid ip6 packet on V11: TC 0xf3, flow 663552, length 65152, next head 0, hop lim 0,  
src 8100:c8::f21f:afff:fedf:2080, dst ff02::1:ffdf:2080.  
<187>1 Jan 9 16:03:07.000 192.168.0.15-1 DRIVER[117467844]: broad_hpc_drv.c(4362) 230149630 %%  
Unit: 0 Blk: 3 MMU MTRO PAR generic parity error.
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell NSeries
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Dell PowerConnect Switch and Router

Support Added: FortiSIEM 4.7.2

Last Modification: FortiSIEM 6.3.1

Vendor Version Tested: Not Provided

Vendor: Dell

Product Information: www.dell.com

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial number, Software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), CPU utilization, Hardware Status	Availability and Performance Monitoring
Syslog			Security and Compliance
Telnet/SSH	Running and Startup configurations	Startup Configuration Change, Difference between Running and Startup configurations	Change monitoring

Event Types

There are no event types defined specifically for this device, but event types are prefixed with "Dell-PowerConnect-".

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog](#)
- [Telnet/SSH](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

The syslog format should be the same as that shown in the example.

Example Syslog

```
<189> Apr 13 15:21:08 192.168.5.43-1 CLI_WEB[103917236]: cmd_logger_api.c(140) 5203 %%  
WEB:192.168.5.101:admin:User requested /VLAN_Membership.html url  
<189> Apr 13 15:21:18 192.168.5.43-1 CLI_WEB[103917236]: cmd_logger_api.c(140) 5204 %%  
WEB:192.168.5.101:admin:User admin logged out  
<190> Apr 13 15:19:32 192.168.5.43-1 CLI_WEB[103917236]: cmd_logger_api.c(260) 5199 %%  
[CLI:admin:192.168.5.15] User has succesfully logged in  
<189> Jun 30 16:04:24 Switch-2-1 TRAPMGR[trapTask]: traputil.c(735) 47619 %% 'startup-config' has  
changed.  
<190> Jun 30 16:04:24 Switch-2-1 UNITMGR[emWeb]: unitmgr.c(6778) 47618 %% Configuration  
propagation successful for config type 0
```

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the

device. To initiate discovery and monitoring of your device over this protocol. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

- `show startup-config`
- `show running-config`
- `show version`
- `show ip route`
- `enable`
- `terminal pager 0`

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell PowerConnect
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Foundry Networks IronWare Router and Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Ironware version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
Telnet/SSH	Running and startup configuration	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
SNMP (V1, V2c)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location
Syslog	Device type	System logs and traffic logs matching acl statements	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "foundry-ironware" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Telnet/SSH](#)
- [Syslog](#)
- [Sample Parsed PowerConnect Syslog Message](#)

SNMP

1. Log in to the device manager for your switch or router with administrative privileges.
2. Enter configuration mode.
3. Run these commands to set the community string and enable the SNMP service.

```
snmp-server community <community> R0
snmp-server enable vlan <vlan id>
```

4. Exit config mode.
5. Save the configuration.

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

Syslog

1. Log in to the device manager for your switch or router with administrative privileges.
2. Enter configuration mode.
3. Run this command to set your FortiSIEM virtual appliance as the recipient of syslog from your router or switch.


```
logging host <FortiSIEM Ip>
```

4. Exit config mode.
5. Save the configuration.

Sample Parsed PowerConnect Syslog Message

```
<14>SJ-Dev-A-Fdy-FastIron, running-config was changed from console

<14>SJ-Dev-A11-Fdy-FastIron, startup-config was changed from telnet client 192.168.20.18
<14>SJ-Dev-A-Fdy-FastIron, phoenix_agent login to USER EXEC mode

<14>SJ-Dev-A-Fdy-FastIron, Interface ethernet3, state up

<14>SJ-Dev-A-Fdy-FastIron, Interface ethernet 20/3, state up

<12>SJ-QA-A-Fdy-BigIron, list 100 permitted udp 173.9.142.98(ntp)(Ethernet 2/1 0004.23ce.ba11) ->
172.16.20.121(ntp), 1 event(s)

<14>SJ-Dev-A-Fdy-FastIron, Bridge root changed, vlan 3, new root ID 80000004806137c6, root
interface 3

<14>SJ-QA-A-Fdy-BigIron, VLAN 4 Port 2/7 STP State -> DISABLED (PortDown)

Jun  4 15:51:18 172.16.20.99 Security: telnet logout by admin from src IP 137.146.28.75, src MAC
000c.dbff.6d00

Jun  4 15:51:12 172.16.20.100 System: Interface ethernet 4/9, state down

Jun  4 03:12:53 172.16.20.100 ACL: ACL: List GWI-in permitted tcp 61.158.162.230(6000)(Ethernet
1/4 0023.3368.f500) -> 137.146.0.0(8082), 1 event(s)

Jun  4 02:54:31 172.16.20.100 ACL: ACL: List XCORE denied udp 137.146.28.75(55603)(Ethernet 1/1
000c.dbde.6000) -> 137.146.3.35(snmp), 1 event(s)

Jun  4 01:49:09 172.16.20.100 STP: VLAN 3104 Port 4/22 STP State -> LEARNING (FwdDlyExpiry)
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

- [Foundry Ironware](#)
- [SNMP Access Credentials for All Devices](#)
- [Telnet Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

Foundry Ironware

Setting	Value
Name	<set name>
Device Type	Foundry Ironware
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

HP/3Com ComWare Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware status: Power Supply, Fan, Temperature	Availability and Performance Monitoring
SNMP (V1, V2c, V3)		Hardware status: Temperature	Availability
Syslog		System logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "comware" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog](#)
- [Example Syslog for ComWare Switch Messages](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Example Syslog for ComWare Switch Messages

```
%Apr 2 11:38:11:113 2010 H3C DEVD/3/BOARD REBOOT:Chasis 0 slot 2 need be rebooted automatically!
%Sep 22 20:38:32:947 2009 H3C DEVD/4/BRD MISPLUG: The board or subcard in slot 1 is not supported.
%Sep 22 20:38:32:947 2009 H3C DEVD/4/BRD MISPLUG: The board type of MR in 1 is different from the
Mate MR's, so the MR can't work properly.
%Sep 22 20:38:32:947 2009 H3C DEVD/2/BRD T00 HOT:Temperature of the board is too high!
%Sep 22 20:38:32:947 2009 H3C DEVD/2/ FAN CHANGE: Chassis 1: Fan communication state changed: Fan
1 changed to fault.
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	H3C Comware
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

HP ProCurve Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware status: Power Supply, Fan, Temperature	Availability and Performance Monitoring
Telnet/SSH	Running and startup configuration	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
SNMP (V1, V2c)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location

Event Types

In **ADMIN > Device Support > Event Types**, search for "procurve" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Telnet/SSH](#)

SNMP

1. Go to **Configuration > SNMP Community > V1/V2 Community**.
2. Enter a **Community Name**.
3. For **MIB-View**, select **Operator**.
4. For Write-Access, leave the selection cleared.
5. Click **Add**.

Telnet/SSH

1. Log into the device manager for your ProCurve switch.
2. Go to **Security > Device Passwords**.
3. Create a user and password for **Read-Write Access**.
Although FortiSIEM does not modify any configurations for your switch, Read-Write Access is needed to read the device configuration.
4. Go to **Security > Authorized Addresses** and add the FortiSIEM IP to Telnet/SSH.
This is an optional step.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	HP ProCurve
Access Protocol	See Access Credentials
Port	See Access Credentials

Setting	Value
Password config	See Password Configuration

HP Value Series (19xx) and HP 3Com (29xx) Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SSH		Configuration	Change management

Event Types

- CPU Monitoring: PH_DEV_MON_SYS_CPU_UTIL
- Memory Monitoring: PH_DEV_MON_SYS_MEM_UTIL
- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL
- Configuration Change: PH_DEV_MON_CHANGE_STARTUP_CONFIG

Rules

- [Availability](#)
- [Performance \(Fixed Threshold\)](#)
- [Performance \(Dynamic Threshold Based on Baselines\)](#)
- [Change](#)

Availability

- Network Device Degraded - Lossy Ping Response
- Network Device Down - no ping response
- Network Device Interface Flapping
- Critical Network Device Interface Staying Down
- Non-critical Network Device Interface Staying Down

Performance (Fixed Threshold)

- Network CPU Warning
- Network CPU Critical
- Network Memory Warning
- Network Memory Critical
- Network Intf Error Warning
- Network Intf Error Critical
- Network Intf Util Warning
- Network Intf Util Critical

Performance (Dynamic Threshold Based on Baselines)

- Sudden Increase In System CPU Usage
- Sudden Increase in System Memory Usage
- Sudden Increase in Network Interface Traffic
- Sudden Increase in Network Interface Errors

Change

- Startup Config Change

Reports

- [Availability](#)
- [Performance](#)
- [Change](#)

Availability

- Availability: Router/Switch Ping Monitor Statistics

Performance

- Performance: Top Routers Ranked By CPU Utilization
- Performance: Top Routers By Memory Utilization

- Performance: Top Router Network Intf By Util, Error, Discards
- Top Routers/Switches by Business Hours Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by Business Hours System Uptime Pct (Achieved System SLA)
- Top Routers/Switches by Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by System Uptime Pct (Achieved System SLA)
- Top Router Interfaces by Days-since-last-use

Change

- Change: Router Config Changes Detected Via Login

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	HP VSeries
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Hirschmann SCADA Firewalls and Switches

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
SNMP	Host Name	SNMP – Uptime, CPU, Memory, Interface utilization, hardware Status, OSPF metrics	Performance Monitoring

Event Types

The following event types are used for performance monitoring:

- PH_DEV_MON_SYS_UPTIME - Uptime monitoring
- PH_DEV_MON_SYS_CPU_UTIL – CPU utilization
- PH_DEV_MON_SYS_MEM_UTIL – Memory utilization
- PH_DEV_MON_NET_INTF_UTIL – Interface utilization
- PH_DEV_MON_HW_STATUS – Hardware status

Rules

All performance monitoring rules apply.

Reports

All performance monitoring reports apply.

Configuration

Configure Hirschmann firewalls and switches for SNMP V1/V2c/V3 discovery and performance monitoring. Define the basic SNMP credentials on FortiSIEM and discover these devices. See [SNMP Access Credentials](#).

Sample Events

The events are standard for all devices.

Juniper Networks JunOS Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, JunOS version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware status: Power Supply, Fan, Temperature	Availability and Performance Monitoring
Telnet/SSH	Running and startup configuration	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
SNMP (V1, V2c, V3)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location
Syslog		System logs and traffic logs matching acl statements	Availability, Security and Compliance
sflow		Traffic flow	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "junos" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog](#)
- [Sample JunOS Syslog Messages](#)
- [sFlow](#)

SNMP

1. Log in to the device manager for your JunOS switch with administrator privileges.
2. Go to **Configure > Services > SNMP**.
3. Under **Communities**, click **Add**.
4. Enter a **Community Name**.
5. Set **Authorization** to **read-only**.
6. Click **OK**.

Syslog

1. Log in to the device manager for your JunOS switch with administrator privileges.
2. Go to **Dashboard > CLI Tools > CLI Editor**.
Edit the syslog section to send syslog to FortiSIEM.
3. **JunOS Syslog Configuration**

```
system {
  ....
  syslog {
    user * {
      any emergency;
```

```

    }
    host <FortiSIEM Ip> {
        any any;
        explicit-priority;
    }
    file messages {
        any notice;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
    time-format year millisecond;
}
....
}

```

4. Click **Commit**.

Sample JunOS Syslog Messages

```

190>May 11 13:54:10 20.20.20.20 mgd[5518]: UI_LOGIN_EVENT: User 'example_user' login, class 'j-
super-user' [5518], ssh-connection '192.168.28.21 39109 172.16.5.64 22', client-mode 'cli'

```

```

<38>Nov 18 17:50:46 login: %AUTH-6-LOGIN_INFORMATION: User phoenix_agent logged in from host
192.168.20.116 on device tty0

```

sFlow

Routing the sFlow Datagram in EX Series Switches

According to Juniper documentation, the sFlow datagram **cannot** be routed over the management Ethernet interface (me0) or virtual management interface (vme0) in an EX Series switch implementation. It can only be exported over the network Gigabit Ethernet or 10-Gigabit Ethernet ports using valid route information in the routing table.

1. Log in to the device manager for your JunOS switch with administrator privileges.
2. Go to **Configure > CLI Tools > Point and Click CLI**.
3. Expand **Protocols** and select **sflow**.
4. Next to **Collector**, click **Add new entry**.
5. Enter the **IP** address for your FortiSIEM virtual appliance.
6. For **UDP Port**, enter **6343**.
7. Click **Commit**.
8. Next to **Interfaces**, click **Add new entry**.
9. Enter the **Interface Name** for all interfaces that will send traffic over sFlow.
10. Click **Commit**.

11. To disable the management port, go to **Configure > Management Access**, and remove the address of the management port.
You can also disconnect the cable.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Juniper JunOS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

MikroTik Router

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	MikroTik RouterOS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Nortel ERS and Passport Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c)		Hardware status: Temperature	
SNMP (V1, V2c, V3)		Layer 2 port mapping: associating switch ports to directly connected host IP/MAC addresses	Identity and location table; Topology

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Nortel ERS / Nortel Passport
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Secure Access Service Edge

FortiSIEM supports these secure access service edge (SASE).

- [Zscaler Private Access \(ZPA\)](#)

Zscaler Private Access (ZPA)

Zscaler Private Access (ZPA) is a Secure Access Service Edge (SASE) service that provides secure, direct access to private applications. ZPA is essentially an agent based ZTNA solution that routes traffic to protected endpoints in the ZPA cloud which has the necessary resource access behind it. This is considered more secure than granting access to an entire subnet like with a traditional VPN and even restricts to where you don't have access to any protocol on the VPN, only the specific service if authenticated (Zero Trust Network Access).

ZPA service uses the LSS (Log Streaming Service) to send logs a SIEM collector via Syslog over TCP (insecure) or Syslog over TLS (secure).

The following topics are covered:

- [Information Collected](#)
- [Configuration](#)

Information Collected

The following log types are collected:

ZPA Event Type	Event Type Prefix for FortiSIEM Events	Collection Method
User Activity	Zscaler-ZPA-UserActivity (4 event types)	Syslog
User Status	Zscaler-ZPA-UserStatus (4 event types)	Syslog
Browser Access	Zscaler-ZPA-BrowserAccess (9 event types)	Syslog
Audit Logs	Zscaler-ZPA-Audit (16 event types)	Syslog
App Connector Status	Zscaler-ZPA-AppConnStatus (4 event types)	Syslog
App Protection/Web Inspection	Zscaler-ZPA-AppProtect (9 event types)	Syslog

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

Three steps are involved. Also, no configuration is required on FortiSIEM.

1. Add App Connectors.
2. Deploy App Connectors.

3. Set up Log Streaming Service (LSS) Forwarding Feed for each log type to a FortiSIEM collector using TCP syslog (or syslog over TLS).

Step 1: Add App Connectors

Reference: <https://help.zscaler.com/zpa/configuring-connectors>

1. Go to Configuration & Control > Private Infrastructure > App Connector Management > App Connectors.
2. Click **Add App Connector**.
3. In the Add App Connector window, take the following steps.

Tab	Configuration Instructions
Choose Key	1. Select Choose an existing provisioning key and select the key from the drop-down or Create a new provisioning key. 2. Click Next.
Signing Certificate	1. From the drop-down, select the certificate that ZPA uses to sign certificates it issues to App Connector. 2. Click Next. If you need to create a new certificate, see instructions here.
App Connector Group	1. Choose Select an existing App Connector Group and select an App Connector group or Add App Connector Group and create one following the instructions here. 2. Click Next.
Create Provisioning Key	Configure as needed, and when done, click Next . See instructions here .
Review	Review your settings, and click Save .
Review Documentation	1. Copy your Provisioning Key information by clicking the Copy icon, then save this in a secure location. 2. Click Done.

Step 2: Deploy App Connectors

Use the following references to deploy your App Connectors.

References:

- <https://help.zscaler.com/zpa/about-deploying-connectors>
- <https://help.zscaler.com/zpa/app-connector-management/app-connector-deployment-guides-supported-platforms>

The location of where to deploy the App Connector is up to you (Cloud environment or on premise, however it should be geographically close to a FortiSIEM collector). A standard distributed FortiSIEM design is to have a FortiSIEM collector in each major data center where you operate, although that design is not required, as long as the App Connector can reach the FortiSIEM collector on TCP 514 (Reliable Syslog) or TCP 6514 (Syslog over TLS).

Step 3: Set up Log Streaming Service (LSS)

Log Streaming Service (LSS) sends logs to a configured App Connector, which is a VM deployed in your on premise or cloud environment. ZScaler sends configured logs to this connector, and the connector is then configured to forward syslog to a FortiSIEM collector.

Reference: <https://help.zscaler.com/zpa/configuring-log-receiver>

To add a Log Receiver, take the following steps.

1. Go to Configuration & Control > Private Infrastructure > Log Streaming Service > Log Receivers.
2. Click **Add Log Receiver**.
3. From the Add Log Receiver window, configure the following tabs:

Tab	Configuration Instructions
Log Receiver	1. In the Name field, enter a name for the log receiver. The name cannot contain special characters, with the exception of periods (.), hyphens (-), and underscores (_). E.g. fortisem_collector_01 2. (Optional) In the Description field, enter a description. 3. In the Domain or IP Address field, enter the fully qualified domain name (FQDN) or IP address of the FortiSIEM collector. This FortiSIEM collector should be reachable outbound from the perspective of the App Connector that is forwarding the logs. 4. In the TCP Port field, enter the TCP port number used by the log receiver. Typically, 514. 5. For TLS Encryption, enable to encrypt traffic between the App Connector and the FortiSIEM collector (optional). If enabled, the collector must have a trusted TLS certificate. 6. From the App Connector Groups drop-down, choose the App Connector groups that can forward logs to the receiver, and click Done. Note: You can search for a specific group, click Select All to apply all groups, or click Clear Selection to remove all selections. 7. When done, click Next.
Log Stream	Take the following steps: 1. From the Log Type drop-down, select User Activity. 2. For Log Template, select JSON. 3. For Log Stream Content, copy/paste the User Activity Custom Log Format below, excluding the "=Begins=" and "=Ends=" separation lines. =User Activity Custom Log Begins= <pre> {"sourcetype" : "zscalerlss-user_activity", "LogTimestamp": %j {LogTimestamp:time}, "Customer": %j{Customer}, "SessionID": %j {SessionID}, "ConnectionID": %j{ConnectionID}, "InternalReason": %j {InternalReason}, "ConnectionStatus": %j{ConnectionStatus}, "IPProtocol": %d {IPProtocol}, "DoubleEncryption": %d{DoubleEncryption}, "Username": %j {Username}, "ServicePort": %d{ServicePort}, "ClientPublicIP": %j </pre>

Tab

Configuration Instructions

```
{ClientPublicIP},"ClientPrivateIP": %j{ClientPrivateIP},"ClientLatitude": %f
{ClientLatitude},"ClientLongitude": %f{ClientLongitude},"ClientCountryCode":
%j{ClientCountryCode},"ClientZEN": %j{ClientZEN},"Policy": %j
{Policy},"Connector": %j{Connector},"ConnectorZEN": %j
{ConnectorZEN},"ConnectorIP": %j{ConnectorIP},"ConnectorPort": %d
{ConnectorPort},"Host": %j{Host},"Application": %j{Application},"AppGroup": %j
{AppGroup},"Server": %j{Server},"ServerIP": %j{ServerIP},"ServerPort": %d
{ServerPort},"PolicyProcessingTime": %d
{PolicyProcessingTime},"ServerSetupTime": %d
{ServerSetupTime},"TimestampConnectionStart": %j
{TimestampConnectionStart:iso8601},"TimestampConnectionEnd": %j
{TimestampConnectionEnd:iso8601},"TimestampCATx": %j
{TimestampCATx:iso8601},"TimestampCARx": %j
{TimestampCARx:iso8601},"TimestampAppLearnStart": %j
{TimestampAppLearnStart:iso8601},"TimestampZENFirstRxClient": %j
{TimestampZENFirstRxClient:iso8601},"TimestampZENFirstTxClient": %j
{TimestampZENFirstTxClient:iso8601},"TimestampZENLastRxClient": %j
{TimestampZENLastRxClient:iso8601},"TimestampZENLastTxClient": %j
{TimestampZENLastTxClient:iso8601},"TimestampConnectorZENSetupComplete": %j
{TimestampConnectorZENSetupComplete:iso8601},"TimestampZENFirstRxConnector":
%j{TimestampZENFirstRxConnector:iso8601},"TimestampZENFirstTxConnector": %j
{TimestampZENFirstTxConnector:iso8601},"TimestampZENLastRxConnector": %j
{TimestampZENLastRxConnector:iso8601},"TimestampZENLastTxConnector": %j
{TimestampZENLastTxConnector:iso8601},"ZENTotalBytesRxClient": %d
{ZENTotalBytesRxClient},"ZENBytesRxClient": %d
{ZENBytesRxClient},"ZENTotalBytesTxClient": %d
{ZENTotalBytesTxClient},"ZENBytesTxClient": %d
{ZENBytesTxClient},"ZENTotalBytesRxConnector": %d
{ZENTotalBytesRxConnector},"ZENBytesRxConnector": %d
{ZENBytesRxConnector},"ZENTotalBytesTxConnector": %d
{ZENTotalBytesTxConnector},"ZENBytesTxConnector": %d
{ZENBytesTxConnector},"Idp": %j{Idp},"ClientToClient": %j{c2c}}\n
```

=User Activity Custom Log Ends=

4. Repeat [Log Stream steps 1-3](#), but with the following changes.
 - a. For step 1, replace **User Activity** with each of the following log types (**User Status, Browser Access, Audit Logs, App Connector Status, App Protection/Web Inspection**).
 - b. In step 3, copy/paste their respective Custom Log Format from the [FortiSIEM Supported Custom Log Formats Table](#) below.
5. Click **Next** when done with configuring all log types.

Review

Examine your configuration. When done, click **Save**.

FortiSIEM Supported Custom Log Formats

Log Type	Custom Log Format
User Status	<pre> {"sourcetype":"zscalerlss-user_status","LogTimestamp": %j {LogTimestamp:time},"Customer": %j{Customer},"Username": %j {Username},"SessionID": %j{SessionID},"SessionStatus": %j {SessionStatus},"Version": %j{Version},"ZEN": %j{ZEN},"CertificateCN": %j {CertificateCN},"PrivateIP": %j{PrivateIP},"PublicIP": %j{PublicIP},"Latitude": %f{Latitude},"Longitude": %f{Longitude},"CountryCode": %j {CountryCode},"TimestampAuthentication": %j {TimestampAuthentication:iso8601},"TimestampUnAuthentication": %j {TimestampUnAuthentication:iso8601},"TotalBytesRx": %d {TotalBytesRx},"TotalBytesTx": %d{TotalBytesTx},"Idp": %j{Idp},"Hostname": %j {Hostname},"Platform": %j{Platform},"ClientType": %j {ClientType},"TrustedNetworks": [%j(,){TrustedNetworks}], "TrustedNetworksNames": [%j(,){TrustedNetworksNames}], "SAMLAttributes": %j {SAMLAttributes},"PosturesHit": [%j(,){PosturesHit}], "PosturesMiss": [%j(,){ PosturesMiss}], "ZENLatitude": %f{ZENLatitude},"ZENLongitude": %f {ZENLongitude},"ZENCountryCode": %j{ZENCountryCode},"FQDNRegistered": %j{fqdn_ registered},"FQDNRegisteredError": %j{fqdn_register_error}}\n </pre>
Browser Access	<pre> {"sourcetype":"zscalerlss-browser_access","LogTimestamp":%j {LogTimestamp:time},"ConnectionID":%j{ConnectionID},"Exporter":%j {Exporter},"TimestampRequestReceiveStart":%j {TimestampRequestReceiveStart:iso8601},"TimestampRequestReceiveHeaderFinish":%j {TimestampRequestReceiveHeaderFinish:iso8601},"TimestampRequestReceiveFinish":%j {TimestampRequestReceiveFinish:iso8601},"TimestampRequestTransmitStart":%j {TimestampRequestTransmitStart:iso8601},"TimestampRequestTransmitFinish":%j {TimestampRequestTransmitFinish:iso8601},"TimestampResponseReceiveStart":%j {TimestampResponseReceiveStart:iso8601},"TimestampResponseReceiveFinish":%j {TimestampResponseReceiveFinish:iso8601},"TimestampResponseTransmitStart":%j {TimestampResponseTransmitStart:iso8601},"TimestampResponseTransmitFinish":%j {TimestampResponseTransmitFinish:iso8601},"TotalTimeRequestReceive":%d {TotalTimeRequestReceive},"TotalTimeRequestTransmit":%d {TotalTimeRequestTransmit},"TotalTimeResponseReceive":%d {TotalTimeResponseReceive},"TotalTimeResponseTransmit":%d {TotalTimeResponseTransmit},"TotalTimeConnectionSetup":%d {TotalTimeConnectionSetup},"TotalTimeServerResponse":%d {TotalTimeServerResponse},"Method":%j{Method},"Protocol":%j{Protocol},"Host":%j {Host},"URL":%j{URL},"UserAgent":%j{UserAgent},"XFF":%j{XFF},"NameID":%j {NameID},"StatusCode":%d{StatusCode},"RequestSize":%d {RequestSize},"ResponseSize":%d{ResponseSize},"ApplicationPort":%d {ApplicationPort},"ClientPublicIp":%j{ClientPublicIp},"ClientPublicPort":%d {ClientPublicPort},"ClientPrivateIp":%j{ClientPrivateIp},"Customer":%j {Customer},"ConnectionStatus":%j{ConnectionStatus},"ConnectionReason":%j {ConnectionReason},"Origin":%j{Origin},"CorsToken":%j{CorsToken}}\n </pre>

Log Type	Custom Log Format
Audit Logs	<pre> {"sourcetype":"zscalerlss-audit_logs","ModifiedTime":%j {modifiedTime:iso8601},"CreationTime":%j{creationTime:iso8601},"ModifiedBy":%d {modifiedBy},"RequestID":%j{requestId},"SessionID":%j {sessionId},"AuditOldValue":%j{auditOldValue},"AuditNewValue":%j {auditNewValue},"AuditOperationType":%j{auditOperationType},"ObjectType":%j {objectType},"ObjectName":%j{objectName},"ObjectID":%d{objectId},"CustomerID":%d {customerId},"User":%j{modifiedByUser},"ClientAuditUpdate":%d{isClientAudit}}\n </pre>
App Connector Status	<pre> {"sourcetype":"zscalerlss-app_connector_status","LogTimestamp": %j {LogTimestamp:time},"Customer": %j{Customer},"SessionID": %j {SessionID},"SessionType": %j{SessionType},"SessionStatus": %j {SessionStatus},"Version": %j{Version},"Platform": %j{Platform},"ZEN": %j {ZEN},"Connector": %j{Connector},"ConnectorGroup": %j {ConnectorGroup},"PrivateIP": %j{PrivateIP},"PublicIP": %j{PublicIP},"Latitude": %f{Latitude},"Longitude": %f{Longitude},"CountryCode": %j {CountryCode},"TimestampAuthentication": %j {TimestampAuthentication:iso8601},"TimestampUnAuthentication": %j {TimestampUnAuthentication:iso8601},"CPUUtilization": %d {CPUUtilization},"MemUtilization": %d{MemUtilization},"ServiceCount": %d {ServiceCount},"InterfaceDefRoute": %j{InterfaceDefRoute},"DefRouteGW": %j {DefRouteGW},"PrimaryDNSResolver": %j{PrimaryDNSResolver},"HostUpTime": %j {HostUpTime},"ConnectorUpTime": %j{ConnectorUpTime},"NumOfInterfaces": %d {NumOfInterfaces},"BytesRxInterface": %d{BytesRxInterface},"PacketsRxInterface": %d{PacketsRxInterface},"ErrorsRxInterface": %d {ErrorsRxInterface},"DiscardsRxInterface": %d {DiscardsRxInterface},"BytesTxInterface": %d {BytesTxInterface},"PacketsTxInterface": %d {PacketsTxInterface},"ErrorsTxInterface": %d {ErrorsTxInterface},"DiscardsTxInterface": %d {DiscardsTxInterface},"TotalBytesRx": %d{TotalBytesRx},"TotalBytesTx": %d {TotalBytesTx}}\n </pre>
App Protection/Web Inspection	<pre> {"sourcetype":"zscalerlss-app_protection","LogTimestamp": %j {LogTimestamp:time},"Customer": %j{Customer}, "ConnectionID": %j{ConnectionID}, "UserID": %j{UserID}, "AssistantID": %j{AssistantID}, "ExchangeSequenceIndex": %d{ExchangeSequenceIndex}, "TimestampRequestReceiveStart": %d {TimestampRequestReceiveStart}, "TimestampRequestReceiveHeaderFinish": %d {TimestampRequestReceiveHeaderFinish}, "TimestampRequestReceiveFinish": %d {TimestampRequestReceiveFinish}, "TimestampRequestTransmitStart": %d {TimestampRequestTransmitStart}, "TimestampRequestTransmitFinish": %d {TimestampRequestTransmitFinish}, "TimestampResponseReceiveFinish": %d {TimestampResponseReceiveFinish}, "TimestampResponseTransmitStart": %d {TimestampResponseTransmitStart}, "TimestampResponseTransmitFinish": %d {TimestampResponseTransmitFinish}, "TotalTimeRequestReceive": %d {TotalTimeRequestReceive}, "TotalTimeRequestTransmit": %d </pre>

Log Type	Custom Log Format
	<pre> {TotalTimeRequestTransmit}, "TotalTimeResponseReceive": %d {TotalTimeResponseReceive}, "TotalTimeResponseTransmit": %d {TotalTimeResponseTransmit}, "Domain": %j{Domain}, "Method": %j{Method}, "Protocol": %j{Protocol}, "ProtocolVersion": %j{ProtocolVersion}, "ContentType": %j{ContentType}, "ContentEncoding": %j{ContentEncoding}, "TransferEncoding": %j {TransferEncoding}, "Host": %j{Host}, "Destination": %j{Destination}, "OriginDomain": %j{OriginDomain}, "URL": %j{URL}, "UserAgent": %j{UserAgent}, "HTTPError": %j{HTTPError}, "ClientPublicIp": %j{ClientPublicIp}, "ClientPort": %d{ClientPort}, "UpgradeHeaderPresent": %d{UpgradeHeaderPresent}, "StatusCode": %d{StatusCode}, "RequestHdrSize": %d{RequestHdrSize}, "ResponseHdrSize": %d {ResponseHdrSize}, "RequestBodySize": %d{RequestBodySize}, "ResponseBodySize": %d{ResponseBodySize}, "Application": %d{Application}, "ApplicationGroup": %d {ApplicationGroup}, "InspectionPolicy": %d{InspectionPolicy}, "InspectionProfile": %d{InspectionProfile}, "ParanoiaLevel": %d{ParanoiaLevel}, "InspectionControlsHitCount": %d{InspectionControlsHitCount}, "InspectionRuleProcessingTime": %d{InspectionRuleProcessingTime}, "InspectionReqHeadersProcessingTime": %d{InspectionReqHeadersProcessingTime}, "InspectionReqBodyProcessingTime": %d{InspectionReqBodyProcessingTime}, "InspectionRespHeadersProcessingTime": %d{InspectionRespHeadersProcessingTime}, "InspectionRespBodyProcessingTime": %d{InspectionRespBodyProcessingTime}, "CertificateId": %d{CertificateId}, "DoubleEncryption": %d{DoubleEncryption}, "SSLInspection": %d{SSLInspection}, "TotalBytesProcessed": %d {TotalBytesProcessed}}\n </pre>

Security Gateways

FortiSIEM supports these security gateways for discovery and monitoring.

- [Barracuda Networks Spam Firewall](#)
- [Blue Coat Web Proxy](#)
- [Cisco IronPort Mail Gateway](#)
- [Cisco IronPort Web Gateway](#)
- [Fortinet FortiMail](#)
- [Fortinet FortiProxy](#)
- [Fortinet FortiWeb](#)
- [Imperva SecureSphere DB Monitoring Gateway](#)
- [Imperva SecureSphere Security Gateway](#)
- [McAfee Web Gateway](#)
- [Microsoft ISA Server](#)
- [Proofpoint](#)
- [Squid Web Proxy](#)
- [SSH Comm Security CryptoAuditor](#)
- [Thales Vormetric Data Security Manager](#)
- [Websense Web Filter](#)

Barracuda Networks Spam Firewall

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, Interfaces, Serial number	CPU utilization, Memory utilization, Interface Utilization	Performance Monitoring
Syslog		Various syslog - scenarios include - mail scanned and allowed/denied/quarantined etc; mail sent and reject/delivered/defer/expired; mail received and allow/abort/block/quarantined etc.	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "barracuda" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog](#)

- [Sample Parsed Barracuda Spam Firewall Syslog Message](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Sample Parsed Barracuda Spam Firewall Syslog Message

```
<23>inbound/pass1[923]: 127.0.0.1 1300386119-473aa6a90001-sB89EM 0 0 RECV - 1 4D760309475 250
2.6.0 <E6BB7C56C6761D42AEAFBF7FC6E17E920156A38D@USNSSEXC174.us.world.example.com> Queued mail for
delivery

<23>scan[9390]: mail.example.net[207.65.119.227] 1300386126-4739a8be0001-R60EVB 1300386126
1300386128 SCAN - release@subject.example.net user1@example.com - 7 61 - SZ:34602 SUBJ:Email
Subject Information April 24, 2012
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Barracuda Spam Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Blue Coat Web Proxy

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, Interfaces, Serial number	CPU utilization, Memory utilization	Performance Monitoring
SNMP		Proxy performance: Proxy cache object count, Proxy-to-server metrics: HTTP errors, HTTP requests, HTTP traffic (KBps); Server-to-proxy metrics: HTTP traffic (KBps), Client-to-proxy metrics: HTTP requests, HTTP Cache hit, HTTP errors, HTTP traffic (KBps); Proxy-to-client metrics: HTTP traffic (KBytes)	Performance Monitoring
Syslog		Admin authentication success and failure	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "blue coat" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog](#)
- [Sample Syslog Event](#)
- [Access Logging](#)

SNMP

The following procedures enable FortiSIEM to discover Bluecoat web proxy.

1. Log in to your Blue Coat management console.
2. Go to **Maintenance > SNMP**.
3. Under **SNMP General**, select **Enable SNMP**.
4. Under Community Strings, click Change Read Community, and then enter a community string that FortiSIEM can use to access your device.
5. Click **OK**.

Syslog

Syslog is used by Blue Coat to send audit logs to FortiSIEM.

1. Log in to your Blue Coat management console.
2. Go to **Maintenance > Event Logging**.
3. Under **Level**, select **Severe Errors, Configuration Events, Policy Messages**, and **Informational**.
4. Under **Syslog**, enter the IP address of your FortiSIEM virtual appliance for **Loghost**.
5. Select **Enable syslog**.
6. Click **Apply**.

Sample Syslog Event

```
<111>2020-12-04T00:15:15 Bluecoatsyslog time-taken="39", c-ip="105.128.196.10", cs-username="user.example", cs-auth-group="-", cs-categories="Web Ads/Analytics", sc-status="200", cs-uri-scheme="https", cs-host="cdn.somedomain.com", cs-uri-port="443", cs-uri-extension="js", cs (User-Agent)="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36", cs-uri-path="/base_src.js", cs-method="GET", cs-bytes="629", r-ip="123.123.25.25", rs(Content-Type)="application/javascript", s-action="TCP_NC_MISS", s-ip="212.212.212.5", sc-bytes="7205", sc-filter-result="OBSERVED", x-exception-id="-", x-virus-id="-", x-rs-certificate-observed-errors="none", x-cs-ocsp-error="-", x-rs-ocsp-error="-", x-rs-connection-negotiated-cipher-strength="high", x-rs-certificate-hostname="*.somedomain.com", x-rs-certificate-hostname-category="Web Ads/Analytics"
```

Access Logging

To configure access logging, take the following steps.

1. Log in to the Blue Coat Management Console.
2. Select **Configuration > Access Logging > Formats**.
3. Select **New**.
4. Type a format name for the custom format and paste the following configs:

```
<111>$(date)T$(x-bluecoat-hour-utc):$(x-bluecoat-minute-utc):$(x-bluecoat-second-utc)
Bluecoatsyslog time-taken=\"$(time-taken)\", c-ip=\"$(c-ip)\", cs-username=\"$(cs-username)\",
cs-auth-group=\"$(cs-auth-group)\", cs-categories=$(cs-categories), sc-status=\"$(sc-
status)\", cs-uri-scheme=\"$(cs-uri-scheme)\", cs-host=\"$(cs-host)\", cs-uri-port=\"$(cs-uri-
port)\", cs-uri-extension=\"$(cs-uri-extension)\", cs(User-Agent)=\"$(cs(User-Agent))\", cs-
uri-path=\"$(cs-uri-path)\", cs-method=\"$(cs-method)\", cs-bytes=\"$(cs-bytes)\", r-ip=\"$(r-
ip)\", rs(Content-Type)=\"$(rs(Content-Type))\", s-action=\"$(s-action)\", s-ip=\"$(s-ip)\",
sc-bytes=\"$(sc-bytes)\", sc-filter-result=\"$(sc-filter-result)\", x-exception-id=\"$(x-
exception-id)\", x-virus-id=\"$(x-virus-id)\", x-rs-certificate-observed-errors=\"$(x-rs-
certificate-observed-errors)\", x-cs-ocsp-error=\"$(x-cs-ocsp-error)\", x-rs-ocsp-error=\"$(x-
rs-ocsp-error)\", x-rs-connection-negotiated-cipher-strength=\"$(x-rs-connection-negotiated-
cipher-strength)\", x-rs-certificate-hostname=\"$(x-rs-certificate-hostname)\", x-rs-
certificate-hostname-category=$(x-rs-certificate-hostname-category)
```

5. Select transport option.
6. Save your format.
7. Click **OK**.
8. Specify the IP address for the client that is receiving the logs.
9. Click **Apply**.

Cisco IronPort Mail Gateway

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP		Ping Status, SNMP Ping Stat, Uptime, CPU Util, Mem Util, Net Intf Stat, Hardware Status	
Syslog		Mail attributes: attributes include MID, ICID, DCID, Sender address, Receiver Address, Mail Subject, Sent Bytes, Attachment, Spam indicator, Virus indicator, Quarantine indicator, SMTP delivery failures and failure codes, mail action - pass, block, clean.	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "ironport-mail" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "ironport mail" in the main content panel **Search...** field to see the reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

1. Log in to your IronPort Mail Gateway device manager with administrator privileges.
2. Edit the Log Subscription settings.
3. For **Log Name**, enter **IronPort-Mail**.
This identifies the log to FortiSIEM as originating from an IronPort mail gateway device.

The default IronPortMailParser will only parse events when the log settings on IronPort is configured with name "IronPort-Mail". If you need to add a different name, then the default parser for IronPortMailParser should be disabled (Uncheck **Enabled**, then click **Apply**), cloned (click **Clone**), and the cloned parser needs to be modified to include the new pattern name. Afterward, the cloned parser should be **Enabled** and moved to the same position (using the **Up/Down** buttons) the disabled default parser was located, then click **Apply** to apply the change.

Example:

Log Name is changed from "IronPort-Mail" to "FortiSiem-IronPort-Text-Mail".



The original line for the cloned IronPortMailParser:

```
<pattern name="patIronportMailMod"><![CDATA[IronPort-Mail|IronPort-Mail-AntiSpam|IronPort-Mail-AntiVirus|IronPort-Mail-MailLog|antispam|antivirus|antivirus_log1|ironport-mail|mail_log1|smtp_logs]]></pattern>
```

Must be changed to:

```
<pattern name="patIronportMailMod">IronPort-Mail|IronPort-Mail-AntiSpam|IronPort-Mail-AntiVirus|IronPort-Mail-MailLog|antispam|antivirus|antivirus_log1|ironport-mail|mail_log1|smtp_logs|euq_logs|FortiSiem-.*|FortiSIEM-.*</pattern>
```

4. For **Retrieval Method**, select **Syslog Push**.
5. For **Hostname**, enter the IP address of your FortiSIEM virtual appliance.
6. For **Protocol**, select **UDP**.

Sample Parsed IronPort Mail Gateway Syslog

```
Tue Sep 24 11:39:49 2012 IronPort-Mail: Info: MID 200257071 ready 24663 bytes from
<someone@example.net>Sep 24 11:39:49 18.0.19.8 IronPort-Mail: Info: MID 1347076 ICID 346818 From:
<john.doe@example.com>Tue Sep 24 11:39:49 2012 IronPort-Mail: Info: Message aborted MID 200257071
Dropped by antivirus
Tue Sep 24 11:39:49 2012 IronPort-Mail: Info: Delayed: DCID 5 MID 200257071 to RID 0 - 4.1.0 -
Unknown address error ('466', ['Mailbox temporarily full.'])[]
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco IronPort AsyncOS Mail
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco IronPort Web Gateway

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		Squid style web logs: attributes include Source IP Address, Destination Host name, Sent Bytes, Received Bytes, HTTP User Agent, HTTP Referrer, HTTP Version, HTTP Method, HTTP Status Code, URL, HTTP Content type, Web Category, HTTP Proxy Action	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "ironport-web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [Syslog](#)
- [Sample Parsed Ironport Web Gateway Syslog](#)

Syslog

1. Log in to your Ironport gateway device manager with administrator privileges.
2. Edit the settings for Log Subscription.

Setting	Value
Log Type	Access Logs
Log Name	IronPort-Web This identifies the log to FortiSIEM as originating from an IronPort web gateway device
Log Style	Squid
Custom Fields	%L %B %u
Enable Log Compression	Clear the selection
Retrieval Method	Syslog Push
Hostname	The IP address of your FortiSIEM virtual appliance
Protocol	UDP

Sample Parsed Ironport Web Gateway Syslog

```
<134>Oct 09 09:19:25 IronPort-Web: Info: 1349795965.314 92 10.163.154.153 TCP_CLIENT_REFRESH_
MISS/200 70798 GET
http://forefrontdl.microsoft.com/server/scanengineupdate/x86/Kaspersky/Package/1210090007/bases/ba
se1b1d.kdc.cab - DIRECT/forefrontdl.microsoft.com application/octet-stream ALLOW_CUSTOMCAT_11-
UnAuthenticated_Applications-APU_No_Auth-NONE-NONE-NONE-DefaultGroup <J_Doe,6.9,-,""-
",-,-,-,-,""-","-,-,-,-,""-","-,-,-,-,""-","-,-,-,-,IW_swup,-,""-","-","-","-","Unknown","-
","-","-","-","6156.35,0,-,""-","-","-","-""> - ""09/Oct/2012:09:19:25 -0600"" 71052 ""V3S;{6ADC64A3-11F9-
4B04-8257-BEB541BE2975};""
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco IronPort AsyncOS Web
Access Protocol	See Access Credentials

Setting	Value
Port	See Access Credentials
Password config	See Password Configuration

Fortinet FortiMail

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		System events (e.g. configuration changes), System up/down/restart events, Performance issues, Admin logon events, malware attachments	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortimail" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortimail" in the main content panel **Search...** field to see the rules associated with this device.

For generic availability rules, see **RESOURCES > Rules > Availability > Network**.

For generic performance rules, see **RESOURCES > Rules > Performance > Network**.

Reports

In **RESOURCES > Reports**, search for "fortimail" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- [Syslog](#)
- [Sample Parsed FortiMail Syslog](#)

Syslog

Configure FortiMail appliance to send logs to FortiSIEM. Make sure the format matches.

In the FortiMail GUI go to **Log & Report > Log Settings > Remote (tab) > New**.

Suggested Logging configuration:

Name	Description
Name	Define a name for the configuration.
Server name/IP	Enter the resolvable DNS name or IP of the FortiSIEM appliance where logs will be sent.
Server port	514
Mode	UDP
Level	Information
Facility	kern
CSV format	leave disabled
Matched session only	leave disabled

Log to Remote Host

Enable	☒
Name:	localsis
Server name/IP:	10.10.11.255
Server port:	514
Protocol:	Syslog
Mode:	UDP
Level:	Information
Facility:	kern
CSV format	☐
Matched session only	☐



Sample Parsed FortiMail Syslog

```
date=2012-08-17 time=12:26:41 device_id=FE100C3909600504 log_id=0001001623 type=event
subtype=admin pri=information user=admin ui=GUI(172.20.120.26) action=login status=success
reason=none msg="User admin login successfully from GUI(172.20.120.26)"
date=2012-07-16 time=12:22:56 device_id=FE100C3909600504 log_id=0200001075 type=statistics
pri=information session_id="q6GJMuPu003642-q6GJMuPv003642" client_name="[172.20.140.94]"
dst_ip="172.20.140.92" endpoint="" from="user@external.lab" to="user5@external.lab"
subject="" mailer="mta" resolved="OK" direction="in" virus="" disposition="Reject"
classifier="Recipient Verification" message_length="188"
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiMail
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Fortinet FortiProxy

Support Added: FortiSIEM 6.3.1

Last Modification: FortiSIEM 6.3.1

Vendor Version Tested: Not Provided

Vendor: Fortinet

Product Information: <https://www.fortinet.com/products/secure-web-gateway/fortiproxy>

- [Log Information](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortiproxy" to see the event types associated with this device.

In 6.3.1, there are over 14,000 event types.

Rules

In **RESOURCES > Rules**, search for "fortiproxy" in the main content panel **Search...** field to see related rules associated with this device.

- FortiAI: Attack Chain Blocked
- FortiAI: Attack Chain Permitted

Reports

In **RESOURCES > Reports**, search for "fortiproxy" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 12 reports available.

- FortiProxy Admin Authentication Events
- FortiProxy App Control App Group Name Summary
- FortiProxy App Control App Name Summary
- FortiProxy App Control Detailed

- FortiProxy UTM Event Summary
- FortiProxy WebFilter Blocked and Passthrough Event Count
- FortiProxy WebFilter Blocked Event Count
- FortiProxy Web Filter Detailed
- FortiProxy Web Filter Events by Web Category, User, and Count
- FortiProxy Webfilter Group by Action,Category, and Count
- FortiProxy WebFilter Passthrough Event Count
- FortiProxy Web Filter User Hit Count

Fortinet FortiWeb

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP	Host Name, Vendor, Model, Version, Hardware Model, hardware	CPU, memory, Disk, Interface, Uptime	Performance monitoring
Syslog		System events (e.g. configuration changes), System up/down/restart events, Performance issues, Admin logon events, Security exploits	Security Monitoring and compliance

Supported Syslog format

Currently FortiSIEM supports FortiWeb native logging format and not CEF format.

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortiweb" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortiweb" in the main content panel **Search...** field to see the rules associated with this device.

For generic availability rules, see **RESOURCES > Rules > Availability > Network**.

For generic performance rules, see **RESOURCES > Rules > Performance > Network**.

Reports

In **RESOURCES > Reports**, search for "fortiweb" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- [Syslog](#)
- [Sample FortiWeb Syslog](#)

Syslog

Configure FortiWeb appliance to send logs to FortiSIEM. Make sure the format matches. Configuration steps can be found in the [FortiWeb Administration Guide Logging section](#). Remember to point your syslog policy to the FortiSIEM collector IP address.

Sample FortiWeb Syslog

```
date=2016-02-18 time=10:00:05 log_id=00001002 msg_id=000067508821 device_
id=FV400D3A15000010 vd="root" timezone="(GMT+3:00)Baghdad" type=event subtype="admin"
pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User
admin changed global from GUI(172.22.6.66)
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiWeb
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Imperva SecureSphere DB Monitoring Gateway

- [Configuration in FortiSIEM](#)

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	<set name>
Device Type	Imperva Securesphere DB Monitoring Gateway
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration
User Name	A user who has access credentials for the device
Password	The password for the user
Super Password	Password for Super

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Imperva SecureSphere DB Monitoring Gateway.
5. To see the jobs associated with Imperva, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Imperva" in the search box.

Imperva SecureSphere Security Gateway

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)			Security and Compliance

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	<set name>
Device Type	Imperva SecureSphere DB Security Gateway
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration
User Name	A user who has access credentials for the device
Password	The password for the user
Super Password	Password for Super

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.

- c. Click **Save**.
4. Click the **Test** drop-down list, and select **Test Connectivity** to test the connection to Imperva SecureSphere DB Security Gateway.
5. To see the jobs associated with Imperva, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Imperva" in the search box.

Sample Events

```
<14>CEF:0|Imperva Inc.|SecureSphere|11.5.0.20_0|Audit|Audit|Informative|dst=10.2.6.194 dpt=3306
duser=wf_settlement src=10.2.6.48 spt=59876 proto=TCP rt=11 April 2016 14:07:09 cat=Audit Default
Rule - All cs2Label=ServerGroup cs3=ProcessMakerDBFX cs3Label=ServiceName cs4=Default MySql
Application cs4Label=ApplicationName cs5=642697783064 cs5Label=EventId cs6=Query
cs6Label=EventType cs7=Default MySql group cs7Label=UserGroup cs8=True cs8Label=UserAuthenticated
cs9= cs9Label=ApplicationUser cs10= cs10Label=SourceApplication cs11= cs11Label=OSUser cs12=
cs12Label=HostName cs13=wf_settlement cs13Label=Database cs14= cs14Label=Schema cs15=SELECT COUNT
(APP_CACHE_VIEW.APP_UID) FROM APP_CACHE_VIEW LEFT JOIN USERS CU ON (APP_CACHE_VIEW.USR_UID=CU.USR_
UID) LEFT JOIN USERS PU ON (APP_CACHE_VIEW.PREVIOUS_USR_UID=PU.USR_UID) LEFT JOIN APP_CACHE_VIEW
APPCVCR ON (APP_CACHE_VIEW.APP_UID=APPCVCR.APP_UID AND APPCVCR.DEL_LAST_INDEX=1) LEFT JOIN USERS
USRCR ON (APPCVCR.USR_UID=USRCR.USR_UID) WHERE APP_CACHE_VIEW.APP_STATUS='TO_DO' AND APP_CACHE_
VIEW.USR_UID='2800810224bbdfef1cc8bb02024369548' AND APP_CACHE_VIEW.DEL_FINISH_DATE IS NULL AND
APP_CACHE_VIEW.APP_THREAD_STATUS='OPEN' AND APP_CACHE_VIEW.DEL_THREAD_STATUS='OPEN'
cs15Label=RawQuery cs16=select count(app_cache_view.app_uid) from app_cache_view left join users
cu on (app_cache_view.usr_uid=cu.usr_uid) left join users pu on (app_cache_view.previous_usr_
uid=pu.usr_uid) left join app_cache_view appcvcr on (app_cache_view.app_uid=appcvcr.app_uid and
appcvcr.del_last_index=?) left join users usrcr on (appcvcr.usr_uid=usrcr.usr_uid) where app_
cache_view.app_status=? and app_cache_view.usr_uid=? and app_cache_view.del_finish_date is ? and
app_cache_view.app_thread_status=? and app_cache_view.del_thread_status=? cs16Label=ParsedQuery
cs17= cs17Label=BindVariables cs18= cs18Label=SQLError cs19=1 cs19Label=ResponseSize cs20=0
cs20Label=ResponseTime cs21=0 cs21Label=AffectedRows
```

McAfee Web Gateway

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		Parsed event attributes: include Source IP, Destination URL, HTTP Method, HTTP User agent, HTTP Status Code, HTTP Content Type, Blocked Reason, Risk	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "mcafee-web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [Syslog](#)
- [Sample Parsed McAfee Web Gateway Syslog Message](#)

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format (CEF)**. The syslog format should be the same as that shown in the example.

Sample Parsed McAfee Web Gateway Syslog Message

```
[21/Feb/2012:11:44:19 -0500] "000000000000" "10.200.11.170 200 ""GET http://example.com/
HTTP/1.1"" ""General News"" ""Minimal Risk"" ""text/html"" 101527 "000000000000"
""000000000000"[30/May/2012:10:39:44 -0400] "" 10.19.2.63 200
"GEThttp://example.com/html.ng/site=cnn&cnn_pagetype=main&cnn_position=126x31_spon2&cnn_
rollup=homepage&page.allowcompete=no&params.styles=fs&Params.User.UserID=4fc6251c068c9f0aa51475025
d0040b8&transactionID=7179860628805012&tile=4893878838331&domId=135492 HTTP/1.1" "Web Ads,
Forum/Bulletin Boards" "MinimalRisk" "text/html" 1 "" "" "0"
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	McAfee WebGateway
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Microsoft ISA Server

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level metrics: CPU utilization, memory utilization	Performance Monitoring
WMI	Application type, service mappings	Process level metrics: uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O	Performance Monitoring
Syslog(via SNARE)	Application type	W3C proxy logs: attributes include Service Instance, Source IP, User, Destination IP, Destination Port, Service Instance, Sent Bytes, Received Bytes, Connection Duration, HTTP User Agent, HTTP Referrer, HTTP Version, HTTP Method, HTTP Status Code, URL, Source interface, Destination interface, Proxy action	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "isa server" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [WMI](#)
- [Syslog](#)

SNMP

- [Enabling SNMP on Windows Server 2003](#)
- [Enabling SNMP on Windows 7 or Windows Server 2008 R2](#)

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you must make sure that the SNMP Management tool has been enabled for your device.

1. In the **Start** menu, go to **Administrative Tools > Services**.
2. Go to **Control Panel > Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Select **Management and Monitoring Tools** and click **Details**.
Make sure that **Simple Network Management Tool** is selected.
If it isn't selected, select it, and then click **Next** to install.
5. Go to **Start > Administrative Tools > Services**.
6. Select and open **SNMP Service**.
7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts**.
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service**.

Enabling SNMP on Windows 7 or Windows Server 2008 R2

SNMP is typically enabled by default on Windows Server 2008, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you should check that SNMP Services have been enabled for your server.

1. Log in to the Windows 2008 Server where you want to enable SNMP as an administrator.
2. In the **Start** menu, select **Control Panel**.
3. Under **Programs**, click **Turn Windows features on/off**.
4. Under **Features**, see if **SNMP Services** is installed.
If not, click **Add Feature**, then select **SMNP Service** and click **Next** to install the service.

5. In the **Server Manager** window, go to **Services > SNMP Services**.
6. Select and open **SNMP Service**.
7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts**.
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service**.

WMI

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- [Creating a Generic User Who Does Not Belong to the Local Administrator Group](#)
- [Creating a User Who Belongs to the Domain Administrator Group](#)

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

- [Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group](#)
- [Enable DCOM Permissions for the Monitoring Account](#)

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add**.
6. Find the user you created, and then click **OK**.
This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.

4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **EditDefault**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

- [Enable Remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group](#)
- [Enable the Monitoring Account to Access the Monitored Device](#)
- [Enable DCOM Permissions for the Monitoring Account](#)
- [Enable Account Privileges in WMI](#)
- [Allow WMI to Connect Through the Windows Firewall \(Windows 2003\)](#)
- [Allow WMI through Windows Firewall \(Windows Server 2008, 2012\)](#)

Enable Remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2**.
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced**.
8. Select the user you created for the monitoring account, and then click **Edit**.
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.

3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run cmd.exe and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and then click **OK**.

You can configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the [User Guide](#).

Syslog

Use the [Windows Agent Installation Guide](#) to configure sending syslog from your device to FortiSIEM.

Sample Microsoft ISA Server Syslog

```
<13>Mar 6 20:56:03 ISA.test.local ISAWebLog 0 192.168.69.9 anonymous Mozilla/5.0
(Windows; U; Windows NT 5.2; en-GB; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12 Y 2011-03-05
21:33:55 w3proxy ISA - 212.58.246.82 212.58.246.82 80 156 636 634
http TCP GET http://192.0.2.82/rss/generic_news/front_page/rss.xml text/html;
charset=iso-8859-1 Inet 301 0x41200100 Local Machine Req ID: 07c10445; Compression:
client=No, server=No, compress rate=0% decompress rate=0% Local Host External 0x400
Allowed 2011-03-05 21:33:55 -
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic

Setting	Value
Access Protocol	SNMP
Community String	<your own>

Proofpoint

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Log](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
API		Alert Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Proofpoint-" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 2 event types defined.

Rules

There are no specific rules available for Proofpoint.

Reports

There are no specific reports available for Proofpoint. You can view all Proofpoint events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Proofpoint".

6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

- [API](#)
- [Setup in FortiSIEM](#)

API

FortiSIEM processes events from Proofpoint via the ProofPoint API. Configure in and obtain from the Proofpoint Portal the Principal and Secret from the API. FortiSIEM uses the ProofPoint API defined [here](#).

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Proofpoint Proofpoint
Access Protocol	Proofpoint SIEM API
Pull Interval	5 minutes
Principal	The access key for your Proofpoint instance.
Secret	The secret for Proofpoint instance.
Confirm Secret	Input the same secret as above for verification.
Organization	Choose the Organization the instance belongs to.
Description	Description about the instance.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field. For this configuration, it should be "tap-api-v2.proofpoint.com".
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Proofpoint.
5. To see the jobs associated with Proofpoint, select **ADMIN > Setup > Pull Events**.

6. To see the received events select **ANALYTICS**, then enter "Proofpoint" in the search box.

Sample Log

```
<![CDATA[2018-09-29 17:56:00 [FSM-PROOFPOINT] [1] [clicksPermitted]:{"campaignId":"46e01b8a-c899-404d-bcd9-189bb393d1a7","classification":"MALWARE","clickIP":"192.0.2.1","clickTime":"2016-06-24T19:17:44.000Z","messageID":"8c6cfedd-3050-4d65-8c09-c5f65c38da81","recipient":"example.user@example.zz","sender":"9facbf452def2d7efc5b5c48cdb837fa@example.zz","senderIP":"192.0.2.255","threatID":"61f7622167144dba5e3ae4480eeee78b23d66f7dfed970cfc3d086cc0dabdf50","threatTime":"2016-06-24T19:17:46.000Z","threatURL":"https://threatinsight.proofpoint.com/#/73aa0499-dfc8-75eb-1de8-a471b24a2e75/threat/u/61f7622167144dba5e3ae4480eeee78b23d66f7dfed970cfc3d086cc0dabdf50","url":"http://example.zz/","userAgent":"Mozilla/5.0(WindowsNT6.1;WOW64;rv:27.0)Gecko/20100101Firefox/27.0"}]]
```

Squid Web Proxy

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, Interfaces, Serial number	CPU utilization, Memory utilization	Performance Monitoring
Syslog		Proxy traffic: attributes include Source IP, Destination IP, Destination Name, Destination Port, URL, Web category, Proxy action, HTTP User Agent, HTTP Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "squid" to see the event types associated with this device.

Configuration

- [SNMP](#)
- [Syslog](#)
- [Configure syslogd \(or rsyslogd\) to Forward the Logs to FortiSIEM](#)
- [Sample Parsed Squid Syslog Messages](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Syslog

1. Add the following line to the logformat section in /etc/squid/squid.conf based of your version of Squid.

For Squid versions earlier than 4.1.1:

```
logformat PHCombined %>a %>p %<A %la %lp %tr %ul %ui %un %us %ue [%tl] %rm "%ru" HTTP/%rv %Hs
%<st %>st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
```

For Squid version 4.1.1 and later:

```
logformat PHCombined %>a %>p %<A %la %lp %tr %ul %ui %un [%tl] %rm "%ru" HTTP/%rv %Hs %<st
%>st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
```

2. Add the following line to the access_log section in /etc/squid/squid.conf.

```
access_log syslog:LOG_LOCAL4 PHCombined
```

3. Restart Squid.

Configure syslogd (or rsyslogd) to Forward the Logs to FortiSIEM

1. Modify /etc/syslog.conf (/etc/rsyslog.conf if running rsyslog) .

```
Local4.*
```

```
@<FortiSIEMIp>
```

2. Restart syslogd (or rsyslogd).

Sample Parsed Squid Syslog Messages

- [Squid on Linux with syslog Locally to Forward to FortiSIEM](#)
- [Squid on Linux with syslog-ng Locally to Forward to FortiSIEM](#)
- [Squid on Linux with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM](#)
- [Squid on Linux with syslog-ng Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM](#)
- [Squid on Solaris with syslog Locally to Forward to FortiSIEM](#)
- [Squid on Solaris with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM](#)

Squid on Linux with syslog Locally to Forward to FortiSIEM

```
<166>squid[28988]: 192.168.25.15 51734 65.54.87.157 172.16.10.40 3128 5989 - - - - -
[22/Apr/2011:17:17:46 -0700] GET "http://col.stj.s-msn.com/br/sc/js/jquery/jquery-1.4.2.min.js"
HTTP/1.1 200 26141 407 "http://www.msn.com/" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US;
rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16" TCP_MISS:DIRECT
```

Squid on Linux with syslog-ng Locally to Forward to FortiSIEM

```
<166>Oct 20 09:21:54 QA-V-CentOS-Syslog-ng squid[7082]: 192.168.20.42 1107 74.125.19.100
172.16.10.34 3128 291 - - - - [20/Oct/2009:09:21:54 -0700] GET
"http://clients1.google.com/generate_204" HTTP/1.1 204 387 603 "http://www.google.com/"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152;
.NET CLR 3.5.30729)" TCP_MISS:DIRECT
```

Squid on Linux with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM

```
<166>Oct 20 10:21:42 172.16.10.40 squid[26033]: 192.168.20.42 1121 66.235.132.121 172.16.10.40
3128 117 - - - - [20/Oct/2009:12:05:49 -0700] GET
"http://metrics.sun.com/b/ss/sunglobal,suncom,sunstruppdev/1/H.14/s21779365053734?" HTTP/1.1 200
746 1177 "http://www.sun.com/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" TCP_MISS:DIRECT
```

Squid on Linux with syslog-ng locally and forward to syslog-ng remotely to forward to FortiSIEM

```
<166>Oct 20 12:44:12 172.16.10.40 squid[26033]: 192.168.20.42 1125 64.213.38.80 172.16.10.40 3128
117 - - - - [20/Oct/2009:12:44:12 -0700] GET "http://www-cdn.sun.com/images/hp5/hp5b_enterprise_
10-19-09.jpg" HTTP/1.1 200 12271 520 "http://www.sun.com/" "Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" TCP_MISS:DIRECT
```

Squid on Solaris with syslog Locally to Forward to FortiSIEM

```
<166>May 6 17:55:48 squid[1773]: [ID 702911 local4.info] 192.168.20.39 1715 72.14.223.18
172.16.10.6 3128 674 - - - - [06/May/2008:17:55:48 -0700] GET "http://mail.google.com/mail/?"
HTTP/1.1 302 1061 568 "http://www.google.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14" TCP_MISS:DIRECT
```

Squid on Solaris with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM

```
<166>Oct 20 13:02:19 172.16.10.6 squid[687]: [ID 702911 local4.info] 192.168.20.42 1112
208.92.236.184 172.16.10.6 3128 201 - - - - [20/Oct/2009:13:02:19 -0700] GET
"http://m.webtrends.com/dcs4f6vsz99k7mayiw2jzupyr_1s2e/dcs.gif?" HTTP/1.1 200 685 1604
"http://www.microsoft.com/en/us/default.aspx" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;
.NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" TCP_MISS:DIRECT
```


SSH Comm Security CryptoAuditor

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	15 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "CryptoAuditor-" in the main content panel **Search...** field to see the event types associated with this device. .

Sample Event Type:

```
<189>Jun 24 15:43:01 auditor ssh-auditor[4067]: CEF:0|SSH|CryptoAuditor|1.6.0|4201|Connection_
received|1|rt=Jun 26 2015 07:48:24 SshAuditorSrc=10.1.78.8 spt=34453 SshAuditorDst=10.1.78.8
dpt=10022 SshAuditorSessionId=21 SshAuditorUsername=testuser SshAuditorRemoteusername=testuser
SshAuditorProtocolsessionId=C089C55D9ADE0A4F901917D69B46B01223A02B70 SshAuditorVirtualLAN=0
cs1=source connection cs1Label=Text
```

```
<189>Jun 24 15:43:01 auditor ssh-auditor[4067]: CEF:0|SSH|CryptoAuditor|1.6.0|4201|Connection_
received|rt=Jun 26 2015 07:48:24 SshAuditorSrc=10.1.78.8 spt=34453 SshAuditorDst=10.1.78.8
dpt=10022 SshAuditorSessionId=21 SshAuditorUsername=testuser SshAuditorRemoteusername=testuser
SshAuditorProtocolsessionId=C089C55D9ADE0A4F901917D69B46B01223A02B70 SshAuditorVirtualLAN=0
cs1=source connection cs1Label=Text
```

Rules

There are no specific rules but generic rules for Generic Servers apply.

Reports

There are no specific reports but generic rules for Generic Servers apply.

Configuration

Configure SSH Comm Security CryptoAuditor to send syslog on port 514 to FortiSIEM.

Vormetric Data Security Manager

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)		1 event type	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "Vormetric-" in the main content panel **Search...** field.

Sample Event Type

```
<14> 2013-06-29T18:44:42.420Z 10.10.10.1 CEF:0|Vormetric, Inc.|dsm|5.2.0.1|DA00048I|update  
host|3|cs4Label=logger cs4=DAO spid=4322 rt=1388986263954 dvchost=example.com suser=USER_1  
shost=test_cpu
```

Rules

There are no specific rules but generic rules for Security Manager and Generic Servers apply.

Reports

There are no specific reports but generic rules for Security Manager and Generic Servers apply.

Configuration

Configure Vormetric Data Security Manager to send syslog in CEF format on port 514 to FortiSIEM.

Websense Web Filter

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Parsed Websense Web Filter Syslog Message](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		Parsed event attributes: include Source IP, Destination Name, Destination URL, HTTP Method, HTTP User agent, HTTP Status Code, HTTP Content Type, Blocked Reason, Website category, HTTP Disposition, Sent Bytes, Recv Bytes, Duration, File Type etc	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "websense_web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

FortiSIEM integrates with Websense Web Filter via syslog sent in the SIEM integration format as described in the [Websense SEIM guide](#). See the instructions on how to install a Websense Multiplexer that integrates with Websense Policy server and creates syslog for consumption by SIEM products such as FortiSIEM.

Sample Parsed Websense Web Filter Syslog Message

```
<159>Feb 28 14:25:32 10.203.28.21 vendor= Websense product=Security product_version=7.7.0
action=permitted severity=1 category=153
user=- src_host=10.64.134.74 src_port=62189 dst_host=mail.google.com dst_ip=74.125.224.53 dst_
port=443 bytes_out=197 bytes_in=76
http_response=200 http_method=CONNECT http_content_type= -
http_user_agent=Mozilla/5.0_(Windows;_U;_Windows_NT_6.1;_enUS;_rv:1.9.2.23)_Gecko/20110920_
Firefox/3.6.23
http_proxy_status_code=200 reason=- disposition=1034 policy=- role=8 duration=0
url=https://mail.google.com
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Websense Web Security
Access Protocol	JDBC
Log Server IP	IP of the log server
Pull Interval	5 minutes
Port	1433
Log Database	wslogdb70_1
URL Database	wslogdb70
URL Category Database	wslogdb70
Disposition Database	wslogdb70
User Name	Name used to access the database

Security Information and Event Management (SIEM)

FortiSIEM supports the following SIEM applications.

- [SAP Enterprise Threat Detection \(ETD\)](#)
- [SAP Enterprise Threat Detection Cloud](#)

SAP Enterprise Threat Detection (ETD)

Support Added: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: SAP

Product: SAP Enterprise Threat Detection

Product Information: <https://www.sap.com/products/financial-management/enterprise-threat-detection.html>

- [Configuration](#)
- [Sample Log](#)

Configuration

To configure SAP Enterprise Threat Detection, take the following steps.

1. Configure the FortiSIEM node with the HTTPS credential for receiving the HTTP(S) POST event by taking the following steps.
 - a. Identity the FortiSIEM node receiving the events. Most likely, this will be the Collector.
 - b. SSH to the Collector and run the command.

```
htpasswd -b /etc/httpd/accounts/passwds <user> '<password>'
```

Note: If the password contains special characters, it is advisable to encode the password in single quotes.

2. Make sure the events are being pushed to the FortiSIEM node using the credentials in [Step 1](#) via this REST API.

```
https://<FSMNodeName>/rawupload?vendor=<vendor>&model=<model>&reptIp=<reptIp>&reptName=<reptHost>
```

where *FSNNodeName* is the resolvable host name or FQDN in [Step 1](#). The parameters Reporting Vendor (vendor), Reporting Model (model), Reporting Device (reptHost), and Reporting IP (reptIP) are needed to create a CMDB entry and populate events.

Argument	Description
vendor	The vendor of the product that the logs originated from.
model	The model of the product that the logs originated from.
reptip	This is the reporting IP, or the source of the log. The value you specify here will populate the CMDB as a reporting device.
reptName	This is the reporting device name, or the hostname of the device sending the logs.

Note: If the Model contains whitespace, such as "Model 24", you must correctly encode spaces and other special characters in the URL parameters.

HTTP Method: POST

HTTP Body: log in json format

Sample Curl to Send a JSON File

This example is sending a SAP Enterprise Threat Detection log.

```
curl -kv -u 'user:password' -d "@json_event.json" -X POST
'https://<FSMNodeName>/rawupload?vendor=SAP&model=ETD&reptIp=192.168.1.20&reptName=LogForwarder1'
```

The above sends the JSON event stored in the file `json_event.json` to FortiSIEM. FortiSIEM then processes it, the resulting event should look like the following in **Log Format**, with an added header attached.

Log Format

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=<vendor>,[reptModel]=<model>,[reptDevName]=<reptName>,[reptDevIpAddr]=<reptIp>,[json]=<JSON>
```

Where <JSON> is the actual JSON log body posted to FortiSIEM.

3. Query the events by using the Reporting Device Name or IP in [Step 2](#) and Event Type, by taking the following steps.
 - a. Go to the **ANALYTICS** tab.
 - b. Run a query for the Reporting IP = '#.#.#' for the last 10 minutes.
 - c. Observe the raw event, it should be in the format of.

Filter By: Event Keywords **Event Attribute** CMDB Attribute Clear All Load Save

Paren	Attribute	Operator	Value	Paren	Next	Row
-	+ Reporting IP	=	1.1.1.1	-	+ AND OR	+

Time Range: Real-time **Relative** Absolute

Last Minutes

Trend Interval: Auto

Result Limit: K rows

Apply & Run Apply Cancel

Sample Log

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=SAP,[reptModel]=ETD,[reptDevName]=sap.edt.device,
[reptDevIpAddr]=192.0.2.0,[json]={ "alerts": [ { "Version": "1.0", "AlertCreationTimestamp":
"2021-09-21T07:45:45.420Z", "AlertId": 812125, "AlertSeverity": "MEDIUM", "AlertStatus":
"FORWARDED", "AlertSource": { "EventLogType": "SystemLog", "SystemIdActor": "System25" },
"AlertSystemIds": [ "System25" ], "HostNames": [ "lab1" ], "Category": "Log Failure", "PatternId":
"624F0A8BB948854F997942AC0EDB2102", "PatternType": "FLAB", "PatternName": "Low Log Amount per
system", "PatternNameSpace": "http://demo", "PatternDescription": "", "MinTimestamp": "2021-09-
21T07:44:39.522Z", "MaxTimestamp": "2021-09-21T07:44:39.522Z", "Text": "Measurement 48 exceeded
threshold 50 for ('Event, Log Type' = 'SystemLog' / 'System ID, Actor' = 'System25')", "Score":
50, "UiLink": "http://192.0.2.10:80/sap/hana/uis/clients/ushell-
app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetail-
show?alert=62037185B38D5449999D57F465F1BBF6", "TriggeringEvents": [ { "Id":
"C60C48EF7B4E4D848F45F1904820C2CC", "Timestamp": "2021-09-21T07:44:39.522Z",
"TechnicalLogEntryType": "SM21_D01", "TechnicalNumber": "481537", "TechnicalTimestampOfInsertion":
"2021-09-21T07:44:40.681Z", "CorrelationId": "120CD18982991EEA9AB8F87143C8DE88",
"CorrelationSubId": "00000000000000000000000000000000", "EventCode": "D01", "EventSemantic":
"Executable, Run, Cancel", "EventLogType": "SystemLog", "EventMessage": "LMDB_UPLOAD_ERRORS 011",
"EventSeverityCode": "50", "EventSourceId": "192.0.2.104", "EventSourceType": "IP Address",
"GenericRiskLevel": "3", "NetworkHostnameActor": "test-1", "NetworkHostnameInitiator": "0.0.0.0",
"NetworkHostnameReporter": "test-1", "NetworkIPAddressInitiator": "0.0.0.0",
"ServiceExecutableName": "00016", "ServiceExecutableType": "B", "ServiceInstanceName": "lab1_BLK_
00", "ServiceProgramName": "RLMDB_UPLOAD_BACKGROUND", "ServiceTransactionName": "S000",
"SystemIdActor": "System25", "SystemGroupIdActor": "BLN", "SystemGroupIdInitiator": "BLN",
"SystemGroupIdIntermediary": "BLN", "SystemIdReporter": "System25", "SystemGroupIdReporter":
"BLN", "SystemGroupIdTarget": "BLN", "SystemTypeActor": "ABBA", "SystemGroupTypeActor": "SAP",
"SystemGroupTypeInitiator": "SAP", "SystemGroupTypeIntermediary": "SAP", "SystemTypeReporter":
"ABBA", "SystemGroupTypeReporter": "SAP", "SystemGroupTypeTarget": "SAP",
"UsernameDomainNameActing": "System25", "UsernameDomainTypeActing": "ABBA", "UserPseudonymActing":
"BLK_BTC_SMP", "EventName": "ExecutableRunCancel", "EventNamespace": "http://sap.com/secmon",
"TechnicalTimestampInteger": "1632210279522" }, { "Id": "765451B9772A4FA580059A7BAD7D149C",
"Timestamp": "2021-09-21T07:44:39.522Z", "TechnicalLogEntryType": "SM21_E0A", "TechnicalNumber":
```



```
"481536", "TechnicalTimestampOfInsertion": "2021-09-21T07:44:40.681Z", "CorrelationId":
"120CD18982991EEA9AB8F87143C8DE88", "CorrelationSubId": "00000000000000000000000000000000",
"EventCode": "E0A", "EventLogType": "SystemLog", "EventMessage": "&aRLMDB_UPLOAD_DISPLAY_
LOG&b000000000000011498140", "EventSeverityCode": "9", "EventSourceId": "192.168.30.104",
"EventSourceType": "IP Address", "GenericRiskLevel": "0", "NetworkHostnameActor": "test-1",
"NetworkHostnameInitiator": "0.0.0.0", "NetworkHostnameReporter": "test-1",
"NetworkIPAddressInitiator": "0.0.0.0", "ServiceExecutableName": "00016", "ServiceExecutableType":
"B", "ServiceInstanceName": "lab1_BLK_00", "ServiceProgramName": "RLMDB_UPLOAD_BACKGROUND",
"ServiceTransactionName": "S000", "SystemIdActor": "System25", "SystemGroupIdActor": "BLN",
"SystemGroupIdInitiator": "BLN", "SystemGroupIdIntermediary": "BLN", "SystemIdReporter":
"System25", "SystemGroupIdReporter": "BLN", "SystemGroupIdTarget": "BLN", "SystemTypeActor":
"ABBA", "SystemGroupTypeActor": "SAP", "SystemGroupTypeInitiator": "SAP",
"SystemGroupTypeIntermediary": "SAP", "SystemTypeReporter": "ABBA", "SystemGroupTypeReporter":
"SAP", "SystemGroupTypeTarget": "SAP", "UsernameDomainNameActing": "System25",
"UsernameDomainTypeActing": "ABBA", "UserPseudonymActing": "BLK_BTC_SMP",
"TechnicalTimestampInteger": "1632210279522" } ] } ] }
```

SAP Enterprise Threat Detection Cloud

Vendor: SAP

Product: Enterprise Threat Detection Cloud

Support Added: FortiSIEM 7.1.x, 7.2.x, 7.3.x via Content Update, FortiSIEM 7.4.1+

Product Information: <https://www.sap.com/products/financial-management/enterprise-threat-detection.html>

Information Collected

FortiSIEM collects SAP Enterprise Threat Detection (ETD) Cloud Alerts from SAP ETD Cloud via generic API poller using the /alerts/v1/Alerts API.

The following log types are collected:

Log Type	Event Type Prefix for corresponding FortiSIEM Events	Collection Method
Informational	SAP-ETD (1 event type)	API

You can go to **Resources > Event Types** and search for these event types by using the prefix.

Configuration

Step 1 - Acquire SAP ETD Cloud Client ID and Secret

1. In the SAP BTP Cockpit, navigate to your Global Account.
2. Go to **Instances and Subscriptions** under the **Instances** section.
3. Find the row for your previously created SAP ETD instance.
4. Click the Actions menu (three-dots icon) for that row.

5. Select **Create Service Key**.
6. Provide a name for the service key and click **Create**.
7. Once the service key is created, find the new row in the table.
8. Click the Actions menu (three-dots icon).
9. Select **View** or **Download**.
10. A pop-up showing the JSON data will appear with the **clientid** and **clientsecret**.
11. Note the **API URL** for token retrieval.
12. Copy and securely save these values.

Step 2 - Configuring FortiSIEM

Prerequisites

You will need the following from your SAP ETD service key JSON file:

- Client ID
- Client Secret
- Instance Hostname from the URL: e.g. `https://etdcloudprod-prod-etd-xxx-eu10.hana.ondemand.com`
FortiSIEM needs the hostname from this: `etdcloudprod-prod-etd-xxx-eu10.hana.ondemand.com`
- Token Auth Endpoint (User Account and Authentication (UAA) URL)

Example Service Key JSON, required values highlighted in Red.

```
{
  "url": "https://etdcloudprod-prod-etd-logcollector-service.cfapps.eu10.hana.ondemand.com",
  "uaa": {
    "tenantmode": "shared",
    "surl": "https://internal-xsuaa.authentication.eu10.hana.ondemand.com",
    "subaccountid": "19f17b61-41ab-465b-xxxx-d4870aaec4b7",
    "credential-type": "binding-secret",
    "clientid": "sb-logcollector-xxxx...",
    "xsappname": "logcollector-xxxx...",
    "clientsecret": "27d8a0b...=",
    "url": "https://etdcloudtest.authentication.eu10.hana.ondemand.com", (token auth url base)
    "uaadomain": "authentication.eu10.hana.ondemand.com",
    "verificationkey": "-----BEGIN PUBLIC KEY----- ...",
    "apiurl": "https://api.authentication.eu10.hana.ondemand.com",
    "identityzone": "etdcloudtest",
    "identityzoneid": "1xxxxx-40ab-465b-xxxx-d4870aaec4b7",
    "tenantid": "1xxxxx-40ab-465b-xxxx-d4870aaec4b7",
    "zoneid": "1xxxxx-40ab-465b-xxxx-d4870aaec4b7",
  }
}
```

Create New Credential

Take the following steps to configure a credential for FortiSIEM.

1. Download the SAP ETD JSON template file, [here](#).
2. Login to FortiSIEM as an administrator.

3. Navigate to **Admin > Setup > Credentials**.
4. Under **Step 1: Enter Credentials**, click **New**.
5. In the **Access Method Definition** window, input the following:
 - a. In the **Name** field, enter the name of the credential. For this example, enter "SAP_ETD_Cloud_Alerts".
 - b. From the **Device Type** drop-down list, select **SAP Enterprise Threat Detection**.
 - c. For **Access Protocol**, select **HTTPS Advanced**.
6. Click **Import Definition**.
 - a. Click **Choose File** and select the JSON template file you downloaded, then click **Import**.
 - b. When the prompt "Definition will be overwritten, continue?" appears, click **Yes**.
7. Click the Edit icon next to **General Parameters**.
 - a. In the **Host Name** field, replace the existing name with your SAP instance hostname.
 - b. Click **OK**.
8. Click the Edit icon next to **Authentication Parameters**.
 - a. In the **Access Token URL** field, replace the existing Access Token URL with your actual OAuth2.0 authorization URL. It should be in the format:
`https://etd-cloud-demo-xxxx.authentication.eu10.hana.ondemand.com/oauth/token?grant_type=client_credentials`
Replace the hostname portion with your UAA URL from your service key.
 - b. In the **Client Id** field, replace the Client Id with your actual Client Id.
In the **Client Secret** field, enter your Client Secret.
 - c. Click **OK**.
9. Click **Save**.

Create Credential to Device Mapping and Initiate Event Pulling

1. Under **Step 2: Enter IP Range to Credential Associations**, click **New**.
Note: If you have more than one collector, first select the collector from the drop-down prior to clicking **+**. If you have 1 collector or no collectors, this drop-down does not appear.
2. Select the Credential you just defined, "SAP_ETD_Cloud_Alerts".
The **IP/Host Name** field is pre-populated.
3. Click **Save**.
4. Select the Credential to Device Mapping and click **Test > Test Connectivity without Ping**.
5. In the next 5 minutes the first events will come in. Click the **Pull Events** tab to monitor.

Check SAP ETD Events in Analytics

To check events from **Analytics**, take the following steps.

1. Navigate to **Analytics > Search**.
2. Click inside the "Edit Filters and Time Range..." field, then enter the following search query:
Event Type CONTAIN SAP-ETD
3. Click **Apply & Run**, and you should see events coming in.

Sample Event

```

Jul 22 15:41:17 2025 etdcloudprod-0xx-prod-etd-cloud-data-retrieval-
service.cfapps.example.hana.ondemand.com 1.1.1.1 SAP_ETD_CLOUD_ALERT: {"AlertId": 25682,
"CreationTimestamp": "2025-07-22T15:40:04.334Z", "MaxTimestamp": "2025-07-22T15:35:24.928Z",
"Measure": 1, "MinTimestamp": "2025-07-22T15:20:24.919Z", "PatternDescription": "Issue an alert if
a successful or unsuccessful logon attempt from external with SAP standard users has occurred.",
"PatternName": "Logon from external with SAP standard users", "Score": 50, "Status": "OPEN",
"Threshold": 1, "Version": "1.1", "Source": [{"Name": "SystemIdActor", "Value": "Lab/200"},
{"Name": "NetworkHostnameInitiator", "Value": "192.168.0.25"}, {"Name": "EventSemantic", "Value":
"User, Logon, Failure"}, {"Name": "UserNameTargeted", "Value": "user02"}]},
"NormalizedTriggeringEvents": [{"AccountDomainNameActing": null, "AccountDomainNameInitiating":
null, "AccountDomainNameTargeted": null, "AccountDomainNameTargeting": null,
"AccountDomainTypeActing": null, "AccountDomainTypeInitiating": null, "AccountDomainTypeTargeted":
null, "AccountDomainTypeTargeting": null, "AttackName": null, "AttackType": null, "CorrelationId":
null, "CorrelationSubId": null, "Event": "AU6", "EventLogType": "SecurityAuditLog",
"EventMessage": null, "EventScenarioRoleOfActor": null, "EventScenarioRoleOfInitiator": null,
"EventSeverityCode": "High", "EventSourceId": "192.168.0.25", "EventSourceType": "IP Address",
"GenericAction": "Logon Targeted User", "GenericCategory": "RFC/CPIC Logon", "GenericDeviceType":
null, "GenericExplanation": null, "GenericGeolocationCodeActor": null,
"GenericGeolocationCodeTarget": null, "GenericOrder": null, "GenericOutcome": null,
"GenericOutcomeReason": "2", "GenericPath": null, "GenericPathPrior": null, "GenericPurpose":
null, "GenericRiskLevel": null, "GenericScore": null, "GenericSessionId": null, "GenericURI":
null, "Id": "313C797B099A4D5295AB08A211C79D7C", "NetworkHostDomainActor": null,
"NetworkHostDomainInitiator": null, "NetworkHostDomainIntermediary": null,
"NetworkHostDomainReporter": null, "NetworkHostDomainTarget": null, "NetworkHostnameActor": "test-
lab-04", "NetworkHostnameInitiator": "192.168.0.25", "NetworkHostnameIntermediary": null,
"NetworkHostnameReporter": "test-lab-04", "NetworkHostnameTarget": null, "NetworkIPAddressActor":
null, "NetworkIPAddressInitiator": "192.168.0.25", "NetworkIPAddressIntermediary": null,
"NetworkIPAddressReporter": null, "NetworkIPAddressTarget": null, "NetworkIPBeforeNATActor": null,
"NetworkIPBeforeNATTTarget": null, "NetworkInterfaceActor": null, "NetworkInterfaceTarget": null,
"NetworkMACAddressActor": null, "NetworkMACAddressInitiator": null,
"NetworkMACAddressIntermediary": null, "NetworkMACAddressReporter": null,
"NetworkMACAddressTarget": null, "NetworkNetworkPrefixActor": null, "NetworkNetworkPrefixTarget":
null, "NetworkPortActor": null, "NetworkPortBeforeNATActor": null, "NetworkPortBeforeNATTTarget":
null, "NetworkPortInitiator": null, "NetworkPortIntermediary": null, "NetworkPortReporter": null,
"NetworkPortTarget": null, "NetworkProtocol": "RFC", "NetworkSessionId": null, "NetworkZoneActor":
null, "NetworkZoneTarget": null, "ParameterDataType": "String", "ParameterDataTypeContext": null,
"ParameterDirection": null, "ParameterDirectionContext": null, "ParameterName": "Logon Type",
"ParameterNameContext": null, "ParameterType": null, "ParameterTypeContext": null,
"ParameterValueDouble": null, "ParameterValueDoublePriorValue": null, "ParameterValueNumber":
null, "ParameterValueNumberContext": null, "ParameterValueNumberPriorValue": null,
"ParameterValueString": "R", "ParameterValueStringContext": null,
"ParameterValueStringPriorValue": null, "ParameterValueTimestamp": null,
"ParameterValueTimestampPriorValue": null, "PrivilegeGranteeName": null, "PrivilegeGranteeType":
null, "PrivilegeIsGrantable": null, "PrivilegeName": null, "PrivilegeType": null,
"ResourceContainerName": null, "ResourceContainerType": null, "ResourceContent": null,
"ResourceContentType": null, "ResourceCount": null, "ResourceName": null, "ResourceNamePrior":
null, "ResourceRequestSize": null, "ResourceResponseSize": null, "ResourceSize": null,
"ResourceSumCriteria": null, "ResourceSumOverTime": null, "ResourceType": null,
"ResourceUnitsOfMeasure": null, "SemanticEventDisplayName": "User, Logon, Failure",

```

```

"ServiceAccessName": null, "ServiceApplicationName": null, "ServiceExecutableName": "00011",
"ServiceExecutableType": "D", "ServiceFunctionName": null, "ServiceInstanceName": "vhcalx3hci_S4H_
00", "ServiceOutcome": "Failure", "ServicePartId": null, "ServiceProcessId": null,
"ServiceProgramName": "SAPMSSY1", "ServiceReferrer": null, "ServiceRequestLine": null,
"ServiceTransactionName": null, "ServiceType": "RFC Logon", "ServiceUserAgent": null,
"ServiceVersion": null, "ServiceWorkflowName": null, "SystemGroupRoleActor": null,
"SystemGroupRoleInitiator": null, "SystemGroupRoleIntermediary": null, "SystemGroupRoleReporter":
null, "SystemGroupRoleTarget": null, "SystemIdActor": "Lab/200", "SystemIdInitiator": null,
"SystemIdIntermediary": null, "SystemIdReporter": "Lab/200", "SystemIdTarget": null,
"SystemRoleActor": "Test", "SystemRoleInitiator": null, "SystemRoleIntermediary": null,
"SystemRoleReporter": "Test", "SystemRoleTarget": null, "SystemTypeActor": "ABAP",
"SystemTypeInitiator": null, "SystemTypeIntermediary": null, "SystemTypeReporter": "ABAP",
"SystemTypeTarget": null, "TechnicalLogCollectorIPAddress": "192.168.0.25",
"TechnicalLogCollectorName": "LABLOCAL", "TechnicalLogCollectorPort": 10514, "TechnicalNumber":
"136092", "TechnicalNumberRange": null, "TimeDuration": null, "Timestamp": "2025-07-
22T15:20:24.919Z", "TimestampOfEnd": null, "TimestampOfStart": null, "TriggerNameActing": null,
"TriggerNameTargeted": null, "TriggerTypeActing": null, "TriggerTypeTargeted": null,
"UserAccountActing": null, "UserAccountInitiating": null, "UserAccountTargeted": "user02",
"UserAccountTargeting": null, "UserDepartmentActor": null, "UserFunctionActor": null,
"UserGroupActor": null, "UserGroupTarget": null, "UserLogonMethod": "Password", "UserTypeActor":
null, "UserTypeInitiator": null, "UserTypeTargeted": "B", "TechnicalGroupId": null,
"NetworkSubnetIdActor": null, "NetworkSubnetIdInitiator": null, "NetworkSubnetIdIntermediary":
null, "NetworkSubnetIdReporter": null, "NetworkSubnetIdTarget": null}, {"AccountDomainNameActing":
null, "AccountDomainNameInitiating": null, "AccountDomainNameTargeted": null,
"AccountDomainNameTargeting": null, "AccountDomainTypeActing": null,
"AccountDomainTypeInitiating": null, "AccountDomainTypeTargeted": null,
"AccountDomainTypeTargeting": null, "AttackName": null, "AttackType": null, "CorrelationId": null,
"CorrelationSubId": null, "Event": "AU6", "EventLogType": "SecurityAuditLog", "EventMessage":
null, "EventScenarioRoleOfActor": null, "EventScenarioRoleOfInitiator": null, "EventSeverityCode":
"High", "EventSourceId": "192.168.0.25", "EventSourceType": "IP Address", "GenericAction": "Logon
Targeted User", "GenericCategory": "RFC/CPIC Logon", "GenericDeviceType": null,
"GenericExplanation": null, "GenericGeolocationCodeActor": null, "GenericGeolocationCodeTarget":
null, "GenericOrder": null, "GenericOutcome": null, "GenericOutcomeReason": "2", "GenericPath":
null, "GenericPathPrior": null, "GenericPurpose": null, "GenericRiskLevel": null, "GenericScore":
null, "GenericSessionId": null, "GenericURI": null, "Id": "0684EE96340F4A218BAF6996835B467A",
"NetworkHostDomainActor": null, "NetworkHostDomainInitiator": null,
"NetworkHostDomainIntermediary": null, "NetworkHostDomainReporter": null,
"NetworkHostDomainTarget": null, "NetworkHostnameActor": "test-lab-04",
"NetworkHostnameInitiator": "192.168.0.25", "NetworkHostnameIntermediary": null,
"NetworkHostnameReporter": "test-lab-04", "NetworkHostnameTarget": null, "NetworkIPAddressActor":
null, "NetworkIPAddressInitiator": "192.168.0.25", "NetworkIPAddressIntermediary": null,
"NetworkIPAddressReporter": null, "NetworkIPAddressTarget": null, "NetworkIPBeforeNATAActor": null,
"NetworkIPBeforeNATTarget": null, "NetworkInterfaceActor": null, "NetworkInterfaceTarget": null,
"NetworkMACAddressActor": null, "NetworkMACAddressInitiator": null,
"NetworkMACAddressIntermediary": null, "NetworkMACAddressReporter": null,
"NetworkMACAddressTarget": null, "NetworkNetworkPrefixActor": null, "NetworkNetworkPrefixTarget":
null, "NetworkPortActor": null, "NetworkPortBeforeNATAActor": null, "NetworkPortBeforeNATTarget":
null, "NetworkPortInitiator": null, "NetworkPortIntermediary": null, "NetworkPortReporter": null,
"NetworkPortTarget": null, "NetworkProtocol": "RFC", "NetworkSessionId": null, "NetworkZoneActor":
null, "NetworkZoneTarget": null, "ParameterDataType": "String", "ParameterDataTypeContext": null,
"ParameterDirection": null, "ParameterDirectionContext": null, "ParameterName": "Logon Type",
"ParameterNameContext": null, "ParameterType": null, "ParameterTypeContext": null,

```

```

"ParameterValueDouble": null, "ParameterValueDoublePriorValue": null, "ParameterValueNumber":
null, "ParameterValueNumberContext": null, "ParameterValueNumberPriorValue": null,
"ParameterValueString": "R", "ParameterValueStringContext": null,
"ParameterValueStringPriorValue": null, "ParameterValueTimestamp": null,
"ParameterValueTimestampPriorValue": null, "PrivilegeGranteeName": null, "PrivilegeGranteeType":
null, "PrivilegeIsGrantable": null, "PrivilegeName": null, "PrivilegeType": null,
"ResourceContainerName": null, "ResourceContainerType": null, "ResourceContent": null,
"ResourceContentType": null, "ResourceCount": null, "ResourceName": null, "ResourceNamePrior":
null, "ResourceRequestSize": null, "ResourceResponseSize": null, "ResourceSize": null,
"ResourceSumCriteria": null, "ResourceSumOverTime": null, "ResourceType": null,
"ResourceUnitsOfMeasure": null, "SemanticEventDisplayName": "User, Logon, Failure",
"ServiceAccessName": null, "ServiceApplicationName": null, "ServiceExecutableName": "00010",
"ServiceExecutableType": "D", "ServiceFunctionName": null, "ServiceInstanceName": "vhcalx3hci_S4H_
00", "ServiceOutcome": "Failure", "ServicePartId": null, "ServiceProcessId": null,
"ServiceProgramName": "SAPMSSY1", "ServiceReferrer": null, "ServiceRequestLine": null,
"ServiceTransactionName": null, "ServiceType": "RFC Logon", "ServiceUserAgent": null,
"ServiceVersion": null, "ServiceWorkflowName": null, "SystemGroupRoleActor": null,
"SystemGroupRoleInitiator": null, "SystemGroupRoleIntermediary": null, "SystemGroupRoleReporter":
null, "SystemGroupRoleTarget": null, "SystemIdActor": "Lab/200", "SystemIdInitiator": null,
"SystemIdIntermediary": null, "SystemIdReporter": "Lab/200", "SystemIdTarget": null,
"SystemRoleActor": "Test", "SystemRoleInitiator": null, "SystemRoleIntermediary": null,
"SystemRoleReporter": "Test", "SystemRoleTarget": null, "SystemTypeActor": "ABAP",
"SystemTypeInitiator": null, "SystemTypeIntermediary": null, "SystemTypeReporter": "ABAP",
"SystemTypeTarget": null, "TechnicalLogCollectorIPAddress": "192.168.0.25",
"TechnicalLogCollectorName": "LABLOCAL", "TechnicalLogCollectorPort": 10514, "TechnicalNumber":
"139651", "TechnicalNumberRange": null, "TimeDuration": null, "Timestamp": "2025-07-
22T15:35:24.928Z", "TimestampOfEnd": null, "TimestampOfStart": null, "TriggerNameActing": null,
"TriggerNameTargeted": null, "TriggerTypeActing": null, "TriggerTypeTargeted": null,
"UserAccountActing": null, "UserAccountInitiating": null, "UserAccountTargeted": "user02",
"UserAccountTargeting": null, "UserDepartmentActor": null, "UserFunctionActor": null,
"UserGroupActor": null, "UserGroupTarget": null, "UserLogonMethod": "Password", "UserTypeActor":
null, "UserTypeInitiator": null, "UserTypeTargeted": "B", "TechnicalGroupId": null,
"NetworkSubnetIdActor": null, "NetworkSubnetIdInitiator": null, "NetworkSubnetIdIntermediary":
null, "NetworkSubnetIdReporter": null, "NetworkSubnetIdTarget": null}}}]

```

Security Orchestration (SOAR)

FortiSIEM supports these Security Orchestration, Automation and Response (SOAR) applications.

- [Fortinet FortiSOAR](#)

Fortinet FortiSOAR

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

What is Discovered and Monitored

Protocol	Log Format	Used for
Syslog	CEF	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortisoar" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configuring FortiSOAR for Syslog Forwarding

To configure FortiSOAR to forward syslog to FortiSIEM, take the following steps:

Note: It is recommended that you refer to the most current FortiSOAR Administration Guide for the latest configuration steps. Configuration steps here from the [7.0.0 FortiSOAR Administration Guide](#).

1. From FortiSOAR, navigate to **Settings > Configuration > Log Forwarding**.
2. Check the **Enable Log Forwarding** checkbox.
3. Configure the Syslog Server Details as follows.

Field	Input
Configuration Name	Input "FortiSIEM".
Server	Input the IP address or FQDN of the FortiSIEM Collector.
Protocol	Select UDP .
Port	Input "514".
Choose Log Types to Forward	Select all options.
Specify Audit Log Detail Level	Select Detailed .
Configure Audit Log Forward Rules	Select what you want logged to FortiSIEM.

4. Click **Save**.

Servers and Workstations

FortiSIEM supports these servers and workstations for discovery and monitoring.

- [Apple MacOS Servers and Workstations](#)
- [HP UX Server](#)
- [IBM AIX Server](#)
- [IBM OS400 Server](#)
- [Linux Server](#)
- [Microsoft Windows Server via OMI/SNMP/WMI](#)
- [Microsoft Windows Server via Agent](#)
- [QNAP Turbo NAS](#)
- [Sun Solaris Server](#)

Apple MacOS Servers and Workstations

Support Added: FortiSIEM 6.3.1

Last Modification: FortiSIEM 6.3.1

Vendor Version Tested: Not Provided

Vendor: Apple

Product: Apple MacOS

Product Information: <https://www.apple.com/macos/>, <https://www.apple.com/macos/server/>

- [Log Information](#)
- [Event Types](#)

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In 6.3.1, there are 17 event types.

HP UX Server

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	Hardware (cpu details, memory)	Memory paging rate, Disk I/O utilization	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "hp-ux" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "hp_ux" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- [SNMP v1 and v2c](#)
- [SSH](#)

SNMP v1 and v2c

1. Make sure that snmp libraries are installed. FortiSIEM has been tested to work with the default HP UX package that comes with snmpd preinstalled.
2. Start snmpd daemon with the default configuration by issuing `/etc/init.d/snmpd restart`.
3. Make sure that snmpd is running.

SSH

1. Make sure that the `vmstat` and `iostat` commands are available. If not, install these libraries.
2. Create a user account that can issue `vmstat` and `iostat` commands. FortiSIEM will use that user account to login to the server.

Settings for Access Credentials

- [SNMP, Telnet, and SSH Access Credentials for All Devices](#)
- [LDAP, LDAPS, LDAP Start TLS / Open LDAP Access Credentials for All Devices](#)
- [LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices](#)

SNMP, Telnet, and SSH Access Credentials for All Devices

See [Access Credentials](#).

LDAP, LDAPS, LDAP Start TLS / Open LDAP Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	HP HPUX
Access Protocol	LDAP / LDAPS / LDAP Start TLS

Settings	Value
Used For	OpenLDAP
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or 389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	HP HPUX
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	Microsoft Active Directory
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or 389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.

Settings	Value
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

IBM AIX Server

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	Hardware (cpu details, memory)	Memory paging rate, Disk I/O utilization	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "ibm_aix" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP v1 and v2c](#)
- [SSH](#)
- [Syslog](#)

SNMP v1 and v2c

1. Make sure that snmp libraries are installed. FortiSIEM has been tested to work with the default AIX package that comes with snmpd preinstalled.
2. Start snmpd daemon with the default configuration by issuing `/etc/init.d/snmpd restart`.
3. Make sure that snmpd is running.

SSH

1. Make sure that the `vmstat` and `iostat` commands are available. If not, install these libraries.
2. Create a user account that can issue `vmstat` and `iostat` commands. FortiSIEM will use that user account to log in to the server.

Syslog

1. Make sure that `/etc/syslog.conf` contains a `*.*` entry and points to a log file.

```
. @<SENSORIPADDRESS>
```

2. Refresh syslogd.

```
# refresh -s syslogd
```

Settings for Access Credentials

- [SNMP, Telnet, and SSH Access Credentials for All Devices](#)
- [LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices](#)
- [LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices](#)

SNMP, Telnet, and SSH Access Credentials for All Devices

See [Access Credentials](#).

LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	IBM AIX
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	OpenLDAP
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or 389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	IBM AIX
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	Microsoft Active Directory
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or

Settings	Value
	389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

IBM OS400 Server

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Parsed IBM OS400 Syslog Messages](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog		General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "os400" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM parses IBM OS 400 logs received via the PowerTech Agent as described [here](#). The PowerTech agent sends syslog to FortiSIEM.

Sample Parsed IBM OS400 Syslog Messages

```
Mar 18 17:49:36 ROBINSON CEF :0|PowerTech|Interact|2.0|UNA0603|A File Server transaction was
allowed for user JOHNDOE.|2| src =10.0.1.60 dst =10.0.1.180 msg=TYPE:JRN CLS :AUD JJOB :QPWFSERVSO
JUSER :JOHNDOE JNBR :025355 PGM :PLKR108JEL OBJECT : LIBRARY : MEMBER: DETAIL: OB JOHNDOE *FILESRV
CRTSTRMFIL QPWFSERVSO LNS0811 000112 00023 /home/JOHNDOE/subfolder
```

```
Mar 18 17:48:36 ROBINSON CEF :0|PowerTech|Interact|2.0|UNA0604|A File Server transaction was
allowed for user JOHNDOE.|2| src =10.0.1.60 dst =10.0.1.180 msg=TYPE:JRN CLS :AUD JJOB :QPWFSERVSO
JUSER :JOHNDOE JNBR :025355 PGM :PLKR108JEL OBJECT : LIBRARY : MEMBER: DETAIL: OB JOHNDOE *FILESRV
DLTSTRMFIL QPWFSERVSO LNS0811 000112 00025 /home/JOHNDOE/BoardReport
```

```
Mar 18 17:53:00 ROBINSON CEF :0|PowerTech|Interact|2.0|UNA0703|A System i FTP Client transaction
was allowed for user JOHNDOE.|3| src =10.0.1.180 dst =10.0.1.180 msg=TYPE:JRN CLS :AUD JJOB
:QTFTP00149 JUSER :JOHNDOE JNBR :029256 PGM :PLKR108JEL OBJECT : LIBRARY : MEMBER: DETAIL: ST
JOHNDOE *FTPCLIENT DELETEFILE QTFTP00149 LNS0811 000112 00033 /QSYS.LIB/PAYROLL.LIB/NEVADA.FILE
```

Linux Server

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Swap space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	OS type, Hardware (cpu details, memory)	Memory paging rate, Disk I/O utilization	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance
Syslog (via FortiSIEM Linux Agent)		File or directory change: User, Type of change, directory or file name	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "linux" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "linux" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "linux" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- [SNMP v1 and v2c](#)
- [SNMP v3](#)
- [SSH](#)
- [Syslog Logging](#)
- [Basic Linux File Monitoring over Syslog](#)

SNMP v1 and v2c

1. Make sure that snmp libraries are installed. FortiSIEM has been tested to work with net-snmp libraries.
2. Log in to your server with administrative access.
3. Make these modifications to the `/etc/snmp/snmpd.conf` file:
 - a. Define the community string for FortiSIEM usage and permit snmp access from FortiSIEM IP.
 - b. Allow FortiSIEM read-only access to the mib-2 tree.
 - c. Allow FortiSIEM read-only access to the enterprise MIB: UCD-SNMP-MIB.
 - d. Open up the entire tree for read-only view.
4. Reduce the logging level to avoid per connection logging which may cause resource issues (see [here](#) for more details):
 - a. Edit `/etc/sysconfig/snmpd` (on RedHat/CentOS) or `/etc/defaults/snmpd` (on Debian/Ubuntu)
 - b. Look for the line that passes the command line options to snmpd. On RedHat Enterprise 6 this looks like:

```
# snmpd command line options
OPTIONS="-LS0-6d -Lf /dev/null -p /var/run/snmpd.pid"
```

- c. Change the range from 0-6 to 0-5:

```
# snmpd command line options
OPTIONS="-LS0-5d -Lf /dev/null -p /var/run/snmpd.pid"
```

5. Restart the snmpd daemon by issuing `/etc/init.d/snmpd restart`.
6. Add the snmpd daemon to start from boot by issuing `chkconfig snmpd on`.

7. Make sure that snmpd is running.

SNMP v3

Configuring rwcommunity/rocommunity or com2sec

1. Log in to your Linux server.
2. Stop SNMP.

```
service snmpd stop
```

3. Use vi to edit the /etc/snmp/snmpd.conf file.
Before you edit this file, make sure you have created a backup, as it is very important to have a valid version of this file so the snmp daemon has correct credentials.

```
vi /etc/snmp/snmpd.conf
```

4. At the end of the file, add this line, substituting your username for snmpv3user and removing the <> tags: rouser <snmpv3user>.
5. Save the file.
6. Use vi to edit the /var/lib/snmp/snmpd.conf file.
Before you edit this file, make sure you have created a backup, as it is very important to have a valid version of this file for the SNMP daemon to function correctly.

```
vi /var/lib/snmp/snmpd.conf
```

7. At the end of the file, add this line, entering the username you entered in step 4, and then passwords for that user for MD5 and DES.
If you want to use SHA or AES, then add those credentials as well.

```
createUser <snmpv3user> MD5 <snmpv3md5password> DES <snmpv3despassword>
```

8. Save the file.
9. Reduce the logging level to avoid per connection logging which may cause resource issues (see [here](#) for more details)
 - a. Edit /etc/sysconfig/snmpd (on RedHat/CentOS) or /etc/defaults/snmpd (on Debian/Ubuntu)
 - b. Look for the line that passes the command line options to snmpd. On RedHat Enterprise 6 this looks like:

```
# snmpd command line options
OPTIONS="-LS0-6d -Lf /dev/null -p /var/run/snmpd.pid"
```

- c. Change the range from 0-6 to 0-5:

```
# snmpd command line options
OPTIONS="-LS0-5d -Lf /dev/null -p /var/run/snmpd.pid"
```

10. Restart SNMP.

```
service snmpd start
chkconfig auditd on
```

11. View the contents of the /var/lib/snmp/snmpd.conf file.

If this works, restarting `snmpd` will have no errors, also the entry that you created under `/var/lib/snmp/snmpd.conf` will be removed:

```
cat /var/lib/snmp/snmpd.conf
```

12. Run `snmpwalk -v 3 -u <snmpv3user> -l authpriv <IP> -a MD5 -A <snmpv3md5password> -x DES -X <snmpv3despassword>`

You will see your `snmpwalk` if this works. If there are any errors, see `net-snmp` for further instructions.

Configuring net-snmp-devel

If you have `net-snmp-devel` on your Linux server/client, follow these steps to configure SNMP v3.

1. Stop SNMP.

```
service snmpd stop
```

2. Run `net-snmp-config --create-snmpv3-user -ro -A <MD5passwordhere> -X <DESPasswordhere> -x DES -a MD5 <SNMPUSERNAME>`.**3. Restart SNMP.**

```
service snmpd start
```

4. Test by following step 10 from above.**SSH**

1. Make sure that the `vmstat` and `iostat` commands are available. If not, install these libraries.
2. Create a user account that can issue `vmstat` and `iostat` commands. FortiSIEM will use that user account to log in to the server.

Syslog Logging

Syslog forwarding can be configured on Linux servers to send the logs to FortiSIEM. There are different options regarding syslog configuration, including Syslog over TLS.

There are typically two commonly-used Syslog demons:

- [Syslog-ng](#)
- [Rsyslog](#)

Basic Syslog-ng Configuration

Follow these steps to enable basic `syslog-ng`:

1. Add the following line to your `syslog-ng` configuration:

```
{ udp("Collector IP" port(514));};
```

2. Restart the syslog-ng service or reload the configuration.

Additional Syslog-ng Configuration Information and Example

Source options are:

`internal()` means syslog-ng internal log messages.

`system()` means depending on your platform, syslog-ng will automatically collect the common log sources.

Filter functions:

`facility(xx,xx,xx)` allows filtering only the defined log facilities

Here is an example of configuring just authpriv and auth log facilities.

Note: Remember to replace italicized text with your content.

1. Open the `/etc/syslog-ng/syslog-ng.conf` file.
2. Add the following configuration.

```
source fsiem_source {
    internal();
    system();
};
filter fsiem_filter {
    facility(auth, authpriv);
};
destination fsiem_destination {
    udp("<collector_ip>" port(514));
};
log{
    source(fsiem_source);
    filter(fsiem_filter);
    destination(fsiem_destination);
};
```

3. Save the file and restart syslog-ng by running the command:
`service syslog-ng restart`
or
`systemctl restart syslog-ng`

Here is an example of verbose logging, where all log facilities are sent.

Note: Remember to replace italicized text with your content.

1. Open the `/etc/syslog-ng/syslog-ng.conf` file.
2. Add the following configuration.

```
source fsiem_source {
    internal();
    system();
};
destination fsiem_destination {
    udp("<collector_ip>" port(514));
};
```



```
log{
    source(fsiam_source);
    destination(fsiam_destination);
};
```

3. Save the file and restart syslog-ng by running the command:

```
service syslog-ng restart
or
systemctl restart syslog-ng
```

Basic Rsyslog Configuration

Follow these steps to enable rsyslog:

1. Add the following lines to your rsyslog configuration:

```
# Send logs to the FortiSIEM Collector
*.* @Collector IP:514
```
2. Restart the rsyslog service or reload the configuration.

Additional Rsyslog Configuration Information and Example

Rsyslog has a list of supported facilities, or app subsystems shown here.

Supported Facility/App Subsystem	Description
auth, authpriv	authentication and authorization logs
cron	cron scheduling
daemon	affects a daemon without any special classification (DNS, NTP, etc)
ftp	ftp server events
kern	kernel messages
lpr	printing subsystem
mail	email subsystem
news	Usenet subsystem messages, NNTP, etc...
syslog	internal syslogd server messages
user	user messages (generic)
uucp	UUCP server messages
local0 - local7	local user

Each message has a priority level, listed here from the most important to least important priority.

emerg, alert, crit, error, warn, notice, info, debug

In the rsyslog conf file, you can reference to log a facility in the format shown here.

`<facility>.<priority> @<server ip or name>:<server_port>`

where @ implies UDP and @@ implies TCP, and the italicized text should be replaced with your information.

A wildcard for any facility can be specified with an asterisk (*). For example:

*auth.** means any priority of auth messages are sent to target.

Here is a walk through example to just log authentication messages to FortiSIEM from modifying the rsyslog.conf file (`vi /etc/rsyslog.conf`)

Note: Remember to replace italicized text with your content.

1. Add the following lines to only add audit trails to be sent to the FortiSIEM collector.
`authpriv.* @<Your_FortiSIEM_Collectors_IP_or_Hostname>:514`
`auth.* @<Your_FortiSIEM_Collectors_IP_or_Hostname>:514`
2. Save the file and restart rsyslog using the following command.
`service rsyslogd restart`
or
`systemctl restart rsyslog.service`
3. log into this server or run a sudo command to confirm that logs appear in FortiSIEM, and that a CMDB entry is created if it does not already exist.
For verbose logging for all facilities and priorities, use the following.
`*.* @<server ip or hostname>:514`

Linux File Monitoring

FortiSIEM has licensed Linux agents that provide additional capabilities, such as custom log forwarding and central management. See the ["Linux Agent Installation Guide"](#) for details on this agent.

Settings for Access Credentials

- [SNMP Access Credentials for All Devices](#)
- [SSH Access Credentials for All Devices](#)

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Microsoft Windows Server via OMI/SNMP/WMI

Support Added: FortiSIEM 1.1

Last Modification: FortiSIEM 7.0.0

Vendor: Microsoft

Product Information: <https://www.microsoft.com/en-us/windows-server>

Supported OS Versions

- Windows 2008 and 2008 R2
- Windows 2012 and 2012 R2
- Windows 2016
- Windows 2019
- Windows 2022
- Windows 10
- Windows 11

Note: Starting with FortiSIEM 6.3.3, you can use Open Management Initiative (OMI) to discover and monitor and collect logs from Windows Servers. OMI uses a different API to collect data from the same WMI classes as WMI. So no changes to the Windows Server side is required to accommodate the OMI based communication. In other words, Windows Servers have to be configured identically for both WMI and OMI, and same restrictions apply for both.

- [What is Discovered and Monitored](#)
- [Data Collection Comparison - Agentless \(WMI/OMI\) versus FortiSIEM Windows Agent](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Windows Server Configuration for Data Collection](#)
- [Setting Access Credentials on FortiSIEM](#)

What is Discovered and Monitored

Installed Software Monitored via SNMP

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system	Uptime, Overall CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count,	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
	version, installed software , running processes, open TCP/UDP ports)	Installed Software change , Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	
SNMP	Vendor specific server hardware (hardware model, hardware serial number, fans, power supply, disk, raid battery). Currently supported vendors include HP and Dell	Hardware module status - fan, power supply, thermal status, battery, disk, memory . Currently supported vendors include HP and Dell	Availability Monitoring
WMI or OMI	Host name, OS (Win32_ComputerSystem), OS Serial Number (Win32_WindowsProductActivation), Memory, Uptime (Win32_OperatingSystem), Bios (Win32_BIOS), CPU (Win32_Processor), Disk info (Win32_LogicalDisk), Network interface (Win32_NetworkAdapterConfiguration), Services (Win32_Service), Running processes (Win32_Process), Installed Patches (Win32_QuickFixEngineering)	Uptime (Win32_OperatingSystem), CPU utilization (Win32_PerfRawData_PerfOS_Processor), Memory utilization, paging/swapping metrics (Win32_PerfRawData_PerfOS_Memory), Disk space utilization (Win32_LogicalDisk), Paging file utilization (Win32_PerfRawData_PerfOS_PagingFile), Disk I/O metrics (Win32_PerfRawData_PerfDisk_LogicalDisk), Network Interface utilization (Win32_PerfRawData_Tcpip_NetworkInterface), Running process metrics (Win32_Process, Win32_Service, Win32_PerfRawData_PerfProc_Process)	Performance Monitoring
WMI or OMI		Security, Application and System Event Logs including logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
Snare agent		Security, Application and System Event Logs including logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
Correlog agent		Security, Application and System Event Logs including logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
FortiSIEM Agent		Security, Application and System Event Logs, DNS, DHCP, IIS, DFS logs, Custom log files, File Integrity Monitoring, Registry Change Monitoring, Installed Software Change Monitoring, WMI and Powershell output monitoring, sysmon, User Entity Behavior Analysis (UEBA)	Security and Compliance
FortiSIEM Agent 5.0.0 and later		Uptime, CPU (total, individual), Memory (Total, Virtual, PageFile), Disk (Total, Individual), Network (Total, Individual), Application (Total, Running process resources).	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
		Application metrics (IIS, ASPNET, DNS, DHCP, NTDS)	

Recommendations:

Use Windows Agent 5.0.0 or later for all log collection, discovery and performance monitoring.

Notes:

- 1. Installed Software Monitored via SNMP** - Although information about installed software is available via both SNMP and WMI/OMI, FortiSIEM uses SNMP to obtain installed software information to avoid an issue in Microsoft's WMI implementation for the Win32_Product WMI class - see [Microsoft KB 974524](#) article for more information. Because of this bug, WMI/OMI calls to the Win32_Product class create many unnecessary Windows event log messages indicating that the Windows Installer has reconfigured all installed applications.
- 2. Winexe execution and its effect** - FortiSIEM uses the **winexe** command during discovery and monitoring of Windows servers for the following purposes.
 - Windows domain controller diagnostic (dcdiag) and replication monitoring (repadmin /replsummary)
 - HyperV Performance Monitoring
 - Windows Custom performance monitoring – to run a command (e.g. powershell) remotely on windows systems

Note: When using the winexe command, you must make sure the Windows Server has installed winexesvc.

- If the Windows Server enabled smbv1, running the winexe command remotely will automatically install the winexesvc command on the Windows Server.
- If the Windows Server only enabled smbv2, you must take the following steps.
 - Run the following command on Windows Powershell to check whether winexesvc is installed.
Get-Service -Name winexesvc
If it is installed, you are done. If it not installed, proceed to the next step.
 - On the FortiSIEM instance, download winexe-static-2 from the following link.
<https://github.com/Opmantek/open-audit/blob/master/other/winexe-static-2>
 - Run the following command.
./winexe-static-2 -U '<Account Name>%<Account Password>' //<Windows Device IP>
'cmd.exe'

The winexe-static-2 command will install winexesvc in the target Windows device automatically.

Data Collection Comparison - Agentless (WMI/OMI) versus FortiSIEM Windows Agent

Data Collection Features	WMI/OMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Security, Application, System Event Logs	Yes	Yes

Data Collection Features	WMI/OMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
File/Folder Edits	Yes	Yes
File Integrity Monitoring (FIM)	No	Yes
IIS Audit Logs	No	Yes
DNS Analytical Logs	No	Yes
Detailed DHCP Audit Logging	No	Yes
Support for all Windows Log Channels	No	Yes
Custom Log Sources	No	Yes
Windows Event Collector (WEC) and Windows Event Forwarding Support	No	Yes
Sysmon Support	No	Yes
Registry Change Monitoring	No	Yes
Installed Software Change Monitoring	No	Yes
WMI and Powershell Output Monitoring	No	Yes
Supports UEBA Telemetry Data	Limited*	Yes

*For more detailed information on supported UEBA event sources, see the latest Online Help [Appendix - Comparing UEBA Sources](#).

Performance Features	WMI/OMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Scalable for Large Environments	No	Yes
EPS Performance	100 EPS max	5K EPS
Performance Monitoring	Yes	Yes, with Windows Agent 5.0.0 and later.

Administrative Features	WMI/OMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Simplified Network Policies	No (TCP 135,1024-65535 inbound)	Yes (443 outbound)
Requires Domain or Local Service Account	No	No

Administrative Features	WMI/OMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Requires Install on Server or Workstation	No	Yes
FIPS Compliant Capable	No	Yes
Log Buffering Upon Connectivity Loss	No	Yes
Supports On and Off Network Monitoring	No	Yes
Secure Log Transmission	Yes	Yes

Event Types

In **ADMIN > Device Support > Event Types**, search for "windows server" to see the event types associated with this application or device.

Rules

In **RESOURCES > Rules**, search for "windows server" in the main content panel **Search...** field to see the rules associated with this application or device.

Reports

In **RESOURCES > Reports**, search for "windows server" in the main content panel **Search...** field to see the reports associated with this application or device.

Windows Server Configuration for Data Collection

- WinRM Configuration
- WMI/OMI Configuration
- Kerberos Configuration for OMI
- SNMP Configuration
- Security Audit Policy Configuration
- File Auditing Policy Configuration
- Disabling Audit Token Right Adjusted Success Events
- Syslog Configuration
- Print Log Configuration

WinRM Configuration

WinRM is needed for WMI/OMI monitoring and also for some FortiSIEM Remediation actions. It is enabled by default.

For WMI/OMI monitoring, WinRM service needs to be running. For FortiSIEM Remediation actions, the following additional steps are needed.

Enable WinRM and Set Authentication

Use the commands below to enable WinRM and set authentication on the target Windows Servers:

1. To configure Windows Server, run the following commands:

```
winrm quickconfig
winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
winrm enumerate winrm/config/listener
```

Notes:

- If HTTPS is not enabled, then open Windows PowerShell console as an administrator, and run the following command.
- Windows 2012 requires CA cert with **EKU 1.3.6.1.5.5.7.3.1**, Server Side authentication, OID to be included. Do not use the powershell command to create a self signed certificate.
`New-SelfSignedCertificate -Subject 'CN=<windows host name>' -TextExtension '2.5.29.37={text}1.3.6.1.5.5.7.3.1'`

Next, follow the instructions for your version of Microsoft Windows Server.

- [Microsoft Windows Server 2012](#)
- [Microsoft Windows Server 2012 R2](#)
- [Microsoft Windows Server Earlier than 2012, or 2016 and Later](#)

Microsoft Windows Server 2012

Windows 2012 requires CA cert with **EKU 1.3.6.1.5.5.7.3.1**, Server Side authentication, OID to be included. Do **NOT** use the PowerShell command to create a self signed certificate.

If HTTPS is not enabled, then open Windows PowerShell console as an administrator, and run the following commands.

```
winrm create winrm/config/Listener?Address=*&Transport=HTTPS '@{Hostname="<windows host name>";
CertificateThumbprint="<thumbprint received by New-Self Signed Certificate>"}'

winrm quickconfig -transport:https

winrm enumerate winrm/config/listener
```

Proceed to [Configure FortiSIEM Client](#).

Microsoft Windows Server 2012 R2

For Microsoft Windows Server 2012 R2, take the following steps.

1. Configure a Certificate Signing Request (CSR) from your Windows 2012 R2 server.
2. Obtain a CA SSL Certificate with a Server side authentication EKU OID.
3. In PowerShell, run the following command:
`Import-Certificate -FilePath: <path of ca certificate> -CertStoreLocation Cert:\LocalMachine\My`
4. From the output, record the thumbprint, for use in the next step. (Example output shown, with thumbprint in **bold**.)

```
PS C:\Users\Administrator> Import-Certificate -FilePath C:\thisserver2.cer -CertStoreLocation
Cert:\LocalMachine\My
    Directory: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
32525BCAC07E59E5321D297F96A94608421EDA71 CN=thisserver, OU=it, O=fortinet, L=sunnyvale,
S=california, C=US
```

5. Run the following commands:
`winrm create winrm/config/Listener?Address=*&Transport=HTTPS '@{Hostname="<windows host name>"; CertificateThumbprint="<thumbprint received by New-Self Signed Certificate>"}`
`winrm quickconfig -transport:https`
`winrm enumerate winrm/config/listener`
6. To configure FortiSIEM Client (Supervisor or Collector), run the following command.
`pip3 install pywinrm`

Microsoft Windows Server Earlier than 2012, or 2016 and Later

If HTTPS is not enabled, then open Windows PowerShell console as an administrator, and run the following commands:

Note: Single quotes are needed for Windows 2016 and later.

```
New-SelfSignedCertificate -Subject 'CN=<windows host name>' -TextExtension '2.5.29.37={text}1.3.6.1.5.5.7.3.1'

winrm create winrm/config/Listener?Address=*&Transport=HTTPS '@{Hostname="<windows host name>";
CertificateThumbprint="<thumbprint received by New-Self Signed Certificate>"}
```

```
winrm quickconfig -transport:https

winrm enumerate winrm/config/listener
```

Next, proceed to [Configure FortiSIEM Client](#).

Configure FortiSIEM Client

To configure FortiSIEM Client (Supervisor or Collector), run the following command.

```
pip install pywinrm
```

WMI/OMI Configuration

These configurations are needed if you are using either WMI or OMI to monitor Windows Servers.

- [WMI/OMI Configuration for Windows 2012, 2012 R2, 2016, 2019, 2022, Windows 10, 11](#)
- [WMI/OMI Configuration for Windows 2008 and 2008 R2](#)

WMI/OMI Configuration for Windows 2012, 2012 R2, 2016, 2019, 2022, Windows 10, 11

You must create an user with sufficient permissions to access WMI objects. This user account will be used from FortiSIEM. There are two cases.

- [Create a User Belonging to the Domain or Local Administrator Group](#)
- [Create a Generic User \(Not Belonging to these Highly Privileged Groups\)](#)

Note the difference in capabilities between these two users

- [Capability Difference between Domain/Local Administrator Users and Generic Users](#)

Create a User Belonging to the Domain or Local Administrator Group

Log in to the Domain Controller with an administrator account.

Step 1. Create a User Belonging to Domain or Local Administrator Group

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **New > User**.
3. Create a new user.
4. Right-click **Domain Admins** in **Users** and select **Properties**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. Click **Advanced > Find Now**, add the **Administrator** and the user which you created during [step 3](#).
7. Click **OK** to close the **User** select dialog.
8. Click **OK** to close the **Domain Admins Properties** dialog.

Step 2: Enable DCOM Permissions for the New User

Log in to the machine you want to monitor with an administrator account.

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.

3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **COM Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that the user has the permission **Allow** for both **Local Access** and **Remote Access**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in [Step 1](#).
8. Click **OK**.
9. In the **COM Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in [Step 1](#).
11. In the **COM Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in [Step 1](#) from [Create a Generic User \(Not Belonging to Highly Privileged Domain Administrator Group\)](#).
13. Click **OK**.

Step 3: Enable Account Privileges in WMI for the New User

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2**.
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**. If the user is not present, then click **Add** to add the user you created.
7. Click **Advanced**.
8. Select the user you created for the monitoring account, and then click **Edit**.
9. In the **Applies onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the **Permission Entry** for **CIMV2** dialog.
11. Click **OK** to close the **Advanced Security Settings** for **CIMV2** dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Step 4: Allow WMI through Windows Firewall

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and then click **OK**. You can configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the User Guide.

Step 5: Make sure WinRM Service is Running

For information on configuring WinRM, see [WinRM Configuration](#). Note that in Windows 10 and Windows 11, it may be disabled by default and you need to enable it.

Create a Generic User (Not Belonging to Highly Privileged Domain Administrator Group)

Log in to the machine you want to monitor with an administrator account.

Step 1. Create a New User Belonging to *Distributed COM Users, Remote Management Users and Performance Monitor Users Groups*

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **New User**.
3. Create a user.
4. Select this user and right-click to select **Properties > Member of** tab.
5. Click **Add > Advanced > Find Now**.
6. Select and add the following groups:
 - **Distributed COM Users** group.
 - **Performance Monitor Users** group.
 - **Remote Management Users** group.

Note: To select multiple groups, hold down the **CTRL** key and click the desired groups.

7. Click **OK** to save.

Step 2: Add the User to Log Reader Group

To configure the non-administrative user to monitor windows event logs, follow the steps below:

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers (Computer Management > Local Users and Groups for servers that are not a domain controller)**.
2. Right-click the non-admin user and select **Properties**.
3. Select the **Member of** tab.
4. Select the group **Event Log Reader** and click **Add**.
5. Click **Apply**.

6. Click **OK** to complete the configuration.

Step 3. Enable DCOM Permissions for the New User

1. Go to **Start > Control Panel > Administrative Tools > Component Services > Computers > My Computer**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **Edit Default**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in [Step 1](#).
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow for Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow for Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in [Step 1](#).
14. Click **OK**.

Step 4: Enable Access to Win32_Service Class

To gain access to Win32_Service, this needs to be executed (with admin privileges) on the Windows box using `cmd.exe` or powershell prompt:

```
sc sdset SCMANAGER D:(A;;;CCLCRPRC;;;AU)(A;;;CCLCRPWPRC;;;SY)(A;;;KA;;;BA)S:(AU;FA;KA;;;WD)
(AU;OIIOFA;GA;;;WD)
```

See Reference: <https://stackoverflow.com/questions/3917477/granting-remote-user-non-admin-the-ability-to-enumerate-services-in-win32-serv/4432737#4432737>

Step 5. Enable WMI Account Privileges for the New User

See the [Enable Account Privileges in WMI for the New User](#) section in **Create a User Belonging to the Domain or Local Administrator Group** for set up instructions to configure WMI.

Step 6: Allow WMI through Windows Firewall

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow apps to communicate through Windows Defender Firewall**.

3. Click **Change settings**.
4. Locate **Windows Management Instrumentation (WMI)**, and click the checkbox to enable your connected networks.
5. Locate **Windows Remote Management**, and click the checkbox to enable to enable your connected networks.
6. Locate **Windows Remote Management (Compatibility)**, and click the checkbox to enable your connected networks.
7. Click **OK**. You can configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the User Guide.

Step 7: Make sure WinRM Service is Running

For information on configuring WinRM, see [WinRM Configuration](#). Note that in Windows 10 and Windows 11, it may be disabled by default and you need to enable it.

Capability Difference between Domain/Local Administrator Users and Generic Users

Windows allows certain WMI classes to be pulled only via Administrator account. The following table shows this clearly.

WMI Class	Administrator	Non-Administrator
Win32_BIOS	Yes	No
Win32_ComputerSystem	Yes	Yes
Win32_LogicalDisk	Yes	No
Win32_NetworkAdapter	Yes	Yes
Win32_NetworkAdapterConfiguration	Yes	Yes
Win32_NTLogEvent	Yes	Yes
Win32_OperatingSystem	Yes	Yes
Win32_Process	Yes	Yes
Win32_Processor	Yes	Yes
Win32_Product	Yes	Yes
Win32_QuickFixEngineering	Yes	No
Win32_Service	Yes	Yes
Win32_UserAccount	Yes	No
win32_Volume	Yes	Yes
Win32_PerfFormattedData_DHCPserver_DHCPserver	Yes	Yes

WMI Class	Administrator	Non-Administrator
Win32_PerfFormattedData_DNS_DNS	Yes	Yes
Win32_PerfFormattedData_W3SVC_WebService	Yes	Yes
Win32_PerfRawData_DirectoryServices_DirectoryServices	Yes	Yes
Win32_PerfRawData_NTDS_NTDS	Yes	Yes
Win32_PerfRawData_PerfDisk_LogicalDisk	Yes	Yes
Win32_PerfRawData_PerfDisk_PhysicalDisk	Yes	Yes
Win32_PerfRawData_PerfOS_Memory	Yes	Yes
Win32_PerfRawData_PerfOS_PagingFile	Yes	Yes
Win32_PerfRawData_PerfOS_Processor	Yes	Yes
Win32_PerfRawData_PerfProc_Process	Yes	Yes
Win32_PerfRawData_Tcpip_NetworkInterface	Yes	Yes

WMI/OMI Configuration for Windows 2008 and 2008 R2

You must create an user with sufficient permissions to access WMI objects. There are two cases.

1. [Create a New User Belonging to Domain or Local Administrator Group](#)
2. [Create a Generic User \(Not Belonging to Highly Privileged Domain Administrator Group\)](#)

Note the difference in capabilities between these two users

[Capability Difference between Domain/Local Administrator Users and Generic Users](#)

Create a New User Belonging to Domain or Local Administrator Group

Log in to the Domain Controller with an administrator account.

Step 1. Create a New User and Add the User to Domain or Local Administrator Group

1. Go to **Start > Control Pane > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you just created in [step 3](#).
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Step 2: Enable DCOM Permissions for the New User

Log in to the machine you want to monitor with an administrator account.

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Step 3: Enable WMI Account Privileges for the New User

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2**.
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced**.
8. Select the user you created for the monitoring account, and then click **Edit**.
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Step 4: Allow WMI to Connect Through the Windows Firewall

Follow the appropriate instructions per your software.

- [Allow WMI to Connect Through the Windows Firewall \(Windows 2003\)](#)
- [Allow WMI through Windows Firewall \(Windows Server 2008, 2012\)](#)

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and then click **OK**. You can configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Step 5: Make sure WinRM Service is Running

For information on configuring WinRM, see [WinRM Configuration](#).

Create a Generic User (Not Belonging to Highly Privileged Domain Administrator Group)

Log in to the machine you want to monitor with an administrator account.

Step 1. Create a New User Belonging to *Distributed COM Users and Performance Monitor Users Groups*

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **New User**.
3. Create a user.
4. Select this user and right-click to select **Properties > Member of** tab.
5. Select **Distributed COM Users** and click **Add**.
6. Click **OK** to save.

This is the account you must use to set up the Performance Monitor Users group permissions.

7. Repeat steps 4 through 6 for the **Performance Monitor Users** group.

Step 2: Add the User to Log Reader Group

To configure the non-administrative user to monitor windows event logs, follow the steps below:

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers (Computer Management > Local Users and Groups** for servers that are not a domain controller).
2. Right-click the non-admin user and select **Properties**.
3. Select the **Member of** tab.
4. Select the group **Event Log Reader** and click **Add**.
5. Click **Apply**.
6. Click **OK** to complete the configuration.

Step 3. Enable DCOM Permissions for the New User

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **Edit Default**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Step 4: Enable WMI Account Privileges for the New User

See the [Enable WMI Account Privileges for the New User](#) section in the **Create a New User Belonging to Domain or Local Administrator Group** instructions to configure WMI.

Step 5: Allow WMI through Windows Firewall (Windows 2003 or Windows Server 2008, 2012)

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.

3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run cmd.exe and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"
netsh firewall add allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and then click **OK**. You can configure FortiSIEM to communicate with your device. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Step 6: Make sure WinRM Service is Running

For information on configuring WinRM, see [WinRM Configuration](#).

Capability Difference between Domain/Local Administrator Users and Generic Users

Windows allows certain WMI classes to be pulled only via Administrator account. The following table shows this clearly.

WMI Class	Administrator	Non-Administrator
Win32_BIOS	Yes	No
Win32_ComputerSystem	Yes	Yes
Win32_LogicalDisk	Yes	No
Win32_NetworkAdapter	Yes	Yes
Win32_NetworkAdapterConfiguration	Yes	Yes
Win32_NTLogEvent	Yes	Yes
Win32_OperatingSystem	Yes	Yes
Win32_Process	Yes	Yes
Win32_Processor	Yes	Yes

WMI Class	Administrator	Non-Administrator
Win32_Product	Yes	Yes
Win32_QuickFixEngineering	Yes	No
Win32_Service	Yes	No
Win32_UserAccount	Yes	No
win32_Volume	Yes	Yes
Win32_PerfFormattedData_DHCPServer_DHCPServer	Yes	Yes
Win32_PerfFormattedData_DNS_DNS	Yes	Yes
Win32_PerfFormattedData_W3SVC_WebService	Yes	Yes
Win32_PerfRawData_DirectoryServices_DirectoryServices	Yes	Yes
Win32_PerfRawData_NTDS_NTDS	Yes	Yes
Win32_PerfRawData_PerfDisk_LogicalDisk	Yes	Yes
Win32_PerfRawData_PerfDisk_PhysicalDisk	Yes	Yes
Win32_PerfRawData_PerfOS_Memory	Yes	Yes
Win32_PerfRawData_PerfOS_PagingFile	Yes	Yes
Win32_PerfRawData_PerfOS_Processor	Yes	Yes
Win32_PerfRawData_PerfProc_Process	Yes	Yes
Win32_PerfRawData_Tcpip_NetworkInterface	Yes	Yes

Kerberos Configuration for OMI

If the Windows Server to be monitored using OMI is part of a Windows Domain that uses Kerberos authentication, then you need to take 2 steps:

1. [Add IP to Windows Server name mapping \(PTR record\) to Windows DNS Server.](#)
2. [Add Windows DNS Server name to the list of resolvers in FortiSIEM Collector.](#)

These steps are needed because FortiSIEM uses IP to communicate while OMI/Kerberos needs host name (FQDN).

Windows DNS Server Configuration

1. Log into your Windows DNS server with an admin account.
2. Find Windows Server DNS Manager.
3. Navigate to **Forward Lookup** under **DNS Zones**, and locate your DNS domain.
4. Under your DNS domain, locate the host name (A records) for each server you are monitoring via OMI and make sure the IP address is correct.

5. Under **Reverse Lookup Zones**, look up the zone corresponding to your subnet. Add a PTR record for each server you are monitoring via OMI.

FortiSIEM Collector Configuration

1. Open the file (/etc/resolv.conf)
2. Add Windows DNS Server name to the list of resolvers.

```
[admin@FSM-User]$ cat /etc/resolv.conf
# Generated by NetworkManager
...
nameserver <Windows DNS Server IP>
...
```

3. Save.

SNMP Configuration

- [Enabling SNMP on Windows Server 2012 R2, Server 2016, Server 2019, Server 2022](#)
- [Enabling SNMP on Windows 7 or Windows Server 2008 R2](#)
- [Enabling SNMP on Windows Server 2003](#)

Enabling SNMP on Windows Server 2012 R2, Server 2016, Server 2019, Server 2022

SNMP is typically enabled by default on Windows Server 2012 R2, Server 2016, and Server 2019. But you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First, you should check that SNMP Services have been enabled for your server.

1. Log in to the Windows 2016 Server where you want to enable SNMP as an administrator.
2. In the **Start** menu, select **Control Panel**.
3. Under **Programs**, click **Turn Windows features on/off**.
4. The **Add Roles and Features Wizard** will open automatically.
5. Select **Role-based** or **feature-based installation**. Click **Next** until the **Features** option appears.
6. Under **Features**, see if **SNMP Services** is installed.
If not, check the checkbox before the **SNMP Service** and click **Next** to install the service.
7. From the **Start** menu, select **Services**. Go to **Services > SNMP Services**.
8. Select and open **SNMP Service**.
9. Click the **Security** tab.
10. Select **Send authentication trap**.
11. Under **Accepted communities**, make sure there is an entry for public that is set to read-only.
12. Select **Accept SNMP packets** from these hosts.
13. Click **Add**.
14. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
15. Click **Add**.

16. Click **Apply**.
17. Under **SNMP Service**, click **Restart service**.
18. 18. Go to **Control Panel > Windows Firewall**.
19. 19. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
20. 20. Select **SNMP Service**, and the click **OK**.

Enabling SNMP on Windows 7 or Windows Server 2008 R2

SNMP is typically enabled by default on Windows Server 2008, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you should check that SNMP Services have been enabled for your server.

1. Log in to the Windows 2008 Server where you want to enable SNMP as an administrator.
2. In the **Start** menu, select **Control Panel**.
3. Under **Programs**, click **Turn Windows features on/off**.
4. Under **Features**, see if **SNMP Services** is installed.
If not, click **Add Feature**, then select **SNMP Service** and click **Next** to install the service.
5. In the **Server Manager** window, go to **Services > SNMP Services**.
6. Select and open **SNMP Service**.
7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts**.
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service**.
16. 18. Go to **Control Panel > Windows Firewall**.
17. 19. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
18. 20. Select **SNMP Service**, and the click **OK**.

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you must make sure that the SNMP Management tool has been enabled for your device.

1. In the **Start** menu, go to **Administrative Tools > Services**.
2. Go to **Control Panel > Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Select **Management and Monitoring Tools** and click **Details**.
Make sure that **Simple Network Management Tool** is selected.
If it isn't selected, select it, and then click **Next** to install.
5. Go to **Start > Administrative Tools > Services**.
6. Select and open **SNMP Service**.

7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts**.
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service**.
16. 18. Go to **Control Panel > Windows Firewall**.
17. 19. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
18. 20. Select **SNMP Service**, and the click **OK**.

Security Audit Policy Configuration

Because Windows generates a lot of security logs, you should specify the categories of events that you want logged and available for monitoring by FortiSIEM.

1. Log in the machine where you want to configure the policy as an administrator.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand **Local Policies** and select **Audit Policy**.
You will see the current security audit settings.
4. Select a policy and edit the **Local Security Settings** for the events you want audited. Recommended settings are:

Policy	Description	Settings
Audit account logon events and Audit logon events	For auditing logon activity	Select Success and Failure
Audit object access events	For auditing access to files and folders. There is an additional configuration requirement for specifying which files and folders, users and user actions will be audited. See the next section, File Auditing Policy Configuration .	Select Success and Failure
Audit system events	Includes system up/down messages	

File Auditing Policy Configuration

When you enable the policy to audit object access events, you also must specify which files, folders, and user actions will be logged. You should be very specific with these settings, and set their scope to be as narrow as possible to avoid excessive logging. For this reason you should also specify system-level folders for auditing.

1. Log in the machine where you want to set the policy with administrator privileges.
On a domain computer, a Domain administrator account is needed

2. Open Windows Explorer, select the file you want to set the auditing policy for, right-click on it, and select **Properties**.
3. In the **Security** tab, click **Advanced**.
4. Select the **Auditing** tab, and then click **Add**.
This button is labeled **Edit** in Windows 2008.
5. In the **Select User or Group** dialog, click **Advanced**, and then find and select the users whose access to this file you want to monitor.
6. Click **OK** when you are done adding users.
7. In the **Permissions** tab, set the permissions for each user you added.

The configuration is now complete. Windows will generate audit events when the users you specified take the actions specified on the files or folders for which you set the audit policies.

Disabling Audit Token Right Adjusted Success Events

As per Microsoft, it is recommended to Disable "Success" auditing for "Audit Token Right Adjusted".

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4703#security-monitoring-recommendations>.

By enabling "Success Auditing" for Audit Token Right Adjusted (Detailed Tracking), 800+ (4703) events can be generated in a second, resulting in this high volume event impacting system performance.

Complete these steps to disable "Success" for "Audit Token Right Adjusted".

1. Log in, with administrator privileges, to the machine where you want to set the policy.
On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand to **Security Settings > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Object > Detailed Tracking**.
4. Go to the **Detailed Tracking** subcategory, and select **Audit Token Right Adjusted**.
5. Double click **Audit Token Right Adjusted**, select the **Configure the following audit events:** checkbox.
6. Uncheck the **Success** checkbox if needed to disable.
7. Click **Apply**.

Syslog Configuration

See the [Windows Agent Installation Guide](#) for information on configuring the sending of syslog from your device to FortiSIEM.

Sample Windows Server Syslog

```
<108>2014 Dec 17 15:05:47 CorreLog_Win_Agent 1NDCITVWCVL05.tsi.lan Login Monitor: Local Console  
User Login: User Name: example-admin
```

Print Log Configuration

FortiSIEM supports pull Windows print log from Windows agent. To configure, take the following steps.

- [Enabling Logging Print Log after WMI Configuration](#)
- [Setup in FortiSIEM](#)

Enabling Logging Print Log after WMI Configuration

After [WMI Configuration](#) is completed, enable logging print log by taking the following steps.

1. Open the **Event Viewer** window and navigate to **Applications and Services Logs > Microsoft > Windows > PrintService**.
2. Click **Operational**.
3. Right click, and select **Properties**.
4. Add a checkmark to the **Enable logging** checkbox.
5. Click **Apply**.
6. Click **OK**.

All print activities will be logged by Event Viewer through WMI. Event logs can be viewed under **Applications and Services Logs -> Microsoft -> Windows -> PrintService -> Operational**.

Setup in FortiSIEM

Take the following steps to access print logs in FortiSIEM.

1. Log on to your Windows Server and navigate to **Event viewer > App and Service logs > Microsoft > windows > printservice > properties**.
2. Copy the full name from log properties.
3. Log onto FortiSIEM in super global.
4. Navigate to **ADMIN > Setup > Windows Agent**.
5. Under **Windows Agent Monitor Templates**, click **New** to create a Monitor Template.
6. In the **Name** field, enter a name for the template.
7. Click the **Event** tab.
8. In the Event Log row, click on **New**.
9. In the **Type** drop-down list, select **Other**.
10. In the **Event Name** field, enter/paste the full name from step 2.
11. Click **< Save**.
12. Click **Save**.
13. Under **Host to Template Associations**, create a host to template association by clicking **New**.
14. In the **Name** field, enter a name.
15. Choose an organization.
16. Select the monitor template you created through steps 5-12.
17. Select a collector.
18. Click **Save**.

19. Click **Apply.**

FortiSIEM now automatically parses events received via WMI or FortiSIEM Windows Agent.

Setting Access Credentials on FortiSIEM

Navigate to **ADMIN > Setup > Credentials**, and in **Step 1: Enter Credentials**, click **New** to create a new Access Credential.

After the credential has been created, navigate to **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping for the newly created Access Credential.

For general information on setting credentials see [Setting Credentials](#). Specific Access Credentials settings are available here.

- [SNMP, Telnet and SSH Access Credentials](#)
- [LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials](#)
- [LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials](#)
- [WMI Access Credentials](#)
- [OMI Access Credentials](#)

SNMP, Telnet and SSH Access Credentials

See [Access Credentials](#).

LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials

Settings	Value
Name	<set name>
Device Type	Microsoft Windows Server *
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	OpenLDAP
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or 389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.

Settings	Value
Base DN	Specify the root of the LDAP tree as the Base DN. For example: dc=companyABC,dc=com
Password Config	See Password Configuration in Access Credentials .
User Name	For user discoveries from an OpenLDAP directory, specify the full DN as the user name. For example: uid=jdoe,ou=hr,ou=unit,dc=companyABC,dc=com
Password	Password of the user able to access this system

LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials

Settings	Value
Name	<set name>
Device Type	Microsoft Windows Server *
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	Microsoft Active Directory
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or 389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.
Base DN	Specify the root of the LDAP tree as the Base DN. For example: dc=companyABC,dc=com
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration in Access Credentials .
User Name	For Microsoft Active Directory, the user name can be just the login name.

Settings	Value
Password	Password of the user able to access this system

WMI Access Credentials

Settings	Value
Name	<set name>
Device Type	Microsoft Windows Server *
Access Protocol	WMI
Pull Interval	1 minute
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration in Access Credentials .
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

OMI Access Credentials

Settings	Value
Name	<set name>
Device Type	Microsoft Windows Server *
Access Protocol	OMI
Authentication	Select "ntlm auth" or "kerberos auth". If you have FIPS enabled, kerberos auth is required for FIPs to work. Kerberos authentication requires the following fields to be entered: • kerberos-AD-Server: Enter the fully qualified domain name or IP Address of the kerberos active directory server. See Kerberos Configuration for more information.

Settings	Value
	• kerberos-domain: Enter the full Kerberos domain name.
Pull Interval	1 minute
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration in Access Credentials .
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

Microsoft Windows Server via Agent

Support Added: FortiSIEM 1.1

Last Modification: FortiSIEM 7.0.0

Vendor: Microsoft

Product Information: <https://www.microsoft.com/en-us/windows-server>

Supported OS Versions

- Windows 2008 and 2008 R2
- Windows 2012 and 2012 R2
- Windows 2016
- Windows 2019
- Windows 2022
- Windows 10
- Windows 11

Overview

FortiSIEM Windows Agent can collect a wide variety of logs and other telemetry from Windows hosts. This document covers how to configure Windows Services to send the required metrics to FortiSIEM.

Compared to OMI based log collection, Windows Agent has many advantages shown in the following table.

Feature	Agent based collection	OMI based collection
Discovery and Performance Monitoring	Yes	Yes (however, installed software can't be discovered)
Collect Security, System, Application logs	Yes	Yes
Collect Sysmon	Yes	No
Collect DNS logs (Debug Logs, Analytical logs)	Yes	No
Collect DHCP logs	Yes	No
Collect IIS logs	Yes	No
Collect Generic Application logs	Yes	No
File Integrity Monitoring	Yes	Limited(1)
Certificate Monitoring	Yes	Limited(1)
Registry Change Monitoring	Yes	Limited(1)
Installed Software Change Monitoring	Yes	No
WMI and Powershell output Monitoring	Yes	No
Windows Event Forwarding Support	Yes	No
User Entity Behavior Anomaly (UEBA) Telemetry	Yes	Limited(1)
Use osquery to get current host information for threat hunting and other use cases	Yes	No
High volume log collection	Yes	Limited(2)

Notes:

- Limited(1) means limited capabilities using Security Event logs
- Limited(2) means that noticeable collection delay observed after 100 events per second.

This document covers the following topics.

- [Configuring Discovery and Performance Monitoring](#)
- [Collecting Windows Security Logs](#)
- [Collecting Windows System and Application Logs](#)
- [Collecting Windows Sysmon Logs](#)
- [Collecting Windows DNS Logs](#)
- [Collecting Windows DHCP Logs](#)
- [Collecting Windows IIS Logs](#)
- [Collecting Generic Application Logs](#)
- [Configuring File Integrity Monitoring](#)
- [Configuring Certificate Monitoring](#)
- [Configuring Registry Change Monitoring](#)

- [Configuring Installed Software Change Monitoring](#)
- [Configuring WMI and PowerShell Output Monitoring](#)
- [Configuring Windows User Entity Behavior Anomaly \(UEBA\)](#)
- [Configuring OpenSSH Operational and Admin Logs](#)
- [Configuring Osquery](#)
- [Recommended Log Sources by Use Case](#)
- [Configuring Windows Event Forwarding](#)

Configuring Discovery and Performance Monitoring

Windows Agent can be configured to discover a host that enables FortiSIEM to populate CMDB, just like Windows OMI based discovery. Discovered information includes:

- **General information** – Host name, OS, version
- **Hardware information** – CPU, memory, network interfaces, disk
- **Software information** – Running services, processes, installed software, patches

Windows Agent can also be configured to monitor system and certain application-level performance metrics:

- **System level** – Uptime, CPU utilization, memory utilization, disk utilization, network interface utilization
- **Process level** – CPU utilization and memory utilization per process
- **Application level** – DNS, DHCP, Active Directory, ASPNET and IIS metrics

No configuration is needed on the Windows side.

On FortiSIEM, follow these steps to configure discovery and performance monitoring:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Monitor** tab.
 - c. Use the checkboxes to select the various items to be discovered or monitored and configure the polling frequency.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Performance Monitoring Events

Type	Event Type	Description
System Performance Monitoring	PH_DEV_MON_SYS_UPTIME	System uptime for a device
	PH_DEV_MON_SYS_CPU_UTIL	System CPU Utilization for a device
	PH_DEV_MON_SYS_MEM_UTIL	System memory Utilization stats for a device
	PH_DEV_MON_SYS_DISK_UTIL	Disk Utilization stats for a device
	PH_DEV_MON_NET_INTF_UTIL	Network Interface utilization stats for a device
Application-level Performance Monitoring	PH_DEV_MON_PROC_RESOURCE_UTIL	Process CPU and Memory Utilization stats
	PH_DEV_MON_APP_DNS_MET	Windows DNS performance metrics
	PH_DEV_MON_APP_DHCP_MET	Windows DHCP performance metrics
	PH_DEV_MON_APP_IIS_MET	Microsoft IIS performance metrics
	PH_DEV_MON_APP_ASPNET_MET	ASP.NET performance metric
	PH_DEV_MON_APP_NTDS_MET	Microsoft directory service performance metrics

Collecting Windows Security Logs

Configuration

On the Windows Server, the following should be done first:

- [Configure Security Audit Logging Policy](#)
- [Configure File Auditing Policy](#)
- [Configure Audit File System Policy](#)
- [Disable Audit Token Right Adjusted Success Events](#)

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.

- a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. At **Event Log**, click **New**.
 - d. From the **Type** drop-down list, select **Security**.
 - e. In the **Include Event** field, leave it as "ALL", or enter the list of security event ids.
 - f. In the **Exclude Event** field, leave it as "NONE" or enter in the list of security event ids.
 - g. Note that setting Include Event to "ALL" and Exclude Event to "NONE" enables all security events.
 - h. Click **Save**.
4. Click **Save**.
 5. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
 6. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
 7. From the **Host** drop-down list, select the host(s).
 8. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
 9. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Configure Security Audit Logging Policy

Configure this policy to specify the categories of events that you want to be logged and available for monitoring by FortiSIEM.

1. Log in to the machine where you want to configure the policy as an administrator.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand **Local Policies** and select **Audit Policy**.
You will see the current security audit settings.
4. Select a policy and edit the **Local Security Settings** for the events you want to be audited. The recommended settings are:

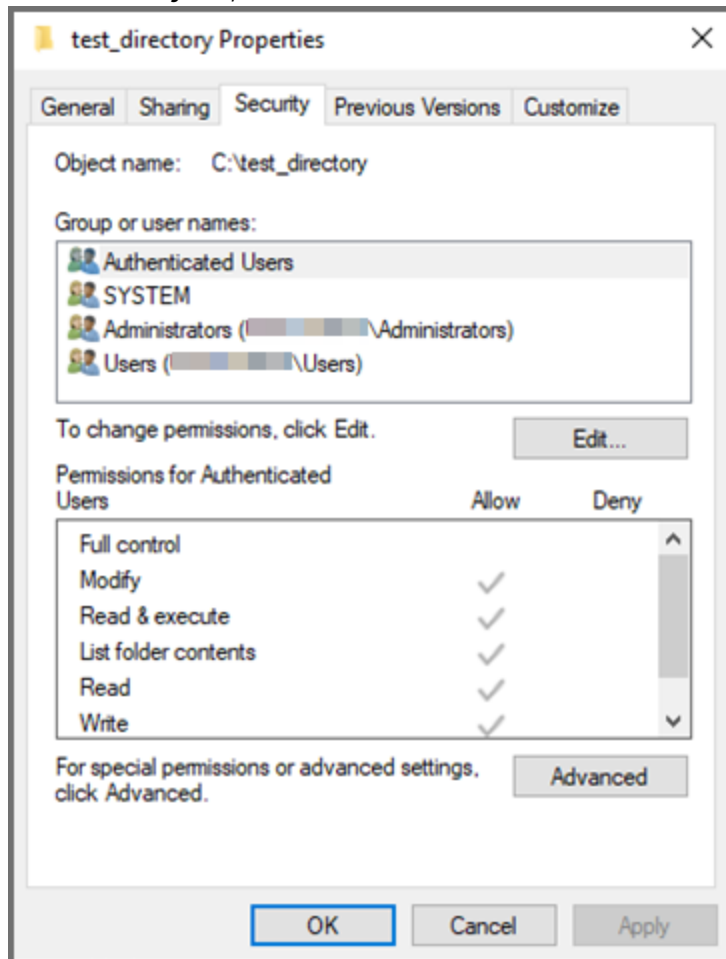
Policy	Description	Settings
Audit account logon events and Audit logon events	For auditing log in activity.	Select Success and Failure .
Audit object access events	For auditing access to files and folders. There is an additional configuration requirement for specifying which files and folders, users and user actions will be audited. See the next section, <i>Configuring File Auditing Policy</i> .	Select Success and Failure .
Audit system events	Includes system up/down messages.	

5. For an Enterprise Server's Domain Group Policy, make sure you set the following under **Group Policy > Local Policies > Audit Policy**:
Policy = Audit object access
Security Setting = Success or Failure

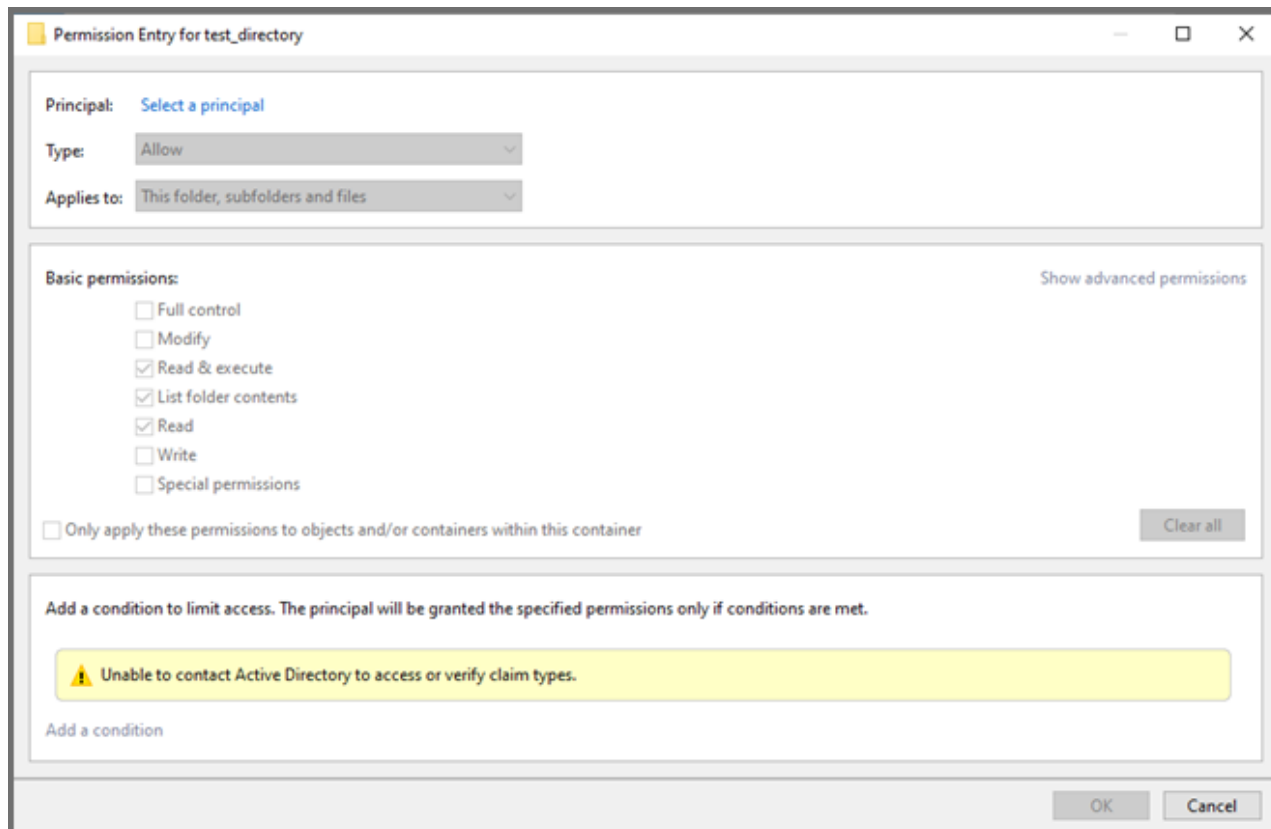
Configure File Auditing Policy

Configure this configuration to *capture user meta data* in file auditing Security logs such as Win-Security-4656, Win-Security-4658, etc...

1. Log in to the machine where you want to set the policy with administrator privileges.
On a domain computer, a Domain administrator account is needed.
2. Open Windows Explorer, select the file you want to set the auditing policy for, right-click on it, and select **Properties**. By default, the **General** tab will be shown. Select the **Security** tab to continue.
3. In the **Security** tab, click **Advanced**.

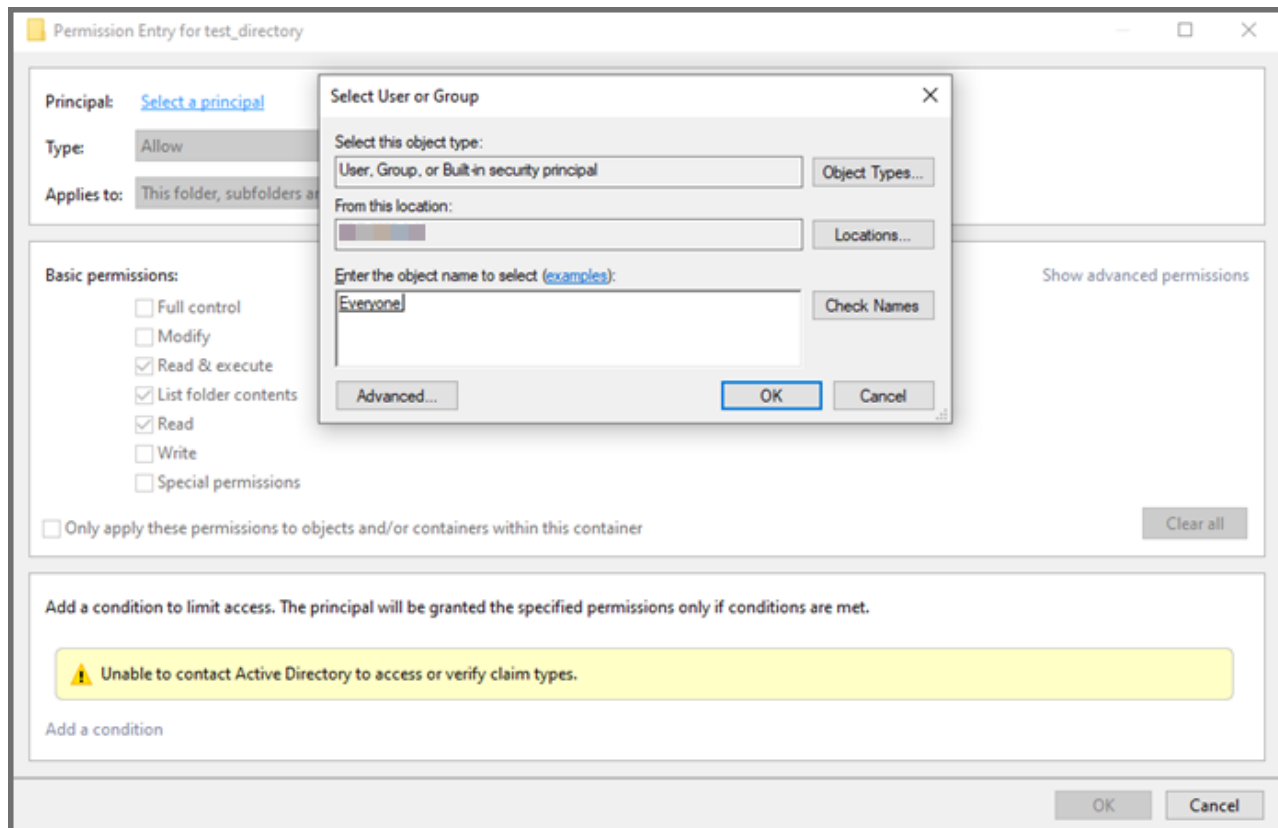


4. Select the **Auditing** tab, and click **Add**, then click **Select a principal**. This button is labeled **Edit** in Windows 2008.



5. In the **Select User or Group** dialog, click **Advanced**, and find and select the users, or groups, whose access to this file you want to monitor. If you want to audit all users access to the audited folder, select **Everyone**

as shown below.



6. Click **OK** after adding the users.
7. In the **Permissions** tab, set the permissions for each user added.
The configuration is now complete. Windows will generate audit events when the users or groups you specified take the actions specified on the files or folders for which you set the audit policies.

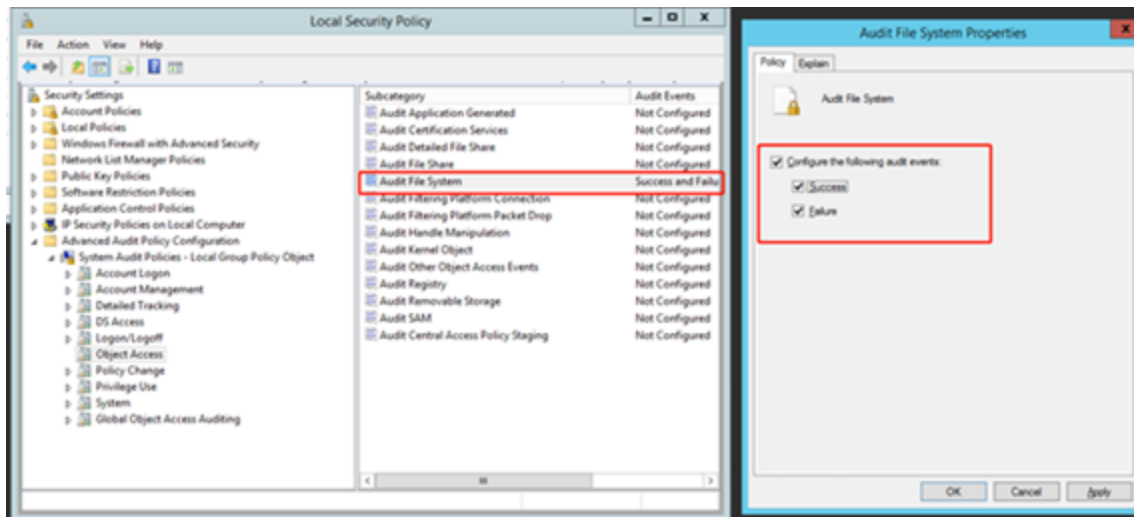
Configure Audit File System Policy

Configure this policy to enable change events for permission and/or ownership changes to files and/or directories. Examples include Win-Security-4662, Win-Security-4663. Without this policy, these events would not be generated.

Complete these steps to enable Audit File System policy:

1. Log in, with administrator privileges, to the machine where you want to set the policy.
On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand the **Advanced Audit Policy Configuration** node.
4. Expand **System Audit Policies-Local Group Policy Object** node.
You will see the current security audit settings.
5. Select **Object Access**.
6. Select **Audit File System** on the left side of the window.
7. Double-click **Audit File System**. In the pop-up window, select both **Success** and **Failure** under **Configure the following audit events**.

8. Click **Apply**, then **OK**.



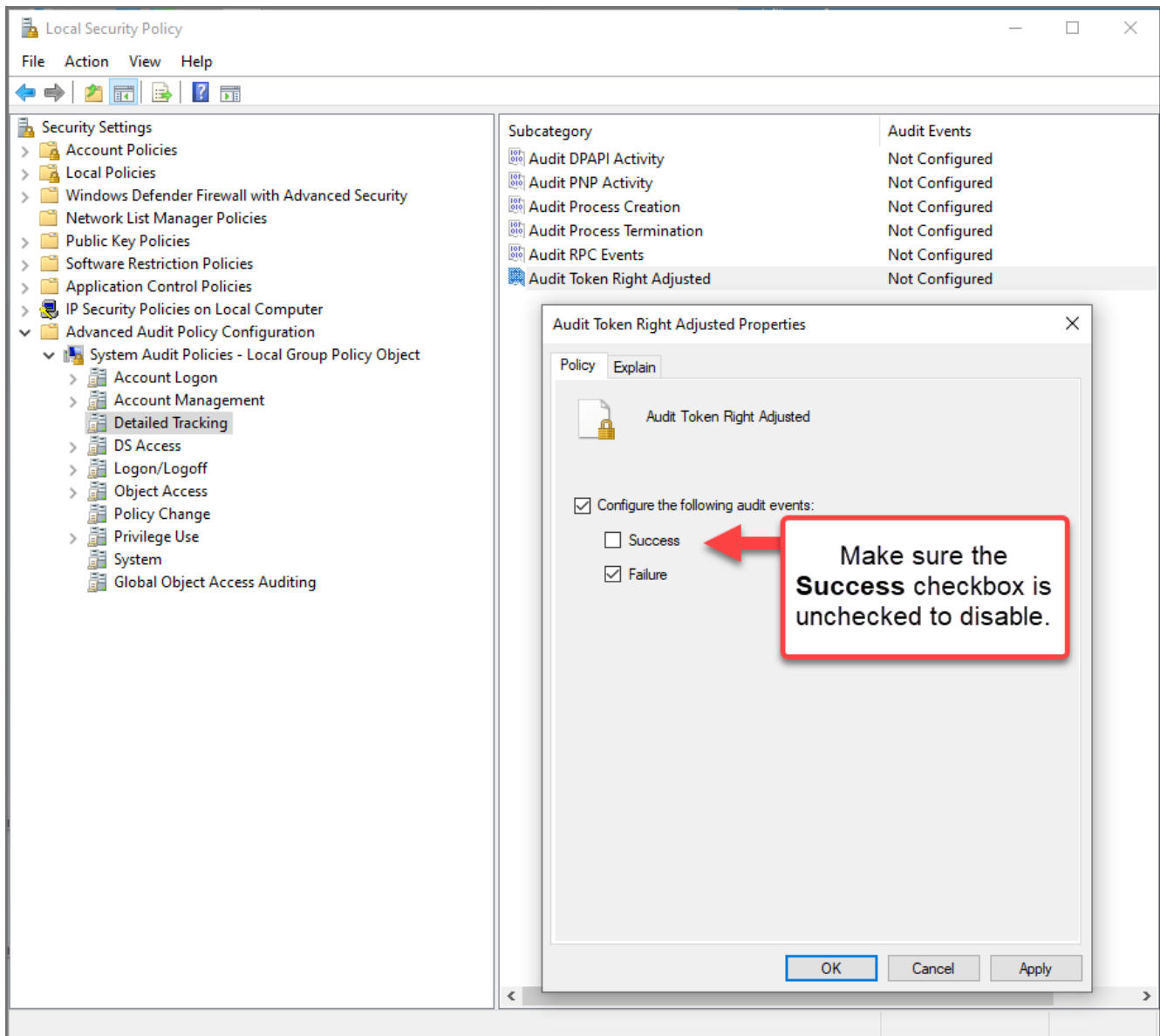
The Audit File System Policy is now enabled. Reboot your system to apply the changes.

Disable Audit Token Right Adjusted Success Events

Configure this to disable some high frequency and low value events such as Win-Security-4703.

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4703#security-monitoring-recommendations>.

1. Log in, with administrator privileges, to the machine where you want to set the policy.
On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand to **Security Settings > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Object > Detailed Tracking**.
4. Go to the **Detailed Tracking** subcategory, and select **Audit Token Right Adjusted**.
5. Double click **Audit Token Right Adjusted**, select the **Configure the following audit events:** checkbox.
6. Uncheck the **Success** checkbox if needed to disable.
7. Click **Apply**.



Important Security Events

The full list of Windows Security event types in FortiSIEM can be found by searching for "Win-Security-" in **Resources > Event Types** from FortiSIEM GUI.

External resource:

- Microsoft's website provides detailed event log descriptions: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/view-the-security-event-log>.

A few selected Windows Security events by use cases are shown below. Event Types follow the pattern: Win-Security-*<id>*

Use case	Event Type	Description
Logon	Win-Security-4624	Windows logon success
	Win-Security-4625	Windows logon failure
	Win-Security-4740	A user account was locked out
	Win-Security-4767	Windows user account unlocked
	Win-Security-4634	Account logoff
	Win-Security-4647	User initiated logoff
Account Management	Win-Security-4720	Windows user account created
	Win-Security-4722	Windows user account enabled
	Win-Security-4725	Windows user account disabled
	Win-Security-4726	Windows user account deleted
	Win-Security-4738	Windows user account changed
	Win-Security-4739	Domain Policy changed
	Win-Security-4741	A computer account was created
	Win-Security-4742	A computer account was changed
	Win-Security-4743	A computer account was deleted
	Win-Security-4727	A security-enabled global group was created
	Win-Security-4728	A member was added to a security-enabled global group
	Win-Security-4729	A member was removed from a security-enabled global group

Use case	Event Type	Description
	Win-Security-4730	A security-enabled global group was deleted
	Win-Security-4731	A security-enabled local group was created
	Win-Security-4732	A member was added to a security-enabled local group
	Win-Security-4733	A member was removed from a security-enabled local group
	Win-Security-4734	A security-enabled local group was deleted
	Win-Security-4735	A security-enabled local group was changed
	Win-Security-4737	A security-enabled global group was changed
	Win-Security-4744	A security-disabled local group was created
	Win-Security-4745	A security-disabled local group was changed
	Win-Security-4746	A member was added to a security-disabled local group
	Win-Security-4747	A member was removed from a security-disabled local group
	Win-Security-4748	A security-disabled local group was deleted
	Win-Security-4749	A security-disabled global group was created
	Win-Security-4750	A security-disabled global group was changed
	Win-Security-4751	A member was added to a security-disabled global group
	Win-Security-4752	A member was removed from a security-disabled global group
	Win-Security-4753	A security-disabled global group was deleted
	Win-Security-4754	A security-enabled universal group was created

Use case	Event Type	Description
	Win-Security-4755	A security-enabled universal group was changed
	Win-Security-4756	A member was added to a security-enabled universal group
	Win-Security-4757	A member was removed from a security-enabled universal group
	Win-Security-4758	A security-enabled universal group was deleted
	Win-Security-4759	A security-disabled universal group was created
	Win-Security-4760	A security-disabled universal group was changed
	Win-Security-4761	A member was added to a security-disabled universal group
	Win-Security-4762	A member was removed from a security-disabled universal group
	Win-Security-4763	A security-disabled universal group was deleted
Configuration Changes	Win-Security-1100	Event logging service shut down
	Win-Security-1102	Windows audit log cleared
	Win-Security-5025	Windows Firewall Service stopped
	Win-Security-4946	A rule added to Windows Firewall exception list
	Win-Security-4947	A Windows Firewall exception rule modified
	Win-Security-4950	A Windows Firewall setting has changed
	Win-Security-4616	The system time was changed
	Win-Security-5030	The Windows Firewall Service failed to start
Network Traffic	Win-Security-5031	Windows Firewall Service blocked an application from accepting incoming connections

Use case	Event Type	Description
	Win-Security-5155	Windows Filtering blocked an application or service from listening on incoming connections
	Win-Security-5157	Windows Filtering blocked a connection
	Win-Security-5152	Windows Filtering blocked a packet
	Win-Security-5153	A more restrictive Windows Filtering Platform filter has blocked a packet
	Win-Security-5156	Windows Filtering allowed a connection
File Audit	Win-Security-4656	A handle to an object was requested
	Win-Security-4658	The handle to an object was closed
	Win-Security-4659	A handle to an object was requested with intent to delete
	Win-Security-4660	An object was deleted
	Win-Security-4661	A handle to an object was requested
	Win-Security-4662	An operation was performed on an object
	Win-Security-4663	An attempt was made to access an object
	Win-Security-4608	Windows is starting up
Startup / Shutdown	Win-Security-4609	Windows is shutting down
	Win-Security-4688	A new process has been created
Process Activity	Win-Security-4689	A process has exited
	Win-Security-4698	scheduled task was created
Scheduled Task	Win-Security-4699	A scheduled task was deleted

Use case	Event Type	Description
	Win-Security-4700	A scheduled task was enabled
	Win-Security-4701	A scheduled task was disabled
	Win-Security-4702	A scheduled task was updated

Sample security events are available [here](#), in the FortiSIEM Online Help Appendix.

Collecting Windows System and Application Logs

Configuration

No configuration is needed on Windows hosts.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. At **Event Log**, create a System Event Log type by clicking **New**.
 - d. From the **Type** drop-down list, select **System**.
 - e. In the **Include Event** field, leave it as "ALL", or enter the list of event ids.
 - f. In the **Exclude Event** field, leave it as "NONE" or enter in the list of event ids.
 - g. Note that setting Include Event to "ALL" and Exclude Event to "NONE" enables all System events.
 - h. Click **Save**.
 - i. At **Event Log**, create a System Event Log type by clicking **New**.
 - j. From the **Type** drop-down list, select **Application**.
 - k. From the **Source** drop-down list, select the source.
 - l. In the **Include Event** field, leave it as "ALL", or enter the list of event ids.
 - m. In the **Exclude Event** field, leave it as "NONE" or enter in the list of event ids.
 - n. Note that setting Include Event to "ALL" and Exclude Event to "NONE" enables all Application events.
 - o. Click **Save**.
4. Click **Save**.
5. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
 - a. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
 - b. From the **Host** drop-down list, select the host(s).

- c. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
- d. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important System and Application Events

The full list of event types can be found by searching for "Win-System-" or "Win-App" in **Resources > Event Types** from FortiSIEM GUI. A few selected events are shown below. Event Types follow the pattern

- Win-System-<Reporting Module>-<id>
- Win-Application-<Reporting Module>-<id>

Type	Event Type	Description
System	Win-System-Microsoft-Windows-Eventlog-104	Application log file was cleared
System	Win-System-EventLog-6005	Windows EventLog service restarted
System	Win-System-EventLog-6006	Windows clean shutdown
System	Win-System-EventLog-6008	Windows dirty shutdown
System	Win-System-Service-Control-Manager-7023	Corrupted or missing system files
System	Win-System-Service-Control-Manager-7036,	Windows Application Status
System	Win-System-Service-Control-Manager-7036-Start	Windows Application Startup
System	Win-System-Service-Control-Manager-7036-Stop	Windows Application Shutdown
System	Win-System-Service-Control-Manager-7040	Windows service status changed
System	Win-System-Service-Control-Manager-7045	Windows Service installed
Application	Win-App-Application-Hang-1002	Application hang
Application	Win-App-Application-Error-1000	Application error
Application	Win-App-Windows-Error-Reporting-1001	Windows Error Reporting
Application	Win-App-MsiInstaller-1033	Windows Installer installed product
Application	Win-App-MsiInstaller-1034	Windows Installer removed the product
Application	Win-App-Microsoft-Windows-SoftwareRestrictionPolicies-868	A user starts a program that is disallowed by a zone rule or hash rule
Application	Win-App-Microsoft-Windows-SoftwareRestrictionPolicies-866	A user starts a program that is disallowed by a path rule

Type	Event Type	Description
Application	Win-App-Microsoft-Windows-SoftwareRestrictionPolicies-882	Access has been restricted by your Administrator by policy rule
Application	Win-System-USER32-1074	Windows shutdown initiated

Sample Windows system logs are available [here](#). Sample application events are available [here](#).

Collecting Windows Sysmon Logs

System Monitor (Sysmon) is a Windows system service that provides a more detailed view of system activity than the Windows security logs:

- Process creation, termination, and tampering
- Network connections initiated by processes and related activity
- Changes to file creation time stamps
- Loading of drivers or DLLs
- PowerShell launching and command logging

Configuration

Sysmon events collected by FortiSIEM Agent will automatically be parsed and analyzed by FortiSIEM.

On **Windows Server** side, follow these steps:

Note: The supported Sysmon versions are 5.02 and above. The latest Sysmon download instructions are available [here](#).

1. Log in to the Windows machine.
2. Download the popular Sysmon configuration file and save it as <https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml>
3. Save the configuration file as `sysmonconfig.xml`
4. Check whether the Sysmon executable is installed or not by running: `Sysmon64.exe -c`
 - a. If Sysmon is running, update the Sysmon configuration by using the command with administrator rights: `sysmon.exe -c sysmonconfig.xml`
 - b. If Sysmon is not available on the system, download and install using the command with administrator rights: `sysmon.exe -accepteula -i sysmonconfig.xml`
5. Check the new configuration using the command: `Sysmon64.exe -c`
6. Check for Sysmon events:
 - a. Go to **Event Viewer > Applications and Service Logs > Microsoft > Windows > Sysmon > Operational**.
 - b. Check for Sysmon logs on the right panel.
 - c. Right-click on **Operational** and choose **Properties**.
 - d. Note the **Full Name** (typically "Microsoft-Windows-Sysmon/Operational") for FortiSIEM configuration.

On **FortiSIEM side**, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. At **Event Log**, click **New**.
 - d. From the **Type** drop-down list, select **Other**.
 - e. In the **Event Name** field, paste the [full name that you acquired from the Windows side configuration](#). Typically this is typically "Microsoft-Windows-Sysmon/Operational".
 - f. In the **Include Event** field, leave it as "ALL", or enter the list of event ids.
 - g. In the **Exclude Event** field, leave it as "NONE" or enter in the list of event ids.
 - h. Note that setting Include Event to "ALL" and Exclude Event to "NONE" enables all Sysmon events.
 - i. Click **Save**.
4. Click **Save**.
5. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
 - a. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
 - b. From the **Host** drop-down list, select the host(s).
 - c. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
 - d. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Sysmon Events

The full list of event types can be found by searching for "Win-Sysmon-" in **Resources > Event Types** from FortiSIEM GUI. A few selected events are shown below. Event Types follow the pattern: Win-Sysmon-*<id>*-*<short description>*

Event Type	Description
Win-Sysmon-1-Create-Process	A Windows process is created
Win-Sysmon-3-Network-Connect-IPv4	TCP/UDP IPv4 connections created by a process
Win-Sysmon-6-Driver-Loaded	A windows driver is being loaded into the system
Win-Sysmon-7-Image-Loaded	A module is loaded within a specific process
Win-Sysmon-10-ProcessAccess	A process opens another process
Win-Sysmon-11-FileCreate	A file is created or overwritten
Win-Sysmon-12-Registry-CreateKey	Window registry key created
Win-Sysmon-12-Registry-DeleteKey	Window registry key deleted

Event Type	Description
Win-Sysmon-27-FileBlockExecutable	Sysmon detects and blocks the creation of executable files (PE format)

Sample Sysmon logs are available [here](#).

Collecting Windows DNS Logs

There are 2 types of DNS logs

- DNS Debug Logs
- DNS Analytical Logs

Here are some external references explaining the capabilities of DNS Debug Logs and DNS Analytical Logs:

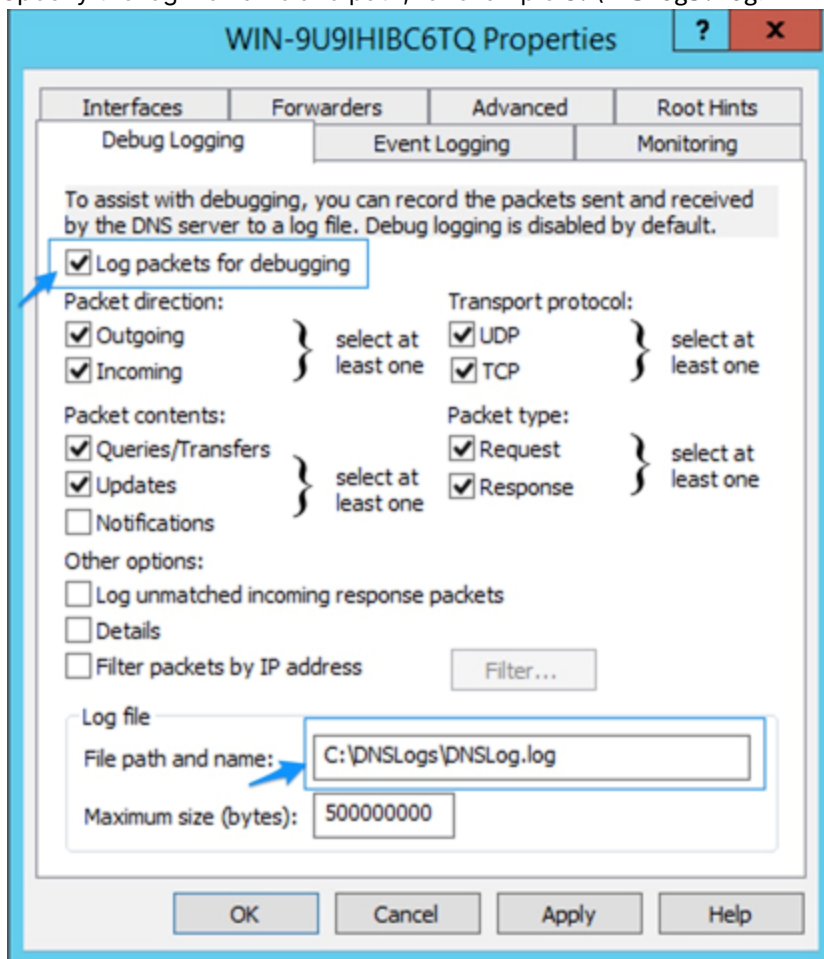
- <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/secrets-from-the-deep-the-dns-analytical-log-part-1/ba-p/1875094>
- <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/secrets-from-the-deep-the-dns-analytical-log-part-3/ba-p/1985830>
- <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/secrets-from-the-deep-the-dns-analytical-log-part-4/ba-p/2076293>
- <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/secrets-from-the-deep-the-dns-analytical-log-part-5/ba-p/3191119>

Configuring DNS Debug Log Collection

DNS Debug Logs contain information about hosts performing DNS Queries, DNS Server configuration changes and DNS Server errors. To collect DNS Debug Logs, take the following steps **on the Windows DNS Server**:

1. Log in to the Windows machine.
2. Configure DNS logging:
 - a. Launch **DNS Manager**.
 - b. Select the specific DNS Server and click **Properties**.
 - c. On **Debug Logging** tab, enable **Log packets for debugging**.

- d. Specify the log file name and path, for example C:\DNSLogs.log.



3. Check for DNS logs. If logs are present, FortiSIEM Agent will automatically collect these logs.

- a. Go to **Event Viewer > Applications and Service Logs > DNS Server**.
- b. Check for DNS logs on the right panel.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. At **Event Log**, click **New**.
 - d. From the **Type** drop-down list, select **DNS**.
 - e. In the **Include Event** field, leave it as "ALL", or enter the list of event ids.
 - f. In the **Exclude Event** field, leave it as "NONE" or enter in the list of event ids.
 - g. Note that setting Include Event to "ALL" and Exclude Event to "NONE" enables all events.

- h. Click **Save**.
4. Click **Save**.
5. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
6. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
7. From the **Host** drop-down list, select the host(s).
8. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
9. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important DNS Debug Log Event Types

The full list of event types can be found by searching for "Win-DNS-" or "AO-WUA-DNS" in **Resources > Event Types** from FortiSIEM GUI. Events "Win-DNS-*<id>*" with id more than 500 are considered DNS Debug logs. A few selected events are shown below.

Event Type	Description
AO-WUA-DNS-A-Query-Success	Successful DNS Domain name to IPV4 query
AO-WUA-DNS-A-Query-Failed	Failed DNS Domain name to IPV4 query
AO-WUA-DNS-AAAA-Query-Success	Successful DNS Domain name to IPV6 query
AO-WUA-DNS-AAAA-Query-Failed	Failed DNS Domain name to IPV6 query
AO-WUA-DNS-PTR-Query-Success	Successful DNS IPV4 to domain name query
AO-WUA-DNS-PTR-Query-Failed	Failed DNS IPV4 to domain name query
Win-DNS-548-Restart-server	A request to restart the DNS server service has been received
Win-DNS-549-Clear-debug-logs	The debug logs have been cleared from on DNS server
Win-DNS-515-Record-create	A resource record of type, name, TTL and RDATA was created in scope of zone
Win-DNS-516-Record-delete	A resource record of type, name and RDATA was deleted from scope of zone
Win-DNS-534-Export-DNSSEC	DNSSEC setting metadata was exported key signing key metadata from zone
Win-DNS-535-Import-DNSSEC	DNSSEC setting metadata was imported on zone

Sample DNS logs are available [here](#).

Configuring DNS Analytical Log Collection

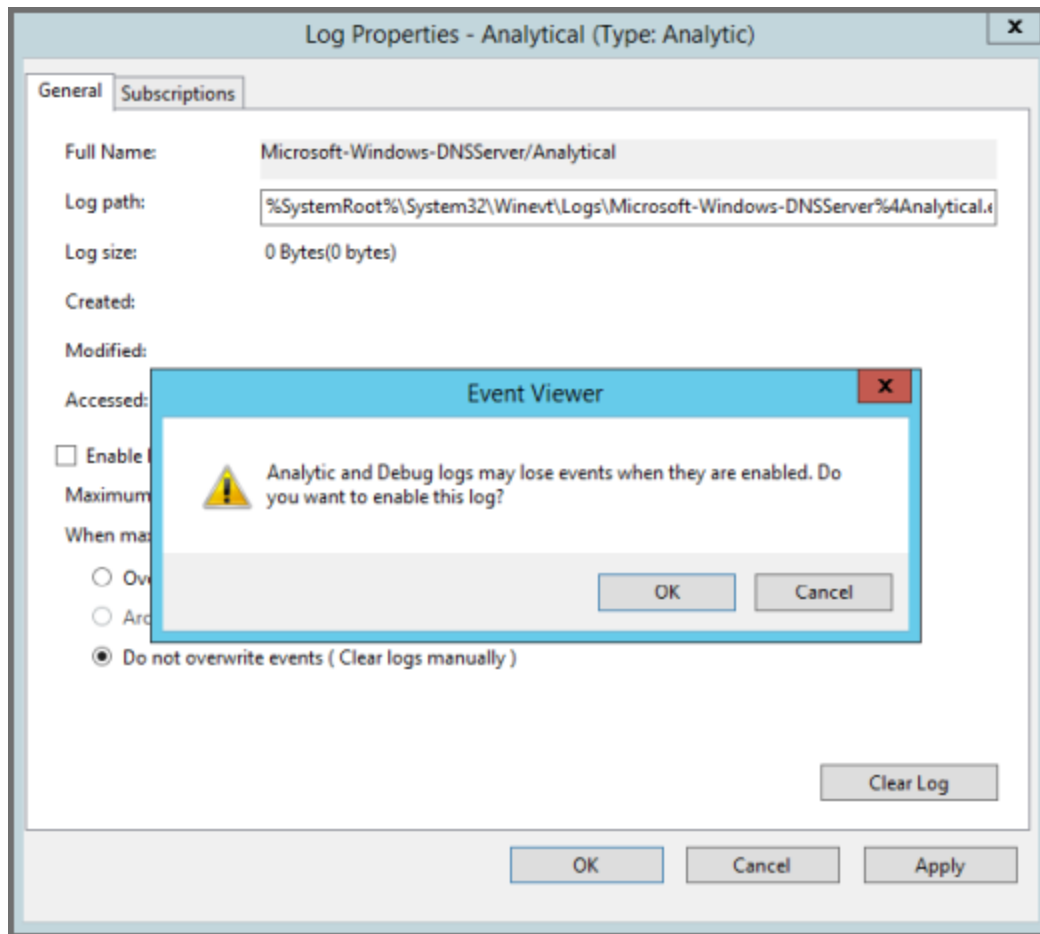
DNS Analytical Logs provide high-performance recording of all DNS transactions using Event Tracing for Windows (ETW). Analytic logs are more performant than legacy DNS Debug log.

To collect DNS Debug Logs, take the following steps **on the Windows DNS Server**:

Notes:

- Microsoft recommends that customers enable DNS Analytical logs only to debug DNS traffic or to troubleshoot DNS server issues. Enabling DNS Analytical logs can cause system performance issues (see [Microsoft Logging and Diagnostics](#)).
 - If the DNS server is running Windows Server 2012 R2, download the hotfix from <http://support.microsoft.com/kb/2956577>
 - You can find more information on this topic in [Enable Analytic and Debug Logs](#) in the Microsoft User Guide.
1. Enter `eventvwr.msc` at an elevated command prompt and press **Enter** to open the Event Viewer.
 2. In the Event Viewer, navigate to **Applications and Services Logs > Microsoft > Windows > DNS-Server**.
 3. Right-click **DNS-Server**, point to **View**, and click **Show Analytic and Debug Logs**. The **Analytical** log is displayed.
 4. Right-click **Analytical** and then click **Properties**.
 5. Under **When maximum event log size is reached**, choose **Do not overwrite events (Clear logs manually)**.
 6. Select the **Enable logging** checkbox.

7. Click **OK** when you are asked if you want to enable this log. See the following example.



8. Click **OK** again to enable the DNS Server Analytic event log.
9. Note the **Full Name** value in the screenshot in [Step7](#): **Microsoft-Windows-DNSServer/Analytical**. This name must be entered in FortiSIEM.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. At **Event Log**, click **New**.
 - d. From the **Type** drop-down list, select **Other**.
 - e. In the **Event Name** field, paste the [full name you acquired during the Windows DNS Server configuration](#).
 - f. In the **Include Event** field, leave it as "ALL", or enter the list of event ids.

- g. In the **Exclude Event** field, leave it as "NONE" or enter in the list of event ids.
 - h. Note that setting Include Event to "ALL" and Exclude Event to "NONE" enables all events.
 - i. Click **Save**.
4. Click **Save**.
5. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
6. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
7. From the **Host** drop-down list, select the host(s).
8. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
9. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important DNS Analytical Log Event Types

The full list of event types can be found by searching for "Win-DNS-" in **Resources > Event Types** from FortiSIEM GUI. Events "Win-DNS-*<id>*" with id less than 500 are considered DNS Analytical logs. A few selected events are shown below.

Event Type	Description
Win-DNS-265-IXFR-request-out	Incremental DNS Zone Transfer request sent
Win-DNS-266-IXFR-request-in	Incremental DNS Zone Transfer request received
Win-DNS-267-IXFR-response-out	Incremental DNS Zone Transfer response sent
Win-DNS-268-IXFR-response-in	Incremental DNS Zone Transfer response received
Win-DNS-269-AXFR-request-out	Full DNS Zone Transfer request sent
Win-DNS-270-AXFR-request-in	Full DNS Zone Transfer request received
Win-DNS-271-AXFR-response-out	Full DNS Zone Transfer response sent
Win-DNS-272-AXFR-response-in	Full DNS Zone Transfer response received
Win-DNS-273-XFR-notification-in	Full DNS Zone Transfer notification received
Win-DNS-274-XFR-notification-out	Full DNS Zone Transfer notification sent
Win-DNS-275-XFR-notify-ACK-in	Full DNS Zone Transfer notification acknowledgement received
Win-DNS-276-XFR-notify-ACK-out	Full DNS Zone Transfer notification acknowledgement sent

Sample DNS logs are available [here](#).

Collecting Windows DHCP Logs

DHCP Logs capture DHCP address assignment activity.

Configuration

On **Windows DHCP Server**, follow these steps.

1. Login to the Windows machine.
2. Configure DHCP logging:
 - a. Launch **DHCP Manager**.
 - b. Select the specific DHCP Server and click **IPv4 > Properties**.
 - c. Enable **DHCP Audit Logging**.
3. Check for DHCP events. If logs are present, FortiSIEM Agent will automatically collect these logs:
 - a. Go to **EventViewer > Applications and Service Logs > Microsoft > Windows > DHCP Server**.
 - b. Check for DHCP logs on the right panel.

On **FortiSIEM side**, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. At **File Log**, check the **DHCP** checkbox.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important DHCP Event Types

The full list of event types can be found by searching for "AO-WUA-DHCP-" in **Resources > Event Types** from FortiSIEM GUI. A few selected events are shown below.

Event Type	Description
AO-WUA-DHCP-IP-ASSIGN	DHCP IP assigned
AO-WUA-DHCP-IP-LEASE-RENEW	DHCP lease renewed
AO-WUA-DHCP-DNS-LEASE-DENY	DHCP lease denied

Event Type	Description
AO-WUA-DHCP-DNS-UPDATE-SUCCESS	DHCP DNS Update Request Success
AO-WUA-DHCP-DNS-UPDATE-FAILED	DHCP DNS Update Request Fail
AO-WUA-DHCP-STOPPED	DHCP service stopped
AO-WUA-DHCP-DATABASE-CLEANUP-BEGIN	DHCP Database cleanup begin

Sample DHCP logs are available [here](#).

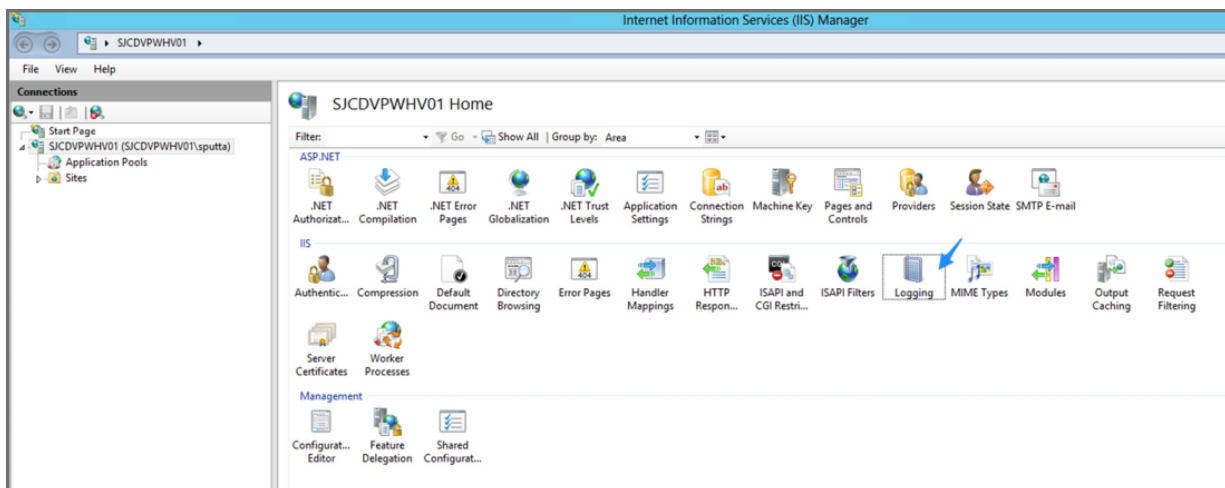
Collecting Windows IIS Logs

IIS Logs capture IIS Web Server activity on Windows host.

Configuration

On Windows IIS Server, follow these steps.

1. Log in to the Windows machine.
2. Configure IIS logging:
 - a. Launch **IIS Manager**.
 - From the **Start** menu, click **Programs** or **All Programs**, and point to **Administrative Tools**.
 - On **Administrative Tools**, Click **Internet Information Services (IIS) Manager**.
 - b. Select the specific **IIS Server** and click the **Logging** icon on the panel on the right side.



- c. Specify the log path if default path (%SystemDrive%\inetpub\logs\LogFiles) does not exist.

The screenshot shows the 'Logging' configuration window for IIS. It includes sections for 'Log File' and 'Log File Rollover'. In the 'Log File' section, the 'Format' is 'W3C', the 'Directory' is '%SystemDrive%\inetpub\logs\LogFiles' (indicated by a blue arrow), and the 'Encoding' is 'UTF-8'. In the 'Log File Rollover' section, the 'Schedule' option is selected with a frequency of 'Daily'.

3. Check for IIS events. If logs are present, FortiSIEM Agent will automatically collect these logs:
 - a. Go to IIS logs default path, example: C:\inetpub\logs\LogFiles\.
 - b. Check for IIS traffic logs.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. At **File Log**, check the **IIS** checkbox.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important IIS Event Types

The full list of event types can be found by searching for "AO-WUA-IIS-" in **Resources > Event Types** from FortiSIEM GUI. A few selected events are shown below.

Event Type	Description
AO-WUA-IIS-Web-Request-Success	Web request successful
AO-WUA-IIS-Web-Request-Redirect	Web request redirected
AO-WUA-IIS-Web-Client-Error	Web request failed - client error
AO-WUA-IIS-Web-Server-Error	Web request failed - server error
AO-WUA-IIS-Web-Forbidden-Access-Denied	Web request denied - forbidden access
AO-WUA-IIS-Web-Bad-Request	Web request denied - bad request
AO-WUA-IIS-Web-Length-Reqd-Access-Denied	Web request denied - length required

Sample IIS logs are available [here](#).

Collecting Generic Application Logs

Windows Agent can monitor when lines get appended to a log file on the host. When this happens, an event is generated.

Configuration

No configuration is needed on the Windows host.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **User Log** tab.
 - c. At **User Log**, click **New**.
 - d. In the **Full File Name** field, enter the full file name (including the path) to be monitored.
 - e. In the **Log Prefix** field, enter a log prefix that needs to be added to the log.
 - f. If the log file contains 1 line split into multiple lines, then add the following to define the multi-line format.
 - i. In the **Start** field, enter a pattern that indicates the start of a multi-line log.
 - ii. In the **End** field, enter pattern that indicates the end of a multi-line log.
 - iii. In the **Max Lines** field, enter the maximum number of lines that a multi-line log can contain.

- g. Click **Save**.
4. Click **Save**.
5. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
6. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
7. From the **Host** drop-down list, select the host(s).
8. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
9. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Application Log File Monitoring Event Type

The following event is generated when a new line is appended to the log file:

AO-WUA-UserFile-<Log Prefix>. The new line is present in the msg attribute.

Configuring File Integrity Monitoring

Windows Agent can detect the following file or directory changes on a host:

- Addition, deletion, modification, renaming
- Permission change
- Ownership change

Importantly, the Agent can *identify the associated user* by correlating with the Security logs and add this information to the generated AO-WUA-FileMon log.

Also, the Agent provides two more features generally applicable to system configuration files:

- The file can be pushed from the Windows host to FortiSIEM. The file is saved on CMDB under **Devices > Configuration Files**. Subsequent changes can be tracked.
- The file can be compared against a baseline and an alert can be generated when the file changes.

Configuration

On **Windows host**, configure the following:

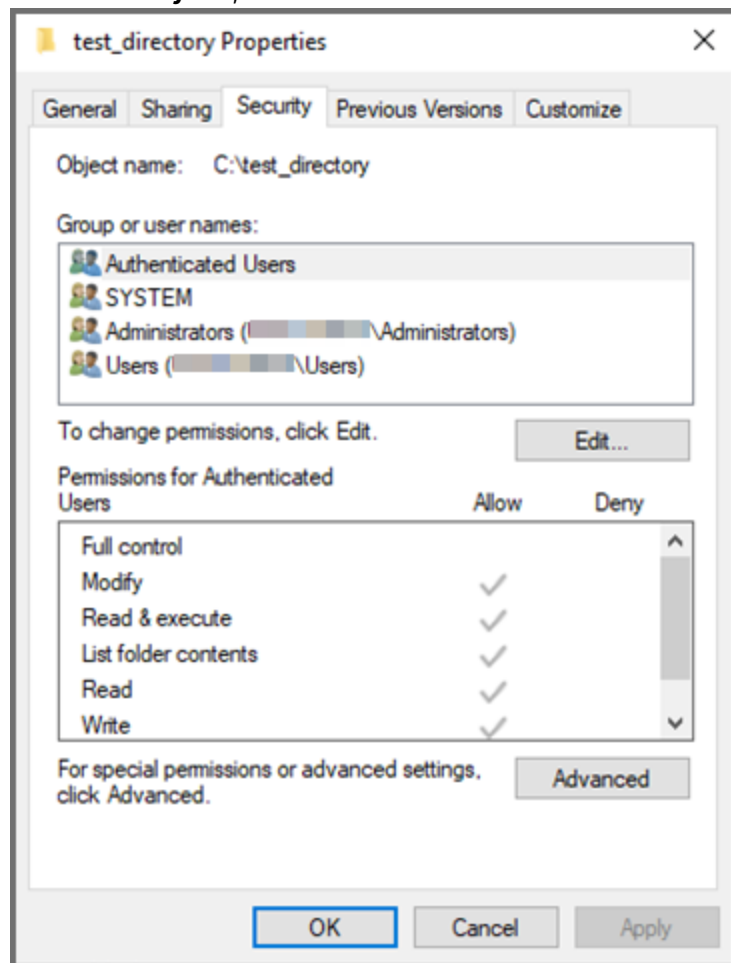
- [Configure File Auditing Policy](#)
- [Configure Audit File System Policy](#)

Configure File Auditing Policy

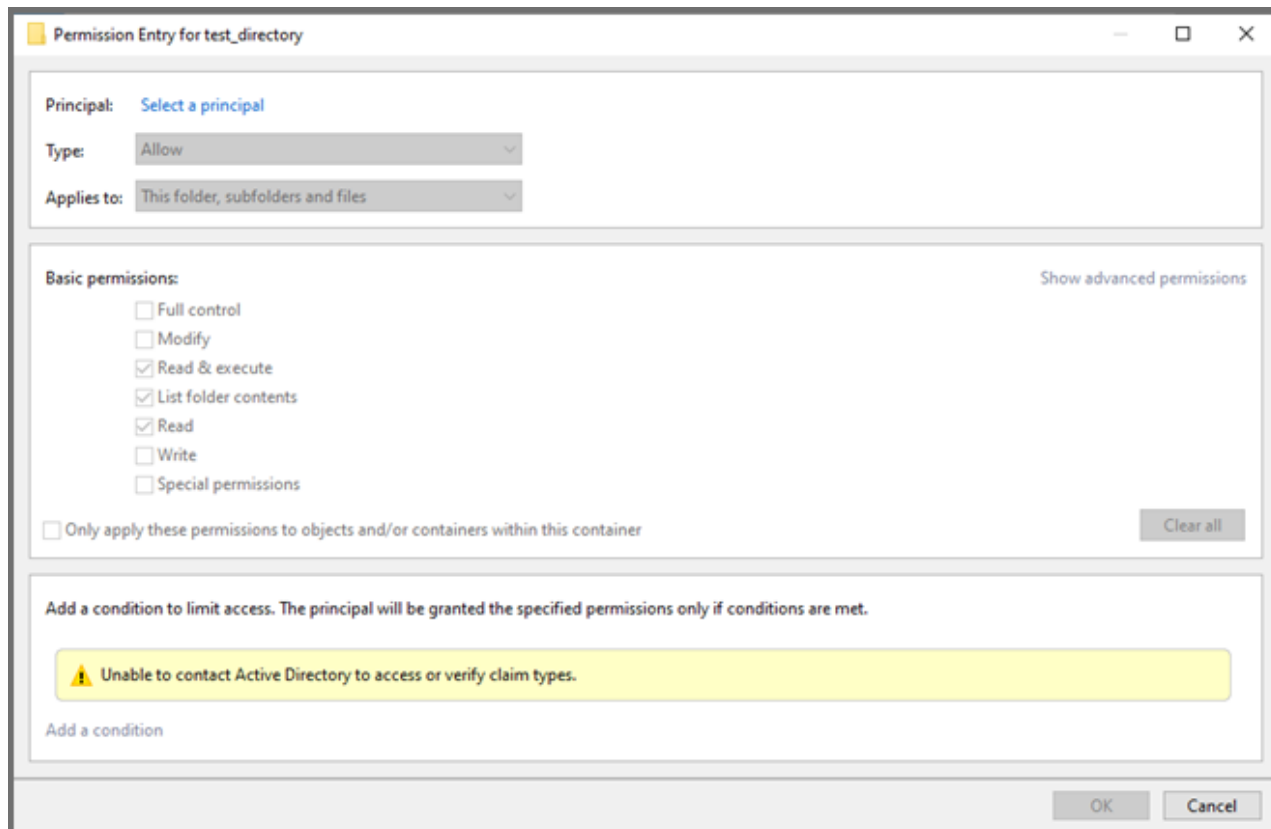
Configure this configuration to *capture user meta data* in file auditing Security logs such as Win-Security-4656, Win-Security-4658 etc.

1. Log in to the machine where you want to set the policy with administrator privileges.
On a domain computer, a Domain administrator account is needed.

2. Open Windows Explorer, select the file you want to set the auditing policy for, right-click on it, and select **Properties**. By default, the **General** tab will be shown. Select the **Security** tab to continue.
3. In the **Security** tab, click **Advanced**.

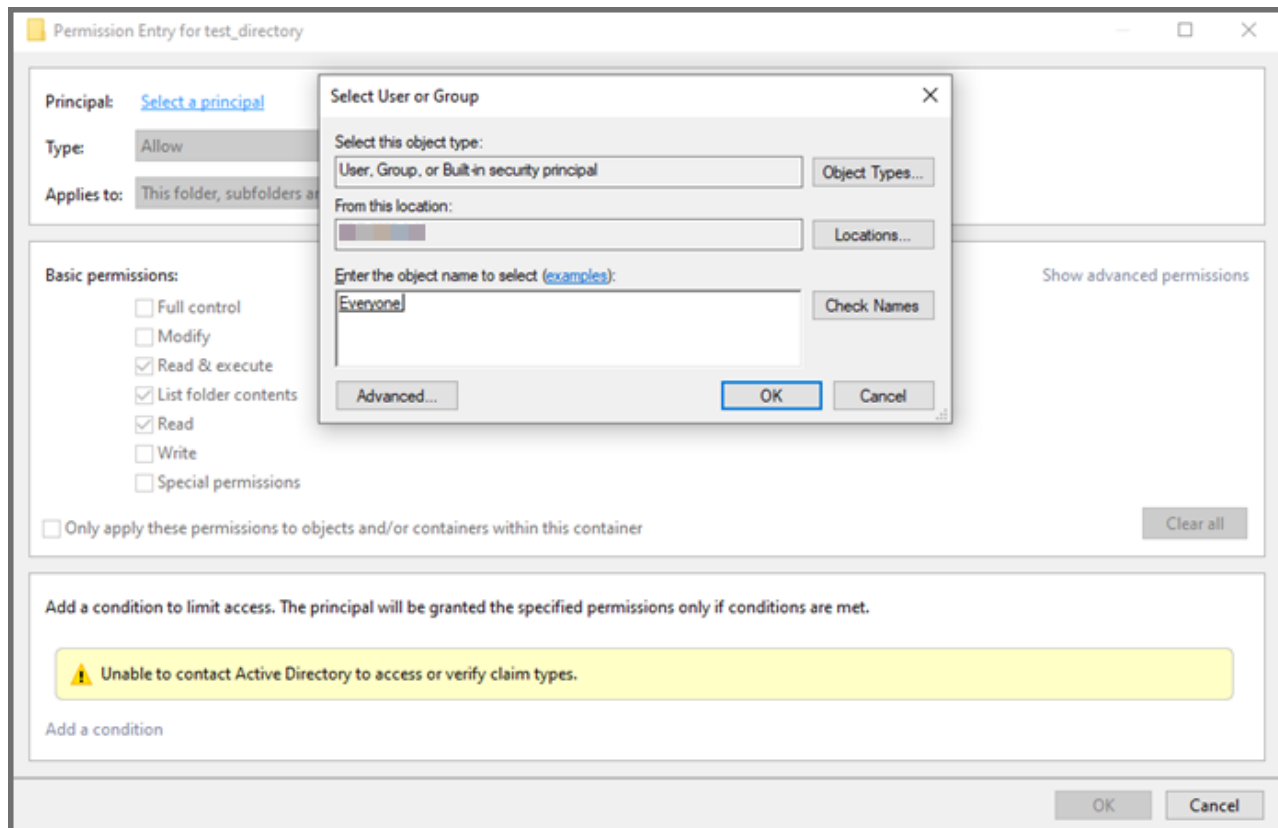


4. Select the **Auditing** tab, and click **Add**, then click **Select a principal**. This button is labeled **Edit** in Windows 2008.



5. In the **Select User or Group** dialog, click **Advanced**, and find and select the users, or groups, whose access to this file you want to monitor. If you want to audit all users access to the audited folder, select **Everyone**

as shown below.



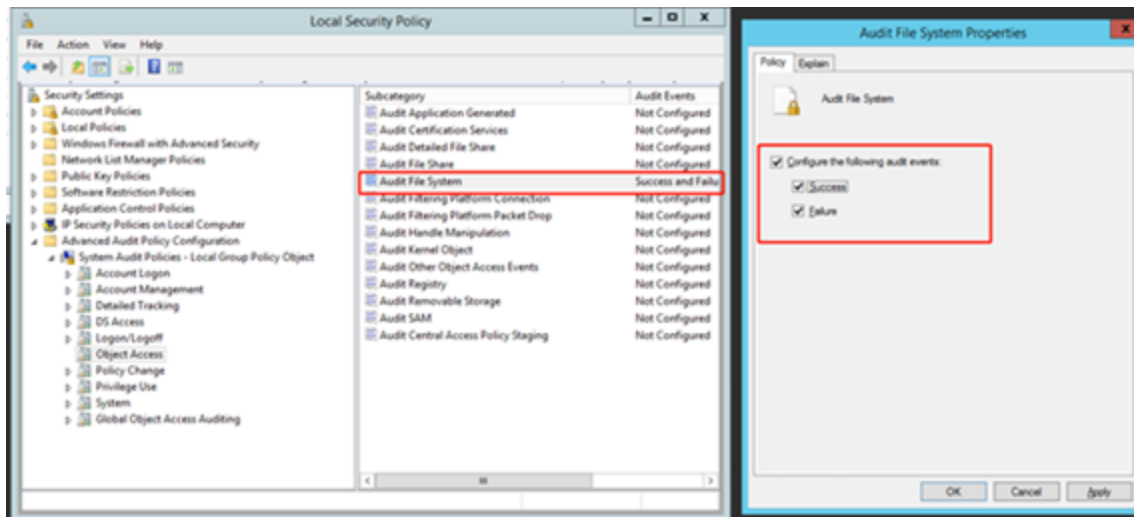
6. Click **OK** after adding the users.
7. In the **Permissions** tab, set the permissions for each user added.
The configuration is now complete. Windows will generate audit events when the users or groups you specified take the actions specified on the files or folders for which you set the audit policies.

Configure Audit File System Policy

Configure this policy to enable change events for permission and/or ownership changes to files and/or directories. Examples include Win-Security-4662, Win-Security-4663. Without this policy, these events would not be generated.

Complete these steps to enable Audit File System policy:

1. Log in, with administrator privileges, to the machine where you want to set the policy.
On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand the **Advanced Audit Policy Configuration** node.
4. Expand **System Audit Policies-Local Group Policy Object** node.
You will see the current security audit settings.
5. Select **Object Access**.
6. Select **Audit File System** on the left side of the window.
7. Double-click **Audit File System**. In the pop-up window, select both **Success** and **Failure** under **Configure the following audit events**.

8. Click **Apply**, then **OK**.

The Audit File System Policy is now enabled. Reboot your system to apply the changes.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **FIM** tab.
 - c. Click **New**.
 - d. In the **File/Directory** field, enter the **File or Directory** (including path) to be monitored.
 - e. Check the **Include Subfolder(s)** checkbox if subfolder(s) should be included.
 - f. Use the **Exclude Subfolder(s)** field to enter any subfolders that should not be included.
 - g. In the **Include File Type** and **Exclude File Type** fields, enter any file types you wish to include or exclude respectively.
 - h. File Content Monitoring (typically applies for configuration files)
 - i. At **On Modify**, check the **Push Files** checkbox if you want the Agent to push the file to FortiSIEM. It will show up in **CMDB > Devices > Configuration Files**.
 - ii. At **On Modify**, check the **Compare Baseline** checkbox if you want FortiSIEM to compare the file to a baseline and create an event when a difference is detected.
 - i. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.

8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important FIM Event Types

These event types can be found by searching for "AO-WUA-FileMon-" in **Resources > Event Types** from FortiSIEM GUI.

Event Type	Description
AO-WUA-FileMon-Added	A windows file or directory created
AO-WUA-FileMon-Modified	A windows file or directory modified
AO-WUA-FileMon-Removed	A windows file or directory deleted
AO-WUA-FileMon-ArchivedBitChange	A windows file archive bit changed
AO-WUA-FileMon-OwnershipChange	A windows file or directory ownership changed
AO-WUA-FileMon-PermissionChange	A windows file or directory permission changed
AO-WUA-FileMon-Renamed-New-Name	A windows file or directory renamed: shows new name
AO-WUA-FileMon-Renamed-Old-Name	A windows file or directory renamed: shows old name
AO-WUA-FileMon-BaselineChange	A Windows file baseline changed

Sample File Integrity Monitoring logs are available [here](#).

Configuring Windows Certificate Monitoring

Windows Agent can detect when a certificate is added / deleted / expiring / expired.

Configuration

No configuration is needed on the Windows host.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Certificate Monitoring** tab.
 - c. For each Certificate Store, indicate the operations that need to be monitored by adding a check to its checkbox: **Add/ Delete / Expiring / Expired**.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.

5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Certificate Monitoring Event Types

These event types can be found by searching for "AO-WUA-Certificate-" in **Resources > Event Types** from FortiSIEM GUI.

Event Type	Description
AO-WUA-Certificate-Added	A Windows certificate was added
AO-WUA-Certificate-Removed	A Windows certificate was removed
AO-WUA-Certificate-Expired	A Windows certificate was expired
AO-WUA-Certificate-Expiring	A Windows certificate is expiring

Sample Certificate Monitoring logs are available [here](#).

Configuring Windows Registry Change Monitoring

Windows Agent can detect when a windows registry changes.

Configuration

No configuration is needed on the Windows host.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Change** tab.
 - c. For **Registry Change**, indicate the root key that need to be monitored and the subkeys that need to be excluded.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).

7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Registry Change Event Types

These event types can be found by searching for "AO-WUA-Registry-" in **Resources > Event Types** from FortiSIEM GUI.

Event Type	Description
AO-WUA-Registry-Added	A registry entry was created
AO-WUA-Registry-Modified	A registry entry was modified
AO-WUA-Registry-Removed	A registry entry was deleted

Sample Registry Change logs are available [here](#).

Configuring Installed Software Change Monitoring

Windows Agent can detect when installed software changes.

Configuration

No configuration is needed on the Windows host.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Change** tab.
 - c. Check the **Installed Software Change** checkbox.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Event Types

These event types can be found by searching for "AO-WUA-Certificate-" in **Resources > Event Types** from FortiSIEM GUI.

Event Type	Description
AO-WUA-InstSw-Added	A software was installed
AO-WUA-InstSw-Removed	A software was removed

Sample Installed Software logs are available [here](#).

Configuring WMI and PowerShell Output Monitoring

Windows Agent can collect the output of any WMI and PowerShell script. The event containing the script output can be parsed and utilized for creating alerts and reports.

Configuration

No configuration is needed on the Windows host.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Script** tab.
 - c. Under **WMI Classes**, click **New**.
 - i. From the **Name** drop-down list, select a name representing the WMI Class category.
 - ii. From the **WMI Class** drop-down list, select the specific WMI Class.
 - iii. Click **Save**.
 - d. Complete the list of WMI Classes you want to monitor by repeating step c.
 - e. Under **Power Shell Script**, click **New**.
 - i. In the **Name** field, enter a name.
 - ii. In the **Script Content** field, enter/paste the PowerShell script.
 - iii. Click **Save**.
 - f. Complete the list of PowerShell scripts you want to monitor by repeating step e.
 - g. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.

6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Event Types

Event Type	Description
AccelOps-WUA-WMI	WMI script monitoring output
AccelOps-WUA-Powershell	PowerShell script monitoring output

Sample PowerShell logs are available [here](#). Sample WMI log is available [here](#).

Configuring Windows User Entity Behavior Anomaly (UEBA)

Agent provides a clean telemetry of file accesses by generating 1 event per file action and including the following fields.

- Host
- User
- Domain
- Resource
- Activity

Such a clean data set enables Anomaly detection via Machine Learning.

Note:

1. Agent UEBA is generated by a kernel module and hence is very efficient
2. Windows Security logs can provide this information but, more than 1 (typically 6-8) Security logs are generated for 1 file action and requires further expensive correlation.
3. Agent FIM can also generate such events. However, the files have to be configured. Agent FIM file change detection is deep (e.g. permission changes) and not as efficient. Also, this needs correlation with Security logs to get user meta data.

Configuration

No configuration is needed on the Windows host.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.

- b. Click the **UEBA** tab.
 - c. Check the **UEBA** checkbox.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Event Types

Event Type	Description
FINS-Windows-file-created	Windows user created file
FINS-Windows-file-deleted	Windows user deleted file
FINS-Windows-file-read	Windows user read file
FINS-Windows-file-written	Windows user wrote file
FINS-Windows-file-moved	Windows user moved file
FINS-Windows-file-downloaded	Windows user downloaded file
FINS-Windows-file-uploaded	Windows user uploaded file
FINS-Windows-new-process-created	Windows new process created
FINS-Windows-process-stopped	Windows process stopped

Sample UEBA logs are available [here](#).

Configuring OpenSSH Operational and Admin Logs

Configuration

On **Windows host**, take the following steps

1. Make sure that you have installed or have a preinstalled OpenSSH service.
2. Go to C:\ProgramData\ssh\ and edit the sshd_config file.
 - a. Find the two lines below and set them to LOCAL6, and INFO respectively and uncomment them.

```
# Logging
SyslogFacility LOCAL6
LogLevel INFO
```

- b. Save the file.

- c. Restart the sshd service by running the following commands.


```
net stop sshd
net start sshd
```
3. Go to Event Viewer and navigate to **Applications and Services Logs > OpenSSH > Operational log** section to confirm logs are now being generated.

On FortiSIEM side, follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Event** tab.
 - c. Under **Event Log**, click **New**.
 - i. From the **Type** drop-down list, select **Other**.
 - ii. In the **Event Name** field, enter "OpenSSH/Operational".
 - iii. Click **Save**.
 - d. Click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Important Event Types

Events will have the following event type: FSM-WUA-WinLog-OpenSSH/Operational

As an example:

```
2024-10-04T23:05:48Z test-lab01.example.com 192.0.2.0 FSM-WUA-WinLog-OpenSSH/Operational
[phCustId]="1" [customer]="Super" [monitorStatus]="Success" [Locale]="en-US"
[MachineGuid]="9265b0da-aa12-48d3-b5d0-d14e711e4713" [timeZone]="-0800"
[extEventRecvProto]="Windows Agent" [domain]="NT AUTHORITY" [user]="SYSTEM"
[userSIDAcctType]="User" [level]="Information" [xml]=<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='OpenSSH'
Guid='{c4b57d35-0636-3bc3-bb32-370f205f9802}' /><EventID>4</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode>0</O
pcode><Keywords>0x4000000000000000</Keywords><TimeCreated SystemTime='2024-10-
04T23:05:47.559828200Z' /><EventRecordID>3</EventRecordID><Correlation></Correlation><Execution
ProcessID='11360' ThreadID='13740' /><Channel>OpenSSH/Operational</Channel><Computer>test-
lab01.example.com</Computer><Security UserID='S-1-5-18' /></System><EventData><Data
```

```
Name='process'>sshd</Data><Data Name='payload'>Server listening on :: port
2222.</Data></EventData><RenderingInfo Culture='en-US'><Message>sshd: Server listening on :: port
2222.</Message><Level>Information</Level><Task></Task><Opcode>Info</Opcode><Channel></Channel><Pro
vider></Provider><Keywords></Keywords></RenderingInfo></Event>
```

Configuring Osquery

Osquery features enables you to query the host for a wide variety of information using SQL query language. For details about osquery, see <https://osquery.readthedocs.io/en/latest/>.

The osquery framework is integrated into FortiSIEM GUI.

- You can run built-in osquery queries on demand by navigating to **Resources > Reports > Osquery**, selecting a report, and clicking **Run**.
- You can create your own osquery by navigating to **Resources > Osquery** and clicking **New**.
- You can schedule the osquery queries to run periodically. Events are generated when osqueries run. Then you can run osquery reports, or write correlation rules or built machine learning models, like any other event. Built-in osquery rules can be found by going to **Resources > Rules** and searching for "osquery".
- You can run osqueries during Incident Investigation.

Osquery framework is built-in to the Windows Agent. No configuration is needed.

On FortiSIEM side, if you wish to run specific osquery queries from Windows Agent(s), follow these steps:

1. Login to GUI.
2. Navigate to **Admin > Setup > Windows Agent**.
3. Under **Windows Agent Monitor Templates**, click **New** to create a Windows Agent Monitoring Template, or select an existing Windows Agent Monitoring Template, and click **Edit**.
 - a. If creating a new Windows Agent Monitor Template, from the **Generic** tab, in the **Name** field, enter a name for the template.
 - b. Click the **Osquery** tab.
 - c. At the **Osquery** drop-down list, select an osquery.
 - d. To add another osquery, click **+**, then make another osquery selection from the drop-down list.
 - e. When done, click **Save**.
4. Under **Host To Template Associations**, click **New** to create an Host To Template Associations, or select an existing one and click **Edit**.
5. If creating a new Host To Template Associations, in the **Name** field, enter a name for this Host To Template Associations.
6. From the **Host** drop-down list, select the host(s).
7. At **Template**, attach the template to one or more hosts by selecting its checkbox, then click **Save**.
8. Under **Host to Template Associations**, click **Apply**.

For configuration information details, see [Configuring Windows Agent](#).

Recommended Log Sources by Use Case

Use Case	Recommended Log Source	Sample Event Type
Logon Audit and Anomaly Detection	Windows Security Log	
Account Management Audit	Windows Security Log	
System Configuration Change Audit	Windows Security Log	
Network Traffic Audit and Anomaly Detection	Windows Security Log	
Service install	Windows System Log	
Application errors	Windows Application Log	
Process Activity Anomaly	Windows Sysmon	
Registry Change Audit	Sysmon or Agent Registry Change	
File Change Audit	Agent FIM	
File Content Change Audit and validating against Golden Image	Agent FIM	
File Activity Anomaly (UEBA) via Machine Learning	Agent UEBA	
Installed Software Changes	Agent Install Software Change	
Certificate Monitoring	Agent Certificate Monitoring	
IP Address Assignment Audit	Agent DHCP Log	
DNS Activity Audit and Anomaly Detection	Agent DNS Debug Log	
Web Server Activity	Agent IIS Log	
System Performance Monitoring	Agent Performance Monitoring	
Getting information from host on demand (for threat hunting)	Agent osquery	
Application Log Monitoring	Agent Userfile	

Configuring Windows Event Forwarding

Using Windows Event Forwarding, it is possible for Windows Servers (called Event Source Computers) to forward events to a central Windows Server where FortiSIEM Windows Agent (called Event Collector Computer) is running. The Agent can then send to FortiSIEM Collector, Worker, and Supervisor nodes. This is an alternative to running FortiSIEM Agent on every Windows Server. FortiSIEM can parse the forwarded Windows events so that the actual reporting Windows Server is captured and all the attributes are parsed as sent by native agents.

The advantage of this approach is that you need fewer agents to deploy. However, this approach has the following disadvantages:

- Only Windows (Security, Application, and System) events can be collected in this way, while FortiSIEM native Agent can collect other information such as User Entity Behavior Monitoring, File Integrity Monitoring, Custom log, Sysmon, Install Software detection, Certificate Monitoring, etc...
- There is a limitation on the number of Event Source Computers that can forward events to a single Event Collector Computer. This depends on the number of events they generate and the hardware resources on the Event Collector Computer.
- [Configure the Event Collector Computer](#)
- [Non-Domain Environments: Configure the Event Source Computer](#)
- [Domain Environments: Configure the Domain Controller](#)

Configure the Event Collector Computer

You must complete the following steps on the Event Collector computer where the FSM Agent is installed:

1. Open a command prompt in an elevated privilege (for example, **Run as Administrator...**) and run this command to configure the Windows Remote Management (WinRM) service:
winrm qc -q
2. Run this command to configure the Windows Event Collector service:
wecutil qc /q
3. Copy and save the following XML in a file (Configuration.xml) and edit the values depending on your requirements or scenario.

The XML configuration will grant the Domain Computers and Network Service accounts as the local event forwarder for the source computers. The XML configuration will contain the language locale, which is same as the Collector computer's language locale.

```
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
  <SubscriptionId>FwdSubscription</SubscriptionId>
  <SubscriptionType>SourceInitiated</SubscriptionType>
  <Description>Source Initiated Subscription</Description>
  <Enabled>true</Enabled>
  <Uri>http://schemas.microsoft.com/wbem/wsmn/1/windows/EventLog</Uri>
  <!-- Use Normal (default), Custom, MinLatency, MinBandwidth -->
  <ConfigurationMode>Custom</ConfigurationMode>
  <Delivery Mode="Push">
    <Batching>
      <MaxItems>1</MaxItems>
      <MaxLatencyTime>1000</MaxLatencyTime>
    </Batching>
    <PushSettings>
      <Heartbeat Interval="30000" />
    </PushSettings>
  </Delivery>
  <Expires>2025-01-01T00:00:00.000Z</Expires>
  <Query>
    <![CDATA[
      <QueryList>
        <Query Path="Security">
          <Select>*</Select>
        </Query>
      </QueryList>]]>
  </Query>
```



```

</Query>
<ReadExistingEvents>true</ReadExistingEvents>
<TransportName>http</TransportName>
<ContentFormat>RenderedText</ContentFormat>
<Locale Language="en-US" />
<LogFile>ForwardedEvents</LogFile>
<AllowedSourceNonDomainComputers></AllowedSourceNonDomainComputers>
<AllowedSourceDomainComputers>0:NSG:NSD:(A;;GA;;;DC)(A;;GA;;;NS)</AllowedSourceDomainComputers>
</Subscription>

```

4. From the Command Prompt, enter the following command to create the subscription according to the specified XML configuration file:
`wecutil cs Configuration.xml`
5. From the Command Prompt, enter the following command to add an inbound and outbound exception in the firewall for port 5985 (http). This enables the Event Source Computer to connect to the Event Collector Computer.:

```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP dir=in
localport=5985 action=allow
```

```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP dir=out
remoteport=5985 action=allow
```

Non-Domain Environments: Configure Event Source Computer

You must complete these steps on the Event Source computer.

1. Open a Command Prompt in an elevated privilege (for example, **Run as Administrator...**) and run the following commands:

```
net localgroup "Event log readers" "NT Authority\Network Service" /add
winrm qc -q
```

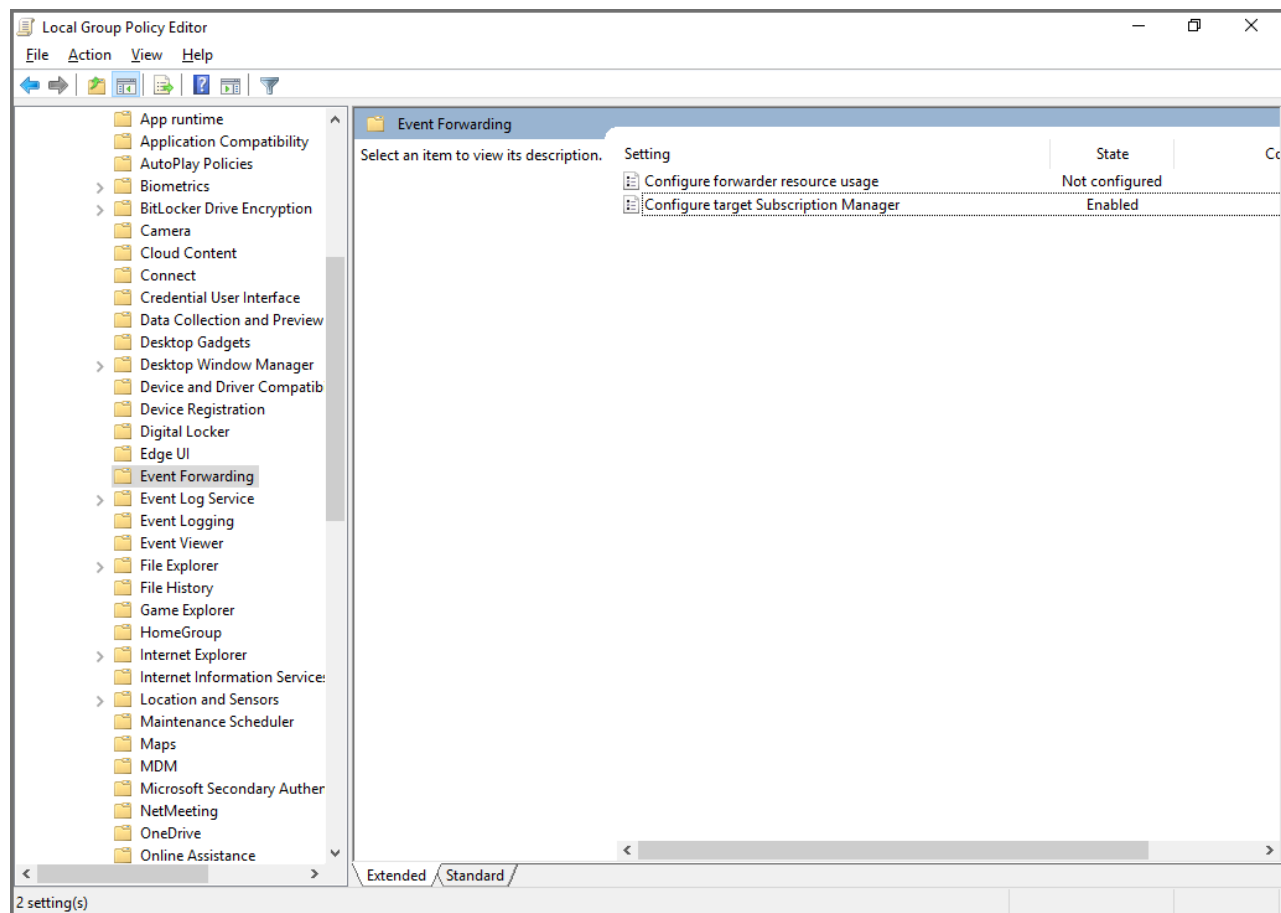
2. From the command prompt, enter the following command to add an inbound and outbound exception in the firewall for port 5985 (http):

```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP dir=in
localport=5985 action=allow
```

```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP dir=out
remoteport=5985 action=allow
```

Now, run the local group policy editor to configure the subscription manager settings, by taking the following steps:

1. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Event Forwarding**.



2. Open **Configure target Subscription Manager**.

Configure target Subscription Manager

Previous Setting Next Setting

☐ Not Configured
 ☒ **Enabled**
☐ Disabled

Comment:

Supported on:

Options:

Help:

This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.

If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.

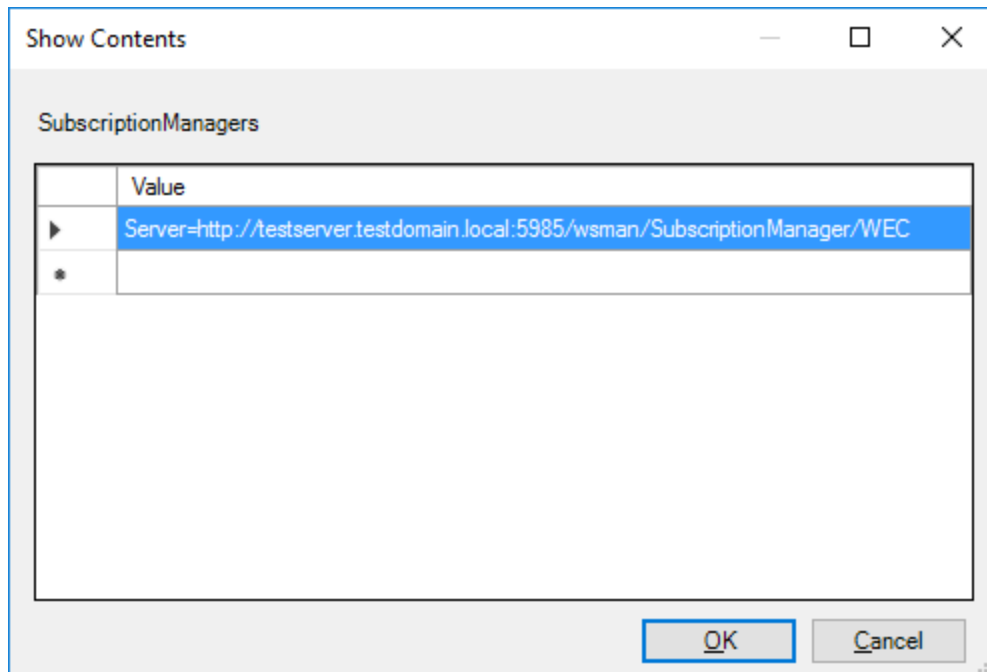
Use the following syntax when using the HTTPS protocol:
 Server=https://<FQDN of the collector>:5986/wsman/SubscriptionManager/WEC,Refresh=<Refresh interval in seconds>,IssuerCA=<Thumb print of the client authentication certificate>. When using the HTTP protocol, use port 5985.

If you disable or do not configure this policy setting, the Event Collector computer will not be specified.

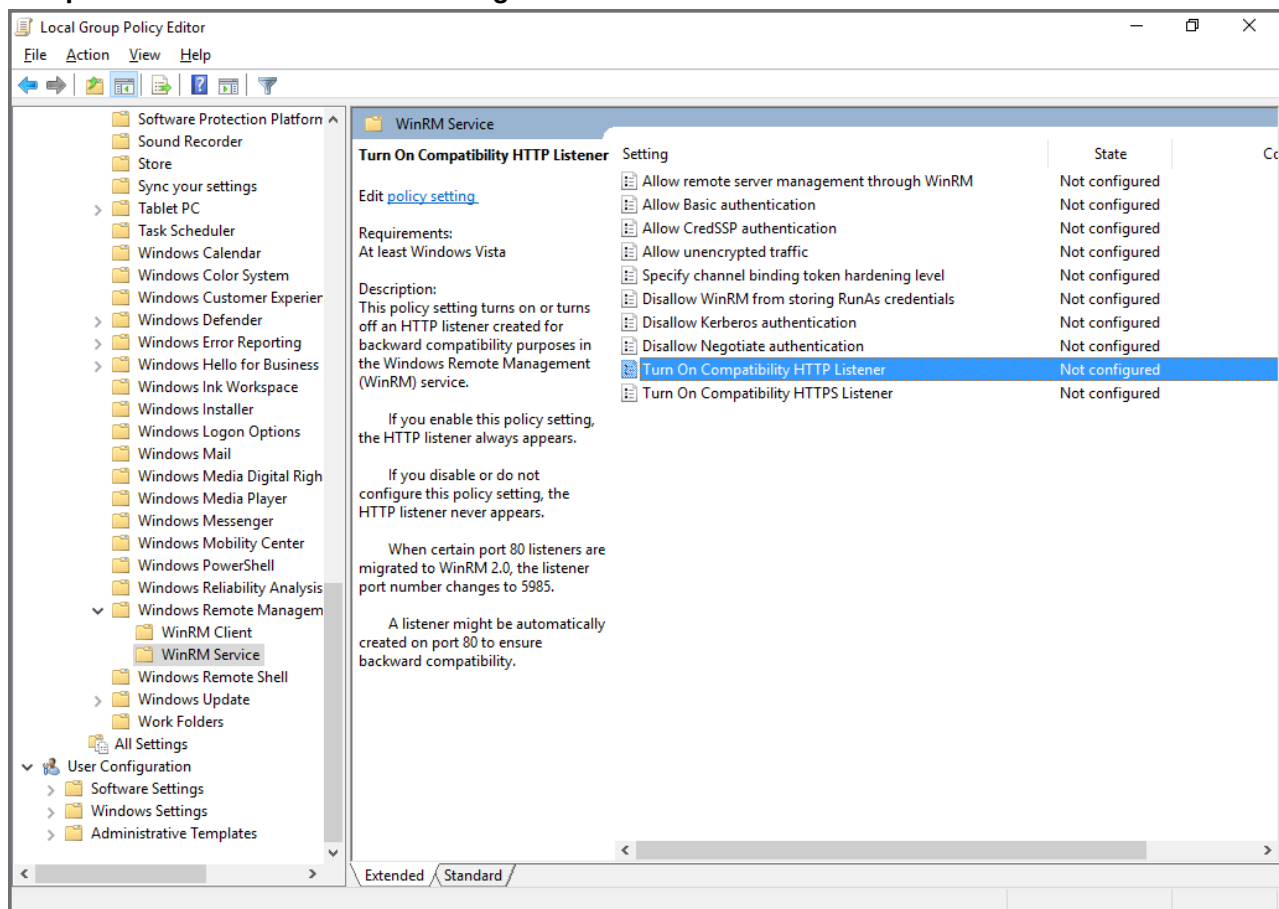
OK **Cancel** Apply

Choose the **Enabled** option.

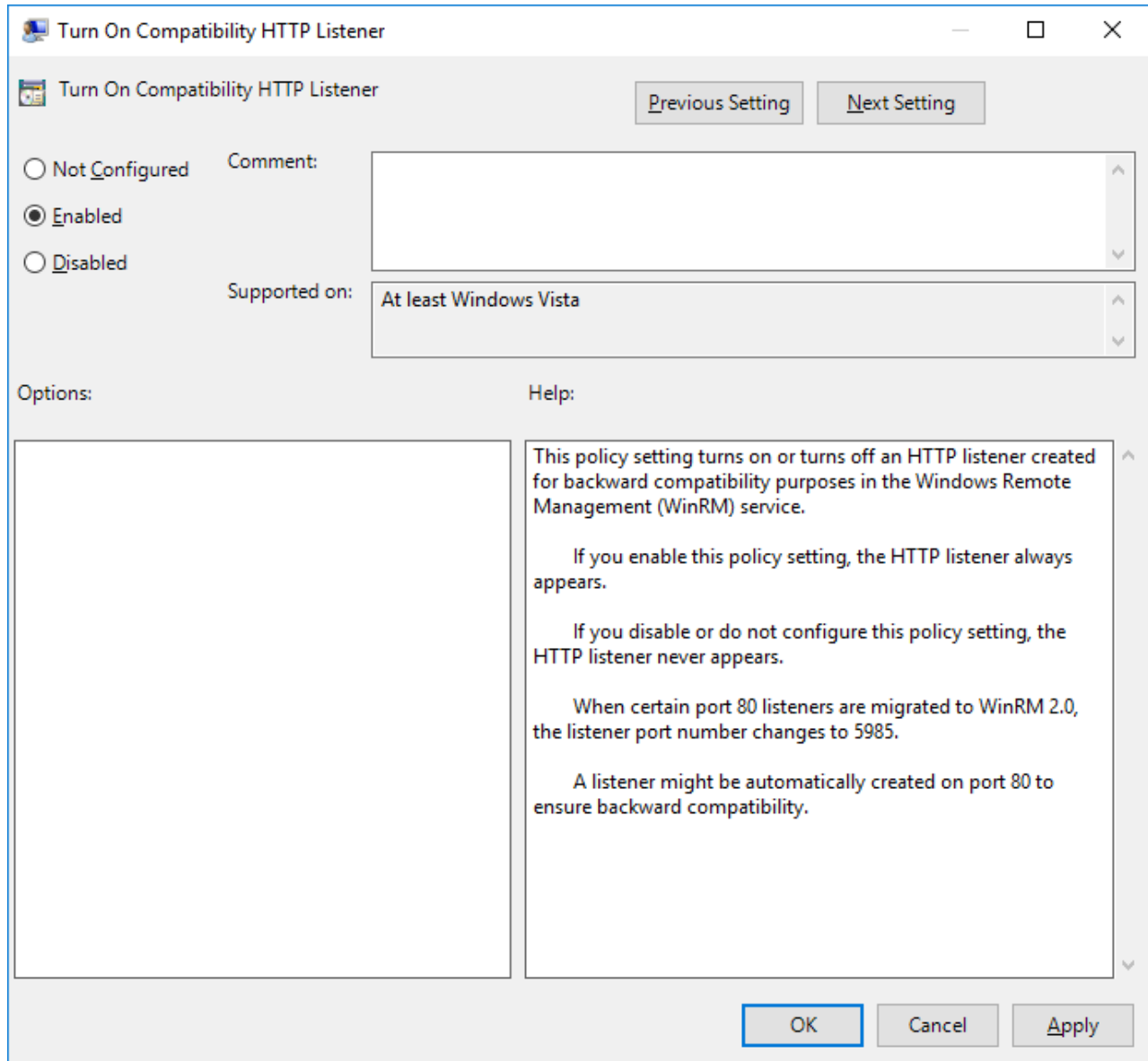
3. Click the **Show...** button beside **SubscriptionManagers**.
4. Add the value `Server=http://<Collector FQDN>:5985/wsman/SubscriptionManager/WEC` to the list and click **OK**.



5. In the **Configure target Subscription Manager** dialog box, click **Apply** and then **OK**.
6. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management > WinRM Service**.



7. Open **Turn On Compatibility HTTP Listener**.
8. Choose the option **Enabled**.

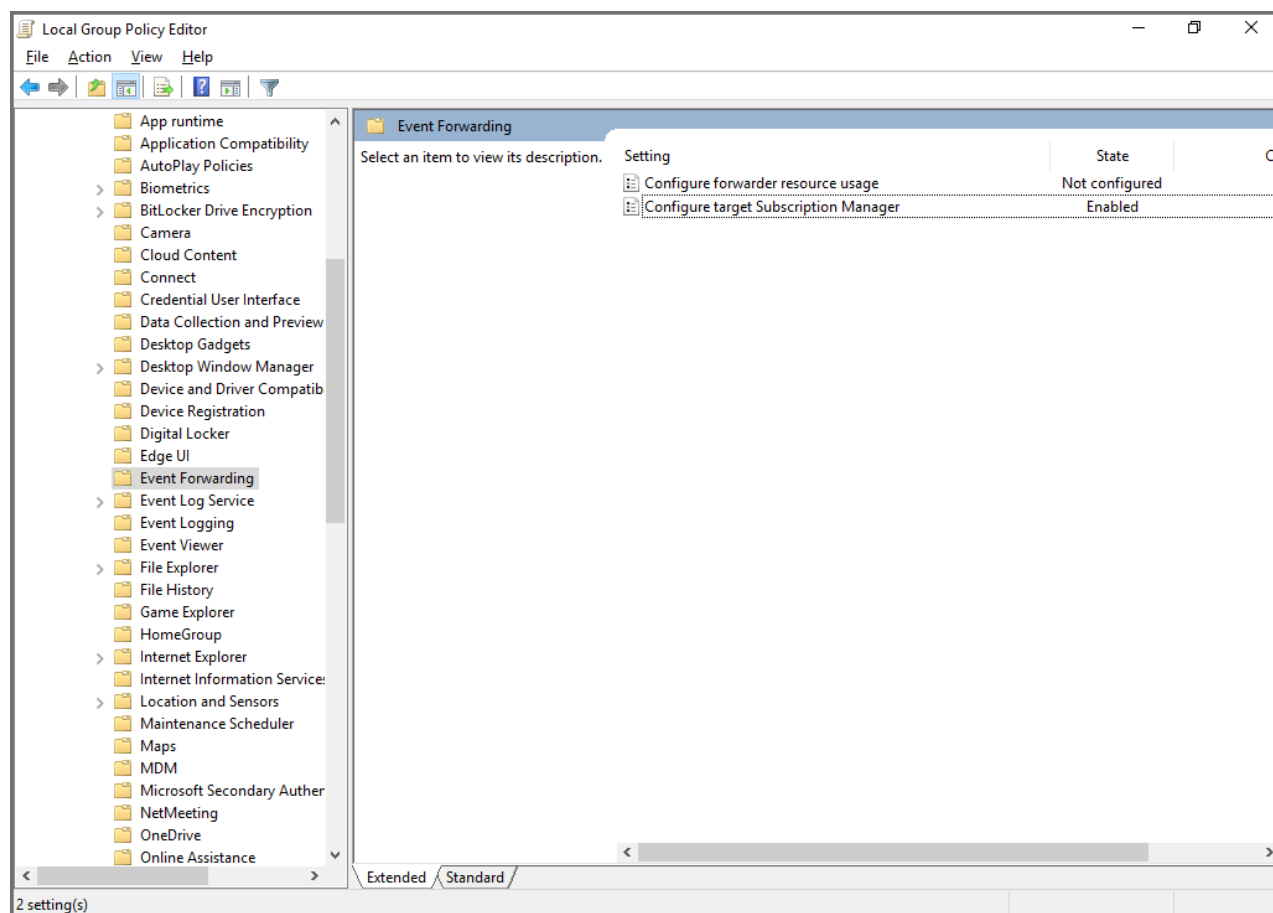


9. Click **Apply** and then **OK**.
10. Close the local policy editor.

Domain Environments: Configure the Domain Controller

The following policy changes must be performed on the Domain Controller.

1. Run the domain group policy editor.
2. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Event Forwarding**.



3. Open **Configure target Subscription Manager**.

Configure target Subscription Manager

Previous Setting Next Setting

☐ Not Configured
 ☒ **Enabled**
☐ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SubscriptionManagers Show...

Help:

This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.

If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.

Use the following syntax when using the HTTPS protocol:
 Server=https://<FQDN of the collector>:5986/wsman/SubscriptionManager/WEC,Refresh=<Refresh interval in seconds>,IssuerCA=<Thumb print of the client authentication certificate>. When using the HTTP protocol, use port 5985.

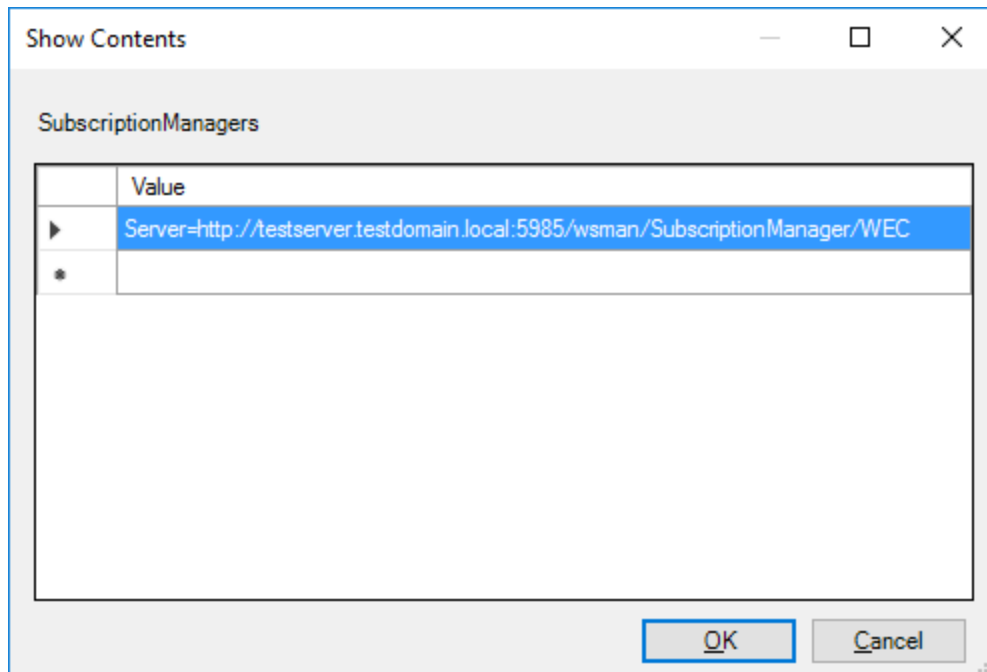
If you disable or do not configure this policy setting, the Event Collector computer will not be specified.

OK Cancel Apply

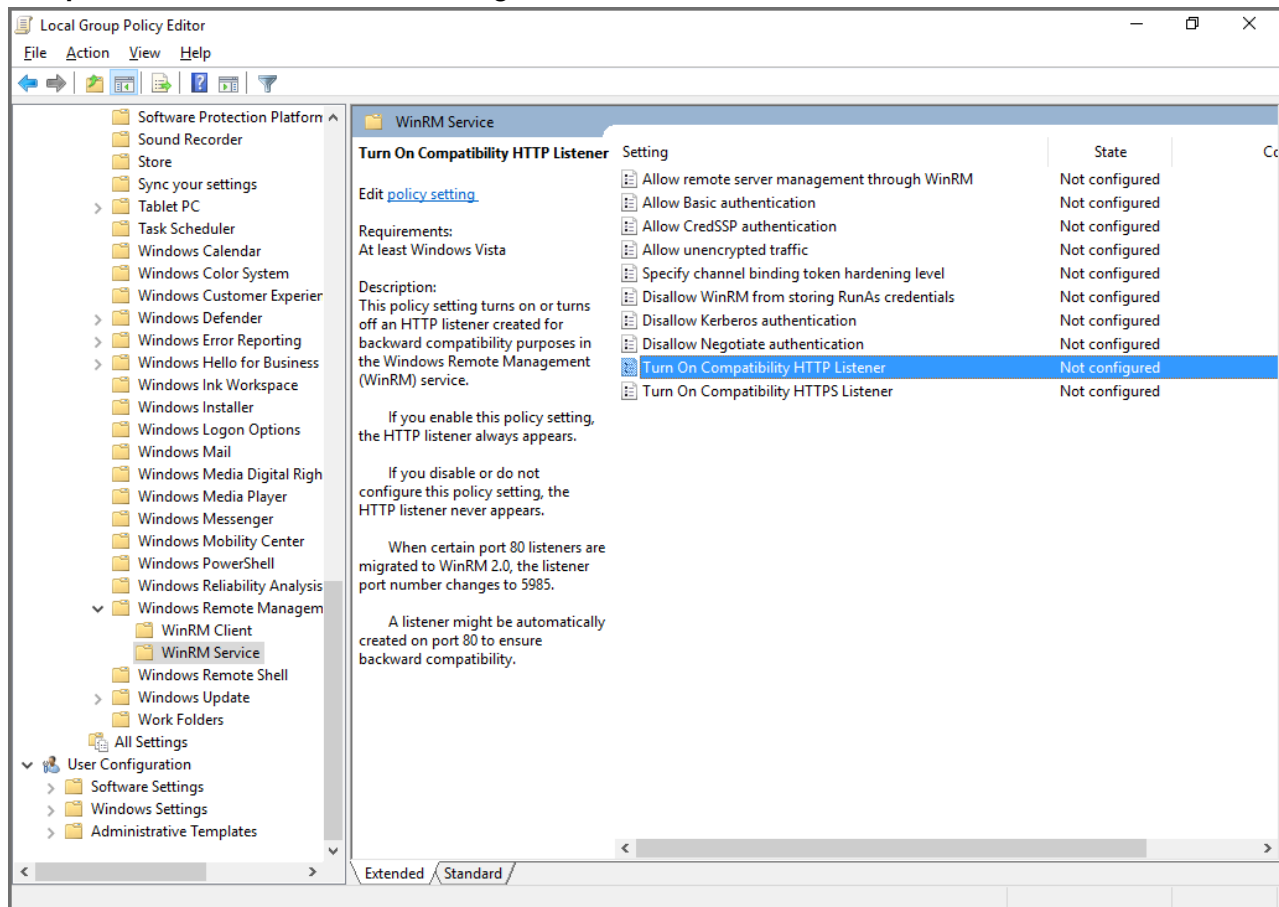
4. Choose the **Enabled** option.

5. Click the **Show...** button beside **SubscriptionManagers**.

6. Add the value `Server=http://<Collector FQDN>:5985/wsman/SubscriptionManager/WEC` to the list and click **OK**.



7. In the **Configure target Subscription Manager** dialog box, click **Apply** and then **OK**.
8. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management > WinRM Service**.



9. Open **Turn On Compatibility HTTP Listener**.
10. Choose the option **Enabled**.

Turn On Compatibility HTTP Listener

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Vista

Options:

Help:

This policy setting turns on or turns off an HTTP listener created for backward compatibility purposes in the Windows Remote Management (WinRM) service.

If you enable this policy setting, the HTTP listener always appears.

If you disable or do not configure this policy setting, the HTTP listener never appears.

When certain port 80 listeners are migrated to WinRM 2.0, the listener port number changes to 5985.

A listener might be automatically created on port 80 to ensure backward compatibility.

OK Cancel Apply

11. Click **Apply** and then **OK**.
12. Close the group policy editor.
13. Start the Command Prompt in admin mode and run the following command:
`gpupdate /force`

Configuring Auditing Policies

The following policy changes must be performed on the Domain Controller (for domain environments) or Source Computers (for non-domain environments).

- [Configure Security Audit Logging Policy](#)
- [Configure File Auditing Policy](#)

- [Configure Audit File System Policy](#)
- [Disable Audit Token Right Adjusted Success Events](#)

Configure Security Audit Logging Policy

Configure this policy to control Windows logging. Because Windows generates many security logs, specify the categories of events that you want to be logged and available for monitoring by FortiSIEM.

1. Log in to the machine where you want to configure the policy as an administrator.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand **Local Policies** and select **Audit Policy**.
You will see the current security audit settings.
4. Select a policy and edit the **Local Security Settings** for the events you want to be audited. The recommended settings are:

Policy	Description	Settings
Audit account logon events and Audit logon events	For auditing log in activity.	Select Success and Failure .
Audit object access events	For auditing access to files and folders. There is an additional configuration requirement for specifying which files and folders, users and user actions will be audited. See the next section, <i>Configuring File Auditing Policy</i> .	Select Success and Failure .
Audit system events	Includes system up/down messages.	

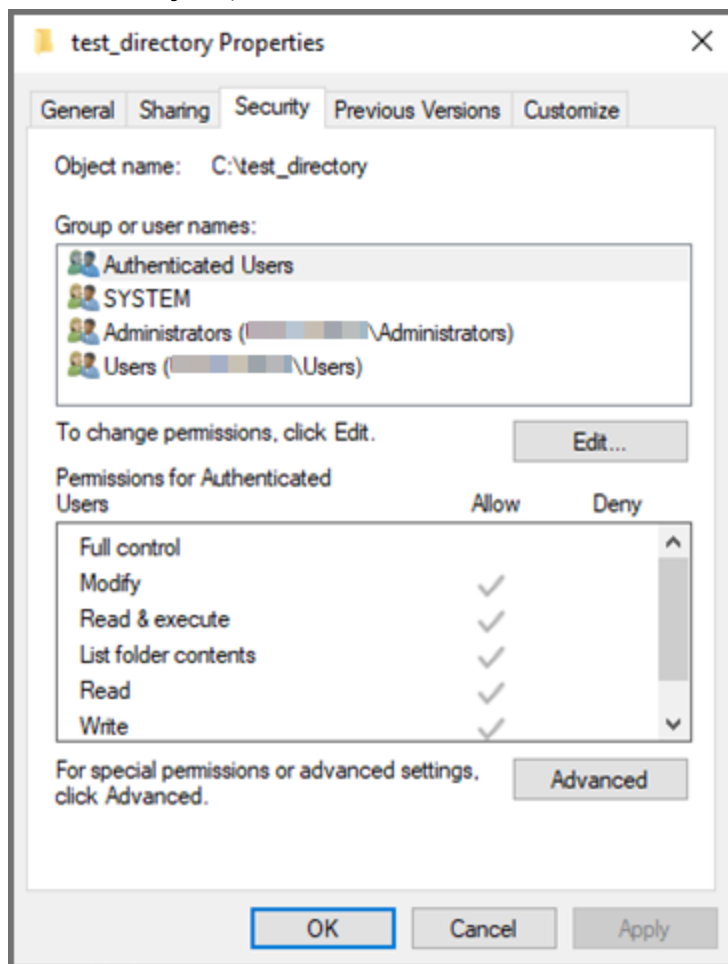
5. For an Enterprise Server's Domain Group Policy, make sure you set the following under **Group Policy > Local Policies > Audit Policy**:
Policy = Audit object access
Security Setting = Success or Failure

Configure File Auditing Policy

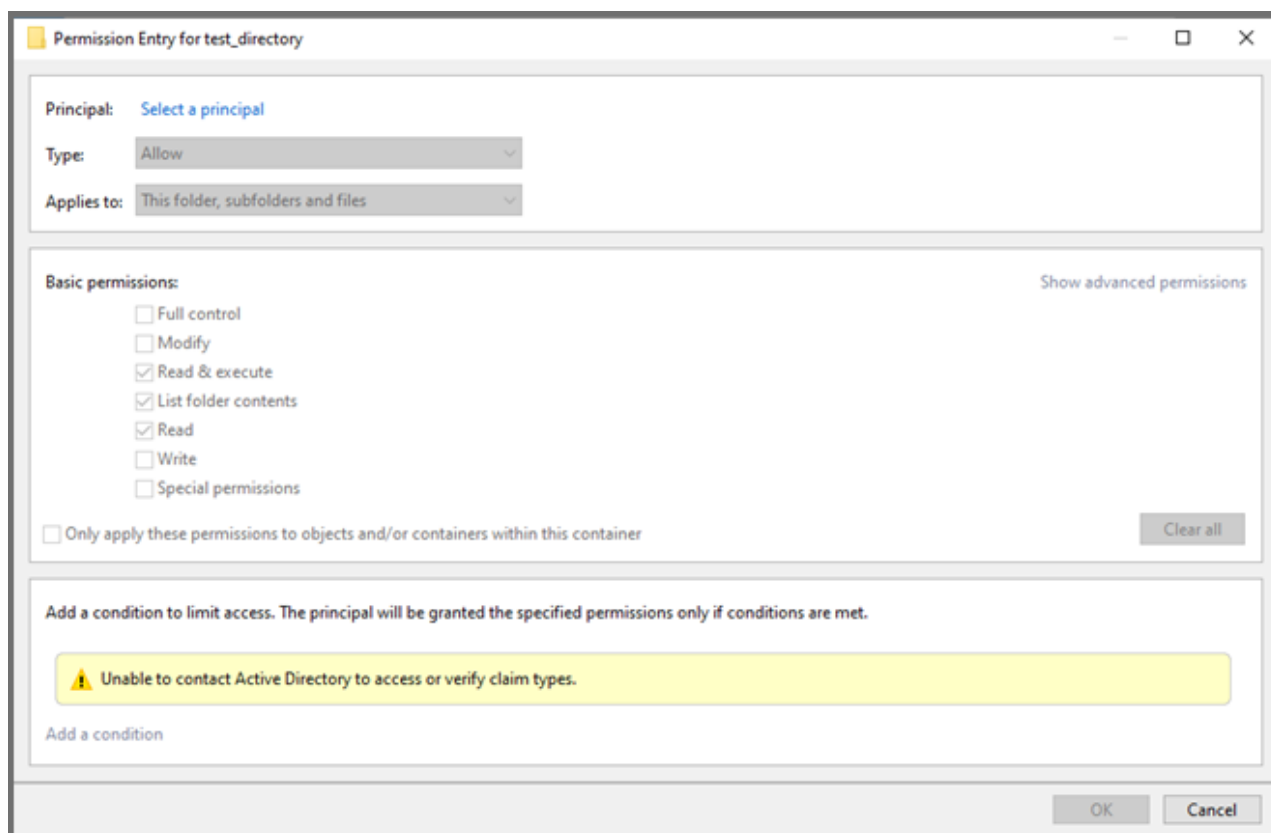
Configure this policy to see user meta data in file auditing events.

1. Log in to the machine where you want to set the policy with administrator privileges.
On a domain computer, a Domain administrator account is needed.
2. Open Windows Explorer, select the file you want to set the auditing policy for, right-click on it, and select **Properties**. By default, the **General** tab will be shown. Select the **Security** tab to continue.

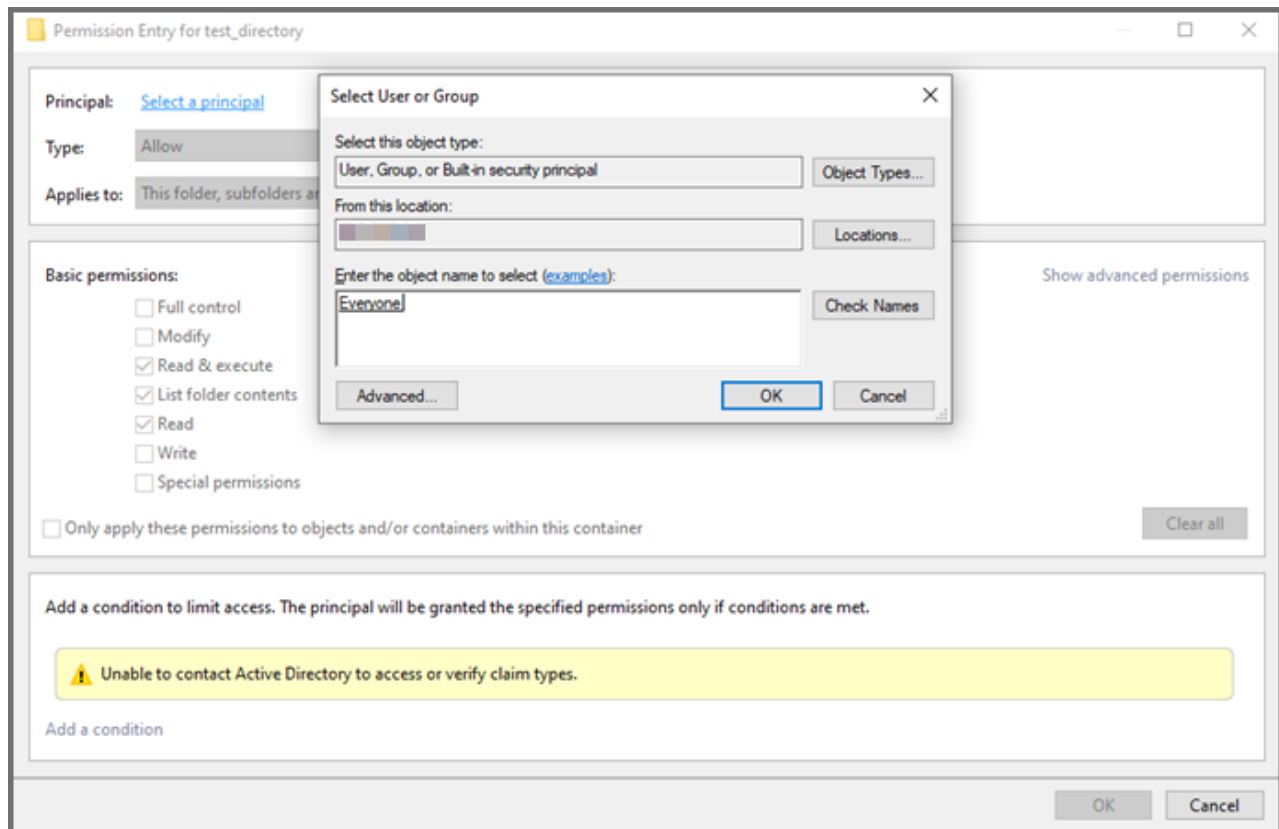
3. In the **Security** tab, click **Advanced**.



4. Select the **Auditing** tab, and click **Add**, then click **Select a principal**. This button is labeled **Edit** in Windows 2008.



5. In the **Select User or Group** dialog, click **Advanced**, and find and select the users, or groups, whose access to this file you want to monitor. If you want to audit all users access to the audited folder, select **Everyone** as shown below.



6. Click **OK** after adding the users.
7. In the **Permissions** tab, set the permissions for each user added.
The configuration is now complete. Windows will generate audit events when the users or groups you specified take the actions specified on the files or folders for which you set the audit policies.

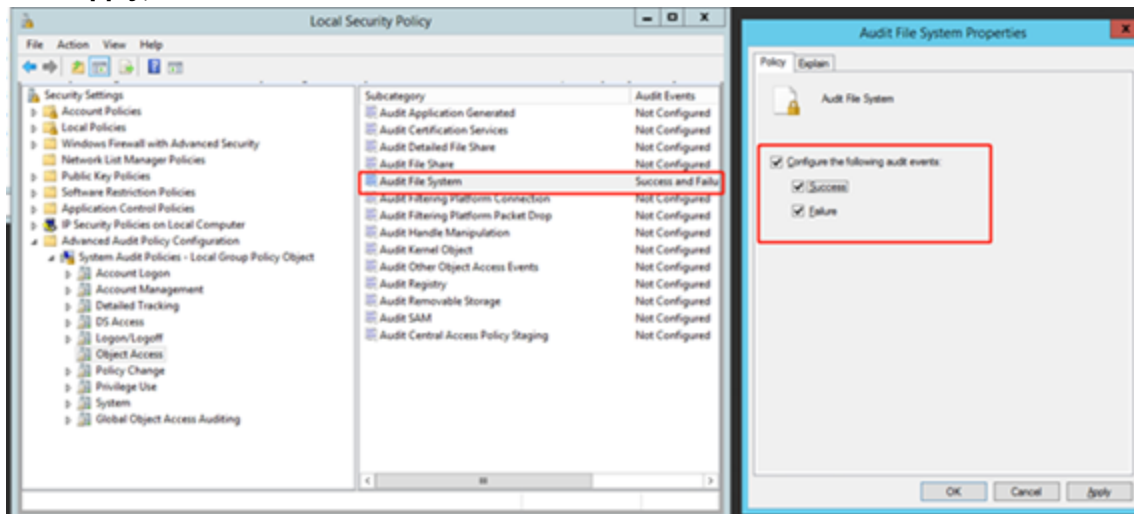
Configure Audit File System Policy

Configure this policy to enable change events for permission and/or ownership changes to files and/or directories. The policy will also upload the monitored files to FortiSIEM.

Complete these steps to enable Audit File System policy:

1. Log in, with administrator privileges, to the machine where you want to set the policy.
On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand the **Advanced Audit Policy Configuration** node.
4. Expand **System Audit Policies-Local Group Policy Object** node.
You will see the current security audit settings.
5. Select **Object Access**.
6. Select **Audit File System** on the left side of the window.
7. Double-click **Audit File System**. In the pop-up window, select both **Success** and **Failure** under **Configure the following audit events**.

8. Click **Apply**, then **OK**.



The Audit File System Policy is now enabled. Reboot your system to apply the changes.

Disable Audit Token Right Adjusted Success Events

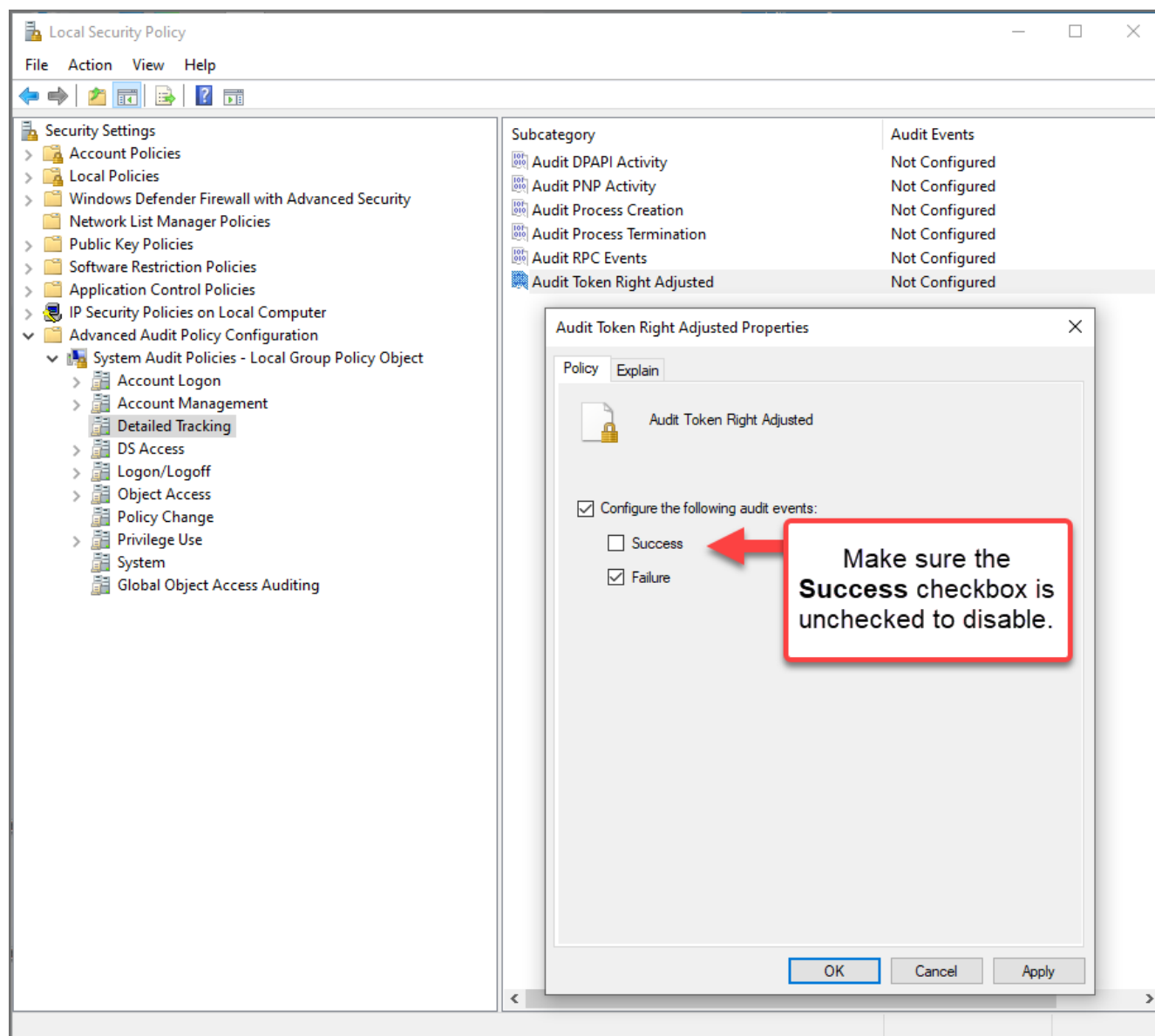
As per Microsoft, it is recommended to Disable "Success" auditing for "Audit Token Right Adjusted".

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4703#security-monitoring-recommendations>.

By enabling "Success Auditing" for Audit Token Right Adjusted (Detailed Tracking), 800+ (4703) events can be generated in a second, resulting in this high volume event impacting system performance.

Complete these steps to disable "Success" for "Audit Token Right Adjusted".

1. Log in, with administrator privileges, to the machine where you want to set the policy.
On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand to **Security Settings > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Object > Detailed Tracking**.
4. Go to the **Detailed Tracking** subcategory, and select **Audit Token Right Adjusted**.
5. Double click **Audit Token Right Adjusted**, select the **Configure the following audit events:** checkbox.
6. Uncheck the **Success** checkbox if needed to disable.
7. Click **Apply**.



QNAP Turbo NAS

Support Added: FortiSIEM 4.7.2

Vendor Version Tested: Not Provided

Vendor: QNAP

Product Information: <https://www.qnap.com/en-us>

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Reports](#)
- [Configuration](#)
- [Sample Logs](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		General logs including events and access.	Security Monitoring

Event Types

In **Admin > Device Support > Event Types**, search for "qnap" to see the event types associated with this device.

Reports

The following report is available for QNAP.

- QNAP Turbo NAS File Access - Reports All Turbo NAS File Accesses (syslog)

Configuration

For syslog, configure QNAP Turbo NAS by accessing QuLog Center and taking the following steps.

References:

- <https://docs.qnap.com/operating-system/qne-network/1.0.x/en-us/sending-system-logs-to-a-syslog-server-35997D85.html>

- <https://www.qnap.com/en/how-to/faq/article/what-kind-of-syslog-format-can-qnap-nas-receive-and-send#>
1. Navigate to **QuLog Service > Log Sender > Send to Syslog Server**.
 2. Toggle **Send logs to remote syslog server** to the **on** position.
 3. Click **Add Destination**, and take the following steps.
 - a. In the **Destination IP** field, enter the FortiSIEM Collector IP address.
 - b. In the **Port** field, enter "514".
 - c. In the **Transfer protocol** field, select UDP.
Note: Optionally, TCP syslog on port 1514 or Syslog over TLS on port 6514 is also supported. See [Syslog over TLS](#) section for more information.
 - d. For **Log type**, select the type(s), for example Event & Access Logs.
 - e. For **Format**, select **RFC-3164**.
 - f. When done, click **Apply**.
Note: Click the **Send a Test Message** button to test.
 4. Verify in FortiSIEM Analytics search that QNAP logs are being ingested.

Sample Logs

```
<30>Jun 25 14:41:36 Galaxy qlogd[8029]: conn log: Users: EXAMPLE\exampleuser123, Source IP: 192.0.20.0, Computer name: 192.0.20.0, Connection type: SAMBA, Accessed resources: STORE/AA Doe - MPLS Project/desktop.ini, Action: Read
```

```
<38>Jun 25 14:42:17 Galaxy qlogd[8029]: conn log: Users: admin, Source IP: 192.0.20.0, Computer name: ---, Connection type: HTTP, Accessed resources: Administration, Action: Login OK
```

Sun Solaris Server

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	Hardware (cpu details, memory)	Memory paging rate, Disk I/O utilization	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "solaris" to see the event types associated with this device.

Configuration

- SNMP v1 and v2c
- SSH

SNMP v1 and v2c

1. Check if the netsnmp package installed. Solaris has built-in snmp packages. If the netsnmp is not installed, use `pkgadd` cmd to install it.

2. Start snmp with the default configuration.

SSH

1. Make sure that the vmstat and iostat commands are available. If not, install these libraries.
2. Create a user account that can issue vmstat and iostat commands. FortiSIEM will use that user account to log in to the server.

Settings for Access Credentials

- [SNMP, Telnet, and SSH Access Credentials for All Devices](#)
- [LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices](#)
- [LDAP, DPAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices](#)

SNMP, Telnet, and SSH Access Credentials for All Devices

See [Access Credentials](#).

LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	Sun Solaris
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	OpenLDAP
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or 389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
Password Config	See Password Configuration
User Name	Name of the user able to access this system

Settings	Value
Password	Password of the user able to access this system

LDAP, DPAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	Sun Solaris
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	Microsoft Active Directory
Server Port	Default - 3268 (Global Catalog port) for LDAP, LDAP Start TLS; 3269 (Global Catalog port) for LDAPS. or 389 for LDAP, LDAP Start TLS; 636 for LDAPS. Note: Global catalog ports when used, are much more performant versus the LDAP ports, but not all LDAP attributes may be present by default in Global Catalog service.
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

Storage

FortiSIEM supports these storage devices for discovery and monitoring.

- [Brocade SAN Switch](#)
- [Dell Compellent Storage](#)
- [Dell EqualLogic Storage](#)
- [EMC Clarion Storage](#)
- [EMC Isilon Storage](#)
- [EMC VNX Storage](#)
- [NetApp Data ONTAP](#)
- [NetApp Filer Storage](#)
- [Nimble Storage](#)
- [Nutanix Storage](#)

Brocade SAN Switch

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		Hardware Status: Fan, Power Supply, Temperature (FortiSIEM Event Type: PH_DEV_MON_HW_STATUS)	Availability Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "brocade" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#)

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Brocade San Switch
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Dell Compellent Storage

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		Hardware component health: Power, Temperature, Fan	Availability Monitoring
SNMP		Volume Utilization	Performance Monitoring

Event Types

- Ping Monitoring: PH_DEV_MON_PING_STAT
- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL
- Hardware Status: PH_DEV_MON_HW_STATUS
- Disk Utilization: PH_DEV_MON_DISK_UTIL

Rules

- [Availability](#)
- [Performance \(Fixed Threshold\)](#)

Availability

- Storage Hardware Warning
- Storage Hardware Critical

Performance (Fixed Threshold)

- NFS Disk space Warning
- NFS Disk Space Critical

Reports

- Dell Compellent Hardware Status
- Top Dell Compellent Devices By Disk Space Util
- Top Dell Compellent Devices By Disk Space Util (Detailed)
- Top Dell Compellent modules by fan speed
- Top Dell Compellent modules by temperature
- Top Dell Compellent modules by voltage

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell Compellent Storage
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Dell EqualLogic Storage

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		Hardware component health: Component name (Disk, Power supply, Temperature, Fan, RAID health), Component status, Host spare ready disk count Overall Disk health metrics: Total disk count, Active disk count, Failed disk count, Spare disk count	Availability Monitoring
SNMP		Connection metrics: Connection Count, Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) Disk performance metrics: Disk Name, Disk I/O Utilization, Disk I/O Queue, Read volume (KBps), Write volume (KBps) Group level performance metrics: Total storage, Used storage, Reserved storage, Reserved used storage, Total volumes, Used volumes, Online volumes, Total snapshot, Used snapshot, Online snapshot	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "equallogic" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "equallogic" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "equallogic" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell EqualLogic
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

EMC Clariion Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
NaviSecCLI	Host name, Operating system version, Hardware model, Serial number, Network interfaces* Installed Software, Storage Controller Ports Hardware components: Enclosures, Fan, Power Supply, Link Control Card, CPU, Disk RAID Groups and the assigned disk LUNs and LUN - > RAID Group mappings Storage Groups and memberships (Host, Port, LUN).	Processor utilization: SP Name, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) Port I/O: Port name, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) RAID Group I/O: RAID Group id, RAID type, Total disk, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) LUN I/O: LUN name, LUN id, Total disk, Used disk, Free disk, Disk util, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) Host HBA Connectivity: Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name, Storage Group, LUN Names, Login Status, Registration Status Host HBA Unregistered Host: Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name Hardware component health: Component name (Disk, Power supply, LCC, Fan, Link, Port), Component status, Host spare ready disk count Overall Disk health: Total disk count, Total disk size (MB), Active disk count, Failed disk count, Spare disk count	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "clariion" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Installing the NaviSecCLI Library in FortiSIEM

Changing NaviSecCLI Credentials

If you change the NaviSecCLI credentials on your EMC Clariion device, the certificates may also be changed and naviseccli may prompt you to accept new certificates. This should only happen the first time after a certificate change, however, FortiSIEM discovery and performance monitoring will fail. You must run NaviSecCLI manually on each Supervisor and Worker in your deployment and accept the certificate, and then rediscover your EMC Clariion device for performance monitoring to resume.

Configuration of your EMC Clariion storage device involves installing EMC's NaviSecCLI library in your FortiSIEM virtual appliance, and then setting the access credentials that the appliance will use to communicate with your device.

1. Log in to your FortiSIEM virtual appliance as root.
2. Copy the file NaviCLI-Linux-64-x86-versionxyz.rpm to the FortiSIEM directory.
3. Run `rpm -Uvh NaviCLI-Linux-64-x86-versionxyz.rpm` to install the rpm package.

```
[root@Rob-SP-94 tmp]# rpm -Uvh NaviCLI-Linux-64-x86-en_US-7.30.15.0.44-1.x86_64.rpm
Preparing... ##### [100%]
1:NaviCLI-Linux-64-x86-en##### [100%]
Please enter the verifying level(low|medium|l|m) to set?
m
Setting medium verifying level
[root@Rob-SP-94 opt]# ls -la
total 40
drwxr-xr-x 8 root root 4096 Aug 22 16:06 .
drwxr-xr-x 29 root root 4096 Aug 16 16:46 ..
drwxr-xr-x 11 admin admin 4096 Jul 23 18:56 glassfish
lrwxrwxrwx 1 root root 16 Aug 16 16:46 Java -> /opt/jdk1.6.0_32
drwxr-xr-x 8 root root 4096 Jun 2 16:35 jdk1.6.0_32
```

```
drwxr-xr-x 5 root root 4096 Aug 22 16:06 Navisphere <----Note this directory was created***
drwxrwxr-x 14 admin admin 4096 Jul 24 11:22 phoenix
drwxrwxr-x 3 root root 4096 Jun 2 16:36 rpm
drwxr-xr-x 8 root root 4096 Jun 18 2010 vmware
[root@Rob-SP-94 opt]#
```

4. Change the user role to the admin su - admin and make sure that the user can run the command `naviseccli -h -User <user> -Password <pwd> -Scope global getall -sp` from the directory `/opt/phoenix/bin`.

```
[root@Rob-SP-94 Navisphere]# cd bin
[root@Rob-SP-94 bin]# su - admin
[admin@Rob-SP-94 ~]$ naviseccli
Not enough arguments
Usage:
[-User <username>] [-Password <password>]
[-Scope <0 - global; 1 - local; 2 - LDAP>]
[-Address <IPAddress | NetworkName> | -h <IPAddress | NetworkName>]
[-Port <portnumber>] [-Timeout <timeout> | -t <timeout>]
[-AddUserSecurity | -RemoveUserSecurity | -DeleteSecurityEntry]
[-Parse | -p] [-NoPoll | -np] [-cmdtime]
[-Xml] [-f <filename>] [-Help] CMD <Optional Arguments>[security -certificate]
[admin@Rob-SP-94 ~]$ pwd
/opt/phoenix/bin
```

5. Make sure that the Navisphere Analyzer module is on.
If the module is off, performance metrics will not be available and discovery will fail. This log shows an example of the module being turned off.

```
[admin@fsiem ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100 getall -sp
Server IP Address:      192.168.1.100
Agent Rev:              7.32.26 (0.95)
SP Information
-----
Storage Processor:      SP A
Storage Processor Network Name:  A-IMAGE
Storage Processor IP Address:    192.168.1.100
Storage Processor Subnet Mask:   255.255.255.0
Storage Processor Gateway Address: 192.168.1.254
Storage Processor IPv6 Mode:      Not Supported
Management Port Settings:
Link Status:              Link-Up
Current Speed:             1000Mbps/full duplex
Requested Speed:           Auto
Auto-Negotiate:            YES
Capable Speeds:            1000Mbps half/full duplex
                           10Mbps half/full duplex
                           100Mbps half/full duplex
                           Auto
System Fault LED:          OFF
Statistics Logging:        OFF    <----- Note: performance statistics are not being
collected
```

```

<----- so FortiSIEM can not pull stats and discovery
will fail.
<----- See how to turn ON Statistics Logging below.
SP Read Cache State      Enabled
SP Write Cache State     Enabled
....

```

6. If the Navisphere Analyzer module is off, turn it on with the `setstats -on` command.

```

[admin@fsiem ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100 setstats -
on
[admin@fsiem ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100 getall -sp

Server IP Address:      192.168.1.100
Agent Rev:              7.32.26 (0.95)

SP Information
-----
Storage Processor:      SP A
Storage Processor Network Name:  A-IMAGE
Storage Processor IP Address:    192.168.1.100
Storage Processor Subnet Mask:   255.255.255.0
Storage Processor Gateway Address: 192.168.1.254
Storage Processor IPv6 Mode:     Not Supported
Management Port Settings:
Link Status:             Link-Up
Current Speed:           1000Mbps/full duplex
Requested Speed:         Auto
Auto-Negotiate:          YES
Capable Speeds:          1000Mbps half/full duplex
                        10Mbps half/full duplex
                        100Mbps half/full duplex
                        Auto

System Fault LED:        OFF
Statistics Logging:      ON <---NOTE that statistics Logging is now ON.
SP Read Cache State     Enabled
SP Write Cache State     Enabled
Max Requests:           N/A
Average Requests:       N/A
Hard errors:            N/A
Total Reads:            1012
Total Writes:           8871
Prct Busy:              6.98
Prct Idle:              93.0
System Date:            10/04/2013
Day of the week:        Friday
System Time:            11:23:48
Read_requests:          1012
Write_requests:          8871
Blocks_read:            26259
Blocks_written:         235896
Sum_queue_lengths_by_arrivals: 27398

```

```
Arrivals_to_non_zero_queue:    3649
....
```

7. Once this command runs successfully, you are ready to set the access credentials for your device in FortiSIEM and initiate the discovery process.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your EMC Clariion storage device over NaviSecCLI.

Setting	Value
Name	<set name>
Device Type	EMC Clariion
Access Protocol	Navisec CLI
Use LDAP	Select to use LDAP to access directory services
User Name	The user you configured to access NaviSecCLI
Password	The password associated with the user

EMC Isilon Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		Hardware component health: Component name (Disk, Power supply, Temperature, Fan), Component status (AO event type: PH_DEV_MON_HW_STATUS) Environmental: Temperature (AO event type: PH_DEV_MON_HW_TEMP), Voltage readings (AO event type: PH_DEV_MON_HW_VOLTAGE) Cluster membership change: (AO event type: PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE)	Availability Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "isilon" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "isilon" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "isilon" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

EMC VNX Storage Configuration

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Like EMC Clarion, FortiSIEM uses Navisec CLI to discover the device and to collect performance metrics. The only difference is that a slightly different command and XML formatted output is used.

Protocol	Information Discovered	Metrics collected	Used for
Navisec CLI	Host name, Operating system version, Hardware model, Serial number, Network interfaces* Installed Software, Storage Controller Ports Hardware components: Enclosures, Fan, Power Supply, Link Control Card, CPU, Disk Storage Pools, RAID Groups and the assigned disks LUNs and LUN -> Storage Pool and RAID Group mappings Storage Groups and memberships (Host, Port, LUN)	Processor utilization: SP Name, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) Storage Pool I/O: RAID Group id, RAID type, Total disk, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) LUN I/O: LUN name, LUN id, Total disk, Used disk, Free disk, Disk util, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps)	Availability and Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
		Host HBA Connectivity: Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name, Storage Group, LUN Names, Login Status, Registration Status Host HBA Unregistered Host: Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name Hardware component health: Component name (Disk, Power supply, LCC, Fan, Link, Port), Component status, Host spare ready disk count Overall Disk health: Total disk count, Total disk size (MB), Active disk count, Failed disk count, Spare disk count	

Configuration

- [Installing the NaviSecCLI Library in FortiSIEM](#)
- [Setting the IP Address for Credential Mapping](#)

Installing the NaviSecCLI Library in FortiSIEM

Changing NaviSecCLI Credentials

If you change the NaviSecCLI credentials on your EMC Clarion device, the certificates may also be changed and naviseccli may prompt you to accept new certificates. This should only happen the first time after a certificate change, however, FortiSIEM discovery and performance monitoring will fail. You must run NaviSecCLI manually on each Supervisor and Worker in your deployment and accept the certificate, and then rediscover your EMC Clarion device for performance monitoring to resume.

Configuration of your EMC Clarion storage device involves installing EMC's NaviSecCLI library in your FortiSIEM virtual appliance, and then setting the access credentials that the appliance will use to communicate with your device.

1. Log in to your FortiSIEM virtual appliance as root.
2. Copy the file NaviCLI-Linux-64-x86-versionxyz.rpm to the FortiSIEM directory.
3. Run `rpm --Uvh NaviCLI-Linux-64-x86-versionxyz.rpm` to install the rpm package.

```
[root@Rob-SP-94 tmp]# rpm -Uvh NaviCLI-Linux-64-x86-en_US-7.30.15.0.44-1.x86_64.rpm
Preparing... ##### [100%]
1:NaviCLI-Linux-64-x86-en##### [100%]
Please enter the verifying level(low|medium|l|m) to set?
m
Setting medium verifying level
[root@Rob-SP-94 opt]# ls -la
total 40
```

```
drwxr-xr-x 8 root root 4096 Aug 22 16:06 .
drwxr-xr-x 29 root root 4096 Aug 16 16:46 ..
drwxr-xr-x 11 admin admin 4096 Jul 23 18:56 glassfish
lrwxrwxrwx 1 root root 16 Aug 16 16:46 Java -> /opt/jdk1.6.0_32
drwxr-xr-x 8 root root 4096 Jun 2 16:35 jdk1.6.0_32
drwxr-xr-x 5 root root 4096 Aug 22 16:06 Navisphere <----Note this directory was created***
drwxrwxr-x 14 admin admin 4096 Jul 24 11:22 phoenix
drwxrwxr-x 3 root root 4096 Jun 2 16:36 rpm
drwxr-xr-x 8 root root 4096 Jun 18 2010 vmware
[root@Rob-SP-94 opt]#
```

4. Change the user role to the admin su - admin and make sure that the user can run the command `naviseccli -h -User <user> -Password <pwd> -Scope global getall -sp` from the directory `/opt/phoenix/bin`.

```
[root@Rob-SP-94 Navisphere]# cd bin
[root@Rob-SP-94 bin]# su - admin
[admin@Rob-SP-94 ~]$ naviseccli
Not enough arguments
Usage:
[-User <username>] [-Password <password>]
[-Scope <0 - global; 1 - local; 2 - LDAP>]
[-Address <IPAddress | NetworkName> | -h <IPAddress | NetworkName>]
[-Port <portnumber>] [-Timeout <timeout> | -t <timeout>]
[-AddUserSecurity | -RemoveUserSecurity | -DeleteSecurityEntry]
[-Parse | -p] [-NoPoll | -np] [-cmdtime]
[-Xml] [-f <filename>] [-Help] CMD <Optional Arguments>[security -certificate]
[admin@Rob-SP-94 ~]$ pwd
/opt/phoenix/bin
```

5. Make sure that the Navisphere Analyzer module is on.
If the module is off, performance metrics will not be available and discovery will fail. This log shows an example of the module being turned off.

```
[admin@fsiem ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100 getall -sp
Server IP Address:      192.168.1.100
Agent Rev:              7.32.26 (0.95)
SP Information
-----
Storage Processor:      SP A
Storage Processor Network Name:  A-IMAGE
Storage Processor IP Address:    192.168.1.100
Storage Processor Subnet Mask:   255.255.255.0
Storage Processor Gateway Address: 192.168.1.254
Storage Processor IPv6 Mode:      Not Supported
Management Port Settings:
Link Status:              Link-Up
Current Speed:             1000Mbps/full duplex
Requested Speed:           Auto
Auto-Negotiate:            YES
Capable Speeds:            1000Mbps half/full duplex
                           10Mbps half/full duplex
```

```

                                100Mbps half/full duplex
                                Auto
System Fault LED:                OFF
Statistics Logging:              OFF    <----- Note: performance statistics are not being
collected                      <----- so AccelOp can not pull stats and discovery will
fail.
                                <----- See how to turn ON Statistics Logging below.
SP Read Cache State              Enabled
SP Write Cache State            Enabled
....

```

6. If the Navisphere Analyzer module is off, turn it on with the `setstats -on` command.

```

[admin@fsiem ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100 setstats -
on
[admin@fsiem ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100 getall -sp

Server IP Address:      192.168.1.100
Agent Rev:              7.32.26 (0.95)

SP Information
-----
Storage Processor:      SP A
Storage Processor Network Name:  A-IMAGE
Storage Processor IP Address:  192.168.1.100
Storage Processor Subnet Mask:  255.255.255.0
Storage Processor Gateway Address: 192.168.1.254
Storage Processor IPv6 Mode:    Not Supported
Management Port Settings:
Link Status:             Link-Up
Current Speed:            1000Mbps/full duplex
Requested Speed:          Auto
Auto-Negotiate:           YES
Capable Speeds:           1000Mbps half/full duplex
                           10Mbps half/full duplex
                           100Mbps half/full duplex
                           Auto

System Fault LED:        OFF
Statistics Logging:      ON    <---NOTE that statistics Logging is now ON.
SP Read Cache State      Enabled
SP Write Cache State     Enabled
Max Requests:            N/A
Average Requests:        N/A
Hard errors:             N/A
Total Reads:             1012
Total Writes:            8871
Prct Busy:               6.98
Prct Idle:               93.0
System Date:             10/04/2013
Day of the week:         Friday
System Time:             11:23:48
Read_requests:           1012

```

```
Write_requests:      8871
Blocks_read:         26259
Blocks_written:      235896
Sum_queue_lengths_by_arrivals: 27398
Arrivals_to_non_zero_queue: 3649
....
```

7. Once this command runs successfully, you are ready to set the access credentials for your device in FortiSIEM and initiate the discovery process.

Setting the IP Address for Credential Mapping

Enter the **Storage Processor** IP address when you associate your device's access credentials to an IP address during the credential set up process. Do not enter any other IP address, such as the **Control Station** IP.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your EMC VNX storage device over NaviSecCLI.

Setting	Value
Name	<set name>
Device Type	EMC VNX
Access Protocol	Navisec CLI
Use LDAP	Select to use LDAP to access directory services
User Name	The user you configured to access NaviSecCLI
Password	The password associated with the user

NetApp Data ONTAP

- [Supported Version](#)
- [Configuration](#)

Supported Version

FortiSIEM supports the latest NetApp ONTAP API version listed here.

- NetApp ONTAP API 8.2

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	NetApp DataONTAP
Access Protocol	NetApp ONTAPI
Transport	- HTTP - HTTPS
Pull Interval	5 minutes
User Name	User name for device access
Password	Password for device access
Description	Description about the device
Settings	Description

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping:
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential in step 2 from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to NetApp Data ONTAP.
5. To see the jobs associated with DataONTAP, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "DataONTAP" in the search box.

NetApp Filer Storage

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Logical volumes, Physical Disks	Uptime, CPU utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Logical Disk Volume utilization	Availability and Performance Monitoring
SNMP		Hardware component health: Component name (Battery, Disk, Power supply, Temperature, Fan), Component status, Failed power supply count, Failed Fan Count Overall Disk health metrics: Total disk count, Active disk count, Failed disk count, Spare disk count, Reconstructing disk count, Scrubbing disk count, Add spare disk count	Availability Monitoring
SNMP		NFS metrics: Cache age, CIFS request rate (IOPS), NFS request rate (IOPS), Disk read rate (IOPS), Disk write rate (IOPS), Network Sent rate (Kbps), Network received rate (Kbps), RPC Bad calls, NFS Bad calls, CIFS Bad calls Detailed NFS V3 metrics: Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) Detailed NFS V4 metrics: Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) Detailed CIFS metrics: Total Read/Write rate (IOPS), Latency	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
		Detailed ISCSI metrics: Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) Detailed FCP metrics: Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) Detailed LUN metrics: LUN Name, Read request rate (IOPS), Write request rate (IOPS), Read/Write latency, Read volume (KBps), Write volume (KBps), Disk queue full	
ONTAP API		Detailed Aggregate metrics: Aggregate name, Read request rate (IOPS), Write request rate (IOPS), Transfer rate, CP Read rate Detailed Volume metrics: Volume Name, Disk Read request rate (IOPS), Disk Write request rate (IOPS), Disk read latency, Disk write latency, NFS Read request rate (IOPS), NFS Write request rate (IOPS), NFS Read latency, NFS Write latency, CIFS Read request rate (IOPS), CIFS Write request rate (IOPS), CIFS Read latency, CIFS Write latency, SAN Read request rate (IOPS), SAN Write request rate (IOPS), SAN Read latency, SAN Write latency Detailed Disk performance metrics: Disk Name, Disk Utilization, Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Transfer operations rate	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "netapp" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "netapp" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "netapp" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

1. Log in to your NetApp device with administrative privileges.
2. Go to **SNMP > Configure**.
3. For **SNMP Enabled**, select **Yes**.
4. Under **Communities**, create a public community with **Read-Only** permissions.
5. Click **Apply**.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Nimble Storage

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		Storage Disk Utilization: Disk name, Total Disk, Used Disk, Free Disk, Disk Utilization	Availability Monitoring
SNMP		Storage Performance metrics: Read rate (IOPS), Sequential Read Rate (IOPS), Write rate (IOPS), Sequential Write Rate (IOPS), Read latency, Write latency, Read volume (KBps), Sequential Read volume (KBps), Sequential Write volume (KBps), Used Volume (MB), Used Snapshot (MB), Non-Sequential Cache Hit Ratio (FortiSIEM Event Type: PH_DEV_MON_NIMBLE_GLOBAL_STAT)	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "nimble" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Nimble Storage NimbleOS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Nutanix Storage

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Process count, CPU utilization, Real and virtual memory utilization, Disk utilization, Process CPU/Memory utilization, Network Interface metrics	Availability and Performance Monitoring
SNMP		Disk Status: Cluster, Controller VM, Disk id, Disk serial, Disk utilization, Total Disk, Used Disk, Free Disk Disk Temp: Disk Id, disk serial, Controller VM, temperature Cluster Status: Cluster, Cluster version, storage utilization, total storage, used storage, IOPS, latency Service Status: Cluster, Controller VM, Cluster VM Status, Zeus Status, Stargate Status	Availability Monitoring
SNMP		Storage Pool Info: Cluster, storage pool name, storage utilization, total storage, used storage, IOPS, latency Container Info: Cluster, Container name, storage utilization, total storage, used storage, IOPS, latency	Performance Monitoring

Event Types

- PH_DEV_MON_SYS_CPU_UTIL

```
[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=1468,[cpuName]=Generic CPU,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.252.20,[cpuUtil]=100.000000,[sysCpuUtil]=0.000000,[userCpuUtil]=0.000000,[waitCpuUtil]=0.000000,
```

```
[kernCpuUtil]=0.000000,[contextSwitchPersec]=0.000000,[cpuInterruptPersec]=0.000000,
[pollIntv]=177,[cpuCore]=8,[loadAvg1min]=2.500000,[loadAvg5min]=2.500000,
[loadAvg15min]=2.390000,[phLogDetail]=
```

- PH_DEV_MON_SYS_MEM_UTIL

```
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9587,[memName]=Physical Memory,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.252.20,[memUtil]=93.210754,[pollIntv]=177,[phLogDetail]=
```

- PH_DEV_MON_SYS_VIRT_MEM_UTIL

```
[PH_DEV_MON_SYS_VIRT_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9590,[memName]=Virtual memory,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.252.20,[virtMemUsedKB]=30773124,[virtMemUtil]=93.210754,[pollIntv]=177,
[phLogDetail]=
```

- PH_DEV_MON_SYS_UPTIME

```
[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=1065,
[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.252.20,[sysUpTime]=1815730,
[sysUpTimePct]=100.000000,[sysDownTime]=0,[pollIntv]=56,[phLogDetail]=
```

- PH_DEV_MON_SYS_DISK_UTIL

```
[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9664,[diskName]=/home/nutanix/data/stargate-storage/disks/9XG6R3HG,
[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.252.20,[appTransportProto]=SNMP
(hrStorage),[diskUtil]=9.229729,[totalDiskMB]=938899,[usedDiskMB]=86658,[freeDiskMB]=852241,
[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_NET_INTF_UTIL

```
[PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phIntfFilter.cpp,
[lineNumber]=319,[intfName]=eth0,[intfAlias]=,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.252.20,[pollIntv]=56,[recvBytes64]=0,[recvBitsPerSec]=0.000000,
[inIntfUtil]=0.000000,[sentBytes64]=0,[sentBitsPerSec]=0.000000,[outIntfUtil]=0.000000,
[recvPkts64]=0,[sentPkts64]=0,[inIntfPktErr]=0,[inIntfPktErrPct]=0.000000,[outIntfPktErr]=0,
[outIntfPktErrPct]=0.000000,[inIntfPktDiscarded]=0,[inIntfPktDiscardedPct]=0.000000,
[outIntfPktDiscarded]=0,[outIntfPktDiscardedPct]=0.000000,[outQLen64]=0,
[intfInSpeed64]=1000000000,[intfOutSpeed64]=1000000000,[intfAdminStatus]=up,
[intfOperStatus]=up,[daysSinceLastUse]=0,[totIntfPktErr]=0,[totBitsPerSec]=0.000000,
[phLogDetail]=
```

- PH_DEV_MON_PROC_RESOURCE_UTIL

```
[PH_DEV_MON_PROC_RESOURCE_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=4378,[swProcName]=python,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.23.20,[procOwner]=,[memUtil]=0.379639,[cpuUtil]=0.000000,[appName]=python,
[appGroupName]=,[pollIntv]=116,[swParam]=/home/nutanix/ncc/bin/health_server.py --log_plugin_
output=true --logtostderr=true,[phLogDetail]=
```

- PH_DEV_MON_SYS_PROC_COUNT

```
[PH_DEV_MON_SYS_PROC_COUNT]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=11378,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.252.20,
[procCount]=327,[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_DISK_STATUS

```
[PH_DEV_MON_NUTANIX_DISK_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=216,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,
[cluster]=AmanoxLab01,[diskId]=24,[ntxControllerVMId]=7,[hwDiskSerial]=9XG6V4DS,
[diskUtil]=35.704633,[totalDiskMB]=916,[freeDiskMBNonRoot]=589,[inodeUsedPct]=0.234492,
[inodeMax]=61054976,[inodeFreeNonRoot]=60911807,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_CLUSTER_STATUS

```
[PH_DEV_MON_NUTANIX_CLUSTER_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=272,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,[cluster]=Lab01,
[clusterVersion]=e16-release-danube-4.1.2-stable-99e1e2dda7a78989136f39132e1f198989ef03a4,
[clusterStatus]=started,[diskUtil]=32.000000,[totalDiskMB]=14482532,[usedDiskMB]=4740567,
[diskRWReqPerSec]=3109.000000,[devDiskRWLatency]=0.631000,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_SERVICE_STATUS

```
[PH_DEV_MON_NUTANIX_SERVICE_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=287,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,[cluster]=Lab01,
[ntxControllerVMId]=5,[ntxClusterVMStatus]=Up,[ntxZeusStatus]=3287, 3310, 3311, 3312, 3389,
3403,[ntxStargateStatus]=5331, 5365, 5366, 5421, 19543,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO

```
[PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=239,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,[cluster]=Lab01,
[spoolId]=1474,[spoolName]=amanoxlab_sp,[diskUtil]=32.733000,[totalDiskMB]=14482532,
[usedDiskMB]=4740567,[diskRWReqPerSec]=155.000000,[devDiskRWLatency]=0.631000,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_CONTAINER_INFO

```
[PH_DEV_MON_NUTANIX_CONTAINER_INFO]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=257,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,[cluster]=Lab01,
[ntxContainerId]=1488,[ntxContainerName]=perflab_ndfs,[diskUtil]=8.357116,
[totalDiskMB]=14482532,[usedDiskMB]=1210322,[diskRWReqPerSec]=0.000000,
[devDiskRWLatency]=0.000000,[phLogDetail]=
```

Rules

Currently there are no system rules defined.

Reports

- Nutanix Cluster Disk Usage
- Nutanix Cluster Performance

- Nutanix Cluster Service Status
- Nutanix Cluster Storage Usage
- Nutanix Container Performance
- Nutanix Container Storage Usage
- Nutanix Storage Pool Performance
- Nutanix Storage Pool Usage

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Nutanix Controller VM
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Threat Intelligence

FortiSIEM supports these threat detection devices:

- [FortiInsight](#)
- [LastLine](#)
- [ThreatConnect](#)

External threat intelligence sources provide information about malware actors (Indicators of Compromise or IOCs). FortiSIEM can be configured to download this information periodically, either incrementally or full updates, according to a schedule you define. IOCs can include Malware IP, Domain, URL, and file hashes. You can write rules to look for matches in real time or reports to look for matches in historical data.

The following external threat intelligence sources are supported out of the box:

- Emerging Threat
- FortiGuard
- FortiSandbox
- Malware Domain
- SANS
- ThreatStream
- ThreatConnect
- TruSTAR
- Zeus

In general, any threat source that provides a CSV file or supports STIC/TAXII standards 1.0, 1.1, and 2.0 can be automatically supported by FortiSIEM. FortiSIEM also provides a Java-based API which can be used to support a new website.

Additional information for specific threat intelligence feeds is available [here](#).

- [Working with AlienVault OTX](#)
- [Working with Dragos IOCs](#)
- [Working with FortiGuard IOCs](#)
- [Working with Malware Patrol](#)
- [Working with OpenCTI Threatfeeds](#)
- [Working with ThreatConnect](#)

Fortinet FortiInsight

FortiInsight is a unique data security and threat detection solution that delivers advanced threat hunting to help you spot, respond to, and manage risky behaviors that put your business-critical data at risk. It combines powerful and flexible Machine Learning with detailed forensics around user actions to bring focus to the facts more rapidly than other solutions.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration in FortiInsight](#)
- [Configuration in FortiSIEM](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information collected	Used for
FortiInsight API	Policy based alerts and AI based alerts	Data security, threat protection

This feature allows FortiSIEM to get Policy-based alerts and AI-based alerts from FortiInsight.

Event Types

In **RESOURCES > Event Types**, enter "FortiInsight" in the main content panel **Search...** field to see the event types associated with this device.

Rules

No defined rules.

Reports

In **RESOURCES > Reports**, enter "FortiInsight" in the main content panel **Search...** field to see the rules associated with this device.

Configuration in FortiInsight

Get an API Key in FortiInsight

Complete these steps in the FortiInsight UI:

1. Login to FortiInsight.
2. Select **Admin > Account** from the left menu.
3. Click **New API Key** to open the New API Key dialog box.
4. Enter a descriptive **Name**.
5. Click **Save** to generate the API key. This will download a file containing the API key information (**Client ID**, **Client Secret**, and **Name**). Make a note of these values; you will need them when you configure FortiSIEM.

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	Fortinet FortiSIEM
Access Protocol	FortiInsight API
Pull Interval	The interval in which FortiSIEM will pull events from FortiInsight. Default is 3 minutes.
Client ID	Access key for your FortiInsight instance.
Client Secret	Secret key for your FortiInsight instance
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your Fortinet FortiInsight credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiInsight.
5. To see the jobs associated with FortiInsight, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "FortiInsight" in the search box.

Sample Events

```
[FORTIINSIGHT_POLICY_ALERT] = {"description":"","events":[{"act":"file
downloaded","app":"chrome.exe","childId":null,"d":"2019-03-
18T13:22:24.344+00:00","id":null,"m":"uqP","mn":{"dh":"tcp://server-10-230-2-
153.lhr5.r.cloudfront.net","dip":"10.1.1.76","dp":61024,"ext":".mkv","fp":"c:\\users\\Administrato
r\\documents\\secret\\prototypedemo1.mkv","fs":2307792448,"loc":
{"altCode":null,"city":"Augsburg","code":"DE","country":"Germany","latitude":"48.3718","longitude"
:"10.8925"},"p":"tcp-ip-
4","sip":"78.47.38.226","sp":443,"ts":1460},"r":"c:\\users\\Administrator\\documents\\secret\\prot
otypedemo1.mkv-> tcp://server-54-230-2-153.lhr5.r.cloudfront.net:443","u":"acmeltd__
engineer2"}],"extendedEvents":[{"act":"file
downloaded","app":"chrome.exe","childId":null,"d":"2019-03-
18T13:22:24.344+00:00","id":null,"latestHostname":"mimas","latestIp":"10.10.0.1","m":"uqP","mn":
{"dh":"tcp://server-54-230-2-
153.lhr5.r.cloudfront.net","dip":"10.1.1.76","dp":61024,"ext":".mkv","fp":"c:\\users\\Administrato
r\\documents\\secret\\prototypedemo1.mkv","fs":2307792448,"loc":
{"altCode":null,"city":"Augsburg","code":"DE","country":"Germany","latitude":"48.3718","longitude"
:"10.8925"},"p":"tcp-ip-
4","sip":"78.47.38.226","sp":443,"ts":1460},"r":"c:\\users\\Administrator\\documents\\secret\\prot
otypedemo1.mkv-> tcp://server-10-230-2-
153.lhr5.r.cloudfront.net:443","resolvedUsername":"","u":"acmeltd__engineer2"}],"id":"AWmQ98PYg7b_
-i6_5Rvg","labels":[""],"policyId":"default_6COnUMjTCB8N","policyName":"Browser
Download","regimes":
["ZoneFox"],"serverIp":"192.0.2.0","serverName":"fortisiemtest.dev.fortiinsight.cloud","severity":
10,"status":"New","time":"2019-03-18T13:22:29.473715+00:00"}
```

Lastline

The Lastline parser collects syslog log events in CEF format.

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Syslog](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog	Device Type	Endpoint activity such as file download, email attachments, network connections.	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Lastline" to see the event types associated with this device.

Rules

There are no specific rules for Lastline, however rules that match the Event Type Groups associated with Lastline Events may trigger.

Reports

There are no specific Reports for Lastline, however reports that match the Event Type Groups associated with Lastline Events may return results.

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514 using CEF formatting.

Sample Events

```
Aug 13 14:48:37 fortisiem CEF:0|Lastline|Enterprise|7.10|appliance-status|Appliance
Status|1|cat=Online cs1=SENSOR cs1Label=deviceType
cs2=https://example/portal#/appliances/config/status/76b80c7ac11a4d37bc6b29e66726b01d
cs2Label=deviceStatusLink deviceExternalId=76b80c7ac11a4d37bc6b29e66726b01d dvc=10.31.61.152
dvchost=example.com end=Aug 13 2018 16:48:37 CEST rt=Aug 13 2018 16:48:37 CEST start=Aug 13 2018
16:48:37 CEST
```

ThreatConnect

- What is Discovered and Monitored
- Configuring ThreatConnect
- Configuring FortiSIEM to Download IOCs from ThreatConnect
- Downloading Other IOCs

What is Discovered and Monitored

Protocol	Information Collected	Used For
ThreatConnect API	Malware Domain, IP, URL and Hash	Detect threats for Security and Compliance

Configuring ThreatConnect

Create an API Key to be used for FortiSIEM communication.

The details are here:

<https://kb.threatconnect.com/customer/en/portal/articles/2188549-creating-user-accounts>

1. Log in to your ThreatConnect portal as an administrative user.
2. Go to **My Profile > ORG Settings**.
3. Click **Create API User**.
These credentials will be created:
 - **Access ID**
 - **Secret Key**
4. Note the **Organization Name**. You will need it in a later step.
5. ThreatConnect contains many threat feeds. If you want to get specific threatfeeds, then you must know the threat feeds that are available for your account. You can see these feeds by navigating to **Browse > Indicators > My ThreatConnect > Intelligent Sources**.

Configuring FortiSIEM to Download IOCs from ThreatConnect

Use the Access ID and Secret Key that were created in the previous section to enable FortiSIEM access.

FortiSIEM can provide the following IOCs from ThreatConnect:

- Malware Domain
- Malware IP
- Malware URL
- Malware Hash

Follow these steps to set up **Malware Domain** downloads from ThreatConnect.

1. Login to FortiSIEM.
2. Go to **RESOURCES > Malware Domain > ThreatConnect Malware Domain**.
3. Click **More > Update**. Select **Update via API**.
4. Enter the following fields
 - a. Set **User Name** to Access ID (Step 3a above).
 - b. Set **Password** to Secret Key (Step 3b above).
 - c. Set **Data Format** to STIX-TAXII.
 - d. For **Collection:**, you have two choices:
 - To get *all* threatfeeds - enter All:<Organization Name> (Step 4 above), or
 - To get *specific* threatfeeds, enter comma-separated values of threatfeeds (obtained from Step 5 above).
 - e. Set **Data Update** = Incremental
5. Click **Save**.
6. Click **Schedule** to specify how often the threat feed will be updated.
 - a. Choose **Start time**.
 - b. Choose **Recurrence pattern**.
 - c. Click **Save**.
7. Wait until the first scheduled download occurs. Then, navigate to **RESOURCES > Malware Domain > ThreatConnect Malware Domain**. Downloaded Malware domains will be displayed in the right-hand table. You can use this object in rules and reports to detect hits.

Downloading Other IOCs

The steps for configuring FortiSIEM to download other IOCs are identical, except for the following details:

- Malware IP—Navigate to **RESOURCES > Malware Domain > ThreatConnect Malware IP**
- Malware URL—Navigate to **RESOURCES > Malware Domain > ThreatConnect Malware URL**
- Malware Hash—Navigate to **RESOURCES > Malware Domain > ThreatConnect Malware Hash**

Virtualization

FortiSIEM supports these virtualization servers for discovery and monitoring.

- [Hyper-V](#)
- [HyTrust CloudControl](#)
- [KVM](#)
- [Nutanix Prism](#)
- [VMware ESX](#)

Hyper-V

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Powershell over WMI		CPU, Memory, Network and Storage metrics both at Guest and Host level.	Performance Monitoring

Event Types

- PH_DEV_MON_HYPERV_OVERALL_HEALTH: HyperV Machine Health Summary

```
[PH_DEV_MON_HYPERV_OVERALL_HEALTH]:[hostIpAddress]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[vmHealthCritCount]=0,[vmHealthOkCount]=10
```

- PH_DEV_MON_HYPERV_OVERALL_SYSINFO: HyperV System Information

```
[PH_DEV_MON_HYPERV_OVERALL_SYSINFO]:[hostIpAddress]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[notificationCount]=10,[virtualProcessors]=52,[totalPages]=67290,[partitionCount]=6,[logicalProcessors]=16
```

- PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC: HyperV Logical Processor Usage

```
[PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC]:[hostIpAddress]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[idleTimePct]=47.30,[guestRunTimePct]=50.88,[hypervisorRunTimePct]=1.97,[totalRunTimePct]=52.84,[cpuInterruptPerSec]=53390.62,[contextSwitchPerSec]=85516.44
```

- PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC: HyperV Root Virtual Processor Usage

```
[PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC]:[hostIpAddress]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[phyMachIpAddress]=172.16.20.180,[phyMachName]=WIN-HH2MFBPMHMR,[guestRunTimePct]=0.19,[hypervisorRunTimePct]=0.04,[totalRunTimePct]=0.23,[cpuInterruptPerSec]=4588.63,[interceptCost]=1458
```

- PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC: HyperV Guest Virtual Processor Usage

```
[PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC]:[hostIpAddr]=172.16.20.185,[hostName]=fsiem-reporter-hyperv-4.3.1.1158,[vmName]=fsiem-reporter-hyperv-4.3.1.1158,[phyMachIpAddr]=172.16.20.180,[phyMachName]=WIN-HH2MFBPMHMR,[guestRunTimePct]=1.06,[hypervisorRunTimePct]=0.70,[totalRunTimePct]=1.77,[cpuInterruptPersec]=6474.56,[interceptCost]=1086
```

- PH_DEV_MON_HYPERV_MEM_PARTITION: HyperV Memory Partition usage

```
[PH_DEV_MON_HYPERV_MEM_PARTITION]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[1gGpaPages]=0,[2mGpaPages]=16385,[4kGpaPages]=9949,[depositedGpaPages]=20946
```

- PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM: HyperV per-VM Memory Partition usage

```
[PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM]:[phyMachIpAddr]=172.16.20.180,[phyMachName]=WIN-HH2MFBPMHMR,[hostIpAddr]=172.16.20.182,[hostName]=fsiem-va-hyperv-4.3.1.1158,[vmName]=fsiem-va-hyperv-4.3.1.1158,[1gGpaPages]=0,[2mGpaPages]=4096,[4kGpaPages]=2089,[depositedGpaPages]=5044
```

- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION: HyperV Root Partition Total Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[1gGpa]=0,[2mGpa]=32613,[4kGpa]=9760,[depositedGpa]=46344
```

- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT: HyperV Root Partition Root Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[1gGpa]=0,[2mGpa]=32613,[4kGpa]=9760,[depositedGpa]=46344
```

- PH_DEV_MON_HYPERV_MEM_VID_PARTITION: HyperV VID Partition Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_VID_PARTITION]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[physicalPages]=8398888,[remotePages]=0
```

- PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM: HyperV per-VM VID Partition Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM]:[phyMachIpAddr]=172.16.20.180,[phyMachName]=WIN-HH2MFBPMHMR,[hostIpAddr]=172.16.20.185,[hostName]=fsiem-reporter-hyperv-4.3.1.1158,[vmName]=fsiem-reporter-hyperv-4.3.1.1158,[physicalPages]=1050632,[remotePages]=0
```

- PH_DEV_MON_HYPERV_MEM_OVERALL: HyperV Root Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_OVERALL]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[freeMemKB]=27519348,[pageFaultsPersec]=0
```

- PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH: HyperV Virtual Switch Network Usage

```
[PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[vSwitch]=broadcom bcm5709c netxtreme ii gige [ndis vbd client] _34 - virtual switch,[recvBitsPerSec]=719403.45,[recvPktsPerSec]=323.03,[sentBitsPerSec]=3382443.50,[sentPktsPerSec]=283.90,[totalPktsPerSec]=323.03[PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,[vSwitch]=broadcom bcm5709c netxtreme ii gige [ndis vbd client] _34 - virtual switch,[recvBitsPerSec]=719403.45,[recvPktsPerSec]=323.03,[sentBitsPerSec]=3382443.50,[sentPktsPerSec]=283.90,[totalPktsPerSec]=323.03
```

- PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER: HyperV Virtual Switch Per Adapter Network Usage

```
[PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER]:[phyMachIpAddr]=172.16.20.180,[phyMachName]=WIN-
HH2MFBPMHMR,[hostIpAddr]=172.16.20.182,[hostName]=fsiem-va-hyperv-4.3.1.1158,[vmName]=fsiem-
va-hyperv-4.3.1.1158,[intfName]=adapter_e1eb0a1f-1b36-48fe-be79-fde20d335364--31575d2f-5085-
45d3-905f-2f3e17342a81,[recvBitsPerSec]=64970.24,[recvPktsPerSec]=20.86,
[sentBitsPerSec]=124741.68,[sentPktsPerSec]=42.61,[totalPktsPerSec]=20.86
```

- PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE: HyperV Virtual Storage Usage

```
[PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[diskName]=e:-hyperinstance-report431-virtual hard disks-fsiem-reporter-
4.3.1.1158-disk2.vhdx,[diskErrors]=2,[diskFlushes]=1267221,[diskReadKBytesPerSec]=0.00,
[diskReadReqPerSec]=0.00,[diskWriteKBytesPerSec]=0.00,[diskWriteReqPerSec]=0.00
```

- PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK: HyperV Logical Disk Usage

```
[PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[diskName]=e:,[ioReadLatency]=0,[ioWriteLatency]=14
```

Rules

- HyperV Disk I/O Warning
- HyperV Disk I/O Critical
- HyperV Guest Critical
- HyperV Guest Hypervisor Run Time Percent Warning
- HyperV Logical Processor Total Run Time Percent Critical
- HyperV Logical Processor Total Run Time Percent Warning
- HyperV Page fault Critical
- HyperV Page fault Warning
- HyperV Remaining Guest Memory Warning

Reports

Look in **RESOURCES > Reports > Device > Server > HyperV**

- HyperV Configuration and Health
- Top HyperV Guests By Virtual Processor Run Time Pct
- Top HyperV Guests by Large Page Size Usage
- Top HyperV Guests by Remote Physical Page Usage
- Top HyperV Root Partitions By Virtual Processor Run Time Pct
- Top HyperV Root Partitions by Large Page Size Usage
- Top HyperV Servers By Logical Processor Run Time Pct
- Top HyperV Servers by Disk Activity
- Top HyperV Servers by Disk Latency
- Top HyperV Servers by Large Page Size Usage

- Top HyperV Servers by Memory Remaining for Guests
- Top HyperV Servers by Remote Physical Page Usage

Configuration

FortiSIEM needs WMI credentials to get the Hyper-V performance metrics. Configure this following the guidelines described in [Microsoft Windows Server Configuration](#).

Settings for Access Credentials

Configure WMI on FortiSIEM.

HyTrust CloudControl

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	Over 70 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "HyTrust-" in the main content panel **Search...** field to see the event types associated with this device or application.

Sample Event Type:

```
<172>Mar 22 03:32:36 htcc136.test.hytrust.com local5: CEF:0|HyTrust|HyTrust
CloudControl|5.0.0.50821|ARC0031|TEMPLATE_OPERATION_ERRORED_ERR|6| rt=Mar 22 2017 03:32:36.196 UTC
act=HostOperation dst=192.168.213.154 src=192.168.213.10 suser=ARC deviceExternalId=6u1b-
esxi2.test.hytrust.com deviceFacility=HostSystem msg=Template operation VH6.0 esxi-check-patch-
version error on host 6u1b-esxi2.test.hytrust.com (192.168.213.154). privilege={}
```

Rules

There are no specific rules but generic rules for Security Manager and Generic Servers apply.

Reports

There are no specific reports but generic rules for Security Manager and Generic Servers apply.

Configuration

Configure HyTrust CloudControl to send syslog on port 514 to FortiSIEM.

KVM

Support Added: FortiSIEM 6.3.1

Last Modification: FortiSIEM 6.3.1

Vendor Version Tested: Not Provided

Vendor: Free Software released under the General Public License (GPL).

Product Information: https://www.linux-kvm.org/page/Main_Page

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Logs](#)

What is Discovered and Monitored

Method	Information discovered	Metrics collected	Logs collected	Used for
syslog	Host name, Reporting IP	None	Virtual Machine monitoring and changes	Security Monitoring

Event Types

- LINUX_Auditd_VIRT_MACHINE_ID
- LINUX_Auditd_VIRT_CONTROL
- LINUX_Auditd_VIRT_RESOURCE

Rules

There are no specific rules.

Reports

There are no specific reports.

Configuration

To configure, take the following steps:

1. Install auditd daemon on linux host. (i.e apt-get install auditd)
2. Edit/etc/audit/auditd.conf and configure as follows (take note of log_format = ENRICHED as this provides the real users behind the UIDs and AUIDs):

Note: This file controls the configuration of the audit daemon.

```
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
```

3. Configure rsyslog to send this logfile via syslog by editing /etc/rsyslog.conf and adding these lines:

Note: This does not need Linux agent.

```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag tag_audit_log:
$InputFileStateFile audit_log
$InputFileSeverity info
```

```
$InputFileFacility local6
$InputRunFileMonitor
*.* @replace.with.fortisiem.collector.IP:514
```

Sample Logs

Sample logs are provided here. For more information on logs, see <https://libvirt.org/auditlog.html>.

```
<182>Jul 26 15:20:36 fsa3000e4 tag_audit_log: type=VIRT_CONTROL msg=audit(1627305635.364:82451):
pid=25686 uid=0 auid=4294967295 ses=4294967295 msg='virt=kvm op=start reason=booted vm="DT_FSR_
Agent" uuid=104735e9-c1ea-44bc-8d99-0fe6fde58b73 vm-pid=25722 exe="/usr/sbin/libvirtd" hostname=?
addr=? terminal=? res=success'UID="root" AUID="unset"
```

```
<182>Jul 26 15:20:36 fsa3000e4 tag_audit_log: type=VIRT_RESOURCE msg=audit(1627305634.788:82437):
pid=25686 uid=0 auid=4294967295 ses=4294967295 msg='virt=kvm resrc=net reason=open vm="DT_FSR_
Agent" uuid=104735e9-c1ea-44bc-8d99-0fe6fde58b73 net=52:54:00:e7:84:3c path="/dev/net/tun"
rdev=0A:C8 exe="/usr/sbin/libvirtd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
```

```
<182>Jul 26 15:20:36 fsa3000e4 tag_audit_log: type=VIRT_MACHINE_ID msg=audit
(1627305634.632:82435): pid=25686 uid=0 auid=4294967295 ses=4294967295 msg='virt=kvm vm="DT_FSR_
Agent" uuid=104735e9-c1ea-44bc-8d99-0fe6fde58b73 vm-ctx=+64055:+64055 img-ctx=+64055:+64055
model=dac exe="/usr/sbin/libvirtd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
```

Nutanix Prism

Support Added: FortiSIEM 6.5.0

Last Modification: FortiSIEM 6.5.0

Vendor Version Tested: Not Provided

Vendor: Nutanix

Product Information: <https://www.nutanix.com/products/prism>

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Sample Log](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		API Audit, Audit, Security Policy Hitlogs, and Flow Service Logs	Security Monitoring

Configuration

To configure syslog monitoring, take the following steps:

For the latest configuration information, see

https://portal.nutanix.com/page/documents/details?targetId=Prism-Central-Guide-Prism-v6_0:mul-syslog-server-configure-pc-t.html

Notes:

- You must have the IP address of the syslog server that is deployed in your environment prior to configuration.
- For forwarding Flow logs, the Flow feature must be enabled.

1. From the main menu, click the gear icon to go to the **Settings** page.
2. From the **Settings** page, click **Syslog Server**.
Note: You can only configure one syslog server per cluster.
3. In the **Server Name** field, enter a name for the server.
4. In the **IP Address** field, enter the IP address.
5. In the **Port** field, enter the port number.
6. From the **Transport Protocol** drop-down list, select TCP or UDP.
7. (Optional) Click the check box to enable Reliable Logging Protocol (RELP).
8. Click **Edit** against **Data Sources**.
9. Select one or more log modules from the following log types. See [Syslog Modules](#) for details.
 - API Audit
 - Audit
 - Security Policy Hitlogs (policy hitlog files logs)
 - Flow Service Logs (flow processes logs)
10. Click **Save** to complete the configuration.

Sample Logs

- [Flow Log](#)
- [Consolidated Audit](#)
- [API Audit](#)

Flow Log

```
<135>2020-06-03T12:12:19.716894+00:00 node-1 flow-hitCount4: INFO:2020/06/03 12:12:18 [dd721468-033f-4368-bdc9-c22a99044421] dt_isolation [Update] SRC=192.0.20.0 DST=192.0.20.10 PROTO=TCP SPORT=22 DPORT=40726 ACTION=DROP ORIG: PKTS=9 BYTES=468 REPLY: PKTS=0 BYTES=0
```

Consolidated Audit

```
<134>2020-06-08T05:27:47.978858-07:00 node-1 consolidated_audit: {"affectedEntityList": [{"entityType":"cluster","name":"Unnamed","uuid":"c6162d80-9d3c-41ba-9928-123456"}], "alertUid":"PairingAudit", "creationTimestampUsecs":"1590479209937393", "defaultMsg":"Failed to pair with remote prism central None: Internal Server Error. Could not create remote connection. Skip pairing", "opEndTimestampUsecs":"1590479209649077", "opStartTimestampUsecs":"1590479209649077", "operationType":"Create", "originatingClusterUuid":"c6162d80-9d3c-41ba-9928-123456", "params":{"remote_cluster_url":""}, "recordType":"Audit", "severity":"Audit", "tenantUuid":"00000000-0000-0000-0000-000000000000", "userName":"perpetuuti-1@nutanixbd.local", "userUuid":"3a8c19be-336d-52f0-bb52-10123456", "uuid":"c47c84ef-2044-4d93-a377-f97706392b93"}
```

API Audit

```
<134>2020-05-29T06:27:22.225134-07:00 node-1 api_audit: INFO 2020-05-29 06:27:13,742 clientType=External||userName=000579e7-ae35-a11d-0000-000000003510||NutanixApiVersion=1.0||httpMethod=GET||restEndpoint=/v1/users/details||entityUuid=||queryParams=||payload=
```

VMware ESX

- [What is Discovered and Monitored](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
VMWare SDK	ESX Server and the Guest hosts running on that server. ESX host clusters. Hardware (CPU, Memory, Disk, network Interface) for all guests, OS vendor and version for all guests. Virtual switch for connecting guest hosts to network interfaces.	Both ESX level and guest host level performance metrics. Guest host level metrics include CPU/memory/disk utilization, CPU Run/Ready/Limited percent, memory swap in/out rate, free memory state, disk read/write rate/latency, network interface utilization, errors, bytes in/out. ESX level metrics include physical CPU utilization, ESX kernel disk read/write latency etc	Performance Monitoring
VMWare SDK		ESX logs include scenarios like ESX level login success/failure, configuration change, Guest host movement, account creation and modification	Availability, Change and Security Monitoring

Configuration

FortiSIEM discovers and monitors VMware ESX servers and guests over the the VMware SDK. Make sure that VMware Tools is installed on all the guests in your ESX deployment, and FortiSIEM will be able to obtain their IP addresses.

Settings for Access Credentials

- [User with System View Credentials](#)
- [Settings for VMware ESX VMSDK Access Credentials](#)

User with System View Credentials

Make sure to provide a user with **System View** permissions who can access the entire vCenter hierarchy when setting up the access credentials for your VMware ESX device. See the VMware documentation on how to set up a user with System View permissions.

Settings for VMware ESX VMSDK Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	VMware ESX Server
Access Protocol	VM SDK
User Name	A user with System View permissions
Password	The password associated with the user

VPN Gateways

FortiSIEM supports these VPN gateways for discovery and monitoring.

- [Cisco VPN 3000 Gateway](#)
- [Cyxtera AppGuard](#)
- [Juniper Networks SSL VPN Gateway](#)
- [Microsoft PPTP VPN Gateway](#)
- [Pulse Secure](#)

Cisco VPN 3000 Gateway

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco_vpn" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog](#)
- [Sample Parsed Cisco VPN 3000 Syslog Message](#)

SNMP

1. Log in to your device with administrative credentials.
2. Go to **Configuration > System > Management Protocols > SNMP Communities**.
3. Click **Add**.

4. For **Community String**, enter public.

Syslog

1. Go to **Configuration > System > Events > Syslog Servers**.
2. Click **Add**.
3. Enter the IP address of your FortiSIEM virtual appliance for Syslog Server.
4. Add a syslog server with FortiSIEM IP Address.

Sample Parsed Cisco VPN 3000 Syslog Message

```
<189>18174 01/07/1999 20:25:27.210 SEV=5 AUTH/31 RPT=14 User [ admin ] Protocol [ Telnet ]  
attempted ADMIN logon. Status: <REFUSED> authentication failure
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco VPN 3K
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cyxtera AppGate

- [Integration Points](#)
- [Event Types](#)
- [Configuring Cyxtera AppGate Software](#)

Integration Points

Protocol	Information Discovered	Used For
Syslog	Access Control log	Security and Compliance

Event Types

Over 70 events are parsed. See event types in **RESOURCES > Event Types** and search for "Cyxtera-AppGate-SDP" in the main content panel **Search...** field.

Configuring Cyxtera AppGate Software

Follow Cyxtera AppGate SDP documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes Cyxtera AppGate syslog, so long as it follows the following format as shown in the sampel syslog:

```
"id":"a51e7e7d-ab5f-444c-b7f8-ca72e4bb940b","timestamp":"2018-10-09T10:23:43.992Z","event_type":"ip_access","version":8,"distinguished_name":"CN=0f1a40d612f741228d7cb73a4308bea8,CN=abc,OU=ACME","entitlement_token_id":"78174080-a34","action":"allow","direction":"down","client_ip":"1.1.1.1","client_port":1392,"packet_size":40,"protocol":"TCP","source_ip":"10.1.1.1","destination_ip":"10.1.1.1","source_port":56100,"destination_port":59721,"connection_type":"established","rule_name":"rule1"
```

Juniper Networks SSL VPN Gateway

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Parsed Juniper Networks SSL VPN Syslog Messages](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "junos_dynamic_vpn" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [Syslog](#)

SNMP

1. Log into your device with administrative credentials.
2. Go to **System > Log/Monitoring > SNMP**.
3. Under **Agent Properties**, enter public for **Community**.

Syslog

- [VPN Access Syslog](#)
- [Admin Access Syslog](#)

VPN Access Syslog

1. Go to **System > Log/Monitoring > User Access > Settings**.
2. Under **Select Events to Log**, select **Login/logout**, **User Settings**, and **Network Connect**.
3. Under **Syslog Servers**, enter the IP address of your FortiSIEM virtual appliance, and set the **Facility** to **LOCAL0**.
4. Click **Save Changes**.

Admin Access Syslog

1. Go to **System > Log/Monitoring > Admin Access > Settings**.
2. Under **Select Events to Log**, select **Administrator changes**, **License Changes**, and **Administrator logins**.
3. Under **Syslog Servers**, enter the IP address of your FortiSIEM virtual appliance, and set the **Facility** to **LOCAL0**.
4. Click **Save Changes**.

Sample Parsed Juniper Networks SSL VPN Syslog Messages

```
<134>Juniper: 2008-10-28 04:34:53 - ive - [192.168.20.82] admin(Users)[] - Login failed using auth
server SteelBelted (Radius Server). Reason: Failed

<134>Juniper: 2008-10-28 03:12:03 - ive - [192.168.20.82] wenyong(Users)[Users] - Login succeeded
for wenyong/Users from 192.168.20.82.

<134>Juniper: 2008-10-28 03:55:20 - ive - [192.168.20.82] wenyong(Users)[Users] - Network Connect:
Session ended for user with IP 172.16.3.240

<134>Juniper: 2008-10-28 03:05:25 - ive - [172.16.3.150] admin(Admin Users)[] - Primary
authentication successful for admin/Administrators from 172.16.3.150

<134>Juniper: 2008-10-28 05:33:02 - ive - [172.16.3.150] admin(Admin Users)[] - Primary
authentication failed for admin/Administrators from 172.16.3.150
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Microsoft PPTP VPN Gateway

- [Configuring Microsoft PPTP](#)
- [Sample Syslog Messages](#)

Configuring Microsoft PPTP

Windows 2003 Server

1. Logon with administrative rights.
2. Configure PPTP VPN.
 - a. Go to Start | All Programs | Administrative Tools | Configure Your Server Wizard, select the Remote Access/VPN Server role. The click the next button which runs the the Routing and Remote Access Wizard.
 - b. On the Routing and Remote Access wizard, follow the following steps:
 - i. Select "Virtual Private Network (VPN) and NAT" and click Next.
 - ii. Select the network interface for use by VPN connection and click Next.
 - iii. Specify the network that VPN clients should connect to in order to access resources and click Next.
 - iv. Select VPN IP Address assignment methodology (DHCP/VPN pool) and click Next.
 - v. Specify VPN pool if VPN pool was chosen in step d and click Next.
 - vi. Identify the network that has shared access to the Internet and click Next.
 - vii. Select if an external RADIUS server is to be used for central authentication and click Next.
 - c. Give users VPN access rights. Open the properties page for a user, select that user's Dial-In properties page and select "Allow access" under Remote Access Permissions.
3. Configure Server Logging - Enable authentication and accounting logging from the **Settings** tab on the properties of the **Local File** object in the **Remote Access Logging** folder in the Routing and Remote Access snap-in. The authentication and accounting information is stored in a configurable log file or files stored in the *SystemRoot\System32\LogFiles* folder. The log files are saved in Internet Authentication Service (IAS) or database-compatible format, meaning that any database program can read the log file directly for analysis.
4. Configure Snare agent to send logs to FortiSIEM.

Sample Syslog Messages

```
<13>Apr  1 09:28:03 dev-v-win03-vc MSPPTPLog      0
```

```
192.168.24.11,administrator,04/01/2009,09:28:00,RAS,DEV-V-WIN03-VC,44,29,4,192.168.24.11,6,2,7,1,5,129,61,5,64,1,65,1,31,192.168.20.38,66,192.168.20.38,4108,192.168.24.11,4147,311,4148,MSRASV5.20,4155,1,4154,Use Windows authentication for all users,4129,DEV-V-
```

```
WIN03-VC\administrator,4130,DEV-V-WIN03-VC\administrator,4127,4,25,311 1 192.168.24.11 04/01/2009  
16:12:12 3,4149,Connections to Microsoft Routing and Remote Access server,4136,1,4142,0
```

Pulse Secure

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Security and Performance alerts	Security and performance monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "PulseSecure" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- [Syslog](#)
- [Sample PulseSecure Syslog Messages](#)

Syslog

Follow the Pulse Secure documentation to send syslog to FortiSIEM.

Sample PulseSecure Syslog Messages

```
<134> 2015-12-18T06:30:29-08:00 PulseSecure: 2015-12-18 06:30:29 - XXX-A1234-VPNSSL01 - [1.1.1.1]
admin(company1 Realm)[some title] - Host Checker policy 'VMS_Host_Checker_Policy' passed on host
'1.1.1.1' address '' for user 'admin'.
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Pulse Secure Pulse Connect
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Vulnerability Scanners

FortiSIEM supports these vulnerability scanners for discovery and monitoring.

- [AlertLogic](#)
- [Digital Defense Frontline Vulnerability Manager](#)
- [Green League WVSS](#)
- [McAfee Vulnerability Manager \(Formerly Foundstone Vulnerability Scanner\)](#)
- [Qualys QualysGuard Scanner](#)
- [Qualys Vulnerability Scanner](#)
- [Rapid7 Nexpose Vulnerability Scanner \(Vulnerability Management On-Premises\)](#)
- [Rapid7 InsightVM \(Platform Based Vulnerability Management\)](#)
- [Tenable.io](#)
- [Tenable Nessus Vulnerability Scanner](#)
- [Tenable Security Center](#)
- [YXLink Vulnerability Scanner](#)

AlertLogic Intrusion Detection and Prevention Systems (IPS)

- Integration Points
- Configuring AlertLogic for FortiSIEM API Access
- Configuring FortiSIEM for AlertLogic API Access

Integration Points

Protocol	Information Discovered	Used For
AlertLogic V3 API	Security Alerts created by AlertLogic	Security and Compliance

Configuring AlertLogic for FortiSIEM API Access

Contact AlertLogic for API access key. This must be entered in FortiSIEM in the next step.

Configuring FortiSIEM for AlertLogic API Access

1. Logon to FortiSIEM
2. Go to **ADMIN > Setup > Credentials**.
3. At **Step 1: Enter Credentials**, click **New** to create AlertLogic API credential:

For Access Protocol = AlertLogic API V3

Setting	Value
Name	<set name>
Device Type	Alert Logic IPS
Access Protocol	AlertLogic API V3
Pull Interval	5 minutes
Password config	See Password Configuration
API Key	The API Key for device access is provided by AlertLogic
Organization	Choose the Organization if it is an MSP deployment and the same credential is to be used for multiple customers

For Access Protocol = AlertLogic IPS

Settings	Description
Name	Enter a name for the credential
Device Type	Alert Logic IPS
Access Protocol	Alert Logic IPS
Pull Interval	The interval in which FortiSIEM will pull events from Alert Logic. Default is 5 minutes.
Access Key ID	Access key for your Alert Logic instance.
Secret Key	Secret key for your Alert Logic instance
Organization	The organization the device belongs to.
Description	Description of the device.

4. At **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter "alertlogic.com" in the **IP/Hostname** field.
 - b. Select the name of the credential created in step 3 from the **Credentials** drop-down list.
 - c. Click **Save**.
5. Select the entry in step 4 and click the **Test** drop-down list and select **Test Connectivity**. If it succeeds, then the credential is correct.
6. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from AlertLogic Cloud service using the AlertLogic V3 API.

To test for events received from AlertLogic:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the AlertLogic entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from AlertLogic in the last 15 minutes. You can modify the time interval to get more events.

Digital Defense Frontline Vulnerability Manager

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Log](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Frontline REST API		Host name, Vulnerability name, Vulnerability CVE ID, Vulnerability score, Operating system	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Digital Defense" to see the event types associated with this device. In FortiSIEM 6.3.0, there are 3 event types defined.

Rules

There are no specific rules available for Digital Defense Frontline Vulnerability Manager, but the rule "Scanner found severe vulnerability" applies.

Reports

There are no specific reports available for Digital Defense Frontline Vulnerability Manager, but the report "Host vulnerabilities found by scanner" can be used.

Configuration

- [Setup in Digital Defense Frontline Vulnerability Manager](#)
- [Setup in FortiSIEM](#)

Setup in Digital Defense Frontline Vulnerability Manager

Complete these steps from the Frontline Vulnerability Manager Portal.

1. Log into [Frontline VM](#).
2. In the site header, select your name and choose **My profile**.
3. On the **API Tokens** tab, select **Create new token**.
4. In the **Add New Token** dialog, enter a token name, and select **OK**. Your token should be created.
5. Below your token name, select **Click to show key** to display your API Key.
6. Copy this information for your Setup in FortiSIEM.

Setup in FortiSIEM

FortiSIEM processes events from the Vulnerability Manager via the Digital Defense API. Obtain your API Key from the Frontline Vulnerability Manager Portal before proceeding.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box, and click **Save** when done.

Settings	Description
Name	Enter a name for the credential.
Device Type	Digital Defense Frontline Vulnerability Manager
Access Protocol	FRONTLINE_API
Pull Interval	5 minutes
Token	Input the API Key from your Digital Defense Frontline Vulnerability Manager API.
Confirm Token	Input the same API Key as above for verification.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Select the name of your credential from the **Credentials** drop-down list. The **IP/Host Name** field should auto populate with "vm.frontline.cloud".
 - b. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Digital Defense Frontline Vulnerability Manager.
5. To see the jobs associated with Digital Defense Frontline Vulnerability Manager, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Frontline" in the search box.

Sample Logs

- [Frontline-Scan-Finished](#)
- [Frontline-Vuln-Detected](#)
- [Frontline-Device-Vuln-Score](#)

Frontline-Scan-Finished

```
{
  "ServerHostName": "vm.frontline.cloud",
  "ServerIp": "54.196.81.232",
  "account": {
    "id": 3516,
    "name": "Fortinet Integration Test",
    "account_id": 3516,
    "account_user": "Dan Hanman",
    "account_user_id": 15006,
    "build_reports": false,
    "businessgroups": {},
    "date_finished": "2021-04-05T23:27:05.004265Z",
    "date_modified": "2021-04-05T23:27:05.146169Z",
    "date_started": "2021-04-05T23:27:03.489965Z",
    "deleting": false,
    "description": "",
    "exclude_from_active_view": false,
    "force_target_detection": false,
    "has_results": false,
    "host_count": 0,
    "id": "298183_20210405T232500Z",
    "is_rna_scan": true,
    "name": "Scan Mar 25, 2021 1:25PM",
    "next_event": null,
    "phCustId": 1,
    "scan_locations": "internal",
    "scan_policy": "Default",
    "status": "completed",
    "status_message": null,
    "status_name": "Completed",
    "workflow": "va_workflow"
  }
}
```

Frontline-Vuln-Detected

```
{
  "ServerHostName": "vm.frontline.cloud",
  "ServerIp": "54.196.81.232",
  "acceptable_risk": null,
  "active_view_active_risk_details": null,
  "active_view_active_risk_score": null,
  "active_view_date_created": null,
  "active_view_date_first_created": null,
  "active_view_threat_rank": null,
  "analyst_threat_intel": null,
  "cve": "",
  "cvss_base_score_v2": 0.0,
  "cvss_base_score_v3": null,
  "cvss_score": "0.0",
  "cvss_version": "2.0",
  "data": "Wordpress 4.0.6 detected",
  "date_finished": null,
  "date_started": null,
  "detect_type": "remote",
  "exploitability": {
    "exploited_in_wild": null,
    "has_exploit_func": false,
    "has_exploit_kit": null,
    "has_exploit_poc": null,
    "is_crimewareable": null,
    "is_exploitable": null,
    "is_priority_exploitable": null
  },
  "false_positive": false,
  "has_notes": false,
  "hidden": false,
  "hide_from_now_on": false,
  "host_hidden": false,
  "host_id": 85634681,
  "hostname": "172.23.177.67",
  "id": 3202200906,
  "id_ddi": 102095,
  "ip_address": "172.23.177.67",
  "labels": [],
  "manually_added": false,
  "manually_added_date_fix_confirmed": null,
  "manually_added_fix_status_name": null,
  "matched_status": "new",
  "phCustId": 1,
  "port": 80,
  "protocol": "http",
  "scan_block_id": "548616",
  "scan_id": "277898",
  "scan_version": 1016281,
  "scan_version_active_risk_details": null,
  "scan_version_active_risk_score": null,
  "scan_version_date_created": "2020-12-02T17:46:12.640112Z",
  "scan_version_host_id": 85634681,
  "scan_version_threat_rank": null,
  "scan_version_vulnerability_id": 3202200906,
  "scanner_version": "3.0.26.2",
  "severities": {
    "ddi": "info",
    "ddi_alt": "trivial",
    "nvd": "low",
    "nvd_alt": "low",
    "pci": "pass",
    "pci_alt": "pass"
  },
  "threat_activity": {
    "1m": 0,
    "1w": 0,
    "1y": 0,
    "3m": 0,
    "total": 0
  },
  "title": "Wordpress Detected",
  "transport": "tcp",
  "tunnel": "none",
  "vuln_class": "explicit"
}
```

Frontline-Device-Vuln-Score

```
{
  "ServerHostName": "vm.frontline.cloud",
  "ServerIp": "54.196.81.232",
  "active_view_active_risk_details": {
    "ars_unweighted": 92.02499999999999,
    "exposure_score": {
      "domain": "WIN-30QQR10MG",
      "domain_host_count": 4,
      "domain_threat_rank": 95.0,
      "external_asset": false,
      "subnet": null,
      "subnet_host_count": 0,
      "subnet_threat_rank": 0,
      "unweighted": 68.5,
      "weight": 0.05000000000000003,
      "weighted": 3.4250000000000003
    },
    "risk_weight": {
      "host_risk_weight": 50.0
    },
    "severity_score": {
      "unweighted": 84,
      "weight": 0.14999999999999999,
      "weighted": 12.6
    },
    "threat_score": {
      "unweighted": 95.0,
      "weight": 0.8000000000000004,
      "weighted": 76.0
    }
  },
  "active_view_cvss_version": 2.0,
  "active_view_date_created": "2020-12-02T17:46:12.640112Z",
  "active_view_date_first_created": "2020-12-02T17:46:12.640112Z",
  "agent_uuid": null,
  "assessed_cis_auth": false,
  "assessed_db_auth": false,
  "assessed_os_auth": false,
  "assessed_threatscan_auth": true,
  "assessed_unauth": true,
  "auth_status": {
    "details": {},
    "extended_details": {
      "cis": null,
      "db": null
    }
  }
}
```

```

{"mssql":null,"mysql":null,"oracle":null,"postgresql":null},"os":
{"linux":null,"vmware":null,"windows":null},"threatscan":"Threat Scan completed
successfully"},"overall":"N/A"},"aws_instance_id":null,"base_scan_id":"277898","date_
finished":null,"date_started":null,"discovery_method":"nbname","dns_name":"","dns_smartname":"WIN-
30QQR10MGG","has_antivirus":true,"has_crimewareable":null,"has_disabled_antivirus":false,"has_
exploitable":null,"has_malware":false,"has_notes":false,"has_outdated_
antivirus":false,"hidden":false,"hide_from_now_on":false,"hostname":"WIN-
30QQR10MGG","id":85634671,"internal":true,"ip_address":"172.23.177.55","is_
compromised":false,"is_retired":false,"labels":[{"color":"blue","deleted":false,"display_
name":"WIN-30QQR10MGG","id":214189,"labeled_by":0,"location":1}],"mac_
address":"00:50:56:8d:16:52","matched_status":"new","named_asset_name":null,"netbios_name":"WIN-
30QQR10MGG","netbios_smartname":"WIN-30QQR10MGG","network_profile_id":7286,"network_profile_
name":"Internal Scanner Profile","notes_distribution":{"asset":false,"asset_only":false,"vuln_
only":false},"os":"Windows Server 2012 R2 Standard","os_family":"windows","os_
type":"server","partially_scanned":false,"pentest_status":null,"phCustId":1,"scan_block_
id":"548616","scan_id":"277898","scan_version":1016281,"scan_version_active":true,"scan_version_
active_risk_details":{"ars_unweighted":92.024999999999991,"exposure_score":{"domain":"WIN-
30QQR10MGG","domain_host_count":4,"domain_threat_rank":95.0,"external_
asset":false,"subnet":null,"subnet_host_count":0,"subnet_threat_
rank":0,"unweighted":68.5,"weight":0.050000000000000003,"weighted":3.4250000000000003},"risk_
weight":{"host_risk_weight":50.0},"severity_score":
{"unweighted":84,"weight":0.14999999999999999,"weighted":12.6},"threat_score":
{"unweighted":95.0,"weight":0.800000000000000004,"weighted":76.0}},{"scan_version_active_risk_
score":92.0250000000000006,"scan_version_cvss_score":10.0,"scan_version_cvss_version":2.0,"scan_
version_date_created":"2020-12-02T17:46:12.640112Z","scan_version_host_id":85634671,"scan_version_
host_rating_list":{"ddi":"D","ddi_alt":"F","nvd":"High","nvd_alt":"High","pci":"Fail","pci_
alt":"Fail"},"scan_version_host_severity_list":{"ddi":"high","nvd":"high","pci":"fail"},"scan_
version_risk_score":175.0,"scan_version_risk_weight":50.0,"scan_version_threat_rank":95.0,"scan_
version_vulnerability_count":29,"scan_version_vulnerability_severity_counts":{"unweighted":{"ddi":
{"counts":{"critical":0,"high":1,"info":21,"low":0,"medium":1,"none":0,"trivial":6},"overall_
security_gpa":1.0},"ddi_alt":{"counts":
{"critical":1,"high":1,"info":0,"low":1,"medium":0,"none":0,"trivial":26},"overall_security_
gpa":0},"nvd":{"counts":{"high":2,"low":24,"medium":3},"overall_security_gpa":0},"nvd_alt":
{"counts":{"high":1,"low":27,"medium":1},"overall_security_gpa":0},"pci":{"counts":
{"fail":2,"pass":27},"overall_security_gpa":0},"pci_alt":{"counts":{"fail":2,"pass":27},"overall_
security_gpa":0}},{"weighted":{"ddi":{"counts":
{"critical":0,"high":1,"info":21,"low":0,"medium":1,"none":0,"trivial":6},"overall_security_
gpa":1.0},"ddi_alt":{"counts":
{"critical":1,"high":1,"info":0,"low":1,"medium":0,"none":0,"trivial":26},"overall_security_
gpa":0},"nvd":{"counts":{"high":2,"low":24,"medium":3},"overall_security_gpa":0},"nvd_alt":
{"counts":{"high":1,"low":27,"medium":1},"overall_security_gpa":0},"pci":{"counts":
{"fail":2,"pass":27},"overall_security_gpa":0},"pci_alt":{"counts":{"fail":2,"pass":27},"overall_
security_gpa":0}}},"scanner_version":"3.0.26.2"}

```


Green League WVSS

- [Configuration in FortiSIEM](#)

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Green League WVSS
Access Protocol	WVSS API
Pull Interval	60 minutes
Domain	Domain name
User Name	User name for device access
Password	Password for device access
Description	Description of the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Green League WVSS.
5. To see the jobs associated with Green League, navigate to **ADMIN > Setup > Pull Events**. To see the received events, navigate to **ANALYTICS**, then enter "Green League" in the search box.

McAfee Foundstone Vulnerability Scanner

Formerly Foundstone Vulnerability Scanner

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Metrics collected	Used for
JDBC (SQL Server)	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id, Vulnerability Score, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "mcafee-vul" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined rules for this device.

Configuration

JDBC

FortiSIEM connects to the faultline database in the McAfee vulnerability scanner to collect metrics. This is a SQL Server database, so you must have set up access credentials for the database over JDBC to set up access credentials in FortiSIEM and initiate discovery.

Settings for Access Credentials

Settings for McAfee Foundstone Vulnerability Scanner JDBC Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	mcafee_jdbc
Device Type	Microsoft SQL Server
Access Protocol	JDBC
Used for	McAfee VulnMgr
Pull Interval (minutes)	5
Port	1433
Database name	faultline
User Name	A user with access to the faultline database over JDBC
Password	The password associated with the user

Qualys QualysGuard Scanner

- Configuration in FortiSIEM

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Qualys QualysGuard Scanner
Access Protocol	Qualys API
Pull Interval	60 minutes
Port	443
User Name	A user who has access to the vulnerability scanner over the API.
Password	Password associated with the user
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Qualys QualysGuard Scanner.
5. To see the jobs associated with Qualys, select **ADMIN > Setup > Pull Events**.
6. To see the received events, select **ANALYTICS**, then enter "Qualys" in the search box.

Qualys Vulnerability Scanner

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Metrics collected	Used for
Qualys API	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "qualys" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "qualys" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Qualys API

Create a user name and password that FortiSIEM can use as access credentials for the API.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. . For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Use Host Name for IP Range in Access Credentials

Enter the host name for your Qualys service rather than an IP address when associating your access credentials to an IP range.

Settings for Qualys Vulnerability Scanner API Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	qualys
Device Type	Qualys QualysGuard Scanner
Access Protocol	Qualys API
Pull Interval (minutes)	5
Port	443
User Name	A user who has access to the vulnerability scanner over the API
Password	The password associated with the user

Rapid7 Nexpose Vulnerability Scanner (Vulnerability Management On-Premises)

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Metrics collected	Used for
Rapid7 Nexpose API	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "rapid7" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Rapid7 Nexpose API

1. Log into the device manager for your vulnerability scanner with administrative credentials.
2. Go to **Administration > General > User Configuration**, and create a user that FortiSIEM can use to access the device.
3. Go to **Reports > General > Report Configuration**.

4. Create a report with the Report Format set to **Simple XML Report Version 1.0** or **NeXpose XML Report Version 2.0**.

FortiSIEM can pull reports only in these formats.

Settings for Access Credentials

Settings for Rapid7 Nexpose API Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Rapid7 NeXpose Security Scanner
Access Protocol	Rapid7 NeXpose API
Pull Interval (minutes)	60
Port	3780
User Name	A user who can access the device over the API
Password	The password associated with the user

Rapid7 InsightVM (Platform Based Vulnerability Management)

- [Integration Points](#)
- [Rapid7 InsightVM API Integration](#)
- [Configuration](#)

Integration Points

Protocol	Information collected	Used For
InsightVM API	Vulnerability scan data	Security and Compliance

Rapid7 InsightVM API Integration

FortiSIEM can pull vulnerability scan data from Rapid7 InsightVM Server via InsightVM API.

InsightVM scan data contains vulnerabilities found on a host. Each host vulnerability is converted into a separate FortiSIEM event with event type Rapid7-InsightVM-Vuln-Detected.

Configuration

- [Configuring Rapid7 InsightVM Server](#)
- [Configuring FortiSIEM](#)

Configuring Rapid7 InsightVM Server

Create an account to be used for FortiSIEM communication.

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access:

Define Rapid7 Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**.

Settings	Description
Name	Enter a name for the credential
Device Type	Rapid7 InsightVM

Settings	Description
Access Protocol	InsightVM API
Pull Interval	Choose the Pull Interval (Default 60 minutes). Fortinet recommends 5 minutes for general cases.
Port	Choose the HTTPS Port (default 3780).
User Name	Enter the User Name for the account created while Configuring Rapid7 InsightVM Server .
Password	Enter the Password for the account created while Configuring Rapid7 InsightVM Server .
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

- In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - Enter the IP address of the Rapid7 Insight VM Server in the **IP/Host Name** field.
 - Select the name of the credential created in [Define Rapid7 Credential in FortiSIEM](#) from the **Credentials** drop-down list.
 - Click **Save**.
- 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.
- Go to **ADMIN > Setup > Discovery**, click **New**, fill out the information and ensure you input the IP address used in Step 1a, and click **Save**.
- Click **Discover** and confirm it succeeds.
- An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Rapid7 InsightVM Server using the InsightVM REST API.

To test for received InsightVM Vulnerability events:

- Go to **ADMIN > Setup > Pull Events**.
- Select the InsightVM entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from InsightVM Server in the last 15 minutes. You can modify the time interval to get more events.

Tenable.io

- [Integration Points](#)
- [Tenable.io API Integration](#)
- [Configuration](#)

Integration Points

Protocol	Logs Collected	Used For
Tenable.io API	Vulnerability scan data	Security and Compliance

Tenable.io API Integration

FortiSIEM can pull vulnerability scan data from Tenable.io Cloud Service via Tenable.io API.

Tenable.io scan data contains vulnerabilities found on a host. Each host vulnerability is converted into a separate FortiSIEM event with event type TenableIO-Vuln-Detected.

Configuration

- [Configuring Tenable.io Cloud Service](#)
- [Configuring FortiSIEM](#)

Configuring Tenable.io Cloud Service

Create an API Key to be used for FortiSIEM communication.

1. Login to your Tenable.io portal using your account.
2. Create API Key for use in FortiSIEM:
 - a. For administrative user.
 - b. Click **Settings > User**.
 - c. In **User** table, click the name of the **User** you want to edit.
 - d. Click the **API Keys** tab in the generate and click **Generate**.
 - e. Click **Save**.
3. For regular user:
 - a. Click **My Account**.
 - b. Click the **API Keys** tab in the generate and click **Generate**.
 - c. Click **Save**.

Configuring FortiSIEM

Define Tenable.io Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Tenable Tenable.io
Access Protocol	TenableIO API
Pull Interval	Choose the Pull Interval (Default 60 minutes). Fortinet recommends 5 minutes for general cases.
Account	Enter the Account obtained from Tenable.io portal (see Configuring Tenable.io Cloud Service).
Access Key	Enter the Access Key obtained from Tenable.io portal (see Configuring Tenable.io Cloud Service).
Secret Key	Enter the Secret Key obtained from Tenable.io portal (see Configuring Tenable.io Cloud Service).
Organization	Choose the Organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter "cloud.tenable.com" in the **IP/Host Name** field.
 - b. Select the name of the credential created in [Define Tenable.io Credential in FortiSIEM](#) from the **Credentials** drop-down list.
 - c. Click **Save**.
2. 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. After **Test Connectivity** succeeds, an entry

will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Tenable.io portal using the API.

To test for received Tenable.io events:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the Tenable.io entry and click **Report**.
3. The system will take you to the **ANALYTICS** tab and run a query to display the events received from Tenable.io in the last 15 minutes. You can modify the time interval to get more events.

Tenable Nessus Vulnerability Scanner

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Metrics collected	Used for
Nessus API	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "nessus" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "nessus" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

To configure a Tenable Nessus Security Scanner, take the following steps:

1. Deploy a Nessus server (5, 6, 7, 8 or 10).
2. Generate an API key. For Nessus 7, Nessus 8, or Nessus 10, obtain the Access Key and Secret Key.
Note: If using Nessus (5) or Nessus 6, create a username and password that FortiSIEM can use to access the API and make sure the user has permissions to view the scan report files on the Nessus device. You can check if your user has the right permissions by running a scan report as that user.
3. Add a target device IP that will be scanned.

4. Login to the FortiSIEM GUI.
5. Navigate to **CMDB > Devices**.
6. Add the target device IP to **CMDB > Devices** in FortiSIEM.
7. Navigate to **ADMIN > Setup**, and click the **Credentials** tab.
8. In **Step 1: Enter Credentials**, click **New**:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these Nessus credential settings in the Access Method Definition dialog box and click **Save**:

Setting	Value
Name	<set name>
Device Type	Choose the appropriate device type: -Tenable Nessus Security Scanner -Tenable Nessus6 Security Scanner -Tenable Nessus7 Security Scanner -Tenable Nessus8 Security Scanner -Tenable Nessus10 Security Scanner
Access Protocol	The access protocol will auto populate based off the device type selected: -Nessus API -Nessus6 API -Nessus7 API -Nessus8 API -Nessus10 API
Pull Interval (minutes)	5 (default 60 minutes)
Port	8834
User Name (for Nessus and 6)	A user who has permission to access the device over the API
Password (for Nessus and 6)	The password associated with the user
Access Key (for Nessus7 and 8)	Obtain the Access Key from Nessus
Secret Key (for Nessus7 and 8)	Obtain the Secret Key from Nessus

9. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
 - a. Select the credential you created earlier from the **Credentials** drop-down list.
 - b. In the **IP/Host Name** field, enter the IP/IP Range or Host Name.
 - c. Click **Save**.
10. Select the new mapping and click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling.
11. Navigate to **ADMIN > Setup > Pull Events**. The yellow star besides the Nessus pull job should turn the color green.

12. Scan the target device IP in the Nessus server, and export the scan report.
13. Navigate to **ANALYTICS** in FortiSIEM, and query the Nessus events with the condition Event Type = Nessus-Vuln-Detected.
14. Compare the events in the FortiSIEM with the scan report exported from the Nessus server.

Note that the severity matching rule between Nessus8 and AO Event are as follows:

Nessus Status	FortiSIEM Event Severity Number
Critical	Event Severity 10
High	Event Severity 9
Medium	Event Severity 6
Low	Event Severity 2
None	Event Severity 3

If Vulnerability CVE ID in FortiSIEM events is not NULL, the target device IP will be added to **INCIDENTS > Risk** in FortiSIEM.

Tenable Security Center

- [Integration Points](#)
- [Tenable.sc \(Security Center\) API Integration](#)
- [Configuration](#)
- [Sample Events](#)

Integration Points

Protocol	Information collected	Used for
Tenable.sc API	Vulnerability scan data	Security and Compliance

Tenable.sc (Security Center) API Integration

FortiSIEM can pull vulnerability scan data via the Tenable.sc API.

Tenable.sc scan data contains vulnerabilities found on a host. Each host vulnerability is converted into a separate FortiSIEM event with event type TenableSC-Vuln-Detected.

Configuration

- [Configuring Tenable.sc for FortiSIEM](#)
- [Configuring FortiSIEM](#)

Configuring Tenable.sc for FortiSIEM

Except for setting your Tenable account user name and password, no special configuration is needed for Tenable.sc.

Configuring FortiSIEM

Use the API Key and Secret in the previous step to enable FortiSIEM access.

- [Define Tenable Security Center Credential in FortiSIEM](#)
- [Create IP Range to Credential Association, Test Connectivity and Pull Events](#)

Define Tenable Security Center Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential:
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Tenable Tenable Security Center
Access Protocol	Tenable.sc API
Pull Interval	Choose the Pull Interval (Default 60 minutes).
Port	Enter the Port number. (Default 443)
User Name	Enter the User Name for the Tenable Security Center account.
Password	Enter the Password for the Tenable Security Center user name account.
Description	Description of the device.

Create IP Range to Credential Association, Test Connectivity and Pull Events

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter the host's IP address or host name in the **IP/Host Name** field.
 - b. Select the name of the credential created in [Define Tenable Security Center Credential in FortiSIEM](#) from the **Credentials** drop-down list.
 - c. Click **Save**.
2. 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.
3. After **Test Connectivity** succeeds, an entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Tenable Security Center using the API.

To test for received Tenable.sc events:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the Tenable.sc entry and click **Report**.
3. The system will take you to the **ANALYTICS** tab and run a query to display the events received from Tenable.sc in the last 15 minutes. You can modify the time interval to get more events.

Sample Events

```
[TenableSc-Vuln-Detected]:[serverIp]=10.10.10.79,[serverName]=sc.tenalab.online,
[scanName]=tensc_job1__ordr_1580449845796,[endTime]=1580538767,[policyName]=6e8a5582-076f-5798-
```

```
b0c3-5384b8854cad-501013/Advanced Scan (Vulnerability),[osName]=linux,
[hostMACAddr]=00:16:3E:5D:7A:71,[osVersion]=Linux Kernel 2.6,[hostName]=target-cent7.lxd,
[hostIpAddr]=10.238.64.9,[startTime]=1580538643,[appPort]=22,[appTransportProto]=tcp,
[eventSeverity]=1,[nessusPluginId]=70658,[nessusPluginName]=SSH Server CBC Mode Ciphers
Enabled,[categoryType]=Misc.,[vulnCVEId]=CVE-2008-5161,[vulnCvssBaseScore]=2.6,
[vulnCvssBaseTemporal]=1.9,[cweId]=200,[vulnDesc]=The SSH server is configured to support
Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext
message from the ciphertext. Note that this plugin only checks for the options of the SSH
server and does not check for vulnerable software versions.,[fileName]=ssh_cbc_supported_
ciphers.nasl,[vulnType]=remote,[threatLevel]=Low,[vulnSolution]=Contact the vendor or consult
product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode
encryption.,[vulnCVESummary]=The SSH server is configured to use Cipher Block Chaining.,
[nessusPluginOutput]= The following client-to-server Cipher Block Chaining (CBC) algorithms are
supported : 3des-cbc aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc The following
server-to-client Cipher Block Chaining (CBC) algorithms are supported : 3des-cbc aes128-cbc
aes192-cbc aes256-cbc blowfish-cbc cast128-cbc

[TenableSc-Vuln-Detected]:[serverIp]=52.170.35.79,[serverName]=sc.tenalab.online,
[scanName]=tensc_job1__ordr_1580449845796,[endTime]=1580538767,[policyName]=6e8a5582-076f-5798-
b0c3-5384b8854cad-501013/Advanced Scan (Vulnerability),[osName]=linux,
[hostMACAddr]=00:16:3E:5D:7A:71,[osVersion]=Linux Kernel 2.6,[hostName]=target-cent7.lxd,
[hostIpAddr]=10.238.64.9,[startTime]=1580538643,[appPort]=0,[appTransportProto]=tcp,
[eventSeverity]=0,[nessusPluginId]=35081,[nessusPluginName]=Xen Guest Detection,
[categoryType]=Misc.,[vulnDesc]=According to the MAC address of its network adapter, the remote
host is a Xen virtual machine.,[fileName]=xen_detect.nasl,[vulnType]=combined,
[threatLevel]=None,[vulnSolution]=Ensure that the host's configuration is in agreement with
your organization's security policy.,[vulnCVESummary]=The remote host is a Xen virtual machine.
```

YXLink Vulnerability Scanner

- [Configuration in FortiSIEM](#)

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	YXLink Vuln Scanner
Access Protocol	YX API
Pull Interval	60 minutes
Port	0
Domain	Domain name
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the YXLink Vulnerability Scanner.
5. To see the jobs associated with YXLink, select **ADMIN > Setup > Pull Events**.
6. To see the received events, select **ANALYTICS**, then enter "YXLink" in the search box.

WAN Accelerators

FortiSIEM supports these wide area network accelerators for discovery and monitoring.

- [Cisco Wide Area Application Server](#)
- [Riverbed SteelHead WAN Accelerator](#)

Cisco Wide Area Application Server

- What is Discovered and Monitored on page 1138
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Software version, Hardware model, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Disk space utilization, Process cpu/memory utilization	Availability and Performance Monitoring

Event Types

Regular monitoring events

- PH_DEV_MON_SYS_UPTIME

```
[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=1053,  
[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,[sysUpTime]=13256948,  
[sysUpTimePct]=100.000000,[sysDownTime]=0,[pollIntv]=56,[phLogDetail]=
```

- PH_DEV_MON_SYS_CPU_UTIL

```
[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=1053,  
[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,[sysUpTime]=13256948,  
[sysUpTimePct]=100.000000,[sysDownTime]=0,[pollIntv]=56,[phLogDetail]=
```

- PH_DEV_MON_SYS_MEM_UTIL

```
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=9822,  
[memName]=Physical Memory,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,[memUtil]=93.438328,  
[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_SYS_DISK_UTIL

```
[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,  
[lineNumber]=9902,[diskName]=/swstore,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,
```

```
[appTransportProto]=SNMP (hrStorage),[diskUtil]=56.931633,[totalDiskMB]=992,[usedDiskMB]=565,
[freeDiskMB]=427,[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_SYS_PROC_COUNT

```
[PH_DEV_MON_SYS_PROC_COUNT]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=11710,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,[procCount]=429,
[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_NET_INTF_UTIL

```
[PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phIntfFilter.cpp,
[lineNumber]=323,[intfName]=GigabitEthernet 1/0,[intfAlias]=,[hostName]=edge.bank.com,
[hostIpAddr]=10.19.1.5,[pollIntv]=56,[recvBytes64]=0,[recvBitsPerSec]=0.000000,
[inIntfUtil]=0.000000,[sentBytes64]=0,[sentBitsPerSec]=0.000000,[outIntfUtil]=0.000000,
[recvPkts64]=0,[sentPkts64]=0,[inIntfPktErr]=0,[inIntfPktErrPct]=0.000000,[outIntfPktErr]=0,
[outIntfPktErrPct]=0.000000,[inIntfPktDiscarded]=0,[inIntfPktDiscardedPct]=0.000000,
[outIntfPktDiscarded]=0,[outIntfPktDiscardedPct]=0.000000,[outQLen64]=0,
[intfInSpeed64]=100000000,[intfOutSpeed64]=100000000,[intfAdminStatus]=,[intfOperStatus]=,
[daysSinceLastUse]=0,[totIntfPktErr]=0,[totBitsPerSec]=0.000000,[phLogDetail]=
```

- PH_DEV_MON_PROC_RESOURCE_UTIL

```
[PH_DEV_MON_PROC_RESOURCE_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=4320,[swProcName]=syslogd,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,
[procOwner]=,[memUtil]=0.038191,[cpuUtil]=0.000000,[appName]=Syslog Server,[appGroupName]=Unix
Syslog Server,[pollIntv]=116,[swParam]=-s -f /etc/syslog.conf-diamond,[phLogDetail]=
```

Rules

Regular monitoring rules

Reports

Regular monitoring reports

Configuration

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco WAAS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Riverbed SteelHead WAN Accelerator

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Software version, Hardware model, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Disk space utilization, Process cpu/memory utilization	Availability and Performance Monitoring
SNMP		Hardware status	Availability and Performance Monitoring
SNMP		Bandwidth metrics: Inbound Optimized Bytes - LAN side, WAN side, Outbound optimized bytes - LAN side and WAN side Connection metrics: Optimized connections, Passthrough connections, Half-open optimized connections, Half-closed Optimized connections, Established optimized connections, Active optimized connections Top Usage metrics: Top source (Source IP, Total Bytes), Top destination (Destination IP, Total Bytes), Top Application (TCP/UDP port, Total Bytes), Top Talker (Source IP, Source Port, Destination IP, Destination Port, Total Bytes) Peer status: For every peer: State, Connection failures, Request timeouts, Max latency	Availability and Performance Monitoring
SNMP Trap		All traps: software errors, hardware errors, admin login, performance issues - cpu, memory, peer latency issues. About 115 traps defined in ADMIN > Device Support > Event. The mapped event types start with "Riverbed-".	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "steelhead" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "steelhead" in the main content panel **Search...** field to see the rules associated with this device.

Reports

There are no predefined reports for this device.

Configuration

- [SNMP](#)
- [SNMP Trap](#)

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "[Discovery Settings](#)" and "[Setting Credentials](#)" in the [User Guide](#).

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Riverbed Steelhead
Access Protocol	See Access Credentials
Port	See Access Credentials

Setting	Value
Password config	See Password Configuration

Wireless LANs

FortiSIEM supports these wireless local area network devices for discovery and monitoring.

- [Aruba Networks Wireless LAN](#)
- [Cisco Wireless LAN](#)
- [CradlePoint](#)
- [FortiAP](#)
- [FortiWLC](#)
- [Motorola WiNG WLAN AP](#)
- [Ruckus Wireless LAN](#)
- [Ubiquiti Wireless LAN](#)

Aruba Networks Wireless LAN

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

FortiSIEM uses SNMP and NMAP to discover the device and to collect logs and performance metrics. FortiSIEM communicates to the WLAN Controller only and discovers all information from the Controller. FortiSIEM does not communicate to the WLAN Access points directly.

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller host name, Controller hardware model, Controller network interfaces, Associated WLAN Access Points	Controller Uptime, Controller Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Radio interface performance metrics	Availability and Performance Monitoring
SNMP Trap	Controller device type	All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "aruba" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "aruba" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP V1/V2c

1. Log in to your Aruba wireless controller with administrative privileges.
2. Go to **Configuration > Management > SNMP**.
3. For **Read Community String**, enter `public`.
4. Select **Enable Trap Generation**.
5. Next to **Read Community String**, click **Add**.
6. Under **Trap Receivers**, click **Add** and enter the IP address of your FortiSIEM virtual appliance.

Sample Aruba Networks Wireless LAN Controller SNMP Trap Messages

```
2008-06-11 11:38:34 192.168.20.7 [192.168.20.7]:SNMPv2-MIB::sysUpTime.0 = Timeticks:
(1355400) 3:45:54.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.14823.2.2.1.1.100.1003 SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.60 =
Hex-STRING: 07 D8 06 0B 13 2E 39 00 2D 07 00 SNMPv2-
SMI::enterprises.14823.2.2.1.1.2.1.1.2.192.168.180.1 = Hex-STRING: 00 1E 52 72 AF 4B
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Aruba ArubaOS WLAN AP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco Wireless LAN

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller host name, Controller hardware model, Controller network interfaces, Associated WLAN Access Points	Controller Uptime, Controller CPU and Memory utilization, Controller Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP Trap	Controller device type	All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco wireless" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP V1/V2c and SNMP Traps

1. Log in to your Cisco wireless LAN controller with administrative privileges.
2. Go to **MANAGEMENT > SNMP > General**.
3. Set both **SNMP v1 Mode** and **SNMP v2c Mode** to **Enable**.
4. Go to **SNMP > Communities**.
5. Click **New** and create a public community string with **Read-Only** privileges.
6. Click **Apply**.
7. Go to **SNMP > Trap Controls**.
8. Select the event traps you want to sent to FortiSIEM.
9. Click **Apply**.
10. Go to **SNMP > Trap Receivers**.
11. Click **New** and enter the IP address of your FortiSIEM virtual appliance as a trap receiver.
12. Click **Apply**.

Sample SNMP Trap

```
2008-06-09 08:59:50 192.168.20.9 [192.168.20.9]:SNMPv2-MIB::sysUpTime.0 = Timeticks: (86919800) 10
days, 1:26:38.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.14179.2.6.3.2
SNMPv2-SMI::enterprises.14179.2.6.2.35.0 = Hex-STRING: 00 21 55 4D 66 B0 SNMPv2-
SMI::enterprises.14179.2.6.2.36.0 = INTEGER: 0 SNMPv2-SMI::enterprises.14179.2.6.2.37.0 =
INTEGER: 1 SNMPv2-SMI::enterprises.14179.2.6.2.34.0 = Hex-STRING: 00 12 F0 0A 3F 15
```

```
2010-11-01 12:59:57 0.0.0.0(via UDP: [172.22.2.25]:32769) TRAP2, SNMP v2c, community 1n3t3ng .
Cold Start Trap (0) Uptime: 0:00:00.00 DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (9165100)
1 day, 1:27:31.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.9.9.599.0.4 SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.1.0 = Hex-STRING: 00 24 D7 36 A0 00 SNMPv2-
SMI::enterprises.9.9.513.1.1.1.1.5.0 = STRING: "AP-2" SNMPv2-SMI::enterprises.9.9.599.1.3.1.1.8.0
= Hex-STRING: 00 25 45 B7 66 70 SNMPv2-SMI::enterprises.9.9.513.1.2.1.1.1.0 = INTEGER: 0 SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.10.0 = IPAddress: 172.22.4.54 SNMPv2-
SMI::enterprises.9.9.599.1.2.1.0 = STRING: "IE\browse" SNMPv2-SMI::enterprises.9.9.599.1.2.2.0 =
STRING: "IE"2011-04-05 10:37:42 0.0.0.0(via UDP: [10.10.81.240]:32768) TRAP2, SNMP v2c, community
FortiSIEM . Cold Start Trap (0) Uptime: 0:00:00.00 DISMAN-EVENT-MIB::sysUpTimeInstance =
Timeticks: (1672429600) 193 days, 13:38:16.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.9.9.615.0.1 SNMPv2-SMI::enterprises.9.9.599.1.3.1.1.1.0 = Hex-STRING: 00 25 BC 80
E8 77 SNMPv2-SMI::enterprises.9.9.599.1.3.1.1.8.0 = Hex-STRING: 6C 50 4D 7D AC 50 SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.9.0 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.513.1.1.1.1.5.0 =
STRING: "AP03-3.rdu2" SNMPv2-SMI::enterprises.9.9.615.1.2.1.0 = INTEGER: 1 SNMPv2-
SMI::enterprises.9.9.615.1.2.2.0 = INTEGER: 5000 SNMPv2-SMI::enterprises.9.9.615.1.2.3.0 =
INTEGER: 1 SNMPv2-SMI::enterprises.9.9.615.1.2.4.0 = INTEGER: 31 SNMPv2-
SMI::enterprises.9.9.615.1.2.5.0 = INTEGER: -60 SNMPv2-SMI::enterprises.9.9.615.1.2.6.0 = INTEGER:
-90 SNMPv2-SMI::enterprises.9.9.615.1.2.7.0 = STRING:
```


[illegible]

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

CradlePoint

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "CradlePoint" to see the event types associated with this application or device.

Rules

No specific rules are written for CradlePoint, but generic rules for Firewall, VPN Gateway, WLAN AP, Router Switch apply where there are matching event types.

Reports

No specific reports are written for CradlePoint, but generic reports for Firewall, VPN Gateway, WLAN AP, Router Switch apply where there are matching event types.

Configuration

Configure syslog forwarding of event information from CradlePoint.

Settings for Access Credentials

None required.

Sample Events

<14>(host) dhcp: Updated DHCP client: hostname 10.4.42.222 58:94:6b:8d:2b:94

FortiAP

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Sample Events](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (to FortiGate)	Access point – Name, OS, Interfaces, Controller (FortiGate)	FortiAP CPU, Memory, Clients, Sent/Received traffic	Performance and Availability Monitoring
Syslog (from FortiGate)	Wireless events		Security and Log Analysis

FortiAPs are discovered from FortiGate firewalls via SNMP. FortiAP logs are received via FortiGate firewalls.

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiGate-Wireless" and "FortiGate-event" to see the event types associated with this device.

Rules

There are generic rules that trigger for this device as event types are mapped to specific event type groups.

Reports

Generic reports are written for this device as event types are mapped to specific event type groups.

Configuration

Configure FortiGate to:

1. Send Syslog to FortiSIEM.
2. Enable SNMP read from FortiSIEM.

Sample Events

FortiSIEM generated performance monitoring events:

```
[PH_DEV_MON_FORTIAP_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortinet.cpp,  
[lineNumber]=688,[hostName]=FAP320C-default,[hostIpAddr]=,[sysUpTime]=7588440,  
[wtpDaemonUpTime]=7588440,[wtpSessionUpTime]=63039960,[numWlanClient]=0,  
[ftntWtpSessionStatus]=55038712,[sentBitsPerSec]=0.000000,[recvBitsPerSec]=0.000000,  
[pollIntv]=180,[phLogDetail]=
```

```
[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortinet.cpp,  
[lineNumber]=698,[cpuName]=FAP320C-default_WTP_CPU,[hostName]=FAP320C-default,  
[hostIpAddr]=,[cpuUtil]=0.000000,[pollIntv]=0,[phLogDetail]=  
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortinet.cpp,  
[lineNumber]=707,[memName]=FAP320C-default_WTP_MEM,[hostName]=FAP320C-default,  
[hostIpAddr]=,[memUtil]=34,[totalMemKB]= 254256 ,[freeMemKB]=254256,[usedMemKB]=0,  
[phLogDetail]=
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiAP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

FortiWLC

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)
- [Sample Events](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller – Name, OS, Serial Number, Interfaces, Associated Access Points – name, OS, Interfaces	Controller – CPU, Memory, Disk, Throughput, QoS statistics, Station count	Performance and Availability Monitoring
Syslog		Hardware/Software errors, failures, logons, license expiry, Access Point Association / Disassociation	Security Monitoring and log analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiWLC" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

To configure syslog for FortiWLC, see the following knowledgebase article [How to send station-log messages from FortiWLC to external sys-log server](#).

Configure FortiWLC to:

1. Send Syslog to FortiSIEM.
2. Enable SNMP read from FortiSIEM.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiWLC
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sample Events

FortiSIEM generated performance monitoring events:

```
[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=281,[cpuName]=CPU,[hostName]=FWLCDemo,[hostIpAddr]=172.30.72.40,
[cpuUtil]=2.000000,[sysCpuUtil]=0.000000,[userCpuUtil]=2.000000,[waitCpuUtil]=98.000000,
[pollIntv]=176,[phLogDetail]=
[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=286,[diskName]=Disk,[hostName]=FWLCDemo,[hostIpAddr]=172.30.72.40,
[diskUtil]=65.000000,[totalDiskMB]=1084,[availDiskMB]=367,[pollIntv]=176,[phLogDetail]=
```

```
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=284,[memName]=PhysicalMemory,[hostName]=FWLCDemo,[hostIpAddr]=172.30.72.40,
[memUtil]=9.000000,[totalMemKB]=3922244,[freeMemKB]=3538244,[usedMemKB]=384000,
[phLogDetail]=
```

```
[PH_DEV_MON_FORTIWLC_SYS_THRUPUT]:[eventSeverity]=PHL_INFO,
[fileName]=deviceFortiWLCWLAN.cpp,[lineNumber]=343,[hostIpAddr]=172.30.72.40,
[pollIntv]=180,[recvBytes]=3940593459,[sentBytes]=4002693999,[recvBitsPerSec]=0.000000,
[sentBitsPerSec]=0.000000,[wlanRecvBytes]=10851874907433110752,
[wlanSentBytes]=9983789733519268498,[wlanRecvBitsPerSec]=0.000000,
[wlanSentBitsPerSec]=0.000000,[phLogDetail]=
```

```
[PH_DEV_MON_FORTIWLC_QOS_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=426,[hostIpAddr]=172.30.72.40,[pollIntv]=176,[qosSessionCount]=1,
```

```
[qosH323SessionCount]=2,[qosSipSessionCount]=3,[qosSccpSessionCount]=4,  
[qosRejectedSessionCount]=5,[qosRejectedH323SessionCount]=6,  
[qosRejectedSipSessionCount]=7,[qosRejectedSccpSessionCount]=8,[qosPendingSessionCount]=9,  
[qosH323PendingSessionCount]=10,[qosSipPendingSessionCount]=11,  
[qosSccpPendingSessionCount]=12,[qosActiveFlowCount]=13,[qosPendingFlowCount]=14,  
[phLogDetail]=
```

```
[PH_DEV_MON_FORTIWLC_STATIONS]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,  
[lineNumber]=511,[hostIpAddr]=172.30.72.40,[pollIntv]=176,[station11a]=1,[station11an1]=2,  
[station11an2]=3,[station11an3]=4,[station11b]=5,[station11bg]=6,[station11gn1]=7,  
[station11gn2]=8,[station11gn3]=9,[stationData]=10,[stationPhone]=11,[stationWired]=12,  
[station11ac1]=13,[station11ac2]=14,[station11ac3]=15,[stationUnknown]=16,[phLogDetail]=
```

FortiWLC Syslog

```
Apr 09 15:07:54 172.18.37.203 ALARM: 12708266551 | system | info | ALR | RADIUS SERVER  
SWITCHOVER FAILED MAJOR Primary RADIUS Server <172.18.1.3> failed. No valid Secondary  
RADIUS Server present. Switchover FAILED for Profile <4089wpa2>
```


Motorola WiNG WLAN AP

- [What is Discovered and Monitored](#)
- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)
- [Settings for Access Credentials](#)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog		All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health	Availability, Security and Compliance

Event Types

Over 127 event types - In **ADMIN > Device Support > Event Types**, search for "Motorola-WiNG" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure devices to send syslog to FortiSIEM - make sure that the version matches the format below.

```
2015-11-11T13:00:16.720960-06:00 co-ap01 %DOT11-5-EAP_FAILED: Client 'FC-C2-DE-B1-43-81' failed 802.1x/EAP authentication on wlan 'OFFICE-WAREHOUSE-RADIUS-WLAN' radio 'co-ap01:R1'
```

```
2015-11-11T12:52:20.437659-06:00 us600001 %SMRT-5-COV_HOLE_RECOVERY_DONE: Radio us-ap10:R2 power changed from 19 to 14
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Motorola WiNG WLAN AP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Ruckus Wireless LAN

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller host name, Controller hardware model, Controller network interfaces, Associated WLAN Access Points	Controller Uptime, Controller Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Controller WLAN Statistics, Access Point Statistics, SSID performance Stats	Availability and Performance Monitoring

Event Types

- PH_DEV_MON_RUCKUS_CONTROLLER_STAT

```
[PH_DEV_MON_RUCKUS_CONTROLLER_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceRuckusWLAN.cpp,[lineNumber]=555,[hostName]=guest-zd-01,[hostIpAddr]=172.17.0.250,[numAp]=41,[numWlanClient]=121,[newRogueAP]=0,[knownRogueAP]=0,[wlanSentBytes]=0,[wlanRecvBytes]=0,[wlanSentBitsPerSec]=0.000000,[wlanRecvBitsPerSec]=0.000000,[lanSentBytes]=166848,[lanRecvBytes]=154704,[lanSentBitsPerSec]=7584.000000,[lanRecvBitsPerSec]=7032.000000,[phLogDetail]=
```

- PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT

```
[PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceRuckusWLAN.cpp,[lineNumber]=470,[hostName]=AP-10.20.30.3,[hostIpAddr]=10.20.30.3,[description]=,[numRadio]=0,[numWlanClient]=0,[knownRogueAP]=0,[connMode]=layer3,[firstJoinTime]=140467251729776,[lastBootTime]=140467251729776,[lastUpgradeTime]=140467251729776,[sentBytes]=0,[recvBytes]=0,[sentBitsPerSec]=0.000000,[recvBitsPerSec]=0.000000,[phLogDetail]=
```

- PH_DEV_MON_RUCKUS_SSID_PERF

```
[PH_DEV_MON_RUCKUS_SSID_PERF]:[eventSeverity]=PHL_INFO,[fileName]=deviceRuckusWLAN.cpp,
[lineNumber]=807,[hostName]=c1cs-guestpoint-zd-01,[hostIpAddr]=172.17.0.250,
[wlanSsid]=GuestPoint,[description]=Welcome SSID for not yet authorized APs.,
[wlanName]=Welcome SSID,[authenMethod]=open,[encryptAlgo]=none,[isGuest]=1,[srcVLAN]=598,
[sentBytes]=0,[recvBytes]=0,[sentBitsPerSec]=0.000000,[recvBitsPerSec]=0.000000,
[authSuccess]=0,[authFailure]=0,[assocSuccess]=0,[assocFailure]=0,[assocDeny]=0,
[disassocAbnormal]=0,[disassocLeave]=0,[disassocMisc]=0,[phLogDetail]=
```

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure the Controller so that FortiSIEM can connect to via SNMP.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Ruckus SmartOS WLAN AP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Ubiquiti Wireless LAN

Ubiquiti Inc. offers wireless networking products and solutions through its technology platforms such as airMAX, EdgeMAX, AmpliFi, airFiber, UFiber, UniFi, and Video.

Support Added: FortiSIEM 6.5.0-7.0.1 via Content Update

Vendor Version Tested: Not Provided

Vendor: <https://www.ui.com/>

Product: Wireless LAN controller

Product Information: <https://www.ui.com/>

- [Event Types](#)
- [Rules](#)
- [Reports](#)
- [Configuration](#)

Event Types

In **ADMIN > Device Support > Event Types**, search for "Ubiquiti" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

To configure, take the following steps.

1. Log in to the UniFi Controller's web interface.
2. Navigate to **Settings**.
3. From **Site**, navigate to the **Remote Logging** section.
4. Check the **Enable remote syslog server** checkbox to enable.
5. In the **Syslog Host** field, enter the FortiSIEM IP address.
6. In the **Syslog Port** field, enter 514.
7. Click **Apply** to save changes.

Using Virtual IPs to Access Devices in Clustered Environments

FortiSIEM communicates to devices and applications using multiple protocols. In many instances, access credentials for discovery protocols such as SNMP and WMI must be associated to the real IP address (assigned to a network interface) of the device, while application performance or synthetic transaction monitoring protocols (such as JDBC) will need the Virtual IP (VIP) assigned to the cluster. Since FortiSIEM uses a single access IP to communicate to a device, you must create an address translation for the Virtual IPs.

1. Log into your FortiSIEM virtual appliance as root.
2. Update the mapping in your IP table to map the IP address used in setting up your access credentials to the virtual IP.

```
iptables -t nat -A OUTPUT -p tcp --destination <access-ip> --dport <destPort> -j DNAT --to-destination <virtual-ip>:<destPort>'
```

As an example, suppose an Oracle database server is running on a server with a network address of 10.1.1.1, which is in a cluster with a VIP of 192.168.1.1. The port used to communicate with Oracle over JDBC is 1521. In this case, the update command would be:

```
iptables -t nat -A OUTPUT -p tcp --destination 10.1.1.1 --dport 1521 -j DNAT --to-destination 192.168.1.1:1521
```

Generic Log API Poller (HTTPS Advanced) Integration

This integration provides a low-code/no-code solution to integrating new logging APIs into FortiSIEM. Users can now directly define an API within FortiSIEM, which will then reach out to the target destination at the specified pull interval, and retrieve log events.

There are some substantial pre-requisites, you must obtain authentication credentials to your target API (Basic Auth, OAuth 2.0 client credentials, API Key, or Bearer Token, etc), and you must understand the elements of the API call to make, such as hostname, URI stem, headers, parameters, and body in both the authentication phase if additional (e.g. OAuth 2.0 token authorization), and the API call's own header/parameters, pagination details to retrieve the event data.

You can ensure your examples work first by using the curl command. Each component of those curl commands you can define in a FortiSIEM credential using the walkthrough below.

Overview

The approximate steps are here:

- Steps 1-5 are related to setting up the ingest of your data.
 - Steps 6+ are related to parsing, setting up rules and reports to make use of your ingested data.
1. Understand the API endpoint you'd like to ingest logs from, ensure you understand the authentication mechanism, API information such as headers, parameters, body if applicable.
 2. Test your understanding with curl to make sure you can retrieve that data manually.
 3. Define a device/application type in FortiSIEM -- Only do this if the device or app you are integrating with is not already defined under **ADMIN > Device Support > Devices/Apps**.
 4. Create a FortiSIEM credential - Selecting your desired device type, selecting protocol "HTTPS Advanced", and plugging in the API information in the appropriate fields
 5. Under **Step 2: Enter IP Range to Credential Associations** in **Admin > Setup > Credentials**, click **Add**, select the credential you just made.
Note: If you'd like a specific collector to make the API call instead of the Supervisor, there will be a collector drop-down to the right that you have to select first.
Click **Test > Test connectivity without ping**.
Check the pull events tab at the top - A yellow star will be present next to your new API job. Wait approximately 5 minutes for first real API call to be made. It should change to a green checkbox.
 6. Go to **Analytics** tab, run query for your data, it will come by default as unknown events until you create a custom parser for the data. If your SIEM is configured to drop unknown events, disable that option temporarily.
 7. Build a custom parser for your audit log data. See information on custom parser training [here](#).
 8. Define Event Types and map them to appropriate event type groups.
 9. Define any necessary rules and reports for the new data.

Take the following general steps.

Define a New Device Type (if one does not exist)

1. Navigate to **ADMIN > Device Support > Devices/Apps**.
2. Click **New**.
3. From the Device/Application Type Definition window, take the following steps.
 - a. From the **Category** drop-down list, select **Application**.
 - b. In the **Vendor** field, enter the vendor name.
 - c. In the **Model** field, enter the model/service name.
 - d. In the **Version** field, enter the specific version of the API to be used, otherwise enter "ANY".
 - e. From the **Device/App Group** drop-down list, select the category group(s) that the new device type will fall under. For example, Firewall, Server, etc...
 - f. From the **Access Protocol** drop-down list, de-select any selected access protocols, then select **HTTPS Advanced**.
 - g. Leave the App Package Group field empty.
 - h. (Optional) In the **Description** field, enter any additional information about the new device type.
 - i. Click **Save**.

Set Up the Access Credentials for the Device Type

1. Navigate to **ADMIN > Setup > Credentials**.
2. Under **Step 1: Enter Credentials**, click **New**.

3. From the **Access Method Definition** window, take the following steps.

- a. In the **Name** field, enter the name of the API.
- b. From the **Device Type** drop-down list select the device type, or leave as **Generic**.
- c. From the **Access Protocol** drop-down list, select **HTTPS ADVANCED**.
- d. In the **Pull Interval** field, configure the pull interval rate. The default interval is 5 minutes.
- e. Select Import Definition or Export Definition.

Import Definition - If someone else has created a logging API credential definition, they can export to a JSON file and provide it to you. You can upload this file to automatically fill in all details. The only items you need to provide yourself are the credentials/secrets required for the API to function.

Export Definition - If you have defined a working API integration, you can export the configuration to a JSON file. This JSON contains everything except the credential/secret/api key as configured under the Authentication tab. Note that this may still contain items containing user specifics such as username, or user specific URI stems, so you may need to remove sensitive data prior to sharing.

- f. From the **Authentication Type** drop-down list, select one of the following configurations:
 - i. Basic Auth
 - ii. OAuth2.0
 - iii. API Key
 - iv. Bearer Token

The [Authentication configuration](#) is dependent on the **Authentication Type** selected.

- g. Click on the Edit icon next to **General Parameters** to configure the logging API Endpoint's basic information.
 - i. In the **Host Name** field, enter the host name of the API endpoint.
Examples: `https://host.example.com` or `host.example.com`
 - ii. In the **URI Stem** field, enter the stem of the API endpoint, which is the part of the URI after the host, but before the arguments. Example: If the intended API call is `https://host.example.com/v1/events?limit=10&eventType=test`, the URI stem is the part that occurs after the hostname, and ends before the ? parameter separator. In this example, the URL stem would be `/v1/events`.
 - iii. From the **HTTP Method** drop-down list, select **GET** or **POST**. Determine your configuration by consulting your vendor's API documentation.
 - iv. Select the **Disable SSL Certificate Check** checkbox if your server does not have a valid SSL certificate. If checked, certificate validation is ignored.
- v. In the **JSON Response Log Key** field, enter the response key that identifies the JSON key value pair containing an array of logs events from the logging API. The system will look under this JSON key, and the value will be treated as an array of log events.

Most JSON APIs, when returning multiple event objects from one API call, will place them under a JSON key. See the following response objects from the API to identify where this value is important.

Example - Response from API is just an array of log events, no other structures.

Response from server:

```
[
```



```
{ ..event1 data...},
{ ..event2 data...}
]
```

JSON Response Key: <leave blank>

Example - Response from API puts array of events under a key named alerts.

```
{
  "metadata1":"xxxx",
  "someotherdata":"xxxx",
  "alerts": [{...event1...},{...event2...},{...event3...}]
}
```

JSON Response Key: alerts

- vi. In the **Log Header** field, enter the header string you want to prepend to each log event. The reasoning for this is because not every JSON log file cleanly identifies that it came from a given source. You can type any string here as a header. We recommend doing vendor + service. For example, if the log header is: "Vendor_Example.COM Event:" then every individual event will look like the following:

```
"Vendor_Example.COM Event: {...json event data here..}"
```

The resulting log events ingested via Analytics will look like the following:

```
<date> <api hostname> <resolved hostname IP> <log header you typed in credential>:
<json event>
Jul 27 15:43:03 2022 api.example.com 1.1.1.1 Vendor_Example.COM Event: {...json
event1...}
Jul 27 15:43:03 2022 api.example.com 1.1.1.1 Vendor_Example.COM Event: {...json
event2...}
```

Note: The colon ':' is inserted after your header, so if your header contains "some header:", your result would be:

```
<date> <api hostname> <resolved hostname IP> some header:: <json event>
```

So if you see double colons, that is the reason.

The **Log Header** field makes building FortiSIEM parsers easy, as they only have to match the header which cleanly identifies the type of event it is and where it came from.

- h. Click on the Edit icon next to **Authentication Parameters** to configure the logging API Endpoint's basic information. The options available in authentication depend on the selection from **Authentication Type**. Follow the configuration based on the Authentication Type you selected: [Basic Auth](#), [Oauth 2.0](#), [API Key](#), or [Bearer Token](#).

If **Basic Auth** was selected for **Authentication Type**, take the following steps.

- i. In the **User Name** field, enter the username for API authentication.
- ii. In the **Password** field, enter the password associated with the username.
- iii. In the **Confirm Password** field, re-enter the passwords associated with the username.
- iv. Click **OK**.
- v. Continue to [Log API Configuration](#).

If **OAuth 2.0** was selected for **Authentication Type**, you will have the following options to set up OAuth 2.0 Client Credentials authorization flow, as well as the header, parameter, and body options of the request.

From the General Tab

- i. In the **Access Token URL** field, enter the full URL to the OAuth 2.0 authorization endpoint.
- ii. From the **Grant Type** drop-down list, select **Client Credentials**. Currently, this is the only OAuth 2.0 authorization flow supported.
- iii. In the **Client Id** field, enter the client Id. Normally, this is obtained from the API. You typically create a set of OAuth credentials on the service, and download this.
- iv. In the **Client Secret** field, enter the client secret. Normally, this is obtained from the API. You typically create a set of OAuth credentials on the service, and download this.
- v. From the **Send Method** drop-down list, select **Send in Body** or **Send as Basic Auth Header**. Use the option specified by the API. The first option will send a pair of x-www-form-urlencoded key-value pairs in the POST body. The second option will base64 encode the 'clientId:clientSecret' into the Authorization header of the post request.
- vi. After configuration of the [Header Tab](#), [Parameter Tab](#), and [Body Tab](#), continue to [Log API Configuration](#).

From Header Tab

Note: You can add up to a total of 10 additional header, 10 parameter and 10 body key-value pairs. They can be of type string (pasted text) or of type date, that will be a calculated date value based on the execution time and/or last execution time.

- i. For OAuth 2.0 POST request to the authorize endpoint, you can specify any additional headers here. Consult your vendor's API documentation on the expected additional headers if any.

From Parameter Tab

Note: You can add up to a total of 10 additional header, 10 parameter and 10 body key-value pairs. They can be of type string (pasted text) or of type date, that will be a calculated date value based on the execution time and/or last execution time.

Parameters are any additional arguments accepted at the end of the URL.

Example: `https://example.com/v1/events?arg1=value&arg2=value`

For **Key Type** string, **Key Name** is the argument name, and **Key Value** is the literal/static value

So for Key Type string, Key Name format, and Key Value json, it would equate to :

`https://example.com/authorize?format=json`

From Body Tab

Note: You can add up to a total of 10 additional header, 10 parameter and 10 body key-value pairs. They can be of type string (pasted text) or of type date, that will be a calculated date value based on the execution time and/or last execution time.

Auth body contains the x-www-form-urlencoded body of key-value pairs that get sent with the OAuth 2.0 authorize request. The options you configure depend on the API you are using, and may not be needed at all.

For example, Microsoft graph requires the following POST Body Key-Value options

Key Type	Key Name	Key Value
string	grant_type	client_credentials
string	scope	https://graph.microsoft.com/.default

Note: FortiSIEM credential automatically adds the `client_id` and `client_secret` to the body.

Here is a CURL example of the Get Token endpoint for Graph:

Note: Replace {tenant} with your tenant!

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" -d 'client_id=xxxx&scope=https://graph.microsoft.com/.default&client_secret=xxxx&grant_type=client_credentials' 'https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token'
```

Notice the `-d` switch contains the POST Body data. The key value pairs are:

`client_id` -> auto-populated.

`client_secret` -> auto-populated.

`grant_type` -> `client_credentials`

`scope` -> `https://graph.microsoft.com/.default`

The first two are handled by FortiSIEM. Additional Key Names such as `grant_type` and `scope` must be entered.

If **API Key** was selected for **Authentication Type**, an API key is supplied either as a header or parameter.

- i. In the **API Key Name** field, enter the parameter name, or the header name.
- ii. In the **API Key Value** field, enter your API key secret value.
- iii. From the **Send Method** drop-down list, select the option appropriate for your API. Some API request this value be placed in the header of the request, or the query parameters. Check your API documentation for more information.

Examples:

If send method is Header: `curl -H "authkey: secret1234" https://example.com/v1/events`

If send method is Param: `curl https://example.com/v1/events?authKey=secret1234`

- iv. Continue to [Log API Configuration](#).

If **Bearer Token** was selected for **Authentication Type**, an API key is supplied either as a header or parameter.

If this option was selected, your API has already generated a Bearer token that is permanent for use. You'll notice that OAuth 2.0 also uses Bearer token, but the token is retrieved at runtime. In some APIs, the token is pre-generated and permanent.

Enter the token value into the **Bearer Token** field, and it will populate the Authorization header automatically.

Example:

A curl equivalent for your API will look like this:

```
curl -H "Authorization: Bearer secret1234" https://example.com/v1/events
```

Continue to [Log API Configuration](#).

- i. **Log API Configuration**

Click on the Edit icon next to **Log API Parameters** to configure the Log API. The Log API definition contains 4 sections - Header, Parameter, Body, and Pagination. The first 3 sections follow a set definition of key-value pairs representing either the header fields, URL parameter key-value pairs, or POST body key-value pairs.

Note: You can add up to a total of 10 additional header, 10 parameter and 10 body key-value pairs. They can be of type string (pasted text) or of type date, that will be a calculated date value based on the execution time and/or last execution time.

Adding a String Key-Value Pair

- i. Click **New**.
- ii. From the **Key Type** drop-down list, select **String**.
- iii. In the **Key Name** field, enter the header name, parameter name, or body key name depending on which tab (Log API Header, Log API Parameter, Log API Body) has been selected.
- iv. In the **Key Value** field, enter the string value.

Example: For the logging API, to set the Header "Content-Type" to application/json, you would configure the following:

Key Type: String

Key Name: Content-Type

Key Value: application/json

The curl equivalent would be:

```
curl -H "Content-Type:application/json" https://example.com/v1/events
```

Adding a Date Key-Value Pair

Most, if not all logging APIs will require a set of a date parameters. Some require a from (oldest) date to retrieve, or both a "from" and "to" parameter.

Since dates for a recurring poller can only be determined at run time, we define a facility to let you define these.

From the Log API **Header**, Log API **Parameter**, or Log API **Body** Tab, take the following steps.

- i. Click **New**.
- ii. From the **Key Type** drop-down list, select **Date**.
- iii. In the **Key Name** field, enter the header name, parameter name, or body key name for the date parameter. Consult your API documentation to determine the proper parameter.
- iv. In the **Key Date Format** drop-down list, select the date format the API expects the date to be supplied in.
- v. From the **Date Use Type** drop-down list, select **FromOperator**, **ToOperator**, or **RangeOperator**.

Date Use Type	Description
FromOperator	This is the oldest time interval. The script formats the last run time into this argument in the selected format.
ToOperator	If required by your API, this will be calculated as the latest date. The script sets this to the current run time in the selected format.
RangeOperator	Defines time interval date ranges within a single URL parameter instead of two parameters.

- vi. From the **Date Operator Type** drop-down list, select the operator used by your API.
Some APIs have date ranges that are inclusive vs exclusive. An API that has inclusive date ranges means that the date you specified includes all events up to and including that timestamp. E.g. $\geq$ or $\leq$. Exclusive date ranges means the API will return events up to the provided timestamp, but not on that timestamp. In other words $>$ or $<$. Consult your API documentation.
- vii. In the **Key Value Prefix** field, enter the Key Value Prefix if needed.
In some rare situations, you may need to prepend a string literal to your date format. In most cases you will leave this blank.
- viii. In the **Key Value Postfix** field, enter the Key Value Postfix field if needed.
In some rare situations, you may need to postfix a string literal to your date format. In most cases you will leave this blank.

If RangeOperator was selected, select the operator from the **Left Date Operator Type** drop-down list, and enter the **Left Key Value Prefix**, the **Left Key Value Postfix**, and **Joiner**. Also, from the **Right Date Operator Type** drop-down list, select the operator, and enter the **Right Key Value Prefix** and **Right Key Value Postfix**. The Range Operator is a special type of date parameter where the parameter contains both date ranges specifying the start and end times that logs should be returned.

Note: URL encoding not used here for readability / example purposes only.

Example of a range parameter in an API call.

```
curl https://graph.microsoft.com/beta/security/incidents?$filter=lastUpdateDateTime ge 2022-07-20T00:00:00.0Z and lastUpdateDateTime lt 2022-07-21T00:00:00.0Z
```

Notice that the date range is specified in one URL parameter called "\$filter".

Some APIs such as Microsoft graph support this complex query logic in a single parameter. Most *other* APIs, have two separate date parameters to identify the start and end time ranges to collect events.

Example:

```
https://example.com/events?from=2022-07-20T00:00:00.0Z&to=2022-07-21T00:00:00.0Z
```

The from parameter is the start range, and the to parameter is the end range.

Example of a Date Parameter

If poll Interval is 5 minutes. Last Poll Time is used for the FromOperator, and ToOperator set to current execution time. (Now – 5 minutes)

```
curl https://example.com/v1/events?from=2022-01-01T00:00:00Z&to=2022-01-01T00:05:00Z
```

Example 2 for RangeOperator

```
curl https://example.com/v1/events?$filter=lastUpdateDateTime+ge+2022-06-06T15:20:50.000Z+and+lastUpdateDateTime+lt+2022-06-06T22:24:03.000Z
```

The **Parameter Key Type** would be **date**.

The **Parameter Key Name** would be "\$filter".

Note: Do not include the quotations.

The **Key Date Format** would be **ISO8601-YYYY-MM-DDThh:mm:ss.sTZD**.

The **Date Use Type** field would be **RangeOperator**.

The **Left Date Operator Type** would be **>=**.

The **Left Key Value Prefix** would be "lastUpdateDateTime+ge+"

Note: Do not include the quotations.

The **Joiner** field would be "+and+"

Note: Do not include the quotations.

The **Right Date Operator Type** would be **<**.

The **Right Key Value Prefix** would be "lastUpdateDateTime+lt+"

Note: Do not include the quotations.

Log API Pagination

This tab defines pagination within your API.

From the **Pagination Method** drop-down list, select the pagination method.

Currently, only the following pagination methods are supported:

- **Link Header** – Uses Web Linking RFC 8288 next header to reference next page of events
- **Offset and Limit** – uses a combination of offset and limit parameters to control pagination
 - In the **Limit Key Name** field, enter the limit key name.
 - In the **Limit Value** field, enter the limit value.
 - In the **Offset Key Name** field, enter the offset key name.
 - In the **Offset Start Value** field, enter the offset start value.
 - In the **Offset Increment Value** field, enter the offset increment value.
 - In the **Offset Max Value** field, enter the offset maximum value.
- **Custom Next Url** – Check either response body or response header for a next URL for paged events.
 - In the **Key Name** field, enter the key name.
 - From the **Key Location** drop-down list, select body or header.
 - From the **Key Type** drop-down list, select URL or URL_STEM.
- **Custom Next Cursor** – Check response body for a cursor parameter to next set of events
 - In the **Cursor Key Name** field, enter the cursor key name.
 - From the **Cursor Type** drop-down list, select parameter.
 - In the **Next Cursor Name** field, enter the next cursor name.
- **None** – No pagination, entire request is returned in one API call. Repeat data possible

Set Up the IP/Host with Created Access Credentials

In **Step 2: Enter IP Range to Credential Associations**, if you have more than one FortiSIEM collector, select the collector that will do the polling from the drop-down list. **Note:** A drop-down list will not appear if you only have one collector.

1. Click **New**.
 - a. Select the credential name you created (during [Set Up the Access Credentials for the Device Type](#)) from the **Credentials** drop-down list. The **IP/Host Name** field should auto populate the URL.
 - b. Click **Save**.

2. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection. If you encounter an error, refer to [Common Errors](#) for additional information that may help you resolve the issue.
3. Wait for approximately 5 minutes.
4. Navigate to **ANALYTICS**, and confirm that events appear.

Common Errors

After clicking on **Test connectivity w/o Ping**, if you receive an error message, review the following for possible causes.

401 - Unauthorized. The credentials you provided were invalid, or most likely not typed in correctly.

403 - General error observe error message.

404 - Not Found, the URI stem / api endpoint is likely not accurate, or the header/parameter values are not correct.

429 - Too Many API calls being made. You may have too many concurrent API endpoints configured to target API.

Contact [Fortinet Support](#) if you have issues resolving any of these errors.

Ingesting JSON Formatted Events Received via HTTP(S) POST

FortiSIEM can receive, parse, and store JSON formatted events received via HTTP(S) POST. Follow these steps to implement this.

1. Configure the FortiSIEM node with the HTTPS credential for receiving the HTTP(S) POST event by taking the following steps.
 - a. Identity the FortiSIEM node receiving the events. Most likely, this will be the Collector.
 - b. SSH to the Collector and run the command.

```
htpasswd -b /etc/httpd/accounts/passwds <user> '<password>'
```

Note: If the password contains special characters, it is advisable to encode the password in single quotes.

2. Make sure the events are being pushed to the FortiSIEM node using the credentials in [Step 1](#) via this REST API:

```
https://<FSMNodeName>/rawupload?vendor=<vendor>&model=<model>&reptIp=<reptIp>&reptName=<reptHost>
```

where *FSMNodeName* is the resolvable host name or FQDN in [Step 1](#). The parameters Reporting Vendor (vendor), Reporting Model (model), Reporting Device (reptHost), and Reporting IP (reptIP) are needed to

create a CMDB entry and populate events.

Argument	Description
vendor	The vendor of the product that the logs originated from.
model	The model of the product that the logs originated from.
reptIp	This is the reporting IP, or the source of the log. The value you specify here will populate the CMDB as a reporting device.
reptName	This is the reporting device name, or the hostname of the device sending the logs.
separator	(Optional) This is used to split the whole content of one file into multiple events. - If it is omitted in the URL, it means one event one file. - Its value only allows the following input characters [% , 0-9, a-Z]. If the value contains any other character, the file name will start with "invalid_event_" and the parser will not parse the file. - For URL special character, please use its encode string. For example: '\n' ---> '%0A' '\n' ---> '%2C'

Note: If the Model contains whitespace, such as "Model 24", you must correctly encode spaces and other special characters in the URL parameters.

HTTP Method: POST

HTTP Body: log in JSON format. The JSON file can be compressed into tar, tgz, gz, zip format, in addition to text support.

Sample Curl to Send a JSON File

This example is sending a SAP Enterprise Threat Detection log.

```
curl -kv -u 'user:password' -d "@json_event.json" -X POST
'https://<FSMNodeName>/rawupload?vendor=SAP&model=ETD&reptIp=192.0.2.20&reptName=LogForwarder
1'
```

The above sends the JSON event stored in the file json_event.json to FortiSIEM. FortiSIEM then processes it, the resulting event should look like the following in **Log Format**, with an added header attached.

Log Format

```
[PH_DEV_MON_CUSTOM_JSON]:[reptVendor]=<vendor>,[reptModel]=<model>,[reptDevName]=<reptName>,[reptDevIpAddr]=<reptIp>,[json]=<JSON>
```

Where <JSON> is the actual JSON log body posted to FortiSIEM.

3. Query the events by using the Reporting Device Name or IP in [Step 2](#) and Event Type in [step 4e](#), by taking the following steps.
 - a. Go to the **ANALYTICS** tab.
 - b. Run a query for the Reporting IP = '#.#.#' for the last 10 minutes.

- c. Observe the raw event, it should be in the format of.

Filter By: Event Keywords **Event Attribute** CMDB Attribute Clear All Load Save

Paren	Attribute	Operator	Value	Paren	Next	Row
⊖	⊕ Reporting IP	=	1.1.1.1	⊖	⊕ AND OR	⊕ 🗑

Time Range: Real-time **Relative** Absolute

Last 10 Minutes

Trend Interval: Auto

Result Limit: 100 K rows

Apply & Run Apply Cancel

4. Create a new parser matching the header format with your provided vendor, model by taking the following steps.
 - a. Login to the Supervisor.
 - b. Navigate to **ADMIN > Device Support > Parsers**.
 - c. From the **Search...** field, enter PHCustomJsonParser.
 - d. Select it, and click **Clone**.
 - e. Make any required changes so that additional event attributes are parsed.
 - f. Name your parser appropriately, for example, `<Vendor>_<Model>_Custom_Parser`.
 - g. Use a similar event format recognizer: `<eventFormatRecognizer><![CDATA[\\[PH_DEV_MON_CUSTOM_JSON]\\:\\[reptVendor\\]=<vendor>,<[reptModel\\]=<model>,]]></eventFormatRecognizer>`

Note: See the [parser training documentation](#) on making a custom parser for your event.
 - h. Validate, Test, and Save the parser.
 - i. Click **Apply All** to deploy the parser changes.
5. If your JSON log events are batched into a single HTTPS POST operation (JSON contains many distinct events), there is a methodology to split the events using the `splitJsonEvent()` function, and discard the original monolithic event. Examine the `SAPEnterpriseThreatDetectionParser` on how to use the function `splitJsonEvent()`.

Syslog

Syslog IPv4 and IPv6

FortiSIEM supports receiving syslog for both IPv4 and IPv6. Parsing of IPv4 and IPv6 may be dependent on parsers.

Syslog over TLS

To receive syslog over TLS, a port must be enabled and certificates must be defined. The following configurations are already added to `phoenix_config.txt` in Super/Worker and Collector nodes.

FortiSIEM 5.x:

```
listen_tls_port_list=6514
tls_certificate_file=/etc/pki/tls/certs/tls_self_signed.crt
tls_key_file=/etc/pki/tls/private/tls_self_signed.key
```

FortiSIEM 6.x, 7.x:

```
listen_tls_port_list=6514
tls_certificate_file=/etc/pki/tls/certs/localhost.crt
tls_key_file=/etc/pki/tls/private/localhost.key
```

Note: The syslog over TLS client must be configured to communicate properly with FortiSIEM.

Common Reasons to use Syslog over TLS

- You are trying to send syslog across an unprotected medium such as the public internet.
- A SaaS product on the Public internet supports sending Syslog over TLS.

Common Integrations that require Syslog over TLS

- SentinelOne Portal Syslog Integration
- Cortex XDR Syslog Integration

Prerequisites

- If using Syslog over TLS over the public internet or with a public DNS, a public IP or port forwarding is required.
- Add a whitelist to restrict all traffic only from the senders source IPs if possible. Certain SaaS products may publish an IP whitelist, while for others, it may not be possible.

How to Generate a Public SSL/TLS Certificate

Take the following steps:

1. Generate a SSL/TLS certificate using a public certificate. A public certificate can be signed by a public certificate authority (CA) such as DigiCert, or GoDaddy.
2. Run the following command on your collector to generate a CSR (Certificate Signing Request)


```
cd /tmp
openssl req -new -newkey rsa:4096 -nodes -keyout /etc/pki/tls/private/tls-collector1.key -out tls-collector1.csr
```
3. Take the following actions when prompted.
 - a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
 - b. Enter your State or Province. For example, California would be "CA".
 - c. Enter your Locality. For example, a city would be "Sunnyvale".
 - d. Enter your desired org name. For example, "Fortinet".
 - e. Enter Unit Name, which is optional. For example, "IT".
 - f. Enter Common Name. It must match the FQDN of collector. For example, "collector1.myorg.fortinet.com".
 - g. Email Address. This can be left blank. Hit "enter" to continue.
 - h. If prompted for a challenge password, hit "enter" to leave blank and continue.
 - i. Hit enter again to confirm.

A Certificate Signing Request is created in /tmp/tls-collector1.csr.
4. Using WinScp or another SCP utility, download this CSR file to your desktop.
5. Go to your preferred public CA, and upload this CSR when prompted to generate a new SSL certificate file. When you have your new Certificate ZIP file, it will normally contain 2-3 files.
6. WinSCP zip file to /tmp of the Collector.
7. Unzip the file if needed, by using the following command.


```
unzip <filename>.zip
```

The .crt file is your certificate, and is usually a concatenation of all chain certificates.
8. Rename the cert files if needed using similar commands here.


```
cd /tmp
mv 11111111.crt tls-collector1.crt
```
9. Copy the cert to the correct folder using the following command.


```
cp tls-collector1.crt /etc/pki/tls/certs/tls-collector1.crt
```
10. Set permissions using the following command.


```
chmod 644 /etc/pki/tls/certs/tls-collector1.crt
chmod 640 /etc/pki/tls/private/tls-collector1.key
chown root:admin /etc/pki/tls/private/tls-collector1.key
```
11. On the Collector, update the /opt/phoenix/config/phoenix_config.txt file to reference the new tls cert using the following command.


```
vi /opt/phoenix/config/phoenix_config.txt
```
12. Locate the following lines in your phoenix_config.txt file.


```
listen_tls_port_list=6514
```

```
tls_certificate_file=/etc/pki/tls/certs/localhost.crt
tls_key_file=/etc/pki/tls/private/localhost.key
and replace the cert and key file with the following:
listen_tls_port_list=6514
tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt
tls_key_file=/etc/pki/tls/private/tls-collector1.key
```

- 13.** Save the file, and as root, restart phParser using the following command.
`killall -9 phParser`

How to Generate a Self Signed SSL/TLS Certificate

Take the following steps:

- 1.** On the Collector, run the following commands as root.
`cd /tmp`
`openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 -keyout /etc/pki/tls/private/tls-collector1.key -out /etc/pki/tls/certs/tls-collector1.crt`
- 2.** Take the following actions when prompted.
 - a.** When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
 - b.** Enter your State or Province. For example, California would be "CA".
 - c.** Enter your Locality. For example, a city would be "Sunnyvale".
 - d.** Enter your desired org name. For example, "Fortinet".
 - e.** Enter Unit Name, which is optional. For example, "IT".
 - f.** Enter Common Name. It must match the FQDN of collector. For example, "collector1.myorg.fortinet.com".
 - g.** Email Address. This can be left blank. Hit "enter" to continue.
 - h.** If prompted for a challenge password, hit "enter" to leave blank and continue.
 - i.** Hit enter again to confirm.
- 3.** Set the appropriate permissions for the private key and certificate generated, by running the following commands.
`chmod 640 /etc/pki/tls/private/tls-collector1.key`
`chown root:admin /etc/pki/tls/private/tls-collector1.key`
`chmod 644 /etc/pki/tls/certs/tls-collector1.crt`
- 4.** On the collector, update the `/opt/phoenix/config/phoenix_config.txt` file to reference the new tls certificate by editing the file, running the following command.
`vi /opt/phoenix/config/phoenix_config.txt`
- 5.** Find the following lines in the file.
`listen_tls_port_list=6514`

```
tls_certificate_file=/etc/pki/tls/certs/localhost.crt
```

```
tls_key_file=/etc/pki/tls/private/localhost.key
```

and replace the cert and key file with the following:

```
listen_tls_port_list=6514
```

```
tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt
```

```
tls_key_file=/etc/pki/tls/private/tls-collector1.key
```

6. Save the file, and as root, restart phParser using the following command.

```
killall -9 phParser
```

7. Make a copy of the certificate file to /tmp, and using WinSCP or another SCP utility, download the Collector Certificate file. For example, you may run the following command.

```
cp /etc/pki/tls/certs/tls-collector1.crt /tmp
```

8. Download /tmp/tls-collector1.crt to your desktop.

Note: You only need the Certificate file and not the private key. The private key will never leave the collector.

SNMP V3 Traps

There are two ways to configure SNMP V3 Traps

- [Manual File Configuration](#)
- [Configuration via Discover](#)

Manual File Configuration

To manually configure your file, take the following steps to enable FortiSIEM to receive SNMP V3 traps, which require credentials.

1. Configure the external device (e.g. FortiGate Firewall) to send SNMP V3 traps to the desired FortiSIEM node (typically a Collector). Note down the Authentication and Encryption protocols and passwords. This information is needed for FortiSIEM configuration in [step 5](#). Make sure the external device is sending traps to the FortiSIEM node.
2. SSH as root to the FortiSIEM node that is going to receive the SNMP V3 trap.
3. Stop phParser process, by running the following command.
`phtools --stop phParser`
4. Get the external device's SNMP engine ID, by taking the following steps:
 - a. Run the following command.
`snmptrapd -f -Dlcd_set_enginetime -Lo`
 - b. Grab the engine ID from the output. The following example shows that the engine ID is `0x800030440430313530` (in hex format).

```
[root@FSM-MYCENTOS8 ~]# snmptrapd -f -Dlcd_set_enginetime -Lo
registered debug token lcd_set_enginetime, 1
Log handling defined - disabling stderr
lcd_set_enginetime: engineID 80 00 30 44 04 30 31 35 30 : boots=0, time=0
lcd_set_enginetime: engineID 80 00 30 44 04 30 31 35 30 : boots=1612992361,
time=28525184
```
5. Update the `/etc/snmp/snmptrapd.conf` file by adding the authentication and encryption credentials for the external device's engine ID in hex format.

Note: You can have multiple entries, but keep in mind that you must have one for each engine ID if multiple devices are sending traps to this FortiSIEM node.

```
createUser -e <engineId> <username> <authprotocol> <authpassphrase> <privprotocol>
<privpassphrase>
```

Setting	Description
engineId	The external device's SNMP engine ID.
username	The user name.

Setting	Description
authprotocol	The authentication protocol for SNMPv3. This can be MD5, SHA, SHA-224, SHA-256, SHA-384, or SHA-512. See the Security Level table for requirements.
authpassphrase	The authentication password phrase.
privprotocol	The privacy protocol. This can be DES, AES, AES-192, or AES-256. See the Security Level table for requirements.
privpassphrase	The privacy password phrase.

Security Level	Description	secName	authProtocol	authPassword	privProtocol	privPassword
noAuthNoPriv	No authentication and no encryption required.	Required	Not Required	Not Required	Not Required	Not Required
authNoPriv	Messages are authenticated but not encrypted.	Required	Required	Required	Not Required	Not Required
authPriv	Messages are authenticated and encrypted.	Required	Required	Required	Required	Required

Here are three examples:

with authPriv

```
createUser -e 0x8000304404313530 trapuser SHA snmpv3pass AES snmpv3pass
```

with authNoPriv

```
createUser -e 0x8000304404313530 trapuser1 SHA snmpv3pass
```

with noauthNoPriv

```
createUser -e 0x8000304404313530 trapuser2
```


6. Start phParser process by running the following command.

```
phtools --start phParser
```
7. Run phstatus to make sure all processes are up.
You should now be receiving SNMP3 V3 Traps. You can go to **ANALYTICS** and run historical searches for the external device's reporting IP.

Configuration via Discover

To configure via the Discover feature, a destination device needs to be configured with SNMP v3 to forward Trap event to FortiSIEM. Take the following steps.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
 - a. Follow the instructions in "[Setting Credentials](#)" in the User's Guide to create a new credential.
 - b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Generic
Access Protocol	SNMP v3
Port	161
Security Level	Select the Security Level: noAuthNoPriv, authNoPriv, or authPriv
Security Name	Enter the security name.
Auth Protocol	Select the Auth Protocol. Note: Only needed if Security Level is authPriv or authNoPriv.
Auth Password	Enter the authentication password. Note: Only needed if Security Level is authPriv or authNoPriv.
Confirm Auth Password	Re-enter the authentication password. Note: Only needed if Security Level is authPriv or authNoPriv.
Priv Protocol	Select the Priv Protocol. Note: Only needed if Security Level is authPriv.

Settings	Description
Priv Password	Enter the Priv Password. Note: Only needed if Security Level is authPriv.
Confirm Priv Password	Re-enter the Priv Password. Note: Only needed if Security Level is authPriv.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
 - a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
 - b. Select the name of your SNMP v3 credential from the **Credentials** drop-down list.
 - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the external device.
5. Navigate to **ADMIN > Setup > Discovery**.
6. Click **New** to create a SNMP v3 discovery definition.
7. In the **Discovery Definition** dialog box, take the following steps:
 - a. In the **Name** field, enter a name for the Discovery Definition.
 - b. From the **Discovery Type** drop-down list, select **Range Scan**.
 - c. In the **Include** field, enter the IP address range.
 - d. Fill in the other fields as necessary.
 - e. When done, click **Save**.
8. Click **Discover**.
9. After the discovery is 100% complete, click the Jobs/Errors icon (upper right). Under the **Jobs** column, an entry of "Update SNMP Traps" should appear. Events can be queried from the **ANALYTICS** page. Also, in **CMDB > Devices**, in the **Summary** tab, the engine ID is displayed. It will also be in the configuration file.

Webhook Integration

Support Added: FortiSIEM 7.2.0

Information: <https://docs.github.com/en/webhooks/about-webhooks>

FortiSIEM in version 7.2.0 and above has added generic support for Webhooks. Prior, FortiSIEM would accept only webhooks with basic authentication using a strict set of POST parameters. Now, any application or SaaS product that supports push events/notifications via Webhooks can utilize this method to send data to FortiSIEM.

Topology

Event occurs in remote system or application -> Webhook fires with a FortiSIEM Collector as the target -> FortiSIEM authenticates the source of the webhook and parses the events.

Note: For publicly hosted SaaS applications utilizing Webhook push notifications to FortiSIEM, a FortiSIEM collector must be reachable on the public internet (virtual IP or static NAT) behind an edge firewall on proto/port

- (HTTPS - TCP 443). If the SaaS provider supports secure VPN tunneling to your organization, that method is preferable.

- [Configuration](#)

Configuration

- [Prerequisite](#)
- [FortiSIEM Setup](#)
- [Checking Webhook Events](#)
- [Webhook Device Setup](#)

Prerequisite

Most applications using webhook push notifications do server TLS certificate validation, which means the target collector must be configured with a public CA signed TLS certificate. See [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#) for configuration information.

FortiSIEM Setup

To configure webhook integration, you will need to take the following general steps.

- [Step 1 - Define a Device/Application Definition](#)
- [Step 2 - Define a Credential](#)
- [Step 3 - Configure Client Application with Generated Endpoint URL](#)

Take the following steps to configure FortiSIEM to get data from other servers by webhook integration.

Step 1 - Define a Device/Application Definition

This step defines the source application or device of the webhooks that FortiSIEM will receive. For several applications, FortiSIEM may have a predefined device or application type already defined with the "webhook" protocol, but if not defined you must first define the application type by taking the following steps.

Note: This example creates an application called "MyVendor - MyModel".

1. Login to FortiSIEM as an administrator.
2. Navigate to **Admin > Device Support**.
3. Select **Devices/Apps**.
4. Click **New**.

From the **Device/Application Type Definition** window, take the following steps.

- a. From the **Category** drop-down list, for this example, select **Application** as this is a SaaS product, not a physical appliance. Normally you would select **Device** or **Application** depending on what you are defining.
- b. In the **Vendor** field, enter the name of the device's vendor, example "MyVendor".
- c. In the **Model** field, enter the model of the device, example "MyModel".
- d. In the **Version** field, enter the device version. Enter "ANY" to indicate any version.

Note: Unless you'd like to define the specific app version, you can normally use "ANY".

- e. From the **Device/App Group** drop-down list, select the applicable groups, either from Devices or Applications. These groups are optional, but are a way to help categorize the source of our events. In our example, under **Applications**, the group "Security Gateway App" most identifies with what the product does, so select **Security Gateway App**.
- f. From the **Biz Service Group** drop-down list, for this example, leave it blank. Similar to Device/App group, business service groups is a logical group that the sending log source can be added to, such as "PCI Service" if in scope for PCI compliance.
- g. From the **Access Protocol** drop-down list, clear out the existing access protocols, and select **Webhook**.
Note: You can use Ctrl-F to search for "webhook" to quickly find it.
- h. Click **Save**.
You now have a device/app definition that is expected to use the webhook access protocol.

Step 2 - Define a Credential

Next, we will define a credential for the application definition we just created. Take the following steps to configure a credential for FortiSIEM.

1. Login to FortiSIEM as an administrator.
2. Navigate to **Admin > Setup > Credentials**.
3. Under **Step 1: Enter Credentials**, click **New**.
4. In the **Access Method Definition** window, input the following:
 - a. In the **Name** field, enter the name of the credential. For this example, use "myvendor_webhook". This serves as the basis of the target endpoint created, e.g. collector01.example.com/webhook/myvendor_webhook
 - b. From the **Device Type** drop-down list, select "MyVendor MyModel" that you created earlier. Normally for webhook integration, you would select a predefined device type that has webhook included as part of their definition.
 - c. The **Access Protocol** selection should already be Webhook. Normally, this should appear or be an option from the **Access Protocol** drop-down list. If it is missing, it means this device type is not expected to use Webhook.
 - d. Leave the **Separator** field as is. The "\n" is the newline linefeed and means that each line in the response is treated as a new log.
 - e. The **Receiver FQDN** field expects the FQDN or IP address of the FortiSIEM collector that will be receiving the webhook traffic. This is used to help dynamically generate an endpoint configuration for you. This should ideally be the FQDN of the collector from the sending application's perspective. For example, if this is a SaaS application on the public internet, this will be a public FQDN, e.g. collector01.example.com.
 - f. The **Reporting Host Name** field expects the source hostname of the sending application. It is used to uniquely identify the logs as it will be in the header of every log. You can use something like example.com if example.com was the vendor's domain.
 - g. **Endpoint** is the dynamically generated webhook endpoint based on the receiver FQDN. This makes it easier to paste this URL as the target of your webhooks in the client application.
 - h. From the **Auth Type** drop-down list lets you choose you authorization type. The webhooks sender must be authenticated for authenticity of the source events, so bad actors cannot pollute the SIEM with incorrect logs.
The following auth methods are supported.

Auth Type	Description/Instruction
Basic Auth	Basic authorization compares the base64(name:password) with the value of the authorization header (authorization: basic xxxx) in an HTTP request. There is an optional helpful UI feature if you'd like to get the exact string the client application should send in the authorization header (if for some reason they don't compute the basic auth themselves). You can get the expected Authorization header value by clicking Get from Header Value after you have entered the User Name, and associated password in the User Name field and Password/Confirm Password fields respectively. This should rarely be needed, as most client applications sending webhooks with basic auth will only require the same username/password and compute this for you.
Simple Secret	Simple Secret compares the secret with the value of header/parameter in HTTP request directly. Enter the shared secret value in the Shared Secret field. From the Auth Part drop-down list, select Header or Parameter, and input either the Header Name or Parameter Name in the Header Name or Parameter Name field, depending on what you selected from the Auth Part drop-down list.
HMAC	HMAC uses a shared secret to create a hash signature with each payload from the HTTP request and then compares the value of the header/parameter in the HTTP request. It is client application dependent on whether they pass the hash in a specific HTTP header value, or an HTTP url parameter. After selecting HMAC, take the following steps. From the Algorithm drop-down list, select SHA-256 or SHA-512. Next, input the Shared Secret value in the Shared Secret field. From the Auth Part drop-down list, select Header or Parameter, and input either the Header Name or Parameter Name in the Header Name or Parameter Name field, depending on what you selected from the Auth Part drop-down list.

i. Click **Save and Deploy**.

This saves the credential definition for this webhook to the SIEM, and creates the API endpoint for the webhook on all collectors in the organization. The endpoint preview field is what is configured in the client application as the target POST endpoint for the webhook events. It is important to note that in most cases certificate validation is enforced by the client application posting to the collector endpoint. This means the collector needs a valid FQDN configured, e.g. collector01.example.com and a valid public CA signed TLS certificate.

See [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#) for configuration information.

Step 3 - Configure Client Application with Generated Endpoint URL

The **Endpoint** field is a preview of the full URL that the client application will POST notifications to. You will configure the client application with this endpoint, and specify the same authentication methods as defined in FortiSIEM.

To get this endpoint, select the credential you created, click **Edit**, then from the **Endpoint** row, copy the URL.

Checking Webhook Events

For new applications not explicitly supported, resulting POST events will likely be labeled as an unknown_eventType or with a generic event type called "Vendor-Model-JSON", since only a generic parser exists to catch these events. You will need to create a dedicated parser to parse additional fields and assign appropriate event types.

Events can be queried from the **Analytics** page, using PH_DEV_MON_CUSTOM_JSON as part of a Raw Event Log search. Take the following steps.

1. Navigate to **Analytics > Search**.
2. Click **Edit Filters and Time Range.....**
3. In **Filter By**, select the **Event Attribute** tab.
4. Enter/select the following:
Attribute = Raw Event Log, Operator = CONTAIN, Value = PH_DEV_MON_CUSTOM_JSON
5. Click **Apply & Run**.

To enhance the custom events so they are properly handled, you will need to create the following:

- Custom Parser (required)
- Custom Event Types (optional)
- Custom Rules (optional)
- Custom Reports (optional)
- Custom Dashboards (optional)

Webhook Device Setup

Enable other server to forward events to FortiSIEM by webhook by following the instructions from that device's documentation.

Note: The webhook endpoint URL that was provided in your FortiSIEM configuration will be needed in the Webhook device configuration here.

When a third party server uses webhook with SSL verification, certificate files signed by a public certificate authority (CA) must be used to update httpd server in FortiSIEM node.

In this situation, take the following steps:

Note: See [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#) for detailed configuration information.

1. Generate a public certificate Generate a SSL/TLS certificate using a public certificate. A public certificate can be signed by a public certificate authority (CA) such as DigiCert, or GoDaddy.
 - a. Use a public certificate to update the following lines in /etc/httpd/conf.d/ssl.conf
SSLCertificateFile
SSLCertificateKeyFile
SSLCertificateChainFile
 - b. Restart httpd by running the following command.
systemctl restart httpd

- c. Test the public certificate by using the following link.
<https://www.ssllabs.com/ssltest/analyze.html>

Flow Support

FortiSIEM supports NetFlow v5, NetFlow v9, IPFIX, sFlow, and JFlow. You need to configure any device to send traffic to FortiSIEM on these ports and FortiSIEM will automatically parse and handle the flows. No other configuration is required.

Flow traffic should be sent to the below specified ports.

Protocol / Port	Network Flow	Supported Versions
UDP / 2055	NetFlow	v5, v9
UDP / 2055	Internet Protocol Flow Information Export (IPFIX)	v10
UDP / 6343	sFlow	v5
UDP / 6343	JFlow	v5

If you want to send to another port, then you need to configure port translation NAT on FortiSIEM.

Netflow IPv4 and IPv6

FortiSIEM supports receiving netflow for both IPv4 and IPv6 and parsing of IP addresses.

Appendix

- [CyberArk to FortiSIEM Log Converter XSL](#)
- [Access Credentials](#)
- [How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate](#)

CyberArk to FortiSIEM Log Converter XSL

```
<?xml version="1.0" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:import href='../Syslog/RFC5424Changes.xsl' />
  <xsl:output method="text" version="1.0" encoding="UTF-8" />
  <xsl:template match="/">
    <xsl:apply-imports />
    <xsl:for-each select="syslog/audit_record">
      <xsl:text>CYBERARK: Product="</xsl:text>
        <xsl:value-of select="Product" />
      <xsl:text>"</xsl:text>
      <xsl:text>;Version="</xsl:text>
        <xsl:value-of select="Version" />
      <xsl:text>"</xsl:text>
      <xsl:text>;Hostname="</xsl:text>
        <xsl:value-of select="Hostname" />
      <xsl:text>"</xsl:text>
      <xsl:text>;MessageID="</xsl:text>
        <xsl:value-of select="MessageID" />
      <xsl:text>"</xsl:text>
      <xsl:text>;Message="</xsl:text>
        <xsl:value-of select="Message" />
      <xsl:text>"</xsl:text>
      <xsl:choose>
        <xsl:when test="Desc!=''">
          <xsl:text>;Desc="</xsl:text>
            <xsl:value-of select="Desc" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="Action!=''">
          <xsl:text>;Action="</xsl:text>
            <xsl:value-of select="Action" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="Location!=''">
          <xsl:text>;Location="</xsl:text>
            <xsl:value-of select="Location" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
    </xsl:for-each>
  </xsl:template>
</xsl:stylesheet>
```

```

</xsl:choose>
<xsl:text>;Issuer="</xsl:text>
  <xsl:value-of select="Issuer" />
<xsl:text>"</xsl:text>
<xsl:choose>
  <xsl:when test="Station!=''">
    <xsl:text>;Station="</xsl:text>
      <xsl:value-of select="Station" />
    <xsl:text>"</xsl:text>
  </xsl:when>
</xsl:choose>
<xsl:choose>
  <xsl:when test="File!=''">
    <xsl:text>;File="</xsl:text>
      <xsl:value-of select="File" />
    <xsl:text>"</xsl:text>
  </xsl:when>
</xsl:choose>
<xsl:choose>
  <xsl:when test="Safe!=''">
    <xsl:text>;Safe="</xsl:text>
      <xsl:value-of select="Safe" />
    <xsl:text>"</xsl:text>
  </xsl:when>
</xsl:choose>
<xsl:choose>
  <xsl:when test="Category!=''">
    <xsl:text>;Category="</xsl:text>
      <xsl:value-of select="Category" />
    <xsl:text>"</xsl:text>
  </xsl:when>
</xsl:choose>
<xsl:choose>
  <xsl:when test="RequestId!=''">
    <xsl:text>;RequestId="</xsl:text>
      <xsl:value-of select="RequestId" />
    <xsl:text>"</xsl:text>
  </xsl:when>
</xsl:choose>
<xsl:choose>
  <xsl:when test="Reason!=''">
    <xsl:text>;Reason="</xsl:text>
      <xsl:value-of select="Reason" />
    <xsl:text>"</xsl:text>
  </xsl:when>
</xsl:choose>
<xsl:choose>
  <xsl:when test="SeverityCategory!=''">

```

```

        <xsl:text>;Severity="</xsl:text>
        <xsl:value-of select="Severity" />
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="GatewayStation!=''">
        <xsl:text>;GatewayStation="</xsl:text>
        <xsl:value-of select="GatewayStation" />
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="SourceUser!=''">
        <xsl:text>;SourceUser="</xsl:text>
        <xsl:value-of select="SourceUser" />
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="TargetUser!=''">
        <xsl:text>;TargetUser="</xsl:text>
        <xsl:value-of select="TargetUser" />
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="TicketID!=''">
        <xsl:text>;TicketID="</xsl:text>
        <xsl:value-of select="TicketID" />
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="LogonDomain!=''">
        <xsl:text>;LogonDomain="</xsl:text>
        <xsl:for-each select="CAProperties/CAProperty">
            <xsl:if test="@Name='LogonDomain'">
                <xsl:value-of select="@Value" />
            </xsl:if>
        </xsl:for-each>
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="Address!=''">
        <xsl:text>;Address="</xsl:text>
        <xsl:for-each select="CAProperties/CAProperty">

```

```

        <xsl:if test="@Name='Address'">
            <xsl:value-of select="@Value" />
        </xsl:if>
    </xsl:for-each>
    <xsl:text>"</xsl:text>
</xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="CPMStatus!=''">
        <xsl:text>;CPMStatus="</xsl:text>
        <xsl:for-each select="CAProperties/CAProperty">
            <xsl:if test="@Name='CPMStatus'">
                <xsl:value-of select="@Value" />
            </xsl:if>
        </xsl:for-each>
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="Database!=''">
        <xsl:text>;Database="</xsl:text>
        <xsl:for-each select="CAProperties/CAProperty">
            <xsl:if test="@Name='Database'">
                <xsl:value-of select="@Value" />
            </xsl:if>
        </xsl:for-each>
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="DeviceType!=''">
        <xsl:text>;DeviceType="</xsl:text>
        <xsl:for-each select="CAProperties/CAProperty">
            <xsl:if test="@Name='DeviceType'">
                <xsl:value-of select="@Value" />
            </xsl:if>
        </xsl:for-each>
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
<xsl:choose>
    <xsl:when test="ExtraDetails!=''">
        <xsl:text>;ExtraDetails="</xsl:text>
        <xsl:value-of select="ExtraDetails" />
        <xsl:text>"</xsl:text>
    </xsl:when>
</xsl:choose>
</xsl:for-each>

```

```
<xsl:text>#13;#10;</xsl:text>
</xsl:template>
</xsl:stylesheet>
```

Access Credentials

- [SNMP Access Credentials](#)
- [SSH Access Credentials](#)
- [Telnet Access Credentials](#)
- [HTTPS Access Credentials](#)
- [Password Configuration](#)
 - [Manual Password Configuration](#)
 - [CyberArk SDK Password Configuration](#)
 - [CyberArk REST API Password Configuration](#)
 - [RAX_CustomerService Password Configuration](#)
 - [RAX_Janus Password Configuration](#)
 - [RAX_MSCloud Password Configuration](#)

SNMP Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP.

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	SNMP
Community String	<your own>

SSH Access Credentials

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	SSH
Port	22
Password Config	See Password Configuration

Setting	Value
User Name	A user who has permission to access the device over SSH
Password	The password associated with the user
Super Password	Enter the super password for the system, if required
Organization	Select an organization from the drop-down list

Telnet Access Credentials

These are the generic settings for providing Telnet access to your device from FortiSIEM

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	Telnet
Port	23
Password Config	See Password Configuration
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user
Super Password	Enter the super password for the system, if required
Organization	Select an organization from the drop-down list

HTTPS Access Credentials

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	HTTPS
Port	443
URI	URI address
Password Config	See Password Configuration
User Name	A user who has permission to access the device over HTTPS

Setting	Value
Password	The password associated with the user
Organization	Select an organization from the drop-down list

Password Configuration

- [Manual Password Configuration](#)
- [CyberArk SDK Password Configuration](#)
- [CyberArk REST API Password Configuration](#)
- [RAX_CustomerService Password Configuration](#)
- [RAX_Janus Password Configuration](#)
- [RAX_MSCloud Password Configuration](#)

Manual Password Configuration

Settings	Description
User Name	The user name for this account
Password	The password for this account
Super Password	The super password for this account
Organization	Select an organization from the drop-down list

CyberArk SDK Password Configuration

Settings	Description
App ID	Application ID (FortiSIEM)
Safe	Safe value
Folder	Folder location (Root)
Object	Object name
User Name	User name
Platform (Policy ID)	Policy ID
Database	Database name
Include Address for Query	
Organization	Select an organization from the drop-down list
Description	Description or comments about the credentials

CyberArk REST API Password Configuration

Settings	Description
Endpoint	The endpoint location of the CyberArk device
Root CA	The root certificate authority
SSL Certificate	Secure sockets layer certificate for authentication
SSL Key File	Secure sockets layer key file for encryption and decryption
App ID	Application ID (FortiSIEM)
Safe	Safe value
Folder	Folder location (Root)
Object	Object name
User Name	User name
Platform (Policy ID)	Policy ID
Database	Database name
Include Address for Query	
Session Token	Session ID used to identify a session
Organization	Select an organization from the drop-down list
Description	Description or comments about the credentials

RAX_CustomerService Password Configuration

Settings	Description
AWS Account Number	Enter the account number.
Azure Subscription ID	Enter the subscription ID.

RAX_Janus Password Configuration

Select RAX_Janus as the Password Config. Supply a Session ID if required.

RAX_MSCloud Password Configuration

Settings	Description
Azure Subscription ID	Enter the subscription ID.

How to Set Up a FortiSIEM Collector with a Public SSL/TLS Certificate

To set up a FortiSIEM Collector with a Public SSL/TLS Certificate, you will need to generate a certificate signing request (CSR), use the CSR to generate a certificate, then configure your FortiSIEM Collector with the certificate.

- [Step 1 - Generate CSR](#)
- [Step 2 - Generate Certificate](#)
- [Step 3 - Configure Collector](#)

Step 1 - Generate CSR

To generate a public SSL/TSL certificate, take the following steps:

1. Run the following commands on your collector to generate a CSR (Certificate Signing Request)

```
cd /tmp  
openssl req -new -newkey rsa:4096 -nodes -keyout /etc/pki/tls/private/tls-collector1.key -  
out tls-collector1.csr
```
2. Take the following actions when prompted.
 - a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
 - b. Enter your State or Province. For example, California would be "CA".
 - c. Enter your Locality. For example, a city would be "Sunnyvale".
 - d. Enter your desired org name. For example, "Fortinet".
 - e. Enter Unit Name, which is optional. For example, "IT".
 - f. Enter Common Name. It must match the FQDN of Collector. For example, "collector1.myorg.fortinet.com".
 - g. Email Address. This can be left blank. Press "Enter" to continue.
 - h. If prompted for a challenge password, press "Enter" to leave blank and continue.
 - i. Press Enter again to confirm.

A Certificate Signing Request is created in /tmp/tls-collector1.csr.

Step 2 - Generate Certificate

Take the following steps to generate a certificate.

1. Using WinSCP or another SCP utility, download the CSR file to your desktop.
2. Go to your preferred public Certificate Authority (CA), e.g. GoDaddy, Comodo, SSL.com, Symantec, and upload this CSR when prompted to generate a new SSL certificate file.

When you have your new certificate zip file, it will normally contain 2-3 files.

Configure Collector

Take the following steps to configure your FortiSIEM Collector with the generated certificate.

1. Use WinSCP to copy the certificate zip file to /tmp on your Collector.
2. Unzip the file if needed, by using the following command.

```
unzip <filename>.zip
```

The .crt file is your certificate, and is usually a concatenation of all chain certificates.

3. Rename the cert files if needed using similar commands here.

```
cd /tmp
```

```
mv 11111111.crt tls-collector1.crt
```

4. Copy the cert to the correct folder using the following command.

```
cp tls-collector1.crt /etc/pki/tls/certs/tls-collector1.crt
```

Note:

If the TLS certificate provided has the entire certificate chain in the certificate, a certificate chain file is not needed.

If the public CA provided in the download is an intermediate cert chain file, you can copy that to the same directory using similar commands here.

```
cp vendorchain_cert.crt /etc/pki/tls/certs/tls-chain-certs.crt
```

```
chmod 644 /etc/pki/tls/certs/tls-chain-certs.crt
```

5. Set permissions using the following commands.

```
chmod 644 /etc/pki/tls/certs/tls-collector1.crt
```

```
chmod 640 /etc/pki/tls/private/tls-collector1.key
```

```
chown root:admin /etc/pki/tls/private/tls-collector1.key
```

The new public CA signed TLS/SSL certificate, associated private key, and any certificate chain certificates must be referenced in the following two Collector files:

```
/etc/httpd/conf.d/ssl.conf
```

```
/opt/phoenix/config/phoenix_config.txt
```

6. Use vi or another text editor to open the ssl.conf file.

```
vi /etc/httpd/conf.d/ssl.conf
```

7. Find the following 3 directives and overwrite the existing values, or use "#" to change the lines to comments.

Note: The last directive is optional. If the TLS cert was directly signed by a root CA, it is not needed. Also, if the cert chain is already chained inside the SSL certificate itself, the intermediate chain file is not needed separately.

```
SSLCertificateFile /etc/pki/tls/certs/tls-collector1.crt
```

```
SSLCertificateKeyFile /etc/pki/tls/private/tls-collector1.key
```

```
SSLCertificateChainFile /etc/pki/tls/certs/tls-chain-certs.crt
```

8. Save the file and restart Apache by running the following command.

```
systemctl restart httpd
```

9. Next, update the /opt/phoenix/config/phoenix_config.txt file to reference the new TLS certificate by using vi or some other text editor.

```
vi /opt/phoenix/config/phoenix_config.txt
```

10. Locate the following line in your phoenix_config.txt file.

```
listen_tls_port_list=6514
```

11. Change the following lines that appear after listen_tls_port_list=6514 so they reference the new TLS certificate.

```
tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt
```

```
tls_key_file=/etc/pki/tls/private/tls-collector1.key
```

12. Save the file, and as root, restart phParser using the following command.

```
killall -9 phParser
```



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.