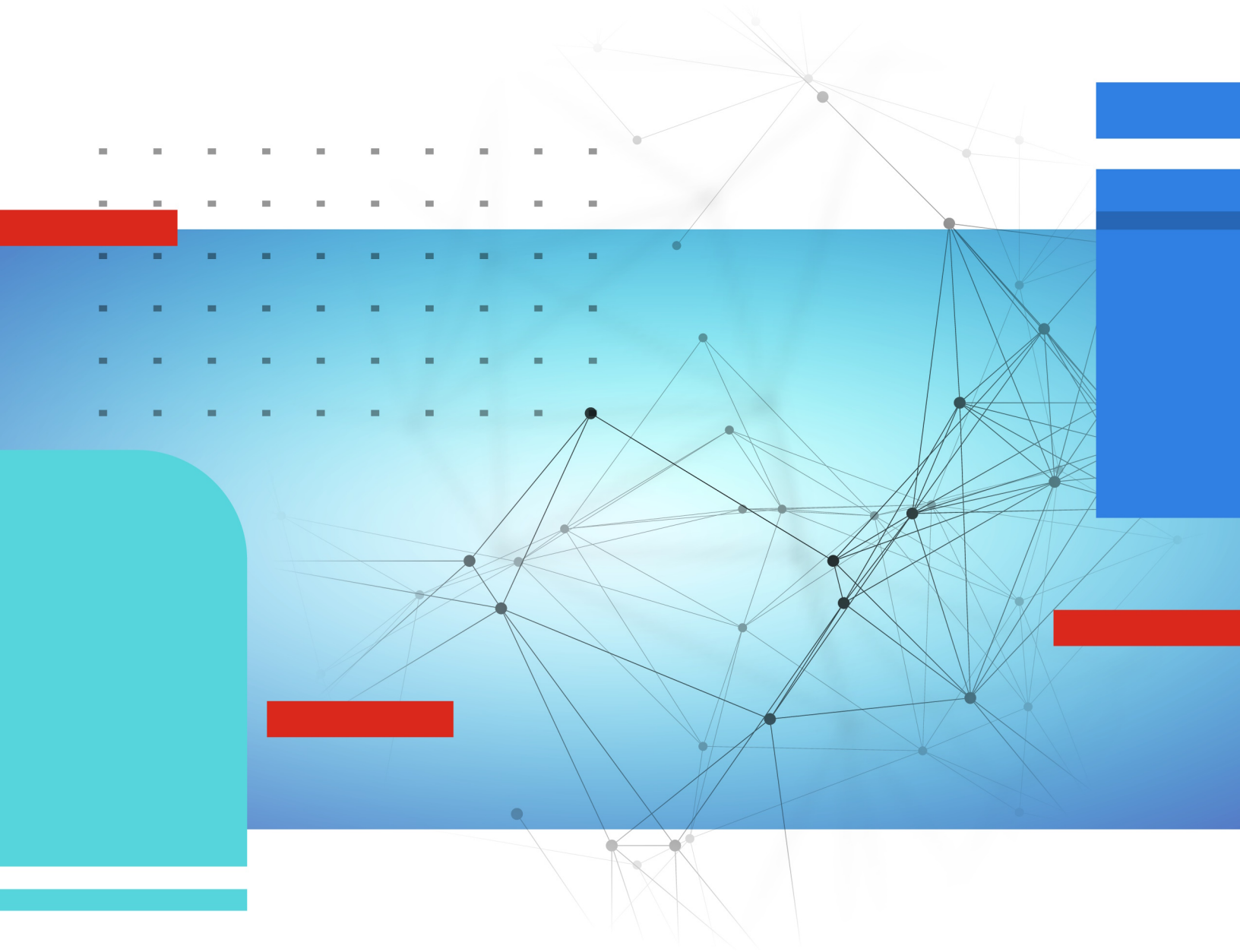
Administration Guide

FortiAnalyzer 7.6.4



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



March 9, 2026
FortiAnalyzer 7.6.4 Administration Guide
05-764-1033776-20260309

TABLE OF CONTENTS

Change Log **12**
Setting up FortiAnalyzer **13**
Connecting to the GUI 13
FortiAnalyzer Setup wizard 14
Activating VM licenses 20
Security considerations 22
Restricting GUI access by trusted host 22
Trusted platform module support 23
Self-encrypting drives 24
UEFI secure boot 27
Real time file system integrity checking 30
Other security considerations 30
GUI overview 30
Panes 33
Color themes 33
Switching between ADOMs 34
Using the right-click menu 34
Using the CLI console 35
Avatars 36
Using the Process Monitor 36
Showing and hiding passwords 37
Google Map integration 38
Target audience and access level 38
Initial setup 39
FortiManager features 39
Next steps 40
Restarting and shutting down 40
FortiAnalyzer Key Concepts **41**
Operation modes 41
Analyzer mode 41
Collector mode 42
Analyzer and Collector feature comparison 42
Analyzer–Collector collaboration 43
FortiAnalyzer Fabric 43
Administrative domains 43
Logs 44
Log encryption 44
Log storage 45
Log rolling 45
Log deletion 45
SQL database 46
Analytics and Archive logs 46
Data policy and automatic deletion 47
Disk utilization for Archive and Analytic logs 47

FortiView dashboard 48
Dashboards 49
Status 49
Customizing the status dashboard 51
System Information widget 51
Changing the host name 52
Configuring the system time 53
Updating the system firmware 54
Backing up the system 57
Restoring the configuration 61
Migrating the configuration 61
Configuring the operation mode 62
System Resources widget 62
License Information widget 63
Registering with FortiCloud 65
Enabling remote access from FortiCloud 66
Activating add-on licenses 66
Migrating FortiAnalyzer-VM licenses 68
License expiration 68
Unit Operation widget 71
Alert Messages Console widget 72
Log Receive Monitor widget 72
Insert Rate vs Receive Rate widget 73
Log Insert Lag Time widget 73
Receive Rate vs Forwarding Rate widget 74
Disk I/O widget 74
Device widgets 74
FortiAnalyzer Cloud Status widget 75
Restart, shut down, or reset FortiAnalyzer 75
Restarting FortiAnalyzer 75
Shutting down FortiAnalyzer 76
Resetting system settings 76
IOT dashboard 76
Email metrics dashboard 78
SOC dashboard 79
Endpoint vulnerability dashboard 80
XDR dashboard 82
Device Manager 83
ADOMs 85
FortiClient EMS devices 86
Unauthorized devices 86
Using FortiManager to manage FortiAnalyzer devices 87
Adding devices 87
Adding devices using the wizard 87
Authorizing devices 89
Hiding unauthorized devices 90

Adding an HA cluster 90
Adding a FortiGate using Security Fabric authorization 91
Managing devices 94
Using the toolbar 94
Editing device information 94
Displaying historical average log rates 96
Connecting to an authorized device GUI 97
Setting values for required meta fields 97
Device groups 98
Adding device groups 99
Managing device groups 99
FortiView 100
FortiView 101
How ADOMs affect FortiView 101
Logs used for FortiView 101
FortiView dashboards 101
Using FortiView 104
Viewing Indicators of Compromise 112
Examples of using FortiView 123
Monitors 125
FortiView monitors 125
Using the monitors dashboard 141
Customizing the monitors dashboard 142
Creating custom widgets 143
Enabling and disabling FortiView 145
Log View and Log Quota Management 146
Types of logs collected for each device 146
Syslog logs 148
Fabric logs 151
Log messages 152
Viewing the log message list of a specific log type 152
Viewing message details 152
Customizing displayed columns 155
Customizing default columns 155
Filtering messages 156
Threat Hunting 159
Monitoring all types of security and event logs from FortiGate devices 161
Viewing historical and real-time logs 162
Viewing raw and formatted logs 162
Custom views 162
Downloading log messages 164
Creating charts with Chart Builder 164
User and endpoint ID log fields 165
FortiMail correlated logs 166
Log groups 167
Log browse 167
Importing a log file 168
Downloading a log file 169

Deleting log files 169
Log and file storage 169
Disk space allocation 170
Log and file workflow 170
Automatic deletion 172
Logs for deleted devices 173
Storage information 174
Configuring log rate receiving limits 176
FortiGate log buffer 177
Fabric View 178
Asset Identity Center 178
Asset Summary 178
Identity Summary 180
Asset List 181
Identity List 185
OT View 189
Configuring endpoint and end user data sources 190
Subnets 191
Creating a subnet list 192
Creating a subnet group 193
Assigning subnet filters to event handlers 194
Fortinet Security Fabric 196
Adding a Security Fabric group 196
Displaying Security Fabric topology 197
Security Fabric traffic log to UTM log correlation 197
Security Fabric ADOMs 199
Enabling SAML authentication in a Security Fabric 201
Incidents & Events 204
Incidents 204
Raising an incident 204
Managing incidents 206
Analyzing an incident 208
Configuring incident settings 212
Adding reports to an incident 212
MITRE ATT&CK® 213
Event Monitor 218
Explorer 218
All Events 221
Default event views 223
Filtering events 224
Viewing event details 225
Acknowledging events 227
Assigning events 227
Suppressing events 227
Managing default views 229
Creating custom views 230
Understanding event statuses 231
Event handlers 231

Predefined basic event handlers 232
Predefined correlation event handlers 266
Predefined event handler examples 270
Geo-alerting event handlers 275
ZTNA login event handlers 284
Malicious IP intrusion event handler 292
Creating a custom event handler 298
Creating a custom correlation handler 304
Using the Automation Stitch for event handlers 310
Using the Generic Text Filter 311
Managing event handlers 312
Enabling event handlers 313
Cloning event handlers 314
Resetting predefined event handlers to factory defaults 314
Importing and exporting event handlers 314
Creating data selectors 316
Creating notification profiles 317
Event collectors 322
Configuring the webhook 325
Event collector logs 327
Event collector events 329
Indicators 330
Managing indicators 331
Indicator enrichment 333
Blocking indicators 334
FortiGuard Services 337
SOC Automation 338
Safeguarding 348
Outbreak Alerts 352
Viewing imported event handlers and reports 355
Security rating update 357
FortiTIP service integration 357
Automation 362
Summary 362
Active connectors 363
Playbooks 382
Playbook templates 390
Playbook triggers and tasks 391
Configuring tasks using variables 392
Importing and exporting playbooks 394
Playbook Monitor 396
SIEM log parsers 397
Log Parsers 398
Assigned Parsers 400
FortiAI 402
Enabling administrator access to FortiAI 403
Using FortiAI 403
FortiAI data privacy 408

FortiAI tokens 409
FortiAI example tasks 413
Example 1: Performing log analysis and filtering 413
Example 2: Performing security reputation checks 416
Example 3: Rendering charts 417
Example 4: Creating an event handler 418
Example 5: Identifying incidents and compromised hosts 420
Example 6: Gathering system process information 421
Example 6: Quarantining an endpoint 423
Example 7: Generating an incident report 424
Reports 425
How reports are populated 425
How ADOMs affect reports 427
Predefined reports, templates, charts, and macros 427
Logs used for reports 428
How charts and macros extract data from logs 428
Report guidance 429
How auto-cache works 429
Generating reports 430
Viewing completed reports 430
Enabling auto-cache 431
Grouping reports 431
Retrieving report diagnostic logs 432
Auto-Generated Reports 433
Scheduling reports 433
Creating reports 433
Creating reports from report templates 433
Creating reports by cloning and editing 434
Creating reports without using a template 435
Reports Settings tab 435
Customizing report cover pages 438
Reports Editor tab 440
Filtering report output 442
Managing reports 444
Organizing reports into folders 445
Importing and exporting reports 446
Report template library 447
Creating report templates 447
Viewing sample reports for predefined report templates 448
Managing report templates 448
List of report templates 449
Chart library 457
Creating charts 457
Managing charts 460
Macro library 460
Creating macros 461
Managing macros 461
Datasets 462

Creating datasets 462
Viewing the SQL query of an existing dataset 465
SQL query functions 465
Managing datasets 466
Aliases and metadata tables 467
Output profiles 469
Creating output profiles 469
Managing output profiles 471
Report languages 471
Exporting and modifying a language 471
Importing a language 472
Deleting a language 472
Report calendar 473
Viewing all scheduled reports 473
Managing report schedules 473
System Settings 475
Logging Topology 475
Network 476
Configuring network interfaces 477
Disabling ports 478
Changing administrative access 478
Static routes 480
Packet capture 480
Aggregate links 481
VLAN interfaces 482
SNMP 483
RAID Management 493
Supported RAID levels 493
Configuring the RAID level 496
Monitoring RAID status 496
Swapping hard disks 497
Adding hard disks 498
Administrative Domains (ADOMs) 498
Root ADOM 499
Default device type ADOMs 499
Organizing devices into ADOMs 500
FortiClient support and ADOMs 500
Enabling and disabling the ADOM feature 502
ADOM device modes 503
Managing ADOMs 504
Fabric Management 509
Storage connectors 509
Certificates 511
Local certificates 511
CA certificates 516
Certificate revocation lists 517
Log Forwarding 518
Modes 518

Configuring log forwarding 519
Output profiles 523
Managing log forwarding 524
Log forwarding buffer 525
Log forwarding to SOCaaS 526
Log Fetching 529
Fetching profiles 529
Fetch requests 531
Synchronizing devices and ADOMs 532
Fetch monitoring 533
Event Log 534
Event log filtering 535
Task Monitor 536
Mail Server 537
Syslog Server 539
Send local logs to syslog server 540
Meta Fields 541
Device logs 542
Configuring rolling and uploading of logs using the GUI 543
Configuring rolling and uploading of logs using the CLI 545
Upload logs to cloud storage 546
Miscellaneous Settings 547
FortiGuard 548
Subscribing FortiAnalyzer to FortiGuard 548
Licensing in an air-gap environment 548
Enabling updates through a web proxy 552
Administrators 554
Trusted hosts 554
Monitoring administrators 555
Disconnecting administrators 555
Managing administrator accounts 555
Creating administrators 557
Editing administrators 561
Deleting administrators 562
Override administrator attributes from profiles 563
Creating administrators for the FortiAnalyzer API 564
Administrator profiles 566
Permissions 567
Privacy Masking 568
Creating administrator profiles 570
Creating administrator profiles for incident & event management 571
Editing administrator profiles 571
Cloning administrator profiles 572
Deleting administrator profiles 572
Authentication 572
Public Key Infrastructure 573
Managing remote authentication servers 574

LDAP servers 576
RADIUS servers 578
TACACS+ servers 579
Remote authentication server groups 580
SAML admin authentication 581
FortiCloud SSO admin authentication 584
Global administration settings 586
Password policy 588
Enhanced administrator password security 589
Password lockout and retry attempts 592
GUI language 593
Idle timeout 593
Security Fabric authorization information for FortiOS 594
Control administrative access with a local-in policy 594
Multi-factor authentication 595
Multi-factor authentication with FortiAuthenticator 595
Multi-factor authentication with FortiToken Cloud 599
High Availability 602
Configuring HA options 602
Log synchronization 605
Configuration synchronization 606
Geo-redundant HA 607
Monitoring HA status 611
If the primary unit fails 611
Load balancing 612
Upgrading the FortiAnalyzer firmware for an operating cluster 612
Collectors and Analyzers 613
Configuring the Collector 613
Configuring the Analyzer 614
Fetching logs from the Collector to the Analyzer 615
Appendix A - Supported RFC Notes 616
Appendix B - Log Integrity and Secure Log Transfer 618
Log Integrity 618
Configuring log integrity settings 618
Verifying log-integrity 618
Secure Log Transfer 619
Configuring secure log transfer settings 620
Log caching with secure log transfer enabled 620
Supported ciphers 622
Maximum TLS/SSL version compatibility 626
Appendix C - FortiAnalyzer Ansible Collection documentation 628
Appendix D - FortiAI token entitlements for FortiAnalyzer 629

Change Log

Date	Change Description
2025-08-25	Initial release.
2025-08-28	Updated Configuring security fabric connectors on page 372 and Blocking indicators on page 334.
2025-09-02	Updated Auto-Generated Reports on page 433.
2025-09-10	Updated Configuring incident settings on page 212.
2025-09-17	Updated Microsoft 365 Defender connector on page 345.
2025-09-18	Added: • Syslog logs on page 148 • Fabric logs on page 151 • Log parsers on page 151
2025-09-19	Updated Updating the system firmware on page 54.
2025-10-14	Updated Configuring rolling and uploading of logs using the GUI on page 543. Removed "File Management".
2025-10-16	Updated Creating administrators for the FortiAnalyzer API on page 564.
2025-10-21	Updated Configuring security fabric connectors on page 372.
2025-10-30	Updated Playbook examples on page 386.
2025-11-20	Updated Activating VM licenses on page 20.
2025-11-27	Updated Configuration synchronization on page 606.
2026-01-05	Updated Endpoint vulnerability dashboard on page 80.
2026-01-09	Updated Configuring the webhook on page 325.
2026-01-12	Updated Outbreak Alerts on page 352.
2026-03-09	Updated Configuring HA options on page 602.

Setting up FortiAnalyzer

This chapter provides information about performing some basic setups for your FortiAnalyzer units.

This section contains the following topics:

- Connecting to the GUI on page 13
- Security considerations on page 22
- GUI overview on page 30
- Target audience and access level on page 38
- Initial setup on page 39
- FortiManager features on page 39
- Next steps on page 40
- Restarting and shutting down on page 40

Connecting to the GUI

The FortiAnalyzer unit can be configured and managed using the GUI or the CLI. This section will step you through connecting to the unit via the GUI.



If you are connecting to the GUI for a FortiAnalyzer virtual machine (VM) for the first time, you are required to activate a license. See Activating VM licenses on page 20.

To connect to the GUI:

1. Connect the FortiAnalyzer unit to a management computer using an Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiAnalyzer unit:
   - IP address: `192.168.1.X`
   - Netmask: `255.255.255.0`
3. On the management computer, start a supported web browser and browse to `https://192.168.1.99`.
   The login dialog box is displayed.
4. Type admin in the *Name* field, leave the *Password* field blank, and click *Login*.
   The *FortiAnalyzer Setup* wizard is displayed.
5. Click *Begin* to start the setup process. See FortiAnalyzer Setup wizard on page 14.
   The *Later* option is available for certain steps in the wizard, allowing you to postone steps. The *Register with FortiCare* step cannot be skipped and must be completed before you can access the FortiAnalyzer appliance or VM.
6. If ADOMs are enabled, the *Select an ADOM* pane is displayed. Click an ADOM to select it.

The FortiAnalyzer home page is displayed.

7. Click a tile to go to that pane. For example, click the *Device Manager* tile to go to the *Device Manager* pane. See also GUI overview on page 30.



If the network interfaces have been configured differently during installation, the URL and/or permitted administrative access protocols (such as HTTPS) may no longer be in their default state.

For information on enabling administrative access protocols and configuring IP addresses, see Configuring network interfaces on page 477.



If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see Static routes on page 480.

After logging in for the first time, you should create an administrator account for yourself and assign the *Super_User* profile to it. Then you should log into the FortiAnalyzer unit by using the new administrator account. See Managing administrator accounts on page 555 for information.

FortiAnalyzer Setup wizard

When you log in to FortiAnalyzer, the FortiAnalyzer Setup wizard is displayed to help you set up FortiAnalyzer by performing the following actions:

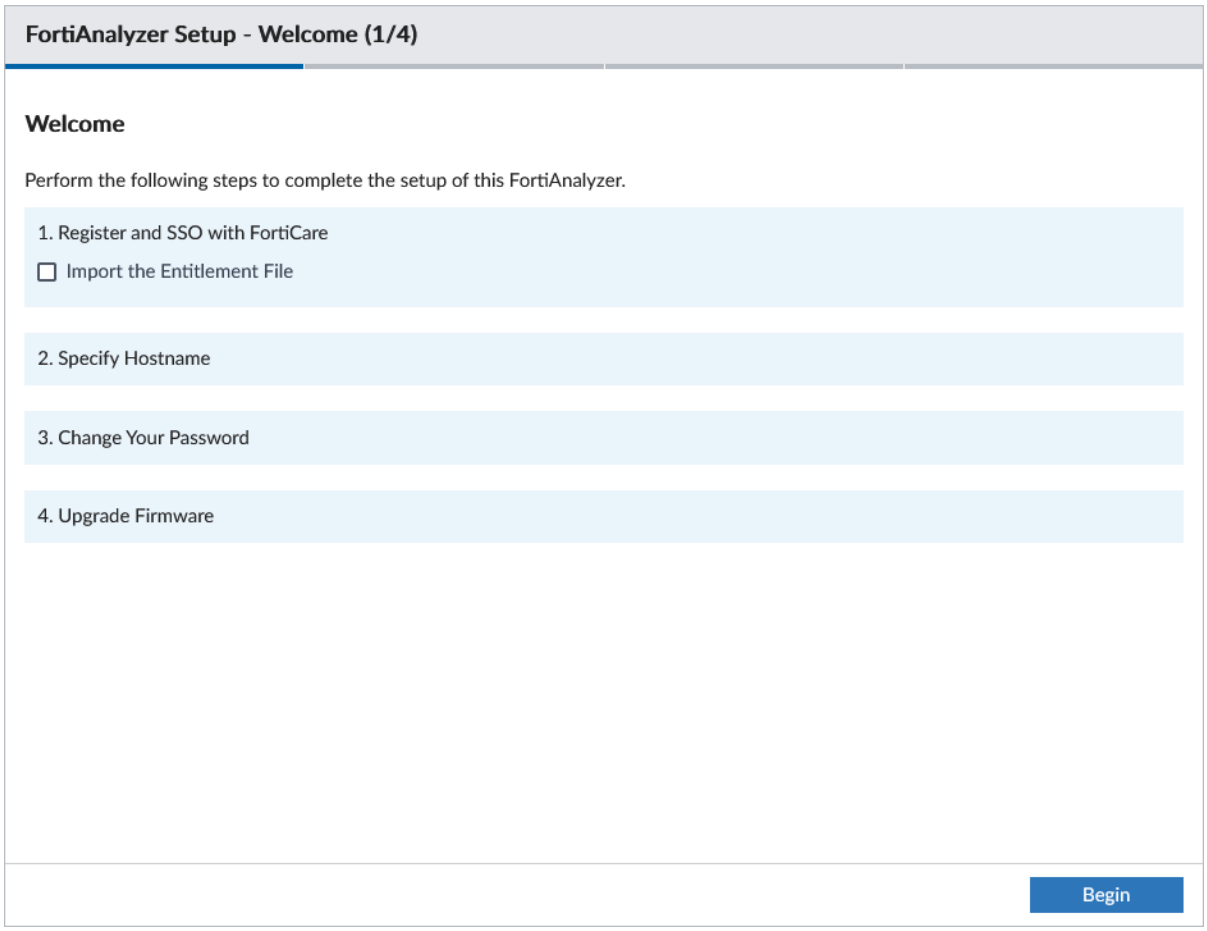
- Registering with FortiCare and enabling FortiCare single sign-on
- Specifying the hostname
- Changing your password
- Upgrading firmware (when applicable)

You can choose whether to complete the wizard now or later.



The FortiAnalyzer Setup wizard requires that you complete the *Register with FortiCare* step before you can access the FortiAnalyzer appliance or VM.

When actions are complete, a green checkmark displays beside them in the wizard, and the wizard no longer displays after you log in to FortiAnalyzer.



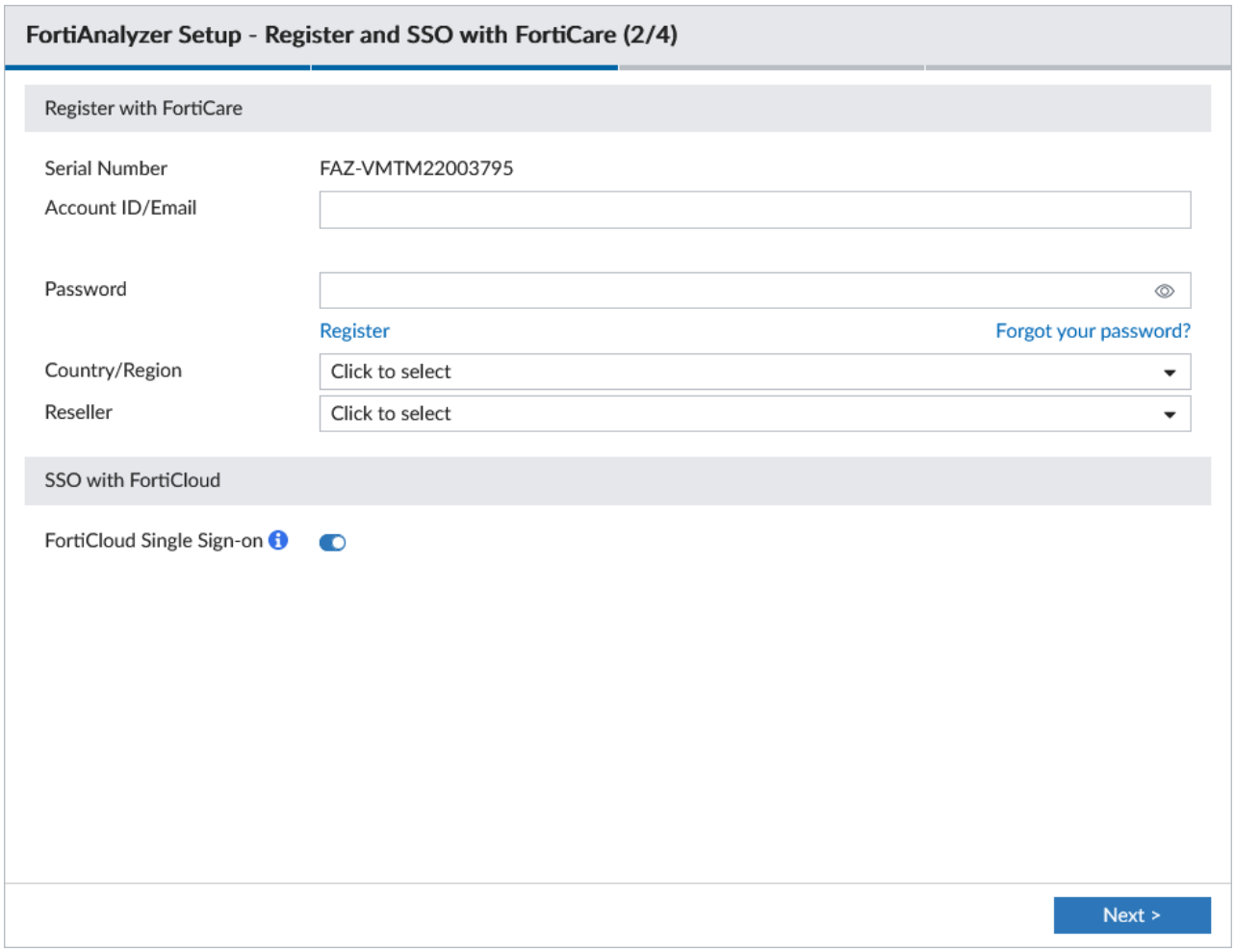
This topic describes how to use the *FortiAnalyzer Setup* wizard.

To use the FortiAnalyzer setup wizard:

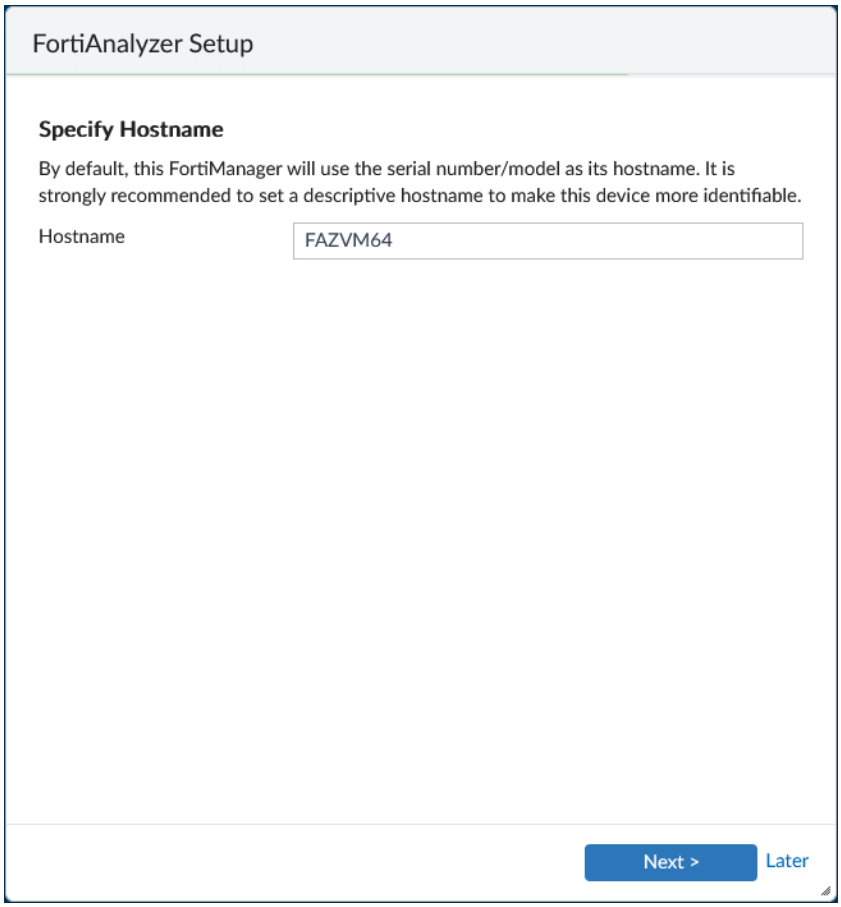
1. Log in to FortiAnalyzer.
   The *FortiAnalyzer Setup* dialog box is displayed.
2. Click *Begin* to start the setup process now.
   Alternately, click *Later* to postpone the setup tasks. Some tasks cannot be postponed.
3. When prompted, register with FortiCare and enable FortiCare single sign-on. You must complete the *Register with FortiCare* step before you can access the FortiAnalyzer appliance or VM.



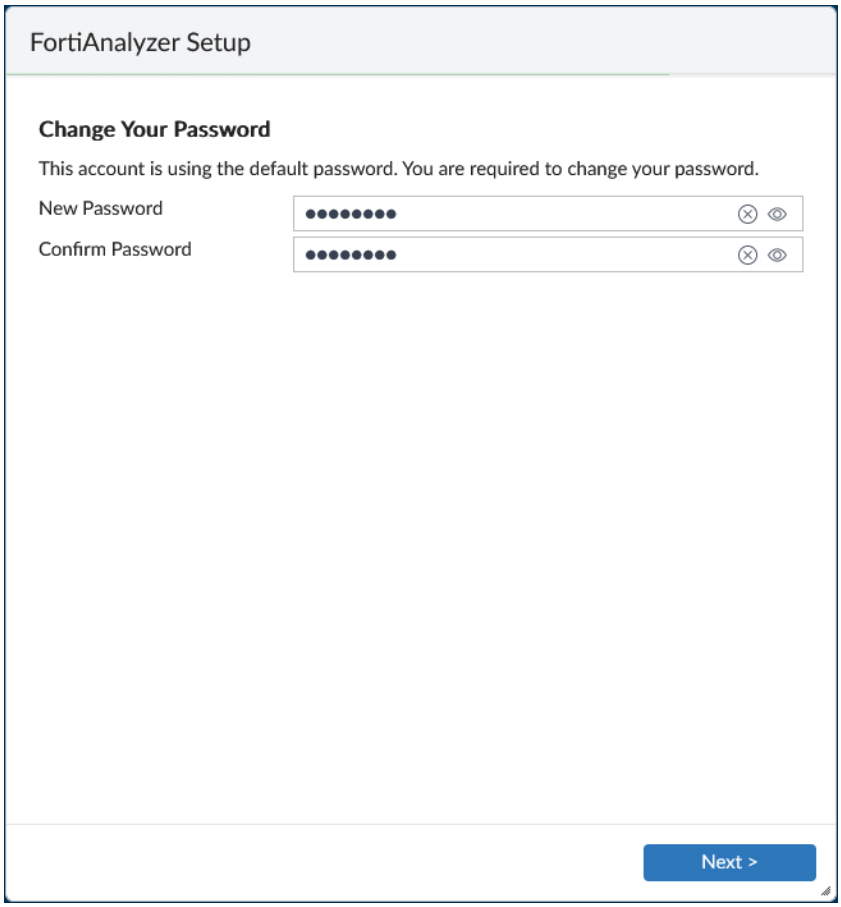
When using FortiAnalyzer in an air-gapped environment, you must manually import your *Entitlement File*. See Licensing in an air-gap environment on page 548.



4. When prompted, specify the hostname.



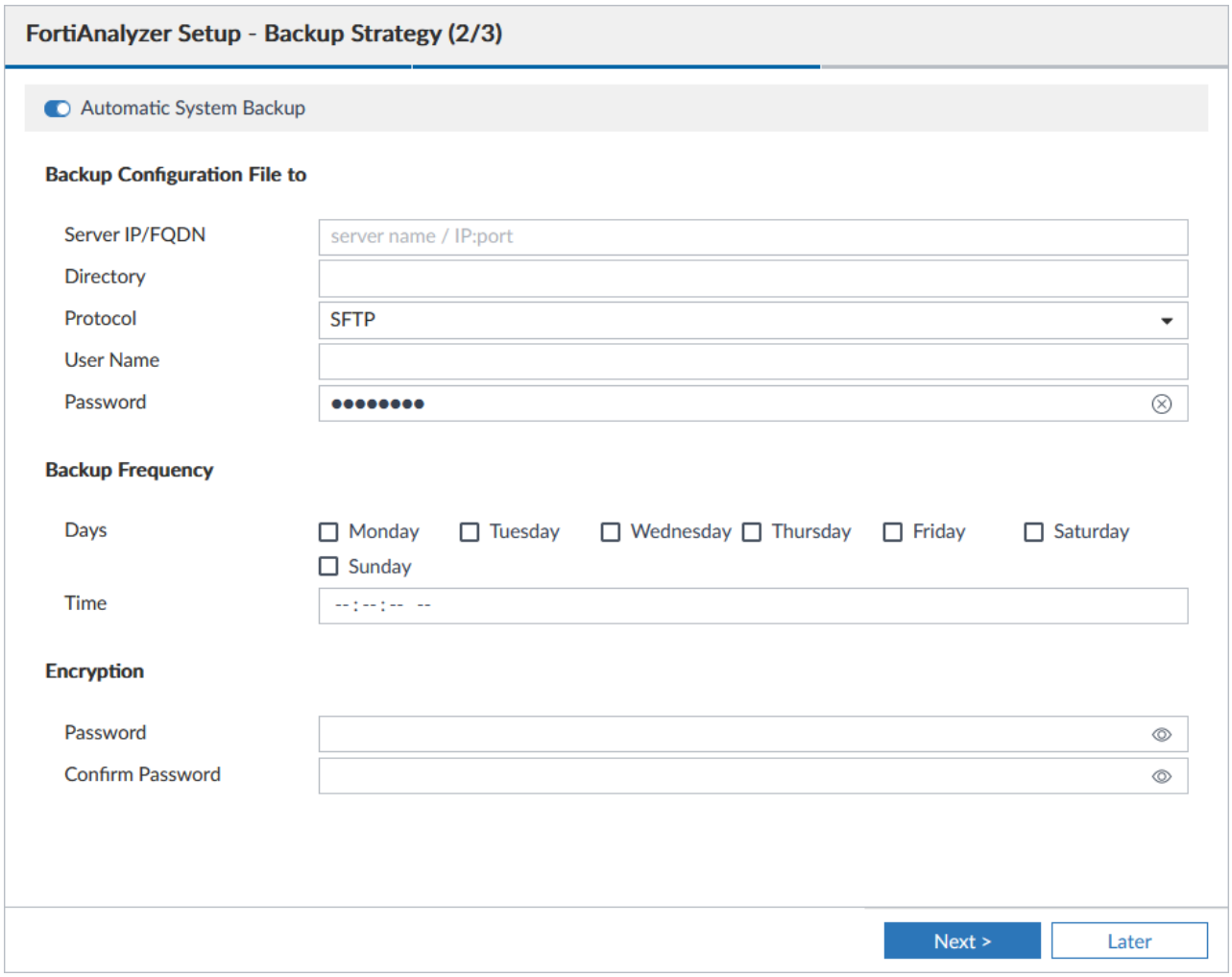
5. In the *Hostname* box, type a hostname.
6. Click *Next*.
7. When prompted, change your password.



By default, the password must be at least 8 characters and must contain uppercase letter(s), lowercase letter(s), number(s), and special character(s).

For more information about the password policy, see Password policy on page 588.

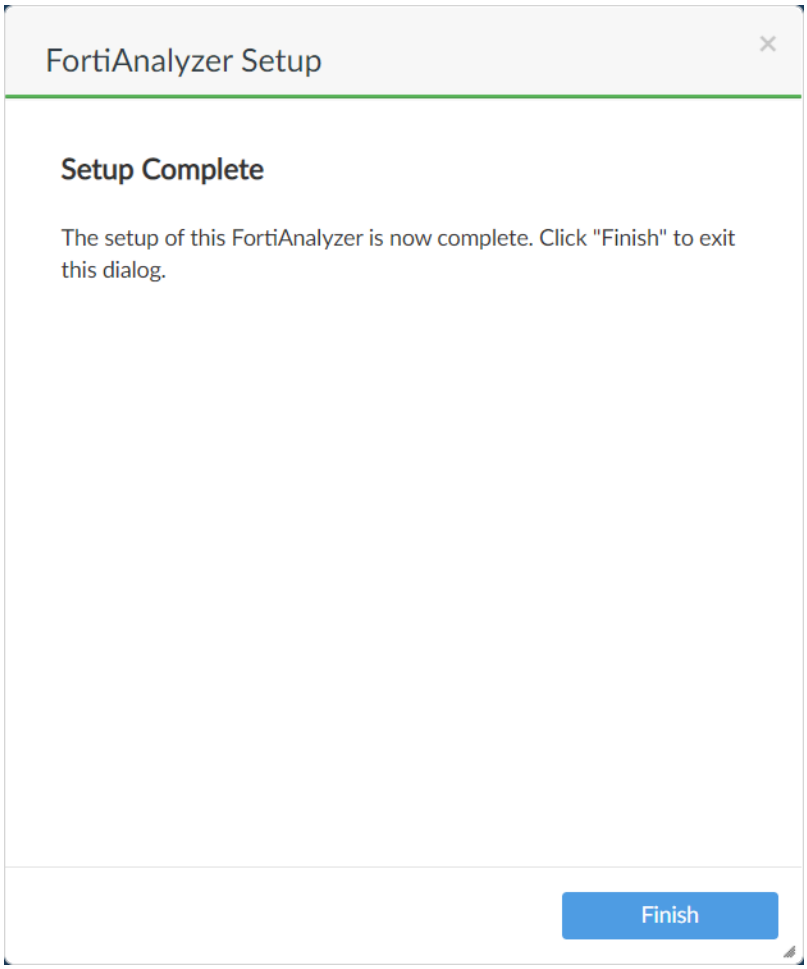
   a. In the *Confirm Password* box, type the new password again.
   b. Click *Next*.
8. When a new firmware version is available for your device on FortiGuard, the *Upgrade Firmware* option in the wizard indicates that a new version is available, and you can click *Next* to upgrade to the new firmware, or *Later* to upgrade later.
9. Configuration of a backup strategy is recommended as part of the initial configuration of your FortiAnalyzer. When prompted, you can optionally configure your backup settings.



a. *Automatic System Backup* is enabled by default. Configure the following to specify your backup settings, or disable automatic backups.

- In *Backup Configuration File to*, configure where the backup file will be sent.
- In *Backup Frequency*, select when the day(s) and time for the backup to be performed.
- In *Encryption*, set an encryption password.

10. Complete the setup by clicking *Finish*.



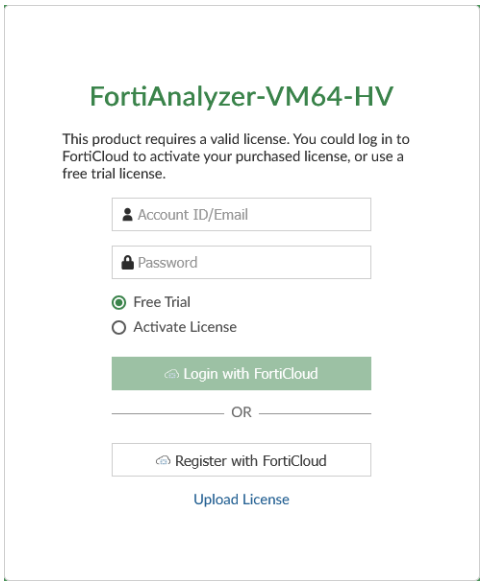
You are logged in to FortiAnalyzer.

Activating VM licenses

If you are logging in to a FortiAnalyzer VM for the first time by using the GUI, you are required to activate a purchased license or activate a trial license for the VM. Before activating your license on FortiAnalyzer, you must register it on FortiCloud. See Registering Assets.

To activate a license for FortiAnalyzer VM:

1. On the management computer, start a supported web browser and browse to `https://<ip address>` for the FortiAnalyzer VM.
   The login dialog displays.



2. Take one of the following actions:

Action	Description
Free Trial	If a valid license is not associated with your FortiCloud account, you can start a free trial license. 1. In the *Account ID/Email* field, enter the account ID or email for your FortiCloud account. 2. In the *Password* field, enter the password for your FortiCloud account. 3. Select *Free Trial*, and then click *Login with FortiCloud*. FortiAnalyzer connects to FortiCloud to get the trial license. The system will restart to apply the trial license. 4. Read and accept the license agreement. For more information, see the *FortiAnalyzer VM Trial License Guide*.
Activate License	If you have a license certificate, you can activate the license using the registration code. 1. In the *Account ID/Email* field, enter the account ID or email for your FortiCloud account. 2. In the *Password* field, enter the password for your FortiCloud account. 3. Select *Activate License*, and then click *Login with FortiCloud*. FortiAnalyzer connects to FortiCloud, and the license agreement is displayed. 4. In the *Registration Code* field, enter the registration code included in your license certificate. 5. In the *IP Address* field, enter the static IP address used for the FortiAnalyzer VM. 6. Read and accept the license agreement. For more information, see the FortiCloud Services Asset Management Admin Guide in the Fortinet Document Library.

Action	Description
Register with FortiCloud	If you do not have a FortiCloud account, you can create one. 1. Click *Register with FortiCloud*. 2. Follow steps to create a new FortiCloud account. For more information, see the FortiCloud Account User Guide in the Fortinet Document Library. 3. Once created, you can proceed to activate a license or a free trial for the FortiAnalyzer VM.
Upload License	If you have the license file (.lic), you can upload the license. 1. Click *Upload License*. 2. Click *Browse* to upload the license file, or drag it onto the field. 3. Click *Upload*. After the license file is uploaded, the system will restart to verify it. This may take a few moments.  To download the license file, go to the Fortinet Technical Support site (https://support.fortinet.com/), and use your FortiCloud credentials to log in. Go to *Asset* > *Manage/View Products*, then click the product serial number. For more information, see the FortiCloud Services Asset Management Admin Guide in the Fortinet Document Library. If you are using this method to license the device in an air-gap environment, see Licensing in an air-gap environment on page 548

Security considerations

You can take steps to prevent unauthorized access and restrict access to the GUI. This section includes the following information:

- Restricting GUI access by trusted host on page 22
- Trusted platform module support on page 23
- Self-encrypting drives on page 24
- UEFI secure boot on page 27
- Real time file system integrity checking on page 30
- Other security considerations on page 30

Restricting GUI access by trusted host

To prevent unauthorized access to the GUI you can configure administrator accounts with trusted hosts. With trusted hosts configured, the administrator user can only log into the GUI when working on a computer with the

trusted host as defined in the administrator account. You can configure up to ten trusted hosts per administrator account. See Administrators on page 554 for more details.

Trusted platform module support

On supported FortiAnalyzer hardware devices, the Trusted Platform Module (TPM) is used to protect system against malicious attacks.

The dedicated module hardens the FortiAnalyzer by storing your `master-encryption-password` which is created when the private data encryption feature is enabled. For more information about which models feature TPM support, see the FortiAnalyzer Data Sheet.

By default, the TPM is disabled. To enable it, you must enable `private-data-encryption` and set the 32 hexadecimal digit `master-encryption-password`.

When private data encryption is enabled, the `master-encryption-password` is used to generate a primary key which encrypts and protects the individual passwords stored on the FortiAnalyzer (for example, FortiAnalyzer Admin passwords, HA passwords, SNMP passwords, and others). These individual passwords are not stored within the TPM themselves.

The primary key is never displayed in the FortiAnalyzer backup file or the system CLI, thereby obscuring the information and leaving the encrypted information in the TPM.



The TPM module does **not** encrypt the disk drive of eligible FortiAnalyzer.

Configuration backups and migrations

The primary key binds the encrypted backup file to a specific FortiAnalyzer unit and never leaves the TPM. When backing up the configuration, the TPM uses the key to encrypt the master-encryption-password in the FortiAnalyzer backup file. When restoring a configuration that includes a TPM protected master-encryption-password:

- If TPM is enabled but has a different master-encryption-password than the FortiAnalyzer backup file, then the configuration cannot be restored.
- If TPM is enabled and the master-encryption-password is the same in the FortiAnalyzer backup file, then the configuration can be restored.

For information on backing up and restoring the configuration, see Backing up the system on page 57 and Restoring the configuration on page 61.

The master-encryption-password is also required when migrating the configuration, regardless if TPM is available on the other FortiAnalyzer model. For more information, see

Migrating the configuration on page 61.

To check if your FortiAnalyzer device has a TPM:

Enter the following command in the FortiAnalyzer CLI:

```
diagnose hardware info
```

The output in the CLI includes `### TPM info`, which displays if the TPM is detected (enabled), not detected (disabled), or not available.

To enable TPM and input the master-encryption-password:

Enter the following command in the FortiAnalyzer CLI:

```
config system global
   set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
Your private data encryption key is accepted.
```

Self-encrypting drives

Self-encrypting drives (SED) are supported for the following models:

- FortiAnalyzer-810G
- FortiAnalyzer-1000G
- FortiAnalyzer-3100G
- FortiAnalyzer-3510G

The following type of key is supported for SED in FortiAnalyzer:

- **Encryption key**: This key can only be changed/created by the user. Exercise caution when changing the encryption key because all of the data previously written to the drive will now be read and decrypted using the new key; therefore, it will become unrecoverable if the user forgets the new key during restoration. However, this is an effective technique for rendering data on the disk unusable and unreadable. It is referred to as an auto-lock feature, which is useful if a drive has to be repurposed (used in a different application where the data is neither required nor wanted) or scrapped.

The SED features are only available using the CLI, not the GUI.

Auto-lock feature

To protect the disk's contents, assign the SED encryption key after RAID has been setup. The disk's contents are protected if plugged into a system unless the encryption key is known and the system supports a similar RAID controller.

To use the auto-lock feature:

1. After RAID setup, enter the following command in the FortiAnalyzer CLI:
   ```
   diagnose system disk sed {sed-key}
   ```
   The key requires 8-32 characters, and it must include upper case, lower case, number, and special character (excluding '\).



If a foreign SED disk is installed, this disk will be unavailable due to auto-lock feature.

Cryptographic erase

To quickly and securely dispose of disks, you can format the drives from the CLI and then use the auto-lock feature.

To complete a cryptographic erase:

1. In the FortiAnalyzer CLI, enter the following command:
   ```
   execute format disks {raid-level}
   ```
2. In the FortiAnalyzer CLI, apply the auto-lock by entering the following command:
   ```
   diagnose system disk sed {sed-key}
   ```

Examples

SED feature disabled

```
diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 52156GB
File System: ext4 51337GB
SED Encryption: Disabled
Groups: 2

Disk 1: OK 3724GB Group-1
Disk 2: OK 3724GB Group-1
Disk 3: OK 3724GB Group-1
```

If there are non-SED disks, they are displayed in the output. For example:

```
diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 52156GB
File System: ext4 51337GB
SED Encryption: Disabled
Groups: 2

Disk 1: OK 3724GB Group-1
Disk 2: OK 3724GB Group-1 non-SED
Disk 3: OK 3724GB Group-1
```

SED feature enabled

1. Use the following command to provide the SED key:
   ```
   diagnose system raid sed {sed-key}
   ```

Variable	Description
sed-key	SED encryption key. 8-32 chars, must include upper case, lower case, number and special chars (exclude '\).

2. Use the following command to verify SED encryption status:
   ```
   diagnose system raid status
   Storcli RAID:
   RAID Level: Raid-50
   RAID Status: OK
   RAID Size: 22353GB
   File System: ext4 22001GB
   SED Encryption: Enabled
   Groups: 2

   Disk 1: OK 3724GB Group-1
   Disk 2: OK 3724GB Group-1
   Disk 3: OK 3724GB Group-1
   Disk 4: OK 3724GB Group-1
   Disk 5: OK 3724GB Group-2
   ```

Working with SED-based systems

To replace an SED disk:

You can replace disks that supports SED feature, regardless of brand, however it's optimal to use the same specification of hard drive in the existing array. The new disk will be automatically rebuilt by the system and it will have the same SED key used by the existing system. This will be transparent for the user.

To reformat after an SED-enabled RAID failure:

If an SED-enabled RAID failure occurs, formatting the drives will effectively clear the SED key. Thus, the user can assign an SED key. For example, see below.

```
FMG-410G # diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: Failed
RAID Size: 22353GB
File System: ext4 22001GB
SED Encryption: Enabled
Groups: 2

Disk 1: OK 3724GB Group-1
Disk 2: OK 3724GB Group-1
Disk 3: OK 3724GB Group-1
Disk 4: OK 3724GB Group-1
Disk 5: OK 3724GB Group-2
Disk 6: OK 3724GB Group-2
```

```
Disk 7: Unused 3724GB
Disk 8: Unused 3724GB Group-2

FMG-410G # execute format disk 50
This operation will format hard disk to ext4 filesystem.
Do you want to continue? (y/n)y

Resetting ...

login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

FMG-410G # diagnose system raid status
Storcli RAID:
RAID Level: Raid-50
RAID Status: OK
RAID Size: 22353GB
File System: ext4 22001GB
SED Encryption: Disabled
Groups: 2

Disk 1: OK 3724GB Group-1
Disk 2: OK 3724GB Group-1
Disk 3: OK 3724GB Group-1
Disk 4: OK 3724GB Group-1
Disk 5: OK 3724GB Group-2
Disk 6: OK 3724GB Group-2
Disk 7: OK 3724GB Group-2
Disk 8: OK 3724GB Group-2
```

To move SED-enabled disks to a new physical chassis:

In situations where SED-enabled disks need to be moved (re-homed) to a new physical chassis, the process will require additional steps. See below.

1. On the target unit, install the same build as the source unit. Install SED capable drives and setup the RAID similar to that of the source unit, and then enable SED using the same key as that of the source unit.
2. Shutdown both units and remove the drives from their respective chassis.
3. Move the source drives and install them to the target chassis.

UEFI secure boot

The BIOS-level signature and integrity checking enforces each FortiAnalyzer GA firmware image, AV engine file, and IPS engine file to be dually-signed by the Fortinet CA and a third-party CA. The BIOS verifies that each file matches their secure hash as indicated by their certificates. Users are warned when there is a failed integrity check, and the system may be prevented from booting depending on the severity and the BIOS security level.

Signature checking occurs when the FortiAnalyzer firmware, AV, and IPS engine files are uploaded. This allows the FortiAnalyzer to warn users of potential risks involved with uploading an unauthenticated file.

The outcome of the signature and integrity check depends on the security level configured in BIOS and the certificate authority that signed the file.

The following table summarizes the use cases and the potential outcome based on the security level.

Use case	Certificate signed by		Outcome based on security level		
	Fortinet CA	Third-party CA	Level 2	Level 1	Level 0
GA-Certified (GA firmware, Beta firmware, Top3 final builds)	Yes	Yes	Accept	Accept	Accept
Non-GA certified (Special builds: Top3 and NPI quick builds)	Yes	No	Warning	Accept	Accept
Interim and Dev builds, or unknown build	No	Yes or No	Reject	Warning	Accept

The FortiAnalyzer secure boot feature supports the following security levels:

- Level 2: in order to operate normally, FortiAnalyzer requires all file signatures to match their secure checksums as indicated on both Fortinet and third-party CA signed certificates.
  - If a file has a Fortinet CA signed certificate but no third-party signed certificates, then FortiAnalyzer can still run but displays a warning in the GUI and CLI.
  - If a file has no valid certificate signed by the Fortinet CA, then FortiAnalyzer is not allowed to run.
- Level 1: in order to operate normally, FortiAnalyzer only requires all file signatures to match their secure checksums as indicated on the Fortinet CA signed certificate.
  - If a file has no valid certificate signed by the Fortinet CA, then FortiAnalyzer can still run but displays a warning in the GUI and CLI.
- Level 0 (not recommended): FortiAnalyzer does not perform code verification.

On FortiAnalyzer without supported BIOS security levels, the device acts like security level 1. For example, on a FortiAnalyzer-VM that does not have BIOS, the security level is defaulted to level 1.

Models that support BIOS security levels:

The following FortiAnalyzer models support setting the security level in the BIOS as of the release of FortiAnalyzer 7.6.4.

- FAZ-810G
- FAZ-1000G
- FAZ-3100G

To verify the security level:

```
# get system status
Version: vx.x.x-buildxxxx xxxxxx (GA)
Secure Boot: Enabled
Security Level: 2
Image Signature: Image is GA Certified
```

To change the security level:

```
Version 2.20.1271. Copyright (C) 2023 American Megatrends, Inc.
BIOS Date: 06/30/2023 Ver: C1820J0B
Press <DEL> or <ESC> to enter setup.
FortiBootLoader

Loading Device Drivers
FortiAnalyzer-810G (21:52-07.17.2023)
Ver:00030003
Serial number:FAZ*************

Total RAM: 32768MB
Boot up, boot device capacity: 15272MB.
Press any key to display configuration menu...   <<============= Press any key when this message
is displayed
......
[C]:  Configure TFTP parameters.
[R]:  Review TFTP parameters.
[T]:  Initiate TFTP firmware transfer.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  System configuration and information.      <<============= Choose System configuration and
information
[Q]:  Quit menu and continue to boot.
[H]:  Display this list of options.

Enter C,R,T,F,B,I,Q,or H:
[T]:  Set menu timeout.
[U]:  Set security level.
[Q]:  Quit menu and continue to boot.
[H]:  Display this list of options.

Enter T,U,Q,or H:
[0]:  Level 0
[1]:  Level 1
[2]:  Level 2
Enter security level setting [1]:2
```



Serial console access to the device is required in order to change the security level settings.

Real time file system integrity checking

Real time file system integrity checking has 2 main purposes.

1. Prevent unauthorized modification of important binaries.
2. Detect unauthorized binaries and prevent them from running.

How it works

When the FortiAnalyzer boots, the system performs a BIOS level integrity check on important internal files. These files are signed and BIOS verifies their signature against their certificates.

Once these files are verified to be authentic, the BIOS can boot the root filesystem and other executables and libraries. Once loaded, real time protection begins. The important executables and binaries are protected from write access and any sort of modifications. Also, it blocks the kernel from loading any modules . Any unauthorized loading of modules will be blocked. If violations are found, logs are triggered.

A hash of all executable binaries and libraries are taken and stored in memory . When there is a hash mismatch when attempting to run a binary, that binary is blocked from running and the system is rebooted.

When there is a missing hash when attempting to run a binary, then the system will be rebooted.

Other security considerations

Other security consideration for restricting access to the FortiAnalyzer GUI include the following:

- Configure administrator accounts using a complex passphrase for local accounts
- Configure administrator accounts using RADIUS, LDAP, TACACS+, or PKI
- Configure the administrator profile to only allow read/write permission as required and restrict access using read-only or no permission to settings which are not applicable to that administrator
- Configure the administrator account to only allow access to specific ADOMs as required

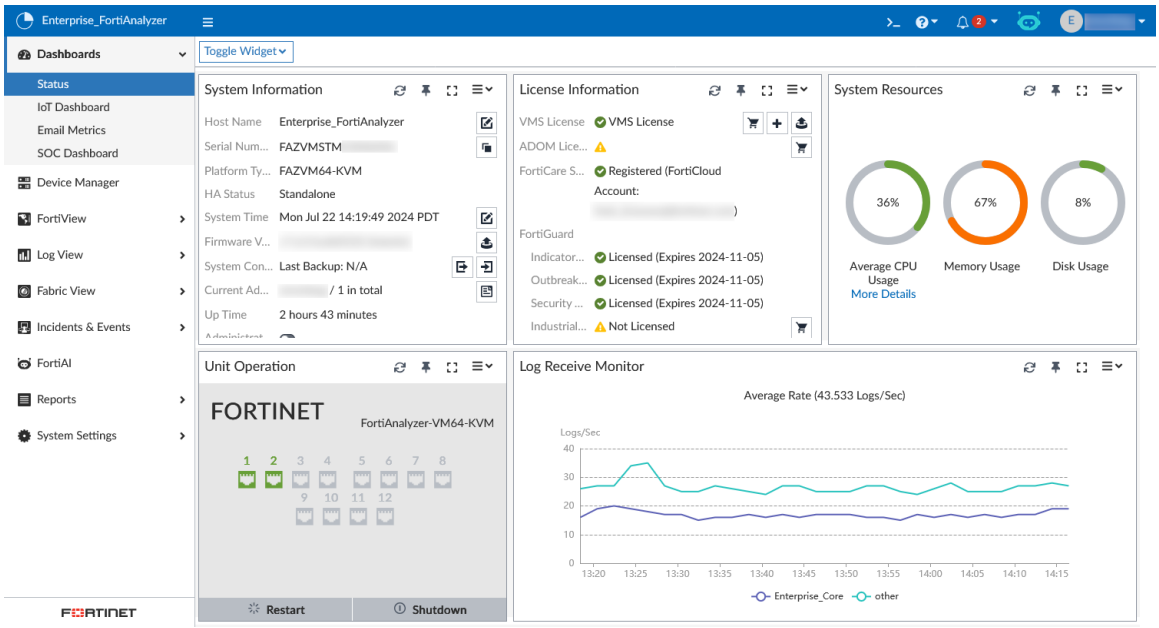


When setting up FortiAnalyzer for the first time or after a factory reset, the password cannot be left blank. You are required to set a password when the *admin* user tries to log in to FortiManager from GUI or CLI for the first time. This is applicable to a hardware device as well as a VM. This is to ensure that administrators do not forget to set a password when setting up FortiAnalyzer for the first time.

After the initial setup, you can set a blank password from *System Settings* > *Administrators*.

GUI overview

When you log into the FortiAnalyzer GUI, the *Dashboard* pane is displayed. The *Dashboard* contains widgets that provide performance and status information. For more information about the *Dashboard*, see Dashboards on page 49



Use the navigation menu on the left to open another pane. The available panes vary depending on the privileges of the current user.

Device Manager	Add and manage devices and VDOMs. See Device Manager on page 83.
FortiView	Summarizes SOC information in *FortiView* and *Monitors* dashboards, which include widgets displaying log data in graphical formats, network security, WiFi security, and system performance in real-time. This pane is not available when the unit is in *Collector* mode.
Log View	View logs for managed devices. You can display, download, import, and delete logs on this page. You can also define custom views and create log groups. See Log View and Log Quota Management on page 146.
Fabric View	
Incidents & Events	Configure and view events for logging devices. See Incidents & Events on page 204. Configure fabric connectors and playbook automation. Playbook automation requires a FortiSoC subscription service. See Automation on page 362. This pane is not available when the unit is in Collector mode.
FortiAI	Use the FortiAI assistant. See FortiAI on page 402.
Reports	Generate reports. You can also configure report templates, schedules, and output profiles, and manage charts and datasets. See Reports on page 425. This pane is not available when the unit is in Collector mode.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See System Settings on page 475.

The banner at the top of the screen is available in every pane.

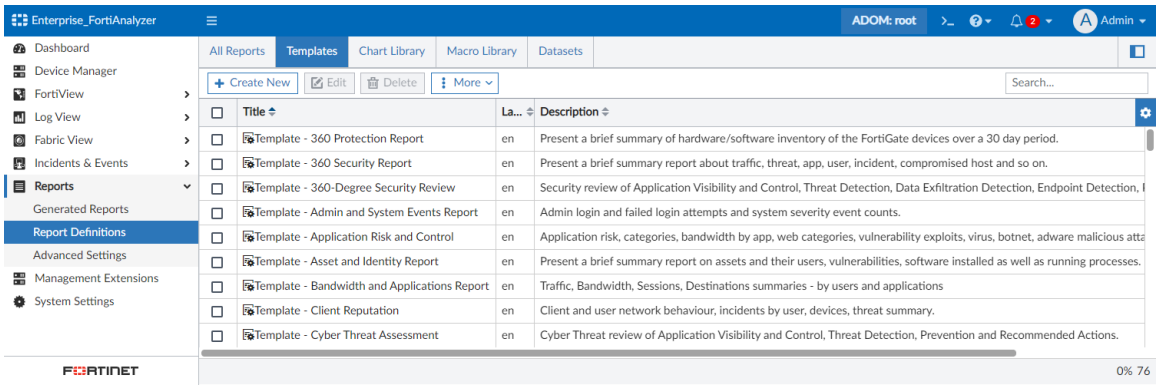
The following options are available in the banner:

<table>
<tr><td>Menu</td><td>Click to collapse or expand the navigation menu on the left.
When collapsed, you can mouse over the icons to view the available panes.</td></tr>
<tr><td>ADOM</td><td>If ADOMs are enabled, the required ADOM can be selected from the dropdown list.
The ADOMs available from the ADOM menu will vary depending on the privileges of the current user.</td></tr>
<tr><td>CLI Console</td><td>Open the CLI console to configure the FortiAnalyzer unit using CLI commands directly from the GUI, without making a separate SSH, or local console connection to access the CLI.
For more information, see Using the CLI console on page 35.
Note: The CLI Console requires that your web browser support JavaScript.</td></tr>
<tr><td>Online Help</td><td>Click to open the FortiAnalyzer online help dropdown which contains the following options:<table><tr><td>Relevant Documentation</td><td>Opens related online help topics on the Fortinet Document Library.
This option is context-sensitive, so it will open to the relevant documentation for the pane you are in.</td></tr><tr><td>Video Tutorials</td><td>Opens the Fortinet Video Library.</td></tr><tr><td>Release Notes</td><td>Opens the FortiAnalyzer's Release Notes for the current version.</td></tr><tr><td>FortiAnswers</td><td>Opens the Fortinet Community.</td></tr><tr><td>FortiCare Debug Report</td><td>Runs the <code>execute tac report</code> CLI command and downloads a local copy of the report.</td></tr></table>You can also open the FortiAnalyzer basic setup video (https://video.fortinet.com/products/fortianalyzer/6.2/).</td></tr>
<tr><td>Notifications</td><td>Click to display a list of notifications. Select a notification from the list to take action on the issue.</td></tr>
<tr><td>FortiAI assistant</td><td>Open the FortiAI Assistant pane. This feature requires a license.
For more information, see FortiAI on page 402.</td></tr>
<tr><td>admin</td><td>From this dropdown, you can:
view the current firmware build of your FortiAnalyzer device.
upgrade the firmware.
open the Process Monitor.
change your password.
update your profile information, including the avatar and theme.
log out of the GUI.</td></tr>
</table>

Panes

In general, each pane four primary parts: the banner, toolbar, tree menu, and content pane.

Banner	Along the top of the page. The banner includes the device name (next to the Fortinet logo) and options to open/close side menu, switch ADOMs (when enabled), open the CLI console, view notifications, view help content, and access the admin menu. In some panes, further options will be included in the banner.
Tree menu	On the left side of the screen. In some panes, further navigation will be available as tabs along the top of the content pane. This additional horizontal menu can be toggled to a vertical menu, if preferred. Use this navigation menu to open panes in the GUI.
Content pane	Contains widgets, lists, configuration options, or other information, depending on the pane, menu, or options that are selected. Most management tasks are handled in the content pane.
Toolbar	Directly above the content pane. The toolbar includes options for managing content in the content pane, such as *Create New* and *Delete*.



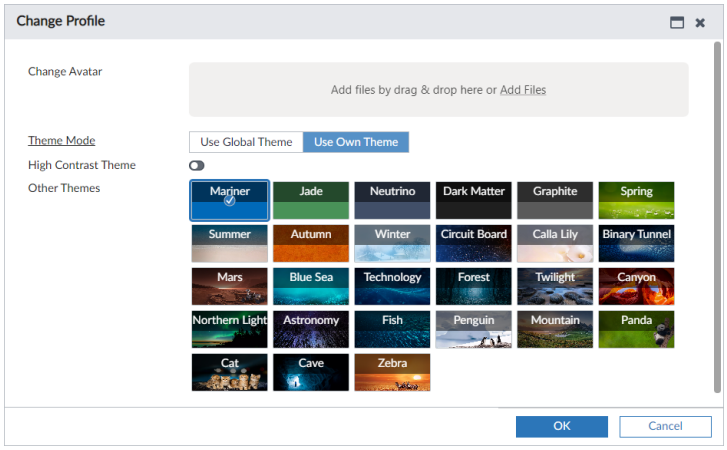
Color themes

You can choose a color theme for the FortiAnalyzer GUI. For example, you can choose a color or image such as jade, summer, or autumn.

By default, all users are assigned the global color theme. To change the global color theme, see Global administration settings on page 586.

To change your color theme:

1. In the banner, open the dropdown for your account and click *Change Profile*.
   The *Change Profile* dialog displays.
2. In the *Theme Mode* field, select *Use Own Theme*.
3. Enable the *High Contrast Theme* or select a color them from the list.



Switching between ADOMs

When ADOMs are enabled, you can move between ADOMs by selecting an ADOM from the *ADOM* button in the banner. You are also prompted to select an ADOM when you log in.



ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See Managing administrator accounts on page 555 for more information.

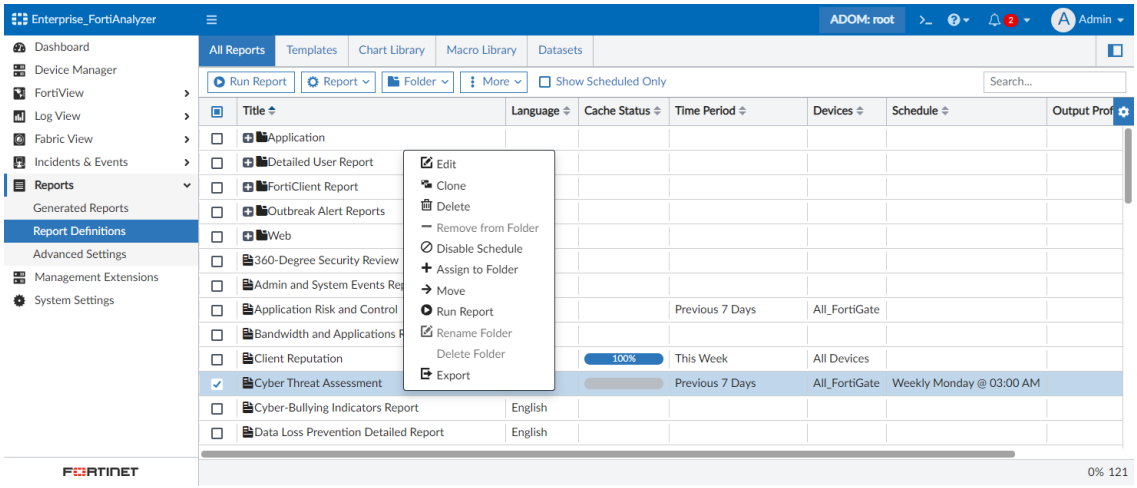
To switch ADOMs:

1. In the banner, click the *ADOM* button.
   The *Select an ADOM* diaolog displays.
2. Click the ADOM to switch to.
   The ADOM you are in displays on the *ADOM* button in the banner.

Using the right-click menu

Options are sometimes available using the right-click menu. Right-click an item in the content pane to display the menu of available options. This menu often includes actions available in the toolbar, as well as some unique actions depending on the pane and its content.

In the following example on the *Reports* pane, you can right-click a report, and select *Edit*, *Clone*, *Delete*, and more.



Using the CLI console

The CLI console is a terminal window that enables you to configure the FortiAnalyzer unit using CLI commands directly from the GUI, without making a separate SSH, or local console connection to access the CLI.

When using the CLI console, you are logged in with the same administrator account that you used to access the GUI. You can enter commands by typing them, or you can copy and paste commands into or out of the console.

For more information about using the CLI, see the *FortiAnalyzer CLI Reference* on the Fortinet Documents Library.



The *CLI Console* requires that your web browser support JavaScript.

To open the CLI console in the GUI, click the CLI Console icon (>_) in the banner.

You can perform the following actions from the top of the CLI Console:

Option	Description
Clear Console	Clear previous text in the console.
Copy History to Clipboard	Copy all text in the console.
Record CLI Commands	Begin recording the next commands entered in the console; click again to finish recording. The commands and outputs from the recording are copied to the clipboard.
Download History	Download all text in the console as a text file.
Reconnect Console	Reconnect to the console, clearing the previous text in the console and returning to the initial prompt.

Option	Description
Run CLI Script	Drag and drop or select a script file to run in the CLI.
Detach	Open the console in a new tab.
CLI of Current Page (if available)	Go to the commands for the current page of the GUI, if they are available.
Minimize	Minimize the console in the GUI.
Full screen	Expand the console to full screen within the GUI.
Close	Close the console.

Avatars

When FortiClient sends logs to FortiAnalyzer, an avatar for each user can be displayed in the *Source* column in the *FortiView* and *Log View* panes. FortiAnalyzer can display an avatar when FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiAnalyzer enabled.

- When FortiClient Telemetry connects to FortiGate, FortiClient sends logs (including avatars) to FortiGate, and the logs display in FortiAnalyzer under the FortiGate device as a sub-type of security.
  The avatar is synchronized from FortiGate to FortiAnalyzer by using the FortiOS REST API.
- When FortiClient Telemetry connects to FortiClient EMS, FortiClient sends logs (including avatars) directly to FortiAnalyzer, and logs display in a FortiClient ADOM.

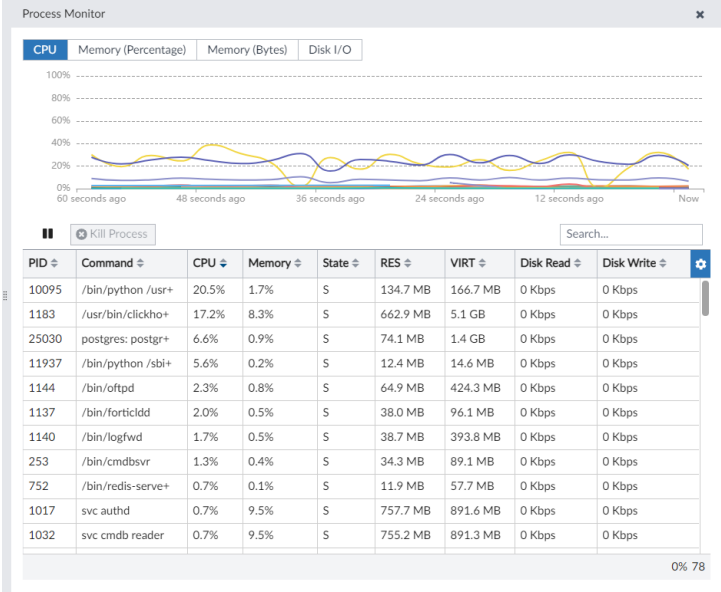
If FortiAnalyzer cannot find the defined picture, a generic, gray avatar is displayed.



You can also optionally define an avatar for FortiAnalyzer administrators. See Creating administrators on page 557.

Using the Process Monitor

The *Process Monitor* displays running processes with their CPU and memory usage as well as their disk I/O levels. Administrators can sort, filter, and terminate processes within the *Process Monitor* pane.



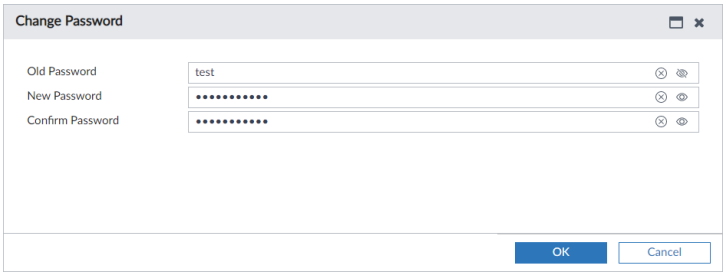
To use the Process Monitor:

1. In the banner, click *[admin_name] > Process Monitor*.
   A line chart and a table view are available in the *Process Monitor* pane. Both the chart and the table refresh automatically unless paused.
2. To change the line chart according to your needs, click *CPU*, *Memory (Percentage)*, *Memory (Bytes)*, or *Disk I/O*.
   The table view will automatically sort by the selection as well.
3. To pause the chart and table from refreshing, click the pause button.
   You can click the play button to resume the automatic refresh.
4. Use the search field to search for any field in the table view.
5. To terminate a process, select it in the table view and click *Kill Process*.

Showing and hiding passwords

In some fields, you can show and hide information by clicking the toggle icon.

For example, see the image of the *Change Password* dialog below. In this example, the *Old Password* is toggled to show the password. The other fields are toggled to hide the password.



Google Map integration

FortiAnalyzer integrates with Google Maps to provide map data for features including but not limited to the following:

- Device location in the Device Manager map view
- FortiView Monitors

Google Maps integration requires the following access. If this access is not available, map data will not be visible on FortiAnalyzer.

- FortiAnalyzer must have access to `https://mapserver.fortinet.com` to register and retrieve the Google Map license.
- The administrator PC must have an internet connection and be able to access to the following sites in order for the browser to be able to download and display the Google Maps and overlay:
  - `https://maps.google.com`
  - `https://maps.googleapis.com`
  - `https://fonts.googleapis.com`
  - `https://mapserver.fortinet.com`

Connecting to the mapserver using a proxy

FortiAnalyzer can also obtain mapserver information from `https://mapserver.fortinet.com` using a web proxy. This can be useful when FortiAnalyzer is operating ina closed network and cannot connect directly to the map server to obtain Map View data to display in the GUI.

To retrieve mapserver information using a web proxy:

1. Ensure that the web proxy has internet access, a working DNS, and is able to access `https://mapserver.fortinet.com`.
2. Configure web proxy settings on your FortiAnalyzer. See Enabling updates through a web proxy on page 552.
3. Confirm that you can access the map server from the FortiAnalyzer using the `diagnose system mapserver test` command.

Target audience and access level

This guide is intended for administrators with full privileges, who can access all panes in the FortiAnalyzer GUI, including the *System Settings* pane.

In FortiAnalyzer, administrator privileges are controlled by administrator profiles. Administrators who are assigned profiles with limited privileges might be unable to view some panes in the GUI and might be unable to perform some tasks described in this guide. For more information about administrator profiles, see Administrator profiles on page 566.



If you logged in by using the `admin` administrator account, you have the *Super_User* administrator profile, which is assigned to the *admin* account by default and gives the `admin` administrator full privileges.

Initial setup

This topic provides an overview of the tasks that you need to do to get your FortiAnalyzer unit up and running.

To set up FortiAnalyzer:

1. Connect to the GUI. See Connecting to the GUI on page 13.
2. Configure the RAID level, if the FortiAnalyzer unit supports RAID. See Configuring the RAID level on page 496.
3. Configure network settings. See Configuring network interfaces on page 477.



Once the IP address of the administrative port of FortiAnalyzer is changed, you will lose connection to FortiAnalyzer. You will have to reconfigure the IP address of the management computer to connect again to FortiAnalyzer and continue.

4. (Optional) Configure administrative domains. See Managing ADOMs on page 504.
5. Configure administrator accounts. See Managing administrator accounts on page 555.



After you configure the administrator accounts for the FortiAnalyzer unit, you should log in again by using your new administrator account.

6. Add devices to the FortiAnalyzer unit so that the devices can send logs to the FortiAnalyzer unit. See Adding devices on page 87.
7. Configure the operation mode. See Configuring the operation mode on page 62 and Operation modes on page 41.

FortiManager features

FortiManager features are not available in FortiAnalyzer 6.2.0 and up.

For information about FortiManager, see the *FortiManager Administration Guide*.



If FortiManager features are enabled in FortiAnalyzer before upgrading to 6.2.0 and later, the existing feature configurations will continue to be available after the upgrade.

FortiManager features carried over during an upgrade can be disabled through the CLI console.

Next steps

Now that you have set up your FortiAnalyzer units and they have started receiving logs from the devices, you can start monitoring and interpreting data. You can:

- View log messages collected by the FortiAnalyzer unit in *Log View*. See Types of logs collected for each device on page 146.
- View multiple panes of network activity in *FortiView > Monitors*. See Monitors on page 125.
- View summaries of threats, traffic, and more in *FortiView* . See FortiView on page 101.
- Generate and view events in *Incidents & Events*. See Incidents & Events on page 204
- Generate and view reports in *Reports*. See Reports on page 425.

Restarting and shutting down

Always use the operation options in the GUI or the CLI commands to reboot and shut down the FortiAnalyzer system to avoid potential configuration problems.

See Restart, shut down, or reset FortiAnalyzer on page 75 in System Settings on page 475.

FortiAnalyzer Key Concepts

This section provides information about basic FortiAnalyzer concepts and terms. If you are new to FortiAnalyzer, use this section to quickly understand this document and the FortiAnalyzer platform.

This section includes the following sections:

- Operation modes on page 41
- Administrative domains on page 43
- Logs on page 44
- Log storage on page 45
- FortiView dashboard on page 48

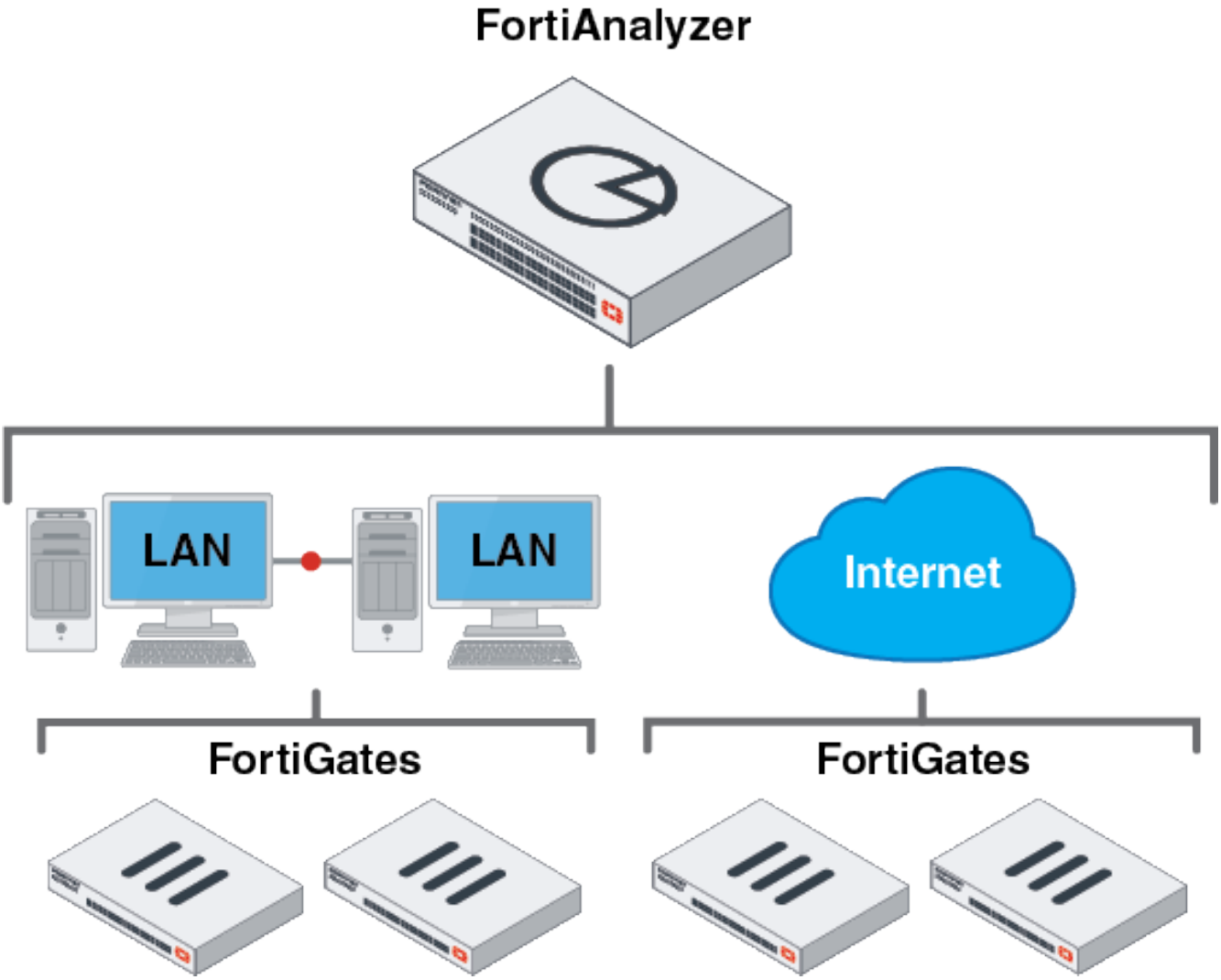
Operation modes

FortiAnalyzer can run in two operation modes: Analyzer and Collector. Choose the operation mode for your FortiAnalyzer units based on your network topology and requirements.

Analyzer mode

Analyzer mode is the default mode that supports all FortiAnalyzer features. Use this mode to aggregate logs from one or more Collectors.

The following diagram shows an example of deploying FortiAnalyzer in Analyzer mode.



Collector mode

When FortiAnalyzer is in Collector mode, its primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. Instead of writing logs to the database, the Collector retains logs in their original binary format for uploading. In this mode, most features are disabled.

Analyzer and Collector feature comparison

Feature	Analyzer Mode	Collector Mode
Device Manager	Yes	Yes

Feature	Analyzer Mode	Collector Mode
FortiView	Yes	No
Log View	Yes	Raw archive logs only
Incidents & Events	Yes	No
Monitoring devices	Yes	No
Reporting	Yes	No
System Settings	Yes	Yes
Log Forwarding	Yes	Yes

Analyzer–Collector collaboration

You can deploy Analyzer mode and Collector mode on different FortiAnalyzer units and make the units work together to improve the overall performance of log receiving, analysis, and reporting. The Analyzer offloads the log receiving task to the Collector so that the Analyzer can focus on data analysis and report generation. This maximizes the Collector's log receiving performance.

For an example of setting up Analyzer–Collector collaboration, see Collectors and Analyzers on page 613.

FortiAnalyzer Fabric

FortiAnalyzer can also join a FortiAnalyzer Fabric which enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzers acting as members.

The FortiAnalyzer Fabric is ideal for use in high volume environments with many FortiAnalyzers. For more information about sizing and design considerations, see the FortiAnalyzer Architecture Guide.

In this mode, FortiAnalyzer Fabric members form a Fabric with one device operating in supervisor mode as the root device. Incident, event, and log information is synced from members to the supervisor using the API.

See the FortiAnalyzer Fabric Deployment Guide for more information.

Administrative domains

Administrative domains (ADOMs) enable the `admin` administrator to constrain the access privileges of other FortiAnalyzer unit administrators to a subset of devices in the device list. For Fortinet devices with virtual domains (VDOMs), ADOMs can further restrict access to only data from a specific VDOM for a device.

Enabling ADOMs alters the available functions in the GUI and CLI. Access to the functions depends on whether you are logged in as the `admin` administrator. If you are logged in as the `admin` administrator, you can access all ADOMs. If you are not logged in as the `admin` administrator, the settings in your administrator account determines access to ADOMs.

For information on enabling and disabling ADOMs, see Enabling and disabling the ADOM feature on page 502. For information on working with ADOMs, see Administrative Domains (ADOMs) on page 498. For information on configuring administrator accounts, see Managing administrator accounts on page 555.

Logs

Logs in FortiAnalyzer are in one of the following phases.

- Real-time log: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file.
- Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline.
- Analytics logs or historical logs: Indexed in the SQL database and online.

In order for FortiAnalyzer to accept logs, the sending device must be registered in FortiAnalyzer. You can add devices to FortiAnalyzer by specifying the serial number and other details, or you may point the device's log settings to the FortiAnalyzer. If initiated by the remote device, the device must be authorized before logs can be received on FortiAnalyzer. See Adding devices on page 87.

For more information on the types of logs collected for each device, see Types of logs collected for each device on page 146.

Log encryption

Beginning in FortiAnalyzer 6.2, all logs from Fortinet devices (using Fortinet's proprietary protocol: OFTP) must be encrypted. FortiAnalyzer encryption level must be equal or less than the sending device's level. For example, when configuring logging from a FortiGate, FortiAnalyzer must have the same encryption level or lower than FortiGate in order to accept logs from FortiGate.

To configure the encryption level on FortiAnalyzer:

1. In the FortiAnalyzer CLI, enter the following commands:
```
config system global
      set enc-algorithm {high | low | medium}
```

To configure the encryption level on FortiGate:

1. In the FortiGate CLI, enter the following commands:
```
config log fortianalyzer setting
      set enc-algorithm {high-medium | high | low}
```

See also Appendix B - Log Integrity and Secure Log Transfer on page 618.

Log storage

Logs and files are stored on the FortiAnalyzer disks. Logs are also temporarily stored in the SQL database.

You can configure data policy and disk utilization settings for devices. These are collectively called log storage settings.

You can configure global log and file storage settings. These apply to all logs and files in the FortiAnalyzer system regardless of log storage settings.

Log rolling

When FortiAnalyzer receives a log, it is stored in a file. Logs will continue to populate this file until its limit is reached, at which time the file is "rolled" which involves compressing the file and creating a new one for further logs of that type. There are two settings that you can use to configure when log rolling occurs, and both may be used at the same time, with rolling taking place when either condition is met.

- Log file size: This is enabled by default and set to 200 MB.
- At a scheduled time: Either daily or weekly at a set time.

Rolling the files daily is recommended to avoid a file from spanning more than 24 hours and masking the actual amount of days you are storing logs for.

See also Configuring rolling and uploading of logs using the GUI on page 543.

Log deletion

When you reach your archive retention limit as defined by allocated storage size or specified days, FortiAnalyzer deletes old logs to make room for new logs. FortiAnalyzer can only delete files, not logs within a file. Controlling file growth is important because storage capacity is not infinite and it directly affects how old logs are deleted to make room for new logs.

FortiAnalyzer will delete old files based on which condition is forcing the deletion:

- Days: Delete the log file that contains logs which are *all* outside the configured day retention period. Log files can span several days, or even months. When this is the case, the file will not be considered eligible for deletion when logs that are within the configured retention days would be deleted. This can lead to Archive indicating it is storing more days than it is configured for (for example, 100/90 days). This is due to the number displaying the oldest log date, and not specifically that it has logs for each day up to that number.
- Storage size: Delete the log file with the oldest *last received* log. This can lead to the administrator not seeing the true amount of logs in analytics since there's no way to indicate that there are no logs for days 60 through 89, only that there are some logs from 90 days ago.

See also Data policy and automatic deletion on page 47 and Disk utilization for Archive and Analytic logs on page 47.

SQL database

FortiAnalyzer supports Structured Query Language (SQL) for logging and reporting. The log data is inserted into the SQL database to support data analysis in *FortiView*, *Log View*, and *Reports*. Remote SQL databases are not supported.

For more information, see FortiView on page 101, Types of logs collected for each device on page 146, and Reports on page 425.

The log storage settings define how much FortiAnalyzer disk space to use for the SQL database.



When FortiAnalyzer is in Collector mode, the SQL database is disabled by default. If you want to use logs that require SQL when FortiAnalyzer is in Collector mode, you must enable the SQL database. See Operation modes on page 41.

Analytics and Archive logs

Logs in FortiAnalyzer are in one of the following phases.

- Real-time log: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file.
- Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline.
- Analytics logs or historical logs: Indexed in the SQL database and online.

Use a data policy to control how long to retain Analytics and Archive logs.

- Archive logs on page 46
- Analytic logs on page 47

Archive logs

When FortiAnalyzer receives a log, it is stored in a file. Logs will continue to populate this file until its limit is reached, at which time the file is "rolled" which involves compressing the file and creating a new one for further logs of that type. These files (rollled or otherwise) count against the archive retention limits and are referred to as *Archived* or *Offline* logs.

You cannot immediately view details about these logs in the *FortiView*, *Log View*, and *Incidents & Events* panes. You also cannot generate reports about the logs in the *Reports* pane.

Archive logs are stored unchanged and can be uploaded to a file server for use as backups.

- If you are using a FortiAnalyzer-VM, you may also choose to snapshot the data drive to backup your logs.
- If you are using a physical FortiAnalyzer which leverages RAID for storage, remember that RAID is not a backup solution.

Log storage in *Archive* is important since it is used to rebuild the database in the event of database corruption, or in some cases during upgrades.

Analytic logs

Immediately following the storage of a log in an archive, the same log is inserted into the SQL database. This function is also known as being *indexed*, and these logs are referred to as *Analytic* or *Online* logs.

Analytic logs are the only logs which are used for analysis in FortiAnalyzer*Log View* (excluding *Log Browse*), *Incidents and Events*, and *Reports*.

Analytic logs are dissected during insertion and any subtypes are stored as their own category. For example, security profile logs such as web filtering logs are sent and stored as Traffic logs when archived, however, Analytics extracts the relevant web filtering fields and stores them in a web filtering table.

Indexed logs take up significantly more space than the same amount of logs in Archive.

Most administrators may need to store between 30 and 60 days in Analytics, however, this should be configured for the amount of time that you would typically need to explore the logs for.

If you need to run analytics for dates outside your Analytics retention, you may perform a database rebuild and load the particular date range. A database rebuild involves purging all logs from Analytics and loading logs for the days of interest from Archive. Once analysis is complete, you can then rebuild once more to load the most current logs into analytics from the archive.

Data policy and automatic deletion

Use a data policy to control how long to keep compressed and indexed logs. When ADOMs are enabled, you can specify settings for each ADOM and the settings apply to all devices in that ADOM. When ADOMs are disabled, settings apply to all managed devices.

A data policy specifies:

- How long to keep Analytics logs indexed in the database
  When the specified length of time in the data policy expires, logs are automatically purged from the database but remain compressed in a log file on the FortiAnalyzer disks.
- How long to keep Archive logs on the FortiAnalyzer disks
  When the specified length of time in the data policy expires, Archive logs are deleted from the FortiAnalyzer disks.

See also Log storage information on page 173.

Disk utilization for Archive and Analytic logs

You can specify how much of the total available FortiAnalyzer disk space to use for log storage. You can specify what ratio of the allotted storage space to use for logs that are indexed in the SQL database and for logs that are stored in a compressed format on the FortiAnalyzer disks. Then you can monitor how quickly device logs are filling up the allotted disk space.



Analytic logs indexed in the SQL database require more disk space than Archive logs (purged from the SQL database but remain compressed on the FortiAnalyzer disks).

An average Analytic log is 600 bytes, and an average Archive log is 80 bytes. By default, after seven days Analytic logs are compressed and are an average of 150 bytes.

Keep this difference in mind when specifying the storage ratio for Analytics and Archive logs.

When ADOMs are enabled, you can specify settings for each ADOM and the settings apply to all devices in that ADOM. When ADOMs are disabled, settings apply to all managed devices. See Log storage information on page 173.

FortiView dashboard

FortiAnalyzer provides dashboards for Security Operations Center (SOC) administrators. FortiView includes monitors which enhance visualization for real-time activities and historical trends for analysts to effectively monitor network activities and security alerts. See FortiView on page 100.

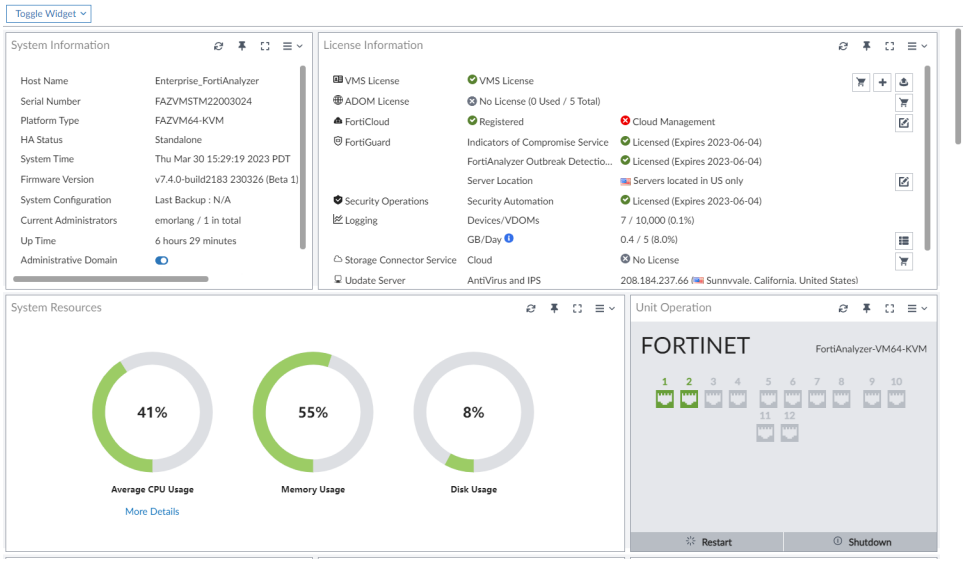
In high capacity environments, the FortiView module can be disabled to improve performance. See Enabling and disabling FortiView on page 145.

Dashboards

The *Dashboards* provide easy access to information, including the performance and status of the FortiAnalyzer, the Internet-of-Things (IoT) devices on the network, email metrics, and security operations.

Status

Dashboards > *Status* contains widgets that provide performance and status information and enable you to configure basic system settings.



The following widgets are available:

Widget	Description
System Information	Displays basic information about the FortiAnalyzer system, such as up time and firmware version. You can also enable or disable Administrative Domains and adjust the operation mode. For more information, see System Information widget on page 51. From this widget you can manually update the FortiAnalyzer firmware to a different release. For more information, see Updating the system firmware on page 54. The widget fields will vary based on how the FortiAnalyzer is configured, for example, if ADOMs are enabled.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 62.

Widget	Description
License Information	Displays whether the unit license is registered to FortiCloud, and if remote access from FortiCloud is enabled. Displays how many devices of the supported maximum are connected to the FortiAnalyzer unit. See License Information widget on page 63. From this widget you can purchase a license, add a license, or manually upload a license for VM systems.
Unit Operation	Displays status and connection information for the ports of the FortiAnalyzer unit. It also enables you to shutdown and restart the FortiAnalyzer unit or reformat a hard disk. For more information, see Unit Operation widget on page 71.
Alert Message Console	Displays log-based alert messages for both the FortiAnalyzer unit and connected devices. For more information, see Alert Messages Console widget on page 72.
Log Receive Monitor	Displays a real-time monitor of logs received. You can view data per device or per log type. For more information, see Log Receive Monitor widget on page 72.
Insert Rate vs Receive Rate	Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 73. The *Insert Rate vs Receive Rate* widget is hidden when the FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.
Log Insert Lag Time	Displays how many seconds the database is behind in processing the logs. For more information, see Log Insert Lag Time widget on page 73. The *Log Insert Lag Time* widget is hidden when the FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.
Receive Rate vs Forwarding Rate	Displays the *Receive Rate*, which is the rate at which FortiAnalyzer is receiving logs. When log forwarding is configured, the widget also displays the log forwarding rate for each configured server. For more information, see Receive Rate vs Forwarding Rate widget on page 74.
Disk I/O	Displays the disk utilization, transaction rate, or throughput as a percentage over time. For more information, see Disk I/O widget on page 74.
Device widgets	For example, widgets such as *Status*, *Disk Quota Usage*, and *Last Log Time*. These widgets display summary information for authorized devices. For more inforamtion, see Device widgets on page 74.
FortiAnalyzer Cloud Status	Displays the status of the FortiAnalyzer Cloud instance according to the connector. For more information, see FortiAnalyzer Cloud Status widget on page 75.

Customizing the status dashboard

The FortiAnalyzer *Status* dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized. It can also be viewed in full screen by selecting the full screen button on the far right side of the toolbar.

Action	Steps
Move a widget	Move the widget by clicking and dragging its title bar, then dropping it in its new location
Add a widget	Select *Toggle Widgets* from the toolbar, then select the name widget you need to add.
Delete a widget	Click the *Close* icon in the widget's title bar.
Customize a widget	For widgets with an edit icon, you can customize the widget by clicking the Edit icon and configuring the settings.
Reset the dashboard	Select *Toggle Widgets* > *Reset to Default* from the toolbar. The dashboards will be reset to the default view.

System Information widget

The information displayed in the *System Information* widget is dependent on the FortiAnalyzer model and device settings. The following information is available on this widget:

Host Name	The identifying name assigned to this FortiAnalyzer unit. Click the edit host name button to change the host name. For more information, see Changing the host name on page 52.
Serial Number	The serial number of the FortiAnalyzer unit. The serial number is unique to the FortiAnalyzer unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	Displays the FortiAnalyzer platform type, for example *FAZVM64* (virtual machine).
HA Status	Displays if FortiAnalyzer unit is in High Availability mode and whether it is the Primary or Secondary unit in the HA cluster.
System Time	The current time on the FortiAnalyzer internal clock. Click the edit system time button to change system time settings. For more information, see Configuring the system time on page 53.
Firmware Version	The version number and build number of the firmware installed on the FortiAnalyzer unit.

	You can access the latest firmware version available on FortiGuard from FortiAnalyzer. Alternately you can manually download the latest firmware from the Customer Service & Support website at https://support.fortinet.com. Click the update button, then select the firmware image to load from the local hard disk or network volume. For more information, see Updating the system firmware on page 54.
System Configuration	The date of the last system configuration backup. The following actions are available: • Click the backup button to backup the system configuration to a file; see Backing up the system on page 57. • Click the restore to restore the configuration from a backup file; see Restoring the configuration on page 61. You can also migrate the configuration to a different FortiAnalyzer model by using the CLI. See Migrating the configuration on page 61.
Current Administrators	The number of administrators currently logged in. Click the current session list button to view the session details for all currently logged in administrators.
Up Time	The duration of time the FortiAnalyzer unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled. Toggle the switch to change the Administrative Domain state. See Enabling and disabling the ADOM feature on page 502.
Operation Mode	Displays the current operation mode of the FortiAnalyzer. Click the other mode to change to it. For more information on operation modes, see Operation modes on page 41.

Changing the host name

The host name of the FortiAnalyzer unit is used in several places.

- It appears in the *System Information* widget on the dashboard.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name.

The *System Information* widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is FortiAnalyzer1234567890, the CLI prompt would be `FortiAnalyzer123456~#`.

To change the host name:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, click the edit host name button next to the *Host Name* field.
3. In the *Host Name* box, type a new host name.

The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.

4. Click the checkmark to change the host name.

Configuring the system time

You can either manually set the FortiAnalyzer system time or configure the FortiAnalyzer unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.



For many features to work, including scheduling, logging, and SSL-dependent features, the FortiAnalyzer system time must be accurate.

To configure the date and time:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, click the edit system time button next to the *System Time* field.
3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiAnalyzer unit's clock with an NTP server:

System Time	The date and time according to the FortiAnalyzer unit's clock at the time that this pane was loaded or when you last clicked the *Refresh* button.
Time Zone	Select the time zone in which the FortiAnalyzer unit is located and whether or not the system automatically adjusts for daylight savings time. Time zone settings can also be for each ADOM. See Creating ADOMs on page 505.
Update Time By	Select *Set time* to manually set the time, or *Synchronize with NTP Server* to automatically synchronize the time.
Set Time	Manually set the data and time.
Select Date	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.
Select Time	Select the time.
Synchronize with NTP Server	Automatically synchronize the date and time.
Server	Enter the IP address or domain name of an NTP server. Click the plus icon to add more servers. To find an NTP server that you can use, go to http://www.ntp.org.
Min	Minimum poll interval in seconds as power of 2 (e.g. 6 means 64 seconds, default = 6).
Max	Maximum poll interval in seconds as power of 2 (e.g. 6 means 64 seconds, default = 10).

4. Click the checkmark to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, you can update FortiAnalyzer firmware. From the *Dashboard* menu in FortiAnalyzer, you can access firmware images on FortiGuard and update FortiAnalyzer. Alternately you can manually download the firmware image from the Customer Service & Support site, and then upload the image to FortiAnalyzer.

For information about upgrading your FortiAnalyzer device, see the *FortiAnalyzer Upgrade Guide* or contact Fortinet Customer Service & Support.

Back up the system



Back up the configuration and database before changing the firmware of FortiAnalyzer. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see Backing up the system on page 57.

Register FortiAnalyzer



Before you can download firmware updates for FortiAnalyzer, you must first register your FortiAnalyzer unit with Customer Service & Support. For details, go to https://support.fortinet.com/ or contact Customer Service & Support.

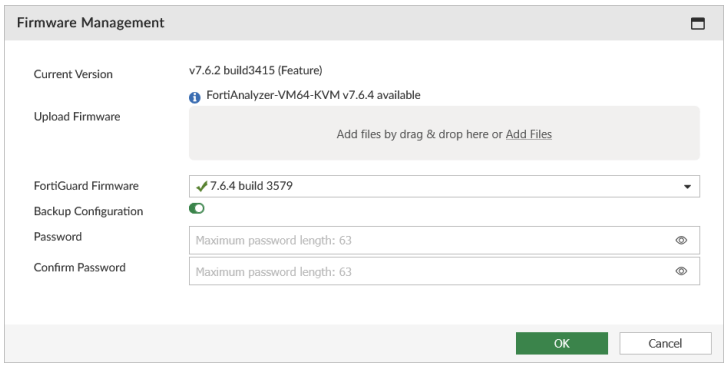
Valid firmware contracts are required to upgrade major/minor versions



If the FortiAnalyzer support contract which includes the *Firmware & General Updates* entitlement has expired, you will be unable to upgrade the firmware to a higher major version, such as from FortiAnalyzer 7.0 to 8.0, or to a higher minor version, such as from FortiAnalyzer 7.4 to 7.6. However, you can upgrade the firmware of a FortiAnalyzer with an expired contract to a higher patch build, such as from FortiAnalyzer 7.4.0 to 7.4.1, to allow for security updates.

To update FortiAnalyzer firmware using FortiGuard:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, beside *Firmware Version*, click *Upgrade Firmware*.
   The *Firmware Management* dialog box opens.



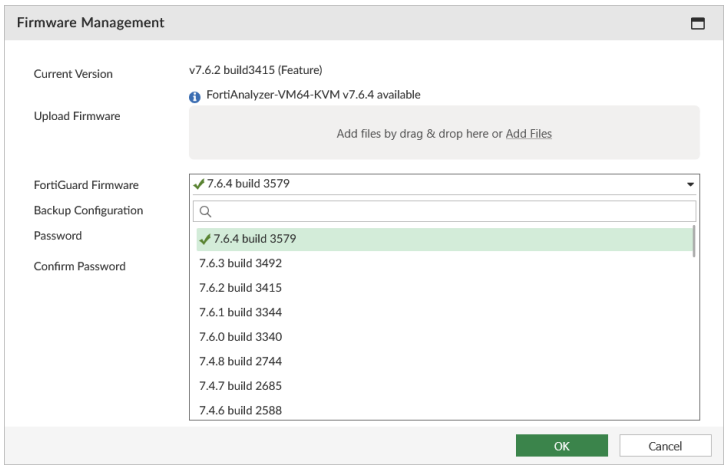
3. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiAnalyzer configuration when performing a firmware upgrade.

   Type and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.

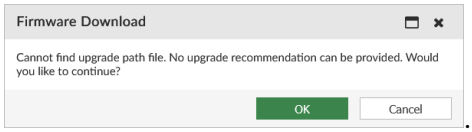
4. From the *FortiGuard Firmware* box, select the version of FortiAnalyzer for the upgrade, and click *OK*.

   The *FortiGuard Firmware* box displays the firmware images available for upgrade:

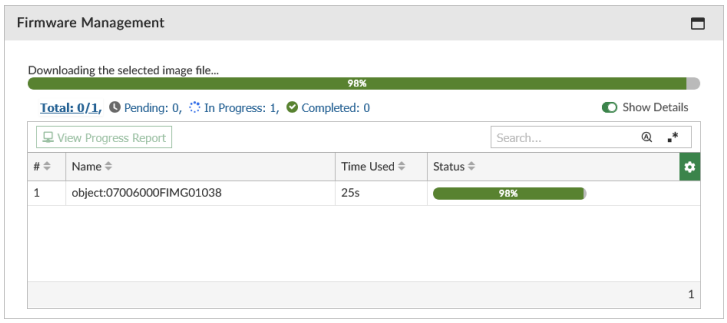
   - When FortiAnalyzer has a valid contract, all available firmware versions are displayed for upgrading or downgrading.
   - When FortiAnalyzer has no valid contract, or the contract is expired, only display the available patch upgrades.
   - A green checkmark displays beside the recommended image for FortiAnalyzer upgrade.



   - If you select an image without a green checkmark, a confirmation dialog box is displayed. Click *OK* to continue.



   - FortiAnalyzer downloads the firmware image from FortiGuard.



- FortiAnalyzer uses the downloaded image to update its firmware, and then restarts.



- After FortiAnalyzer restarts, the upgrade is complete.

To manually update FortiAnalyzer firmware:

1. Download the firmware (the `.out` file) from the Customer Service & Support website, https://support.fortinet.com/.
2. Go to *Dashboards* > *Status*.
3. In the *System Information* widget, in the *Firmware Version* field, click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.
4. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiAnalyzer configuration when performing a firmware upgrade.

   Type and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.
5. Drag and drop the file onto the dialog box, or click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal and then click *Open*.
6. Click *OK*.

   Your device will upload the firmware image and you will receive a confirmation message when the upgrade was successful.

   Attempting to upgrade major/minor versions without a valid *Firmware & General Updates* entitlement will result in an error message, and the upgrade will not proceed.



Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server> <IP of server>
      <username on server> <password>
```

For more information, see the FortiAnalyzer CLI Reference.

7. Refresh the browser and log back into the device.
8. Go to *Device Manager* module and make sure that all formerly added devices are still listed.
9. Open the other functional modules and make sure they work properly.

Firmware maturity levels

FortiAnalyzer 7.6.0 and later firmware images use tags to indicate the following maturity levels:

- The *Feature* tag indicates that the firmware release includes new features. It can also include bug fixes and vulnerability patches where applicable.
- The *Mature* tag indicates that the firmware release includes no new, major features. Mature firmware will contain bug fixes and vulnerability patches where applicable.

Administrators can use the tags to identify the maturity level of the current firmware in the GUI or CLI.

Administrators can view the maturity level of each firmware image that is available for upgrade on the Firmware Management dialog box. When upgrading from mature firmware to feature firmware, a warning message is displayed.

To view maturity levels for firmware in the GUI:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, beside *Firmware Version*, click *Upgrade Firmware*.
   The *Firmware Management* dialog box opens.
3. From the *FortiGuard Firmware box*, select the version of FortiManager for the upgrade.
   The Firmware Version displays the version with build number and either (Mature) or (Feature).

To view maturity levels for firmware in the CLI:

In this example, the *Version* field includes `.F` to indicate that the maturity level is feature:

```
# get system status
   Platform Type : FMG-3000G
   Platform Full Name : FortiManager-3000G
   Version : vx.x.x0-buildxxxx 240620 (GA.F)
```

In this example, the *Version* field includes `.M` to indicate that the maturity level is mature:

```
# get system status
   Platform Type : FMG-3000G
   Platform Full Name : FortiManager-3000G
   Version : vx.x.x-buildxxxx 240620 (GA.M)
```

Backing up the system

Fortinet recommends that you back up your FortiAnalyzer configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal affect to the network. You should also back up your configuration after making any changes to the FortiAnalyzer configuration or settings that affect connected devices.

Fortinet recommends backing up all configuration settings from your FortiAnalyzer unit before upgrading the FortiAnalyzer firmware. See Updating the system firmware on page 54.

Only one backup can be performed at a time. If a backup is started while another backup is already ongoing, a message is displayed indicating that the backup has failed and an event is added to the Event Log with the message: *Backup all settings fail (backup in progress)*.

An MD5 checksum is automatically generated in the event log when backing up the configuration. You can verify a backup by comparing the checksum in the log entry with that of the backup file. The filename is also included in the event log for reference.



FortiAnalyzer uses AES-GCM encryption for backup configurations.

Perform a system backup

To back up the FortiAnalyzer configuration:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.
3. Select the *Backup Now* tab.
4. Enter and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.



The character " \" is used in the FortiAnalyzer CLI as an escape character.

If your encryption password contains the \ character, you must either escape it (by adding an additional \) or use single quotes around the password when referring to it in the CLI. For example:

- `execute backup all-settings ftp 10.0.0.1 backup/backup1.dat admin admin1234 ~jFeS.Z/i\\ilA~gnAaq=8c1n`gCabc`
- `execute backup all-settings ftp 10.0.0.1 backup/backup1.dat admin admin1234 '~jFeS.Z/i\ilA~gnAaq=8c1n`gCabc'`

5. Select *OK* and save the backup file on your management computer.

Scheduling automatic backups

You can configure FortiAnalyzer to automatically backup your configuration on a set schedule.

To schedule automatic backup in the GUI:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.
3. Select the *Schedule Backup* tab.
4. Enable the *Enable Schedule Backup* option, and configure the options including the backup location, backup frequency, and an encryption password.
5. Click *OK*.

To schedule automatic backup in the CLI:

1. In the FortiAnalyzer CLI, enter the following command:
   ```
   config system backup all-settings
   ```
2. Configure the backup settings:
   ```
   set status {enable | disable}
   set server {<ipv4_address>|<fqdn_str>}
   set user <username>
   set directory <string>
   set week_days {monday tuesday wednesday thursday friday saturday sunday}
   set time <hh:mm:ss>
   set protocol {ftp | scp | sftp}
   set passwd <passwd>
   set crptpasswd <passwd>
   end
   ```

For example, the following configuration uses the FTP protocol to backup the configuration to server `172.20.120.11` in the `/usr/local/backup` directory every Monday at 1:00pm.

```
config system backup all-settings
   set status enable
   set server 172.20.120.11
   set user admin
   set directory /usr/local/backup
   set week_days monday
   set time 13:00:00
   set protocol ftp
end
```

For more information, see the FortiAnalyzer CLI Reference Guide on the Fortinet Documents Library.

View backup history

After performing backups, you can view the backup history to see all backups performed on the FortiAnalyzer. Only successful backups are displayed in the Backup History table. An entry is added to the Event Log when the backup fails, for example when there is already a backup in progress.

To see backup history:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.
3. Select the *Backup History* tab.
   The backup history displays the *Date & Time*, *Admin*, *Size* and *Status* of each backup.

MD5 checksum

To find the MD5 checksum generated with the backup:

1. In the GUI, go to *System Settings* > *Event Log*.
2. In the *Changes* column for the event log, note the MD5 checksum.

Perform backups using SCP

You can use secure copy protocol (SCP) with a SSH certificate to back up the FortiAnalyzer system configuration.

The following is an example of SSH certificate generation to be used with SCP for configuration backup. This example uses RSA but can also be applied to ED25519 keys.

To configure a SSH certificate for backup using SCP:

1. Create a SSH CA user key pair.
   ```
   ssh-keygen -t rsa -b 4096 -f ~/.ssh/ssh_user_ca
   ```
2. Create a SSH CA host key pair.
   ```
   ssh-keygen -t rsa -b 4096 -f ~/.ssh/ssh_host_ca
   ```
3. Copy the CA host `ssh_host_ca*` to `/etc/ssh/`.
4. Sign the user's public key using the host CA key.
   ```
   ssh-keygen -s ~/.ssh/ssh_host_ca -I qa -n qa -V +52w ~/.ssh/ssh_user_ca.pub

   ssh-keygen -Lf ~/.ssh/ssh_user_ca-cert.pub
   /root/.ssh/ssh_user_ca-cert.pub:
      Type: ssh-rsa-cert-v01@openssh.com host certificate
      Public key: RSA-CERT SHA256:/Ue4vx5n2oUp+XhwLuAkadsfa0YTt7dpuZgbZ8TBNuw
      Signing CA: RSA SHA256:/Ue4vx5n2oUp+XhwLuAkIkvadfadTt7dpuZgbZ8TBNuw (using rsa-sha2-512)
      Key ID: "qa"
      Serial: 0
      Valid: from 2023-09-25T14:24:00 to 2024-09-23T14:25:08
      Principals: qa
      Critical Options: (none)
      Extensions: (none)
   ```

   In the example command `ssh-keygen -s ~/.ssh/ssh_host_ca -I qa -n qa -V +52w ~/.ssh/ssh_user_ca.pub`, the `-n qa` option specifies the username (*qa*) that will be allowed to authenticate using the signed certificate. This should match the username used to log in to the FortiAnalyzer device when transferring backups via SCP.

5. Edit the SSH server config file at `/etc/ssh/sshd_config` and make the *TrustedUserCAKeys* directive to point to the user CA public key.
   ```
   TrustedUserCAKeys /etc/ssh/ssh_host_ca.pub
   ```
6. Restart the sshd process to make the configuration change take effect.
   ```
   systemctl restart sshd
   ```
7. On FortiAnalyzer, configure the SSH certificate.
   ```
   config sys certificate ssh
      edit ssh_cert_1
         set certificate "ssh_user_ca-cert.pub"
         set private "ssh_user_ca"
      end
   ```
8. Configure backup of all settings using SCP .
   ```
   execute backup all-settings scp <server IP> <path and file name> <username> <ssh-cert>
   ```

For more information on configuration of backup settings in the FortiAnalyzer CLI, see the FortiAnalyzer CLI Reference.

Restoring the configuration

You can use the following procedure to restore your FortiAnalyzer configuration from a backup file on your management computer.

To restore the FortiAnalyzer configuration:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, click the restore button next to *System Configuration*. The *Restore System* dialog box opens.
3. Configure the following settings then select *OK*.

Choose Backup File	Select *Browse* to find the configuration backup file you want to restore, or drag and drop the file onto the dialog box.
Password	Type the encryption password.
Overwrite current IP and routing settings	Select the checkbox to overwrite the current IP and routing settings.
Migrate from a different platform	Enable this option to migrate the uploaded database from a different version or platform. See Migrating the configuration on page 61. • When this option is disabled, the default operation of FortiAnalyzer is to restore the database based on the uploaded file. • When the option is enabled, the FortiAnalyzer migrates the database of the uploaded file.

Migrating the configuration

You can back up the configuration of one FortiAnalyzer and then use the GUI or CLI to migrate the settings to another FortiAnalyzer on the same or different platform or version.

If you encrypted the FortiAnalyzer configuration file when you created it, you need the password to decrypt the configuration file when you migrate the file to another FortiAnalyzer model.



When migrating the database from another platform, all configurations except the system settings are migrated. These system settings must be manually copied from the original FortiAnalyzer model to the other FortiAnalyzer model.

To migrate the FortiAnalyzer configuration using the GUI:

1. In one FortiAnalyzer model, go to *Dashboards* > *Status*.
2. Back up the system. See Backing up the system on page 57.
3. In the other FortiAnalyzer model, go to *Dashboards* > *Status*.
4. If the configuration file is for multiple ADOMs, enable *Administrative Domains* in the *System Information* widget before migrating.

5. Click on the *Restore* option next to *System Configuration*.
   The *Restore System* dialog appears.
6. Enable the option to *Migrate from a different platform*.
7. Upload the backup file from the migrating platform, and click *OK*.
8. After migrating, update the system settings, as needed.

To migrate the FortiAnalyzer configuration using the CLI:

1. In one FortiAnalyzer model, go to *Dashboards* > *Status*.
2. Back up the system. See Backing up the system on page 57.
3. In the other FortiAnalyzer model, go to *Dashboards* > *Status*.
4. If the configuration file is for multiple ADOMs, enable *Administrative Domains* in the *System Information* widget before migrating.
5. Open the CLI Console, and enter the following command:
   ```
   execute migrate all-settings <ftp | scp | sftp> <server> <filepath> <user> <password>
         <cryptpasswd>
   ```
6. After migrating, update the system settings, as needed.

Configuring the operation mode

The FortiAnalyzer unit has two operation modes: Analyzer and Collector. For more information, see Operation modes on page 41.

When FortiAnalyzer is operating in Collector mode, the SQL database is disabled by default so logs that require the SQL database are not available in Collector mode unless the SQL database is enabled.

To change the operation mode:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, select *Analyzer* or *Collector* in the *Operation Mode* field
3. Click *OK* in the confirmation dialog box to change the operation mode.

System Resources widget

The *System Resources* widget displays the usage status of the CPUs, memory, and hard disk. You can view system resource information in real-time or historical format, as well as average or individual CPU usage.

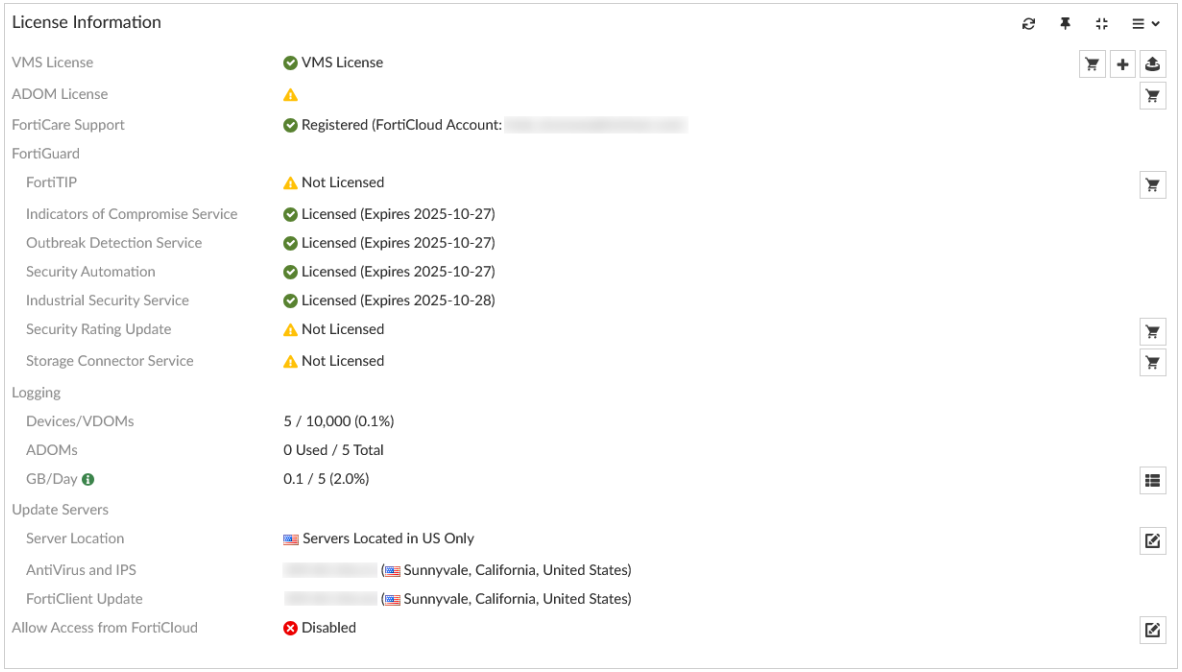
On VMs, warning messages are displayed if the amount of memory or the number of CPUs assigned are too low, or if the allocated hard drive space is less than the licensed amount. These warnings are also shown in the notification list (see GUI overview on page 30). Clicking on a warning opens the *FortiAnalyzer VM Install Guide*.

To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

To view individual CPU usage, from the Real-Time display, click on the CPU chart. To go back to the standard view, click the chart again.

License Information widget

The *License Information* widget displays the number of devices connected to the FortiAnalyzer.



VMS License	VM license information and status. Click the *Add License* button to log in to FortiCloud and activate an add-on license. See Activating add-on licenses on page 66. Click the *Upload License* button to upload a new VM license file. This field is only visible for FortiAnalyzer VM. The *Duplicate* status appears when users try to upload a license that is already in use. Additionally, the following message will be displayed in the Notifications: *Duplicate License has been found! Your VM license will expire in XX hours (Grace time: 24 hours)* Users will have 24 hours to upload a valid license before the duplicate license is blocked.
ADOM License	ADOM license information and status. For Hardware models, the default number of ADOMs can be found in the Release Notes on docs.fortinet.com.

	For FortiAnalyzer-VM Subscription licenses, 5 ADOMs are included. They are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.
FortiCloud	License registration status with FortiCloud. Displays *Not Registered* or *Registered*. When *FortiCloud* displays *Not Registered*, a *Register Now* link is available. You can click the *Register Now* link to register the device or VM license with FortiCloud. See Registering with FortiCloud on page 65. If registered, you can enable/disable remote access from FortiCloud. See Enabling remote access from FortiCloud on page 66
FortiAI License	FortiAI license information and status. See FortiAI on page 402.
FortiGuard	
FortiTIP	The license status. For more information, see FortiTIP service integration on page 357.
Indicators of Compromise Service	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
Outbreak Detection Service	The license status. For more information, see Outbreak Alerts on page 352.
Security Automation	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
Industrial Security Service	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
Security Rating Update	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
Storage Connector Service	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
Secure DNS Server	The SDNS server license status. Click the upload image button to upload a license key.
Server Location	The locations of the FortiGuard servers, either global or US only. Click the edit icon to adjust the location. Changing the server location will cause the FortiAnalyzer to reboot.
Security Operations	The license status.
Logging	

	Device/VDOMs	The total number of devices and VDOMs connected to the FortiAnalyzer and the total number of device and VDOM licenses.
	GB/Day	The gigabytes per day of logs allowed and used for this FortiAnalyzer. Click the show details button to view the GB per day of logs used for the previous 6 days. FortiAnalyzer displays a warning after exceeding the quota for more than 7 days, and it is recommended that you review your daily logging or upgrade your license to accommodate the extra logs. The GB/Day log volume can be viewed per ADOM through the CLI using: `diagnose fortilogd logvol-adom <name>`.
Storage Connector Service		The cloud storage license status. Displays usage statistics as well as the license expiration date when a valid license is present. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
Update Server		
	AntiVirus and IPS	The IP address and physical location of the Antivirus and IPS update server.
	Web and Email Filter	The IP address and physical location of the web and email filter update server.
	FortiClient Update	The IP address and physical location of the FortiClient update server.

Registering with FortiCloud

Register your device with FortiCloud to receive customer services, such as firmware updates and customer support.



To view a list of registered devices, go to the Fortinet Technical Support site (https://support.fortinet.com/), and use your FortiCloud credentials to log in. Go to *Asset* > *Manage/View Products*.

See also Activating VM licenses on page 20.

To register a FortiAnalyzer device:

1. Go to *Dashboards* > *Status*.
2. In the *License Information* widget, click *Register Now* for FortiCloud.
   The registration dialog opens.
3. Enter the device details.
4. Click *OK*. FortiAnalyzer connects to FortiCloud and registers the device.
   A confirmation message appears at the top of the content pane, and the *Status* field changes to *Registered*.

Enabling remote access from FortiCloud

Enable remote access to your device from FortiCloud.

The device must be registered with FortiCloud to enable remote access.



You cannot enable remote access from FortiCloud if the FortiAnalyzer is managed by a FortiManager. You must disable the management before enabling remote access.

For a FortiAnalyzer high availability (HA) cluster, only the primary unit needs to register and enable remote access from FortiCloud.

To enable remote access from FortiCloud using the GUI:

1. Go to *Dashboards* > *Status*.
2. In the *License Information* widget, click the edit icon for *FortiCloud*.
   The *Cloud Management* dialog opens.
3. Enable *Cloud Management*.
4. In the *Password* field, type the password for the FortiCloud account.
   The *Serial Number* and FortiCloud *Account ID/Email* are automatically populated.
5. Click *OK*.

To enable remote access from FortiCloud using the CLI:

1. Enter the following command to set central management to `cloud-management`:
   ```
   config system central-management
      set type cloud-management
   ```
   If the `central management` type is set to `fortimanager` (default) or `none`, remote access from FortiCloud will be disabled.
2. Enter the following command to log in to FortiCloud:
   ```
   execute cloud-remote-access login <id> <password> <domain> <email confirm>
   ```

Activating add-on licenses

If you have purchased an add-on license and have a FortiCloud account, you can use the *License Information* widget to activate an add-on license. You will need the contract registration code to activate the license.

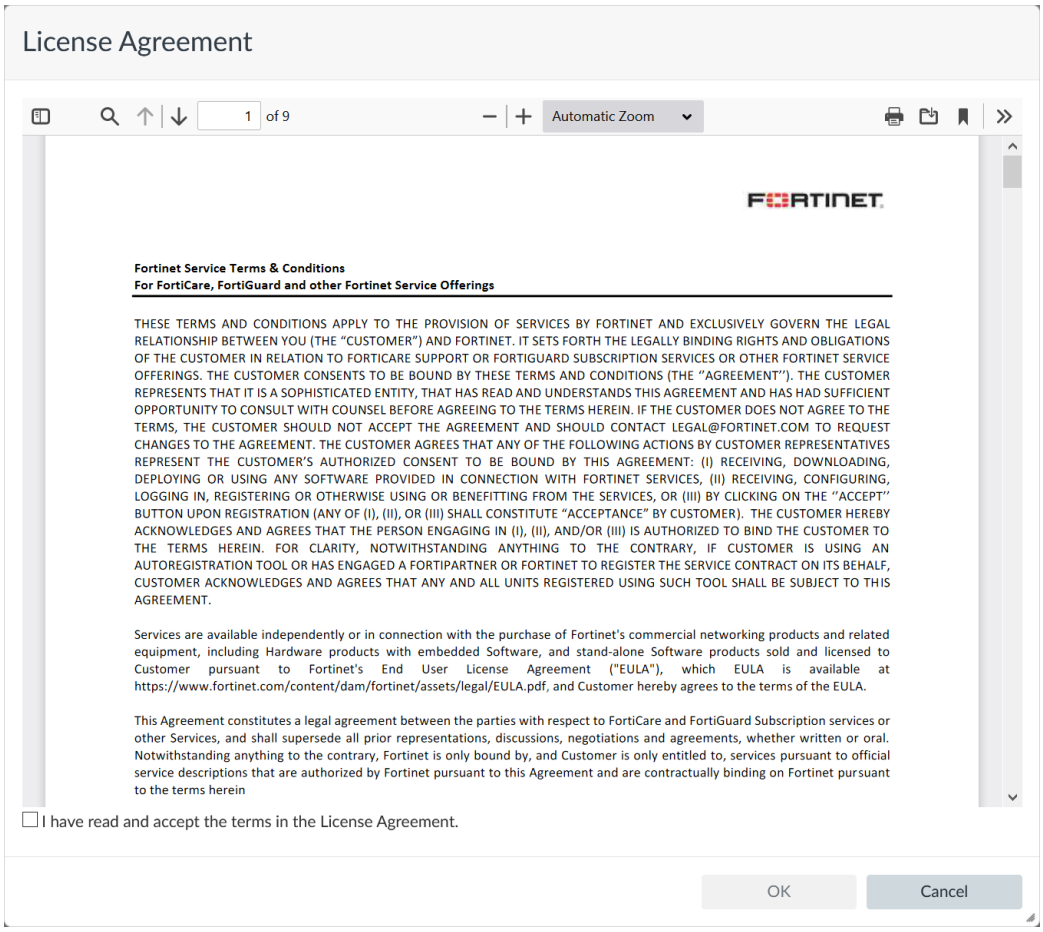
After you enter the contract registration code for the license, FortiAnalyzer communicates with FortiCloud to activate the license.

To purchase a new license:

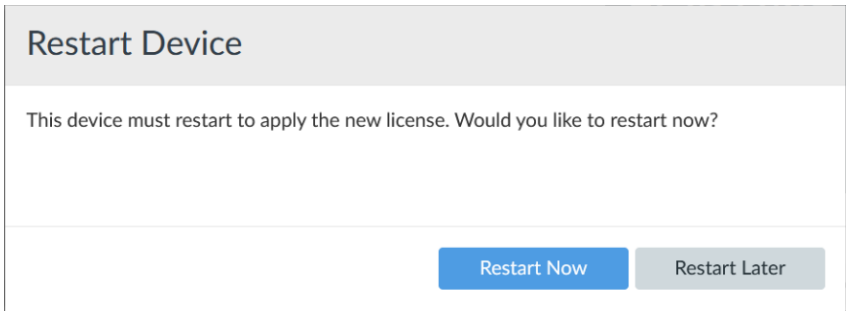
1. Go to the Fortinet Technical Support site at https://support.fortinet.com/.
2. Log in by using your FortiCloud account credentials.
3. Purchase a license.
   You will receive an email from Fortinet with a PDF attachment that includes a contract registration code.

To add a license:

1. Go to *Dashboards* > *Status*.
2. In the *License Information* widget, beside the *VM License* option, click the *Add License* button.
   The *Add License* dialog box is displayed.
3. Complete the following options, and click *OK*:
   a. In the *Account ID/Email* box, type the email for your FortiCloud account.
   b. In the *Password* box, type the password for your FortiCloud account.
   c. In the *Registration Code* box, enter the contract registration code for the add-on license.
   The *License Agreement* is displayed.



4. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *OK*.
   The *Restart Device* dialog box is displayed.



5. Click *Restart Now* to apply the license.
   FortiAnalyzer restarts, and the license is applied.
6. Go to *Dashboard* > *License Information* widget.
   The *VM License* option displays *Valid <license name>*.

Migrating FortiAnalyzer-VM licenses

You can apply a VM subscription license (VM-S) on top of an existing FortiAnalyzer-VM license, allowing you to migrate your FortiAnalyzer-VM (perpetual) to the VM-S (subscription) model. FortiAnalyzer will use the new license's serial number and notify all connected FortiGate models of the change.

Alternatively, you can migrate an existing subscription license to a perpetual license using the same process.

To migrate a license:

1. Download your new subscription license file from FortiCare, which includes the new serial number.
2. In the FortiAnalyzer-VM CLI, run the following command:
   ```
   execute migrate serial-number-list <new serial number>
   ```
   After running the command, OFTP will automatically restart.
3. After a short wait, run the following command in the FortiAnalyzer CLI to ensure that each FortiGate is connected to the FortiAnalyzer.
   ```
   diagnose test application oftpd 3
   ```
4. Install the new license file through the FortiAnalyzer GUI.
   FortiAnalyzer will automatically reboot once the license file has been added.
5. After the FortiAnalyzer reboots, use the following CLI commands on FortiAnalyzer to verify that FortiGate devices are able to connect and send logs, and check that the new serial number and license information has been migrated on FortiAnalyzer.
   ```
   diagnose test application oftp 3
   diagnose debug vminfo
   get system status
   ```

License expiration

This topic explains what licenses are available for FortiAnalyzer and what occurs when they expire.

You can see the current status of FortiAnalyzer licenses in the license information widget. See License Information widget on page 63.

License type	Expiration impact
FortiAnalyzer VM	
Trial License (Evaluation)	Expiration impact not applicable. The trial license is free, limited, and non-expiring. It is available with a FortiCare account. Only one free trial per product, per account, can be active at a time. For more information, see the FortiAnalyzer VM Trial License Guide.
VMS (Subscription)	FortiAnalyzer can no longer manage devices or provide update services. If the FortiAnalyzer VM's license expires for an HA member, the unlicensed member will no longer be connected in the HA cluster. The configuration sync status is `negotiating` for the unlicensed member. You will not be able to show the HA status from the unlicensed member.
VM (Perpetual)	Expiration impact not applicable. The perpetual license does not expire.  The serial number prefix distinguishes if the FortiAnalyzer VM has a perpetual or subscription license: • Perpetual: FAZ-VMTM# • Subscription: FAZVMSTM# To migrate VM licenses, see Migrating FortiAnalyzer-VM licenses on page 68.
FortiCare Support	FortiCare services included with *FortiCare Elite* or *FortiCare Premium* are suspended, including *Firmware & General Updates* and *Enhanced Support* coverage.
Firmware & General Updates `FMWR`	Firmware upgrades are suspended.
Enhanced Support `ENHN`	Access to FortiCare support services are suspended. FortiCare support is included as part of either your FortiCare Premium or FortiCare Elite subscription.
FortiAI Assistant Subscription `AISN`	Access to the FortiAI assistant is restricted and you can not access the assistant chat to prompt it with questions or commands.
FortiAI Token Top-up License `AITK`	The topup tokens will no longer be available for use in the FortiAI assistant. If you have added multiple FortiAI Token Top-up Licenses, the newly added license will be activated after the previous license expires with no interruption.
FortiGuard	Access to features with the existing objects already retrieved from FortiGuard is still available; however, FortiAnalyzer will no longer receive updates or new objects from FortiGuard.

License type	Expiration impact
FortiTIP `TIPE`	Hyperlinks to outbreaks or threat intel are no longer accessible through the FortiAnalyzer GUI.
Indicators of Compromise Service `PBDS`	Indicators of compromise are still identified using the existing TIDB package on the FortiAnalyzer. The updated TIDB packages will not be downloaded by FortiAnalyzer.
Outbreak Detection Service `FOAS`	*Outbreaks Alerts* still displays alerts already received from FortiGuard and existing outbreak alert event handlers and reports remain in the FortiAnalyzer. New alerts are not added to the *Outbreak Alerts* pane and new outbreak alert event handlers and reports will not be downloaded from FortiGuard.
Security Automation `SOAR`	Previously downloaded content pack objects, including reports, event handlers, log parsers, and playbooks, remain on the FortiAnalyzer. These objects will not be updated from FortiGuard and new content pack objects will not be added.
Industrial Security Service `ISSS`	OT information already received in FortiAnalyzer will still be visible in FortiAnalyzer dashboards and reports. Further OT information will not be added to FortiAnalyzer.
Security Rating Update `FGSA`	Security rating information already received in FortiAnalyzer will still be visible in FortiAnalyzer dashboards and reports. Further security rating information will not be added or updated in FortiAnalyzer.
Storage Connector Service `SCPC`	FortiAnalyzer can no longer be configured to forward logs to cloud storage. The logs already on the cloud storage will still be available.

The table below displays the name of the licenses as found in FortiCare and the FortiAnalyzer GUI and CLI.

FortiCare	License Information widget	CLI*
VM License	VMS License	VMLS VM license
ADOM Subscription**	ADOM License**	Not visible
Enhanced Support	Not visible	ENHN Enhanced Support
Firmware & General Updates	Not visible	FMWR Firmware & General Updates
Telephone Support	Not visible	COMP Telephone Support
Hardware Coverage	Not visible	Not visible
FortiAI Subscription	FortiAI License	AISN FortiAI Subscription
AI Token	FortiAI Token Top-up License	AITK

FortiCare	License Information widget	CLI*
FortiGuard		
FortiTIP Enterprise Subscription	FortiTIP	TIPE FortiTIP Service
FortiGuard IOC	Indicators of Compromise Service	PBDS post breach detection / FortiGuard IOC
FAZ Outbreak Alert Service	Outbreak Detection Service	FOAS FAZ Outbreak Alert Service
FortiAnalyzer Security Automation	Security Automation	SOAR SOAR and SIEM bundle service / FortiAnalyzer Security Automation
FortiGuard OT Security Service	Industrial Security Service	ISSS FortiGuard OT Security Service
FortiGuard Attack Surface Security Service	Security Rating Update	FGSA FortiGuard Attack Surface Security Service
Not visible	Storage Connector Service	SCPC cloud storage service
Not visible	Not visible	FRVS Vulnerability Management

*The licenses can be viewed in the FortiAnalyzer CLI using the following commands:

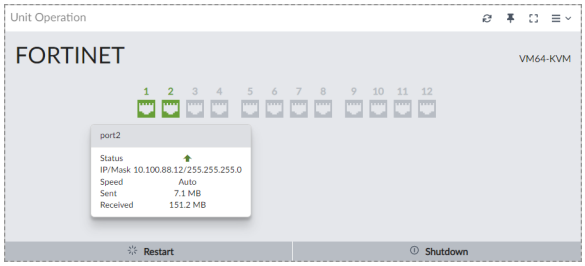
- `diagnose license list`
- `diagnose fmupdate dbcontract`

** Only displayed for the subscription VM license type. This option is not visible for perpetual licenses.

Unit Operation widget

The *Unit Operation* widget graphically displays the status of each port. The port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection.

Hover the cursor over the ports to view a pop-up that displays the full name of the interface, the IP address and netmask, the link status, the speed of the interface, and the amounts of sent and received data.

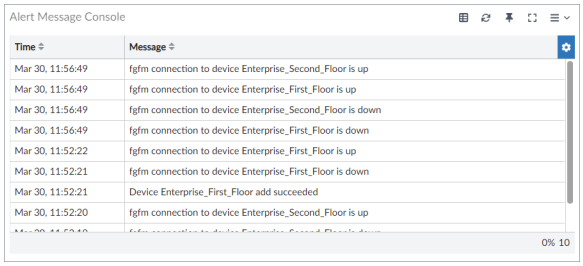


Alert Messages Console widget

The *Alert Message Console* widget displays log-based alert messages for both the FortiAnalyzer unit itself and connected devices.

Alert messages help you track system events on your FortiAnalyzer unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time the event occurred.

Alert messages can also be delivered by email, syslog, or SNMP.



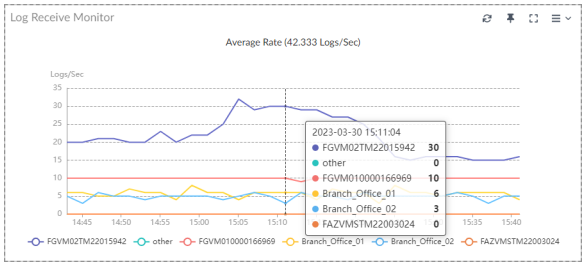
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

To view a complete list of alert messages, click *Show More* from the widget toolbar. The widget will show the complete list of alerts. To clear the list, click *Delete All Messages*. Click *Show Less* to return to the previous view.

Log Receive Monitor widget

The *Log Receive Monitor* widget displays the rate at which the FortiAnalyzer unit receives logs over time. Log data can be displayed by either log type or device.

Hover the cursor over a point on the graph to see the exact number of logs that were received at a specific time. Click the name of a device or log type to add or remove it from the graph. Click *Edit* in the widget toolbar to modify the widget's settings.



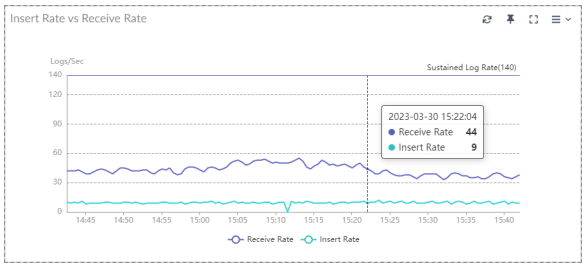
Insert Rate vs Receive Rate widget

The *Insert Rate vs Receive Rate* widget displays the log insert and log receive rates over time.

- Log receive rate: how many logs are being received.
- Log insert rate: how many logs are being actively inserted into the database.

If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.

Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted at a specific time. Click *Receive Rate* or *Insert Rate* to remove those data from the graph. Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval.

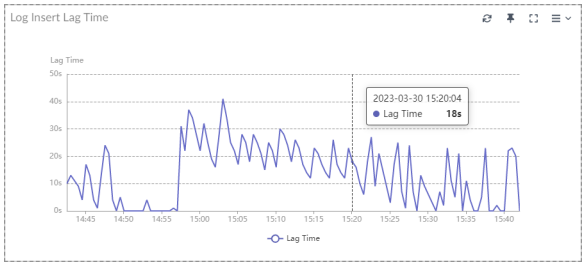


This widget is hidden when FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.

Log Insert Lag Time widget

The *Log Insert Lag Time* widget displays how many seconds the database is behind in processing the logs.

Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval (0 to disable) of the widget.

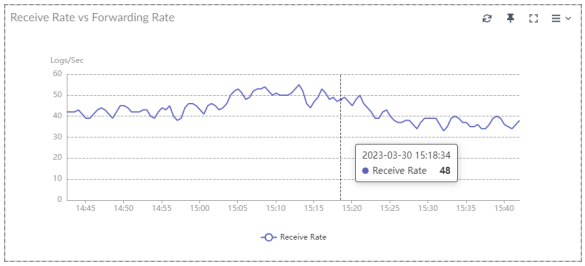


This widget is hidden when FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.

Receive Rate vs Forwarding Rate widget

The *Receive Rate vs Forwarding Rate* widget displays the rate at which the FortiAnalyzer is receiving logs. When log forwarding is configured, the widget also displays the log forwarding rate for each configured server.

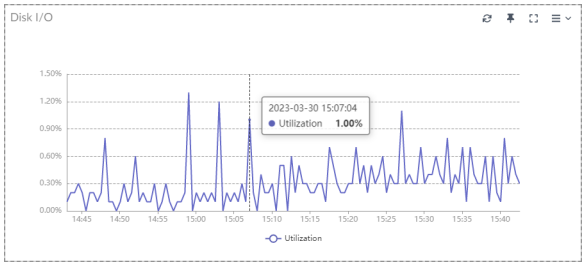
Click the edit icon in the widget toolbar to adjust the time period shown on the graph and the refresh interval, if any, of the widget.



Disk I/O widget

The *Disk I/O* widget shows the disk utilization (%), transaction rate (requests/s), or throughput (KB/s), versus time.

Click the edit icon in the widget toolbar to select which chart is displayed, the time period shown on the graph, and the refresh interval (if any) of the chart.



Device widgets

The following widgets in *Dashboards* > *Status* provide a summary of the devices that are added and authorized in the FortiAnalyzer. These widgets link to other panes in the GUI, which provide more detailed information.

Click one of the following widgets to open *Device Manager*. For more information, see Device Manager on page 83

- *Log Status*
- *Disk Quota Usage*

- *Last Log Time*

FortiAnalyzer Cloud Status widget

The *FortiAnalyzer Cloud Status* widget displays the status of the FortiAnalyzer Cloud instance according to the connector. This includes the following information about the connected FortiAnalyzer Cloud instance:

- *Entitled Usage GB/day*
- *Used GB/day*

You can use the following commands in the on-premise FortiAnalyzer CLI to troubleshoot the FortiAnalyzer Cloud connector:

- To check if the token has been configured correctly on the FortiAnalyzer Cloud connector:

```
diagnose test application logfwd 3
```

- To check if the connection is successful and to view the log forwarding rate:

```
diagnose test application logfwd 4
```

For more information about the FortiAnalyzer Cloud connector, see Connector actions on page 364.

Restart, shut down, or reset FortiAnalyzer

Always use the operation options in the GUI or the CLI commands to reboot and shut down the FortiAnalyzer system to avoid potential configuration problems.

Restarting FortiAnalyzer

To restart the FortiAnalyzer unit from the GUI:

1. Go to *Dashboards* > *Status*.
2. In the *Unit Operation* widget, click the *Restart* button.
3. Enter a message for the event log, then click *OK* to restart the system.

To restart the FortiAnalyzer unit from the CLI:

1. From the CLI, or in the *CLI Console* menu, enter the following command:

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

2. Enter *y* to continue. The FortiAnalyzer system will restart.

Shutting down FortiAnalyzer

To shutdown the FortiAnalyzer unit from the GUI:

1. Go to *Dashboards* > *Status*.
2. In the *Unit Operation* widget, click the *Shutdown* button.
3. Enter a message for the event log, then click *OK* to shutdown the system.

To shutdown the FortiAnalyzer unit from the CLI:

1. From the CLI, or in the *CLI Console* menu, enter the following command:
```
execute shutdown
The system will be halted.
Do you want to continue? (y/n)
```
2. Enter y to continue. The FortiAnalyzer system will shutdown.

Resetting system settings

FortiAnalyzer settings can be reset to factory defaults using the CLI.

To reset settings to factory defaults:

1. From the CLI, or in the *CLI Console* menu, enter the following command:
```
execute reset {adom-settings | all-except ip | all-settings | all-shutdown}
```

Variable	Description
`adom-settings <adom> <version> <mr> <ostype>`	Reset an ADOM's settings. • `<adom>`: The ADOM name. • `<version>`: The ADOM version. • `<mr>`: The major release number. • `<ostype>`: Supported OS type.
`all-except-ip`	Reset all settings except the current IP address and route information.
`all-settings`	Reset to factory default settings.
`all-shutdown`	Reset all settings and shutdown.

2. Enter y to continue. The device will reset settings based on the type of reset performed. For example, `execute reset all-settings` will reset all FortiAnalyzer to factory defaults.

IOT dashboard

The *IOT Dashboard* displays information about Operation Technology (OT) and Internet of Things (IoT) devices.

License requirements:

- To display OT devices in this dashboard, the FortiAnalyzer and FortiGate devices must have OT Security Service entitlements.
- To display IoT devices in this dashboard, the FortiGate devices must be licensed for the IoT Detection Service.

FortiOS devices must use version 7.4 or higher to send OT information to FortiAnalyzer.

Use the time range dropdown to filter all widgets in the *IOT Dashboard*. After clicking *Edit*, you can select which widgets should appear using the *Toggle Widget* dropdown. You can also resize and move widgets according to your preference. Once the changes are complete, click *Save* to save the changes, or click *Reset* to reset to the default settings.

By default, the *Total Devices* and *IoT Devices* widgets display at the top of the dashboard. The following counts are included in these widgets:

Count	Description
Total Devices	The total number of devices, including network devices, endpoints devices, and IoT/OT devices.
New Devices	The number of newly added devices in the selected time range.
Identified	The number of devices that can be recognized using the existing device detection method.
Unidentified	The number of devices that cannot be recognized.
Total IoT Devices	The total number of detected IoT devices.
New IoT Devices	The number of newly added IoT devices in the selected time range.

There are also seven other widgets providing further details about the OT/IoT devices:

Widget	Description
Device Category	A donut chart of the device categories for all devices. The available device categories are listed on the FortiGuard website.
IoT Vendors	A donut chart of the vendors that manufacture the IoT devices.
Vulnerabilities by Vendor	A donut chart of vulnerabilities detected from the IoT devices grouped by the device vendor.
New Devices Detected	A line chart of all new devices detected over the selected time range by device category.
Alerts Distribution	A sankey chart that displays the number of alerts sorted by severity (Critical, High, Medium), and then further sorted by device category.
Top IoT Devices with Vulnerabilities	Lists the top 5 IoT devices by highest number of Critical and High vulnerabilities.
IoT Devices with Internet Connection	Lists all IoT devices that have traffic going to the internet.

Email metrics dashboard

The *Email Metrics* dashboard correlates FortiMail logs and FortiGate logs to provide visibility for email traffic.



FortiAnalyzer requires FortiMail logs to display this dashboard.

Use the time range dropdown and device dropdown to filter all widgets in the dashboard. You can customize which widgets appear in the dashboard as well. After clicking *Edit*, select which widgets should appear using the *Toggle Widget* dropdown. You can also resize and move widgets in this display. Once the changes are complete, click *Save*.

The following widgets are available in *Email Metrics*:

Widget	Description
Utilization	Displays an overview of email traffic in the network. This includes the following: • *Average Emails Processed Per Day* • *Average Emails Bandwidth Per Day* • *Average Emails Size*
Productivity	Displays data primarily related to mass recipient emails, including *Email Flagged as Spam* and *Suspected Newsletter*. This widget also includes a count for E*mails Detected with Adult Content*.
Security	Displays a summary of threats and attacks originated by emails. This includes the following: • *Known or Suspected Attachment-based Attacks* • *Known or Suspected URL-based Attack* • *Known or Suspected Impersonation-based Threats*
Email Bandwidth	An area chart that displays the amount of bandwidth used by email traffic, which includes data for inbound emails and spam emails over time. Mouse over the chart to display a tooltip of values for inbound and spam emails at that time.
Email Count	A stacked bar chart that displays the number of emails over time by inbound emails and spam emails. Mouse over the chart to display a tooltip of values for inbound or spam emails at that sample time.
Top Senders by Email Size	A pie chart that displays the email accounts which have sent the largest emails by size. Mouse over the chart to display a tooltip of the email account and the amount of emails sent by size and percentage.
Top Recipients by Email Size	A pie chart that displays the email accounts which have received the largest emails by size. Mouse over the chart to display a tooltip of the email account and the amount of emails received by size and percentage.

Widget	Description
Top Recipients by Count	A race bar chart that displays the top email accounts with highest number of emails received. The chart is animated to show the number of emails for each account over time.
Top Senders by Count	A race bar chart that displays the top email accounts with highest number of emails sent. The chart is animated to show the number of emails for each account over time.
Top Malware Senders	Displays email accounts that have sent the highest number of malwares using email.
Top Phishing Senders	Displays email accounts with the highest number of attempts to send phishing emails.
Top Spam Senders	Displays spammer email accounts sorted by email count.

SOC dashboard

The *SOC Dashboard* provides an overview of incidents, events, and alerts. By clicking on widgets in the dashboard, you can open the detailed information in the *Incidents & Events* pane, as well as other panes in the FortiAnalyzer GUI.

Use the time range dropdown to filter all widgets in the *SOC Dashboard*. You can customize which widgets appear in the dashboard. After clicking *Edit*, select which widgets should appear using the *Toggle Widget* dropdown. You can also resize and move widgets in this display. Once the changes are complete, click *Save*.

By default, the *Statistics* widget displays at the top of the dashboard. The following is available in the *Statistics* widget in the *SOC Dashboard*:

Statistic	Description
High Severity Incidents	Displays the number of high severity incidents within the filtered time range. Click the card to open *Incidents & Events > Incidents*, filtered by high severity and the same time range as *SOC Dashboard*.
Outbreak Alerts	Displays the number of outbreak alerts within the filtered time range. Click the card to open *Incidents & Events > Event Monitor > All Events*, filtered by `triggername=*outbreak*` and the same time range as *SOC Dashboard*.
Compromised Host	Displays the number of compromised hosts within the filtered time range. Click the card to open *FortiView > Threats > Indicator of Compromise*, filtered by the same time range as the *SOC Dashboard*.
Affected Users	Displays the number of the affected User IDs according to the chosen time range. Click the card to open the Identity tab in *Fabric View > Asset Identity Center > Asset Identity List*, filtered by the User ID and the same time range as the *SOC Dashboard*.

Statistic	Description
Active Connector	Displays the number of active connectors. Click the card to open *Incidents & Events > Automation > Connectors*.
Device Types	Displays the number of unique platforms. Click the card to open *Device Manager*.

In addition to the *Statistics* widget, the following widgets are also available in the *SOC Dashboard*:

Widget	Description
Events Map	Displays the top events with their affected endpoints and the severity of events (critical, high, medium, low) within the filtered time range and sorted by the number of events.
Incident Category	Displays the number of incidents by incident category within the filtered time range. Click a bubble to open *Incidents & Events > Incidents*, filtered by category and the same time range as *SOC Dashboard*.
Top Incidents	Displays the top incidents sorted by severity. Click an entry to open the *Incident Analysis* pane for that incident.
Events and Incidents	Displays the log types, events severity, and incident severity. Mouse over to display the number of events and the number of incidents generated by events.
Connector Health	Displays the connectors' icons, names, and status.

Endpoint vulnerability dashboard

To collect information for the managed endpoint vulnerability dashboard:



This dashboard uses Fabric logs, which are only available in Fabric ADOMs.

You must add the FortiClient EMS as an authorized device and create a FortiClient EMS Connector in a Fabric ADOM to populate this dashboard.

1. In FortiAnalyzer, go to a Fabric ADOM.
2. In *Incidents & Events > Automation > Active Connectors*, create a new FortiClient EMS Connector. See Configuring security fabric connectors on page 372.

   Once the FortiClient EMS Connector is configured, the *Update Asset, Identity and Vulnerability in Sequence* playbook is automatically created in *Incidents & Events > Automation > Playbook* . This default playbook gets the endpoints and their vulnerabilities from EMS. It is scheduled to run once per day, but it can be edited according your needs.
3. In *Incidents & Events > Automation > Playbook*, enable the *Update Asset, Identity and Vulnerability in Sequence* playbook for the FortiClient EMS Connector. See Playbooks on page 382.

4. In *Fabric View* > *Asset Identity Center* > *Asset Identity List*, add the FortiClient EMS Connector as a data source.
   a. In *Fabric View* > *Asset Identity Center* > *Asset Identity List*, click *More* > *Data Sources*.
      The *Data Source Selection* dialog displays.
   b. Click *Create New*.
   c. From the *Data Source* dropdown, select *EMS Connector*.
   d. Enable the *Status*.
   e. For the *Connectors* field, select the EMS connector that you have created.
   f. Click *OK*.
5. In *Device Manager*, add the FortiClient EMS as an authorized device.
   a. In *Device Manager*, click *Add Device*.
      The *Add Device* dialog displays.
   b. In the *Name* field, enter a name for the FortiClient EMS.
   c. For *Link Device By*, select *Serial Number*.
   d. In the Serial Number field, enter the serial number for the FortiClient EMS.
      The *Device Model* field automatically populated with *FortiClient-EMS*.
   e. Click *Next*.
      The dialog displays the status for adding the device and confirms when the device is succesfully added.

   The FortiClient EMS will receive the related endpoint vulnerabilities logs.

   When the *Update Asset, Identity and Vulnerability in Sequence* playbook is run, it will call the EMS API to get all endpoints and vulnerabilities data, and it will be inserted as Fabric (SIEM) logs. The predefined EMS-Connector Log Parser is automatically assigned to the device to parse the logs; you can find this parser and confirm its assignment in *Incidents & Events* > *Log Parser*.

   Multiple EMS connectors are supported. If needed, repeat the steps to create another EMS connector.

The *Endpoint Vulnerability* dashboard displays endpoint vulnerability information from EMS connectors. It includes the following widgets:

Widget	Description
Endpoints by Vulnerability Severity	A donut chart displaying the endpoints by vulnerability severity.
Vulnerability Age Distribution (Total Count)	Donut charts displaying vulnerabilities (total and unique) by age.
Vulnerability Age Distribution (Unique Vuln)	
Top 10 Vulnerable Windows	Bar charts displaying the endpoints with the largest number of critical and high vulnerabilities.
Top 10 Vulnerable MacOS	
Top 10 Vulnerable Linux	

Widget	Description
Historical Trends Windows	Line charts displaying the historical trends of vulnerabilities by severity.
Historical Trends MacOS	
Historical Trends Linux	
Top Vuln App Trend	A line chart displaying the top vulnerable apps over time.
Vuln Per Category	A bar chart displaying the number of vulnerabilities by category.
Top 20 Vulnerable Applications	A bar chart displaying the number of critical and high vulnerabilities by application.
Top 10 Vulnerabilities Windows	Tables displaying the top vulnerabilities.
Top 10 Vulnerabilities MacOS	
Top 10 Vulnerabilities Linux	
Top 20 Users Own Multiple Devices	A table displaying the users, including their number of unique hosts and a list of their devices.

XDR dashboard

The *XDR Dashboard* provides a real-time view of all alerts and incidents, including their severity and status. It includes the following widgets:

Widget	Description
XDR Dashboard	The left-side of this widget displays a real-time animation that displays the flow of alerts from Fortinet devices. Whenever an alert is added, it is added to the total Alerts count and shown coming from the device. The Alerts count is the total number of alerts that occurred within the filtered time range. The right-side of this widget displays the total number of Incidents, including counts by severity and status. This information is real-time as well based on the filtered time range.
Critical XDR Alerts	Displays a table view of the alerts with critical severity in the filtered time range. Click an alert to open a separate pane with the alert details. For more information about this pane, see the description for the event details pane in Explorer on page 218.
Alert History	Displays an area graph of stacked alert counts by severity within the filtered time range.

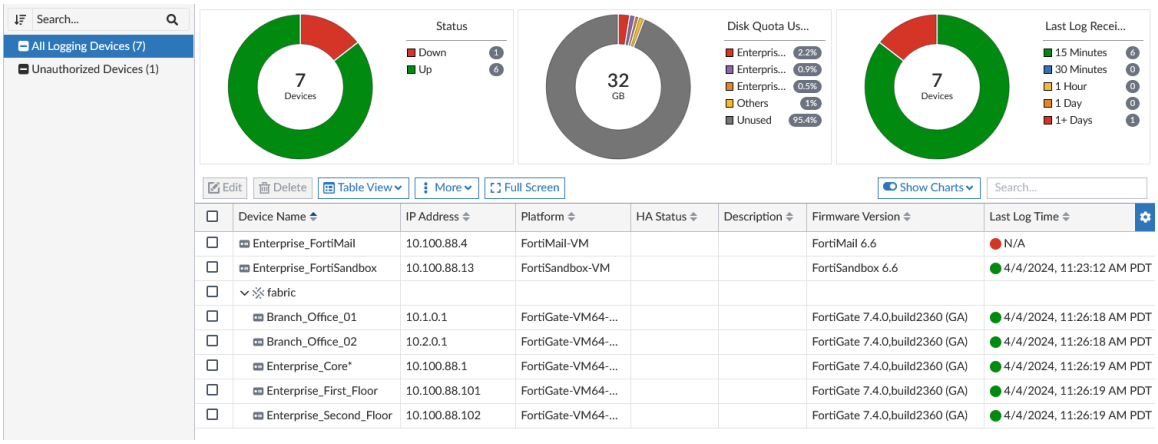
Device Manager

Use the *Device Manager* pane to add, configure, and manage devices and VDOMs.

After you add and authorize a device or VDOM, the FortiAnalyzer unit starts collecting logs from that device or VDOM. You can configure the FortiAnalyzer unit to forward logs to another device. See Log Forwarding on page 518.

You can toggle between a *Table View* and *Map View* from the toolbar in *Device Manager*.

Table View:



Three donut charts display above the list of authorized devices:

- *Status*
- *Disk Quota Usage*
- *Last Log Received Within*

By default, the *Show Charts* toggle is enabled. You can select which charts appear by selecting them in the *Show Charts* dropdown, or you can hide all the charts by disabling the *Show Charts* toggle.

Mouse over the charts to see more information in a tooltip. Click a section of a chart to filter the charts and the table by that information. You can apply multiple filters across the charts. Once filtered, a filter icon appears next to the chart title; click the filter icon to remove the filter.

The colors in the *Disk Quota Usage* donut chart represent different devices, per the legend next to the chart. The colors do not represent an exceeded disk quota. For example, red in the *Disk Quota Usage* chart depicted above represents one of the devices; it does not represent an exceeded disk quota.

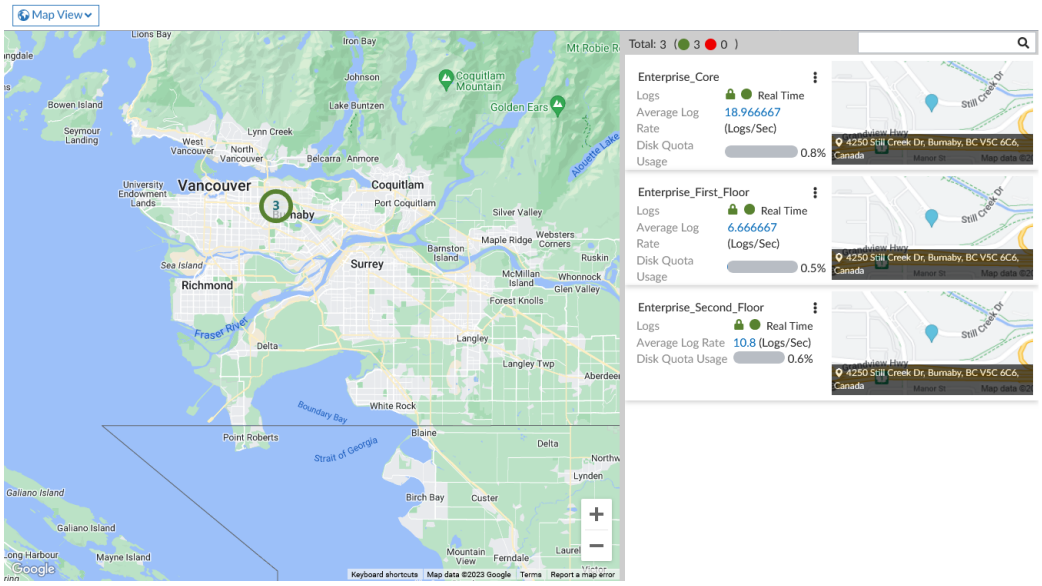
If you create a custom device group, it appears in the *Device & Groups* tree menu. Select the device group to display information about those devices.

The *Device Manager* table view includes the following default columns for authorized devices:

Column	Description
Device Name	Displays the name of the device.
IP Address	Displays the IP address for the device.
Platform	Displays the platform for the device.
HA Status	Displays information if the device is part of a High Availability cluster. You can manually identify devices as part of an HA cluster by editing the device information. See Editing device information on page 94.
Description	Displays a description of the device.
Firmware Version	Displays the firmware version of the device.
Serial Number	Displays the serial number of the device. The serial number is unique to the unit and does not change with firmware upgrades.
Last Log Time	Displays the date and time that the last log was received from the device.
Status	Displays the status of the device as *Up* or *Down*. The *Up*/*Down* state is based on the status of the OFTP connection (if OFTP is supported by the device) and/or the last log receiving time. For near realtime logging, the default log receiving threshold to determine if the device is *Up* or *Down* is 15 minutes. For scheduled uploading, the default is 6 hours. You can configure both of these settings in the `config system log settings` CLI: • `set log-interval-dev-no-logging <interger>`: Set the interval in minutes of no logs received from a device before the device is considered *Down*. • `set log-upload-interval-dev-no-logging <interger>`: Set the interval in minutes of no logs uploaded from a device before the device is considered *Down*.
Logging Mode	Displays the logging mode for the device. A lock icon displays when a secure tunnel is being used to transfer logs from the device to the FortiAnalyzer unit.
Average Log Rate (Logs/Sec)	Displays the average rate at which the device is sending logs to the FortiAnalyzer unit in log rate per second. Click the number to display a graph of historical average log rates.
Disk Quota Usage	Displays how much of the allotted disk storage space has been consumed by logs.

You can mouse-over the colmns to reveal a filter icon. Click the icon to filter the table by information in that column. You can filter by *Contains*, *Exact Match*, and *NOT*. Enter in the *Search* field and click the + icon to add a filter or select a suggestion and click *Apply*. To remove the filter, click the filter icon for the column and select *Remove*.

Map View:



The *Map View* provides an interactive map displaying the physical locations of authorized devices. You can navigate the map by using your mouse. Zoom in or out with the scroll wheel or with the plus (+) or minus (-) buttons on the map. When zoomed in, only the devices that are currently visible on the map are displayed in the sidebar. The sidebar provides information about the devices, including logging status, average log rate, and disk quota usage.

ADOMs

You can organize connected devices into ADOMs to better manage the devices. ADOMs can be organized by:

- Firmware version: group all 7.0 devices into one ADOM, and all 7.2 devices into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Administrator users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.
  FortiAnalyzer, FortiCache, FortiClient, FortiDDos, FortiMail, FortiManager, FortiSandbox, FortiWeb, Chassis, and FortiCarrier devices are automatically placed in their own ADOMs.
- Security Fabric: group all devices that are within the Security Fabric.

Each administrator profile can be customized to provide read-only, read/write, or restrict access to various ADOM settings. When creating new administrator accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your administrator users. For more information on ADOM configuration and settings, see Administrative Domains (ADOMs) on page 498.

FortiClient EMS devices

You can add FortiClient EMS servers to FortiAnalyzer. Authorized FortiClient EMS servers are added to the default FortiClient ADOM. You must enable ADOMs to work with FortiClient EMS servers in FortiAnalyzer. When you select the FortiClient ADOM and go to the *Device Manager* pane, the FortiClient EMS servers are displayed. See also FortiClient support and ADOMs on page 500.

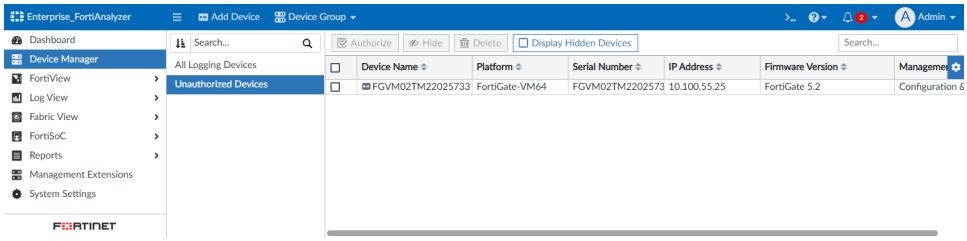
Unauthorized devices

When a device is configured to send logs to FortiAnalyzer but has not yet been authorized, it is displayed in *Device Manager > Device & Groups > Unauthorized Devices*. From this device group, you can authorize, delete, or hide devices by using the toolbar buttons or the right-click menu.

The *Unauthorized Devices* device group is not available when all added devices are authorized.

Enable *Display Hidden Devices* to view devices that were previously hidden.

Click *Return* to view the *Device Manager* pane containing authorized devices.



The *Unauthorized Devices* device group includes the following default columns:

Column	Description
Device Name	Displays the name of the device.
Platform	Displays the platform for the device.
Serial Number	Displays the serial number of the device. The serial number is unique to the unit and does not change with firmware upgrades.
Firmware Version	Displays the firmware version of the device.
IP Address	Displays the IP address for the device.
Management Mode	Displays the management mode of the device.

Using FortiManager to manage FortiAnalyzer devices

You can add FortiAnalyzer devices to FortiManager and manage them. When you add a FortiAnalyzer device to FortiManager, FortiManager automatically enables FortiAnalyzer features. FortiAnalyzer and FortiManager must be running the same OS version, at least 5.6 or later.

Logs are stored on the FortiAnalyzer device, not the FortiManager device. You configure log storage settings on the FortiAnalyzer device; you cannot change log storage settings using FortiManager.

For more information, see *Adding FortiAnalyzer devices* in the FortiManager Administration Guide.

In *Device Manager* on FortiAnalyzer, a message informs you the device is managed by FortiManager and all changes should be performed on FortiManager to avoid conflict. The top right of this pane displays a lock icon. If ADOMs are enabled, the *System Settings > ADOMs* pane displays a lock icon beside the ADOM managed by FortiManager. When you delete FortiAnalyzer from FortiManager, the ADOM on FortiAnalyzer should be unlocked. If the ADOM remains locked, you will not be able to manage the devices. To unlock the ADOM, enter the following command in the FortiAnalyzer CLI:

```
diagnose dvm adom unlock <adom>
```

For more information about this command, see the FortiAnalyzer CLI Reference.

Adding devices

You must add and authorize devices and VDOMs to FortiAnalyzer to enable the device or VDOM to send logs to FortiAnalyzer. Authorized devices are also known as devices that have been promoted to the DVM table.



You must configure devices to send logs to FortiAnalyzer. For example, after you add and authorize a FortiGate device with FortiAnalyzer, you must also configure the FortiGate device to send logs to FortiAnalyzer. In the FortiGate GUI, go to *Log & Report > Log Settings*, and enable *Send Logs to FortiAnalyzer/FortiManager*.

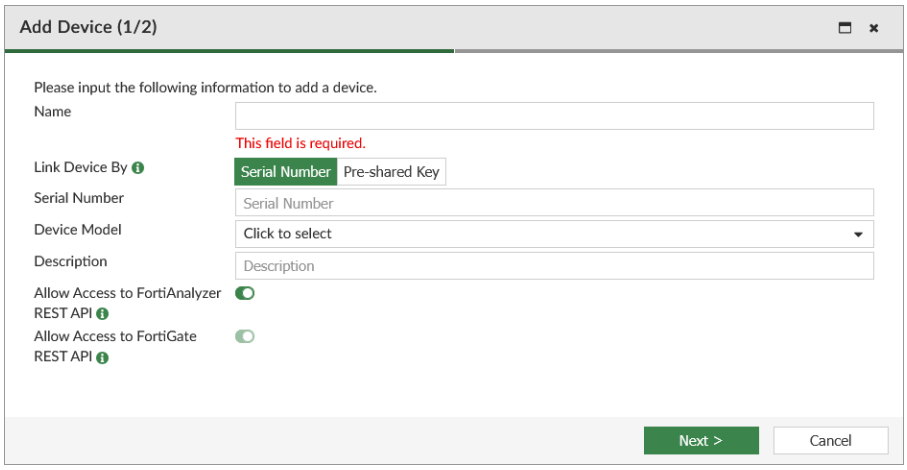
Adding devices using the wizard

This section describes how to add model devices and VDOMs to the FortiAnalyzer using zero-touch provisioning (ZTP).

When using the *Add Device* wizard, model devices added to the FortiAnalyzer unit using a serial number are authorized and are ready to begin sending logs. When a FortiGate model is configured using a pre-shared key, you must also configure the key on the device itself before it will be authorized on FortiAnalyzer.

To add devices using the wizard:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* and click *Add Device*.
   The Add Device wizard opens. You can add devices by serial number or pre-shared key.



3. Configure the following settings:

Name	Type a name for the device.
Link Device By	Select *Serial Number* or *Pre-shared Key*. Depending on your selection, the device model will automatically link to a real device by serial number or configured pre-shared key.
Serial Number	Enter the device's serial number.
Pre-shared Key	Enter a pre-shared key for the device. If using a pre-shared key, each device must have a unique pre-shared key Only FortiGate devices can be added to FortiAnalyzer using a pre-shared key. You must also configure this pre-shared key on the corresponding FortiGate device. See Configuring a pre-shared key on FortiGate on page 88
Device Model	Select the model of the device from the dropdown.
Description	Type a description of the device (optional).
Allow Access to FortiAnalyzer REST API	Enable to allow the authorized FortiGate device to consume the FortiAnalyzer's REST API.
Allow Access to FortiGate REST API	This toggle is read-only. This setting indicates if the device allows FortiAnalyzer to access its JSON APIs configured on the device side. This setting must be configured on the FortiGate.

4. Click *Next*.
   The device is added to the ADOM and, if successful, is ready to begin sending logs to the FortiAnalyzer unit.
5. Click *Finish* to finish adding the device and close the wizard.

Configuring a pre-shared key on FortiGate

When configuring a FortiGate model device on FortiAnalyzer using a pre-shared key, the pre-shared key must also be configured on FortiGate using the following CLI commands. This can be done after the FortiGate has been configured to send logs to FortiAnalyzer in *Log & Report > Log Settings*.

To configure a pre-shared key on FortiGate:

1. In the FortiGate CLI, enter the following commands.
```
config log fortianalyzer setting
   set preshared-key <pre-shared key>
```

Authorizing devices

You can configure supported devices to send logs to the FortiAnalyzer device. These devices are displayed in the root ADOM as unauthorized devices. You can quickly view unauthorized devices by clicking *Unauthorized Devices* in the quick status bar. You must authorize the devices before FortiAnalyzer can start receiving logs from the devices.

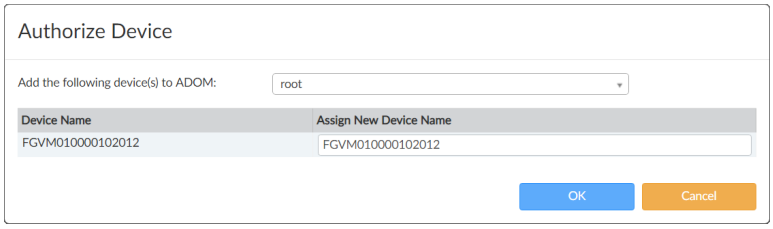
When ADOMs are enabled, you can assign the device to an ADOM. When authorizing multiple devices at one time, they are all added to the same ADOM.

By default, FortiAnalyzer expects you to use the default admin account with no password. If the default admin account is no longer usable, or you have changed the password, the device authorization process fails. If the device authorization fails, delete the device from FortiAnalyzer, and add the device again by using the *Add Device* wizard, where you can specify the admin login and password.

When you delete a device or VDOM from the FortiAnalyzer unit, its raw log files are also deleted. SQL database logs are not deleted.

To authorize devices:

1. In the root ADOM, go to *Device Manager* and click *Unauthorized Devices* in the quick status bar. The content pane displays the unauthorized devices.
2. If necessary, select the *Display Hidden Devices* check box to display hidden unauthorized devices.
3. Select the unauthorized device or devices, then click *Authorize*. The *Authorize Device* dialog box opens.



4. If ADOMs are enabled, select the ADOM in the *Add the following device(s) to ADOM* list. If ADOMs are disabled, select *root*. The default value is *None*.

If you try to authorize devices having different firmware versions than the selected ADOM version, the system shows a *Version Mismatch Warning* confirmation dialog.

If you authorize the devices in spite of the warning, the configuration syntax may not be fully supported in the selected ADOM.

5. Click *OK* to authorize the device or devices.
The device or devices are authorized, and FortiAnalyzer can start receiving logs from the device or devices.

Hiding unauthorized devices

You can hide unauthorized devices from view, and choose when to view hidden devices. You can authorize or delete hidden devices.

To hide and display unauthorized devices:

1. In the root ADOM, go to *Device Manager* and click *Unauthorized Devices* in the quick status bar. The content pane displays the unauthorized devices.
2. Select the unauthorized device or devices, then click *Hide*.
   The unauthorized devices are hidden from view.
   You can view hidden devices by selecting the *Display Hidden Devices* check box.

Adding an HA cluster

You can use a HA cluster to synchronize logs and data securely among multiple FortiGate devices.

An HA cluster can have a maximum of four devices: one primary device with up to three backup devices. All the devices in the cluster must be of the same FortiGate series and must be visible on the network.



You can use auto-grouping in FortiAnalyzer to group devices in a cluster based on the group name specified in Fortigate's HA cluster configuration. For auto-grouping to work properly, each FortiGate cluster requires a unique group name.

If a unique group name is not used, auto-grouping should be disabled.

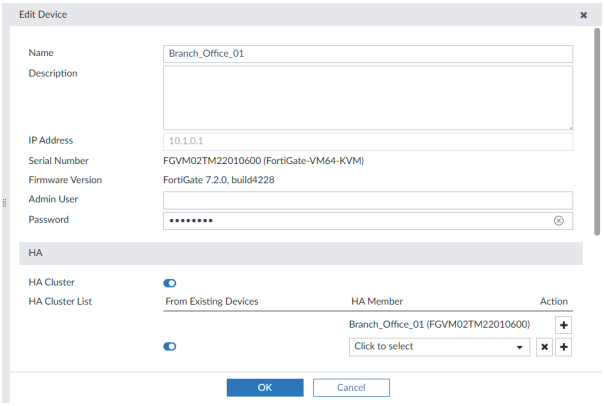
```
FAZ # config system global
   (global)# set ha-member-auto-grouping disable
```

FortiAnalyzer supports FortiGate HA cluster contracts with virtual serial numbers (vSN). To confirm the vSN in the FortiAnalyzer CLI, use the following command: `diagnose dvm device list`. The command output will include the "`logical-sn`" of the FortiGate HA cluster.

To create a HA cluster:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Add the devices to the *Device Manager*.
3. Choose a primary device, and click *Edit*.
4. In the *Edit Device* pane, enable *HA Cluster*.
5. In the *Action* column, click the *Add* icon.

6. In the *Add Existing Device* column, enable the toggle to select an existing device from the dropdown.



Alternatively, you can disable the toggle and enter the Serial Number of the device.



Adding the devices before you create the HA is recommended.

7. Add more devices to the HA cluster as necessary, and click *OK*.
   The maximum is three backup devices.

To view the HA in the *Device Manager*, click *Column Settings* > *HA Status*.

Adding a FortiGate using Security Fabric authorization

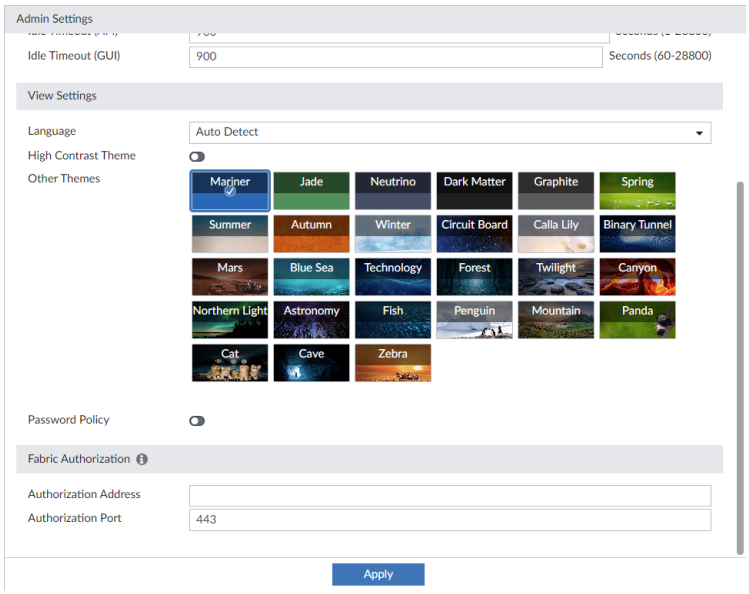
The following steps describe how to add and authorize a FortiGate device on FortiAnalyzer through the FortiAnalyzer Fabric connector configuration on FortiOS.



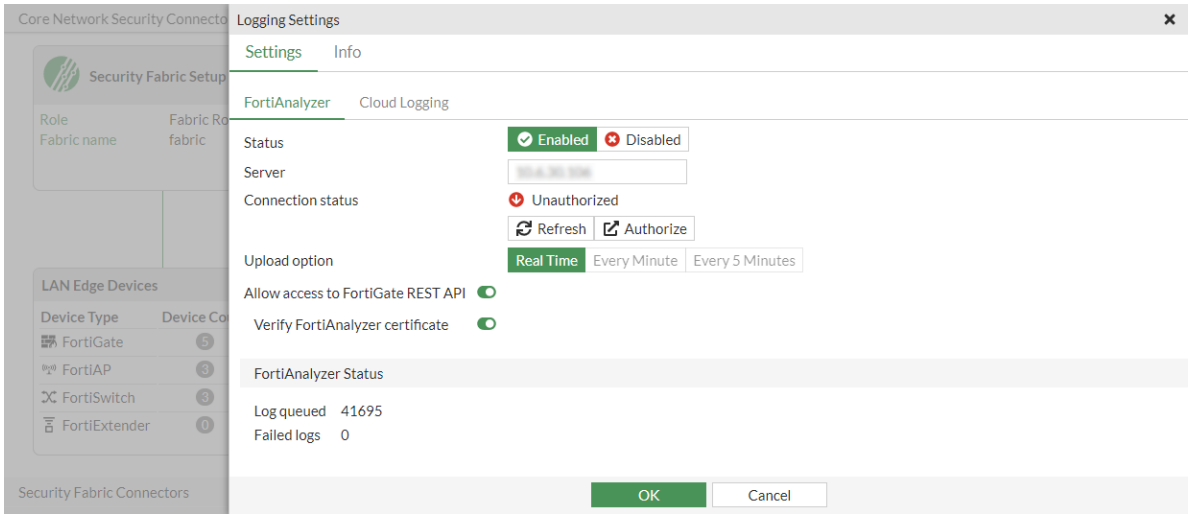
FortiAnalyzer authentication through the FortiGate Fabric connector configuration is available when both FortiAnalyzer and FortiGate devices are on 7.0.1 or higher.

To authorize a FortiGate on FortiAnalyzer using Fabric authorization:

1. In FortiAnalyzer, go to *System Settings* > *Settings* and configure the *Fabric Authorization* address and port.

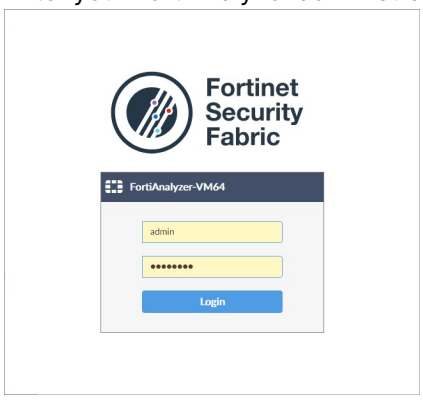


2. On the FortiGate, go to *Security Fabric* > *Fabric Connectors*, and double-click the *Logging & Analytics* card.
3. Select the *Settings* tab, and then select the *FortiAnalyzer* tab.
4. Configure the details of your FortiAnalyzer, including the IP address, and click *OK*.
   The FortiAnalyzer *Connection status* is *Unauthorized*.



5. Click *Authorize*.
   The Fortinet Security Fabric authorization dialog appears.

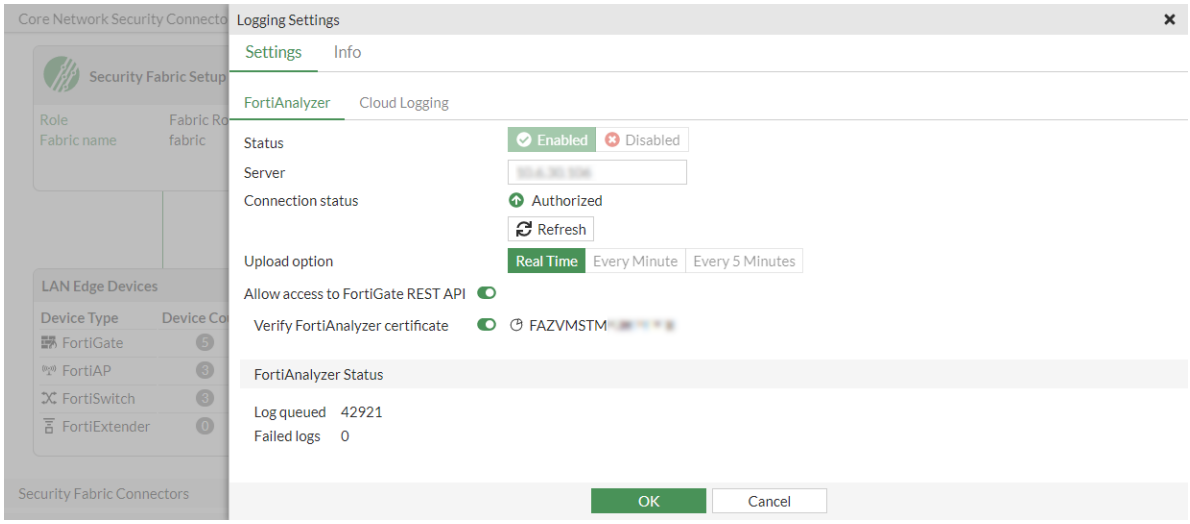
6. Enter your FortiAnalyzer administrator credentials, and click *Login*.



7. Select *Approve* to allow FortiAnalyzer to authorize the FortiGate, and click *OK*.



If the authorization is successful, you will see a message confirming that the FortiGate is authorized by FortiAnalyzer.



8. Log in to FortiAnalyzer, and go to *Device Manager*.
The FortiGate is included in the list of authorized devices.



Managing devices

Use the tools and commands in the *Device Manager* pane to manage devices and VDOMs.

Using the toolbar

The following buttons and menus are available for selection on the toolbar:

Button	Description
Add Device	Opens the *Add Device Wizard* to add a device to the FortiAnalyzer unit. The device is added, but not authorized. Unauthorized devices are displayed in the *Unauthorized Devices* tree menu.
Device Group	Displays menu items including *Create New Group*, *Edit Group*, and *Delete Group*. New device groups are added to the *Device & Groups* tree menu. Select a custom device group to edit or delete it.
Edit	Edits the selected device.
Delete	Deletes the selected devices or VDOMs from the FortiAnalyzer unit. When you delete a device, its raw log files are also deleted. SQL database logs are not deleted.
Table View/Map View	Select the view from the dropdown.
More	Displays more menu items, including *Import Device List* and *Export Device List*.
Full Screen	Toggle the table view to full screen.
Show Charts	Enable or disable the charts that display above the *Table View*. From the dropdown, you can select the charts that display above the *Table View*.
Column Settings	Click to select which columns to display or select *Reset to Default* to display the default columns.
Search	Type the name of a device. The content pane displays the results. Clear the search box to display all devices in the content pane.

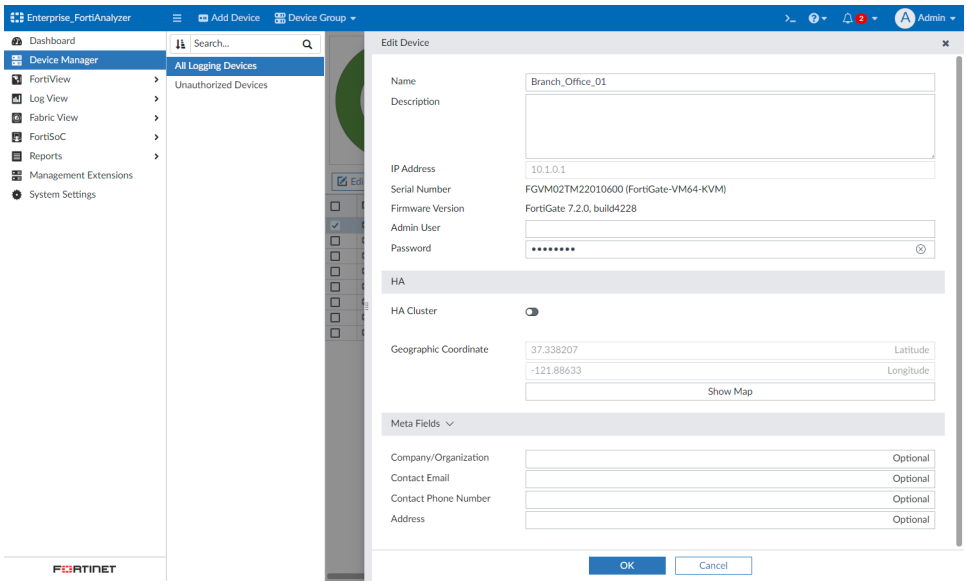
Editing device information

Use the *Edit Device* page to edit information about a device. The information and options available on the *Edit Device* page depend on the device type, firmware version, and which features are enabled.

To edit information for a device or model device:

1. Go to *Device Manager* > *Device & Groups*.
2. In the tree menu, select the device group.

3. In the content pane, select the device or model device and click *Edit*, or right-click on the device and select *Edit*.
   The *Edit Device* pane displays.



4. Edit the device settings and click *OK*.

Name	Change the name of the device.
Description	Type a description of the device.
IP Address	Displays the IP address.
Serial Number	Displays the serial number of the device.
Firmware Version	Displays the firmware version of the device.
Admin User	Change the administrator user name for the device. If the FortiAnalyzer serial number is not specified on the FortiGate or if *Certificate Verification* is disabled, the admin user/password specified here is used by FortiAnalyzer to login to the FortiGate. For more information on Certificate Verification, see the FortiGate/FortiOS CLI Reference.
Password	Change the administrator user password for the device.
Allow Access to FortiAnalyzer REST API	Enable to allow the authorized FortiGate device to consume the FortiAnalyzer's REST API.
Allow Access to FortiGate REST API	This toggle is read-only. This setting indicates if the device allows FortiAnalyzer to access its JSON APIs configured on the device side. This setting must be configured on the FortiGate.
HA Cluster	Select to identify the device as part of an HA cluster, and to identify the other device in the cluster by selecting them from the drop-down list, or by inputting their serial numbers.

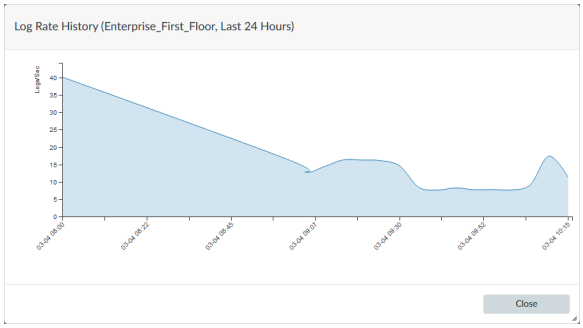
Geographic Coordinate	Displays the latitude and longitude of the device. Click *Show Map* to view and edit the device location. The default location is `0,0`. This field is used to display the location of the device on maps throughout the GUI. See also Google Map integration on page 38.
Meta Fields	Displays default and custom meta fields for the device. Optional meta fields can be left blank, but required meta fields must be defined. See also Setting values for required meta fields on page 97.
Company/Organization	Optionally, enter the company or organization information.
Contact Email	Optionally, enter the contact email.
Contact Phone Number	Optionally, enter the contact phone number.
Address	Optionally, enter the address where the device is located.

Displaying historical average log rates

You can display a graph of the historical, average log rates for each device.

To display historical average logs rates:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* and view your authorized devices.
3. In the *Average Log Rate (Logs/Sec)* column, click the number to display the graph.



4. Hover the cursor over the graph to display more details.

Connecting to an authorized device GUI

You can connect to the GUI of an authorized device from *Device Manager*.

To connect to an authorized device GUI:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager*.
3. Right-click the device that you want to access, and select *Connect to Device*.
4. If necessary, change the port number and click *OK*.
   You are directed to the login page of the device GUI.

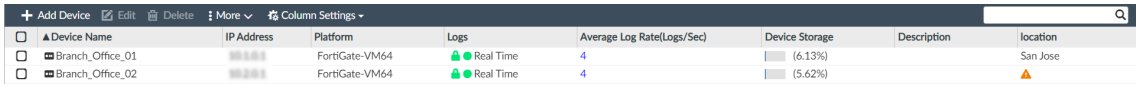
Setting values for required meta fields

When a required meta field is defined for a device object, a column automatically displays on the *Device Manager* pane. The column displays the value for each device. When the required meta field lacks a value, an exclamation mark displays, indicating that you must set the value.

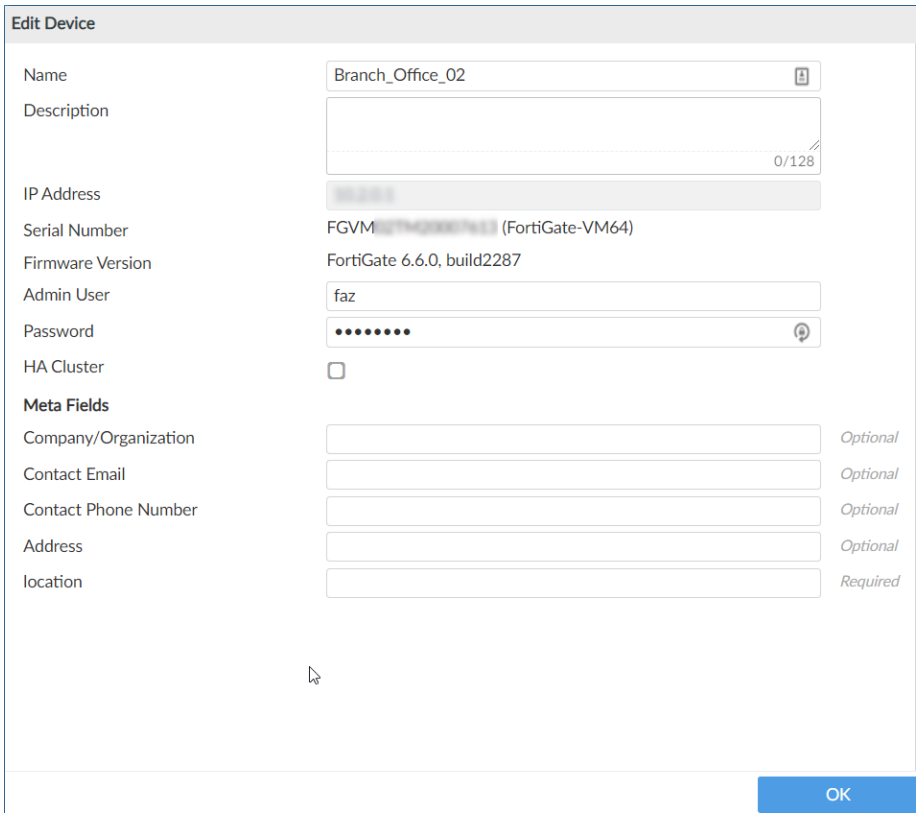
See also Meta Fields on page 541.

To set values for required meta fields:

1. Go to *Device Manager*.
2. View the columns.
   A column displays for required meta fields.
   In the following example, a column named *location* is displayed for the required meta field named *location*. A value of *San Jose* is defined for one device, but no value is defined for the other device.



3. Right-click the device that lacks a value, and select *Edit*.
   The *Edit Device* pane is displayed.



4. Under *Meta Fields*, complete the options labeled as *Required*, and click *OK*. The value displays on the *Device Manager* pane.

Device groups

Device groups are displayed in *Device Manager* > *Device & Groups*. All devices added to FortiAnalyzer are included in a default device group. You can create custom device groups as well to organize devices for convenient selection in other features of FortiAnalyzer.

Type in the *Search* field to search for device groups by name. Click  to sort the list of device groups in ascending or descending alphabetical order. The default device group will always remain at the top of the list. Select the device group to display its list of devices in the *Device Manager* pane.



The maximum number of device groups that can be created is the same as the maximum number of devices/VDOMs supported for your VM license or model. See the FortiAnalyzer data sheet on https://www.fortinet.com/ for information about the maximum number of supported devices/VDOMs for your VM license or device.

Adding device groups

Once created, custom device groups can be selected in device filters for *FortiView* and *Log View*, and they can also be used in event handlers and reports.

To create a custom device group:

1. Go to *Device Manager*.
2. From the *Device Group* dropdown in the toolbar, click *Create New Group*.
   The *Create New Device Group* dialog opens.
3. In the *Group Name* field, type a name to identify the group of devices.
   Description is optional.
4. Click *Add Member* to view the list of devices and existing device groups.
5. Select the check box for each device to add to the group, and click *Add*.



FortiAnalyzer allows nested device groups. For example, you can create *Device Group A* and add it under *Device Group B*.

6. Click *OK*.
   The device group is now available in *Device Manager*.

Managing device groups

You can manage device groups from *Device Manager*. The device groups display in the left-pane. This includes default device groups, such as *All Logging Devices* and *Unauthorized Devices*. Right-click a device group to open the shortcut menu, which is also available from the *Device Group* dropdown.

From the *Device Group* dropdown in the toolbar, select one of the following options:

Option	Description
Create New Group	Create a new device group.
Edit Group	Edit the selected device group. You cannot edit default device groups.
Delete Group	Delete the selected device group. You cannot delete default device groups.

FortiView

Use FortiView to view the *FortiView* and *Monitors* panes.

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

Monitors is designed for network and security operation centers where dashboards are displayed across multiple large monitors.

- FortiView on page 101
- Monitors on page 125



To allow tuning of CPU and memory usage in high capacity environments, you can opt to disable FortiView, which stops the background processing for this feature. See Enabling and disabling FortiView on page 145.

FortiView

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

FortiView allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and others. You can use it to investigate traffic activity such as user uploads/downloads or videos watched on YouTube on a network-wide user group or on an individual-user level.

In *FortiView* dashboards, you can view summaries of log data such as top threats to your network, top sources of network traffic, and top destinations of network traffic.

Depending on which dashboard you are viewing, information can be viewed in different formats: table, bubble, map, or tile. Alternative chart types are available in each widget's *Settings* menu.

For each summary, you can drill down to see more details.

FortiGate, FortiCarrier, and FortiClient EMS devices support *FortiView*.

Some dashboards require that specific log types are enabled before they can be used. When an ADOM does not include any logs of the required type, the dashboard appears in gray and includes an information icon that indicates what logs must be enabled before the dashboard can be used.



The FortiView module, which includes the *FortiView* pane, can be disabled to improve performance in high capacity environments. For more information, see Enabling and disabling FortiView on page 145

How ADOMs affect FortiView

When ADOMs are enabled, each ADOM has its own data analysis in *FortiView*.

Fabric ADOMs will show data analysis from all eligible devices in the Security Fabric.

Logs used for FortiView

FortiView displays data from *Analytics* logs. Data from *Archive* logs is not displayed in *FortiView*. For more information, see Analytics and Archive logs on page 46.

FortiView dashboards

Many dashboards display a historical chart in a table format to show changes over the selected time period.

If you sort by a different column, the chart shows the history of the sorted column. For example, if you sort by *Sessions Blocked/Allowed*, the chart shows the history of blocked and allowed sessions. If you sort by *Bytes Sent/Received*, the chart shows the history of bytes sent and received.

When you drill down to view a line item, the historical chart show changes for that line item.

FortiView dashboards for FortiGate and FortiCarrier devices

Category	View	Description
Threats	Top Threats	Lists the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus.
	Threat Map	Displays a map of the world that shows the top traffic destinations starting at the country of origin. Threats are displayed when the threat score is greater than zero and either the source or destination IP is a public IP address. The *Threat Window* below the map, shows the threat, source, destination, severity, and time. The color gradient of the lines indicate the traffic risk. A yellow line indicates a high risk and a red line indicates a critical risk. This view can be filtered by device, time, source, and destination. See also Viewing the threat map on page 106.
	Indicator of Compromise	Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats. To use this feature: 1. UTM logs of the connected FortiGate devices must be enabled. 2. The FortiAnalyzer must subscribe to FortiGuard to keep its threat database up-to-date.
	FortiSandbox Detection	Displays a summary of FortiSandbox related detections. The following information is displayed: Filename, End User and/or IP, Destination IP, Analysis (Clean, Suspicious or Malicious rating), Action (Passthrough, Blocked, etc.), and Service (HTTP, FTP, SMTP, etc.). Select an entry to view additional information in the drilldown menu. Clicking a FortiSandbox action listed in the *Process Flow* displays details about that action, including the *Overview*, *Indicators*, *Behavior Chronology Chart*, *Tree View*, and more. Information included in the *Details* and *Tree View* tab is only available with FortiSandbox 3.1.0 and above.

Category	View	Description
Traffic	Top Sources	Displays the highest network traffic by source IP address and interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Source Addresses	Displays the top source addresses by source object, interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Destinations	Displays the highest network traffic by destination IP addresses, the applications used to access the destination, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Destination Addresses	Displays the top destination addresses by destination objects, applications, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Country/Region	Displays the highest network traffic by country in terms of traffic sessions, including the destination, threat score, sessions, and bytes.
	Policy Hits	Lists the policy sessions by policy, device name, VDOM, number of hits, bytes, and last used time and date.
	DNS Logs	Summarizes the DNS activity on the network. Double click an entry to drill down to the specific details about that domain.
	ZTNA Servers	ZTNA servers by bytes.
Shadow IT	Top Cloud Applications	Displays the top cloud applications used on the network. When viewing information about an application, FortiAnalyzer will first check the Shadow IT database, and if no results are found, it will use the metadata.
	Top Cloud Users	Displays the top cloud users on the network.
Applications & Websites	Top Applications	Displays the top applications used on the network including the application name, category, risk level, and sessions blocked and allowed. Bytes sent and received can also be enabled through the widget settings. Top Applications can be viewed as a stackbar, bar, table, or bubble chart. For a usage example, see Finding application and user information on page 123.
	Top Website Domains	Displays the top allowed and blocked website domains on the network.
	Top Website Categories	Displays the top website categories.

Category	View	Description
	Top Browsing Users	Displays the top web-browsing users, including source, group, number of sites visited, browsing time, and number of bytes sent and received.
VPN	SSL & Dialup IPsec	Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec). You can view VPN traffic for a specific user from the top view and drilldown views. In the top view, double-click a user to view the VPN traffic for the specific user. In the drilldown view, click an entry from the table to display the traffic logs that match the VPN user and the destination.
	Site-to-Site IPsec	Displays the names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network.
System	Admin Logins	Displays the users who logged into the managed device.
	System Events	Displays events on the managed device.
	Resource Usage	Displays device CPU, memory, logging, and other performance information for the managed device. Resource Usage includes two widgets: *Resource Usage Average* and *Resource Usage Peak*.
	Failed Authentication Attempts	Displays the IP addresses of the users who failed to log into the managed device.

Using FortiView

When ADOMs are enabled, *FortiView* displays information for each ADOM. Please ensure you are in the correct ADOM. See Switching between ADOMs on page 34.

- Viewing FortiView dashboards on page 105
- Filtering FortiView on page 107
- Creating custom views for FortiView on page 108
- Viewing related logs on page 110
- Exporting filtered summaries on page 110
- Monitoring resource usage of devices on page 111
- Long-lived session handling on page 111

Viewing FortiView dashboards

When viewing FortiView dashboards, use the controls in the toolbar to select a device, specify a time period, refresh the view, and switch to full-screen mode.

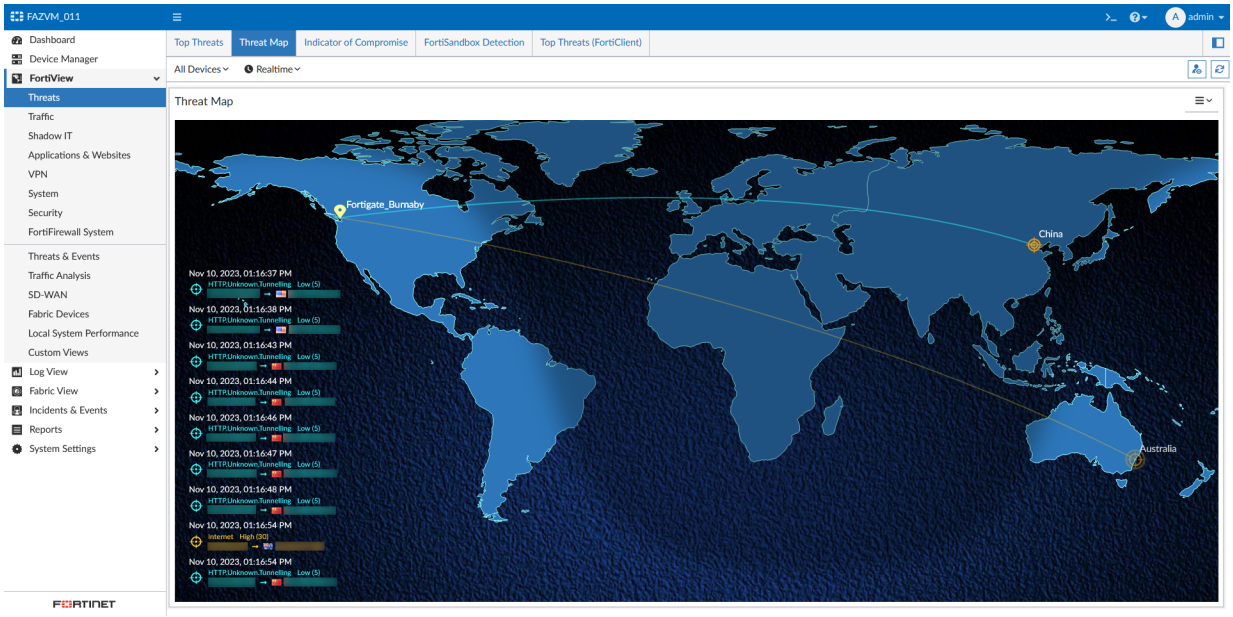
Many widgets on FortiView dashboards let you drill down to view more details. To drill down to view more details, click, double-click, or right-click an element to view details about different dimensions in different tabs. You can continue to drill down by double-clicking an entry. Click the close icon in the widget's toolbar to return to the previous view.

Many FortiView widgets support multiple chart types such as table view, bubble view, map view, tile view, etc.

- In widgets that support multiple views, select the settings icon in the top-right corner of the widget to choose another view.
- If sorting is available, there is a *Sort By* dropdown list in the top-left.
- Some widgets have a *Show* dropdown list in the bottom-right for you to select how many items to display.
- To sort by a column in table view, click the column title.
- To view more information in graphical views such as bubble, map, or user view, hover the mouse over a graphical element.

Some dashboards require that specific log types are enabled before they can be used. When an ADOM does not include the log type(s) required, the dashboard appears in gray and includes an information icon that indicates what logs must be enabled.

Viewing the threat map



You can view an animated world map that displays threats from unified threat management logs. By default, threats are displayed from all devices in real-time.

The threat map can also be filtered according to your needs. From the toolbar, you can filter threats in the threat map by devices and timeframe. At the top right of the widget, click *menu icon* > *Settings* to filter by the threats' source and destination.

When filtering a specific timeframe, the threat map will display in replay mode. In this mode, you can use the play/pause button to watch a replay of the threat map in the selected timeframe. You can adjust the speed of the replay by increasing or decreasing the *Replay rate*. All threats will appear in the overlay threat window as they occur on the map.



You must specify the longitude and latitude of the device to enable threats for the device to display in the threat map. You can edit the device settings to identify the geographical location of the device in *Device Manager*. For more information, see Editing device information on page 94

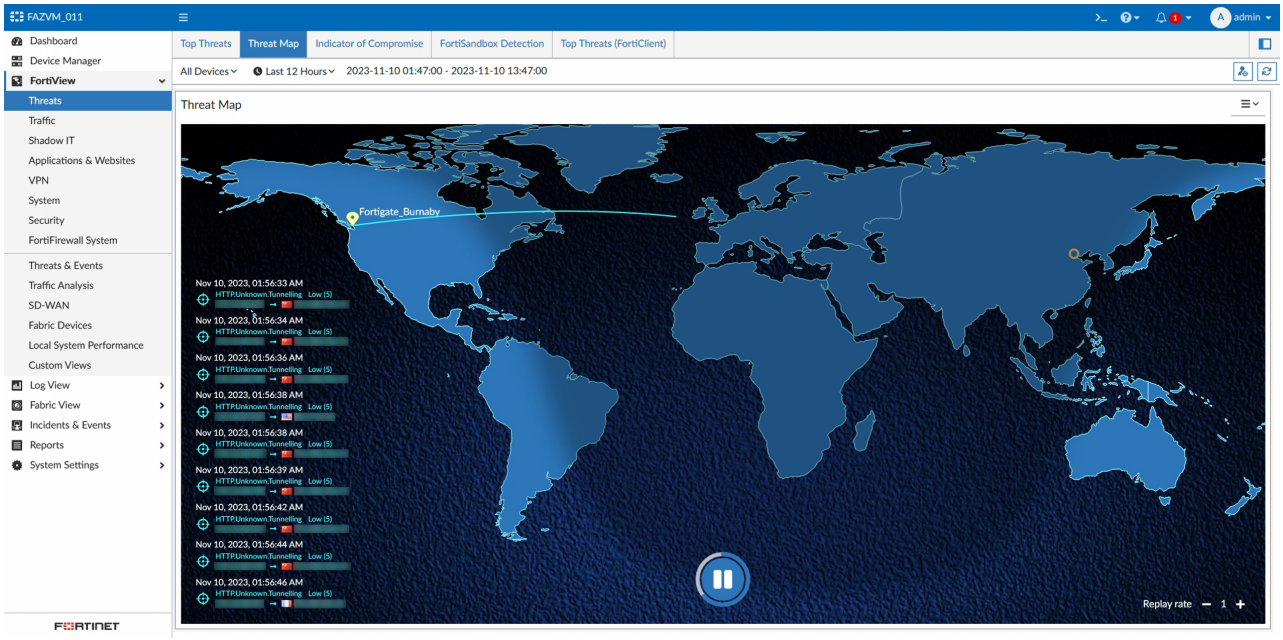
To view the threat map in realtime:

1. Go to *FortiView* > *Threats* > *Threat Map*.
2. In the timeframe filter, select *Realtime*.
   You can also filter devices from the toolbar. To filter the *Source* and *Destination* of the threats, click *menu icon* > *Settings*.
3. In the map, view the geographic location of the threats.
   Threats are displayed when the threat level is greater than zero.
   - A white line indicates a low threat.
   - A yellow line indicates a high threat.
   - A red line indicates a critical threat.

4. In the *Threat Window*, view the *Time*, *Threat*, *Severity(Score)*, *Source*, and *Destination* for each threat.

To view the threat map in replay mode:

1. Go to *FortiView* > *Threats* > *Threat Map*.
2. In the timeframe filter, select the timeframe to replay in the threat map.
   You can also filter devices from the toolbar. To filter the *Source* and *Destination* of the threats, click *menu icon* > *Settings*.
   Once the replay is loaded, it will begin playing automatically.
3. In the map, view the geographic location of the threats.
   Threats are displayed when the threat level is greater than zero.
   - A white line indicates a low threat.
   - A yellow line indicates a high threat.
   - A red line indicates a critical threat.
4. To adjust the *Replay rate*, click the minus (-) or plus (+).
   All threats will appear in the overlay threat window as they appear on the map.
5. In the *Threat Window*, view the *Time*, *Threat*, *Severity(Score)*, *Source*, and *Destination* for each threat.
6. To pause the replay, click the pause button.
7. To resume the replay, click the play button.
   The ring around the play/pause button indicates the progress of the replay.



Filtering FortiView

Filter *FortiView* widgets using the *Add Filter* box in the toolbar or by right-clicking an entry and selecting a context-sensitive filter. You can also filter by specific devices or log groups and by time.

The following settings are saved per user after navigating to different panes, refreshing, or logging out:

- devices
- time period
- widget settings, such as chart type, table mode, and top X settings
- widget configuration, such as added/hidden widgets, size, and layout

Once you return to *FortiView*, the above filters will still be applied. Other filters, such as those set using *Add Filter* or using the context menu, will reset after visiting another pane, refreshing the browser, or logging out.

To filter FortiView widgets using filters in the toolbar:

1. Specify filters in the *Add Filter* box.
   - Filter Mode: In the selected summary view, click *Add Filter* and select a filter from the dropdown list, then type a value. Click NOT to negate the filter value. You can add multiple filters and connect them with “and” or “or”.
   - Text Search: Click the *Switch to Text Search* icon at the right end of the *Add Filter* box. In Text Search mode, enter the search criteria (log field names and values). Click the *Switch to Filter Mode* icon to go back to Filter Mode.
2. In the *Device* list, select a device.
3. In the *Time* list, select a time period.



UUID logging must be enabled in FortiGate/FortiOS to filter traffic by object name, including `Source Object` and `Destination Object`. See the FortiGate/FortiOS Administration Guide for more information about UUID logging.

To filter FortiView widgets using the right-click menu:

In the selected view, right-click an entry and select a filter criterion (*Search <filter value>*).

Depending on the column in which your mouse is placed when you right-click, *FortiView* uses the column value as the filter criteria. This context-sensitive filter is only available for certain columns.

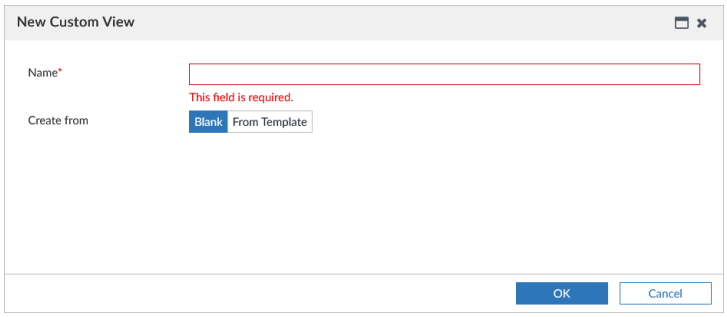
Creating custom views for FortiView

Use *FortiView > Custom Views* to save the widgets, filter settings, device selection, and the time period for a FortiView dashboard.

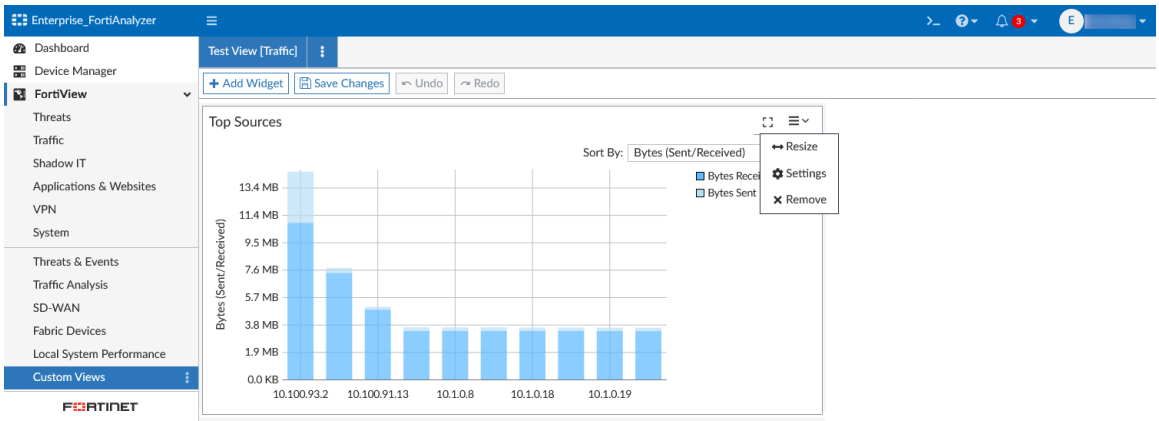
You can also create custom views directly from a FortiView dashboard after setting the device and time period filters.

To create a custom view from *FortiView > Custom Views*:

1. Go to *FortiView*.
2. In the sidebar, click the menu icon for *Custom View*, and select *Create New*.
   The *New Custom View* dialog displays.



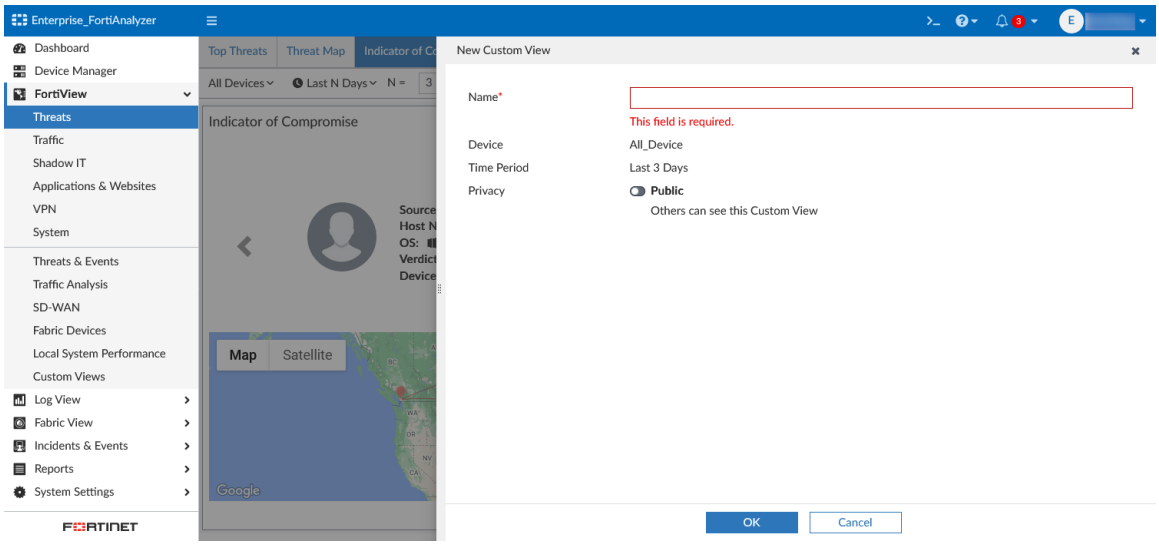
3. In the *Name* field, enter a name for the custom view.
4. In the *Create from* field, select *Blank* or *From Template*.
5. If creating the custom view *From Template*, select a FortiView dashboard from the dropdown.
6. Click *OK*.
   The custom view is now available under *FortiView > Custom Views > <name>*.



7. To add widgets for the dashboard, click *Add Widget*.
8. To resize or remove widgets, select *Resize* or *Remove* from the menu icon for that widget.
   You can also change the *Settings* for each widget, as needed.
9. To move widgets, drag and drop them on the dashboard.
10. To save the custom view, click *Save Changes*.

To create a custom view from a FortiView dashboard:

1. Go to *FortiView > <dashboard>*.
   In this example, the admin goes to *FortiView > Threats > Indicator of Compromise*.
2. In the toolbar, configure the device, time period, and filters.
3. In the toolbar, click *Create Custom View*.
   The *New Custom View* pane displays.



4. In the *Name* field, enter a name for the custom view.
   The *Device* and *Time Period* display.
5. For the *Privacy* field, toggle to *Public* or *Private* according to your need.
6. Click *OK*.
   The custom view is now available under *FortiView > Custom Views > <name>*. You cannot add or remove widgets from custom views created with this method.

To edit, rename, or delete a custom view:

1. Go to *FortiView > Custom Views*.
2. Click the menu icon next to the custom view to edit, rename, or delete.
3. Select *Edit*, *Rename*, or *Delete*.
   You can only Edit custom views that have been created via FortiView > Custom Views. See To create a custom view from FortiView > Custom Views: on page 108.

Viewing related logs

You can view the related logs for a FortiView summary in *Log View*. When you view related logs, the same filters that you applied to the *FortiView* summary are applied to the log messages.

To view related logs for a *FortiView* summary, right-click the entry and select *View Related Logs*.

Exporting filtered summaries

You can export filtered *FortiView* summaries or from any level of drilldown to PDF and report charts. Filtered summaries are always exported in table format.

To export a filtered summary:

1. In the filtered summary view or its drilldown, select the *tools* icon in the top-right corner of the widget and choose *Export to PDF* or *Export to Report Chart*.

2. In the dialog box, review and configure settings:
   - Specify a file name for the exported file.
   - In the *Top* field, specify the number of entries to export.
   - If you are in a drilldown view, the tab you are in is selected by default. You can select more tabs. If you are exporting to report charts, the export creates one chart for each tab.
3. Click *OK*.

Charts are saved in the *Chart Library*. You can use them in the same way you use other charts.



Only log field filters are exported. Device and time period filters are not exported.

Monitoring resource usage of devices

You can monitor how much FortiAnalyzer system resources (e.g., CPU, memory, and disk space) each device uses. When ADOMs are enabled, this information is displayed per ADOM. In a specific ADOM, you can view the resource usage information of all the devices under the ADOM.

Go to *FortiView* > *System* > *Resource Usage* to monitor resource usage for devices.

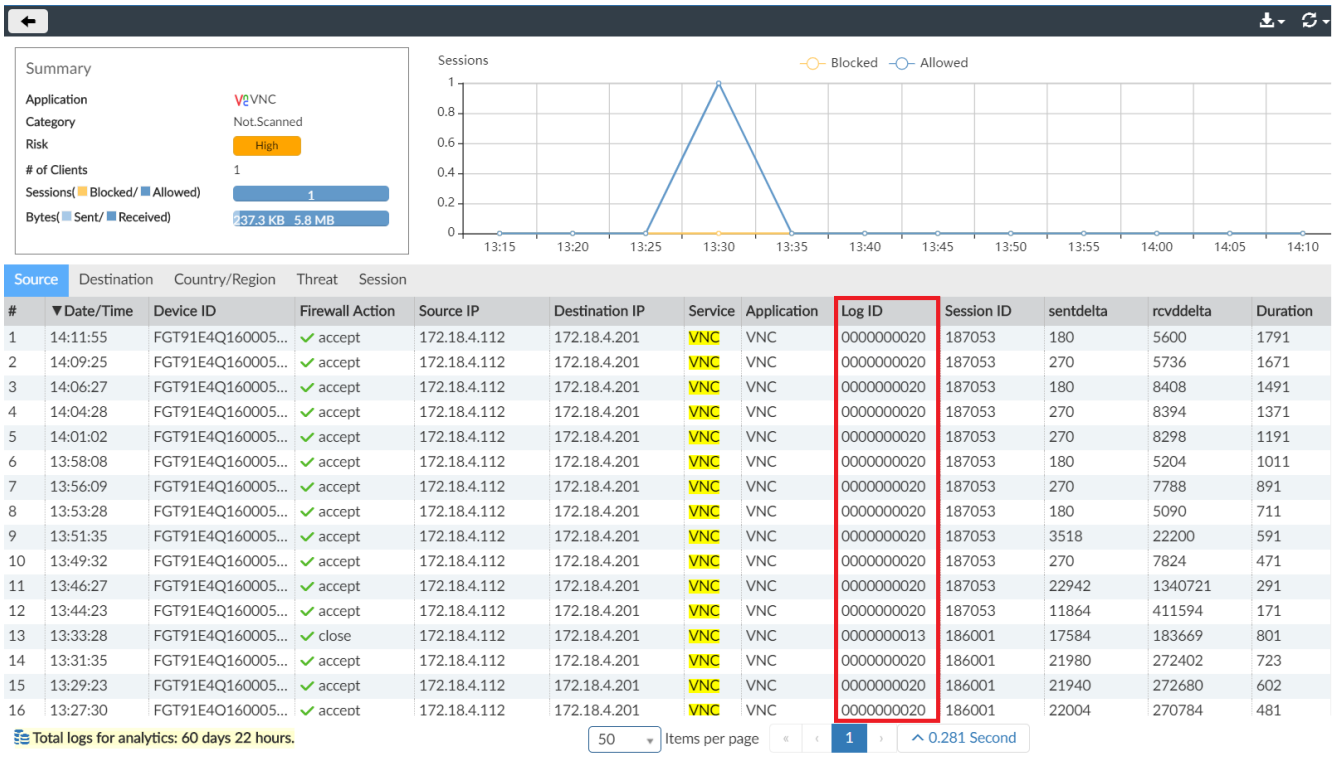
Long-lived session handling

Because traffic logs are only sent at the end of a session, long-lived sessions can be unintentionally excluded when narrowing searches in FortiView. To account for this, interim traffic logs can be enabled through FortiOS, allowing FortiView to show the trend of session history rather than one large volume once the session is closed.

For a long-lived session with a duration greater than two minutes, interim traffic logs are generated with the *Log ID* of *20*.

- For interim traffic logs, the *sentdelta* and *rcvddelta* fields are filled in with an increment of bytes which are sent/received after the start of the session or previous interim traffic log.
- Interim traffic logs are not counted in *Sessions*, but the *sentdelta* and *recvddelta* in related traffic logs will be added when calculating the sent and received bytes.

When a long-lived session ends, a traffic log with a *Log ID* of *13* is sent which indicates the session is closed.



When enabled, interim logs must be handled specially for *Reports* and *Events* to avoid multiple counting.

Viewing Indicators of Compromise

Indicators of Compromise service (IOC) is a licensed feature.

When using *Indicator of Compromise*, it is recommended to turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard on page 548.

The IOC service downloads the threat database from FortiGuard and detects suspicious events and potentially compromised network traffic using sophisticated algorithms. For more information about how FortiGuard collects indicators of compromise, see the FortiGuard website.

Depending on the log type, FortiAnalyzer identifies possible compromised hosts by checking the threat database against the log's IP address, domain, and URL. The following table displays which data in the logs are checked against the threat database:

Log type	Data
Attack logs	URLs, Domains, and IP addresses
DNS	IP addresses

Log type	Data
Email filter logs	URLs, Domains, and IP addresses
Event logs	Threat type
Traffic logs	IP addresses
Web Filter	URLs, Domains, and IP addresses

The results for each affected end user is displayed in *Indicator of Compromise*. You can drill down from table to review the details of the affected host, including the detect pattern and detect method for each indicator of compromise. You can also drill down further from these detections to review the logs where the matches were initially found in FortiAnalyzer. See Working with IOC information on page 113.

Indicator of Compromise can be configured to rescan logs at regular intervals using new definitions from FortiGuard. Email filter logs from FortiMail devices are also supported by IOC, and can be rescanned when enabled in the *Indicator of Compromise* rescan settings. See Managing an IOC rescan policy on page 117.

Understanding IOC entries

When a log entry is received and inserted into the SQL database, the log entry is scanned and compared to the blocklist and suspicious list in the IOC threat database that is downloaded from FortiGuard.

If a match is found in the blocklist, FortiAnalyzer displays the endpoint in *Indicator of Compromise* with a *Verdict* of *Infected*.

If a match is found in the suspicious list, FortiAnalyzer flags the endpoint for further analysis.

When an endpoint is displayed in *Indicator of Compromise*, all the suspicious logs which contributed are listed.

When the database is rebuilt, all log entries are reinserted and rescanned.

Working with IOC information

Go to *FortiView* > *Threats* > *Indicator of Compromise*.

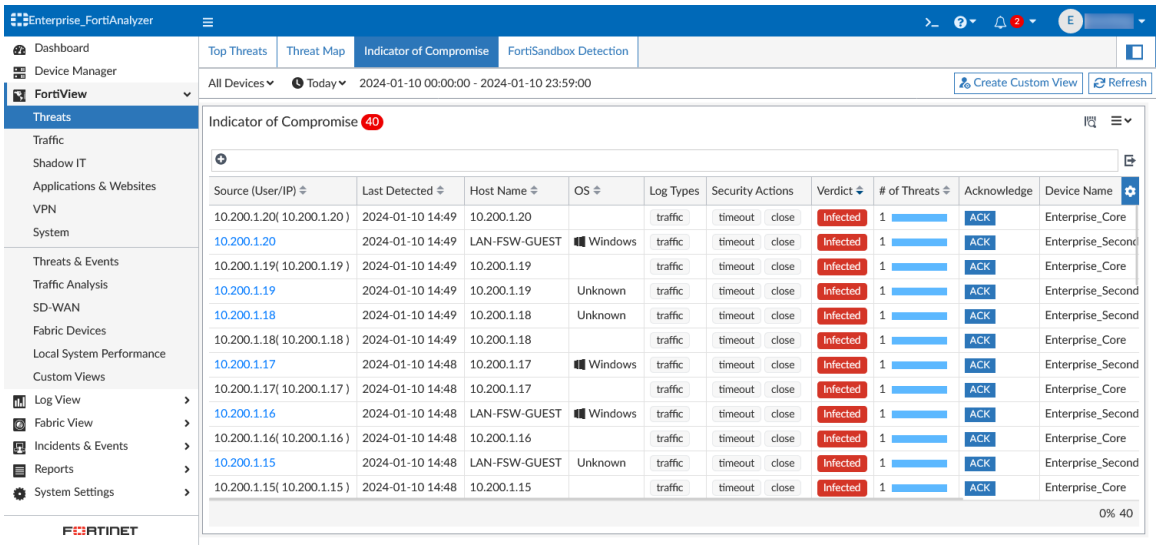
Click the *Settings* icon to change the following:

Chart Type	Select one of the following: *table* (default), *users IOC*, or *bubble*.
Show Top	Select the number of results to display. Different options are available according to the *Chart Type*.
Show Acknowledged	Include acknowledged sources in the results. Disabled by default.
Only Show Rescan	Only display results from rescan tasks. Disabled by default.

For information about rescan settings, see Managing an IOC rescan policy on page 117

You can set the devices, time period, and filters for the dashboard. If there are regularly used filters, you can create a custom view. See Creating custom views for FortiView on page 108

Using Indicator of Compromise when Chart Type = table:



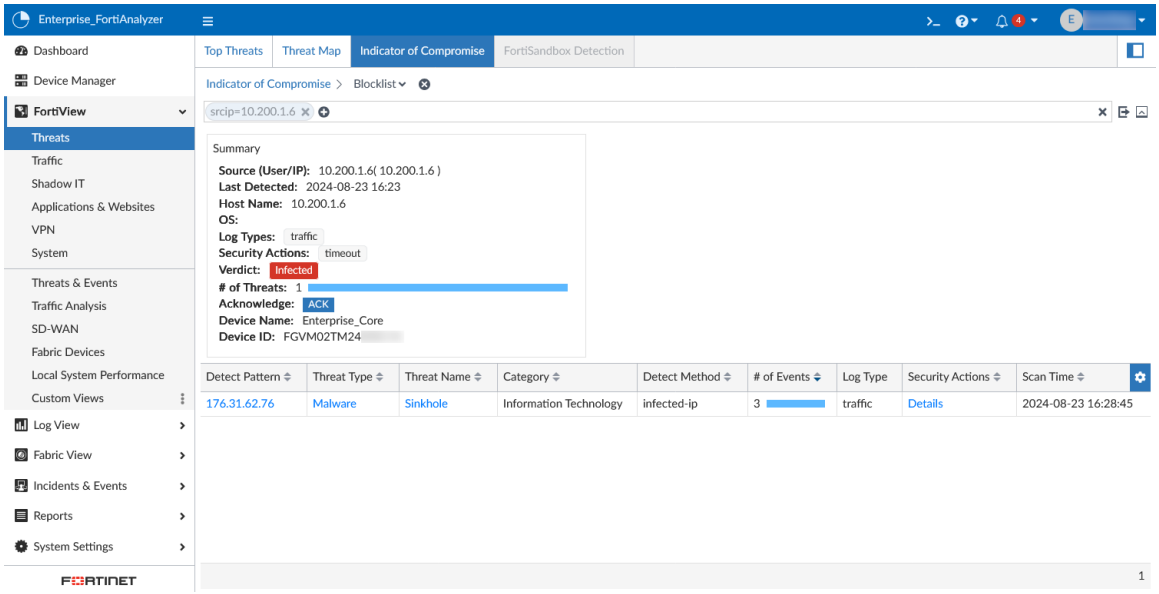
This chart type displays IOC line items in a table view. The total number of sources with indicators for compromise is displayed above the table. Click the export icon to export the table information into a PDF or report chart.

There is a record for each source, and the *# of Threats* column displays the number of unique threat names associated with that end user. To filter the table, click *+* to add a filter such as device ID, log type, or security action.

The following columns are available:

Source (User/IP)	The endpoint/end user that with indicator(s) of compromise.
Last Detected	The last time a threat was detected on the end user. A rescan icon indicates that threats found also include results from an IOC rescan task.
Host Name	The host name of the end user.
OS	The OS used by the end user.
Log Types	The log types that identified the threats. This could be traffic, web filter, DNS, or email filter log types.
Security Actions	The actions taken against the threats, such as block, timeout, or close.
Verdict	When threats are identified using the blocklist, the verdict is `Infected`.
# of Threats	The number of unique threats associated with the end user. You can drill down by double-clicking the record to view the different threats in the *Blocklist* and *Suspicious* table views. In those views, you will also be able to drill down further to the different logs where matches were found to the threat database.
Acknowledge	Indicates if the potential compromise has been acknowledged by the user. To add an acknowledgment comment, click *ACK* and submit desired remark.
Device Name	The related logging device.

To drill down and view threat details for a particular endpoint, right-click a row and select *Blocklist* or *Suspicious*. Alternatively, double-click a row to open the *Blocklist*. You can toggle between *Blocklist* and *Suspicious* from this view.



The *Blocklist* and *Suspicious* table views list all unique threats detected for the end user. A summary of the end user is provided above the table.

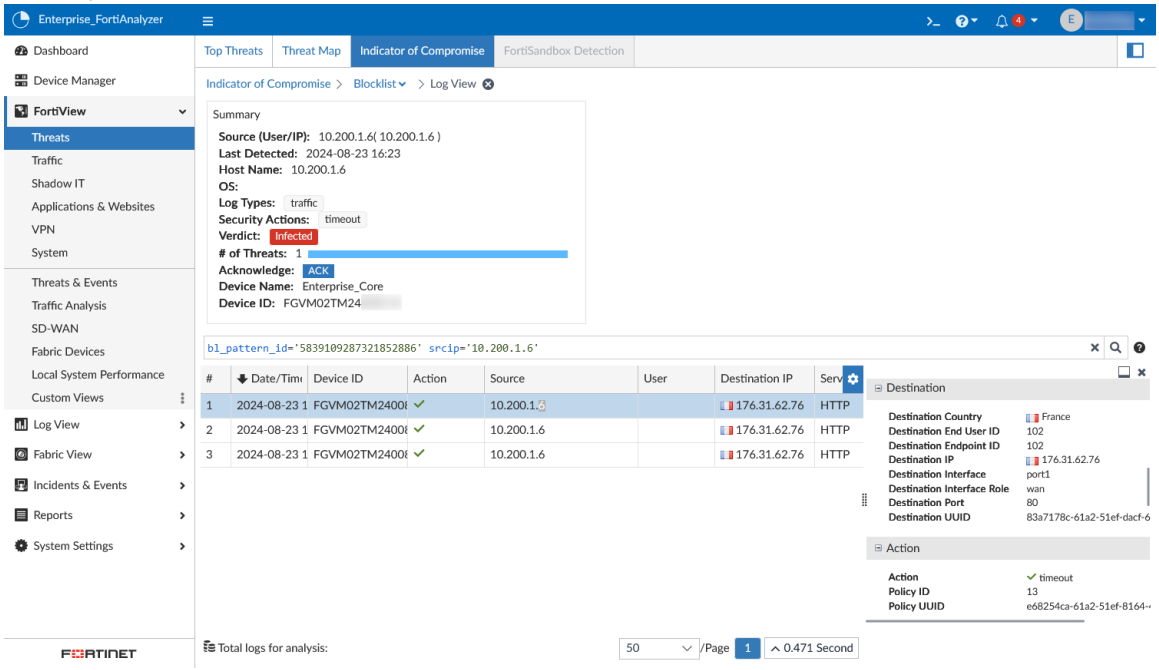
The following columns are available:

Detect Patterns	The IP, URL, or domain that was matched to the blocklist or suspicious list in the threat database. When FortiAnalyzer has a valid license for the FortiTIP service, click this hyperlink to open the FortiTIP instance with the related threat intel. This includes the indicator, risk score, FortiGuard live rating, related kill chain, and more. For more information, see FortiTIP service integration on page 357.
Threat Type	The threat type as defined in FortiGuard. Click for a brief description.
Threat Name	The threat name as defined in FortiGuard. Click for a brief description.
Category	The category for the threat.
Detect Method	The method for detecting the compromise. In the example above, it is "`infected-ip`", which means an IP in the logs matches a blocklist IP in the threat database. Threats can also be detected through infected URLs and domains identified on the threat database.
# of Events	The number of events matching this detect pattern that have been flagged for the end user. There is a separate log for each event. You can double-click the row to find more information about the logs.
Log Type	The log type(s) where the potential compromise was detected.

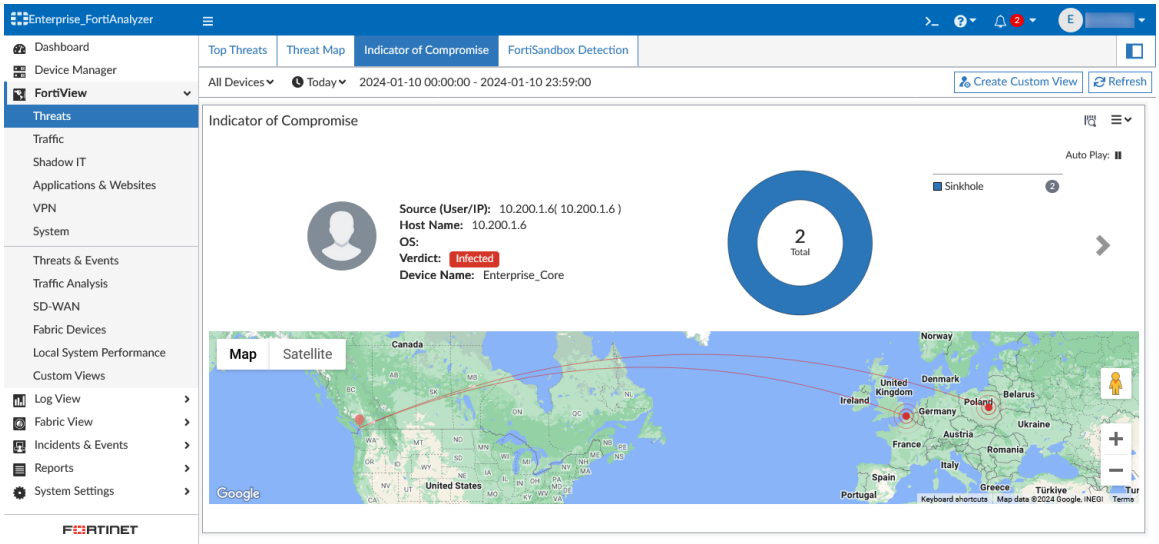
Security Actions	The action that has been taken against the detection, such as blocked or timeout. Click for more details, including the Device ID and VDOM.
Scan Time	When the user was last scanned for IOC.

Double-click a record in the table to open *Log View* filtered to display the related events. For example, double-clicking a record in the *Blocklist* table will display *Log View* filtered by the `bl_pattern_id` and the `srcip`.

In the *Log View*, you can double-click a record in the table to open the log details. Note that you have not left *FortiView*, so you can click the breadcrumbs at the top of the pane to navigate back to the *Blocklist* or *Indicator of Compromise* views. See below.



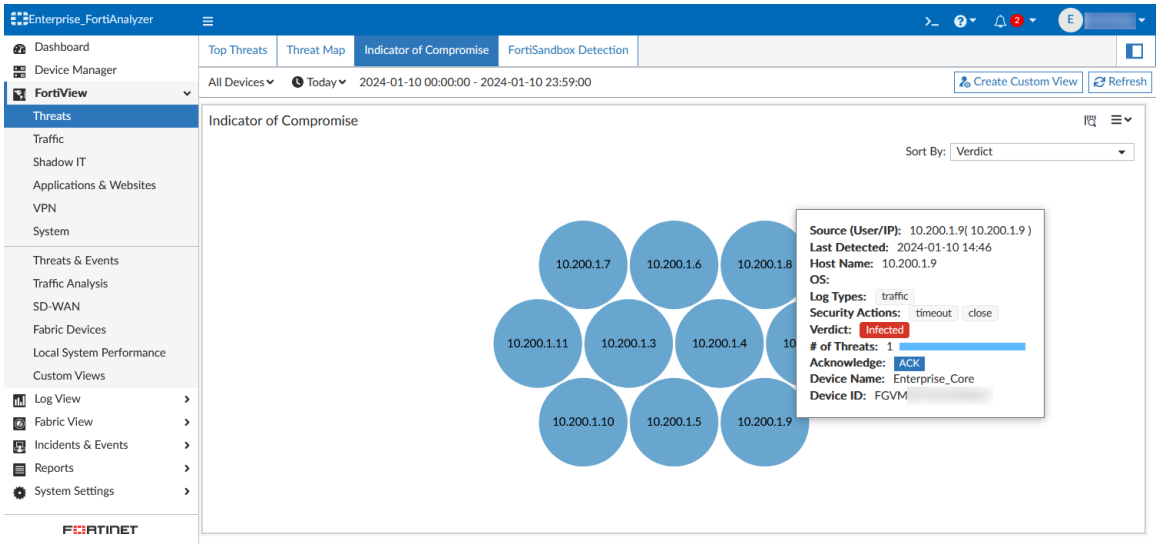
Using Indicator of Compromise when Chart Type = users IOC:



This chart type includes two panes: a rotating list of users and a map of incidents.

The rotating list of users automatically rotates through indicators of compromise. This includes the endpoint information and the number of unique threat names associated with that end user. You can pause autoplay or click > or < to manually move to another user.

Using Indicator of Compromise when Chart Type = bubble:



In the *Sort By* dropdown, select which top IOC to display in the bubble chart: by verdict or by number of threats. Mouse-over a bubble to display the following information:

- *Source*
- *Last Detected*
- *Host Name*
- *OS*
- *Log Types*
- *Security Actions*
- *Verdict*
- *# of Threats*
- *Achnowledge*
- *Device Name*
- *Device ID*

Double-click a bubble to drill down to the *Blocklist* view for the related end user.

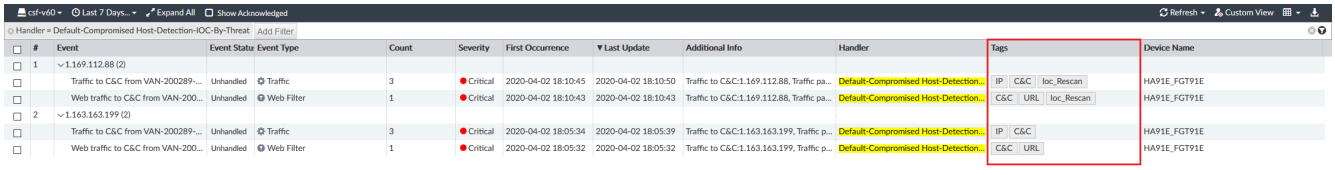
Managing an IOC rescan policy

Indicator of Compromise can be configured to scan previous entries on regular intervals or when a new package is received from FortiGuard so that FortiAnalyzer performs a rescan using the latest available definitions.

Requirements for managing an IOC rescan policy:

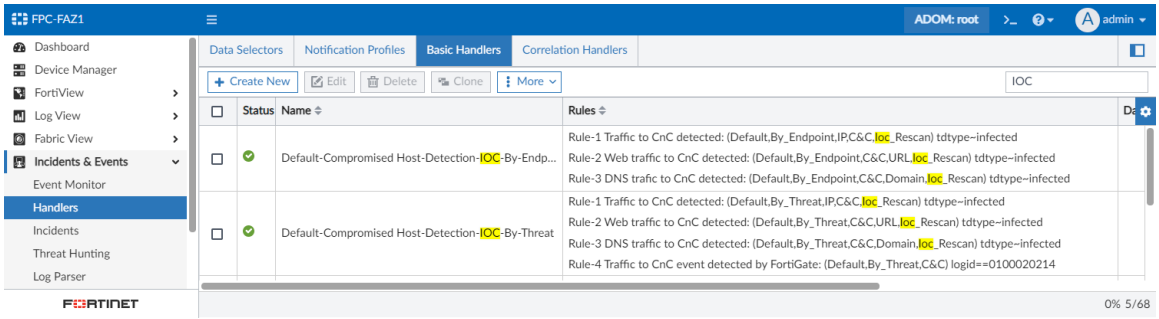
- This feature requires a valid Indicators of Compromise (IOC) service license. The rescan options are not available in the GUI or CLI without a license.
- The administrator must have *Read-Write* privileges for *System Settings* in order to configure global IOC rescan settings.

When IOC rescan is performed, the *Ioc_Rescan* tag is added to rescanned logs. Event handlers that include the *Ioc_Rescan* tag in their rules will process rescanned logs and generate new alerts tagged with *Ioc_Rescan*. Real-time logs matching these event handler rules continue to generate alerts without the *Ioc_Rescan* tag.



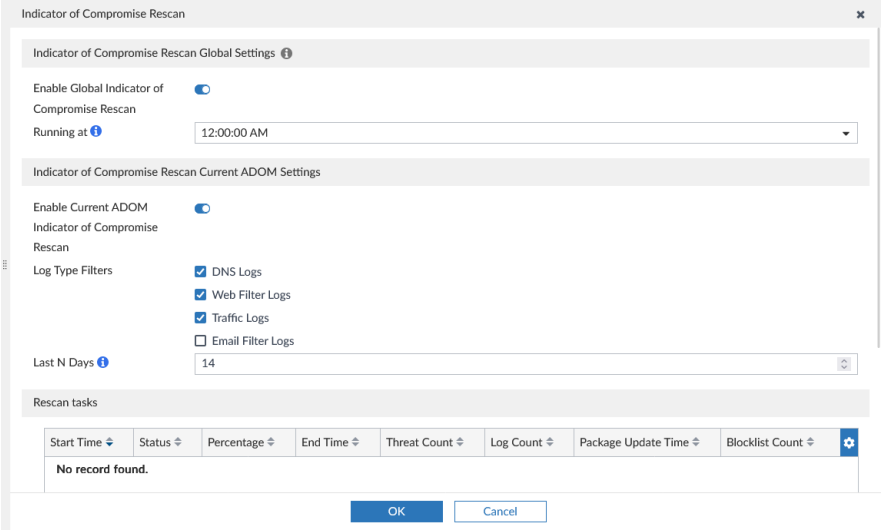
By default, the following basic event handlers include *Ioc_Rescan* tag for all rules:

- Default-Compromised Host-Detection-IOC-By-Endpoint
- Default-Compromised Host-Detection-IOC-By-Threat



To configure rescan settings and check rescan results:

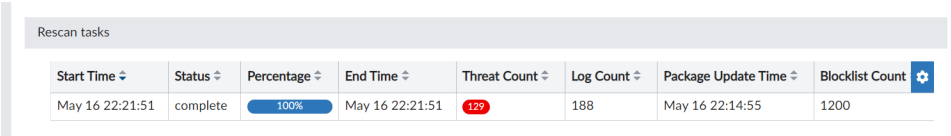
1. Go to *FortiView > Threats > Indicator of Compromise*.
2. Click the *Rescan Task* icon above the table view.
   The *Indicator of Compromise Rescan* pane displays.



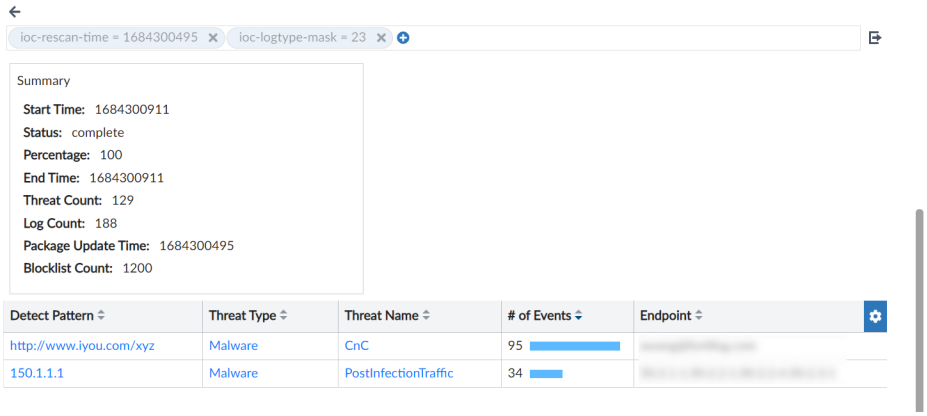
3. Configure the *Indicator of Compromise Rescan Global Settings*.
   a. Toggle *Enable Global Indicator of Compromise Rescan* to *On*.
   b. Set the running time to a specific hour of the day, or select *package update* to perform a rescan when a package update is received.
4. Configure the *Indicator of Compromise Rescan Current ADOM Settings*.
   a. Toggle *Enable Current ADOM Indicator of Compromise Rescan* to *On*.
   b. Select the log types to be scanned (*DNS*, *Web Filter logs*, *Traffic logs*, or *Email filter logs*).
   c. Set the number of previous days' logs to be scanned.

   By default, DNS, web filter, and traffic logs are enabled, and the scan will cover the last 14 days. The maximum recommended number of scan days is calculated based on historical scan speeds, or 30 days if no previous scans have been done.
5. Rescan jobs are shown in the *Rescan tasks* table, which includes the following columns:

Start Time	The task's start time.
Status	The status of the task (complete, running, etc.). Running tasks can be canceled by clicking the cancel icon in the *Status* column.
Percentage	Task progress as a percentage.
End Time	The task's end time.
Threat Count	Configure the parameters for the selected action.
Log Count	The total number of logs with threats.
Package Update Time	The IOC package update time.
Blocklist Count	A count of the newly detected threats added to the blocklist.



6. Select a non-zero threat count number in the table to drilldown to view specific task details, including the *Detect Pattern*, *Threat Type*, *Threat Name*, *# of Events*, and *Endpoint*.



In *FortiView > Threats & Events > Indicator of Compromise*, a rescan icon is displayed in the *Last Detected* column if threats are found during a rescan. To view only those hosts that had threats found during a rescan, go to the *Settings* and enable *Only Show Rescan*.

For FortiMail email filter rescans, the endpoint which visited an allowed URL will be marked as compromised if the URL is blocklisted in the latest URL blocklist. The compromised hosts are the users' email addresses which can be found in the *To* field of the log.

Indicators of Compromise

Indicators of Compromise (IOC) detects compromised client hosts (endpoints) by comparing the IP, domain, and URL visited against the TIDB package, downloaded daily from FortiGuard. Compromised hosts are listed in *FortiView* in a table or map style, and drilling down on a compromised endpoint displays the details of detected threats.

- The TIDB package contains a blocklist which is made up of IPs, domains and URLs, and a suspicious URL list (*also called Crowdsource URLs*). Only suspicious URLs have a score rating in the TIDB package. Once a URL is included in the blocklist, the suspicious score rating is no longer performed.
- Once a new TIDB package has been downloaded by FortiAnalyzer, the previous package becomes obsolete.
- The *blocklist statistics by endpoint* are updated in near realtime (ASAP), and *suspicious rating statistics by endpoint* are updated on a half-hour schedule.
- The IOC inspection is performed on a daily cycle because the updated FortiGuard TIDB package is received daily. At the end of the day, the IOC endpoint summary is fixed and will not receive additional changes, and a new summary will be created for the next day.
- Web Filter, DNS, and traffic logs from FortiGate, and email filter logs from FortiMail are inspected.
- The IOC module requires a license. Without a license, only demo TIDB packages are loaded into the FortiAnalyzer image, and no updated package from FortiGuard is used in the IOC function.
- When a threat is detected, FortiAnalyzer sends a notification to the FortiGate via REST API. The FortiGate can be configured to take automatic action against detected threats.
- IOC threat detection can be performed in both *realtime* and *rescan* mode. Realtime detection monitors new incoming logs, whereas rescan mode checks historical logs against the new blocklist once an updated TIDB package is available. Rescan mode does not check historical logs against the suspicious list. Realtime detection is always enabled, and IOC rescan can be enabled or disabled.

Understanding suspicious list detection

The suspicious list is crowdsourced each day by FortiGuard AI from millions of global endpoint devices. The list is comprised of IPs, URLs, and domains that have a low reputation, usually because they are questionable websites.

The TIDB package includes threat ranking scores which FortiAnalyzer normalizes using its internal logic. When an endpoint visits a site that matches one included in the suspicious list, the score is deposited into the "reputation account" for that endpoint. The total normalized score is then used to determine a verdict for the endpoint. The higher the score, the higher the confidence. When a new TIDB package becomes available, the process to determine a verdict begins again. FortiAnalyzer processes logs for all monitored endpoints against the new TIDB and will determine a verdict for each endpoint based on their new normalized score.

Endpoints that visit suspicious sites on an infrequent basis are at a low risk for compromise and are not included in the *Indicator of Compromise* watch list. The FortiAnalyzer IOC engine continues to monitor these endpoints until it has enough confidence to produce a verdict, at which point they are given the verdict *Low Suspicious* and are added to the watch list. Endpoints that regularly visit suspicious sites are at a higher risk for infection or may already be infected with zero-day malware. These endpoints are assigned a verdict and are added to the *Indicator of Compromise* watch list.

Suspicious verdicts include:

- High suspicious (high confidence)
- Medium suspicious (medium confidence)
- Low suspicious (low confidence)

In the example below, an endpoint visits multiple sites included in the suspicious list, and as a result, has its verdict changed from *Low suspicious* to *Medium suspicious*. The data included in this example is purely hypothetical for the purpose of illustration.

Activity time stamp	Suspicious site visited by endpoint	Ranking of suspicious site	Suspicious score of endpoint	FortiAnalyzer IOC verdict
Time stamp 1	suspicious-url-1	60	60	Low suspicious
Time stamp 2	suspicious-ip-2	100	160	Low suspicious
Time stamp 3	suspicious-domain-3	40	200	Medium suspicious

The specific algorithm used for the decision to change the verdict of an endpoint is internal to FortiAnalyzer.

Viewing IOC licenses and TIDB package downloads

To check the license downloaded from FortiGuard in the CLI:

```
diagnose fmupdate dbcontract
FL-1KE3R16000271 [SERIAL_NO]
  AccountID:
  Industry:
  Company:
  Contract:  1
```

```
        PBDS-1-99-20250104
  Contract Raw Data:
        Contract=PBDS-1-99-20250104:0:1:1:0
```

In the output, *PBDS* is the IOC license.

To check the IOC package in the CLI:

```
diagnose fmupdate fds-getobject

FAZ object version information
ObjectId                Description             Version         Size    Created Date Time
-------------------------------------------------------------------------------------------
-
...
00001000TIDB00100       ThreatIntel DB          00000.01052     34 MB   19/04/14 20:10
ext_desc:ThreatIntel DB
00001000TIDB00100       ThreatIntel DB          00000.01053     37 MB   19/04/16 04:13 <latest>
ext_desc:ThreatIntel DB
...
```

FortiAnalyzer periodically syncs its own IOC TIDB files to the version of IOC package downloaded by *fmupdate*. This is performed on a one hour schedule.

To check the license and TIDB version used by FortiAnalyzer in the CLI:

```
diagnose test application sqllogd 204 stats

License of post breach detection installed.
License expiration : 2025-Jan-04
TIDB version : 00000.01017-1902242107
TIDB load time : 2019-02-24 14:11:2
```

Configuring FortiGate to FortiAnalyzer REST API authentication

FortiGate to FortiAnalyzer REST API authentication allows the FortiAnalyzer to send IOC alerts and trigger configured automation rules, if configured.

To configure REST API authentication:

1. Go to the *Device Manager* in the FortiAnalyzer.
2. Edit the FortiGate device to set the FortiGate super admin username and password.
   This is the only way to configure REST API authentication prior to 6.2.

Alternatively, when configuring logging to FortiAnalyzer on FortiGate, you can go to *Security Fabric* > *Settings* and enable *Allow access to FortiGate REST API* and *Trust FortiAnalyzer by serial number*.

Throttling IOC alerts

To avoid flooding FortiGate with event alerts, you can configure a throttle which allows only one alert to be sent within a set period of time for the same endpoint.
The default time period is one day (1440 minutes).

To set an IOC alert throttle in the CLI:

```
config system log ioc
(ioc)# set
 notification             Disable/Enable Ioc notification.
 notification-throttle    Minute value for throttling the rate of IoC notifications.

(ioc)# get
notification        : enable
notification-throttle: 1440
```

Examples of using FortiView

You can use FortiView to find information about your network. The following are some examples.

- Finding application and user information on page 123
- Analyzing and reporting on network traffic on page 124
- Finding FortiGate C&C detection logs on page 124

Finding application and user information

Company ABC has over 1000 employees using different applications across different divisional areas, including supply chain, accounting, facilities and construction, administration, and IT.

The administration team received a $6000 invoice from a software provider to license an application called Widget-Pro. According to the software provider, an employee at Company ABC is using Widget-Pro software.

The system administrator wants to find who is using applications that are not in the company's list of approved applications. The administrator also wants to determine whether the user is unknown to FortiGuard signatures, identify the list of users, and perform an analysis of their systems.

To find application and user information:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *FortiView* > *Applications & Websites* > *Top Applications*.
3. Click *Add Filter*, select *Application*, type `Widget-Pro`.
4. If you do not find the application in the filtered results, go to *Log View* > *FortiGate* > *Traffic*.
5. Click the *Add Filter* box, select *Source IP*, type the source IP address, and apply the filter.

Analyzing and reporting on network traffic

A new administrator starts at #1 Technical College. The school has a free WiFi for students on the condition that they accept the terms and policies for school use.

The new administrator is asked to analyze and report on the top source and destinations students visit, the source and destinations that consume the most bandwidth, and the number of attempts to visit blocked sites.

To review the source and destination traffic and bandwidth:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *FortiView > Traffic > Top Sources*.
3. Go to *FortiView > Traffic > Top Destinations*.
   If available, select the icon beside the IP address to see its WHOIS information.

Finding FortiGate C&C detection logs

FortiGate detected botnet events while performing an IOC scan. The administrator wants to view the C&C and logs with SOC view in Compromised Hosts.

To view C&C detection logs:

1. Go to *FortiView > Threats > Compromised Hosts*.
2. In the main view, right-click an entry and select *Blocklist*, or double-click an entry. The *Blocklist* is displayed.
   C&C detection logs have the following values:

Column	Value
Threat Name	`*.Botnet` (for example, `Asprox.Botnet`)
Detect Method	`detected-by-fgt`
Log Type	`attack`

3. In the *Blocklist* drill-down view, double-click an entry to view related logs. *Log View* is displayed.
   C&C detection entries appear in either the *Attack Name* or *Message* columns with one of the following values:

Column	Value
Attack Name	`*.Botnet` (for example, `Asprox.Botnet`)
Message	`Botnet C&C *` (for example, `Botnet C&C Communication`)

Monitors

The monitors in *FortiView* are designed for a network and security operations center where multiple dashboards are displayed on large monitors.

In the *FortiView* monitors, dashboards display widgets with both real-time monitoring and historical trends. Centralized monitoring and awareness help you to effectively monitor network events, threats, and security alerts. Use the *FortiView* monitors to view multiple panes of network activity, including monitoring network security, indicators of compromise, endpoints, Security Fabric, WiFi security, and FAZ system performance.

A typical scenario is to set up dashboards and widgets to display information most relevant to your network and security operations. Use the main monitors in the middle to display important dashboards in a larger size. Then use the monitors on the sides to display other information in smaller widgets.

For example, use the top monitor in the middle to display the *Top Threat Destinations* widget in full screen, use the monitor(s) below that to display other *Threats* widgets, use the monitors on the left to display *WiFi* widgets at the top and *Local System Performance* widgets at the bottom, and use the monitors on the right as a workspace to display widgets showing the busiest network activity. You can move, add, or remove widgets.

Monitor dashboards and widgets are very flexible and have the following features:

- You can create predefined or custom dashboards.
- For both predefined and custom dashboards, you can add, delete, move, or resize widgets.
- You can add the same dashboard multiple times on the same or different monitors.
- Each widget monitors one activity.
- You can add the same widget multiple times and apply different settings to each one. For example, you can add widgets to monitor the same activity using a different chart type, refresh interval, or time period.
- You can resize widgets or display a widget in full screen.

Some dashboards and widgets require that specific log types are enabled before they can be used. When an ADOM does not include any logs of the required type, the dashboard or widget appears in gray and includes an information icon that indicates what logs must be enabled before it can be used.

Some dashboards and widgets display maps, which require an internet connection. For more information, see Google Map integration on page 38. The maps will use the devices' geographic coordinates, which can be set when Editing device information on page 94



FortiView, including the monitors, can be disabled to improve performance in high capacity environments. For more information, see Enabling and disabling FortiView on page 145



To prevent timeout, ensure *Idle Timeout* is greater than the widget's *Refresh Interval*. See Idle timeout on page 593 and Settings icon on page 141.

FortiView monitors

FortiView includes predefined dashboards, which are listed below the separator in the *FortiView* tree menu.

Both predefined and custom dashboards can be modified. For example, the default *Threats* dashboard includes four widgets: *Top Threats*, *Top Threat Destinations*, *Threat Map*, and *Top Virus Incidents Over Time*. These widgets can be removed, enlarged, reduced, or customized, and new widgets can be added to the dashboard.

For more information, see Customizing the monitors dashboard on page 142.

FortiView include the following predefined monitors:

Category	Monitor	Description
Threats & Events	Threats on page 128	Monitor the top security threats to your network.
	Indicator of Compromise on page 129	Monitor compromised and suspicious web use in your network.
	FortiSandbox Detections on page 129	Monitor FortiSandbox detections on your network.
	Local Threat Research on page 130	Monitor local threat research.
	Data Loss Prevention on page 130	Monitor data loss prevention detection.
	Threat (FortiClient) on page 130	Monitor threat activity from FortiClient.

Category	Monitor	Description
Traffic Analysis	Traffic on page 130	Monitor the traffic on your network.
	Applications & Websites on page 131	Monitor the application and website traffic on your network.
	ZTNA on page 132	Monitor ZTNA metrics.
	VPN on page 132	Monitor VPN activity on your network.
	Traffic Shaping Monitor on page 133	Monitor traffic shaping information.
	Endpoints on page 133	Monitor endpoint activity on your network.
	Endpoints (FortiClient) on page 134	Monitor endpoint activity from FortiClient.
	Traffic (FortiDDOS) on page 134	Monitor FortiDDoS detected traffic activity. This chart requires Intrusion Prevention logs to be enabled.
	Traffic (FortiFirewall) on page 134	Monitors FortiFirewall traffic.
	Applications & Websites (FortiClient) on page 135	Monitor application and website activity from FortiClient.
	VPN (FortiFirewall) on page 135	Monitors FortiFirewall VPN usage.
	FortiClient Software Inventory on page 135	Monitor the FortiClient endpoints sending logs to FortiAnalyzer.
	FortiMail on page 135	Monitor FortiMail statistics.
	FortiProxy on page 136	Monitor information from FortiProxy devices.

Category	Monitor	Description
SD-WAN	SD-WAN Network on page 137	Monitor secure software-defined networking.
	SD-WAN Application on page 137	Monitor SD-WAN applications.
	SD-WAN Summary on page 138	Monitor SD-WAN operations.
Fabric Devices	WiFi on page 139	Monitor WiFi access points and SSIDs.
	IoT on page 139	Monitor IoT devices.
	Fabric State of Security on page 140	Monitor your network's Security Fabric rating, score, and topology. The information for this dashboard is available after you create a Security Fabric group in FortiGate and add it in FortiAnalyzer. The Security Fabric can be selected in the settings options for each widget.
Local System Performance	Local System Performance on page 140	Monitor the local system performance of the FortiAnalyzer unit.



When upgrading versions prior to FortiAnalyzer 6.2.0, custom dashboards will not be migrated and must be recreated.

Threats

Threats includes the following widgets:

Threat Map	Threats happening across the world. By default, the threats are displayed in *Realtime*. Open the settings for the widget to filter the time, source, and destination.
Top Threat Destinations	A world map, spinning 3D globe, or table showing the top 10, 20, 50, 100 threat destinations. On the map view, hover the cursor over data points to see the source device and IP address, destination IP address and country, threat level, and the number of incidents (blocked and allowed).
Top Threats	The top threats to your network. Hover the cursor over data points to see the threat, category, threat level, threat score (blocked and allowed), and the number of incidents (blocked and allowed). The following incidents are considered threats: • Risk applications detected by application control • Intrusion incidents detected by IPS

	• Malicious web sites detected by web filtering • Malware/botnets detected by antivirus
Top Threats by Weight & Count	The top threats by weight and count to your network from risk applications, intrusion incidents, malicious websites, and malware/botnets.
Top Virus Incidents Over Time	The top virus incidents over time.

Indicator of Compromise

Indicator of Compromise includes the following widget:

Indicator of Compromise	Suspicious web use compromises. By default, this widget includes two panes: a rotating list of users and a map of incidents. The rotating list of users automatically rotates through indicators of compromise. You can pause autoplay or click > or < to manually move to another user. The map displays the location of incidents. Click the *Rescan Task* icon to configure the rescan settings and check rescan results. For more information, see Managing an IOC rescan policy on page 117. Click the *Settings* icon to change the following: • *Chart Type*: users IOC (default) or table. • *Show Top*: different options are available according to the *Chart Type*. • *Refresh Interval*: *Every 30 Minutes* by default. • *Autoplay Interval*: *Every 20 Seconds* by default. • *Show Acknowledged*: disabled by default. • *Only Show Rescan*: disabled by default.

For more information, see Viewing Indicators of Compromise on page 112.

FortiSandbox Detections

FortiSandbox Detections includes the following widgets:

FortiSandbox Detection	FortiSandbox detection detail, including date, file name, end user, destination IP, analysis, action, and service.
FortiSandbox - Scanning Statistics	The number of files detected by FortiSandbox by type: Malicious, Suspicious, Clean, and Others.
FortiSandbox - Top Malicious & Suspicious File Users	Users or IP addresses that have the highest number of malicious and suspicious files detected by FortiSandbox.

Local Threat Research

Local Threat Research includes the following widgets:

Local Threat Prevalence	The top threats based on the current ADOM. The threat map can be viewed by *Virus*, *IPS*, *Botnet*, and *Application*. Hover your mouse over a datapoint in the chord chart to view additional details. Local Threat Research data is from FortiGuard and not from FortiGate.

Threat (FortiClient)

Threat (FortiClient) includes the following widgets:

Threat	The top threats to your network from risk applications, intrusion alerts, malicious websites, and malware/botnets. Only visible in a Fabric ADOM.

Data Loss Prevention

Data Loss Prevention includes the following widgets:

DLP Trends	Data loss prevention trends by number of blocked and allowed events.
Top Destination Countries	Top destination countries by data loss prevention occurrences and bytes.
Top Users	Top users by data loss prevention occurrences and bytes.
Top Protocols	Top protocols by data loss prevention occurrences and bytes.
Top DLP Events	Top data loss prevention events in a table view.
Top DLP Profile Hits	Top data loss prevention profile hits by occurrences and bytes.
Sensitive Files being Accessed	Sensitive files being accessed, including their data loss prevention occurences.

Traffic

Traffic includes the following widgets:

Top Sources	The highest network traffic by source IP address and interface, sessions (blocked and allowed), threat score (blocked and allowed), and bandwidth (sent and received).
Top Country/Region	The historical network traffic by country/region, sessions, bandwidth, or threat score.

Top Policy Hits	Top policy hits from recent traffic.
Top Destinations	Top destinations from recent traffic by bandwidth or sessions.
Traffic Over Time by Sessions	The historical destinations from recent traffic.
Policy Hits Over Time by Bandwidth	The historical policy hits from recent traffic.
User Data Flow	Bandwidth breakdown of top user destination country/region or application usage.
Top Sources Today	Near real-time network traffic by blocked and allowed sessions.
Top Interface of Sent Bit Rate	Line charts for the top 10 sent bit rate of interfaces over the specified time period. Mouse over the line charts to view bit rate information for each interface.
Top Interface of Received Bit Rate	Line charts for the top 10 received bit rate of interfaces over the specified time period. Mouse over the line charts to view bit rate information for each interface.

Applications & Websites

Applications & Websites includes the following widgets:

Top Website Domains	Top website domains from recent traffic.
Top Cloud Applications	Top cloud applications from recent traffic.
Top Applications	The top applications used on the network, including application name, risk level, category, sessions (blocked and allowed), and bytes (sent and received).
Top Browsing User	Top browsing users from recent traffic.
Cloud Applications Over Time by Sessions	The historical sessions of cloud applications used on the network.
Top Applications Over Time by Sessions	The historical sessions of applications used on the network, including application name, risk level, category, sessions (blocked and allowed), and bytes (sent and received).
Top Endpoint Applications	The top applications used on the network, including application name, risk level, category, sessions (blocked and allowed), and bytes (sent and received). Only available in a Fabric ADOM.
Website Browsing Over Time by Sessions	The historical websites browsing sessions from recent traffic.

Browsing User Over Time by Bandwidth	The historical browsing users from recent traffic.

ZTNA

ZTNA includes the following widgets:

Statistics	The number of blocked sessions, users, and devices.
Connection Attempts	The number of connection attempts allowed and blocked.
Devices	The number of devices connected and blocked.
ZTNA Device Tags	The number of ZTNA device tags.
User Overview	The number of high risk users, including a summary of the top high risk users.
Known Devices with Failed Posture Check	The number of known devices with a failed posture check by user.
Bandwidth Trends	Bandwidth trends.
Top Users by Connections	Top users by number of connections, allowed and blocked.
Private Apps Access	A list of private apps, including their number of allowed and blocked connections.
Public Cloud Business Apps Access	A list of public cloud business apps, including their number of allowed and blocked connections.
Users	The number of users connected and blocked.
Policy Overview	The number of violated policies, including a summary of the top violated policies.
Private & Public Applications Access Failure History	Private and public app access failures.
CASB Apps Access	A list of CASB apps, including their number of allowed and blocked sessions.

VPN

VPN includes the following widgets:

Top Dialup VPN	The users accessing the network using SSL or IPsec over a VPN tunnel.
VPN Site-to-Site	The names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network.

Traffic Shaping Monitor

This dashboard monitors the traffic shaping information in FortiGate logs. It includes the following widgets:

Bandwidth	The bandwidth of traffic shapers over time. Mouse over the line chart to display the bandwidth at a specific time.
Top Applications and Traffic Shaping	The total traffic by application. Mouse over the stacked bar chart to display a summary of application traffic and dropped bytes for that application. Click a bar in the chart to display the user information for that application in a table view. This view includes a summary of the application traffic, including the number of sessions and bytes (sent/received) by user. This widget displays the top five applications by default.
Dropped Bytes Over Time Per Shaper	The total dropped bytes per shaper. Mouse over the line chart to display a summary of dropped bytes per shaper at a specific time. Click a shaper in the legend to hide/unhide it in the line chart. Greyed-out shapers in the legend are hidden in the line chart. Click *More details* to display the traffic shaping policy hits information in a table view. This table includes the total sessions and bytes (sent/received) by shaping policy.

Endpoints

Endpoints includes the following widgets:

Top Endpoint Vulnerabilities	Vulnerability information about FortiClient endpoints including vulnerability name and CVE ID.
Top Endpoint Vulnerabilities (FortiClient)	Vulnerability information about FortiClient endpoints including vulnerability name and CVE ID. Only available in a Fabric ADOM.
Top Endpoint Devices with Vulnerabilities	Vulnerability information about FortiClient endpoints including source IP address and device.
Top Endpoint Devices with Vulnerabilities (FortiClient)	Vulnerability information about FortiClient endpoints including source IP address and device. Only available in a Fabric ADOM.
User Vulnerabilities Summary	User vulnerabilities summary.
All Endpoints	All endpoints.
All Endpoints (FortiClient)	All endpoints.

Top Endpoint Threats	Top threats from all endpoints.
Top Endpoints Applications	Top applications from all endpoints. Only available in a Fabric ADOM.

Endpoints (FortiClient)

Endpoints (FortiClient) includes the following widgets:

Top Endpoint Vulnerabilities (FortiClient)	Vulnerability information about FortiClient endpoints including vulnerability name and CVE ID. Only available in a Fabric ADOM.
Endpoint Devices	Information about FortiClient endpoints including source IP address, device, and vulnerabilities. Only available in a Fabric ADOM.
All Endpoints (FortiClient)	All endpoints.

Traffic (FortiDDOS)

Traffic (FortiDDOS) includes the following widgets:

Top Source (FortiDDoS)	Top source IP addresses from recent traffic. Only available in a Fabric ADOM.
Top Destination (FortiDDoS)	Top destination IP addresses from recent traffic. Only available in a Fabric ADOM.
Top Type (FortiDDoS)	Top types from recent traffic. Only available in a Fabric ADOM.

Traffic (FortiFirewall)

Traffic (FortiFirewall) includes the following widgets:

Top Sources	The highest network traffic by source IP address and interface, sessions (blocked and allowed), threat score (blocked and allowed), and bandwidth (sent and received).
Top Country/Region	The historical network traffic by country/region, sessions, bandwidth, or threat score.
Top Policy Hits	Top policy hits from recent traffic.
Top Destinations	Top destinations from recent traffic by bandwidth or sessions.

Traffic Over Time by Sessions	The historical destinations from recent traffic.
Policy Hits Over Time by Bandwidth	The historical policy hits from recent traffic.
User Data Flow	Bandwidth breakdown of top user destination country/region or application usage.

Applications & Websites (FortiClient)

Applications & Websites (FortiClient) includes the following widgets:

Application	The top applications used on the network, including application name, risk level, category, sessions (blocked and allowed), and bytes (sent and received). Only available in a Fabric ADOM.
Website	Top website domains from recent traffic. Only available in a Fabric ADOM.

VPN (FortiFirewall)

VPN (FortiFirewall) includes the following widgets:

Top Dialup VPN	The users accessing the network using SSL or IPsec over a VPN tunnel.
VPN Site-to-Site	The names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network.

FortiClient Software Inventory

FortiClient Software includes the following widget:

FortiClient Software Inventory	The total number of apps installed, top apps, new apps installed, top apps by installs, and top hosts by number of apps.

FortiMail

FortiMail includes the following widgets:

Statistics History	The statistics history from FortiMail that displays the summary of total messages and spam in the selected time period. Place your mouse over a line in the chart to view a tooltip which includes the total messages and total spam for the corresponding date and time.

Top Sender by Categories	The top email, virus, and spam senders in the selected time period. Place your mouse over a bar in the graph to view a tooltip which includes the sender, count, size, virus count, and spam count. This widget may be viewed by *Count*, *Size*, *Virus Count*, and *Spam Count*.
Top Recipient by Categories	The top email, virus, and spam recipients in the selected time period. Place your mouse over a bar in the graph to view a tooltip which includes the recipient, count, size, virus count, and spam count. This widget may be viewed by *Count*, *Size*, *Virus Count*, and *Spam Count*.
Threat Statistics	The summary of spam and virus mail in the selected time period. Place your mouse over a bar in the graph to view a tooltip which includes the date/time, classifier, and count. This widget may be viewed by *Count* and *Size*. This widget can be also be displayed as a donut chart which includes charts for total mail, virus mail, and spam mail.
Mail Statistics	The summary of email messages where the FortiMail detected viruses, spam, or neither in the selected time period. Place your mouse over a bar in the graph to view a tooltip which includes the date/time, classifier, and count. This widget may be viewed by *Count*, *Size*, *Scan Speed*, and *Transfer Speed*.
Outbreak Statistics (FortiSandbox)	The summary of the number of email messages that the FortiSandbox unit is scanning in the selected time period. Email messages are tracked as either clean, containing a malicious file, or containing a malicious URL. Place your mouse over a bar in the graph to view a tooltip which includes the date/time, clean, malicious file, and malicious URL. This widget requires a FortiSandbox.
Statistics Summary	The summary of spam, viruses, and not spam in the selected time period, including the classifier details per category, the corresponding total number of every classifier, the subtotal number, the subtotal percentage of every category, and the total number of all emails.

FortiProxy

FortiProxy includes the following widgets:

Top Proxy Sources	Top proxy sources by number of sessions.
Top Proxy Destinations	Top proxy destinations by number of sessions.
Top Website Domains	Top website domains by number of sessions.
Top Threats Destinations	Top threat destinations by threat level.

Top Threats	Top threats by threat level.
Top Applications	Top applications by risk.
Top DLP Events	Top DLP events by number of incidents.

SD-WAN Network

The *SD-WAN > Network* monitor includes the following widgets:

SD-WAN Bandwidth Overview	The bandwidth of the SD-WAN network over time. This widget displays a line chart of the sent/received rate (bps) in the selected time period for SD-WAN members interfaces.
SD-WAN Performance Status	The SD-WAN performance status comparison with interfaces. Mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check. Click on a scatter chart to view additional details.
Top SD-WAN SLA Issues	The top SD-WAN SLA issues. The *Sort By: Speed* option in this widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
SD-WAN Events	This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.
SD-WAN Interfaces	The information for SD-WAN interfaces and ADVPN shortcut interfaces. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
Audio MOS Score	The MOS score by interface. Mousing over the chart displays a summary of the MOS score and VoIP quality at that point. The interface must have a performance SLA with MOS enabled to display in the chart.
Speed Test	The upload and download speeds for all tests run on SD-WAN interfaces through a specified time. This widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
Health Check Status	This widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.



To update the *Refresh Interval*, click the settings icon at the top of the widget, and then select a value from the dropdown.

To filter a chart, click a key in the legend.

SD-WAN Application

The *SD-WAN > Application* monitor includes the following widgets:

Application Performance Overview	A table view for application performance, including the following columns: • *Application Name* • *Latency (ms)* • *Jitter (ms)* • *Packet Loss (%)* • *TCP Retransmission* • *SYN/ACK Retransmission* Double-click a row in the table to drill down for further information about the application. This drill down includes the following widgets: • *Latency Overview*: a line chart displaying total response time, server response time, and network response time. • *Connection Stability*: a line chart displaying jitter, original packet jitter, and reply packet jitter. • *Retransmission*: a stacked bar chart displaying the original, reply, SYN, and SYN-ACK retransmission by time. • *Reliability Monitor*: a bar chart displaying the packet loss, original packet loss, and reply packet loss percentages as well as the original TCP reset and reply TCP reset.
SD-WAN Rules Utilization	The SD-WAN rule traffic utilization by interface and application.
SD-WAN Utilization by Application	The share of bandwidth utilization by application for each WAN link.
Application Bandwidth Utilization	The total bandwidth from all applications as well as the bandwidth per-SD-WAN interface. This widget can be viewed in a sanky chart or table chart format.
Per-Application Performance	The performance for the selected application based on chosen metric. You can select an application in the widget's *Application* dropdown menu. *Latency*, *Jitter*, *Packet Loss*, and *Bandwidth* metrics are available.
Global-Application Performance	The global application performance for the selected metric. *Latency*, *Jitter*, and *Packet Loss* metrics are available.



To update the *Refresh Interval*, click the settings icon at the top of the widget, and then select a value from the dropdown.

To filter a chart, click a key in the legend.

SD-WAN Summary

The *SD-WAN > Summary* monitor includes the following widgets:

SD-WAN Health Overview	The SD-WAN devices' status.

Top SD-WAN SLA Issues	The SD-WAN SLA issues. The *Sort By: Speed* option in this widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
Top SD-WAN Applications	The SD-WAN devices' top applications.
SD-WAN Top Device Throughput	The SD-WAN devices' throughput.
Top SD-WAN Talkers	The SD-WAN devices' top talkers.
Speed Test By Bandwidth	The combined upload and download speeds for all tests run on SD-WAN interfaces on each device. This widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
Speed Test Summary	The upload and download speeds for all tests run on SD-WAN interfaces through the specified time period on selected devices. This widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.



To update the *Refresh Interval*, click the settings icon at the top of the widget, and then select a value from the dropdown.

To filter a chart, click a key in the legend.

WiFi

WiFi includes the following widgets:

Authorized APs	The names of authorized WiFi access points on the network.
Top Rogue APs	The top SSID (service set identifiers) of unauthorized WiFi access points on the network. Hover the cursor over data points to see the SSID and total live time.
Top SSID	The top SSID (service set identifiers) of authorized WiFi access points on the network. Hover the cursor over data points to see the SSID and bytes (sent and received).
Top SSID Over Time by Bandwidth	The historical SSID (service set identifiers) traffic of authorized WiFi access points on the network.
WiFi Clients	The top WiFi access points on the network by bandwidth/sessions.

IoT

IoT includes the following widget:

IoT Inventory	The total number of IoT devices installed.

	This includes summaries for the new IoT apps installed, top IoT apps, top IoT users, and top IoT by number of hosts.

Fabric State of Security

Security Fabric includes the following widgets.

The information for this dashboard is available after you create a Security Fabric group in FortiGate and add it in FortiAnalyzer. The Security Fabric can be selected in the settings options for each widget.

Security Fabric Rating Report	A report showing the security rating details of connected Security Fabric devices. Click a milestone to drill down and hover the cursor over data points to see more details.
Security Fabric Score	The current and historical Security Fabric scores. The Historical Security Fabric Scores pane displays your Security Fabric score over time and how it compares to the industry average and the industry score range. You can hide the Historical Security Fabric Scores pane.
Security Fabric Topology	A topology map showing the logical structure of connected Security Fabric devices.
Best Practices Overview	Overview of the device best practices across regions of North America, Latin America, EMEA, and APAC.

Local System Performance

This dashboard monitors the system performance of the FortiAnalyzer unit running FortiView. It includes the following widgets:

Multi Core CPU Usage	The usage status of a multi-core CPU.
Insert Rate vs Receive Rate	The number of logs received vs the number of logs actively inserted into the database, including the maximum and minimum rates. • Receive rate: how many logs are being received. • Insert rate: how many logs are being actively inserted into the database. If the insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.
CPU & Memory Usage	The usage status of the CPU and memory.
Disk I/O	The disk *Transaction Rate* (I/Os per second), *Throughput* (KB/s), or *Utilization* (%). The *Transaction Rate* and *Throughput* graphs also show the maximum and minimum disk activity.
Receive Rate vs Forwarding Rate	The number of logs received vs the number of logs forwarded out, including the maximum and minimum rates. • Receive rate: how many logs are being received. • Forward rate: how many logs are being forwarded out.

Resource Usage Average	Overview of average resource usage history across all devices.
Resource Usage Peak	Overview of peak resource usage history across all devices.
Failed Authentication Attempts	Top unauthorized connections from recent traffic.
System Events	Top system events from recent traffic.
Admin Logins	Top admin logins from recent traffic.

Using the monitors dashboard

FortiView monitors contain widgets that provide network and security information. Use the controls in the dashboard toolbar to work with a dashboard.

Add Widget	Add widgets from the list available.
Edit Layout	Remove, resize, or move widgets on a predefined dashboard.
Devices	Select the devices to include in the widget data. The device list will also include a Security Fabric if available. To select a Security Fabric, you need to first create a Security Fabric group in FortiGate and add the Security Fabric group in FortiAnalyzer.
Time Period	Select a time period from the dropdown menu, or set a custom time period.
Dark Mode	Enable/disable dark mode. Dark mode shows a black background for the widgets in the dashboard.
Refresh	Refresh the data in the widgets.
Hide Side-menu or Show Side-menu	Using the main toolbar, you can hide or show the tree menu on the left. In a typical SOC environment, the side menu is hidden and dashboards are displayed in full screen mode.

Use the controls in the widget title bar to work with widgets.

Settings icon	Change the settings of the widget. Widgets have settings applicable to that widget, such as how many of the top items to display, *Time Period*, *Refresh Interval*, and *Chart Type*.
View different chart types	Some widget settings let you choose different chart types such as the *Disk I/O* and *Top Countries* widget. You can add these widgets multiple times and set each widget to show a different chart type.
Hide or show a data type	For widgets that show different data types, click a data type in the title bar to hide or show that data type in the graph.

	For example, in the *Insert Rate vs Receive Rate* widget, click *Receive Rate* or *Insert Rate* in the title bar to hide or show that data. In the *Disk I/O* widget, click *Read* or *Write* in the title bar to hide or show that data type.
View more details	Hover the cursor over a widget's data points to see more details.
View a narrower time period	Some widgets have buttons below the graph. Click and drag the buttons to view a narrower time period.
Zoom in and out	For widgets that show information on a map such as the *Top Threat Destinations* widget, use the scroll wheel to change the zoom level. Click and drag the map to view a different area.

Customizing the monitors dashboard

You can add any widget to a custom or predefined dashboard. You can also move, resize, or remove widgets. You cannot rename or delete a predefined dashboard. To reset a predefined dashboard to its default settings, open the dashboard and click *Edit Layout* > *Reset Layout*.

To create a dashboard:

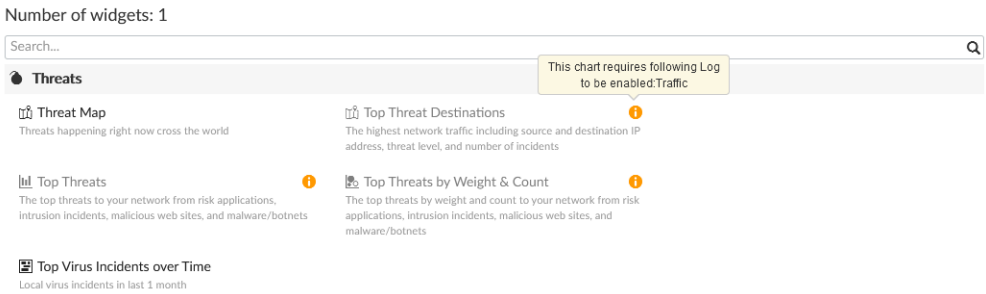
1. In *FortiView*, click the menu icon for *Custom Views*.
   Mouse-over *Custom Views* to display the menu icon.
2. From the shortcut menu, click *Create New*.
3. Specify the *Name* and whether you want to create a blank dashboard or use a template.
   If you select *From Template*, specify which predefined dashboard you want to use as a template.
4. Click *OK*. The new dashboard appears in the tree menu.
5. Select widgets to include on the dashboard, and click *Save Changes*.

To display Security Fabric in Monitor:

1. Create a Security Fabric in FortiGate.
2. Add the Security Fabric in FortiAnalyzer.
3. Go to *FortiView* > *Fabric Devices* > *Fabric State of Security*.
4. Select the Security Fabric from the *Devices* menu.

To add a widget:

1. Select the predefined or custom dashboard where you want to add a widget.
2. Click *Add Widget* to see a list of available widgets. Select the widget(s) you would like to add.
   Some widgets can only be added when their corresponding log type is enabled in the ADOM, for example, the *Top Threats* widget requires that *Traffic* logs are enabled. Widgets that cannot be added appear in gray and include an information icon indicating what logs must be present in the ADOM before the widget can be added to the dashboard.



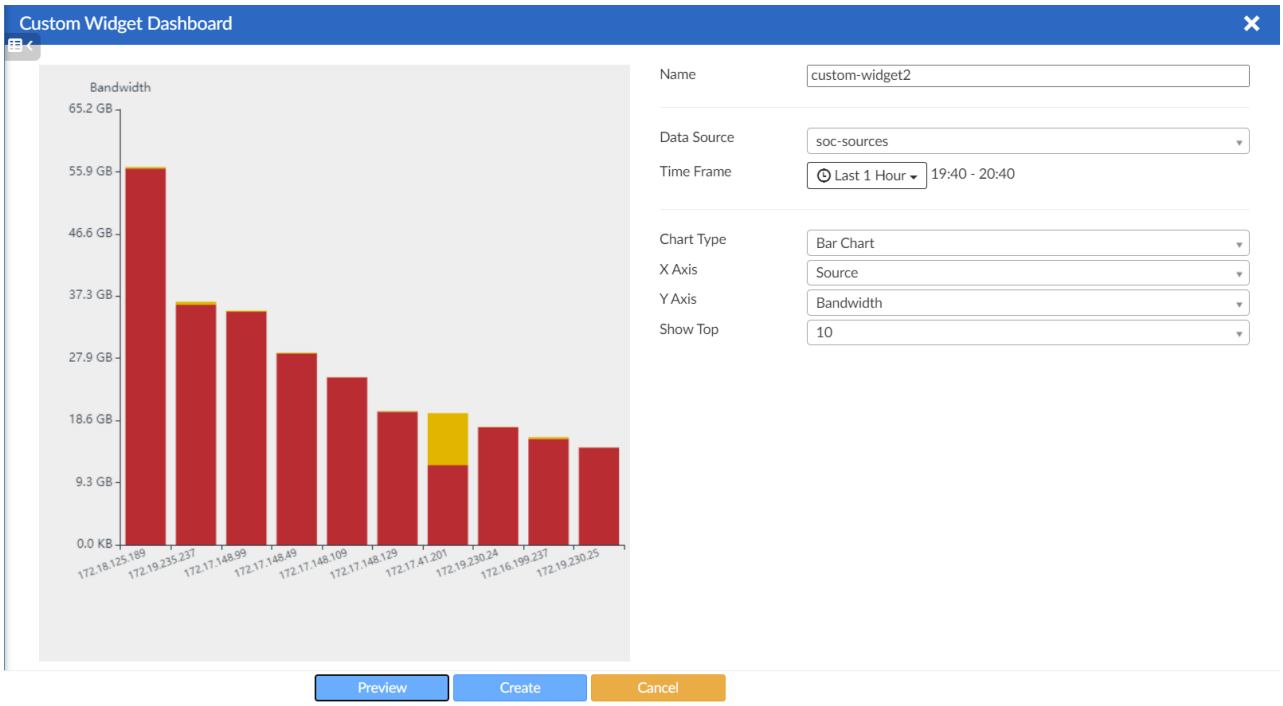
3. When you have finished adding widgets, click *Save Changes* to close the *Add Widget* pane.

Creating custom widgets

Custom widgets can be created and added to custom dashboards in *FortiView* > *Monitors*.

To create a custom widget:

1. Go to *FortiView* > *Custom View* and select a previously configured custom dashboard.
2. Click *Add Widget*.
   For information on creating and managing dashboards, see Customizing the monitors dashboard on page 142
3. Scroll to the *Custom Widgets* field and click *Add Widget*.
   The *Custom Widget Dashboard* opens.
4. Configure the following information for your widget.



Name	Enter a name for the widget.
Data Source	Select a data source for the widget. The following data sources are available: • soc-sources • soc-destinations • soc-threats • soc-sdwan-stats
Time Frame	Select the time frame. You can specify a custom time frame by clicking *Custom...*, choosing the start and end date, and clicking *Apply*.
Chart Type	Choose how the data is presented in the widget from one of the following options: • Bar Chart • Line Chart • Pie Chart • Donut Chart
X Axis	Select the source type for the X axis. The sources available for selection depend on the data source selected. X Axis is only available when the chart type is Bar or Line.
Y Axis	Select the source type for the Y axis. The sources available for selection depend on the data source selected. Y Axis is only available when the chart type is Bar or Line.
Category	Select the data category. The categories available for selection depend on the data source selected. Category is only available when the chart type is Pie or Donut.
Value	Select the data value. The values available for selection depend on the data source selected. Value is only available when the chart type is Pie or Donut.
Show Top	Select the number of results that are displayed in the widget. Options include the top 10, 20, 50, and 100 results.

5. Click *Preview* to preview the widget based on the information selected.
6. Click *Create* to save your changes.
   After the widget has been created, you can select it in the *Add Widget* window to add it to your dashboard. For information on managing your dashboard, see Using the monitors dashboard on page 141.

To edit a custom widget:

1. In any custom dashboard, click *Add Widget*.
2. Right-click on the custom widget that you want to edit, and click *Edit*
3. Edit the widget's settings, and click *Update*.

To delete a custom widget:

1. In any custom dashboard, click *Add Widget*.
2. Right-click on the custom widget that you want to delete, and click *Delete*.

Enabling and disabling FortiView

The FortiAnalyzer *FortiView* module can be disabled for performance tuning through the CLI. When disabled, the GUI will hide FortiView and stop background processing for this feature.

To disable *FortiView* in the CLI:

```
config system global
   set disable-module fortiview-noc
end
```

To enable *FortiView* in the CLI:

```
config system global
   unset disable-module
end
```



Disabling FortiView will cause the FortiAnalyzer to return the following error message when the FortiGate attempts to retrieve FortiAnalyzer data: `Server Error: FortiView\/NOC function is disabled on FortiAnalyzer`.

The FortiGate GUI displays the message: `Failed to retrieve FortiView data`.

Log View and Log Quota Management

You can view log information by device or by log group.



When rebuilding the SQL database, *Log View* is not available until the rebuild is complete. Click the *Show Progress* link in the message to view the status of the SQL rebuild.

When ADOMs are enabled, each ADOM has its own information displayed in *Log View*.

Log View > *Logs* > *All / Fortinet Logs* can display the real-time log or historical (Analytics) logs.

Log View > *Logs* > *Log Browse* can display logs from both the current, active log file and any compressed log files.

For more information, see Analytics and Archive logs on page 46.

Types of logs collected for each device

FortiAnalyzer can collect logs from the following device types: FortiADC, FortiAnalyzer, FortiAuthenticator, FortiCache, FortiCarrier, FortiCASB, FortiClient, FortiDDoS, FortiDeceptor, FortiEDR, FortiGate, FortiIsolator, FortiMail, FortiManager, FortiNAC, FortiNDR, FortiPAM, FortiProxy, FortiSandbox, FortiSOAR, FortiSRA, FortiWeb, and Syslog servers. Following is a description of the types of logs FortiAnalyzer collects from each type of device:

Device Type	Log Type
Fabric	Normalized
FortiADC	Event, Intrusion Prevention, Traffic
FortiAnalyzer	Event, Application
FortiAuthenticator	Event
FortiGate	Traffic Security: Antivirus, Intrusion Prevention, Application Control, Web Filter, File Filter, DNS, Data Loss Prevention, Email Filter, Web Application Firewall, Vulnerability Scan, VoIP, FortiClient Event: Endpoint, HA, Compliance, System, Router, VPN, User, WAN Opt. & Cache, WiFi, FortiSASE  File Filter logs are sent when the File Filter sensor is enabled in the FortiOS Web Filter profile. You can enable the File Filter sensor in FortiOS at *Security Profiles* > *Web Filters*.

Device Type	Log Type
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiCarrier	Traffic, Event, GTP
FortiCASB	Data Loss Prevention
FortiClient	Traffic, Event, Vulnerability Scan
FortiDDoS	Event, Intrusion Prevention
FortiDeceptor	Event
FortiEDR	Event: Audit, System Event, Security Event
FortiIsolator	Traffic, Event
FortiMail	History, Event, Antivirus, Email Filter  FortiMail logs support cross-log functionality. When viewing History, Event, Antivirus, or Email Filter logs from FortiMail, you can click on the Session ID to see correlated logs. For more information, see FortiMail correlated logs on page 166.
FortiManager	Event
FortiNAC	Event
FortiNDR	Event, NDR, Netflow Attack: Attack Chain, Malware
FortiPAM	Data Loss Prevention, Event, Protocol, Secret, SSH, Traffic, Antivirus, Zero-Trust Network Access
FortiProxy	Traffic, Event, Antivirus, Web Filter
FortiSandbox	Malware, Network Alerts
FortiSOAR	Event
FortiSRA	Data Loss Prevention, Event, Protocol, Secret, SSH, Traffic, Antivirus, Zero-Trust Network Access
FortiToken	Event
FortiWeb	Attack, Event, Traffic  You can view a subset of FortiWEB packet logs which contain additional HTTP request information. See Viewing message details on page 152.
Syslog	Generic



The logs displayed on your FortiAnalyzer depends on the device type logging to it and the enabled features.

ADOMs must be enabled to support non-FortiGate logging. In a Security Fabric ADOM, all device logs are displayed.

Traffic logs

Traffic logs record the traffic flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through FortiGate, this type of logging is also called firewall policy logging. Firewall policies control all traffic attempting to pass through the FortiGate unit, between FortiGate interfaces, zones, and VLAN sub-interfaces.

ZTNA logs: FortiAnalyzer syncs unified ZTNA logs with FortiGate. ZTNA logs are a sub-type of FortiGate traffic logs, and can be viewed in *Log View > FortiGate > Traffic*. You can filter for ZTNA logs using the sub-type filter and optionally create a custom view for ZTNA logs. See Custom views on page 162.

Security logs

Security logs (FortiGate) record all antivirus, web filtering, file filtering, application control, intrusion prevention, email filtering, data loss prevention, vulnerability scan, and VoIP activity on your managed devices.

DNS logs

DNS logs (FortiGate) record the DNS activity on your managed devices.

Event logs

Event logs record administration management and Fortinet device system activity, such as when a configuration changes, or admin login or HA events occur. Event logs are important because they record Fortinet device system activity which provides valuable information about how your Fortinet unit is performing. FortiGate event logs includes *System*, *Router*, *VPN*, *User*, and *WiFi* menu objects to provide you with more granularity when viewing and searching log data. The ForiSASE log subtype is also available; for more information, see "Filtering for event logs generated when FortiManager installs configuration to FortiSASE" in Filtering messages on page 156.

Application Logs

Application logs record playbook and incident activity on FortiAnalyzer. Logs are generated and stored separately for each ADOM. Application logs can only be viewed on the local FortiAnalyzer.

Syslog logs

Syslog logs are standardized generic logs that can be sent from third-party or Fortinet devices to FortiAnalyzer. These logs can be used to collect information about system events, warnings, and other messages from the logging devices.

When syslog logs are sent to FortiAnalyzer, they can be viewed in *Log View > Logs > Fortinet Logs > Syslog*. The content of the syslog log is included unparsed in the *Message* field of *Log View*.

You can use wildcards (*) to filter *Log View* for information in the syslog logs. For example, if `hostname=<endpoint>` is included in the syslog log messages from a device, you can filter *Log View* by `Message=*hostname=example*` to return all logs from a specific endpoint. You must have knowledge of the syslog log format to filter effectively using this method.

Syslog logs are also supported in reports and event handlers, but the use case is limited because the information is not parsed into normalized fields, such as source IP, timestamp, event type, and so on. Instead, these objects would have to be configured using the limited fields populated for the logs in *Log View* > *Logs* > *Fortinet Logs* > *Syslog*.

With an appropriate log parser for the logging device in FortiAnalyzer, however, these syslog logs can be parsed, normalized, and inserted into the SIEM database (siemdb) as **fabric logs**. The table below briefly demonstrates the difference.

Log parser available?	Description
No	The **syslog logs** can be viewed in *Log View* > *Logs* > *Fortinet Logs* > *Syslog*. These logs have limited use in reports and event handlers because the information is not parsed into normalized fields, such as source IP, timestamp, event type, and so on. Instead, the information from the syslog log is included unparsed in the *Message* field.
Yes	The syslog logs will be parsed, normalized, and inserted into the SIEM database (siemdb) as **fabric logs**. These logs can be viewed in *Log View* > *Logs* > *All*. You can use the normalized fields to effectively create reports and event handlers for correlation and analysis. You can also leverage predefined dashboards, reports, and event handlers when they are available for the fabric logs. For more information, see Fabric logs on page 151.

Configuring a device to send syslog logs

You can configure third-party devices and Fortinet devices to send syslog logs to FortiAnalyzer. To do so, you must add FortiAnalyzer as a syslog server for the device and configure it to send logs to FortiAnalyzer. The device will then appear in *Device Manager*, where it can be authorized and added to a Fabric ADOM.

This topic provides a brief overview for configuring a device to send syslog logs to FortiAnalyzer. You must review the device's documentation to complete configuration properly on that device.

To configure the device to send syslog logs to FortiAnalyzer:

1. In the logging device, add FortiAnalyzer as a syslog server and configure the device to send logs to FortiAnalyzer.
   On FortiAnalyzer, the device will appear in *Device Manager* with the unauthorized devices.
2. In FortiAnalyzer, go to *Device Manager* and authorize the logging device.
   If you are using ADOMs, add the syslog device to a Fabric ADOM.

If FortiAnalyzer does not have a log parser for this device, the logs will be available in *Log View* > *Logs* > *Fortinet Logs* > *Syslog*.

If FortiAnalyzer does have a log parser for this device, it will be automatically assigned to the device based on the log format and the logs will be available in *Log View > Logs > All*. For more information about fabric logs and log parsers, see Fabric logs on page 151.

For more information about log parsers, see Log parsers on page 151.

Sending syslog logs over TLS

You can configure FortiAnalyzer to use an externally signed local (custom) certificate for OFTP connection between the syslog device and FortiAnalyzer for logging over TLS. Make sure to complete the config and check connection according to the syslog device you are using.

To generate a certificate signing request from FortiAnalyzer:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Click *Create New/Import > Generate CSR*.
3. Enter the relevant information in the certificate signing request, and then click *OK*.
4. Select the newly created CSR and click *Download*.
5. To generate the certificate, sign the CSR with either a public CA or private CA.
   For example, you can use a FortiAuthenticator to sign the CSR. For more information, see the FortiAuthenticator Administration Guide.
6. After signing the CSR, export and download the certificate.
7. In FortiAnalyzer, import the signed certificate:
   a. Go to *System Settings > Certificates > Local Certificates*.
   b. Click *Create New/Import > Certificate*.
   c. In the *Type* field, select *Local Certificate*.
   d. In the *Certificate File* field, drag and drop or select the signed certificate.
   e. Click *OK*.
8. The certificate status will change from *PENDING* to *OK* once the certificate is uploaded correctly.

To configure the use of the local certificate and restart the OFTP daemon:

1. Once the certificate has been imported, enter the following command in the FortiAnalyzer CLI to use the local certificate:
```
config system certificate oftp
   set mode local
   set local "<name of the certificate>"
end
```
2. In the FortiAnalyzer CLI, enter the following command to restart the OFTP daemon:
```
diagnose test application oftpd 99
```
3. If a private CA was used, you must import the signed CA certificate in the logging device as well.
4. Validate the connection status to FortiAnalyzer in the logging device.
   This step will vary according to the logging device. For generic steps to establish connection, see Configuring a device to send syslog logs above.

To set the TCP port for receiving syslog over TLS:

Enter the following command in the FortiAnalyzer CLI:

```
config system log settings
   set syslog-over-tls-port {514 | 6514}
end
```

Variable	Description
syslog-over-tls-port {514 | 6514}	Set the TCP port for receiving syslog over TLS: • 514: Default port for syslog over TLS receiving (default). • 6514: Port 6514 recommended by RFC 5425.

Fabric logs

Fabric logs are logs that have been parsed, normalized, and inserted into the FortiAnalyzer's SIEM database (siemdb). FortiAnalyzer can parse logs from third-party and Fortinet devices according to the log parsers available in FortiAnalyzer. The fabric logs from all devices in the fabric ADOM are visible within *Log View > Logs > All*.

Fabric logs enhance FortiAnalyzer's SIEM capabilities to analyze and correlate logs from many logging devices in the network. FortiAnalyzer can effectively generate reports and trigger event handlers using the normalized fields of these fabric logs.



Imported log files and logs that are received prior to log parser assignment are not included in the SIEM database.

Log parsers

Log parsers are required to parse, normalize, and insert logs into the siemdb as fabric logs. Enabled log parsers are assigned automatically to devices based on their logs using matching patterns. If the appropriate log parser is not available or enabled in FortiAnalyzer, the logs will not be parsed or inserted to the siemdb as fabric logs. Instead, you can find and use the logs only by their device and log type in the correct ADOM.

There are many predefined log parsers for third-party and Fortinet devices in FortiAnalyzer. The log parsers are automatically assigned to devices based on the format of the incoming logs. In addition, there are also predefined dashboards, reports, and event handlers that utilize fabric logs from third-party and Fortinet devices. To review the list of built-in predefined log parsers and the normalized fields, see the Fabric Normalization Reference.

Further predefined log parsers, reports, and event handlers are also available from FortiGuard when FortiAnalyzer has a valid license for the Security Automation Service. For a list of additional objects available through FortiGuard, see the SOC Automation Content Pack.

If there is no predefined log parser, you can configure a custom log parser for the device in FortiAnalyzer. See the FortiAnalyzer Custom Log Parsers document.

You can view, create, manage, and validate log parsers within FortiAnalyzer from *Incidents & Events > Log Parsers > Log Parsers*. For more information, see SIEM log parsers on page 397.

Log parser reference documentation:

- To review the list of built-in predefined log parsers and the normalized fields, see the Fabric Normalization Reference.
- To review the list of predefined log parsers available through FortiGuard, see the SOC Automation Content Pack.
- To create a custom log parsers, see the FortiAnalyzer Custom Log Parsers document.
- To manage existing log parsers, see SIEM log parsers on page 397 in this Administration Guide.

Log messages

You can view log information by device or by log group.

Viewing the log message list of a specific log type

You can find FortiMail and FortiWeb logs in their default ADOMs.

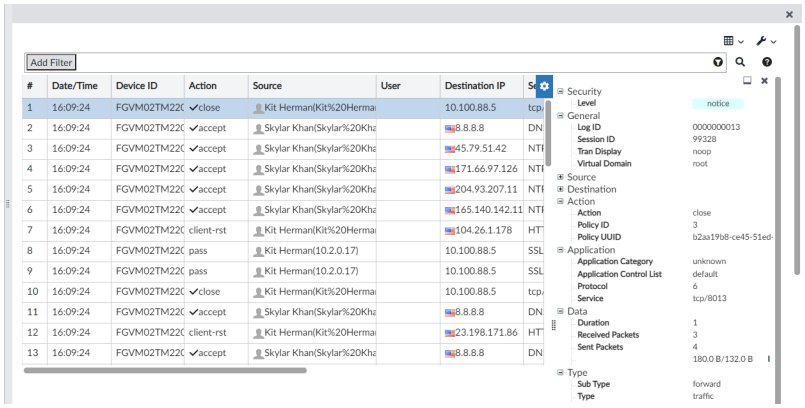
To view the log message list:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Log View* > *Logs* > *Fortinet Logs*, and select the appropriate device type.
3. From the toolbar, select the appropriate log type.
   The corresponding log messages list is displayed.

Viewing message details

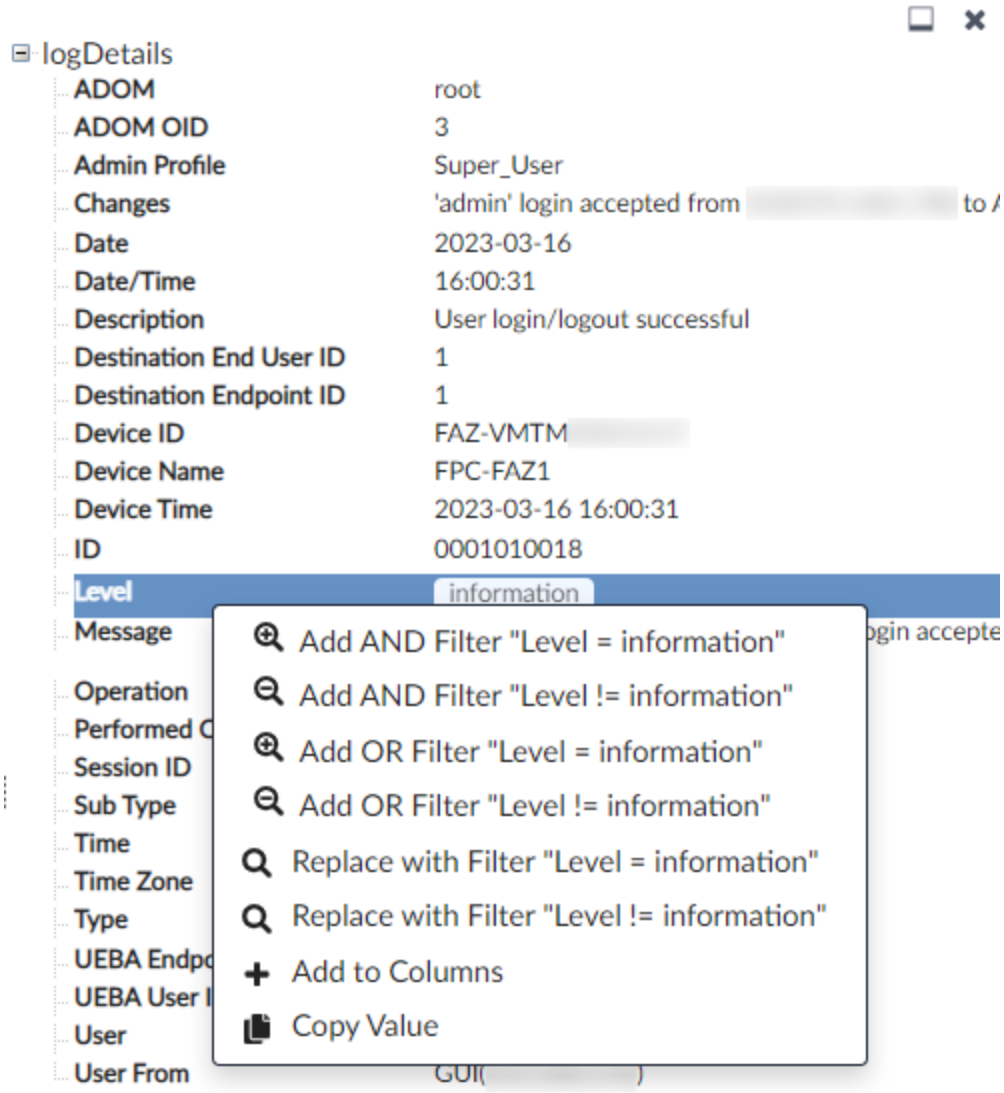
To view message details:

1. Double-click a message in the message list.
   The details pane is displayed to the right of the message list, with the fields categorized in tree view.



You can display the log details pane below the message list by clicking the *Bottom* icon in the log details pane. When the log details pane is displayed below the message list, you can move it to the right of the log message list by clicking the *Right* icon. This is sometimes referred to as docking the pane to the bottom or right of the screen.

The log details pane provides shortcuts for adding or replacing filters and for showing or hiding a column. Right-click a log field to select an option.

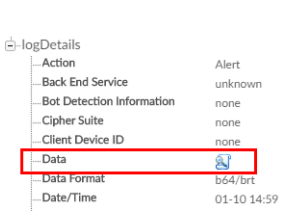


If the log message contains UTM logs, you can click the UTM log icon in the log details pane to open the UTM log view window.

If the log message contains IPS signature information, you can click the IPS signature link under *Attack Name* to view the IPS Signature details in a dialog window.

To view FortiWEB packet logs:

1. Go to *Log View* > *Logs* > *Fortinet Logs*, and select the FortiWeb device type.
2. From the log type dropdown, select *Attack* log.
3. Double-click a message in the list to open the log details pane.
4. In the *Data* field, click the *Device* icon. The *View Attack Content* dialog displays a subset of FortiWEB's packet log (headers, arguments, and a truncated HTTP body). The maximum size of the packet log is 8 KB.





The *Device* icon is also available in the *Data* column. To display the column, click *More Columns*, and select *Data* from the dropdown.

To download an encrypted archive file in ZIP format:

You can set packet capture (PCAP) files to download from FortiAnalyzer encrypted and/or in ZIP format.

By default, PCAP files are downloaded in ZIP format. To adjust this setting, use the following command in the FortiAnalyzer CLI:

```
config system log pcap-file
   set download-mode {plain | zip | zip-with-password}
end
```

You can download archive files from logs via the FortiAnalyzer GUI in the log detail panel. The below example demonstrates how to download a PCAP file that is encrypted in ZIP format.

1. In the FortiAnalyzer CLI, set the pcap-file download mode to zip-with-password:
   ```
   config system log pcap-file
      set download-mode zip-with-password
   end
   ```
2. In the FortiAnalyzer GUI, go to *Log View* and double-click a log containing an archive file.
3. In the *Data* section, click the download icon for the *Archive* field.

   The file is downloaded and the password displays in the FortiAnalyzer GUI. You can copy the password, as needed.

   To unlock the downloaded file, if appropriate, you must use the password.

Customizing displayed columns

The columns displayed in the log message list can be customized and reordered as needed.

To customize the columns and their order in the table:

1. In the table header, click the settings icon.
   The available columns vary depending on the device and log type.
2. Select the columns that should display for the table.
   Use the search bar above the list to find columns, if needed.
   When a column is added, it is automatically added in the sequence displayed in the list. The added column is highlighted in the table when added for reference.
3. To rearrange the order of the columns in the table, drag and drop the columns to the appropriate order in the list.
4. If needed, you can reset the columns by clicking *Reset to Default*.
5. To change the default view to the current columns and order,click *Save as Default*.
   Only a Super_User administrator profile can set the default view. To reset default columns to the system default, see Customizing default columns on page 155.
6. To save the changes, click away from the list of columns.



You can add or remove a log field column in the log details pane. Double-click a log to open the log details pane, and then right-click the log field and select *Add to Columns* or *Remove from Columns*.

Customizing default columns

In *Log View*, you can select the columns that are displayed as the default. In *Log View* > *Logs* for the appropriate device type and log type, click the settings icon in the table header. After selecting the appropriate columns, click *Save as Default*. For more information, see Customizing displayed columns on page 155.

Customizing the default column view can only be done on a Super_User administrator profile.

Default column customization is applied per devtype/logtype across all ADOMs.

The GUI displays columns based on the following order of priority:

1. Displays the user's column customizations (if defined).
2. Displays the default columns set by the Super_User administrator (if defined).
3. Displays the system default columns.

Customized default column configuration is preserved during upgrades.



To reset default columns to the system default, deselect *all* columns from the *Column Settings* selection menu and then select *Set as Default*.

Filtering messages

You can apply filters to the message list. Filters are not case-sensitive by default. If available, select *Tools* > *Case Sensitive Search* to create case-sensitive filters.

Filtering messages using filters in the toolbar

1. Go to the appropriate *Log View*.
2. In the toolbar, make other selections, such as devices and time period.
3. From the *More* dropdown, you can toggle between a *Case Sensitve Search* and a *Case Insensitive Search*.
4. In the table header, click the settings icon to select the available columns in the table.
   When a column is added, it is automatically added in the sequence displayed in the list. The added column is highlighted in the table when added for reference. You can drag and drop the columns to rearrage their display order.
5. In the search bar, add filters for the table:

Toggling between Filter Mode and Text Mode	From the dropdown next to the search bar, select *Filter Mode* or *Text Mode*. The filter criteria is maintained when toggling between the modes. See below for more information about these modes.
Filter Mode	Click *Add Filter* to select a filter from the dropdown list. Then select an operator (=, !=, <, >, >=, <=, ~, or !~) and a value for the filter; you can begin typing a value to select it from the list. Click *Apply* to add the filter. Click the *Add Filter* again to add another filter. It will be added with an `AND` relationship to the previous filter; click the AND to toggle between `AND` (all filters are met) and `OR` (one of the filters are met). When adding a filter, only displayed columns are available in the dropdown list. To add more columns, click the settings icon in the table header.
Text Mode	In text mode search, enter the search criteria (log field names, operators, and values).
Remove filters	After entering filters, you can click the "x" at the left side of the search bar to remove the filters.
Search operators and syntax	Click the help icon at the right end of the *Add Filter* box to view search operators and syntax. See also Filter search operators and syntax on page 158.

CLI string “freestyle” search	Searches the string within the indexed fields configured using the CLI command: `config ts-index-field`.
	For example, if the indexed fields have been configured using these CLI commands:
	`config system sql`
	`  config ts-index-field`
	`  edit "FGT-traffic"`
	`  set value "app,dstip,proto,service,srcip,user,utmaction"`
	`  next`

```
    end
end
```

Then if you type "Skype" in the *Add Filter* box, FortiAnalyzer searches for "Skype" within these indexed fields: `app,dstip,proto,service,srcip,user` and `utmaction`.

You can combine freestyle search with other search methods, for example: `Skype user=David`.



UUID logging must be enabled in FortiGate/FortiOS to filter FortiGate traffic logs by object name, including `Source Object` and `Destination Object`. See the FortiGate/FortiOS Administration Guide for more information about UUID logging.

Filtering messages using the right-click menu

In the log message table view, right-click an entry to select a filter criteria from the menu. Depending on the column you right-clicked, *Log View* uses the column value as the filter criteria. This context-sensitive filter is only available for certain columns.

You can perform the following filter actions from the right-click menu:

- Add a filter entry with an *AND* condition, such as `AND event_type=traffic`
- Add a filter entry with an *AND* negate condition, such as `AND event_type!=traffic`
- Add a filter entry with an *OR* condition, such as `OR event_type=traffic`
- Add a filter entry with an *OR* negate condition, such as `OR event_type!=traffic`
- Replace all filters with the selected entry, such as `event_type=utm`
- Replace all filters with the selected negate, such as `event_type!=utm`

If no filter is used before right-click filtering, the new filter will be added no matter which option is selected in the right-click menu.



To see log field name of a filter/column, right-click the column of a log entry and select a context-sensitive filter. The *Add Filter* box shows log field name.

Context-sensitive filters are available for each log field in the log details pane. See Viewing message details on page 152.

Filtering messages using smart action filters

For *Log View* windows that have an *Action* column, the *Action* column displays smart information according to policy (log field action) and utmaction (UTM profile action).

The *Action* column displays a green checkmark *Accept* icon when both policy and UTM profile allow the traffic to pass through, that is, both the log field action and UTM profile action specify *allow* to this traffic.

The *Action* column displays a red X *Deny* icon and the reason when either the log field action or UTM profile action deny the traffic.

If the traffic is denied due to policy, the deny reason is based on the policy log field action.

If the traffic is denied due to UTM profile, the deny reason is based on the FortiView `threattype` from `craction`. `craction` shows which type of threat triggered the UTM action. The `threattype`, `craction`, and `crscore` fields are configured in FortiGate in Log & Report. For more information, see the *FortiOS - Log Message Reference* in the *Fortinet Document Library*.

A filter applied to the *Action* column is always a smart action filter.



The smart action filter uses the FortiGate UTM profile to determine what the *Action* column displays. If the FortiGate UTM profile has set an action to *allow*, then the *Action* column will display that line with a green *Accept* icon, even if the `craction` field defines that traffic as a threat. The green *Accept* icon does not display any explanation.

In the scenario where the `craction` field defines the traffic as a threat but the FortiGate UTM profile has set an action to *allow*, that line in the Log View *Action* column displays a green *Accept* icon. The green *Accept* icon does not display any explanation.

Filter search operators and syntax

Operators or symbols	Syntax
And	Find log entries containing all the search terms. Connect the terms with a space character, or "and". Examples: 1. `user=henry group=sales` 2. `user=henry and group=sales`
Or	Find log entries containing any of the search terms. Separate the terms with "or" or a comma ",". Examples: 1. `user=henry or srcip=10.1.0.15` 2. `user=henry,linda`
Not	Find log entries that do NOT contain the search terms. Add "-" before the field name. Example: `-user=henry`
>, <	Find log entries greater than or less than a value, or within a range. This operator only applies to integer fields. Example: `policyid>1 and policyid<10`
IP subnet, range, subnet list search	Find log entries within a certain IP subnet, IP range, subnet list, or subnet group. Examples: 1. `srcip=192.168.1.0/24` 2. `srcip=10.1.0.1-10.1.0.254` 3. `srcip=SubnetGrp_Name_A` 4. `srcip=Subnet_Name_A` To create a subnet list or subnet group, see Subnets on page 191.
Reg Exp search	You can use regular expression searches for all field types. Examples: 1. `srcip~"192\.168\.1\.*"` 2. `policyid~"1.*"` 3. `user~"^A.*"` (to find user starting with "A")



Log View also supports the regex (regular expresion) syntax.

Filtering FortiClient log messages in FortiGate traffic logs

For FortiClient endpoints registered to FortiGate devices, you can filter log messages in FortiGate traffic log files that are triggered by FortiClient.

To filter FortiClient log messages:

1. Go to *Log View* > *Logs* > *Fortient Logs* > *FortiGate* > *Traffic*.
2. In the *Add Filter* box, type `fct_devid=*`. A list of FortiGate traffic logs triggered by FortiClient is displayed.
3. In the message log list, select a FortiGate traffic log to view the details.
4. Click the *FortiClient* tab, and double-click a FortiClient traffic log to see details.
   The *FortiClient* tab is available only when the FortiGate traffic logs reference FortiClient traffic logs.

Filtering for event logs generated when FortiManager installs configuration to FortiSASE

When FortiManager is configured to manage FortiSASE, event logs will be generated by FortiOS when configuration is installed to FortiSASE. The log output from FortiOS will include the FortiManager device name as well as the admin username.

To filter for logs generated when FortiManager installs configuration to FortiSASE:

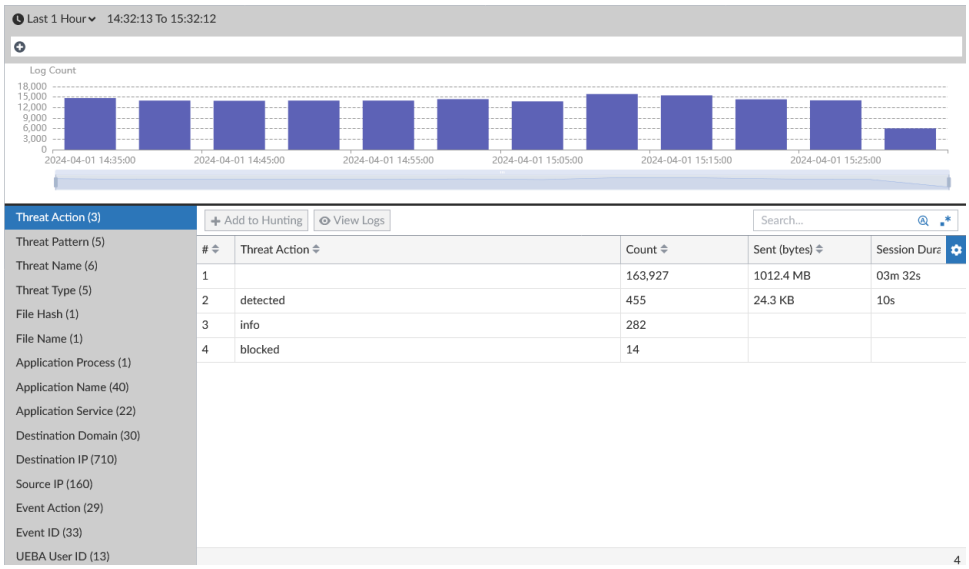
1. *Log View* > *Logs* > *Fortinet Logs* > *FortiGate*
2. From the *Event* dropdown, select *FortiSASE*.
   The *Remote Device Name* column displays the FortiManager device name.
   The *Remote Admin* column displays the FortiManager admin username.

Threat Hunting

The *Threat Hunting* pane offers a SOC analytics dashboard using the SIEM database. *Threat Hunting* uses cached data to allow SOC analysts to quickly drilldown on logs in fields of interest. To view the *Threat Hunting* dashboard, go to *Log View* > *Logs* > *Threat Hunting*. The *Threat Hunting* dashboard includes a log count chart and SIEM log analytics table.

The *Threat Hunting* dashboard is only available in Fabric ADOMs when ADOMs are enabled.

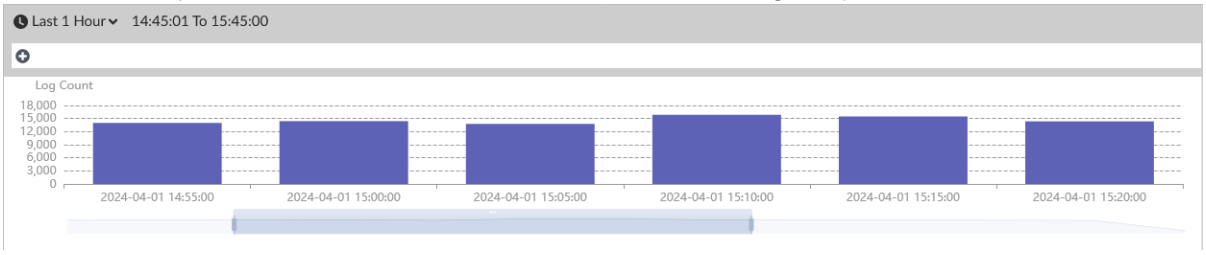
To change the displayed time range, select a time from the dropdown in the top-left corner of the dashboard. You can configure custom time ranges by selecting either *Last N Minutes*, *Last N Hours*, or *Last N Days*. Apply filters to the dashboard using *Add Filter* or by selecting an item in the table and clicking Add to Hunting. Only logs matching the selected time range and filter are displayed in the SIEM log analytics table.



Using the log count chart

A chart displaying the total log count during the specified time range is presented at the top of the *Threat Hunting* dashboard.

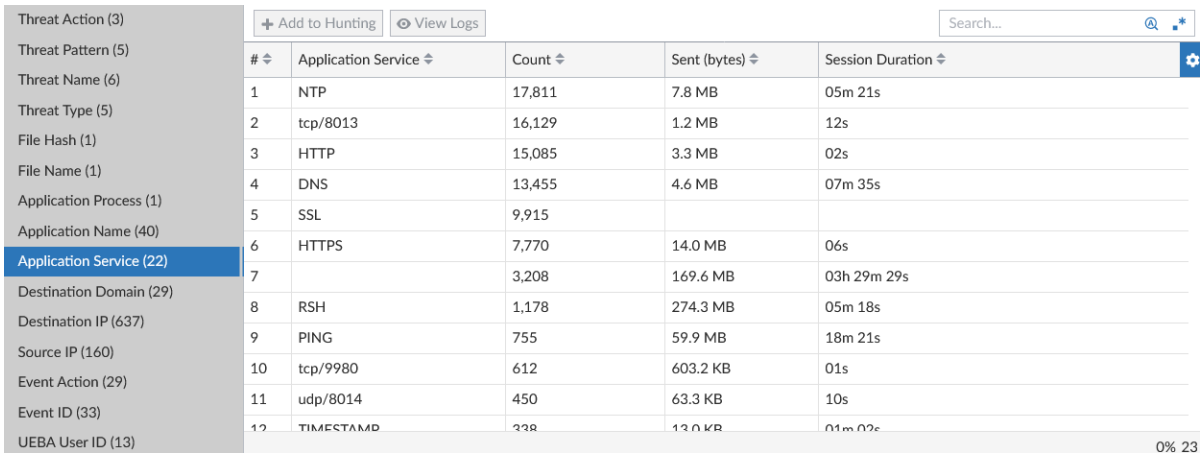
You can zoom in and out on the displayed time range by using your mouse's scroll wheel or by adjusting the timebar below the graph. You can adjust the time bar by dragging the start and stop bars on either side of the selected time range, or by clicking and dragging the entire time range to the left or right. Only logs displayed within the time period visible in the chart are shown in the SIEM log analytics table.



Using the SIEM log analytics table

The SIEM log analytics table contains a list of fields of interest in the left menu as well as the analytics table. You can select a field from the left menu to view corresponding data in the table. The table includes a row for the null value of that field, if applicable. For example, see the image below where *Application Service* is blank (null) in row 5.

Double-click an item in the table to open the log drilldown page which displays detailed log information. Alternatively, you can select an item in the table and click *View Logs*. A separate pane displays the logs in a table view. This feature includes the same functions as are available in other panes throughout *Log View*, including the search bar filter, time filter, columns settings, right-click filter, and more. See Viewing message details on page 152



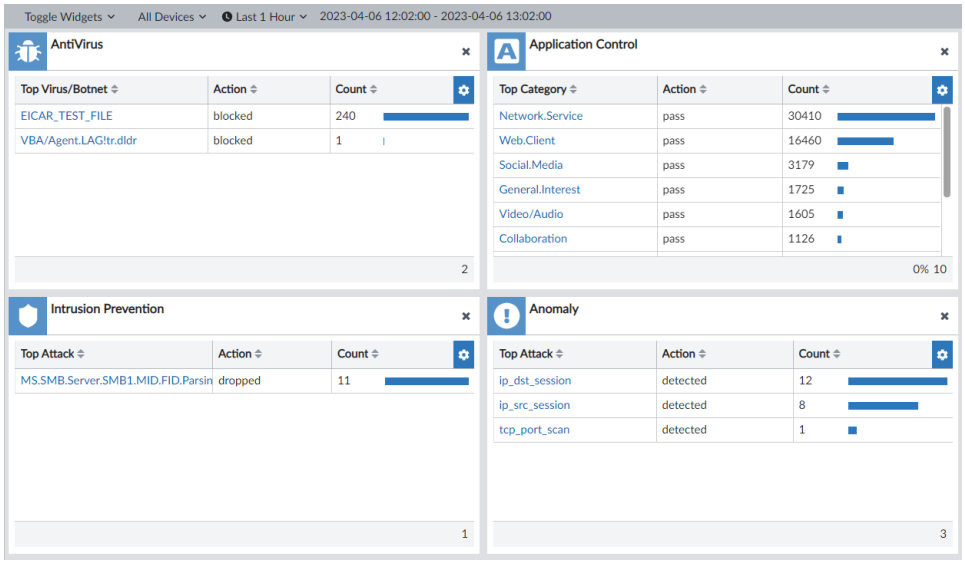
Monitoring all types of security and event logs from FortiGate devices

You can monitor all types of security and event logs from FortiGate devices in:

- *Log View > Logs > FortiGate > Security > Summary*
- *Log View > Logs > FortiGate > Event > Summary*

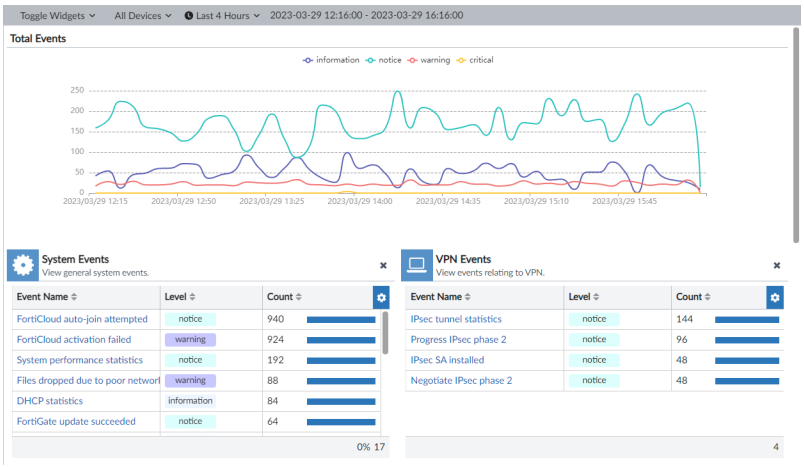
All widgets in these dashboards can be filtered by FortiGate device and timeframe in the toolbar. The widgets can be toggled on/off from the *Toggle Widgets* dropdown. By clicking an event name in the widget, you can open a list view of those logs filtered by the devices and timeframe you selected on the dashboard.

Security > Summary dashboard:



Event > Summary dashboard:

The summary dashboard for event logs includes a *Total Events* widget, which displays a line chart of the event logs by level. You can hover your cursor over the line chart to display a summary of the count and time at that point. This widget cannot be toggled off.



Viewing historical and real-time logs

By default, *Log View* displays historical logs. *Custom View* and *Chart Builder* are only available in historical log view.

To view real-time logs, in the log message list view toolbar, click *More* > *Real-time Log*.

To switch back to historical log view, click *More* > *Historical Log*.

Viewing raw and formatted logs

By default, *Log View* displays formatted logs. The log view you select affects available view options. You cannot customize columns when viewing raw logs.

To view raw logs, in the log message list view toolbar, click *More* > *Raw Log* .

To switch back to formatted log view, click *More* > *Formatted Log*.

For more information about FortiGate raw logs, see the *FortiGate Log Message Reference* in the Fortinet Document Library. For more information about raw logs of other devices, see the *Log Message Reference* for the platform type.

Custom views

Use *Custom View* to save the filter setting, device selection, and the time period you have specified.

Custom views can be set as public or private. Public custom views can be viewed by all administrators, whereas private custom views can only be viewed by the creator. Users cannot make changes to custom views created by other administrators but can right-click the view and select *Save As* to copy it.

To create a new custom view:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Log View*, and select a device type and log type.
3. In the content pane, customize the log view as needed by adding filters, specifying devices, and/or specifying a time period.
4. In the toolbar, click the *Create Custom View*.
5. Configure the following options, and click *OK* to save.

Option	Description
Name	Enter a name for the custom view.
Log Type	Displays the log type currently used to filter *Log View*. This will be used for the custom view.
Devices	Displays the devices currently used to filter *Log View*. These will be used for the custom view.
Time Period	Displays the time period used to filter the current content pane. This will be used for the custom view.
Privacy	Toggle to *Public* or *Private*. • **Public**: Others can view this custom view displayed in *Log View > Favorites*. • **Private**: Only you can see this custom view displayed in *Log View > Favorites*.

To edit a custom view:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to the *Log View > Favorites*, and select the custom view to be updated.
3. In the toolbar, edit the filter settings.
4. In the tree menu, select the menu icon next to your custom view, and select *Save*.

To rename a custom view:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to the *Log View > Favorites*.
3. Click the menu icon next to your custom view, and select *Rename*.
4. Change the name of the custom view, and click *OK*.

To change the visibility of a custom view:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to the *Log View > Favorites*.

3. Click the menu icon next to your custom view, and select *Share with Others*.
4. Toggle *Privacy* to *Public* or *Private*, and click *OK*.

Downloading log messages

You can download historical log messages to the management computer as a text or CSV file. You cannot download real-time log messages.

To download log messages:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Log View*, and select a device type and log type.
3. In the toolbar, click *More* > *Download*.
4. In the *Download Logs* dialog box, configure download options:
   - In the *Log file format* dropdown list, select *Text* or *CSV*.
   - To compress the downloaded file, select *Compress*.
   - To download only the current log message page, select *Current Page*. To download all the pages in the log message list, select *All Pages*.
5. Click *Download*.

By default, the maximum number of logs downloaded from each log download is `100000`. You can update this setting from the FortiAnalyzer CLI using the following command:

```
config system log settings
   set download-max-logs <integer>
end
```

Enter an integer integer between `100` and `5000000`.

Creating charts with Chart Builder



You can also create charts in *Reports* > *Report Definitions* > *Chart Library*. See Chart library on page 457

Log View includes a *Chart Builder* for you to build custom charts for each type of log messages.

To create charts with Chart Builder:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Log View*, and select a device type and log type.
3. In the toolbar, click *More* > *Chart Builder*.
4. In the *Chart Builder* pane, configure the chart and click *Save*.

Option	Description
Name	Enter a name for the chart.
Columns	Select which columns of data to include in the chart based on the log messages that are displayed on the *Log View* page.
Group By	Select how to group data in the chart.
Order By	Select how to order data in the chart.
Sort	Select a sort order for data in the chart.
Show Limit	Enter the number of rows to be shown per page.
Device	Displays the device(s) currently selected in *Log View*.
Time Frame	Displays the time frame currently selected in *Log View*.
Search	Displays the filters currently used in *Log View*.
Query	Displays the query being built.
Preview	Displays a preview of the chart.

5. Once a chart has been created, it can be inserted into a new report. See Reports Editor tab on page 440.

User and endpoint ID log fields

Log information about user and endpoint IDs is available in *Log View* and can be viewed by configuring these fields as displayed columns. See Customizing displayed columns on page 155.

UEBA User ID and *UEBA Endpoint ID* fields with values below 1024 are special cases which are tracked by FortiAnalyzer's UEBA. See the table below for information on what each value represents.

Value	Name	Description
1	EPEU_NOT_IMPL_DEVTYPE	EP and EU not implemented for this devtype.
2	EPEU_NOT_IMPL_LOGTYPE	EP and EU not implemented for this logtype.
3	EPEU_NO_ENOUGH_INFO	Not enough information to identify an EP or EU.
4	EPEU_CANNOT_GET_UID	Cannot get a UID range (max limit reached).
5	EPEU_INTERNAL_ERROR	Internal error (e.g. cannot allocate memory).
6	EPEU_HA_BACKUP_ASK_FAIL	Ask primary failed and could not recover.
7	EPEU_HA_REBUILD_THROTTLE	Prevent too many EP and EU requests during database rebuilding.
8	EPEU_CLIENT_ASK_FAIL	Ask server failed and could not recover.
10	EPEU_NOT_SUPPORT_LOGVER	Log version is not supported.

Value	Name	Description
100	EPEU_ID_LOCAL_HOST	Local host event, such as a local host event in FortiGate.
101	EPEU_ID_UNTRACK_IP	IP is public and related interface role is not LAN.
102	EPEU_ID_UNTRACK_LOGID	Log ID is not identified.
103	EPEU_ID_UNTRACK_TOOMANYIP	Too many IPs on one MAC.
104	EPEU_ID_UNTRACK_VPN_IP	Do not track VPN IP.



When a device has FortiClient installed and FortiAnalyzer is able to retrieve endpoint information, all interfaces of this device will belong to a single endpoint with the FCT-UID as the key. For devices without FortiClient that have multiple NICs, each interface appears as a separate endpoint.



The *User ID* and *UEBA User ID* fields are interchangeable and contain the same information.

The *Endpoint ID* and *UEBA Endpoint ID* fields are interchangeable and contain the same information.

FortiMail correlated logs

FortiMail logs support cross-log functionality. When viewing History, Event, Antivirus, or Email Filter logs from FortiMail, you can click the *Session ID* to see correlated logs. For example, when viewing the History logs from FortiMail, you can click the *Session ID* to view the correlated Event, Antivirus, and Email Filter logs in that session.



When VDOMs are used to divide FortiMail into two or more virtual units, cross-log searches display correlated log data from FortiMail's VDOMs, including those assigned to different ADOMs. VDOM results are included only when performing the cross-log search through FortiMail's History log view, but results include correlated data for all available log types (History, Events, Antivirus, and Email Filter).

To view correlated FortiMail logs:

1. Go to *Log View* > *Logs* > *Fortinet Logs* > *FortiMail* > *History*.
   History logs are used for this example, but the same functionality is available for the other FortiMail log types.
2. Click the *Session ID* for a History log.
   The *Correlated Logs for Session ID* pane displays.
3. Click the log type to view correlated logs for only that log type. Alternatively, click *All* to view correlated logs for all log types.
   The *All* tab includes the following options:

Wrap text	Enabled by default. When enabled, the information will be wrapped in columns according to their width for readability. This applies to columns such as *To*, *From*, *Message*, and *Subject*.
Export to PDF	Download a PDF of the correlated logs.

Log groups

You can group devices into log groups. You can view FortiView summaries, display logs, generate reports, or create event handlers for a log group. Log groups are virtual so they do not have SQL databases or occupy additional disk space.



A maximum of 100 devices can be included in a log group.

When you add a device with VDOMs to a log group, all VDOMs are automatically added.

To create a new log group:

1. Go to *Log View* > *Log Settings* > *Log Group*.
2. In the content pane toolbar, click *Create New*.
3. In the *Create New Log Group* pane, configure the following:

Option	Description
Name	Enter a name for the log group.
Description	Optionally, enter a description for the log group.
Device Type	Select the device type for the log group.
Devices	Select the devices to include in the log group, and then click *OK*.

4. Click *OK*.

Log browse

When a log file reaches its maximum size or a scheduled time, FortiAnalyzer rolls the active log file by renaming the file. The file name is in the form of `xlog.N.log`, where `x` is a letter indicating the log type, and `N` is a unique number corresponding to the time the first log entry was received. For information about setting the maximum file size and log rolling options, see Device logs on page 542.

Log Browse displays log files stored for both devices and the FortiAnalyzer itself, and you can log in the compressed phase of the log workflow.



In Collector mode, if you want to view the latest log messages, select the latest log file to display its log messages.

To view log files:

1. Go to *Log View* > *Logs* > *Log Browse*
2. Select a log file, and click *Display* to open the log file and display the log messages in formatted view. You can perform all the same actions as with the log message list. See Viewing message details on page 152.

Importing a log file

Imported log files can be useful when restoring data or loading log data for temporary use. For example, if you have older log files from a device, you can import these logs to the FortiAnalyzer unit so that you can generate reports containing older data.

Log files can also be imported into a different FortiAnalyzer unit. Before importing the log file you must add all devices included in the log file to the importing FortiAnalyzer.

To insert imported logs into the SQL database, the `config system sql start-time` and `rebuild-event-start-time` must be **older** than the date of the logs that are imported **and** the storage policy for analytic data (the *Keep Logs for Analytics* field) must also extend back far enough.

To set the SQL start time and rebuild event start time using CLI commands:

```
config system sql
   set start-time <start-time-and-date>
   set rebuild-event-start-time <start-time-and-date>
end
```

Where `<start-time-and-date>` is in the format `hh:mm yyyy/mm/dd`.

For more information, see the FortiAnalyzer CLI Reference on the Fortinet Document Library.

To import a log file:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Log View* > *Logs* > *Log Browse*, and click *Import*.
3. In the *Device* dropdown, select the device that the imported log file belongs to or select *[Taken From Imported File]* to read the device ID from the log file.
   If you select *[Taken From Imported File]*, the log file must contain a `device_id` field in its log messages.
4. Drag and drop the log file onto the dialog box, or click *Add Files* and locate the file to be imported on your local computer.
5. Click *OK*. A message appears, stating that the upload is beginning, but will be canceled if you leave the page.

6. Click *OK*. The upload time varies depending on the size of the file and the speed of the connection.
   After the log file is successfully uploaded, FortiAnalyzer inspects the file:
   - If the `device_id` field in the uploaded log file does not match the device, the import fails. Click *Return* to try again.
   - If you selected *[Taken From Imported File]* and the FortiAnalyzer unit's device list does not currently contain that device, an error is displayed stating *Invalid Device ID*.

Downloading a log file

You can download a log file to save it as a backup or to use outside the FortiAnalyzer unit. The download consists of either the entire log file or a partial log file, as selected by your current log view filter settings and, if downloading a raw file, the time frame specified.

To download a log file:

1. Go to *Log View* > *Logs* > *Log Browse* and select the log file that you want to download.
2. In the toolbar, click *Download*.
3. In the *Download Log File(s)* dialog, configure download options:
   - In the *Log file format* dropdown list, select *Native*, *Text*, or *CSV*.
   - If you want to compress the downloaded file, select *Compress*.
4. Click *Download*.

Deleting log files

To delete log files:

1. Go to *Log View* > *Logs* > *Log Browse*.
2. Select one or more files, and click *Delete*.
3. Click *OK* to confirm.

Log and file storage

Logs and files are stored on the FortiAnalyzer hard disks. Logs are also temporarily stored in the SQL database.

When a SIEM license is added, a SIEM database is created to store normalized Fabric logs.

When ADOMs are enabled, settings can be specified for each ADOM that apply only to the devices in it. When ADOMs are disabled, the settings apply to all managed devices.

Data policy and disk utilization settings for devices are collectively called log storage settings. Global log and file storage settings apply to all logs and files, regardless of log storage settings (see Automatically Delete settings in Configuring rolling and uploading of logs using the GUI on page 543). Both the global and log storage settings are always active.

The log rate and log volume per ADOM can be viewed through the CLI using the following commands:

```
diagnose fortilogd lograte-adom <name>
diagnose fortilogd logvol-adom <name>
```

Disk space allocation

On the FortiAnalyzer, the system reserves 5% to 20% of the disk space for system usage and unexpected quota overflow. The remaining 80% to 95% of the disk space is available for allocation to devices.

Reports are stored in the reserved space.

Total Available Disk Size	Reserved Disk Quota
Small Disk (up to 500GB)	The system reserves either 20% or 50GB of disk space, whichever is smaller.
Medium Disk (up to 1TB)	The system reserves either 15% or 100GB of disk space, whichever is smaller.
Large Disk (up to 3TB)	The system reserves either 10% or 200GB of disk space, whichever is smaller.
Very Large Disk (5TB and higher)	The system reserves either 5% or 300GB of disk space, whichever is smaller.

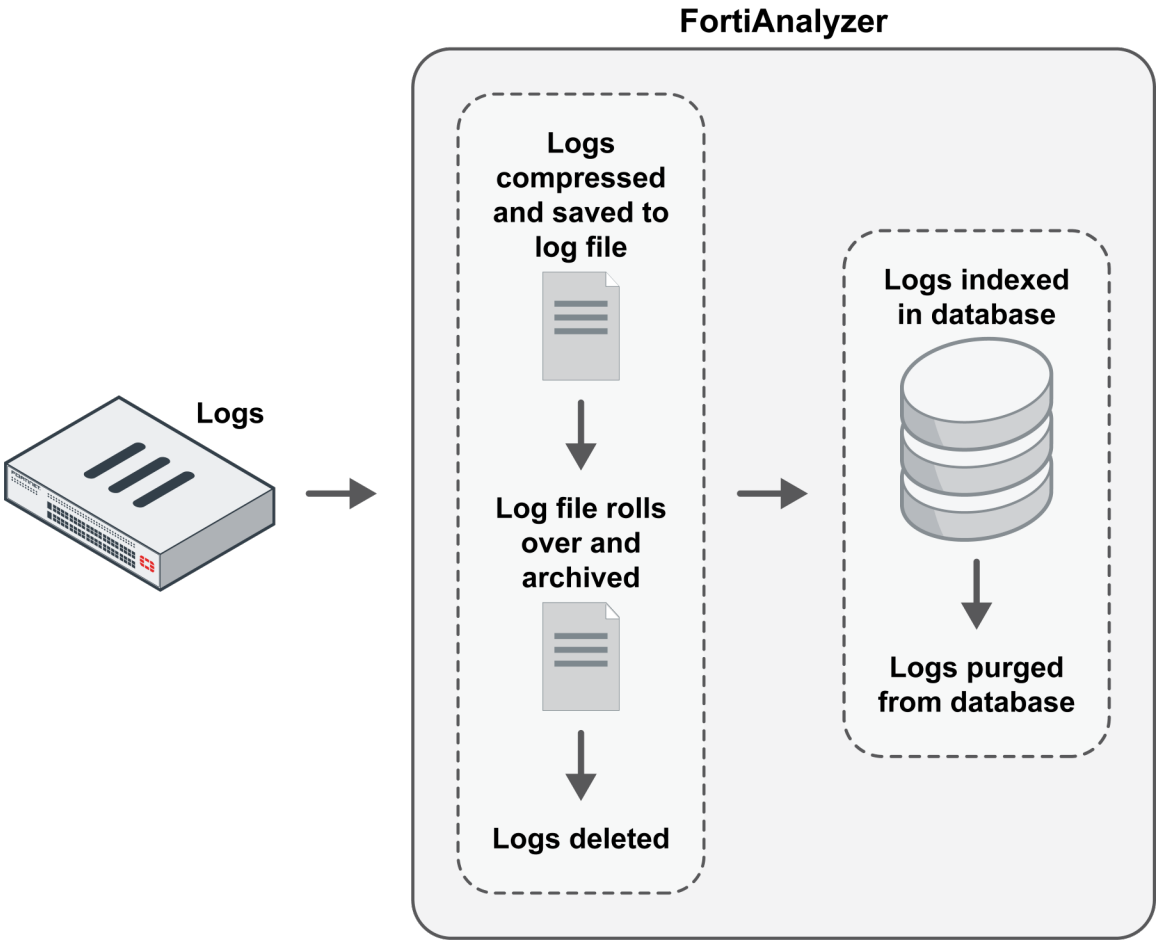
The RAID level you select determines the disk size and the reserved disk quota level. For example, a FortiAnalyzer 1000C with four 1TB disks configured in RAID 10 is considered a large disk, so 10%, or 100GB, of disk space is reserved.

Log and file workflow

When devices send logs to a FortiAnalyzer unit, the logs enter the following workflow automatically:

1. Compressed logs are received and saved in a log file on the FortiAnalyzer disks.
   When a log file reaches a specified size, FortiAnalyzer rolls it over and archives it, and creates a new log file to receive incoming logs. You can specify the size at which the log file rolls over. See Device logs on page 542.
2. Logs are indexed in the database to support analysis.
   You can specify how long to keep logs indexed using a data policy. See Log storage information on page 173.
3. Logs are purged from the database, but remain compressed in a log file on the FortiAnalyzer disks.

4. Logs are deleted from the FortiAnalyzer disks.
   You can specify how long to keep logs using a data policy. See Log storage information on page 173.



In the indexed phase, logs are indexed in the database for a specified length of time so they can be used for analysis. Indexed, or Analytics, logs are considered online, and details about them can be used viewed in the *FortiView*, *Log View*, and *Incidents & Events* panes. You can also generate reports about the logs in the *Reports* pane.

In the compressed phase, logs are compressed and archived in FortiAnalyzer disks for a specified length of time for the purpose of retention. Compressed, or Archived, logs are considered offline, and their details cannot be immediately viewed or used to generate reports.

The following table summarizes the differences between indexed and compressed log phases:

Log Phase	Location	Immediate Analytic Support
Indexed	Compressed in log file and indexed in database	Yes. Logs are available for analytic use in *FortiView*, *Incidents & Events*, and *Reports*.
Compressed	Compressed in log file	No.

Automatic deletion

Logs and files are automatically deleted from the FortiAnalyzer unit according to the following settings:

- Global automatic file deletion

  The *Automatically Delete* settings in *Device Log Settings* specify when to delete the oldest Archive logs, quarantined files, reports, and archived files from disks, regardless of the log storage settings. For more information, see Configuring rolling and uploading of logs using the GUI on page 543.
- Data policy

  Data policies specify how long to store Analytics and Archive logs for each device. When the specified length of time expires, Archive logs for the device are automatically deleted from the FortiAnalyzer device's disks.
- Disk utilization

  Disk utilization settings delete the oldest Archive logs for each device when the allotted disk space is filled. The allotted disk space is defined by the log storage settings. Alerts warn you when the disk space usage reaches a configured percentage.



When log trimming is performed by disk quota enforcement, tables from both the SQL and SIEM databases are considered together, and the oldest table, identified by the timestamp of logs inside, is trimmed. The process repeats until the quota is within the defined threshold. The SIEM database is always partitioned by day, whereas the size of the SQL database partition can be configured in FortiAnalyzer settings. For information on SIEM logs, see Types of logs collected for each device on page 146.

All deletion policies are active on the FortiAnalyzer unit at all times, and you should carefully configure each policy. For example, if the disk fullness policy for a device hits its threshold before the global automatic file deletion policy for the FortiAnalyzer unit, Archive logs for the affected device are automatically deleted. Conversely, if the global automatic file deletion policy hits its threshold first, the oldest Archive logs on the FortiAnalyzer unit are automatically deleted regardless of the log storage settings associated with the device.

The following table summarizes the automatic deletion polices:

Policy	Scope	Trigger
Global automatic file deletion	All logs, files, and reports on the system	When the specified length of time expires, old files are automatically deleted. This policy applies to all files in the system regardless of the data policy settings associated with devices.
Data policy	Logs for the device with which the data policy is associated	When the specified length of retention time expires, old Archive logs for the device are deleted. This policy affects only Archive logs for the device with which the data policy is associated.
Disk utilization	Logs for the device with which the log storage settings are associated	When the specified threshold is reached for the allotted amount of disk space for the device, the oldest Archive logs are deleted for the device. This policy affects only Archive logs for the device with which the log storage settings are associated.

Logs for deleted devices

When you delete one or more devices from FortiAnalyzer, the raw log files and archive packets are deleted, and the action is recorded in the local event log. However, the logs that have been inserted into the SQL database are not deleted from the SQL database. As a result, logs for the deleted devices might display in the *Log View* and *FortiView* panes, and any reports based on the logs might include results.

The following are ways you can remove logs from the SQL database for deleted devices.

- Rebuild the SQL database for the ADOM to which deleted devices belonged or rebuild the entire SQL database.
- Configure the log storage policy. When the deleted device logs are older than the *Keep Logs for Analytics* setting, they are deleted. Also, when analytic logs exceed their disk quota, the SQL database is trimmed starting with the oldest database tables. For more information, see Configuring log storage policy on page 175.
- Configure global automatic file deletion settings in *System Settings > Advanced > Device Log Settings > Automatically Delete*. When the deleted device logs are older than the configured setting, they are deleted. For more information, see Configuring rolling and uploading of logs using the GUI on page 543.



System Settings > Advanced > Device Log Settings > Automatically Delete configures global settings that override other log storage settings and apply to all ADOMs.

Log storage information

To view log storage information and to configure log storage policies, go to *System Settings > ADOMs*.

If ADOMs are enabled, you can view and configure the data policies and disk usage for each ADOM.

The log storage policy affects only the logs and databases of the devices associated with the log storage policy. Reports are not affected. See Disk space allocation on page 170.

The following options are available:

Option	Description
Create New	Create a new ADOM. This option is only available when ADOMs are enabled.
Edit	Edit the selected ADOM's log storage policy.
View Storage Info	View the storage usage, analystics policy, and archive policy.
Delete	Delete the ADOM. You can only delete empty ADOMs.
Enter ADOM	If ADOMs are enabled, enter the ADOM.
Enable ADOM	Enable the ADOM feature. For more information, see Administrative Domains (ADOMs) on page 498.
Disable ADOM	Disable the ADOM. This option is only available when ADOMs are enabled.
Collapse Devices / Expand Devices	Collapse or expand the list of devices in the table view.

Option	Description
Refresh	Refresh the page.
Search	Enter a search term to search the list. You can toggle match case and regular expression for the search, as needed.

The following columns are available in the table view:

Column	Description
Name	The name of the ADOM. ADOMs are listed in groups: *Security Fabric*, *FortiGates*, and *Other Device Types*.
ADOM Type	The type of ADOM.
Allocated Storage	The total storage allocated for the ADOM.
Devices	The devices currently in the ADOM. You can expand the list of devices in the row and click to *View Details* in a separate pane.
Comments	Comments included in the description of the ADOM.
Time Zone	The time zone set for the ADOM.
Analytics (Actual/Config Days)	The age, in days, of the oldest Analytics logs (Actual Days), and the number of days Analytics logs will be kept according to the data policy (Config Days).
Archive (Actual/Config Days)	The age, in days, of the oldest Archive logs (Actual Days) and the number of days Archive logs will be kept according to the data policy (Config Days).
Analytics Usage (Used/Max)	How much disk space Analytics logs have used, and the maximum disk space allotted for them.
Archive Usage (Used/Max)	How much disk space Archive logs have used and the maximum disk space allotted for them.

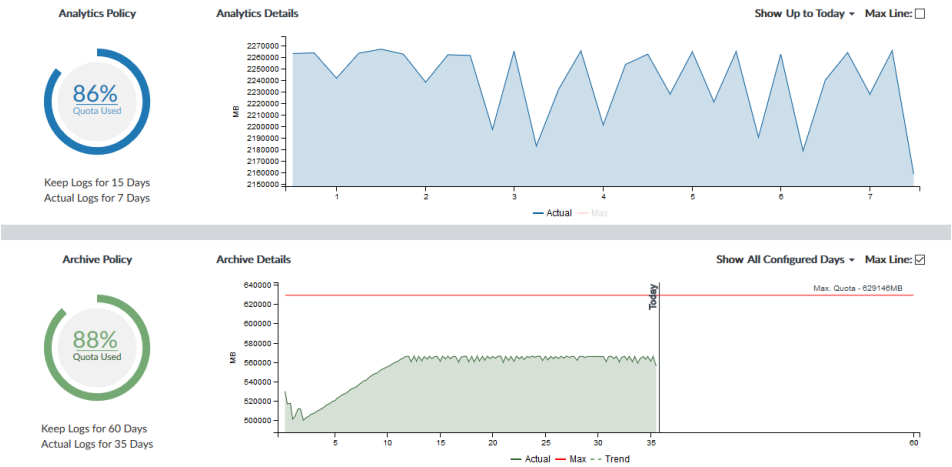
Storage information

To view log storage policy and statistics, go to *System Settings* > *ADOMs*, select an ADOM, and click *View Storage Info*.

There are two sections for the logs storage information:

- Analytics logs
- Archive logs

Each section includes a policy diagram to visualize the quota used and a details graph to view the usage over time.



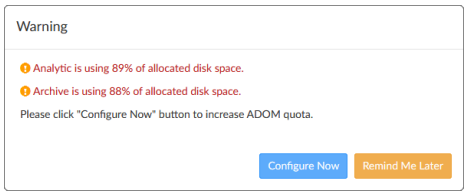
The policy diagrams show the percentage of the disk space quota that is used. Mouse over the diagram to view the used, free, and total allotted disk space. The configured length of time that logs are stored is also shown.

The graphs show the amount disk space used over time. Enable *Max Line* to show a line on the graph for the total space allotted. Mouse over the graph to view the used and available disk space at that date and time. Click the graph to view a breakdown of the disk space usage by device.

Analytics Storage Statistics - Last 15 Days

Device Name	Analytics Usage		Average Log Rate (logs/sec)	Peak Log Rate (logs/sec)
FGT37D0000000000	743.1 GB	38.35%	1087.14	1615.27
FG800C0000000000	221.4 MB	0.01%	4.24	35.58
Weixixixi_WiFi	3.1 GB	0.16%	4.48	32.80
FG3K2D0000000000	51.3 GB	2.65%	77.29	781.74
FG1K2D0000000000	716.4 GB	36.97%	1048.14	2376.82
FG100D0000000000	423.8 GB	21.87%	619.99	1726.02

When the used quota approaches 100 percent, a warning message displays when accessing the *Storage Statistics* pane.



Click *Configure Now* to open the *Edit Log Storage Policy* dialog where you can adjust log storage policies to prevent running out of allocated space (see Configuring log storage policy on page 175), or click *Remind Me Later* to resolve the issue another time.

Configuring log storage policy

The log storage policy affects the logs and databases of the devices associated with the log storage policy.

If you change log storage settings, the new date ranges affect Analytics and Archive logs currently in the FortiAnalyzer device. Depending on the date change, Analytics logs might be purged from the database, Archive logs might be added back to the database, and Archive logs outside the date range might be deleted.

To configure log storage settings:

1. Go to *System Settings* > *ADOMs*
2. Right-click or select an ADOM, and then select *Edit*. Alternatively, you can double-click the ADOM.
   The *Edit ADOM* pane displays. Go to the log storage policy sections at the bottom of the pane.
3. Configure the following settings, then click *OK*.

Data Policy		
	Keep Logs for Analytics	Specify how long to keep Analytics logs. If set to 0, the Analytics logs will be kept for unlimited days.
	Keep Logs for Archive	Specify how long to keep Archive logs. Make sure your setting meets your organization's regulatory requirements. If set to 0, the Archive logs will be deleted after rolling. Note that the rolled log files will be kept until the next retention policy check, which occurs every twelve hours.
Disk Utilization		
	Allocated	Specify the amount of disk space allotted. See also Disk space allocation on page 170.
	Analytics: Archive	Specify the disk space ratio between Analytics and Archive logs. Analytics logs require more space than Archive logs. Select *Modify* to change the setting.
	Alert and Delete When Usage Reaches	Specify the percentage of allotted disk space usage that will trigger an alert messages and start automatically deleting logs. The oldest Archive log files or Analytics database tables are deleted first.

Configuring log rate receiving limits

You can manually configure log rate limits for devices in an ADOM or for specific logging devices. By default, no rate limit is enforced.

When setting the log rate limit to manual in the CLI, you can specify a default device log rate and a per device/ADOM rate. Both a default and per device limit can be set simultaneously, in which case the per device limit will take priority for configured devices.

You can view configured logging rates in the CLI using the following command: `diagnose test application fortilogd 17` and `diagnose test application oftpd 17`.

To configure the default device log rate limit:

In the FortiAnalyzer CLI, enter the following commands:

```
config system log ratelimit
   set mode manual
      set device-ratelimit-default <set the rate limit, for example 2000>
   end
```

To configure the log rate limit per device:

In the FortiAnalyzer CLI, enter the following commands:

```
config system log ratelimit
   set mode manual
      config ratelimits
         edit <rate limit profile, for example "1">
            set filter-type devid
            set filter <device serial number>
            set ratelimit <set the rate limit, for example 3000>
         next
      end
```

To configure the log rate limit per ADOM:

In the FortiAnalyzer CLI, enter the following commands:

```
config system log ratelimit
   set mode manual
      config ratelimits
         edit <rate limit profile, for example "1">
            set filter-type adom
            set filter <ADOM name>
            set ratelimit <set the rate limit, for example 3000>
         next
      end
```

To disable the log rate limit:

In the FortiAnalyzer CLI, enter the following commands:

```
config system log ratelimit
   set mode disable
end
```

FortiGate log buffer

Reliable logging from FortiGate to FortiAnalyzer prevents lost logs when the connection between FortiGate and FortiAnalyzer is disrupted. If connection is lost between the FortiAnalyzer and FortiGate device, logs will be cached and sent to FortiAnalyzer once the connection resumes. For more information, see *FortiAnalyzer log caching* in the FortiGate / FortiOS Administration Guide.

FortiGates with an SSD disk also have a configurable log buffer. When the connection to FortiAnalyzer is unreachable, the FortiGate is able to buffer logs on disk if the memory log buffer is full. The logs queued on the disk buffer can be sent successfully once the connection to FortiAnalyzer is restored. For more information, see *Log buffer on FortiGates with an SSD disk* in the FortiGate / FortiOS Administration Guide.

Fabric View

The *Fabric View* module enables you to view assets and create subnets. The *Fabric View* tab is available in version 6.0 ADOMs and later.

This section contains the following topics:

- Asset Identity Center on page 178
- Subnets on page 191

Asset Identity Center

The *Fabric View > Asset Identity Center* is the central location for security analysts to view endpoint and user information to make sure they are compliant. Endpoints are important assets in a network as they are the main entry points in a cybersecurity breach.

The asset information is useful for the following:

- **Incident response**: check assets that are infected or vulnerable as part of your SOC analysis and incident response process.
- **Compliance**: identify unknown and non-compliant users and endpoints.

The *Asset Identity Center* is also useful for user and endpoint mapping. Some users might use multiple endpoints in the network, endpoints might use multiple different interfaces to connect, network interfaces might have multiple IP addresses, and so on. A map of users and their endpoints gives you better visibility when you analyze logs, events, and incidents. This also helps with your reporting.

This topic includes the following information:

- Asset Summary on page 178
- Identity Summary on page 180
- Asset List on page 181
- Identity List on page 185
- OT View on page 189
- Configuring endpoint and end user data sources on page 190

Asset Summary

The *Asset* dashboard in *Fabric View > Asset Identity Center > Summary* includes widgets for analysis of endpoints.

You can click *Toggle Widgets* to select which widgets are visible on the dashboard, and refine the list of endpoints included in the widgets by using the dashboard filter. You can also apply filters from some widgets.

By default, the following widgets are displayed in the dashboard:

Widget	Description
OT/IoT Vulnerability	Displays OT/IoT vulnerabilities detected on assets by severity.
Top 10 OT/IoT Vulnerability	Displays the top 10 OT/IoT vulnerabilities detected on assets.
Top 10 Asset with OT/IoT Vulnerability	Displays the top 10 assets with OT/IoT vulnerabilities detected.
OT/IoT Mitigated Vulnerability (60 Days)	Displays the top assets with mitigated OT/IoT vulnerabilties in the past 60 days. Click the settings icon to sort in ascending or descending order, and to filter by top 5, top 10, or top 20.
Detection Method	Displays endpoint detections by method.
Detection Source	Displays a breakdown of the asset center data sources. Click the settings icon to sort in ascending or descending order, and to filter by top 5, top 10, or top 20.
Identification/Unidentified Asset	Displays the number of detected endpoint assets that are identified and unidentified.
Hardware/OS Distribution	Displays endpoint hardware operating system distribution. Click the settings icon to adjust the view, and to filter by top 5, top 10, or top 20.
Discovery Timeline	Displays an asset discovery timeline. Click the settings icon to adjust the time filter or disable/enable the refresh interval.
Identified Active Asset	Displays identified asset visibility over the past 24 hours to 52 weeks.
Assets By Location	Displays identified assets by location. Click the settings icon to adjust the view, and to filter by top 5, top 10, or top 20.
Identified Activity Timeline	Displays a first seen, last update, and last seen identified asset activity timeline. Click the settings icon to adjust the time filter or disable/enable the refresh interval.
Changes Timeline	Displays an asset changes timeline. Click the settings icon to adjust the time filter or disable/enable the refresh interval.
Unidentifed Active Asset	Displays unidentified asset visibility over the past 24 hours to 52 weeks.
Unidentifed Activity Timeline	Displays a first seen, last update, and last seen unidentified asset activity timeline. Click the settings icon to adjust the time filter or disable/enable the refresh interval.

To use the dashboard filter:

1. Go to *Fabric View* > *Asset Identity Center* > *Summary*, and select *Asset*.
2. Click the settings icon in the top-right corner of the pane.
   The following options are displayed.

Tags Filter	Select *Include* or *Exclude*, and select a tag from the *Tags Field* dropdown. You can click the add icon next to the tags field to add additional items to be included or excluded. Click the trash icon to remove a field.
Hardware\OS	Select a hardware/OS type from the dropdown to only display endpoints with the matching hardware or operating system type.
Detect Method	Select a detection method in the dropdown to only display endpoints that were detected by the specified method.
Device Filter	Select devices to filter by or select *All*.

3. Click *OK*.

Identity Summary

The *Identity* dashboard in *Fabric View* > *Asset Identity Center* > *Summary* includes widgets for analysis of end users.

You can click *Toggle Widgets* to select which widgets are visible on the dashboard, and refine the list of endpoints included in the widgets by using the dashboard filter. You can also apply filters from some widgets.

By default, the following widgets are displayed in the dashboard:

Top Users	Displays asset user data. Click the settings icon to sort in ascending or descending order, and to filter by top 5, top 10, or top 20.
Number of Active Users	Displays user visibility data over the past 24 hours to 52 weeks.
User Groups	Displays user groups. Click the settings icon to sort in ascending or descending order, and to filter by top 5, top 10, or top 20.
User's Location	Displays user numbers by location. Click the settings icon to sort in ascending or descending order, and to filter by top 5, top 10, or top 20.
User's Manager	Displays user numbers by manager. Click the settings icon to sort in ascending or descending order, and to filter by top 5, top 10, or top 20.
Discovery Timeline	Displays the user discovery timeline. Click the settings icon to adjust the time filter or disable/enable the refresh interval.

Activity Timeline	Displays the user activity timeline. Click the settings icon to adjust the time filter or disable/enable the refresh interval.
Endpoint Tag Distribution	Displays the distribution of endpoint tags. Click the settings icon to sort in ascending or descending order, and to filter by top 5, top 10, or top 20.

To use the dashboard filter:

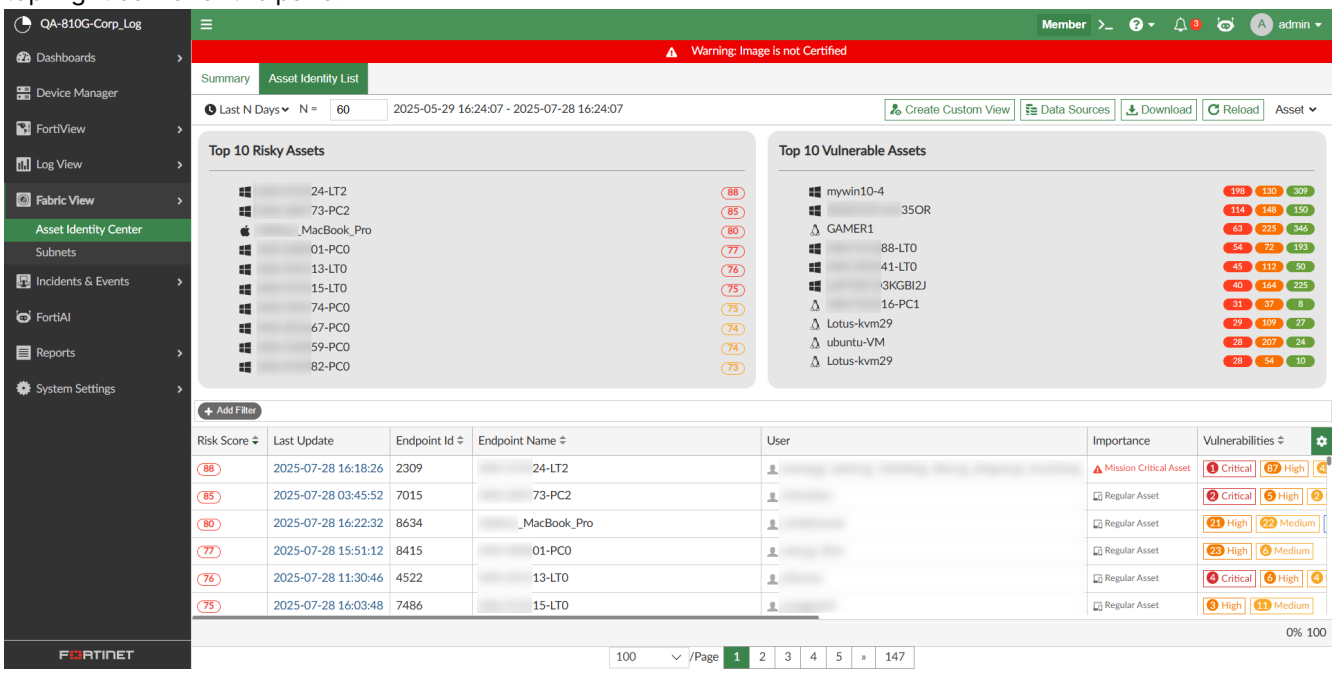
1. Go to *Fabric View* > *Asset Identity Center* > *Summary* and select *Identity*.
2. Click the settings icon in the top-right corner of the pane.
   The following options are displayed.

Device Filter	Select devices to filter by or select *All*.
User Group	Select user groups to filter by or select *All*.

3. Click *OK*.

Asset List

To open the Asset List, go to *Fabric View* > *Asset Identity Center* > *Asset Identity List* and select *Asset* in the top-right corner of the pane.



There are two widgets at the top of the pane:

- *Top 10 Risky Assets*: displays the top 10 risky assets based on risk score.
- *Top 10 Vulnerable Assets*: displays the top 10 most vulnerable assets based on number of vulnerabilities.

The table below the widgets lists all endpoints and users from relevant logs. While the widgets provide this information at a glance, you can also sort the table by *Risk Score* or *Vulnerabilities* to see which endpoints and users have the highest risk or number of vulnerabilities.



If there is no FortiClient in your installation, then endpoint and end user information is limited.

- Endpoints are detected based on MAC address and displayed by IP address instead of host name.
- User related information might not be available.
- Detailed information such as OS version, avatar, and social ID information are not available.

When applicable to your environment, endpoint information from VMware logs will also be included in the Asset and Identity tables. This requires a third-party vSphere connector. For more information, see Connector actions on page 364.

The following default columns are available in the table. You can click the settings icon above the table to add or remove columns according to your needs.

Column	Description
Endpoint Name	Endpoint host name.
User	The name of the user. Click the name to view the corresponding user information in the *Identity Center* pane.
Importance	The importance for the asset. You can update the importance for an asset by double-clicking the asset and, in the endpoint details pane, selecting the importance: • *Regular Asset* • *Important Asset* • *Critical Asset* • *Mission Critical Asset*
Risk Score	The risk score for the asset based on its related alerts and vulnerabilities.
Vulnerabilities	The number of vulnerabilities for critical, high, medium, and low vulnerabilities. Endpoint vulnerability information is retrieved when a playbook runs the *Get Vulnerabilities* action using the FortiClient EMS connector. See Automation on page 362. Click a record in the *Vulnerabilities* column to display the *View Vulnerabilities* pane. This pane includes a table view with the following columns: • *Vulnerability ID* • *Type* • *Severity* • *Reference* • *Description* Click a hyperlink in the *Reference* column to view the vulnerability details in the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD).

Column	Description
OT/IoT Vulnerabilities	The number of OT/IoT vulnerabilities. Click the number to view the details. To view the details of the vulnerability, you must have a valid license for the OT/IoT service (Industrial Security Service).
Tags	Tags are used to group and identify assets to assist SOC analysts with incident management and prioritization. Tags can be defined by FortiClient EMS or when creating subnets and subnet groups in FortiAnalyzer. FortiClient EMS tags are determined based on the *Classification Tag* assigned in FortiClient EMS. Tags are displayed in the Asset Center when a playbook retrieves information about that endpoint using the *Get Endpoints* task available with a FortiClient EMS connector. See Connector actions on page 364. Subnet tags are configurable when creating new subnets and subnet groups in FortiAnalyzer. See Subnets on page 191.
IP Address	IP address the endpoint is connected to. A user might be connected to multiple endpoints.
MAC Address	Endpoint MAC address.
Hardware / OS	OS name and version.
Last Update	The date and time the log was updated. Click the time to view the latest logs in a separate tab for *Log View*.

To filter the asset list:

1. In the toolbar, select a time period from the dropdown.
   This will filter the widgets and the table view.
2. In the search bar above the table, click *Add Filter*.
   These filters are only applied to the table view.
3. Select the field, and then select the value.
4. Click *Apply*.

To create a custom view:

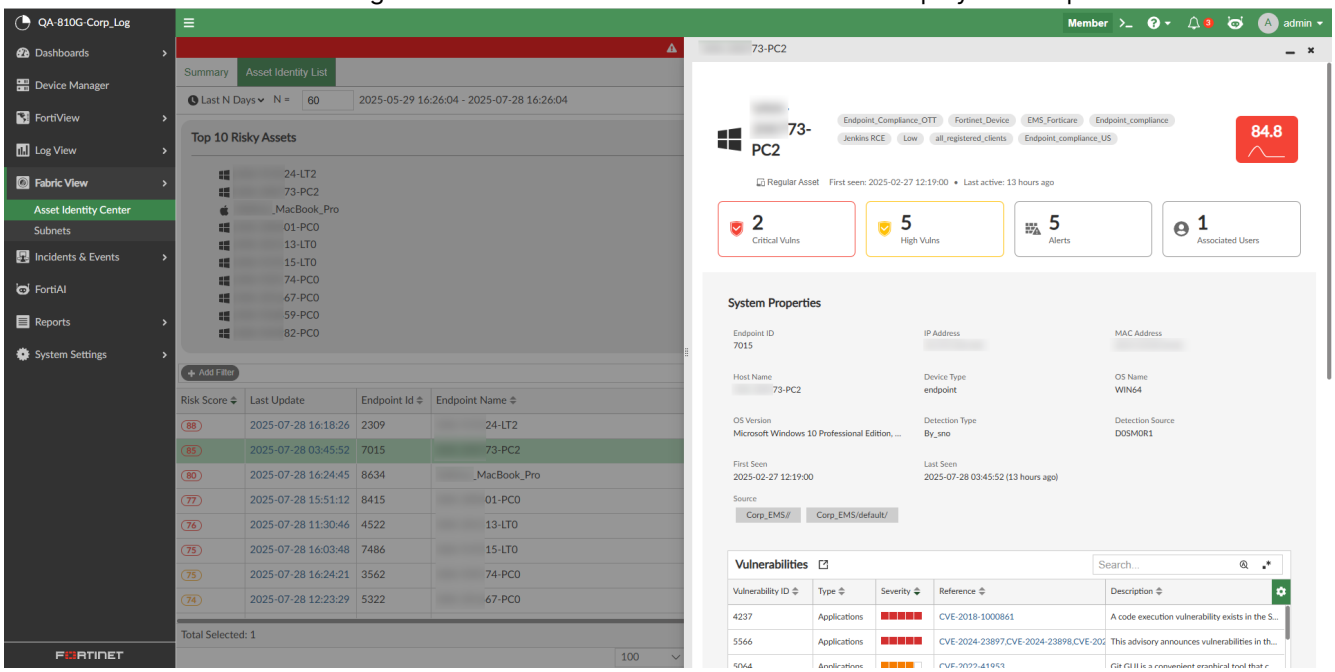
1. Filter the asset list using the time period dropdown and the search bar.
2. Click *Create Custom View*.
   The *Create Custom View* dialog displays. The *Time Period* and *Search* are populated according to the currently set filters.
3. In the *Name* field, enter a name for the custom view.
4. Toggle *Privacy* to *Private* or *Public*.
5. Click *OK* to save the custom view.
   The view is saved under *Fabric View* > *Asset Identity Center* > *Custom View*. After the custom view is created, you can rename, change the privacy setting, duplicate, or delete the custom view by clicking the settings icon next to the custom view name.

To download the table view as a CSV file:

1. Filter the table view using the time period dropdown and the search bar.
2. Click *Download*.
   The *Export to CSV* dialog displays.
3. In the *File Name* field, enter a file name.
4. For *Options*, select one of the following:
   - *Export all columns*: export all columns, regardless of the columns that are enabled for the table in the GUI.
   - *Export customized columns only*: export only the columns that have been enabled in the GUI. Click the settings icon above the table view to enable/disable columns.
5. Click *OK*.
6. Select a location for the file, and click *Save*.

Endpoint details pane

Click an asset in one of the widgets or double-click a record in the table to display the endpoint details.



The endpoint details pane is named according to the endpoint name. It includes the following information:

- Endpoint name
- Risk score
- Importance
- First seen / last active
- Number of critical vulnerabilities, high vulnerabilities, alerts, and associated users
- System properties, including endpoint ID, IP address, MAC address, host name, and more
- Vulnerabilities, if applicable
- Related alerts, if applicable

- User information, if applicable; this includes risk score, source FortiGate, location, associated endpoints, and more

You can update the asset importance and investigate alerts from the endpoint details pane.

To update the asset importance:

1. In the endpoint details pane, click the current asset importance.
2. Select one of the following from the list of asset importance:
   - *Regular Asset*
   - *Important Asset*
   - *Critical Asset*
   - *Mission Critical Asset*

To investigate vulnerabilities from the endpoint details pane:

1. In the endpoint details pane, go to the *Vulnerabilities* table.
   By default, the table includes the following columns:
   - *Vulnerability ID*
   - *Type*
   - *Severity*
   - *Reference*
   - *Description*
2. Click a hyperlink in the *Reference* column to view the vulnerability details in the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD).

To investigate related alerts from the endpoint details pane:

1. In the endpoint details pane, go to the *Related Alerts* table.
   By default, the table includes the following columns:
   - *Severity*
   - *Last Occurred*
   - *Event*

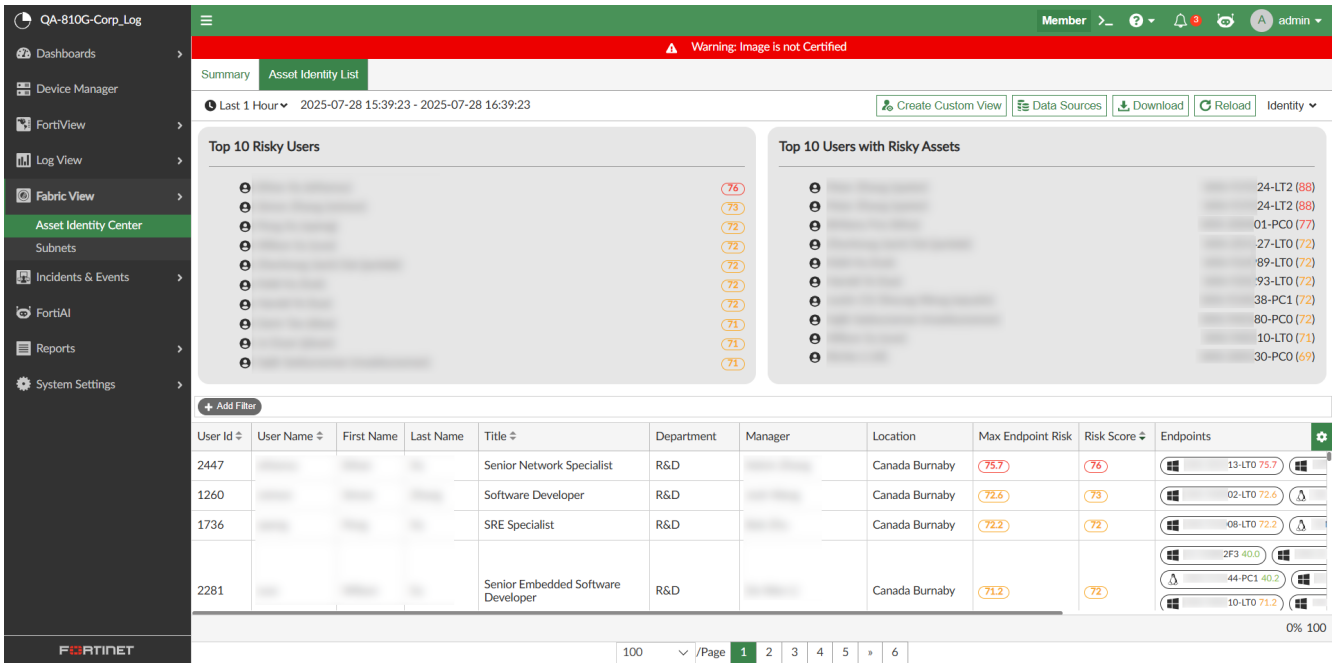
   You can sort the columns and use the search bar to find a specific alert.

   Click an alert in the table to display a pane with more information about the event.

   The event details pane is named after the event. For more information, see *Event details pane* in Explorer on page 218.

Identity List

To open the Identity List, go to *Fabric View* > *Asset Identity Center* > *Asset Identity List* and select *Identity* in the top-right corner of the pane.



There are two widgets at the top of the pane:

- *Top 10 Risky Users*: displays the top 10 risky users based on risk score.
- *Top 10 Users with Risky Assets*: displays the top 10 user and associated endpoint risk scores.

The table below the widgets lists all users from relevant logs.



End user information is limited if there is no FortiClient in your installation.

- Endpoints are detected based on MAC address and displayed by IP address instead of host name.
- User related information might not be available.
- Detailed information such as OS version, avatar, and social ID information are not available.

When applicable to your environment, endpoint information from VMware logs will also be included in the Asset and Identity tables. This requires a third-party vSphere connector. For more information, see Connector actions on page 364.

The following default columns are available in the table. You can click the settings icon above the table to add or remove columns according to your needs.

Column	Description
User Name	The name of the user.
First Name	The user's first name.
Last Name	The user's last name.
Title	The user's title.
Department	The user's department.

Column	Description
Manager	The user's manager.
Location	The user's location.
Endpoints	Endpoint host name, IP address, or MAC address. A user may be connected to multiple endpoints. Click the endpoint to display the corresponding endpoint details pane. For more information, see the endpoint details pane in Asset List on page 181.
Max Endpoint Risk	The highest risk score for an associated endpoint.
Risk Score	The risk score for the user based on their related alerts and vulnerabilities.
First Seen	The first seen time according to the logs.
Last Seen	The last seen time according to the logs.

To filter the identity list:

1. In the toolbar, select a time period from the dropdown.
   This will filter the widgets and the table view.
2. In the search bar above the table, click *Add Filter*.
   These filters are only applied to the table view.
3. Select the field, and then select the value.
4. Click *Apply*.

To create a custom view:

1. Filter the identity list using the time period dropdown and the search bar.
2. Click *Create Custom View*.
   The *Create Custom View* dialog displays. The *Time Period* and *Search* are populated according to the currently set filters.
3. In the *Name* field, enter a name for the custom view.
4. Toggle *Privacy* to *Private* or *Public*.
5. Click *OK* to save the custom view.
   The view is saved under *Fabric View* > *Asset Identity Center* > *Custom View*. After the custom view is created, you can rename, change the privacy setting, duplicate, or delete the custom view by clicking the settings icon next to the custom view name.

To download the table view as a CSV file:

1. Filter the table view using the time period dropdown and the search bar.
2. Click *Download*.
   The *Export to CSV* dialog displays.
3. In the *File Name* field, enter a file name.
4. For *Options*, select one of the following:

- *Export all columns*: export all columns, regardless of the columns that are enabled for the table in the GUI.
- *Export customized columns only*: export only the columns that have been enabled in the GUI. Click the settings icon above the table view to enable/disable columns.

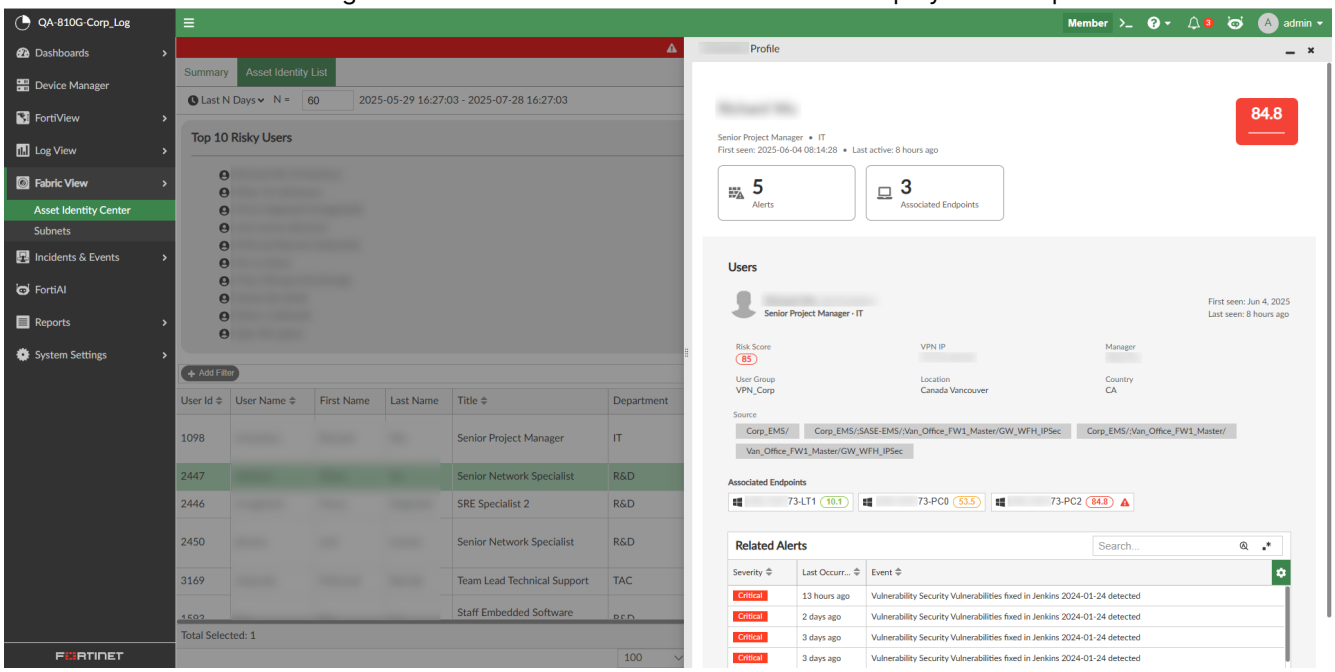
5. Click *OK*.
6. Select a location for the file, and click *Save*.

To configure the display settings in the Social column:

1. Go to *Log View* > *Tools icon* > *User Display Preferences*.
2. Select the order preference tab you want to configure.
   Tabs include *Name*, *Picture*, *Email*, *Phone Number*, and *Social*.
3. Rearrange the order preference as per your needs by drag-and-dropping an entry. For names, pictures, emails, and phone numbers, only the top entry will appear in the identity pop-up window.
4. User information can be disabled by moving the *Show* toggle to the *Off* position in the respective tabs.

User profile pane

Click a user in one of the widgets or double-click a record in the table to display the user profile details.



The user profile pane is named according to the user name. It includes the following information:

- First name / last name
- Risk score
- First seen / last active
- Number of alerts and associated endpoints
- User information, if applicable; this includes risk score, source FortiGate, location, associated endpoints, and more

Click the associated endpoint to open the endpoint details pane. For more information about this pane, see *Endpoint details pane* in Asset List on page 181.

- Related alerts, if applicable

  Click an alert to review the event details. The event details pane is named after the event. For more information, see *Event details pane* in Explorer on page 218.

OT View

The *Fabric View* > *Asset Identity Center* > *Asset Identity List* > *OT View* displays the relationships between endpoints, allowing you to analyze the structure. While in *OT View*, you can click and drag to pan the view of the OT information. View controls are also available in the top right of the pane to zoom in, zoom out, and fit view.

FortiOS devices must use version 7.4 or higher to send OT information to FortiAnalyzer.

The following actions are available in the toolbar:

Option	Description
Select Devices	Select the devices include in the OT view.
Group By	Select how the devices should be grouped in the OT view.
Lock/Unlock View	Lock or unlock the endpoints. After unlocking, the device can move only in parallel at the level.
Hide/Show Connection	Hide or show the connection cables between devices.
Search	Search for an endpoint in the OT view.
Custom View	Save the current view as a custom view.

To create a custom view:

1. In the toolbar, click the column settings icon, and select the columns you want to display.
2. Click *Custom View*. The *Save as New Custom View* dialog is displayed.
3. In the *Name* field, enter a name for the custom view, and click *OK*. The view is saved under *Fabric View* > *Asset Identity Center* > *Custom View*.

To change the visibility of a custom view:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. In *Fabric View* > *Asset Identity Center* > *Custom View*, select the menu icon next to your custom view, and select *Share with Others*.
   You can also *Rename*, *Save As* (clone), or *Delete* the custom view.
3. Set the *Privacy* field to *On: Public* or *Off: Private*, and click *OK*.

Configuring endpoint and end user data sources

You can configure the data sources used in the *Fabric View* > *Asset Identity Center* > *Asset Identity List* to specify which sources are used to identify endpoints and end users. Data source modification is configured per ADOM.

The following data sources are configurable in FortiAnalyzer:

FortiGate Log	By default, the log identification of endpoints and end users is enabled for all devices and subnets. You can create rules to specify which FortiGate devices and which subnets are excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.
FortiClient Log	By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which FortiClient devices are excluded in the data source. Set the status to *OFF* to disable identification of endpoints and end users from the specified devices or all devices.
FortiMail Log	By default, the log identification of endpoints and end users is disabled for all devices. You can create rules to specify which FortiMail devices and domains are included in the data source.
FortiWeb Log	By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which FortiWeb devices and which subnets are excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.
FortiNAC Log	By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which FortiNAC devices and which subnets can be excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.
EMS Connector	By default, the log identification of endpoints and end users is disabled for all EMS connectors. You can create rules to specify which EMS connectors can be included in the data source.



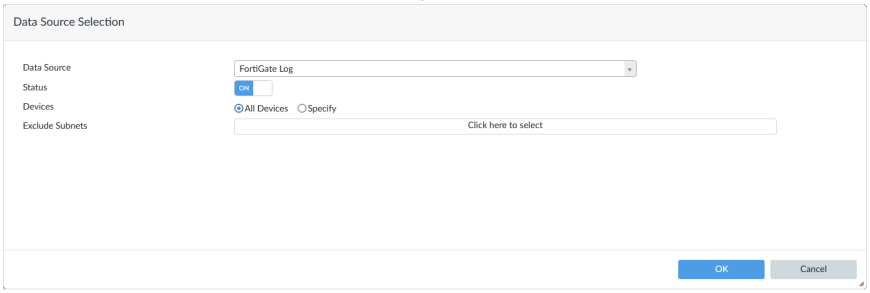
Rules created for individual devices have priority over those created for "all devices".

You can configure the same data source multiple times when the device or connector is unique. When a conflict arises, you will see a message indicating the data source for that device already exists, and you will have the option to override the existing data source.

To configure data sources:

1. Go to *Fabric View* > *Asset Identity Center* > *Asset Identity List*, and click *More* > *Data Sources*.
   The *Data Source Selection* dialog opens. You can create, edit, and delete data sources in this dialog.

2. To create a new data source, click *Create New*.
The *Data Source Selection* wizard opens.



3. Configure your data source. Different fields appear for different data source types:

Data Source	Select the data source that you want to configure. Data sources include *FortiGate Log*, *FortiClient Log*, *FortiMail Log*, *FortiWeb Log*, *FortiNAC Log*, and *EMS Connector*. Depending on your selection, different configurable fields will appear below.
Status	Enable or disable the data source by setting the *Status* to *ON* or *OFF*. When the data source is disabled, FortiAnalyzer will not identify endpoints and end users in this ADOM from the devices, domains, or connectors configured in the data source.
Devices	*Devices* is only available when the data source is *FortiGate Log*, *FortiClient Log*, *FortiMail Log*, *FortiWeb Log*, or *FortiNAC Log*. Select *All Devices* or *Specify* to select individual devices.
Exclude Subnets	*Exclude Subnets* is only available when the data source is *FortiGate Log*, *FortiWeb Log*, or *FortiNAC Log*. Select subnets to be excluded from the data source selection. You can create subnets in *Fabric View* > *Fabric* > *Subnets*. See Subnets on page 191.
Include Domains	*Include Domains* is only available when the data source is *FortiMail Log*. Enter domains to be included in the data source selection.
Connectors	*Connectors* is only available when the data source is *EMS Connector*. Select an EMS connector to be included in the data source selection. See Configuring security fabric connectors on page 372.

4. Click *OK* to save changes to the data source.
Once created, you can edit and delete the data sources from the *Data Source Selection* dialog.

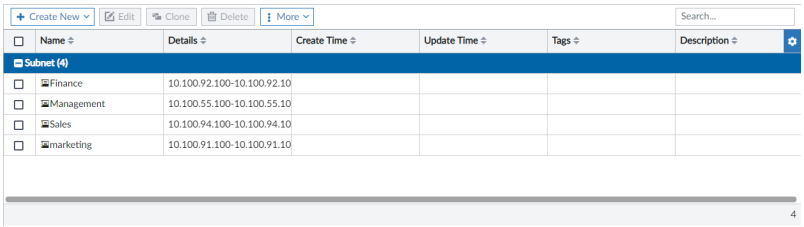
Subnets

In *Fabric View* > *Subnets*, you can define subnet lists which can be added to subnet groups.

Subnet lists and groups can be used to create include and exclude lists in event handlers and reports.

You can filter for subnet lists and subnet groups in *Log View*. See Filtering messages on page 156.

Creating, updating, or deleting subnets will generate local event logs.



Subnets includes the following options in the toolbar and right-click menu:

Create New	Create a new subnet or subnet group.
Edit	Edit the selected subnet or subnet group.
Clone	Clone the selected subnet or subnet group.
Delete	Delete the selected subnet(s) or subnet group(s).
Import	Import a subnet or subnet group.
Export	Export a subnet or subnet group in either a text or zipped format.

Subnet filtering for event handlers is supported in FortiGate, FortiWeb, FortiMail, and Fabric ADOMs.

A maximum of 10,000 subnet objects can be created.

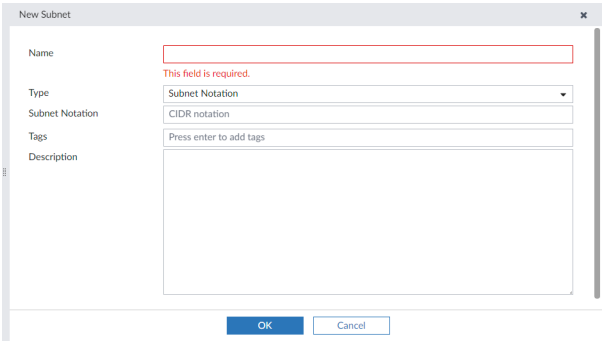
- Creating a subnet list on page 192
- Creating a subnet group on page 193
- Assigning subnet filters to event handlers on page 194

Creating a subnet list

To create a new subnet:

1. Go to *Fabric View* > *Subnets*.

2. From the *Create New* dropdown, select *Subnet*.
   The *New Subnet* wizard opens.

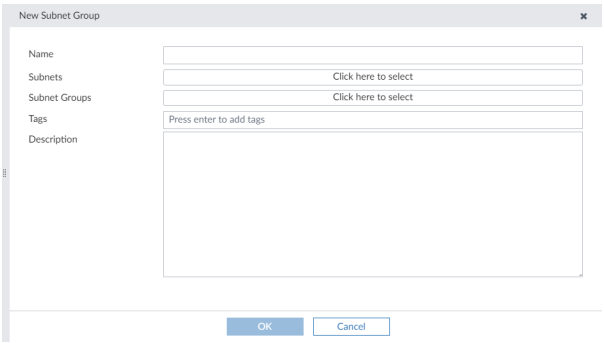


3. Enter a name for the subnet.
4. Select a *Subnet type* and configure the corresponding information.
   Subnet types include:
   - *Subnet Notation*
   - *IP Range*
   - *Batch Add*
5. Enter any *Tags* to be associated with this subnet. Tags are displayed in Assets when the endpoint IP falls within the subnet. SeeAsset List on page 181.
6. Optionally, enter a description.
7. Click *OK*.
   Once a subnet has been created, it can be edited, cloned, or deleted by highlighting it and selecting the corresponding action in *Subnet List* toolbar.

Creating a subnet group

To create a subnet group:

1. Go to *Fabric View* > *Connectors* > *Subnets*.
2. From the *Create New* dropdown, select *Subnet Group*.
   The *New Subnet Group* pane opens.



3. Enter a name for the subnet group.
4. Select the subnet entries to be included in the group and select *OK* in the pop-up window.
5. Optionally, select one or more existing subnet groups to be nested in the new subnet group as a member.

6. Enter any *Tags* to be associated with this subnet group. Tags are displayed in *Assets* when the endpoint IP falls within the subnets that are a part of this group. SeeAsset List on page 181.
7. Optionally, enter a description.
8. Click *OK*.

   Once a subnet group has been created, it can be edited, cloned, or deleted by highlighting it and selecting the corresponding action in *Subnet List* toolbar.

Assigning subnet filters to event handlers

You can streamline SOC processes by defining a subnet allowlist/blocklist for event handlers. These addresses can be linked to any event handler through a data selector, enabling or preventing the selected subnets from triggering an event. Creating a subnet allowlist/blocklist in data selectors eliminates the need to specify common networks in every event handler.

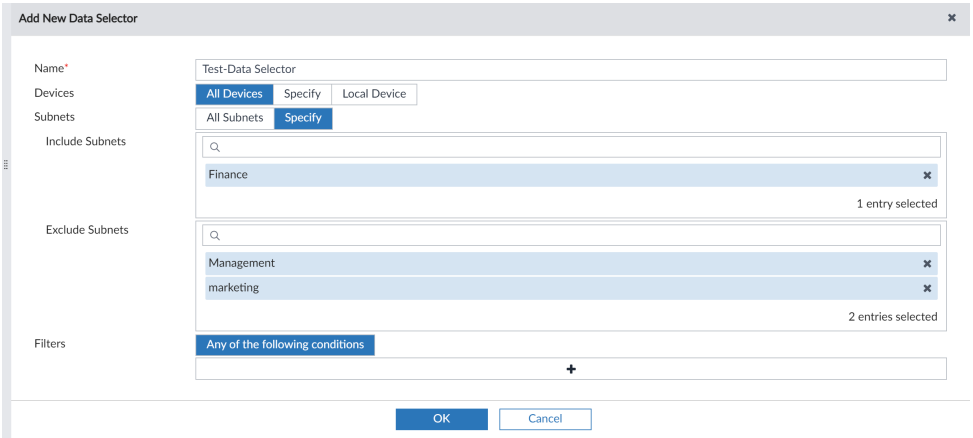
To include or exclude subnets in an event handler:

1. Go to *Incidents & Events* > *Event Handlers* > *Data Selectors*.
2. Click *Create New*.

   The *Add New Data Selector* pane displays.

   You can also *Clone* or *Edit* an existing data selector to include or exclude subnets.
3. In the *Subnets* field, select *Specify*.

   The *Include Subnets* and *Exclude Subnets* fields display.
4. Select the subnets to include or exclude in event handlers as part of the data selector.
5. Configure the other options for the data selector, and click *OK*. For more information, see Creating data selectors on page 316.



6. Go to *Incidents & Events* > *Handlers* > *Event Handlers*.
7. Select an event handler to add the data selector to, and click *Edit*.

   The *Edit Basic Event Handler* pane displays.

   You can also create a custom event handler to add the data selector to.
8. From the *Data Selector* dropdown, select the data selector configured to include or exclude the selected subnets.

9. Configure the other options for the event handler, and click *OK*. For more information, see Creating a custom event handler on page 298.
10. Add the data selector to other event handlers, as needed.



If a conflict arises between the exclude and include lists, the exclude list will take priority.



Subnet filters work when either SRCIP or DSTIP hit the subnet, meaning SRCIPs and DSTIPs share the same subnet filters.

Fortinet Security Fabric

FortiAnalyzer can recognize a Security Fabric group of devices and display all units in the group on the *Device Manager* pane. See Adding a Security Fabric group on page 196. FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from the units in a Security Fabric group as if the logs are from a single device. You can also view the logging topology of all units in the Security Fabric group for additional visibility. See Displaying Security Fabric topology on page 197.

FortiAnalyzer provides dynamic data and metadata exchange with the Security Fabric and uses the data in FortiView and Reports for additional visibility. A default report template lets you monitor new users, devices, applications, vulnerabilities, threats and so on from the Security Fabric.

A set of dashboard widgets lets you review audit scores for a FortiGate Security Fabric group with recommended best practices and historical audit scores and trends.

If FortiClient is installed on endpoints for endpoint control with FortiGate, you can use the endpoint telemetry data collected by the Security Fabric agent to display user profile photos in reports and FortiView.

Adding a Security Fabric group

Before you can add a Security Fabric group to FortiAnalyzer, you need to create the Security Fabric group in FortiGate.

Fortinet recommends using a dedicated Super_User administrator account on the FortiGate for FortiAnalyzer access. This ensures that associated log messages are identified as originating from FortiAnalyzer activity. This dedicated Super_User administrator account only needs *Read Only* access to *System Configuration*; all other access can be set to *None*.

Once a Security Fabric group is added in FortiAnalyzer, it can be used to filter other panes, such as *Log View* and *FortiView*. You can select the Security Fabric or individual devices in the fabric from the *Device* filter in those panes.

To add a Security Fabric group:

1. Go to *Device Manager* > *Unauthorized Devices*.
2. Select all the devices corresponding to the Security Fabric group created in FortiGate.
3. Authenticate the Security Fabric group by clicking the *Warning* icon (yellow triangle) beside the corresponding FortiGate root.



4. Enter the *Authentication Credentials*. The authentication credentials are the ones you specified in FortiGate. Once the FortiGate root has been authenticated, the *Warning* icon will disappear.

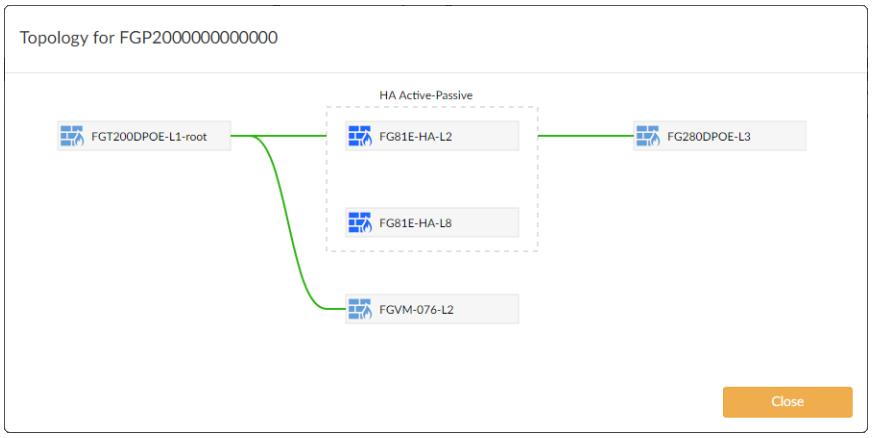
5. After authentication, it takes a few minutes for FortiAnalyzer to automatically populate the devices under the FortiGate root which creates the Security Fabric group.

Displaying Security Fabric topology

For Security Fabric devices, you can display the Security Fabric topology.

To display the Security Fabric topology:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager*.
3. Right-click a Security Fabric device and select *Fabric Topology*.
   A pop-up window displays the Security Fabric topology for that device.
   If you selected *Fabric Topology* by right-clicking a device within the Security Fabric group, the device is highlighted in the topology. If you selected *Fabric Topology* by right-clicking the name of the Security Fabric group, no device is highlighted in the topology.



Security Fabric traffic log to UTM log correlation

FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions/bandwidth together with its UTM threats. Within a single FortiGate, the correlation is performed by grouping logs with the same session IDs, source and destination IP addresses, and source and destination ports.

In a Cooperative Security Fabric (CSF), the traffic log is generated by the ingress FortiGate, while UTM inspection (and subsequent logs) can occur on any of the FortiGates. This means that the traffic logs did not have UTM related log fields, as they would on a single FortiGate. Different CSF members also have different session IDs, and NAT can hide or change the original source and destination IP addresses. Consequently, without a proper UTM reference, the FortiAnalyzer will fail to report UTM threats associated with the traffic.

This feature adds extensions to traffic and UTM logs so that they can be correlated across different FortiGates within the same security fabric. It creates a UTM reference across CSF members and generates the missing UTM related log fields in the traffic logs as if the UTM was inspected on a single FortiGate.

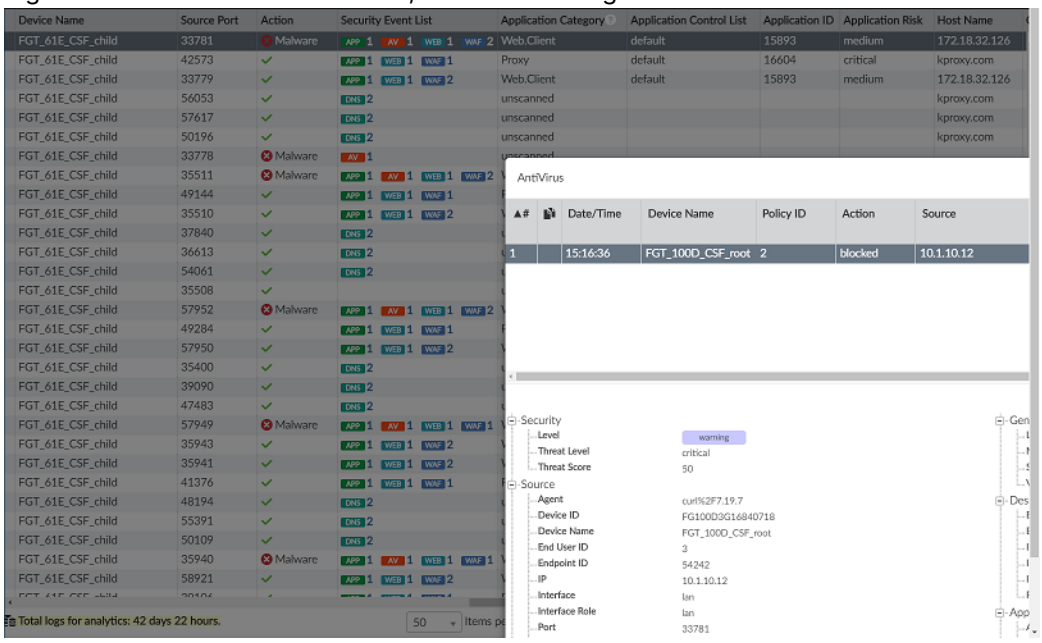
NAT translation is also considered when searching sources and destinations in both traffic and UTM logs. The FortiGate will generate a special traffic log to indicate the NAT IP addresses to the FortiAnalyzer within the CSF.

Traffic logs to DNS and SSH UTM references are also implement - the DNS and SSH counts in Log View can now be clicked on to open the related DNS and SSH UTM log. IPS logs in the UTM reference are processed for both their sources and destinations in the same order, and in the reverse order as the traffic log. The FortiGate log version indicator is expanded and used to make a correct search for related IPS logs for a traffic log.

This feature requires no special configuration. The FortiAnalyzer will check the traffic and UTM logs for all FortiGates that are in the same CSF cluster and create the UTM references between them.

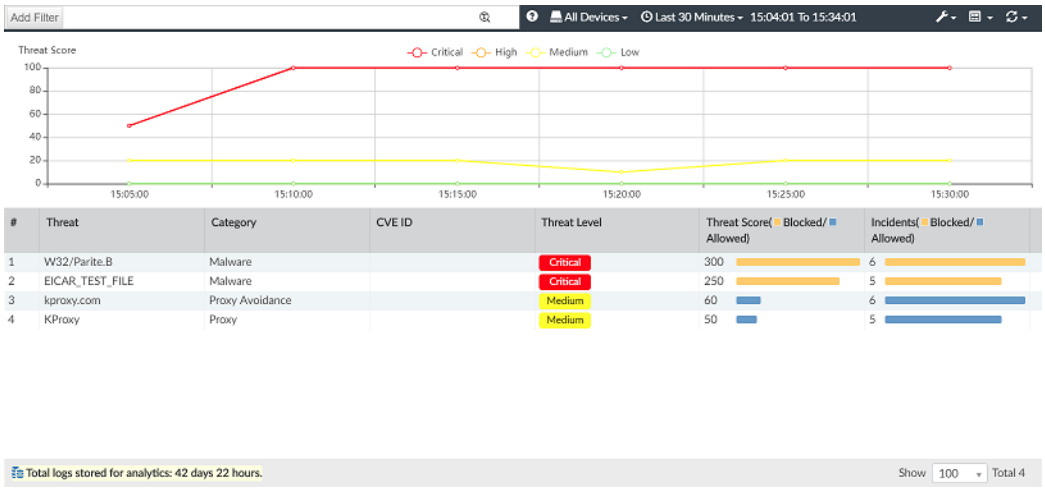
To view the logs:

1. On the FortiAnalyzer, go to *Log View* > *FortiGate* > *Traffic*.
   The UTM security event list, showing all related UTM events that can happen in another CSF member, is shown.
2. Click the count beside a UTM event to open the related UTM event log window. In this example, the traffic log is from the CSF child FortiGate, and the UTM log is from the CSF root FortiGate.

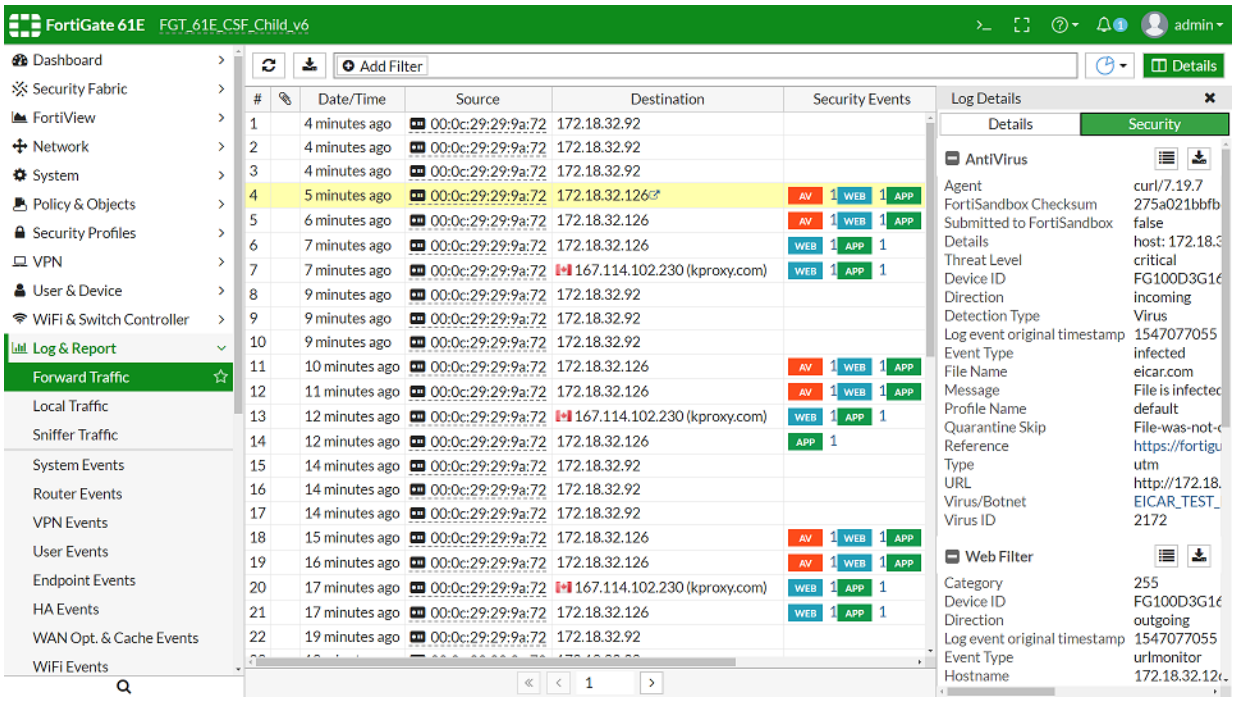


Like other UTM logs, newly added DNS and SSH UTM references can also be shown in the FortiAnalyzer Log View. Clicking the count next to the DNS or SSH event opens the respective UTM log.

3. Go to *FortiView* > *Threats* > *Top Threats*. All threats detected by any CSF member are shown.



4. The created UTM reference is also transparent to the FortiGate when it gets its logs from the FortiAnalyzer. On the FortiGate, the traffic log shows UTM events and referred UTM logs from other CSF members, even though the FortiGate does not generate those UTM log fields in its traffic log. In this example, the CSF child FortiGate shows the referred UTM logs from the CSF root FortiGate.



Security Fabric ADOMs

All Fortinet devices included in a Security Fabric can be placed into a Security Fabric ADOM, allowing for fast data processing and log correlation. Fabric ADOMs enable combined results to be presented in the *Device Manager*, *Log View*, *FortiView*, *Incidents & Events* and *Reports* panes.

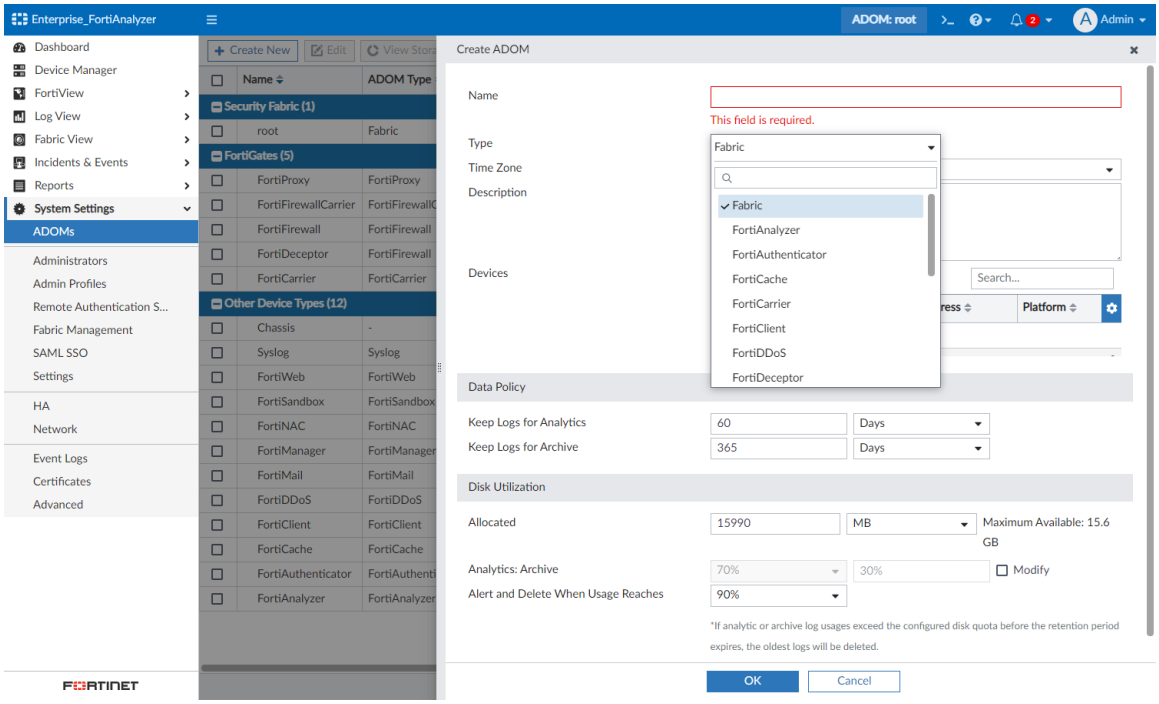
In a Fabric ADOM:

- *Device Manager*: View and add all Fortinet devices in the Security Fabric to the Fabric ADOM, including FortiGate, FortiSandbox, FortiMail, FortiDDoS, and FortiClient EMS.
- *Log View*: View logs from all Security Fabric devices.
- *FortiView*: FortiDDoS and FortiClient EMS widgets are available.
- *Incidents & Events*: Predefined event handlers for FortiGate, FortiSandbox, FortiMail, and FortiWeb ADOMs are available, and triggered events are displayed for all device types.
- *Reports*: View predefined reports, templates, datasets, and charts for all device types. Charts from all device types can be inserted into a single report.

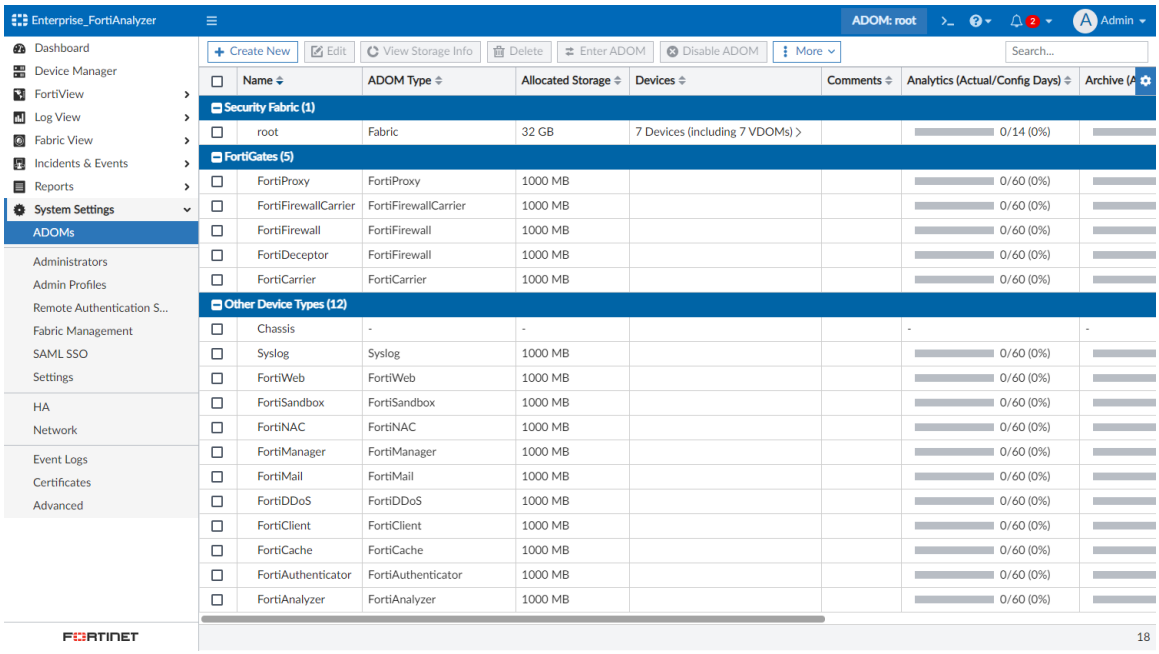
Creating a Security Fabric ADOM

To create a Fabric ADOM:

1. In FortiAnalyzer, go to *System Settings* > *ADOMs*.
2. Select *Create New*.
3. Configure the settings for the new Fabric ADOM and select *Fabric* as the type.
   See Creating ADOMs on page 505 for more information on the individual settings.



4. Select *OK* to create the ADOM.
   The Fabric ADOM is listed under the *Security Fabric* section of *All ADOMs*.



Migrating to a Fabric ADOM

You can change an existing non-Fabric ADOM to a Fabric ADOM using the FortiAnalyzer CLI.

1. In the FortiAnalyzer CLI, enter the following commands:
   ```
   execute migrate fabric <fabric name>
   ```
   A note is displayed informing you of the number of ADOMs that will be affected, and once begun, a summary is displayed and the system will reboot.

Enabling SAML authentication in a Security Fabric

When FortiGate is configured as a SAML SSO IdP in a Security Fabric, FortiAnalyzer can register itself to FortiGate as an SAML service provider, allowing for simplified configuration of SAML authentication.

When FortiAnalyzer is configured as a Fabric SP, a default SSO administrator is automatically created for each Security Fabric. When a user logs in through Fabric SSO, the Fabric IdP provides the user's profile name. If FortiAnalyzer has a profile with a matching name, the profile is assigned to the user. Otherwise, the profile of the SSO administrator is assigned to the user by default.

Before configuring FortiAnalyzer as a Fabric SP, *Security Fabric Connection* and *FortiAnalyzer Logging* must be configured on the root FortiGate.



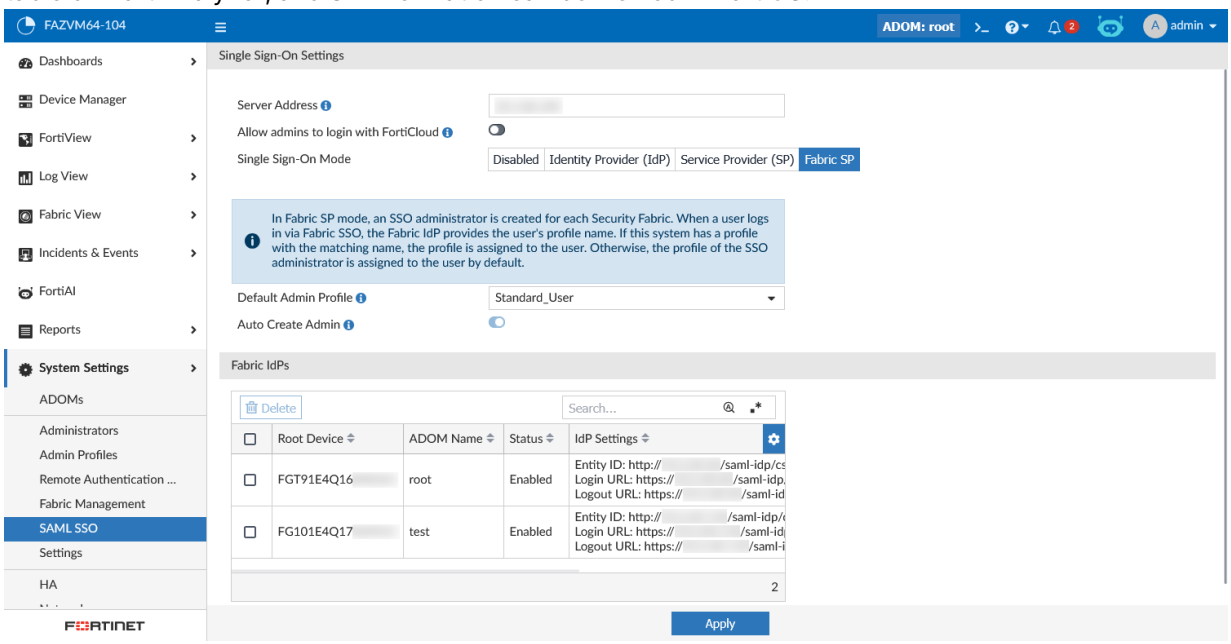
When ADOMs are enabled, SSO users can only access the ADOM that includes the root FortiGate.

To configure FortiAnalyzer as a Fabric SP:

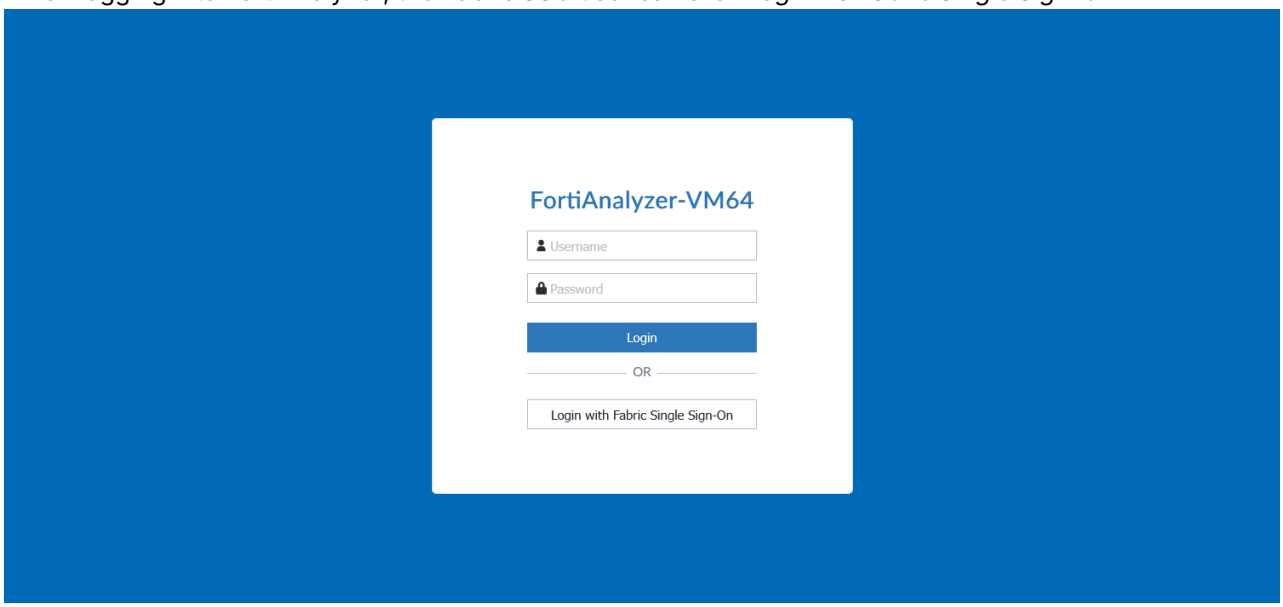
1. Before configuring FortiAnalyzer as a Fabric SP, configure the following on the root FortiGate:
   a. To enable *FortiAnalyzer Logging* on the root FortiGate, see Logging to FortiAnalyzer in the FortiGate / FortiOS Administration Guide.
   b. To configure a *Security Fabric Connection* on the root FortiGate, see Configuring the root FortiGate and downstream FortiGates in the FortiGate / FortiOS Administration Guide.
   c. To enable *SAML Single Sign-on* on the root FortiGate, see Configuring the root FortiGate as the IdP in the FortiGate / FortiOS Administration Guide.
2. In the FortiAnalyzer GUI, enable the *Fabric SP Single Sign-On Mode*.
   a. Go to *System Settings* > *SAML SSO*.
   b. Select *Fabric SP* as the *Single Sign-On Mode*.
   c. Enter the address of the FortiAnalyzer SP.
   d. Select a *Default Admin Profile*.

      The *Auto Create Admin* setting is enabled by default for Fabric SP. SSO admins will be created automatically if they do not exist. The admins can be found in the FortiAnalyzer GUI under *System Settings* > *Administrators* with the name "`CSF_SSO_FG<serial number>`".
   e. Click *Apply*.

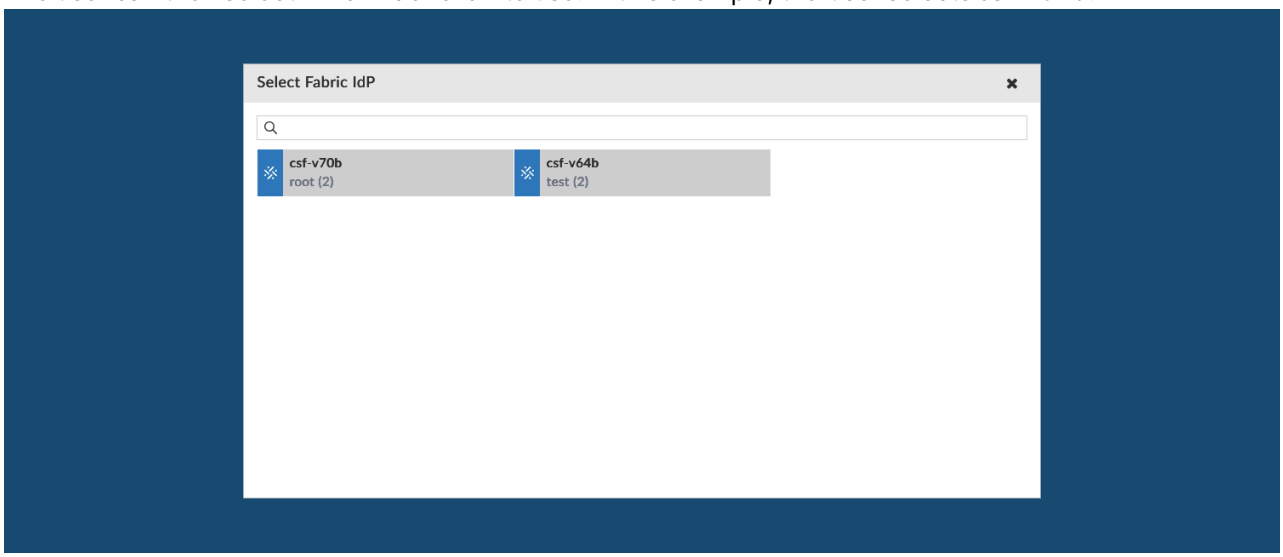
      The FortiAnalyzer will automatically detect the IdP FortiGate and register itself as a SAML SP. This process may take up to ten minutes. Once completed, IdP information is displayed in the Fabric IdPs table on FortiAnalyzer, and SP information can be viewed in FortiOS.



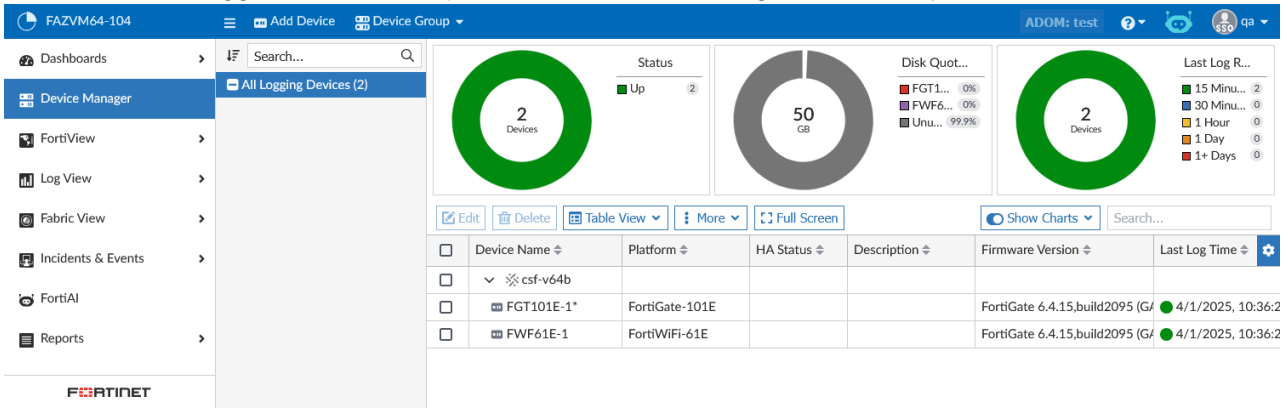
3. When logging into FortiAnalyzer, the Fabric SSO user can click *Login via Fabric Single Sign-On*.



The user can then select which Fabric IdP to use. In this example, theruser selects *csf-v64b*.



The user is then logged into FortiAnalyzer with access according to the admin profile.



Incidents & Events

Use *Incidents & Events* to generate, monitor, and manage alerts and events from logs. The live monitoring of security events is a powerful and enabling feature for security operations. Incidents can be created from events to track and respond to suspicious or malicious activities.

You can also use *Incidents & Events* to review FortiGuard Services, MITRE ATT&CK® coverage, Automation, and SIEM log parsers.

Incidents

Incidents can be created to track and analyze events.

Incidents raised from the *Event Monitor* contain event details, as well as information and actions helpful for administrator analysis. From the incident's analysis page, administrators can assign, edit, export, or delete incidents, view audit history, and manage attached reports, events, and comments.

Incidents can be viewed at *Incidents & Events > Incidents > Incidents*.

For more information about incidents, see the following topics:

- Raising an incident on page 204
- Managing incidents on page 206
- Analyzing an incident on page 208
- Configuring incident settings on page 212
- Adding reports to an incident on page 212

From *Incidents & Events > Incidents*, you can also review incidents and events according to the MITRE ATT&CK® and MITRE ATT&CK® ICS matrices. For more information, see MITRE ATT&CK® on page 213.

Raising an incident

You can raise an incident only from alerts generated for one endpoint.

Incidents can be raised in the following ways:

- In *Incidents & Events > Incidents > Incidents*, click *Create New* in the toolbar. This opens the *Create New Incident* pane.
- In *Incidents & Events > Event Monitor > All Events*, right-click an event and select *Create New Incident*. This opens the *Create New Incident* pane with the applicable fields filled in, such as the *Affected Endpoint*.

The following is a description of the options available in the *Create New Incident* pane.

Option	Description
Incident Name	Enter a name for the incident.
Incident Category	Select a category from the dropdown list.
MITRE Tech ID	Select the MITRE ATT&CK technique ID(s) that the incident may correspond to. The techniques are organized in the list according to their MITRE domain and tactic. The incident will be included in count for the MITRE ATT&CK matrix. For more information, see MITRE ATT&CK® on page 213.
Severity	Select a severity level from the dropdown list.
Status	Select a status from the dropdown list.
Affected Endpoint	In the *Raise Incident* pane, the affected endpoint is filled in and cannot be changed. In the *Create New Incident* pane, select the affected endpoint from the dropdown list.
Description	Enter a description.
Assigned To	The admin account to which the incident is assigned.

Automatically created incidents

Incidents can also be automatically created when:

- an event handler is configured to automatically create an incident when triggered.
- the alert grouping feature is enabled to generate incidents to group events of specified severity level with the same target.
- the *Automated Correlation Threat Hunting* playbook is run after the *Malicious IP Intrusion Detection* event handler is triggered.



The *Automatically Create Incident* (`auto-raise-incident`) event handler option has high priority. When it is enabled, triggering the handler will cause it to create an incident according to the `auto-raise-incident` option, not according to alert grouping or the automated correlation threat hunting playbook.

To automatically create incidents when events are triggered from a specific event handler:

1. In an event handler configuration, enable the option to *Automatically Create Incident*.
   Once the handler triggers an alert, a new incident is created with the name as `<Handler Name>: <Event Subject>`. If there are new events with same subject, they will be directly attached to the same incident. A new incident is created if the event has a new subject, or if the existing incident's status has changed to *Closed*. In the *Incidents* pane, these incidents display `<alertid>/Auto-Raised` in the *Incident Reporter* column.

For more information about configuring event handlers, see Creating a custom event handler on page 298.

The *Automatically Create Incident* option is enabled in some predefined event handlers. For example, many Outbreak Alert event handlers from FortiGuard will automatically create incidents to ensure steps are completed for remediation.

To automatically create incidents by grouping alerts:

The alert grouping feature is enabled by default to automatically raise an incident to group alerts with severity greater than or equal to `critical` when they share the same target.

1. In the FortiAnalyzer CLI, configure the following setting:

```
config system log alert
   set min-severity-to-raise-incident-by-grouping {critical | high | none}
end
```

Variable	Description
min-severity-to-raise-incident-by-grouping {critical | high | none}	Set the minimum severity to raise incident by grouping (default = critical). • `critical`: Raise incident by grouping alerts when alert-severity is critical. • `high`: Raise incident by grouping alerts when alert-severity is critical or high. • `none`: Do not raise incident by grouping alerts.

When set to `critical` or `high`, events with the set severity will create an incident if have target(s). New events with the same target will then be attached to the created incident. If an incident is created with two targets in the initial event (such as A,B), the next events with [A] or [B] as the target will be added to the existing incident.

After closing an incident that was automatically created for grouping alerts, a new incident will be created when a new event has the same target as the closed incident.

To automatically create incidents to correlate threats for malicious IP detection:

The *Automated Correlation Threat Hunting* playbook automatically creates incidents when the *Malicious IP Intrusion Detection* event handler is triggered. For more information, see Malicious IP intrusion event handler on page 292.

Managing incidents

You can review created incidents in *Incidents & Events* > *Incidents* > *Incidents*. The incidents are displayed in a table view.

There are three charts displayed above the table:

- *Severity*
- *Status*
- *Category*

By default, the *Show Charts* toggle is enabled. You can select which charts appear by selecting them in the *Show Charts* dropdown, or you can hide all the charts by disabling the *Show Charts* toggle.

Mouse over the charts to see more information in a tooltip. Click a section of a chart to filter the charts and the table by that information. You can apply multiple filters across the charts. Once filtered, a filter icon appears next to the chart title; click the filter icon to remove the filter. You can also filter the table by the time frame dropdown in the toolbar.

In the table view, you can use the *Incident Reporter* column to identify if an incident was manually created or if it was created automatically. If it was created automatically, the incident reporter will be the name of the playbook or event handler that generated the incident. For more information about automatically creating incidents from event handlers, see Creating a custom event handler on page 298.

You can perform the following actions from the toolbar:

- Create a new incident
- Edit an incident
- Delete incidents
- Enrich an indicator within the incident
- Block or unblock an indicator within the incident
- Export an incident's analysis
- Export the incident table view as a CSV
- Edit the incident settings

To create an incident:

See Raising an incident on page 204.

To edit an incident:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Select or right-click an incident and click *Edit*.
   The *Edit Incident* pane displays.
3. Edit the incident.
   For more information about the available options, see Raising an incident on page 204. The *Incident Number*, *Incident Date / Time*, and *Affected Endpoint* cannot be edited.
   Incidents can also be edited from their *Analysis* page. See Analyzing an incident on page 208.

To delete an incident:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Select or right-click an incident and click *Delete*.
   You can also select multiple incidents to delete them at the same time. If you do not select any incidents, the option to *Delete All* is available in the toolbar.
   The *Delete Incident* dialog displays.
3. To confirm the action, click *OK*.

To enrich an indicator within the incident:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Select or right-click an incident with an indicator and click *Enrich*.

If there is no indicator for the incident, the option will be grayed out.

For more information, see Indicator enrichment on page 333.

To block an indicator within the incident:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Select or right-click an incident with a suspicious indicator and click *Block*.
   If there is no indicator for the incident or there is no authorized FortiManager connector, the option will be grayed out.

You can also unblock indicators from the *Incidents* pane. For more information about blocking or unblocking indicators, see Blocking indicators on page 334.

To export an incident's analysis:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Select an incident, and click *More* > *Export*.
   You can also right-click an incident, and click *Export*.
3. In the *Export Incident* pane, review the preview for the export.
   The export includes the incident summary, events, comments, and endpoints.
4. Toggle *Include Events* according to your needs.
5. Set the *Maximum Rows* for tables in the export. The default is `100`.
6. Click *Export HTML* or *Export PDF*.
   The file is saved to the management computer.

To export the incident table view:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Using the charts and the time period dropdown, filter the table according to your needs.
3. Click *More* > *Export Table as CSV*.
   The CSV is saved to the management computer.

Analyzing an incident

In *Incidents & Events* > *Incidents* > *Incidents*, select an incident or right-click an incident and select *Analysis*. Alternatively, you can double-click an incident to open the *Incident Analysis* pane. The *Incident Analysis* pane displays the incident's affected endpoint and user, audit history, attached events, reports, comments, and more.



Some features of incident analysis are only available with the applicable license.

You can perform the following actions from the toolbar in the *Incident Analysis* pane:

Action	Description
Edit Layout	Edit the layout of the widgets. You can toggle and resize widgets according to your needs. Select the number of *Columns* to use for the layout. Use *Undo* and *Redo* as you make your changes to the layout. Click *Save* to save the changes, or *Reset* to reset to the defaults.
Export Incident	Export the incident analysis as HTML or PDF. In the *Export Incident* pane, you can review a preview of the export. You can toggle to *Include Events* and set the *Maximum Rows* for tables in the export in this pane as well.
Enrich	Enrich an indicator within the incident. For more information, see Indicator enrichment on page 333.
Block/Unblock	Block or unblock an indicator within the incident. For more information, see Blocking indicators on page 334.
Execute Playbook	Select a playbook to execute. In the *Select Playbook to Run* pane, you can select a playbook from the table view and click *Run*. If there are configurable parameters for the playbook, you will be asked to configure them in the *Manually Run Playbook* dialog. Once run, the *Playbook Tasks* dialog displays the live progress of the playbook job, including the job details, a timeline, and the raw log information.
Run Report	Run a report against the affected endpoint. In the *Run Report* pane, select the *Endpoint*, *Report*, and *Time Period*. Only reports with *Auto Cache* and *Extended Log Filtering* enabled can be run from an incident. For more information, see Reports Settings tab on page 435. To attach the report to the incident, see Adding reports to an incident on page 212.
Quarantine	Quarantine the affected endpoint. In the *Quarantine Endpoint* dialog, select the *Endpoint* and the *Connector*.
Refresh	Refresh the widgets.

The *Incident Analysis* pane includes the following widgets:

Widget	Description
Incident Summary	General information about the incident. You can review and modify the following information: • **Incident Number**: The unique incident ID. This is displayed, but cannot be modified. • **Incident Name**: The name of the incident. • **Incident Date/Time**: The date and time that the incident was created. This is displayed, but cannot be modified.

Widget	Description
	• **Incident Update Date/Time**: The date and time that the incident was last updated. This is displayed, but cannot be modified. • **Incident Category**: The incident category, including *Unauthorized Access*, *Denial of Service (DoS)*, *Malicious Code*, *Improper Usage*, *Scans/Probes/Attempted Access*, and *Uncategorized*. • **MITRE Tech ID**: The techniques associated with the incident. These can be added via the dropdown list, which organizes the techniques by domain and tactic. • **Severity**: The severity of the incident, including *High*, *Medium*, and *Low*. • **Status**: The current status of the incident, including *New*, *Analysis*, *Response*, *Closed: Remediated*, and *Closed: False Positive*. • **Affected Endpoint**: The endpoint associated with this incident. This is displayed, but cannot be modified. • **Description**: A description of the incident provided by the administrator. • **Assigned To**: A dropdown menu of administrators to which the incident can be assigned. After making modifications, click *Update* to save your changes.
Affected Endpoint/User	Information about the affected endpoint/user. When multiple endpoints/users are associated with the incident, the total number is displayed and you can click the forward or backwards arrow on the tile to cycle between them.
Comments	Displays comments made by administrators for this incident with a timestamp. The most recent comments appear at the top of the list. Enter a comment and click *POST* to create a new comment. Existing comments can be edited and deleted by administrators.
Affected Assets	Displays affected asset(s) in a table view. Includes the endpoint, user, IP address, and MAC address of the asset. Click a user in the *User* column to display endpoint information in a separate dialog.
Incident Timeline	The timeline of the events raised for the incident. Scroll using your mouse wheel to change the displayed time frame. Mouse over the event to display a tooltip of its details.
Events	Displays the events that have been raised for this incident in a table view. You can use the search bar to search for events; toggle *Match Case* and *Use Regular Expression* using the icons in the search bar. When FortiAnalyzer has a valid license for the FortiTIP service, click the hyperlink in the *Outbreak Name* column to open the FortiTIP instance with the outbreak information. This includes a summary, outbreak details, hunt rules, mitigations, and more. For more information, see FortiTIP service integration on page 357.

Widget	Description
	You can perform the following actions after selecting an event: • **View Logs**: Open the *View Logs* pane, display the related logs for the event in a table view. • **Search in Log View**: Open *Log View* filtered by the event in a new tab. • **Suppress**: Suppress this event and identical or similar events according to suppression criteria. See Suppressing events on page 227. • **Delete**: Delete the event.
Audit History	Displays the history of changes made to an incident, including the user who made the change and information about the type of change that was made. Click *Expand All* to see additional details.
Executed Playbooks	The history of executed playbooks related to the incident. Click *Execute Playbook* to run a playbook configured with the *On_Demand* trigger. See Automation on page 362. Click a record for an executed playbook to view the , the *Playbook Tasks* dialog, which displays the job details, a timeline of the playbook execution, and the raw log information.
Indicators	Displays indicators attached to an incident from FortiGuard, FortiMail, or event handlers. Hover your mouse over an indicator to view detailed information from FortiGuard or click *Details* under *Results* to view information from FortiMail including sender reputation and email statistics. Indicator information can be attached to incidents using the FortiGuard and FortiMail connector in playbooks, or when an incident is created from an event that includes indicators identified in the event handler. You can enrich or block indicators from this widget.
Reports	Attach and manage reports related to this incident. The reports are displayed in a table view, listing the report name, format, time range, and devices. See Adding reports to an incident on page 212.
Processes	Displays endpoint processes associated with this incident including the process ID, process path, and network connection. Select a time period to view by choosing a snapshot from the snapshot dropdown. Processes can be displayed in a table format or as raw data.
Software	Displays endpoint software associated with this incident including the software, installation path, and installation time. Select a time period to view by choosing a snapshot from the snapshot dropdown. Software can be displayed in a table format or as raw data.

Widget	Description
Vulnerabilities	Displays endpoint vulnerabilities associated with this incident including the vulnerability name, ID, severity, and category. Select a time period to view by choosing a snapshot from the snapshot dropdown. Vulnerabilities can be displayed in a table format or as raw data.

Configuring incident settings

To configure incident settings, go to *Incidents & Events* > *Incidents* > *Settings*.

When an incident is created, updated, or deleted, you can send a notification to external platforms using selected fabric connectors. To create fabric connectors to external platforms, such as ServiceNow or MS Teams, see Configuring ITSM connectors on page 378.

To configure incident notification settings:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Click *More* > *Settings*.
3. Select a *Fabric Connector* from the dropdown list.
4. Select which notifications you want to receive:
   - *Send notification when new incident is created.*
     Incidents in New status will not trigger notification.
   - *Send notification when new incident is updated.*
   - *Send notification when new incident is deleted.*
5. To add more fabric connectors, click *Create New* and repeat the above steps to configure notification settings.

Adding reports to an incident

Reports can be attached to incidents to include historical data relevant to that incident.

Reports can be added to incidents through the following methods:

1. Reports can be manually added by an admin from the *Reports* module or from the incident's *Incident Analysis* pane.
2. Reports can be automatically added to an incident by a playbook. See Automation on page 362.

Once a report has been attached to an incident, it can be viewed, managed, and downloaded from the *Reports* widget on the incident's *Incident Analysis* pane. Multiple reports can be attached to a single incident.

To attach reports from an incident:

1. Go to *Incidents & Events* > *Incidents* > *Incidents*.
2. Select an incident or right-click and select *Analysis*.

The *Incident Analysis* pane displays.

3. In the *Reports* widget, and click *Add*.
4. Select one or more previously generated reports, and click *OK*.

To attach reports from Reports:

1. Go to *Reports* > *Generated Reports*.
2. Right-click on a report, and select *Add to Existing Incident*.
   If you select *Create New Incident*, the you can create a new incident with the report attached. For information about the fields in the *Create New Incident* dialog, see Raising an incident on page 204.
3. Select an incident from the list, and click *OK*.

MITRE ATT&CK®

MITRE (MIT Research Establishment) ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a framework for handling cyber threats. This framework consists of tactics and techniques organized into matrices. With the appropriate license, you can leverage these matrices in the FortiAnalyzer GUI:

- *Incidents & Events* > *Incidents* > *MITRE ATT&CK®*
- *Incidents & Events* > *Incidents* > *MITRE ATT&CK® ICS*

The column headers in the MITRE ATT&CK matrices are tactics, and the tiles within these columns are the relevant techniques.

FortiAnalyzer associates incident and event information with the relevant tactics and techniques. FortiAnalyzer also displays coverage in the MITRE ATT&CK matrices, so you can determine which event handlers help to cover specific tactics and techniques.



The *MITRE Domain* and *MITRE Tech ID* fields in event handlers are used to associate the handlers and their resulting events to the correct tactic and technique. For more information about configuring event handlers, see Creating a custom event handler on page 298 and Creating a custom correlation handler on page 304.

This topic explains the two options available in *MITRE ATT&CK®* and *MITRE ATT&CK® ICS*:

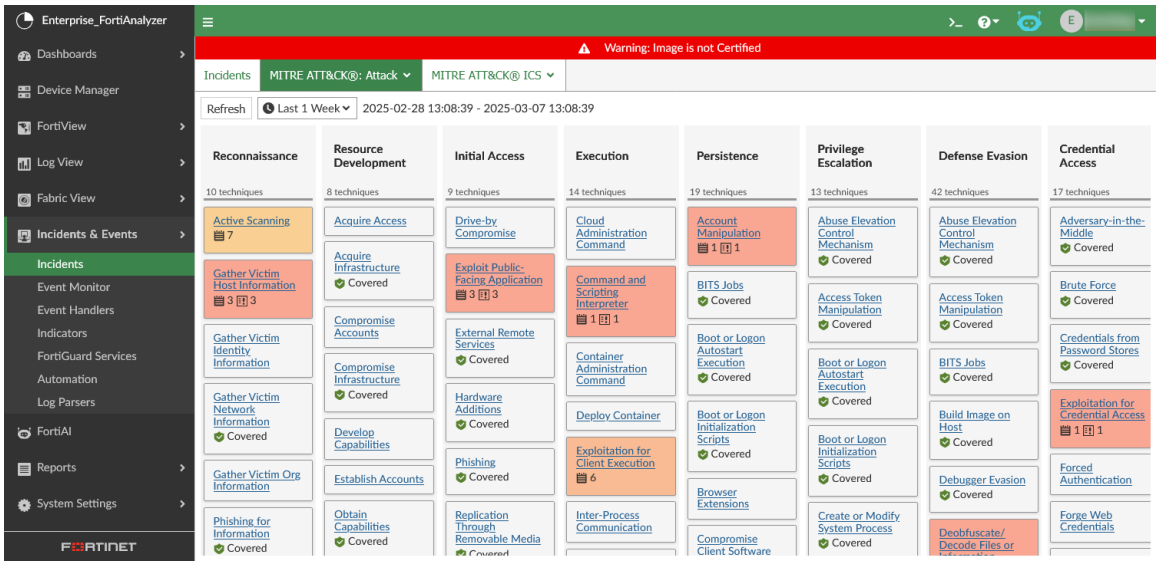
- Attack
- Coverage

The examples displayed below are for the *MITRE ATT&CK®* pane, but the same functionality exists for the *MITRE ATT&CK® ICS* pane.

The OT Security Service is required for FortiAnalyzer to use all functionality in the *MITRE ATT&CK® ICS* pane. For more information about this service, see the FortiAnalyzer Datasheet.

Attack

You can review incident and event information organized within the MITRE ATT&CK matrices from the *Attack* tab. Each technique includes a hyperlink to the relevant information at https://attack.mitre.org/techniques. You can filter the matrices using the time frame dropdown, and you can refresh the matrices as needed.

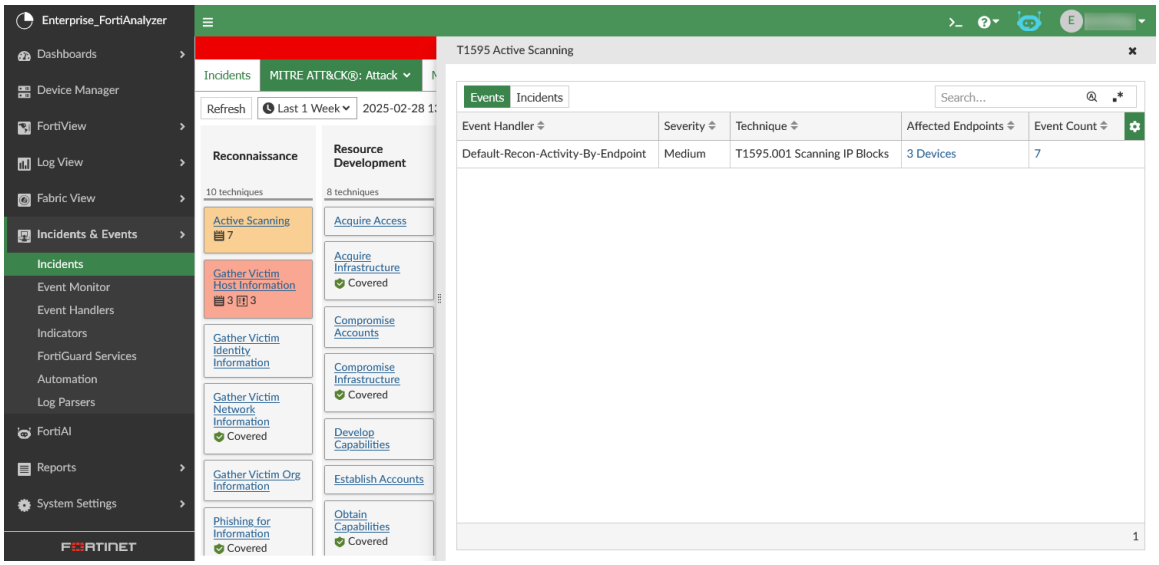


If there are events associated with the technique, an icon and count displays on the tile. A separate icon and count displays for the associated incidents as well. Mouse over the tile to display the information in a tooltip. If there are sub-techniques, the tooltip breaks down which sub-technique the events and incidents are associated with.

Double-click a tile with associated events or incidents to open a pane for that technique. In this pane, you can toggle between table views for *Events* and *Incidents*.

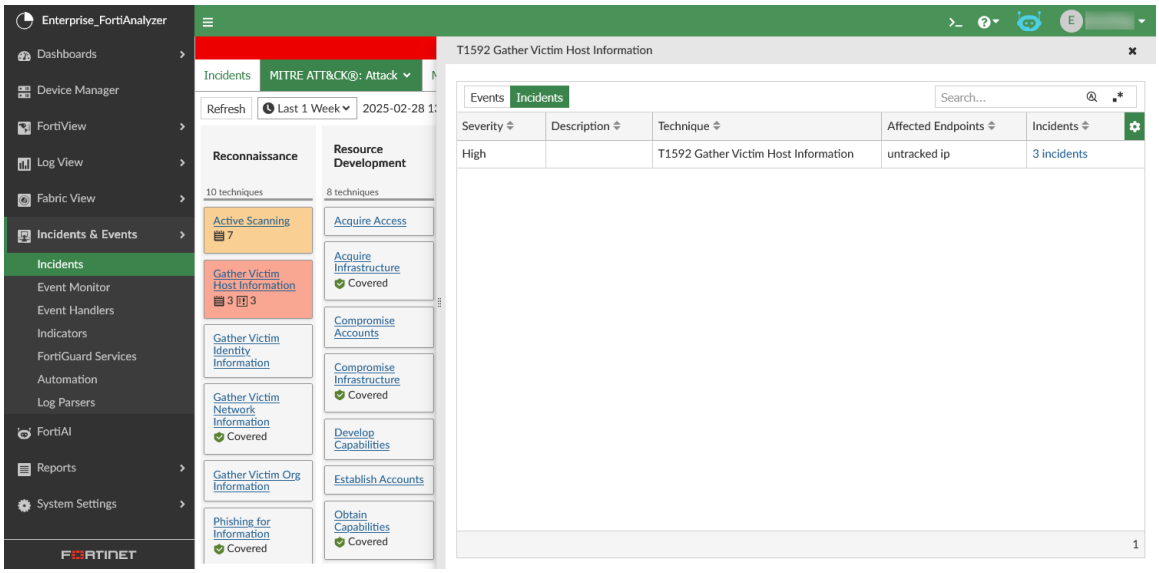
The table view for *Events* includes the following information:

Column	Description
Event Handler	The event handler that generated the event(s).
Severity	The severity of the event(s).
Technique	The technique or sub-technique related to the event(s).
Affected Endpoints	The number of affected devices. Click the count for affected endpoints to open another pane with the list of endpoints found in the events.
Event Count	The event count related to that event handler and technique or sub-technique. Click the event count to open the *Event Monitor* in a new tab. It is filtered by the selected handler and time range from the matrix. For more information, see Event Monitor on page 218.



The table view for *Incidents* includes following information:

Column	Description
Severity	The severity of the incident(s).
Description	The description for the incident.
Technique	The technique or sub-technique related to the incident(s).
Affected Endpoints	The number of affected endpoints. Click the count for affected endpoints to open another pane with the list of endpoints found in the incidents.
Incidents	The incident count related to that technique or sub-technique. Click the incident count to open the *Incidents & Events* > *Incidents* > *Incidents* pane in a new tab. It is filtered by incidents of the selected technique. For more information, see Incidents on page 204.

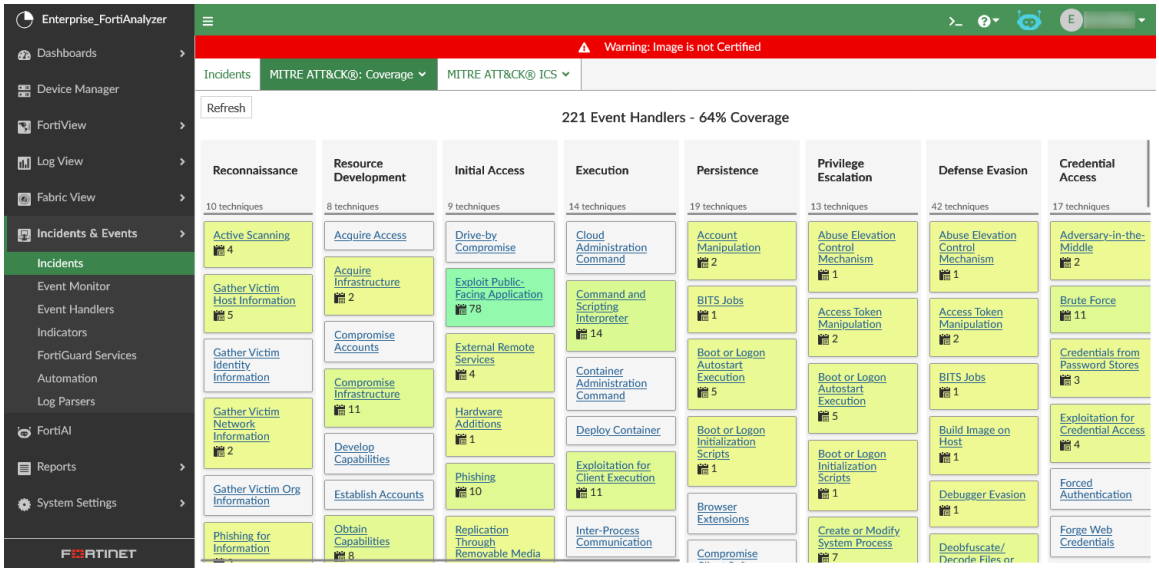


If there are no events or incidents associated with a technique but it has at least one event handler, a covered icon displays on the tile. Mouse over the tile to display the number of event handlers and the list of sub-techniques in a tooltip. To review the coverage in more detail, go to the *Coverage* tab. See Coverage.

If there are no events, incidents, or event handlers associated with a technique, the tile will not display any icons and the mouse-over tooltip will not be available.

Coverage

You can review event handler coverage according to the MITRE ATT&CK matrices from the *Coverage* tab. Each technique includes a hyperlink to the relevant information at https://attack.mitre.org/techniques. You can refresh the matrices as needed.



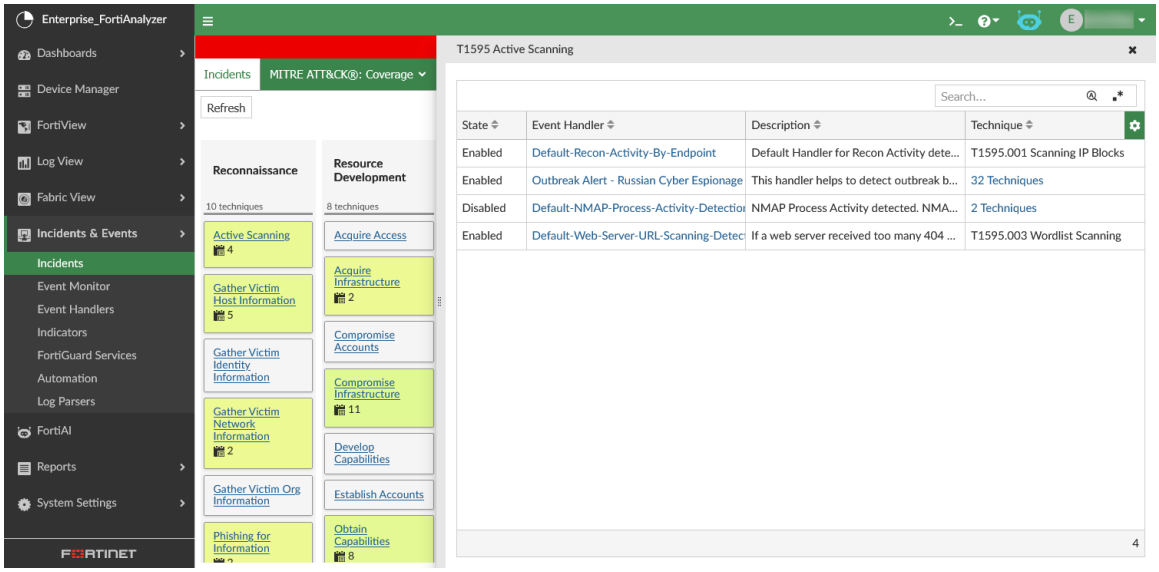
When a basic or correlation event handler is associated with a technique, it will be included as part of the coverage for that technique. The tile displays an icon and count for associated event handlers. Mouse over the

tile to display the information in a tooltip. This includes the total event handler count and a breakdown of the count for each sub-technique, if they are available.

One event handler can be associated to multiple techniques and sub-techniques.

Click a tile with coverage to open a table view of event handlers for that technique. The table includes the following information:

Column	Description
State	The state of the event handler: *Enabled* or *Disabled*.
Event Handlers	The name of the event handler. Click the name to view the event handler configuration. You can edit the *Status*, *MITRE Domain*, and *MITRE Tech ID* from this pane, if needed. After updating the coverage for an event handler, refresh the *MITRE ATT&CK®* matrix to display the changes.
Description	The description of the event handler.
Technique	The technique or sub-technique(s) associated with the event handler. If there are multiple sub-techniques associated with the event handler, the count will be provided in this column. Click the count to display which sub-techniques are associated with the event handler.



If there are no event handlers associated with a technique, *Enabled* or *Disabled*, the tile will not display any icons and the mouse-over tooltip will not be available.

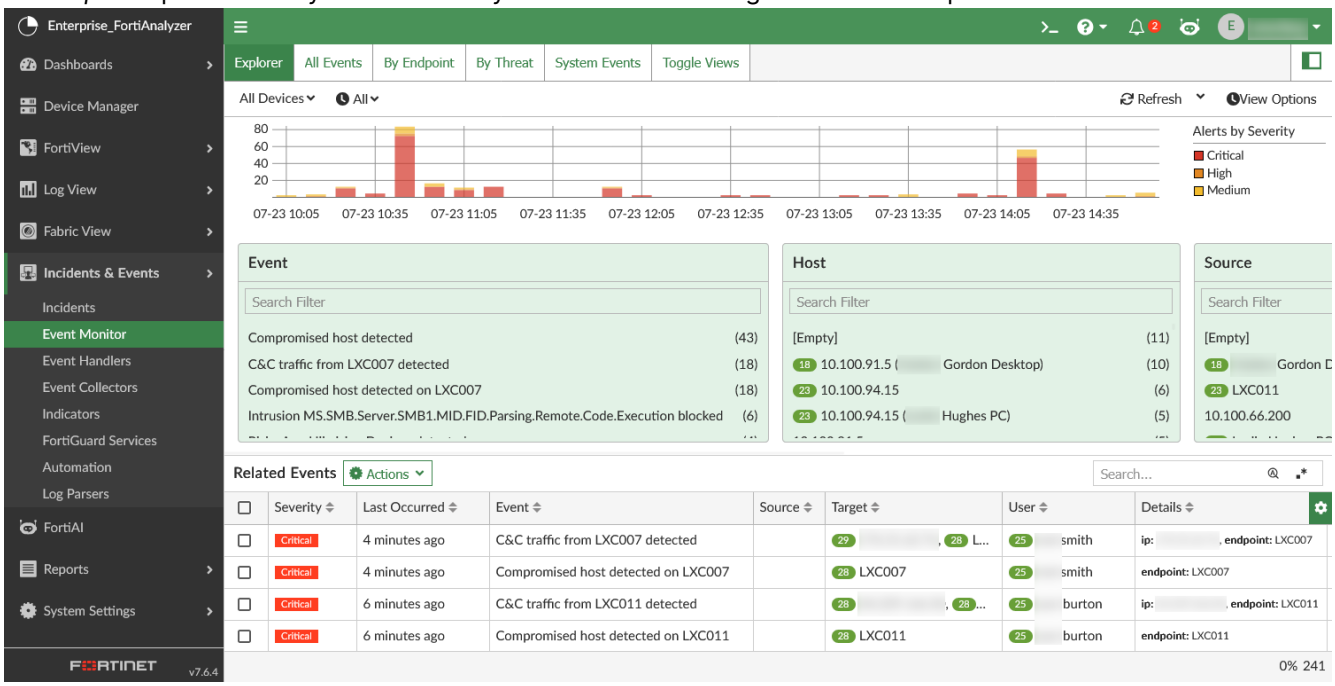
Event Monitor

After event handlers start generating events, view events and event details in *Incidents & Events* > *Event Monitor*.

When rebuilding the SQL database, you might not see a complete list of historical events. However, you can always see events in real-time logs. You can view the status of the SQL rebuild by checking the *Rebuilding DB* status in the *Notification Center*.

Explorer

The *Explorer* pane allows you to efficiently monitor events using a timeline and quick filters.



You can perform the following actions from the toolbar:

Devices	Select devices from the dropdown to filter the pane.
Time Period	Select a time period to filter the pane. Select *Custom* to specify a time period not in the dropdown list.
Refresh	Click to manually refresh the pane. From the dropdown, you can select an automatic refresh interval.
View Options	Toggle visibility for the timeline and quick filters. The timeline and all quick filters are enabled by default.

The *Explorer* pane includes the following sections:

Timeline	Displays the number of alerts by severity in a stacked bar chart on a timeline. A legend for the severity displays next to the timeline. You can click a severity level in the legend or on the bar chart to filter the pane by that severity level. Click the severity level again to remove the filter.
Quick Filters	Displays the available values to filter the pane by according to the following fields: • Event • Host • Source • Target • User The available values are impacted by the device, time period, and quick filters that are already set in the pane. Click a value in the quick filter widgets to filter the pane by that value. Click multiple values to apply the filters with an AND relationship. You can use the *Search filter* bar in the quick filter widgets to find specific values. To remove the filters, click *Clear Filters* in the quick filter widget.
Related Events	Displays the events in a table view. Use the search bar to find specific events in the table. You can perform the following actions on the events:

Action	Description
Search in Log View	Open *Log View* in a separate tab, filtered to display all logs associated with the event.
Create New Incident	Create a new incident from the event. See Raising an incident on page 204.
Add to Existing Incident	Attach the event to an existing incident. In the *Attach to Incident* dialog, enter an incident number or select an incident from the table and click *OK*.
Suppress	Suppress this event and identical or similar events according to suppression criteria. For more information, see Suppressing events on page 227.



When applicable, the risk score will appear next to the endpoint or user in the quick filters and related events table.

The following columns are available for the *Related Events* table view:

Column	Description
Severity	The event severity level.

Column	Description
Last Occured	How long ago the most recent log occured related to the event.
Event	The event subject line.
Endpoint	The affected endpoint.
Source	The source of the event activity. This is the actor or system that initiated the action; it could be a user, IP, device, or process. See additional explanation below the table.
Target	The affected target. This could be a device, user, service, or file. See additional explanation below the table.
User	The affected user.
Event Type	The event type, such as *Traffic*.
Event Status	The event status, such as *Unhandled* or *Mitigated*.
Details	A breakdown of target IPs and endpoints.
Device Name	The device that sent logs to trigger the event.
Rule	The rule that triggered the event.
Event Handler	The event handler containing the rule that triggered the event.

The *Source* and *Target* fields can support incident triage and prioritization. They can help determine if a threat is external or internal, and they make it easier to understand the attack impact and intent.

Examples:

- If a hacker tries to break into a server:
  Source = hacker's IP or device
  Target = the server
- If a user logs into a system:
  Source = the user
  Target = the system being accessed

FortiAnalyzer assigns the *Source* and *Target* based on the group-by fields in the triggered event handler.

- *Source*: source IP, source user, process name
- *Target*: destination IP, target host, affected user or object

For more information about event handler configuration, see Creating a custom event handler on page 298.

Event details pane

You can double-click a record in the *Related Events* table to open an event details pane. This pane is named after the event, and it displays with the following tabs:

Tab	Description
Event Details	Displays the event details in a formatted view. You can toggle to view the raw JSON. You can use the search bar to find specific information within the event details.

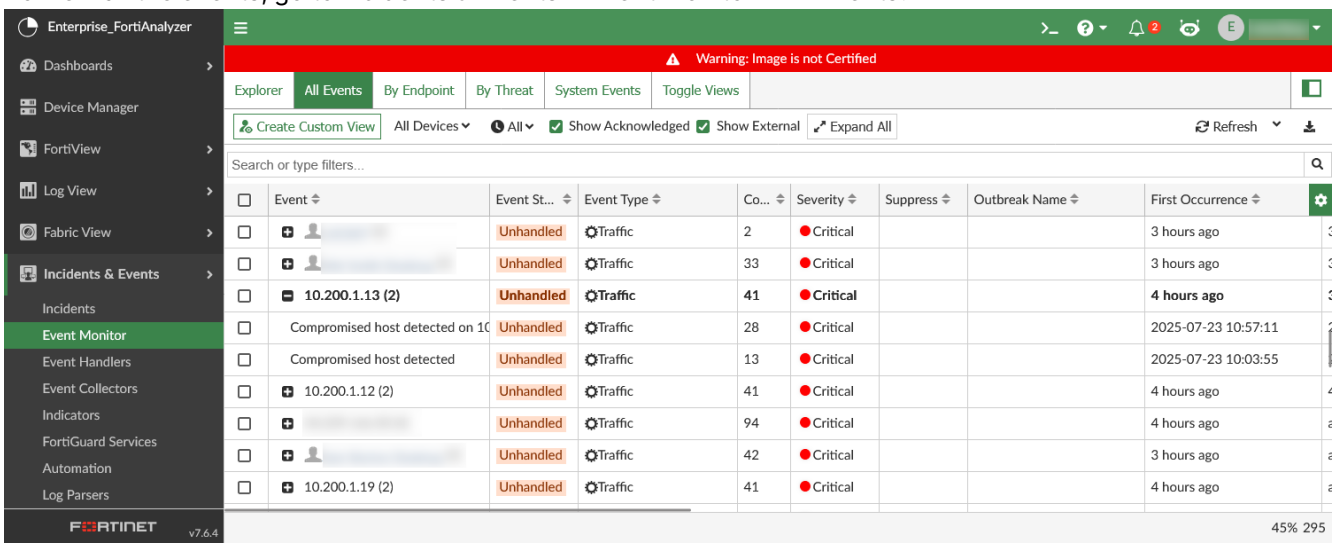
Tab	Description
	In the *Formatted View*, you can click the value in the *Endpoint* field to display the endpoint details pane. For more information about this pane, see Asset List on page 181.
Triggering Logs	Displays a sample of logs that triggered the event. You can view the log details in this tab.
Rule Summary	Displays information about the event handler rule that triggered the event. This includes the rule name, description, log type, severity, pattern, threshold, and group by information.
Comment	Add or edit a comment for the event.
Context	Displays a timeline for related events. From the *Entity* dropdown, select the entity/entities to include in the timeline. Click events in the timeline to open the event details pane.

The *Actions* dropdown in this pane includes the same actions as available from the *Related Events* table. See Related Events above.

To support investigation, you can also access the event details pane from endpoints and users in the *Asset Identity List*. For more information, see Asset List on page 181 and Identity List on page 185.

All Events

To view all the events, go to *Incidents & Events* > *Event Monitor* > *All Events*.



You can perform the following actions from the toolbar:

Create Custom View	Save the current view including filter settings, device selection, and time period. See Creating custom views on page 230.

Devices	Select devices from the dropdown to filter the table view.
Time Period	Select a time period to filter the table view. Select *Custom* to specify a time period not in the dropdown list.
Show Acknowledged	Enable to include acknowledged events in the table view. See Acknowledging events on page 227.
Show External	Enable to include external alerts in the table view. You must configure event collectors for external alerts. See Event collectors on page 322.
Collapse All/Expand All	Click to expand or collapse the event details displayed in the table view.
Refresh	Click to manually refresh the table view. Alternatively, from the dropdown, you can specify an automatic refresh interval for the table view.
Save CSV	Click to download the current table view of events in a CSV file.
Filters	Enter filters for the table view. See Filtering events on page 224.
Column Settings	Select which columns are displayed for the table view.

By right-clicking an event in the table view, you can perform the following actions from the shortcut menu:

Acknowledge	Acknowledge the event. See Acknowledging events on page 227.
Comment	Enter a comment for the event. The comment is displayed in the *Comment* column, which can be added to the table view from *Column Settings*.
Assign To	Select an admin to assign the event to. The assigned admin is displayed in the *Assigned To* column, which can be added to the table view from *Column Settings*.
Suppress	Suppress this event and identical or similar events according to suppression criteria. For more information, see Suppressing events on page 227.
View Logs	Open a table view of sampled logs associated with the event. For example, if there are 20 associated logs that triggered the event under the same conditions, only one sample log display in the *View Logs* pane. To view all logs associated with the event, use *Search in Log View*.
Search in Log View	Open *Log View* in a separate tab, filtered to display all logs associated with the event.
Create New Incident	Create a new incident from the event. See Raising an incident on page 204.
Add to Existing Incident	Attach the event to an existing incident. In the *Attach to Incident* dialog, enter an incident number or select an incident from the table and click *OK*.
Filter by <criteria> =	Filter for events that are equal to the criteria that you right-clicked in the table view. See Filtering events on page 224.
Filter by <criteria> !=	Filter for events that are not equal to the criteria that you right-clicked in the table view. See Filtering events on page 224.

In addition to the actions describe above, you can also click the hyperlinks in the event monitor to view more information. The table below lists applicable default columns with hyperlinks:

Event	If applicable, click the hyperlink to view the *Endpoint Information* dialog. In this dialog, you can click the endpoint name to open the *Asset Identity List* filtered by that endpoint. The *Asset* table is displayed by default; you can switch to the Identity table, if needed. For more information, see Asset List on page 181 and Identity List on page 185.
Outbreak Name	When FortiAnalyzer has a valid license for the FortiTIP service, click the hyperlink to open the FortiTIP instance with the outbreak information. This includes a summary, outbreak details, hunt rules, mitigations, and more. For more information, see FortiTIP service integration on page 357.
Handler	Click the hyperlink to open the *Edit Event Handler* pane for that event handler. The rule that generated the event will be highlighted. For more information about editing event handlers, see Creating a custom event handler on page 298.

Default event views

FortiAnalyzer event handlers apply one or more tags to events, allowing the events to be grouped into views in the *Event Monitor*. These views are visible in the navigation.

Default views are organized into three view categories under *Incidents & Events* > *Event Monitor*:

- *By Endpoint*: Provides security event views from an endpoint perspective.
- *By Threat*: Provides security event views from a threat perspective.
- *System Events*: Provides event views which cover device system events.

In order for events to be displayed in default views, the corresponding event handler(s) must be enabled. Refer to the chart below for a list of the predefined event handlers that must be enabled to support each default view:

View category	Default view	Required predefined event handler
By Endpoint	All Security Events	Displays all events within category with enabled handlers
	Compromised Hosts	Default-Botnet-Communication-Detection-By-Endpoint Default-Compromised Host-Detection-IOC-By-Endpoint
	Sandbox Detections	Default-Sandbox-Detections-By-Endpoint
	Malware Activity	Default-Sandbox-Detections-By-Endpoint Default-Malicious-File-Detection-By-Endpoint
	Ongoing Intrusions	Default-Malicious-Code-Detection-By-Endpoint
	Malicious Domain/URL Access	Default-Risky-Destination-Detection-By-Endpoint
	High Risk App Usage	Default-Risky-App-Detection-By-Endpoint
By Threat	All Security Events	Displays all events within category with enabled handlers
	C&C Call Backs	Default-Botnet-Communication-Detection-By-Threat Default-Compromised Host-Detection-IOC-By-Threat
	Sandbox Detections	Default-Sandbox-Detections-By-Threat
	Malware Activity	Default-Sandbox-Detections-By-Threat Default-Malicious-File-Detection-By-Threat
	Ongoing Intrusions	Default-Malicious-Code-Detection-By-Threat
	Malicious Domain/URL Access	Default-Risky-Destination-Detection-By-Threat
	High Risk App Usage	Default-Risky-App-Detection-By-Threat
System Events	Local Device	Local Device Event
	All	Displays all events within category with enabled handlers
	FortiGate	Default FOS System Events

Default views can be hidden or disabled. For more information, see Managing default views.

Admins can copy existing views to create custom views. For more information, see Creating custom views.

Filtering events

Filter the *Event Monitor* using *Add Filter* in the toolbar or by right-clicking an entry and selecting a context-sensitive filter. You can also filter by specific devices or timeframes.

To filter events using text mode:

1. Type the filter and its condition. Use the log field names and values.
2. To add more filters, type the connector (*AND* or *OR*) and then type the next filter.

To filter events using the right-click menu:

Right-click a filter criteria in the table view and select one of the following:

- *Filter by <criteria> =*: Filter for events that are equal to the criteria you selected.
- *Filter by <criteria> !=*: Filter for events that are not equal to the criteria you selected.

These options are only available for certain columns.

To launch Search in Log View from an event:

In the event list, right-click an entry and select *Search in Log View*.

Log View will launch with the filter automatically filled in with the following information:

- Log type of the event
- Time range (the first to the last occurrence of the event)
- Event trigger and group by value

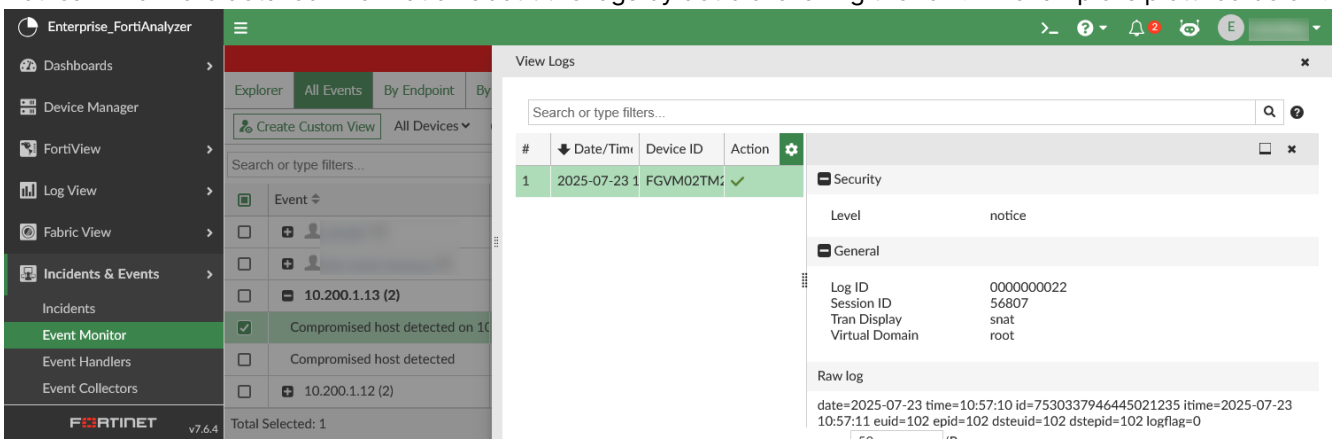
Viewing event details

In the *Event Monitor*, the tables will display rows in hierarchical structure: there will be parent rows with related child rows when applicable. You can click the expand option in a parent row to reveal the children. The children make up the parent row, but each child row will have its own related logs and event details. You can review these event and log details separately. Additionally, you can create incidents from parent rows or from individual child rows according to your needs.

To view log details for an event:

1. In the *Event Monitor*, select the child row.
2. Right-click the row and select *View Logs*.
   The *View Logs* pane displays.
3. If there are many logs, you can use the filters to find specific logs that helped to generate the event.

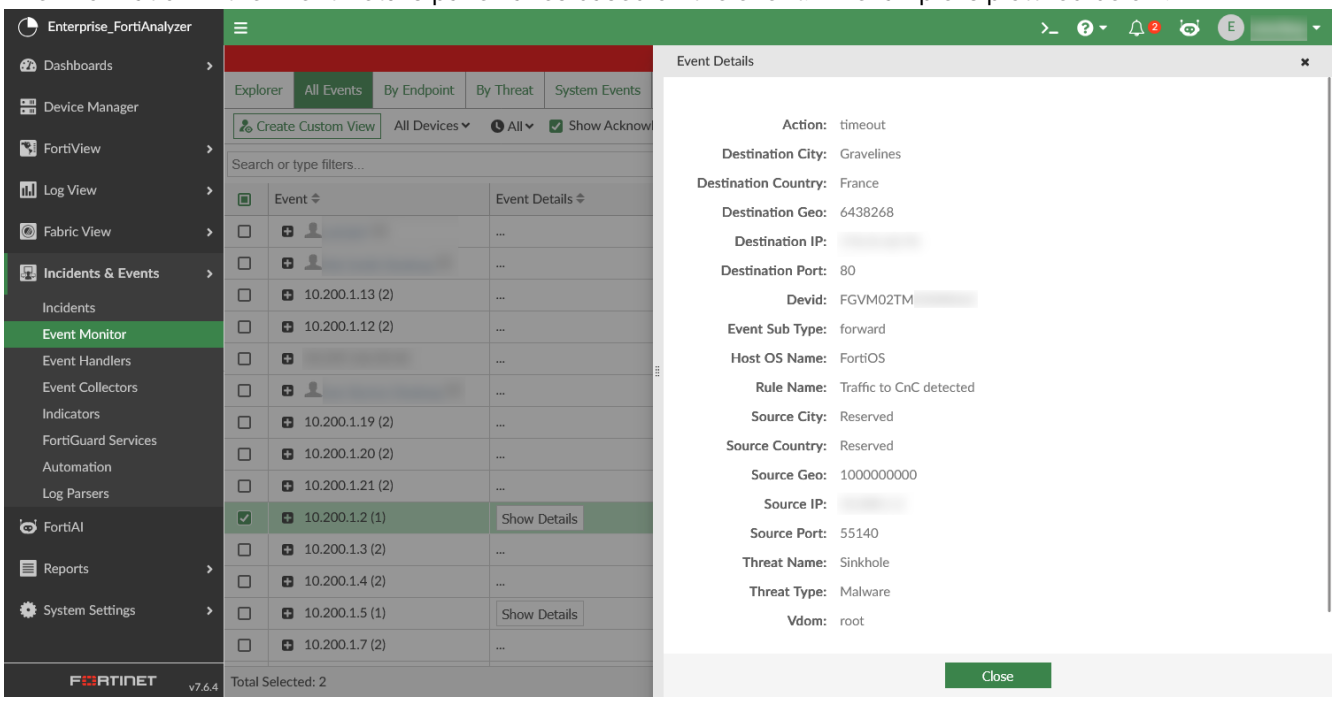
You can find more detailed information about the logs by double-clicking the row. An example is pictured below.



To view event details:

1. In the *Event Monitor*, make sure the *Event Details* column is included in the table.
   To check and update the enabled columns, click the settings icon above the table.
2. In the *Event Details* column for the related event, click *Show Details*.
   The *Event Details* pane displays.

The information in the *Event Details* pane varies based on the event. An example is pictured below.



IPS Signature Lookup

You can view IPS signature information from the event details when they are available by clicking on the link included in the log's *Attack Name* column. You can add the *Attack Name* column to the table using *Column*

Settings.

After clicking the attack name link, a dialog window appears which includes the IPS signature information. You can click *Show Raw Data* to display the raw information and access additional features including a search option.

Acknowledging events

Acknowledging an event removes it from the event list. Click *Show Acknowledged* to view acknowledged events.

You can enable the *Acknowledged By* and *Acknowledged Time* columns from the column settings option in the toolbar.

Acknowledged By displays the username of the administrator who acknowledged the event, and *Acknowledged Time* displays the time and date that the event was acknowledged.

To acknowledge events:

1. Go to *Incidents & Events* > *Event Monitor* and select a dashboard.
2. In the event list, select one or more events, then right-click and select *Acknowledge*.

Assigning events

Events can be assigned to administrators.

To view the administrator assigned to an event, enable the *Assigned To* column in the table from the column settings option in the toolbar. The *Assigned To* column displays the username of the administrator assigned to the event.

To assign an event:

1. Go to *Incidents & Events* > *Event Monitor* and select a table view (All Events, By Endpoint, By Threat, System Events, or a Custom View).
2. Expand a parent line to view the children in the table view.
3. Right-click an event, and select *Assign To*.
   The *Assign to Admin* pane displays.
4. Select a user from the dropdown or select *Assign to Myself*, and click *OK*.
   When enabled, the *Assigned To* column displays the username of the administrator assigned to the event.

Suppressing events

In some scenarios, FortiAnalyzer event handlers may be generating many identical events, which adds work for SOC analysts to investigate. In scenarios where the cause of these identical events has already been identified, the SOC analysts may want to suppress the events to avoid excess alerts and unnecessary follow up.

For example:

- **Impossible travel**: When an employee travels, they may access corporate resources from multiple devices, such as a cell phone and a remote PC acting as a jump station. These access attempts, originating from different locations, may trigger impossible travel events on FortiAnalyzer that could be suppressed from this user for the appropriate timeframe.
- **High resource usage**: A heavily loaded server may trigger high resource usage events, potentially indicating a denial-of-service attack. However, if the cause high resource usage has been identified or the SOC analysts want to reduce alerts while they complete investigation, they may suppress these events for an appropriate timeframe.

Event suppression does not have to completely prevent an event handler rule from generating events. As in the impossible travel example above, the events can be suppressed according to specific criteria applied to the rule, such as suppressing only related events involving the user that is traveling. When you are suppressing events, the suppression criteria is based on the event selected in the event monitor or incident. The criteria can also be further configured according to your needs.

To suppress events:

1. Go to *Incidents & Events > Event Monitor* or *Incidents & Events > Incidents > Incident Analysis*.
   In the *Event Monitor*, you can find the appropriate event by filtering the tables.
   In the *Incident Analysis* pane, you can find the appropriate event in the *Event* widget.
2. Right-click the event and select *Suppress*.
   The *Suppress Event* pane displays with the following information populated by default based on the event:

Event	The event name. This field cannot be edited.
Handler	The name of the event handler that contains the detection rule. This field cannot be edited.
Detection Rule	The event handler rule that will be suppressed according to the suppression criteria below. This field is populated with the event handler rule that triggered the event. This field cannot be edited.
Suppression Criteria	The conditions that will prevent events from being generated by the event handler rule; the log data must match all of the conditions to be suppressed. The conditions are prepopulated according to the log data of the event that you are using to suppress the rule. You can change, add, or remove conditions according to your needs.
Expiry	
Date Time	The expiry date and time for the event suppression. You can select the date and time for expiry.

3. Configure the *Suppression Criteria*.
   - To remove a condition, click the X icon in the *Action* column for the condition.
   - To add a condition, click a plus (+) icon in the *Action* column for one of the conditions.
   - To edit an existing or new condition, select a *Log Field* and *Match Criteria* and then enter a *Value*.

   Events will be suppressed from the event handler rule when the log data matches all of the configured conditions.

4. In the *Date Time* field, select an expiry date and time for the event suppression.
5. In the *Comment* field, enter a brief explanation for the event suppression. This field is optional.
6. Click *OK*.
   The *Suppress* column in the table view indicates that similar events will be suppressed. You can view and edit the suppression criteria by repeating the steps above.

To filter the event monitor by suppressed events:

1. Go to *Incidents & Events > Event Monitor* and select the appropriate table view, such as *All Events*.
   When an event has been suppressed, the *Suppress* column will display `Suppressed` for that row. Mouse over `Suppressed` to display the expiry date and time in a tooltip.
2. To filter the table view, right-click `Suppressed` and select one of the following:
   - *Filter by Suppress = yes* to display only suppressed events.
   - *Filter by Suppress != yes* to display only events that have not been suppressed.

   Alternatively, you can manually enter the filter in the search bar above the table.

To view, edit, or delete event suppression:

You can view, edit, and delete event suppression from the *Event Handlers*, *Event Monitor*, and *Incident Analysis* panes. The example below uses *Event Monitor*.

1. Go to *Incidents & Events > Event Monitor* and find the suppressed event.
2. In the *Handler* column for the suppressed event, click the event handler name.
   The *Edit Event Handler* pane displays.
   In the *Rules* section, each rule has a *Suppression* icon. This icon is only clickable when there is event suppression configured using events generated by the rule. The rule that triggered the event is highlighted for reference in the GUI.
3. Click the *Suppression* icon for the rule.
   The *Suppress* pane displays. The configured event suppression(s) display in a table view. The table will also display expired event suppression.
   From this pane, you can view, edit, and delete event suppression:
   - To view and edit, select the event suppression and click *Edit*.
   - To delete, select the event suppression and click *Delete*.

Managing default views

Default views in the By Endpoint, By Threat, and System Events view categories can be disabled or copied as a custom view, allowing you to display only the views that are useful to the user.

To toggle default views:

1. Go to *Incidents & Events > Event Monitor > Toggle Views*.
2. Select the *Default Views* that should be visible in the GUI navigation.
3. Click *Save*.

Creating custom views

To create a custom view:

1. Go to *Incidents & Events* > *Event Monitor* > *All Events*.
2. Add filters that you want to include in the custom view.
3. Click *Create Custom View*.
   If you are creating the custom view from another table view, such as *By Endpoint* or *By Threat* rather than *All Events*, you can click the current default view in the tool bar and select *Save as New Custom View*.
   The *Save as New Custom View* dialog displays.
4. In the *Name* field, enter a name for the custom view.
5. From the *Category* dropdown, select the category the view should be included in:
   - *By Endpoint*
   - *By Threat*
   - *System Events*
   - *Custom View*
6. Toggle *Public* according to your needs:
   - *Enabled*: Others can see this custom view.
   - *Disabled*: Only you can see this custom view.
7. Select *OK* to save the view.
   The custom view is now available in the selected category.

To edit a custom view:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to the existing event monitor custom view.
3. If you are editing the filters:
   a. Edit the filters in the toolbar and filter bar.
   b. From the view dropdown, select *Save*.
      Alternatively, you can select *Save as New Custom View* to save a new view.
4. If you are editing the custom view name, category, or visibility:
   a. From the view dropdown, select *Edit*.
      To delete the custom view, select *Delete*.
   b. In the *Edit Custom View* pane, configure the *Name*, *Category*, and *Public* visibility.
   c. Click *OK* to save the changes.

Understanding event statuses

In the *Event Monitor* dashboards, you can view the status of an event in the *Event Status* column. Event statuses include *Unhandled*, *Mitigated*, *Contained*, and *(blank)*.

Event statuses are applied by the associated event handler. When creating a custom event handler, you can manually select an event status or choose to allow FortiAnalyzer to decide.

In general, when *Allow FortiAnalyzer to choose* is selected, the event status for UTM events is applied based on the following:

Event status	Description
Unhandled	The security event risk is not mitigated or contained, so it is considered open. **Example**: an IPS/AV log with *action=pass* will have the event status *Unhandled*. Botnet and IoC events are also considered *Unhandled*.
Contained	The risk source is isolated. **Example**: an AV log with *action=quarantine* will have the event status *Contained*.
Mitigated	The security risk is mitigated by being blocked or dropped. **Example**: an IPS/AV log with *action=block/drop* will have the event status *Mitigated*.
(Blank)	Other scenarios.

Event handlers

Basic event handlers and correlation event handlers determine what events are generated from logs.

For basic event handlers, an event is generated when one of the rules in the event handler is met. Each rule in the basic event handler has an OR relationship with the others.

For correlation event handlers, an event is generated when a set of rules are met in correlation sequence. For correlation handlers, you can define both the rules and the operators (AND, AND_NOT, OR, FOLLOWED_BY, and NOT_FOLLOWED_BY).

There are predefined event handlers for FortiGate, FortiSandbox, FortiMail, and FortiWeb devices. In a Security Fabric ADOM, all predefined event handlers are displayed. Some predefined event handlers are disabled by default, but you can enable them from the GUI.

You can also create your own custom event handlers. An easy way to create a custom event handler is to clone a predefined event handler and customize its settings.

Data selectors and notification profiles are configured separately from event handlers, and then selected as part of configuring predefined or custom event handlers as needed. Data selectors determine which devices, subnets, and filters to use for the handler, and notification profiles determine if and where to send alert

notifications when an event is generated by the handler. These groupings promote reusability, which results in increased efficiency and a reduction in human error when configuring event handlers.

When ADOMs are enabled, each ADOM has its own event handlers and list of events. Ensure you are in the correct ADOM when working in *Incidents & Events*. You can import and export the event handlers, allowing you to develop custom event handlers and deploy them in bulk to other ADOMs or FortiAnalyzer units, if needed.



Event handlers generate events only from Analytics logs and not Archive logs. For more information, see Analytics and Archive logs.

In an Analyzer–Collector collaboration scenario, the Analyzer evaluates the event handlers. For more information, see Analyzer–Collector collaboration.

In *Incidents & Events* > *Handlers*, you can manage the *Data Selectors*, *Notification Profiles*, *Basic Handlers*, and *Correlation Handlers* separately.

In this section, you will find the following topics:

- Predefined basic event handlers on page 232
- Predefined correlation event handlers on page 266
- Creating data selectors on page 316
- Creating notification profiles on page 317
- Creating a custom event handler on page 298
- Creating a custom correlation handler on page 304
- Using the Automation Stitch for event handlers on page 310
- Using the Generic Text Filter on page 311
- Managing event handlers on page 312
- Enabling event handlers on page 313
- Cloning event handlers on page 314
- Resetting predefined event handlers to factory defaults on page 314
- Importing and exporting event handlers on page 314

Predefined basic event handlers

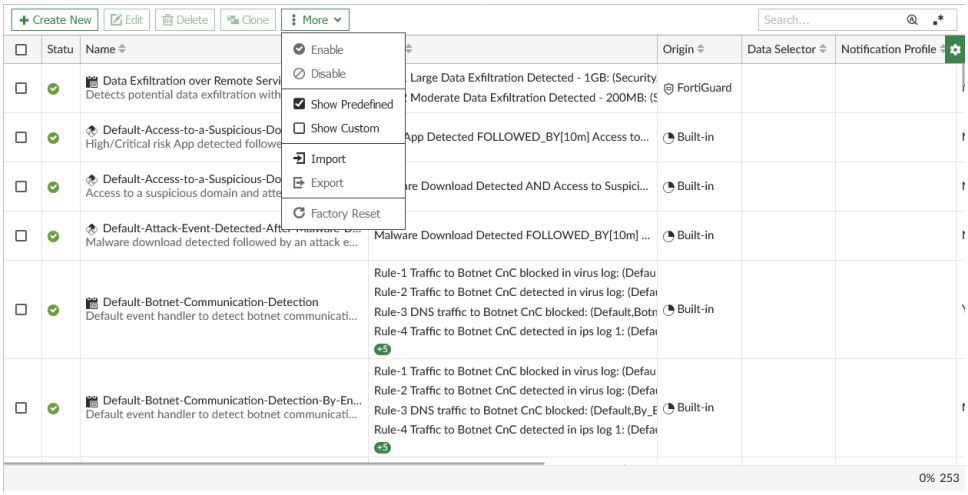
FortiAnalyzer includes many predefined event handlers that you can use to generate events. You can easily create a custom event handler by cloning a predefined event handler and customizing its settings. See Cloning event handlers on page 314.

If you wish to recieve notifications from a pedefined event handler, configure a notification profile and assign it to the event handler. See Creating notification profiles on page 317.



In 6.2.0 and up, predefined event handlers have been consolidated and have multiple rules that can be enabled or disabled individually.

To view predefined event handlers in the FortiAnalyzer GUI, go to *Incidents & Events > Event Handlers > Event Handlers*. From the *More* dropdown, select *Show Predefined*. The predefined event handlers display with *Origin = Built-in*. An icon in the *Name* column indicates if the event handler is a basic event handler or a correlation event handler. For more information about correlation event handlers, see Predefined correlation event handlers on page 266.



The following are a small sample of FortiAnalyzer predefined basic event handlers.

Event Handler	Description
Default-Compromised-Host-Detection-IOC-By-Threat	Default event handler to detect compromised hosts by FortiAnalyzer IOC feature grouped by threat. Enabled by default MITRE Tech IDs: • T1071.001 Web Protocols • T1071.004 DNS • T1041 Exfiltration Over C2 Channel **Rule 1: Traffic to CnC detected** • Event Severity: Critical • Log Device Type: FortiGate • Log Type: Traffic Log > Any • Log Field: Destination IP, Endpoint • Log messages that match all of the following filters: • *tdtype~infected* • Event Status: Unhandled • Tags: IP, C&C, Ioc_Rescan • Custom Message: Traffic to C&C:${dstip}, Traffic path: PolicyID ${policyid}\${dstintf}\${dstip}:${dstport} **Rule 2: Web traffic to CnC detected** • Event Severity: Critical • Log Device Type: FortiGate • Log Type: Web Filter

Event Handler	Description

	• Log Field: Hostname URL, Source Endpoint
	• Log messages that match all of the following filters:
	  • *tdtype~infected*
	• Event Status: Unhandled
	• Tags: C&C, URL, Ioc_Rescan
	• Custom Message: Traffic to C&C:${hostname}, Traffic path: PolicyID ${policyid}\${dstintf}\${dstip}:${dstport}
	Rule 3: DNS traffic to CnC detected
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: DNS Log
	• Log Field: QNAME, Source Endpoint
	• Log messages that match all of the following filters:
	  • *tdtype~infected*
	• Event Status: Unhandled
	• Tags: C&C, Domain, Ioc_Rescan
	• Custom Message: Traffic to C&C:${qname}, Traffic path: PolicyID ${policyid}\${dstintf}\${dstip}:${dstport}
	Rule 4: Traffic to CnC event detected by FortiGate
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: Event Log > System
	• Log Field: Source IP
	• Log messages that match all of the following filters:
	  • *logid==0100020214*
	• Event Status: Unhandled
	• Tags: C&C
	• Custom Message: FGT detected traffic to IOC location, from the source ip:${srcip}

Default-Data-Leak-Detection-By-Threat	Default data leak detection handler grouped by threat. Disabled by default MITRE Tech ID: • T1005 Data from Local System **Rule 1: Data leak detected** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: DLP • Log Field: Filter Category, Source Endpoint • Log messages that match all of the following filters: • *action==log-only* or *action==allow*

Event Handler	Description
	• Event Status: Unhandled • Tags: Signature, Leak • Custom Message: File:${filename} (Type:${filetype}, Size:${filesize}), Traffic path: PolicyID ${policyid}\${dstip}:${dstport} **Rule 2: Data leak blocked** • Event Severity: Low • Log Device Type: FortiGate • Log Type: DLP • Log Field: Filter Category, Source Endpoint • Log messages that match all of the following filters: • *action!=log-only* and *action!=allow* • Event Status: Mitigated • Tags: Signature, Leak • Custom Message: File:${filename} (Type:${filetype}, Size:${filesize}), Traffic path: PolicyID ${policyid}\${dstip}:${dstport}

Default-Sandbox-Detections-By-Endpoint	Default handler to track file submission and malware detection by FortiSandbox grouped by endpoint.
	Disabled by default
	MITRE Tech IDs:
	• T1041 Exfiltration Over C2 Channel
	Rule 1: Malware detected
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: AntiVirus
	• Log Field: Source Endpoint, Virus Name
	• Log messages that match all of the following filters:
	  • *logid==0211009235* or *logid==0211009237*
	• Event Status: Unhandled
	• Tags: Sandbox, Signature, Malware
	• Custom Message: Malware:${virus} with severity:${crlevel} found in file:${filename} from ${dstip}:${dstport}, Reference: ${ref}
	Rule 2: Malware blocked
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: AntiVirus
	• Log Field: Source Endpoint, Virus Name
	• Log messages that match all of the following filters:
	  • *logid==0211009234* or *logid==0211009236*
	• Event Status: Mitigated
	• Tags: Sandbox, Signature, Malware

Event Handler	Description
	• Custom Message: Malware:${virus} with severity:${crlevel} found in file:${filename} from ${dstip}:${dstport}, Reference: ${ref} **Rule 3: Sandbox detected Malware** • Event Severity: Critical • Log Device Type: FortiGate • Log Type: AntiVirus • Log Field: Source Endpoint • Log messages that match any one of the following filters: • *logid==0201009238* and *fsaverdict==malicious* • Event Status: Unhandled • Tags: Sandbox, Malware • Custom Message: File:${filename}, Traffic path: ${dstintf} (Policy:${policyid})\${dstip}:${dstport}, Checksum:${analyticscksum}

Default-Shadow-IT-Events	Default event handler to detect unsanctioned user, application and file exfiltration for cloud access.
	This event handler requires a FortiCASB connector configured on FortiAnalyzer. See Configuring security fabric connectors on page 372. This automatically creates the *Get Cloud Service Data (FortiCasb Connector)* playbook, which must be enabled for this event handler to generate events. See Playbooks on page 382.
	Disabled by default
	MITRE Tech ID:
	• T1011 Exfiltration Over Other Network Medium
	Rule 1: Unsanctioned Applications detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Application Control
	• Log Field: Source IP, Application Name
	• Log messages that match all of the following filters:
	  • *(siflags & 1) == 0 && siappid >=0*
	• Event Status: Unhandled
	• Tags: Unsanctioned_App
	• Custom Message: Unsanctioned application ${app} with app risk: ${apprisk} detected on: ${devname} with message: ${msg}
	Rule 2: File Exfiltration Attempts detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Application Control
	• Log Field: Source IP, Application Name
	• Log messages that match all of the following filters:
	  • *(siflags & 4) == 4*

Event Handler	Description
	• Event Status: Unhandled • Tags: File_Exfiltration • Custom Message: File exfiltration detected on: ${devname} with message: ${msg} **Rule 3: Unsanctioned Users detected** • Event Severity: High • Log Device Type: FortiGate • Log Type: Application Control • Log Field: Source IP, Application Name • Log messages that match all of the following filters: • *(siflags & 1) == 1 && (siflags & 2) == 0* • Event Status: Unhandled • Tags: Unsanctioned_User • Custom Message: Unsanctioned user: ${unauthuser} with app risk: ${apprisk} detected on: ${devname} with message: ${msg}
Local Device Event	Default local device event handler. Available only in the Root ADOM. Enabled by default Data Selector: Default Local Device Selector **Rule 1: Critical or important events** • Event Severity: Medium • Log Device Type: Local Device • Log Type: Event • Log Field: Log Description • Log messages that match the following filters: • *Level Greater Than or Equal To Warning* • Tags: System, Local
Default-NOC-Interface-Events	Event handler for FortiGate device type logs to generate events for vlan/interface status up or down, and DNS service on interface status. Disabled by default MITRE Tech ID: • T1489 Service Stop **Rule 1: Interface status changed to up** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *action="interface-stat-change"* and *status="UP"* • Tags: NOC, Interface • Custom message: Device ${devname}, status changed to ${status}

Event Handler	Description

	with message ${msg}.
	Rule 2: Interface status changed to down
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *action="interface-stat-change"* and *status="DOWN"*
	• Tags: NOC, Interface
	• Custom message: Device ${devname}, status changed to ${status} with message ${msg}.
	Rule 3: DNS server config added
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *cfgpath="system.dns-server"* and *action="Add"*
	• Tags: NOC, Interface, DNS
	• Custom Message: Device ${devname}, DNS server status changed with message ${msg}.
	Rule 4: DNS server config deleted
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match all of the following filters:
	  • *cfgpath="system.dns-server"* and *action="Delete"*
	• Tags: NOC, Interface, DNS
	• Custom Message: Device ${devname}, DNS server status changed with message ${msg}.

Default-NOC-FortiExtender-Events	Event handler for FortiGate device type logs to generate events for FortiExtender alerts, authorization and controller activity events. Disabled by default MITRE Tech ID: • T1499.001 OS Exhaustion Flood **Rule 1: FortiExtender Authorized** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > FortiExtender • Log Field: SN, Log Description

Event Handler	Description

	• Log messages that match any one of the following filters:
	  • *action="FortiExtender Authorized"*
	• Tags: NOC, FortiExtender
	• Custom message: Device: ${ip} ${action} with message: ${msg}
	Rule 2: Warning event detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > FortiExtender
	• Log Field: SN, Log Description
	• Log messages that match any one of the following filters:
	  • *level="warning"*
	• Tags: NOC, FortiExtender
	• Custom message: ${action} on ${ip} with message: ${msg}
	Rule 3: Alert event detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > FortiExtender
	• Log Field: SN, Log Description
	• Log messages that match any one of the following filters:
	  • *level="alert"*
	• Tags: NOC, FortiExtender
	• Custom message: ${action} on ${ip} with message: ${msg}
	Rule 4: Critical event detected
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: Event > FortiExtender
	• Log Field: SN, Log Description
	• Log messages that match any one of the following filters:
	  • *level="critical"*
	• Tags: NOC, FortiExtender
	• Custom message: ${action} on ${ip} with message: ${msg}
	Rule 5: Error event detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > FortiExtender
	• Log Field: SN, Log Description
	• Log messages that match any one of the following filters:
	  • *level="error"*
	• Tags: NOC, FortiExtender
	• Custom message: ${action} on ${ip} with message: ${msg}

Event Handler	Description

	Rule 6: Emergency event detected
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: Event > FortiExtender
	• Log Field: SN, Log Description
	• Log messages that match any one of the following filters:
	  • *level="emergency"*
	• Tags: NOC, FortiExtender
	• Custom message: ${action} on ${ip} with message: ${msg}
	Rule 7: FortiExtender controller activity detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > FortiExtender
	• Log Field: SN, Log Description
	• Log messages that match any one of the following filters:
	  • *logid="0111046401"* and *logdesc="FortiExtender controller activity"*
	• Tags: NOC, FortiExtender
	• Custom message: ${action} on ${ip} with message: ${msg}
	Rule 8: FortiExtender controller activity error detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > FortiExtender
	• Log Field: SN, Log Description
	• Log messages that match any one of the following filters:
	  • *logid="0111046402"* and *logdesc="FortiExtender controller activity error"*
	• Tags: NOC, FortiExtender
	• Custom message: ${action} on ${ip} with message: ${msg}

Default-NOC-Routing-Events	Event handler for FortiGate device type logs to generate events for changes in routing information including BGP Neighbor Status, Routing information change, OSFP Neighbor Status, Neighbor Table Changed and VRRP State Changed. Disabled by default **Rule 1: Routing information changed** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > Any • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *logdesc="Routing information changed"*

Event Handler	Description

	• Tags: NOC, Routing
	• Custom message: ${logdesc} on ${devname} with message ${msg}
	Rule 2: BGP neighbor status changed
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Router
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc="BGP neighbor status changed"*
	• Tags: NOC, Routing
	• Custom message: ${devname}. BGP neighbor status changed with message ${msg}
	Rule 3: OSPF or OSPF6 neighbor status changed
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Router
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="OSPF neighbor status changed"* OR *logdesc=="OSPF6 neighbor status changed"*
	• Tags: NOC, Routing
	• Custom message: ${logdesc} on ${devname} with message ${msg}
	Rule 4: Neighbor table changed
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Router
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="neighbor table change"*
	• Tags: NOC, Routing
	• Custom message: ${logdesc} on ${devname} with message ${msg}
	Rule 5: VRRP state changed
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Router
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="VRRP state changed"*
	• Tags: NOC, Routing
	• Custom message: ${logdesc} on ${devname} with message ${msg}

Event Handler	Description

Default-NOC-Network-Events	Event handler for FortiGate device type logs to generate network events including SNMP queries, routing information changes, DHCP server and status changes.
	Disabled by default
	Rule 1: Device SNMP query failed
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match all of the following filters:
	  • *logid="0100029021"* AND *logdesc="SNMP query failed"*
	• Tags: NOC, Network
	• Custom message: Device: ${devname} ${logdesc} with message: ${msg}
	Rule 2: Device routing information changed
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="Routing information changed"*
	• Tags: NOC, Network
	• Custom message: Device: ${devname} ${logdesc} with message: ${msg}
	Rule 3: DHCP client lease granted or usage high
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="DHCP client lease granted"* OR *logdesc=="DHCP lease usage high"* OR *logdesc=="DHCP lease usage full"*
	• Tags: NOC, Network
	• Custom message: DHCP status on Device ${devname} is ${logdesc} with message: ${msg}
	Rule 4: SNMP enabled
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:

Event Handler	Description
	• *cfgpath="system.snmp.sysinfo"* and *logdesc="Attribute configured"* and *cfgattr=status[disable->enable]* • Tags: NOC, Network • Custom message: Device ${devname} ${logdesc} ${cfgattr} with message ${msg}. **Rule 5: SNMP disabled** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *cfgpath="system.snmp.sysinfo"* and *logdesc="Attribute configured"* and *cfgattr=status[enable->disable]* • Tags: NOC, Network • Custom message: Device ${devname} ${logdesc} ${cfgattr} with message ${msg}. **Rule 6: DHCP server status changed** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description • Log messages that match all of the following filters: • *cfgpath="system.dhcp.server"* and *logdesc="Object attribute configured"* • Tags: NOC, Network • Custom message: DHCP server status change ${cfgattr} with message ${msg}. **Rule 7: DHCP lease renewed** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *dhcp_msg="Ack"* and *logdesc="DHCP Ack log"* • Tags: NOC, Network • Custom message: Host ${hostname} with message ${msg}. **Rule 8: DHCP lease released** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description

Event Handler	Description
	• Log messages that match all of the following filters: • *dhcp_msg="Release"* and *logdesc="DHCP Release log"* • Tags: NOC, Network • Custom message: Host ${hostname} with message ${msg}.

Default-NOC-Switch-Events	Event handler for FortiGate device type logs to generate events for Switch-Controller added/deleted or authorized/deauthorized, Switch-Controller Status, Interface flapping, LAG/MCLAG and split-brain status, Cable test/diagnosis and physical port up/down.
	Disabled by default
	MITRE Tech ID:
	• T1489 Service Stop
	Rule 1: Switch-Controller activity detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Message
	• Log messages that match all of the following filters:
	  • *(subtype="switch-controller")* and *(logdesc=="Switch-Controller discovered"* OR *logdesc=="Switch-Controller authorized"* OR *logdesc=="Switch-Controller deauthorized"* OR *logdesc=="Switch-Controller deleted"* OR *logdesc=="Switch-Controller warning")*
	• Tags: NOC, Switch, Controller
	• Custom message: ${logdesc}
	Rule 2: Vlan interface change has occurred
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc='FortiSwitch system'* and *msg~"interface vlan"*
	• Tags: NOC, Switch, Controller
	• Custom message: Device ${devname} interface vlan change with message: ${msg}
	Rule 3: Port switch detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Message
	• Log messages that match any one of the following filters:
	  • *logdesc="FortiSwitch link"* AND *msg~"switch port"*

Event Handler	Description

	• Tags: NOC, Switch, Controller
	• Custom message: ${logdesc} on Device: ${devname} with message: ${msg}
	Rule 4: Device flap detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Message
	• Log messages that match any one of the following filters:
	  • *msg~"flap"*
	• Tags: NOC, Switch, Controller
	• Default message
	Rule 5: Device LAG-MCLAG status change
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *msg~"lag"* OR *msg~"mclag"*
	• Tags: NOC, Switch, Controller
	• Custom message: Device: ${devname} LAG-MCLAG status update with message: ${msg}
	Rule 6: Device MCLAG split-brain detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *log_id=0115032695* and *msg~"MCLAG split-brain"*
	• Tags: NOC, Switch, Controller
	• Custom message: Device ${devname} ${msg}.
	Rule 7: Device cable diagnose detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *log_id=0115032699* and *msg~"CABLE DIAGNOSE"*
	• Tags: NOC, Switch, Controller
	• Custom message: Device ${devname} ${msg}.

Event Handler	Description

	Rule 8: Device come up detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *log_id=="0115032695"* and *msg~"come up"*
	• Tags: NOC, Switch, Controller
	• Custom message: Device ${devname} ${msg}.
	Rule 9: Device gone down detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Any
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *log_id=="0115032695"* and *msg~"gone down"*
	• Tags: NOC, Switch, Controller
	• Custom message: Device ${devname} ${msg}.

Default-NOC-HA-Events	Event handler for FortiGate device type logs to generate events for HA cluster updates and alerts including HA Device interface failure, Cluster Priority Changed, cluster member state moved, device interface down, HA device syncronization status, connection to FortiAnalyzer status, FortiManager tunnel connection status and connection with CSF member status. Disabled by default MITRE Tech ID: • T1489 Service Stop **Rule 1: HA device interface failed** • Event Severity: High • Log Device Type: FortiGate • Log Type: Event > HA • Log Field: Device Name, Message • Log messages that match any one of the following filters: • *logdesc=="HA device interface failed"* and *logid=="0108037898"* • Tags: NOC, HA, Cluster • Default message **Rule 2: Device set as HA primary** • Event Severity: High • Log Device Type: FortiGate • Log Type: Event > HA • Log Field: Device Name, Log Description

Event Handler	Description

	• Log messages that match any one of the following filters:
	  • *logdesc=="Device set as HA primary"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device: ${devname} has been set to HA Primary with msg: ${msg}
	Rule 3: Cluster state moved or Heartbeat device interface down
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > HA
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="Virtual cluster member state moved"* OR *logdesc=="Heartbeat device interface down"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device: ${devname} ${logdesc} with HA role: ${ha_role}
	Rule 4: Synchronization activity detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > HA
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="HA secondary synchronization failed"* OR *logdesc=="Secondary sync failed"* OR *logdesc="Synchronization status with master"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device: HA synchronization status for Device: ${devname} ${logdesc}. Message: ${msg}. Status is: ${sync_status}
	Rule 5: FortiAnalyzer connection up
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *action="connect"* and *status="success"* and *logdesc="FortiAnalyzer connection up"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device ${devname} ${msg}.
	Rule 6: FortiAnalyzer connection failed
	• Event Severity: High
	• Log Device Type: FortiGate

Event Handler	Description

	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that any one all of the following filters:
	  • *action="connect"* and *status="failure"* and *logdesc="FortiAnalyzer connection failed"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device ${devname} ${msg}.
	Rule 7: Upstream connection with CSF member established and authorized
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	• *direction="upstream"* and *logdesc="Connection with CSF member established and authorized"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device ${devname} ${msg}.
	Rule 8: Upstream connection with authorized CSF member terminated
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *direction="upstream"* and *logdesc="Connection with authorized CSF member terminated"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device ${devname} ${msg}.
	Rule 9: FortiManager tunnel connection up
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *action="connect"* and *status="success"* and *logdesc="FortiManager tunnel connection up"*
	• Tags: NOC, HA, Cluster
	• Custom message: Device ${devname} ${logdesc} with message - ${msg}.
	Rule 10: FortiManager tunnel connection down
	• Event Severity: High

Event Handler	Description
	• Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *action="connect"* and *status="failure"* and *logdesc="FortiManager tunnel connection down"* • Tags: NOC, HA, Cluster • Custom message: Device ${devname} ${logdesc} with message - ${msg}.

Default-NOC-Wireless-Events	Event handler for FortiGate device type logs to generate events for wireless wifi, AP updates and alerts including AP Status Change and Fake/Rogue AP detection, wireless client status change added/removed/allowed or denied status, signal to noise ratio (SNR) poor/fair/good, SSID status up/down.
	Disabled by default
	Rule 1: Fake AP detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: Device Name, SSID
	• Log messages that match any one of the following filters:
	  • *logid="0104043567"* AND *logdesc=="Fake AP detected"*
	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: ${logdesc}. SN: ${sndetected}
	Rule 2: Rogue AP detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: Device Name, SSID
	• Log messages that match any one of the following filters:
	  • *logid=="0104043563"* AND *logdesc=="Rogue AP detected"*
	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: ${logdesc}. SN: ${sndetected} with message: ${msg}
	Rule 3: Wireless event log id matched
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: Device Name, Message
	• Log messages that match any one of the following filters:
	  • *subtype="wireless"* AND (*logid=="0104043551"* OR *logid=="0104043552"* OR *logid=="0104043553"*)
	• Tags: NOC, Wireless, Wifi, AP

Event Handler	Description

	• Custom message: ${logdesc}. of AP: ${ap}
	Rule 4: Wireless client activity detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • (*logdesc=="Wireless client associated"* OR *logdesc=="Wireless client authenticated"* OR *logdesc=="Wireless client disassociated"* OR *logdesc=="Wireless client deauthenticated"* OR *logdesc=="Wireless client idle"* OR *logdesc=="Wireless client denied"* OR *logdesc=="Wireless client kicked"* OR *logdesc="Wireless client IP assigned"* OR *logdesc=="Wireless client left WTP"* OR *logdesc=="Wireless client WTP disconnected"*)
	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: ${logdesc} for ${ssid} with message: ${msg}
	Rule 5: Signal-to-noise ratio is poor
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: Device Name
	• Log messages that match any one of the following filters:
	  • *snr<="24"*
	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: SSID ${ssid}. has a poor quality SNR at ${snr} dB.
	Rule 6: Signal-to-noise ratio is fair
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: Device Name
	• Log messages that match any one of the following filters:
	  • *snr>="25"* and *snr<="40"*
	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: SSID ${ssid}. has fair quality SNR at ${snr} dB.
	Rule 7: Signal-to-noise ratio on is excellent
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: Device Name
	• Log messages that match any one of the following filters:
	  • *snr>="41"*

Event Handler	Description

	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: SSID ${ssid}. has excellent quality SNR at ${snr} dB.
	Rule 8: Physical AP radio ssid up
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: SSID, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc="Physical AP radio ssid up"* and *action="ssid-up"*
	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: Device ${sn} SSID status change with message ${msg}.
	Rule 9: Physical AP radio ssid down
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > Wireless
	• Log Field: SSID, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc="Physical AP radio ssid down"* and *action="ssid-down"*
	• Tags: NOC, Wireless, Wifi, AP
	• Custom message: Device ${sn} SSID status change with message ${msg}.

Default-NOC-Security-Events	Event handler for FortiGate device type logs to generate events for security events including Admin Logins failed or disabled, Admin or Admin Monitor Disconnected, Admin password expired and UTM Profile changes. Disabled by default **Rule 1: Admin login failed or desabled** • Event Severity: High • Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *logdesc=="Admin login failed"* OR *logdesc=="Admin login disabled"* OR *logdesc=="SSL VPN login fail"* • Tags: NOC, Security, Login, Password • Custom message: ${logdesc} for ${user} on device: ${devname} due to: ${reason} with message: ${msg} **Rule 2: Admin password expired** • Event Severity: High • Log Device Type: FortiGate • Log Type: Event > System

Event Handler	Description

	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="Admin password expired"*
	• Tags: NOC, Security, Login, Password
	• Custom message: Device: ${devname} ${logdesc} with message: ${msg}
	Rule 3: Admin disconnected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="Admin disconnected"* OR *logdesc=="Admin monitor disconnected"*
	• Tags: NOC, Security, Login, Password
	• Custom message: ${logdesc} on device: ${devname} with message: ${msg}
	Rule 4: AV or IPS change detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="AV updated by admin"* OR *logdesc=="IPS package - Admin update successful"* OR *logdesc=="AV package update by SCP failed"* OR *logdesc=="IPS package failed to update via SCP"* OR *logdesc=="IPS custom signatures backup failed"*
	• Tags: NOC, Security, Login, Password
	• Custom message: Device: ${devname} ${logdesc} with message: ${msg}

Default-NOC-Fabric-Events	Event handler for FortiAnalyzer and FortiGate log device type to detect Fabric events, including device offline, CSF member connection status down or terminated, CSF member configuration changes, automation stitch triggered , licenses that are expiring or failed updates. Disabled by default MITRE Tech ID: • T1529 System Shutdown/Reboot **Rule 1: Device offline detected** • Event Severity: High • Log Device Type: FortiAnalyzer • Log Type: Application Log

Event Handler	Description

	• Log Field: Logging Device Name, Message
	• Log messages that match any one of the following filters:
	  • *desc="Device offline"*
	• Tags: NOC, Fabric
	• Custom message: ${logdev_id} is offline
	Rule 2: FortiAnalyzer connection down detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Message
	• Log messages that match any one of the following filters:
	  • *logdesc="FortiAnalyzer connection down"*
	• Tags: NOC, Fabric
	• Default message
	Rule 3: Connection with authorized CSF member terminated
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Message
	• Log messages that match all of the following filters:
	  • *logdesc="Connection with authorized CSF member terminated"*
	• Tags: NOC, Fabric
	• Custom message: ${logdesc} on: ${devid} due to: ${reason}
	Rule 4: Automation stitch triggered
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc="Automation stitch triggered"*
	• Tags: NOC, Fabric
	• Custom message: ${logdesc} on: ${devname} with message: ${msg} and stitch action: ${stitchaction}
	Rule 5: Device license failed or expiring detected
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Message
	• Log messages that match any one of the following filters:
	  • *logdesc~"license failed"* OR *logdesc~"license expiring"*

Event Handler	Description

	• Tags: NOC, Fabric
	• Custom message: ${logdesc} on: ${devid}
	Rule 6: System update or failure detected
	• Event Severity: Critical
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Message
	• Log messages that match all of the following filters:
	  • *logdesc~"update"* AND *logdesc~"failed"*
	• Tags: NOC, Fabric
	• Custom message: ${logdesc} on: ${devname} with message: ${msg}
	Rule 7: Security fabric settings change detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="Settings modified by Security Fabric service"* OR *logdesc=="Looped configuration in Security Fabric service"* OR *logdesc=="Connection with CSF member established and authorized"* OR *logdesc=="Connection with authorized CSF member terminated"* OR *logdesc=="Serial number of upstream is changed"*
	• Tags: NOC, Fabric
	• Custom message: Device: ${devname} change with message: ${msg}

Default-NOC-System-Events	Event handler for FortiGate device type logs to generate events for system events including Power failure and device shutdown, High Resource usage (CPU, Mem, Storage), log device full status warnings and disk rolled, and devices entering/exiting conserve mode. Disabled by default MITRE Tech IDs: • T1496 Resource Hijacking • T1529 System Shutdown/Reboot **Rule 1: Device shutdown detected** • Event Severity: Critical • Log Device Type: FortiGate • Log Type: Event > System • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *logdesc="Device shutdown"* • Tags: NOC, System, Power, CPU, Memory, Storage

Event Handler	Description

	• Custom message: ${devname} experienced $logdesc with message: ${msg}
	Rule 2: Device conserve mode detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logid=="0100022011"* OR *logid=="0100022802"*
	• Tags: NOC, System, Power, CPU, Memory, Storage
	• Custom message: ${logdesc} on Device: ${devname} with message ${msg}
	Rule 3: Disk or memory is full
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logdesc=="Disk log full over first warning"* OR *logdesc=="Memory log full over first warning level"* OR *logdesc=="Memory log full over second warning level"* OR *logdesc=="Memory log full over final warning level"* OR *logdesc=="Disk full" OR logdesc=="Disk log rolled"* OR *logdesc=="Log disk full"*
	• Tags: NOC, System, Power, CPU, Memory, Storage
	• Custom message: Device: ${devname} ${logdesc} with message: ${msg}
	Rule 4: Device high CPU consumption detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *cpu>="80"*
	• Tags: NOC, System, Power, CPU, Memory, Storage
	• Custom message: ${devid} performance cpu: ${cpu}
	Rule 5: Device high memory consumption detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > System
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:

Event Handler	Description
	• *mem>="75"* • Tags: NOC, System, Power, CPU, Memory, Storage • Custom message: ${devid} performance memory: ${memory}
Default-NOC-VPN-Events	Event handler for FortiGate device type logs to generate events for VPN status changes including IPsec Phase1 error or failure, and Phase2 Up/Down and errors, Ipsec Tunnel Up/Down, VPN SSL login failures, IPSec ESP Error, IPsec DPD failures. Disabled by default MITRE Tech IDs: • T1133 External Remote Services • T1572 Protocol Tunneling **Rule 1: User SSL VPN login failed** • Event Severity: High • Log Device Type: FortiGate • Log Type: Event > VPN • Log Field: Device Name, Source End User • Log messages that match any one of the following filters: • *logid=="0101039426"* and *action=="ssl-login-fail"* • Tags: NOC, VPN • Custom message: ${logdesc} due to: ${reason} **Rule 2: IPsec phase 1 error or status fail detected** • Event Severity: High • Log Device Type: FortiGate • Log Type: Event > VPN • Log Field: Device Name, Message • Log messages that match any one of the following filters: • (*logid=="0101037124"* OR *logid=="0101037120"*) and (*logdesc=="IPsec phase 1 error"* OR *status="fail"*) • Tags: NOC, VPN • Custom message: ${logdesc} due to: ${status} with reason: ${reason} **Rule 3: IPsec ESP error detected** • Event Severity: High • Log Device Type: FortiGate • Log Type: Event > VPN • Log Field: Device Name, Message • Log messages that match any one of the following filters: • *logid=="0101037131"* and *logdesc=="IPsec ESP"* • Tags: NOC, VPN • Custom message: ${status} on: ${devname}, ${error_num} **Rule 4: IPsec DPD failed** • Event Severity: High

Event Handler	Description

	• Log Device Type: FortiGate
	• Log Type: Event > VPN
	• Log Field: Device Name, Message
	• Log messages that match any one of the following filters:
	  • *logid=="0101037136"* and *logdesc=="IPsec DPD failed"*
	• Tags: NOC, VPN
	• Custom message: ${msg} on device: ${devname}
	Rule 5: Device tunnel-up or tunnel-down detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > VPN
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logid="0101037138"* and (*action="tunnel-up"* or *action= "tunnel-down"*)
	• Tags: NOC, VPN
	• Custom message: ${msg} due to: ${action}
	Rule 6: IPsec phase 2 error detected
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > VPN
	• Log Field: Device Name, Message
	• Log messages that match any one of the following filters:
	  • *logid=="0101037125"* and *logdesc=="IPsec phase 2 error"*
	• Tags: NOC, VPN
	• Custom message: ${logdesc} due to: ${reason}
	Rule 7: Device phase2-up or phase2-down detected
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > VPN
	• Log Field: Device Name, Message
	• Log messages that any one all of the following filters:
	  • *logid=="0101037139"* and (*action=="phase2-up"* OR *action=="phase2-down"*)
	• Tags: NOC, VPN
	• Custom message: ${logdesc} due to: ${action}

Default-NOC-SD-WAN-Events	Event handler for FortiGate device type logs to generate events for SD-WAN status, alerts, and health check events including SLA targets/SLA met or not met for jitter, latency, packetloss, Health-check server status (alive or dead), status (up or down), and member status change. Disabled by default

Event Handler	Description

	MITRE Tech IDs:
	• T1499.002 Service Exhaustion Flood
	• T1529 System Shutdown/Reboot
	Rule 1: SLA failed for jitter
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match any one of the following filters:
	  • *subtype=="sdwan"* AND *metric=="jitter"* AND *msg~"SLA failed"*
	• Tags: NOC, SD-WAN
	• Custom message: On ${devname} the SLA for the ${healthcheck} failed for ${metric} with the current value of ${jitter} which violates the target ID ${slatargetid}.
	Rule 2: SLA failed for latency
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match any one of the following filters:
	  • *subtype=="sdwan"* AND *metric=="latency"* AND *msg~"SLA failed"*
	• Tags: NOC, SD-WAN
	• Custom message: On ${devname} the SLA for the ${healthcheck} failed for ${metric} with the current value of ${latency} which violates the target ID ${slatargetid}.
	Rule 3: SLA failed for packetloss
	• Event Severity: High
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match any one of the following filters:
	  • *subtype=="sdwan"* AND *metric=="packetloss"* AND *msg~"SLA failed"*
	• Tags: NOC, SD-WAN
	• Custom message: On ${devname} the SLA for the ${healthcheck} failed for ${metric} with the current value of ${packetloss} which violates the target ID ${slatargetid}.
	Rule 4: Device status changed to die
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN

Event Handler	Description

	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logid="0113022925"* AND *newvalue="die"*
	• Tags: NOC, SD-WAN
	• Custom message: Device: ${devname} with status ${newvalue}. ${msg}.
	Rule 5: Device status changed to alive.
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:
	  • *logid="0113022925"* AND *newvalue="alive"*
	• Tags: NOC, SD-WAN
	• Custom message: Device: ${devname} with status ${newvalue}. ${msg}.
	Rule 6: Device status is up
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match any one of the following filters:
	  • *logid="0113022925"* AND *status=="up"*
	• Tags: NOC, SD-WAN
	• Custom message: Device: ${devname} ${msg} status is ${status}.
	Rule 7: Device status is down
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match any one of the following filters:
	  • *logid="0113022925"* AND *status=="down"*
	• Tags: NOC, SD-WAN
	• Custom message: Device: ${devname} ${msg} status is ${status}.
	Rule 8: Number of pass member changed
	• Event Severity: Medium
	• Log Device Type: FortiGate
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Log Description
	• Log messages that match any one of the following filters:

Event Handler	Description
	• *logid="0113022923"* AND *msg="Number of pass member changed."* • Tags: NOC, SD-WAN • Custom message: ${msg} from ${oldvalue} to ${newvalue} for ${devname} **Rule 9: Member status changed** • Event Severity: Medium • Log Device Type: FortiGate • Log Type: Event > SD-WAN • Log Field: Device Name, Log Description • Log messages that match any one of the following filters: • *logid="0113022923"* AND *msg="Member status changed. Member out-of-sla."* • Tags: NOC, SD-WAN • Custom message: ${msg}. Member is now ${member} on ${devname}.
Default-NOC-Docker-Events	Event handler for FortiGate device type logs to generate events for Docker including inlcuding container enabled/disabled, CPU value set/max reached and MEM value set/max reached. Disabled by default **Rule 1: Memory report detected** • Event Severity: Medium • Log Device Type: FortiManager • Log Type: Event • Log Field: Type, Subtype • Log messages that match any one of the following filters: • *log_id=="0042010266"* and *msg~"MEM"* • Tags: NOC, Docker • Custom message: Device ${devname} with message ${msg}. **Rule 2: CPU report detected** • Event Severity: Medium • Log Device Type: FortiManager • Log Type: Event • Log Field: Type, Subtype • Log messages that match any one of the following filters: • *log_id=="0042010266"* and *msg~"CPU"* • Tags: NOC, Docker • Custom message: Device ${devname} with message ${msg}. **Rule 3: Status changed to disable** • Event Severity: Medium • Log Device Type: FortiManager • Log Type: Event

Event Handler	Description

	• Log Field: Type, Subtype
	• Log messages that match any one of the following filters:
	  • *log_id="0001010026"* and *changes~"status=disable"*
	• Tags: NOC, Docker
	• Custom message: Device ${devname} with changes ${changes}.
	Rule 4: Status changed to enable
	• Event Severity: Medium
	• Log Device Type: FortiManager
	• Log Type: Event
	• Log Field: Type, Subtype
	• Log messages that match any one of the following filters:
	  • *log_id="0001010026"* and *changes~"status=enable"*
	• Tags: NOC, Docker
	• Custom message: Device ${devname} with changes ${changes}.

ZTNA Brute Force Login	Detects various brute force login attempts in ZTNA environments.
	Enabled by default
	Rule 1: High Volume of Failed Authentications from Multiple Non-Existing Users
	Triggers an event when 100 or more non-existing users have failed authentications to a host name within 10 minutes.
	• Event Severity: Medium
	• Log Device Type: Fabric
	• Log Type: Normalized
	• Log Field: Host Name
	• Log messages that match all of the following filters:
	  • Data Source Type = FortiAuthenticator
	  • Event Sub Type = Authentication
	  • Event ID = 20101
	• Event Message: High volume of failed authentications from multiple non-existing users to host: $groupby1
	• Tags: ZTNA, Login, AccountDiscovery, BruteForce, CredentialSurfing
	Rule 2: Authentication Failed from Multiple Geo Locations
	Triggers an event when an existing account fails to authenticate from three or more different geo locations within five minutes.
	• Event Severity: High
	• Log Device Type: Fabric
	• Log Type: Normalized
	• Log Field: User ID
	• Log messages that match all of the following filters:
	  • Data Source Type = FortiAuthenticator

Event Handler	Description
	• Event Sub Type = Authentication • Event Profile contains AUTH_FAIL • UEBA User ID > 1024 • Event Message: Authentication failed from multiple geo locations for user: $groupby1 • Tags: ZTNA, Login, Geo, BruteForce **Rule 3: Brute Force Login Attack** Triggers an event when and existing user has 10 or more failed authentications with an event profile containing AUTH_FAIL_LOCK within 10 minutes. • Event Severity: Medium • Log Device Type: Fabric • Log Type: Normalized • Log Fields: User ID, Event Profile • Log messages that match all of the following filters: • Data Source Type = FortiAuthenticator • Event Sub Type = Authentication • Event Profile contains AUTH_FAIL • UEBA User ID > 1024 • Event Message: Brute force login attack for user: $groupby1 • Tags: ZTNA, Login, BruteForce **Rule 4: High Volume of Failed Authentications to Same Non-Existing User** Triggers an event when a non-existing user has at least 100 or more failed authentications within 1440 minutes (one day). • Event Severity: Medium • Log Device Type: Fabric • Log Type: Normalized • Log Field: User ID • Log messages that match all of the following filters: • Data Source Type = FortiAuthenticator • Event Sub Type = Authentication • Event ID = 20101 • Event Message: High volume of failed authentications for non-existing user: $groupby1 • Tags: ZTNA, Login, BruteForce, DoS
ZTNA Login Anomaly Detection	Detects various suspicious login scenarios in ZTNA environments. Enabled by default **Rule 1: Authentication to Multiple Services Failed** Triggers an event when a user has failed authentications to three or more services within 10 minutes.

Event Handler	Description

	• Event Severity: Medium
	• Log Device Type: Fabric
	• Log Type: Normalized
	• Log Field: User ID
	• Log messages that match all of the following filters:
	  • Data Source Type = FortiAuthenticator
	  • Event Sub Type = Authentication
	  • Event Profile contains AUTH_FAIL
	  • UEBA User ID > 1024
	• Event Message: Authentication to multiple services failed for user: $groupby1
	• Tags: ZTNA, Login, PrivilegeEscalation
	Rule 2: Successful Authentication from Multiple Geo Locations
	Triggers an event when a user has successful authentication from three or more unique geo locations within 10 minutes.
	• Event Severity: Critical
	• Log Device Type: Fabric
	• Log Type: Normalized
	• Log Field: User ID
	• Log Filter by Text:
	  • `data_sourcetype = 'FortiAuthenticator' and euid > 1024 and ((event_subtype = 'User' and event_profile = 'SAML_IDP_PORTAL_LOGIN') or (event_subtype = 'Authentication' and event_profile ~ 'AUTH_OK'))`
	• Event Message: Suspicious successful authentication from multiple geo locations for user: $groupby1
	• Tags: ZTNA, Login, Geo, ImpossibleTravel
	Rule 3: Successful Authentication from Multiple Endpoints
	Triggers an event when a user has successful authentication from five or more different host_IPs within 10 minutes.
	• Event Severity: High
	• Log Device Type: Fabric
	• Log Type: Normalized
	• Log Field: User ID, Host Name
	• Log Filter by Text:
	  • `data_sourcetype = 'FortiAuthenticator' and euid > 1024 and ((event_subtype = 'User' and event_profile = 'SAML_IDP_PORTAL_LOGIN') or (event_subtype = 'Authentication' and event_profile ~ 'AUTH_OK'))`
	• Event Message: Suspicious successful authentication from multiple endpoints for user: $groupby1 to host $groupby2
	• Tags: ZTNA, Login, LateralMovement

Event Handler	Description
	Rule 4: Successful Authentication from Sanctioned Countries Triggers an event when a user has at least one successful authentication from sanctioned countries within 10 minutes. • Event Severity: Medium • Log Device Type: Fabric • Log Type: Normalized • Log Field: User ID • Log Filter by Text: • `data_sourcetype='FortiAuthenticator' and euid>1024 and ((event_subtype='User' and event_profile='SAML_IDP_PORTAL_LOGIN') or (event_subtype='Authentication' and event_profile~'AUTH_OK')) and (src_geo_country='Russian Federation' or src_geo_country='Belarus' or src_geo_country='Iraq' or src_geo_country='Sri Lanka' or src_geo_country='Central African Republic' or src_geo_country='Syrian Arab Republic' or src_geo_country='Libyan Arab Jamahiriya' or src_geo_country='Korea, Democratic People\'s Republic of' or src_geo_country='Nicaragua' or src_geo_country='China' or src_geo_country~'Iran' or src_geo_country='Venezuela' or src_geo_country='Yemen' or src_geo_country='Lebanon' or src_geo_country='Myanmar' or src_geo_country~'Sudan' or src_geo_country~'Moldova' or src_geo_country~'Congo' or src_geo_country='Guatemala' or src_geo_country='Ukraine' or src_geo_country='Haiti' or src_geo_country='Somalia' or src_geo_country='Zimbabwe')` • Event Message: Successful authentication from sanctioned countries for user: $groupby1 • Tags: ZTNA, Login, Geo, PolicyViolation, Compliance

Below are examples of raw logs that would trigger the associated default event handler.

Default Event Handler	Example Log
Local Device Event	`id=6872390755323740160 itime=2020-09-14 10:06:03 euid=1 epid=1 dsteuid=1 dstepid=1 log_id=0034043006 subtype=logdb type=event level=warning time=10:06:03 date=2020-09-14 user=system action=delete msg=Requested to trim database tables older than 60 days to enforce the retention policy of Adom root. userfrom=system desc=Trim local db devid=FAZ-VMTM20001572 devname=FAZ-VMTM20001572 dtime=2020-09-14 10:06:03 itime_t=1600103163`
Default-Compromised Host-Detection-by IOC-By-Threat	`date=2020-09-20 time=07:41:20 id=6874471739997290516 itime=2020-09-20 00:41:20 euid=3 epid=1161 dsteuid=3 dstepid=101 type=utm subtype=ips level=warning sessionid=917509475 policyid=2 srcip=172.16.93.164 dstip=5.79.68.109 srcport=51392 dstport=80`

Default Event Handler	Example Log
	proto=6 logid=0421016399 service=HTTP eventtime=1537181449 crscore=30 crlevel=high srcintfrole=lan dstintfrole=wan direction=outgoing url=/ hostname=survey-smiles.com profile=default eventtype=malicious-url srcintf=95-FortiCloud dstintf=OSPF msg=URL blocked by malicious-url-list devid=FG100D3G02000011 vd=root dtime=2020-09-20 07:41:20 itime_t=1600587680 devname=FG100D3G02000011
Default-Risky-App-Detection-By-Threat	date=2020-09-20 time=07:41:23 id=6874471752882192399 itime=2020-09-20 00:41:23 euid=3 epid=1201 dsteuid=3 dstepid=101 type=utm subtype=app-ctrl level=information action=pass sessionid=3003333495 policyid=79 srcip=172.16.80.218 dstip=122.195.166.40 srcport=38625 dstport=26881 proto=6 logid=1059028704 service=tcp/26881 eventtime=1537399002 incidentserialno=603516169 crscore=5 crlevel=low direction=outgoing apprisk=high appid=6 srcintfrole=lan dstintfrole=wan applist=scan appcat=P2P app=BitTorrent eventtype=app-ctrl-all srcintf=80-software-r dstintf=port7 msg=P2P: BitTorrent_HTTP.Track, devid=FG100D3G02000011 vd=root dtime=2020-09-20 07:41:23 itime_t=1600587683 devname=FG100D3G02000011
Default_NOC_Routing_Events	date=2021-02-08 time=10:36:09 eventtime=1612809370040652208 tz="-0800" logid="0103027001" type="event" subtype="router" level="information" vd="root" logdesc="VRRP state changed" interface="port1" msg="VRRP vrid 200 vrip 172.17.200.200 changes state from Master to Backup due to ADVERTISEMENT with higherer priority received"

FortiOS system events

FortiOS predefined system event handlers are consolidated into a single event handler with multiple rules called *Default-FOS-System-Events*.

Events are organized by device in the *Incidents & Events* dashboards, which can be expanded to view all related events.

Default-FOS-System-Events rules apply tags to each event, allowing you to identify which *Default-FOS-System-Events* rule triggered the event.



If you are upgrading from a version before FortiAnalyzer 6.2.0, the existing legacy predefined handlers which are enabled or have been modified will be available as custom handlers. In the *Event Handler List*, select the *More* dropdown and choose *Show Custom*.

Predefined correlation event handlers

FortiAnalyzer includes some predefined correlation event handlers that you can use to generate events.

If you wish to recieve notifications from a pedefined correlation event handler, configure a notification profile and assign it to the correlation event handler. See Creating notification profiles on page 317.

To view predefined event handlers in the FortiAnalyzer GUI, go to *Incidents & Events > Event Handlers > Event Handlers*. From the *More* dropdown, select *Show Predefined*. The predefined event handlers display with *Origin = Built-in*. An icon in the *Name* column indicates if the event handler is a basic event handler or a correlation event handler. For more information about basic event handlers, see Predefined basic event handlers on page 232.

Predefined correlation event handlers are created for use cases to identify the following:

- C&C (Command and Control)
- Credential Access
- Defense Evasion
- Execution
- Exfiltration
- Initial Access
- Lateral Movement
- Persistence
- Privilege

The following are a small sample of FortiAnalyzer predefined correlation event handlers.

<table>
<tr><th>Correlation Handler</th><th>Description</th></tr>
<tr><td>Default-Suspicious-Traffic-From-Infected-Endpoint</td><td>This handler is to detect if an endpoint is infected and there is a large traffic from the same endpoint.
Enabled by default
Event Severity: Medium
Tags: C&C
Threshold Duration: 1440 minutes
Correlation Sequence:
Logic Group 1
<table><tr><th colspan="2">Traffic to Botnet CnC detected or blocked in virus log</th></tr><tr><td>Log Device Type</td><td>FortiGate</td></tr><tr><td>Log Type</td><td>Antivirus</td></tr><tr><td>Log Field</td><td>Source Endpoint</td></tr><tr><td>Log messages that match any of the following conditions:</td><td>• Log ID Equal To 0202009248
• Log ID Equal To 0202009249</td></tr></table></td></tr>
</table>

Correlation Handler	Description	
	Traffic to Botnet CnC detected or blocked in virus log	
	Trigger an event when:	A group contains 1 or more log occurences
	OR	
	Traffic to CnC detected	
	Log Device Type	FortiGate
	Log Type	Traffic Log > Any
	Log Field	Endpoint
	Log messages that match any of the following conditions:	*tdtype~infected*
	Trigger an event when:	A group contains 1 or more log occurences
	OR	
	Web traffic to CnC detected	
	Log Device Type	FortiGate
	Log Type	Web Filter
	Log Field	Source Endpoint
	Log messages that match any of the following conditions:	*tdtype~infected*
	Trigger an event when:	A group contains 1 or more log occurences
	OR	
	DNS traffic to CnC detected	
	Log Device Type	FortiGate
	Log Type	DNS Log
	Log Field	Source Endpoint
	Log messages that match any of the	*tdtype~infected*

Correlation Handler	Description
	DNS traffic to CnC detected
	following conditions:
	Trigger an event when: A group contains 1 or more log occurences
	FOLLOWED_BY, within *15m* Logic Group 2
	Traffic from endpoint
	Log Device Type: FortiGate
	Log Type: Traffic Log > Any
	Log Field: Endpoint
	Log messages that match any of the following conditions:
	Trigger an event when: The sum of `sentbyte` is greater than or equal to `100 Mega Byte`
	Correlation Criteria: • *Traffic to Botnet CnC detected or blocked in virus log endpoint = Traffic to CnC detected endpoint* • *Traffic to CnC detected endpoint = Web traffic to CnC detected endpoint* • *Web traffic to CnC detected endpoint = DNS traffic to CnC detected endpoint* • *DNS traffic to CnC detected endpoint = Traffic from endpoint endpoint*
Default-Brute-Force-Account-Login-Attack-FAZ	This handler is to detect if an account login failed many times not followed by a login success for FortiAnalyzer. Enabled by default MITRE Tech ID: • T1110.001 Password Guessing Event Severity: Medium Tags: Credential Access, login, attack Threshold Duration: 30 minutes Correlation Sequence:
	Login Failed 5 Times
	Log Device Type: FortiAnalyzer

<table>
<tr><th>Correlation Handler</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th colspan="2">Login Failed 5 Times</th></tr>
<tr><td>Log Type</td><td>Event Log</td></tr>
<tr><td>Log Field</td><td>Device ID</td></tr>
<tr><td>Log messages that match any of the following conditions:</td><td>Operation Equal To login failed</td></tr>
<tr><td>Trigger an event when:</td><td>A group contains 5 or more log occurences</td></tr>
</table>
NOT_FOLLOWED_BY, within 5m
<table>
<tr><th colspan="2">Login Success</th></tr>
<tr><td>Log Device Type</td><td>FortiAnalyzer</td></tr>
<tr><td>Log Type</td><td>Event Log</td></tr>
<tr><td>Log Field</td><td>Device ID</td></tr>
<tr><td>Log messages that match any of the following conditions:</td><td>Operation Equal To login</td></tr>
<tr><td>Trigger an event when:</td><td>A group contains 1 or more log occurences</td></tr>
</table>
Correlation Criteria:
Login Failed 5 Times devid = Login Success devid
</td></tr>
<tr><td>Default-Brute-Force-Account-Login-Attack-FGT</td><td>This handler is to detect if an account login failed many times not followed by a login success for FortiGate.
Enabled by default
MITRE Tech ID:
T1110.001 Password Guessing
Event Severity: Medium
Tags: Credential Access, login, attack
Threshold Duration: 1440 minutes
Correlation Sequence:
<table>
<tr><th colspan="2">Login Failed 5 Times</th></tr>
<tr><td>Log Device Type</td><td>FortiGate</td></tr>
<tr><td>Log Type</td><td>Event Log > System</td></tr>
</table>
</td></tr>
</table>

Correlation Handler	Description
	Login Failed 5 Times Log Field: Device ID Log messages that match any of the following conditions: Log ID Equal To 0100032002 Trigger an event when: A group contains 5 or more log occurences *NOT_FOLLOWED_BY*, within *5m* **Login-Success** Log Device Type: FortiGate Log Type: Event Log > System Log Field: Device ID Log messages that match any of the following conditions: Log ID Equal To 0100032001 Trigger an event when: A group contains 1 or more log occurences Correlation Criteria: • *Login Failed 5 Times devid = Login-Success devid*

Predefined event handler examples

The following section provides more details about use cases for select predefined event handlers. In addition to describing the event handler rule details, these topics will also briefly describe the required logs, log parsers, and the resulting events generated by the event handler.

The following examples are provided:

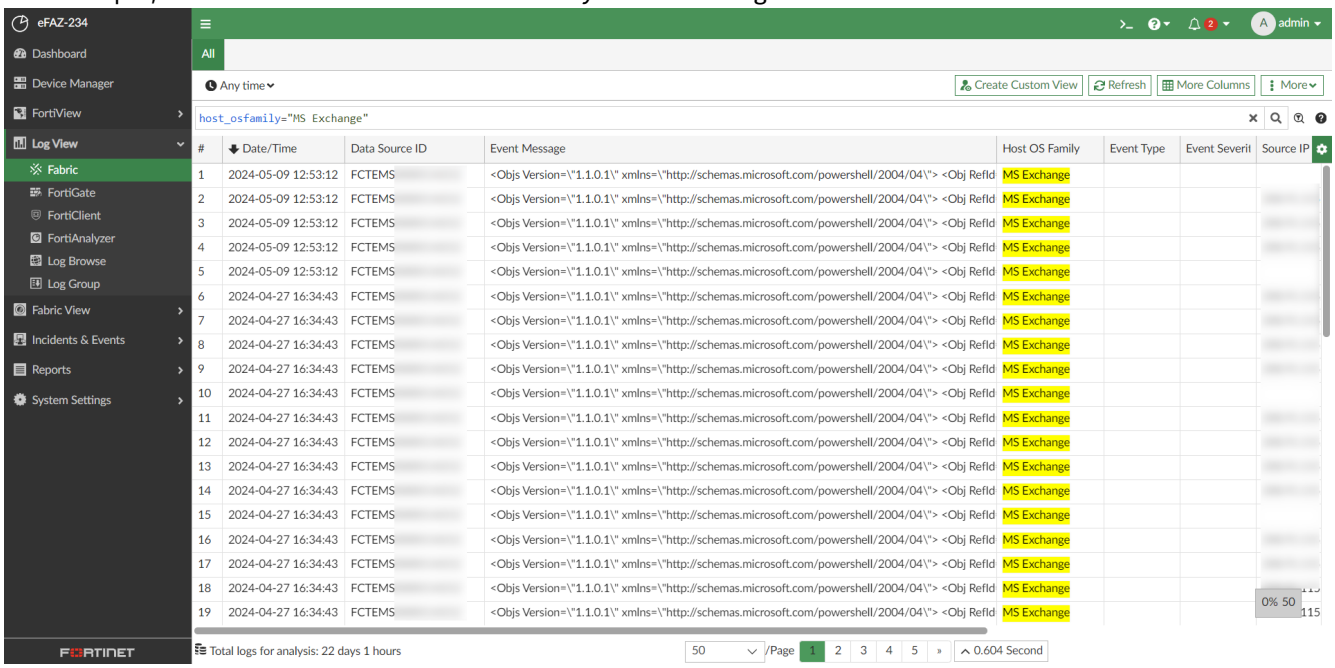
- MS Exchange Server event handlers on page 270
- Geo-alerting event handlers on page 275
- Excessive email sending event handler on page 289

MS Exchange Server event handlers

The predefined *Windows Event Log Parser* parses MS Exchange Server logs into the SIEM database. You can identify these Fabric logs by the *Host OS Family* in *Log View*. These logs are required for the event handlers

used in the examples in this topic.

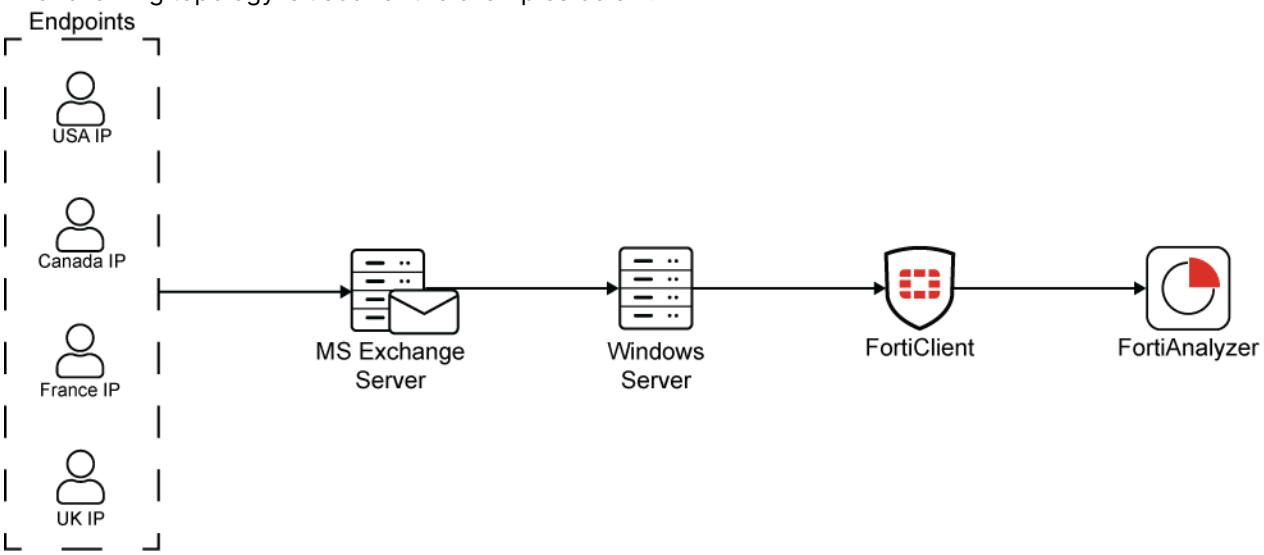
For example, see below where the *Host OS Family* is `MS Exchange`.



The following predefined event handlers are available to detect suspicious activities in the MS Exchange Server:

- MS Exchange - Large Email
- MS Exchange - Multiple Failed Deliveries
- MS Exchange - Suspicious Email Activity

The following topology is used for the examples below.



MS Exchange - Large Email

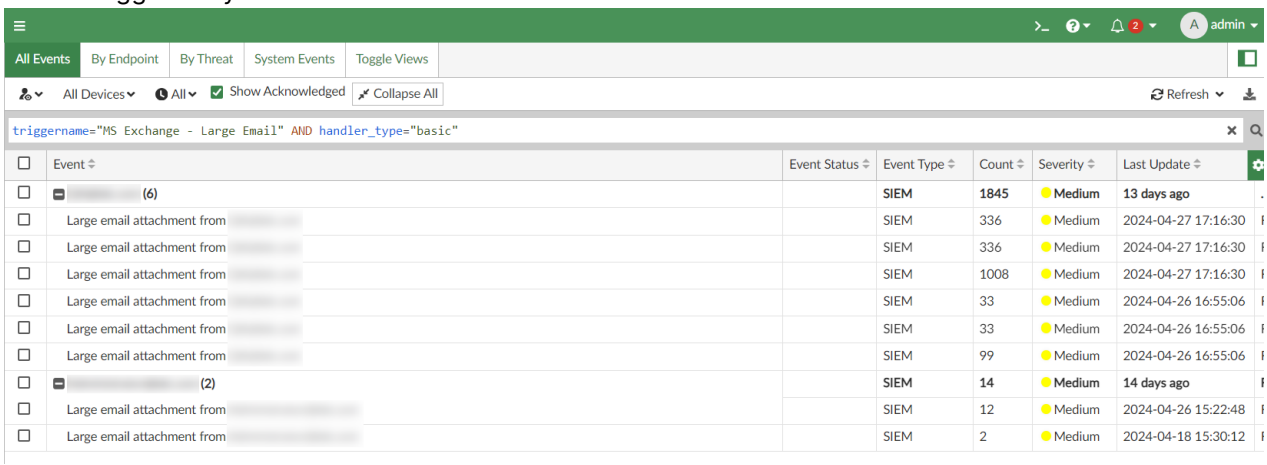
MS Exchange - Large Email is a basic event handler that uses MS Exchange Server logs to detect large email attachments (greater than 10485760 net sent bytes) being transported in the Microsoft Exchange Server.

This event handler uses the predefined data selector *Default Microsoft Exchange Transport Log* to ensure the proper devices and logs are used to trigger events.

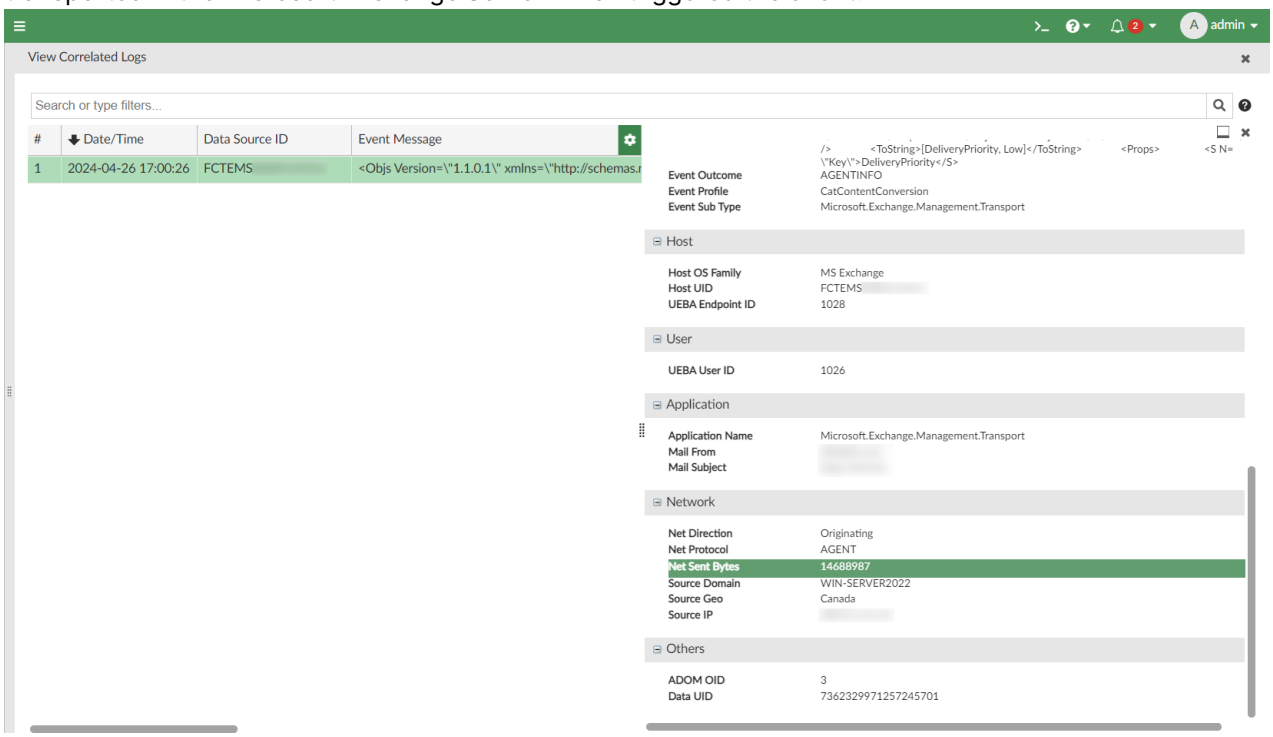
Rule details:

Rule	Description
Large Email Attachment Detected	Triggers an event when a large email attachment (greater than 10485760 net sent bytes) is being transported in the Microsoft Exchange Server. Event Severity: Medium Log Field: Mail From, Host Name Logs that match all of the following filters: • `Net Sent Bytes (net_sentbytes) > 10485760` Event Message: Large email attachment from $groupby1 Tags: MSExchange, Exfiltration Additional Info: From: ${groupby1}, Server: ${groupby2}

Events triggered by this event handler are visible in the *Event Monitor*:



You can double-click an event to view the related logs. In this example, there was 14688987 net sent bytes transported in the Microsoft Exchange Server which triggered the event.



MS Exchange - Multiple Failed Deliveries

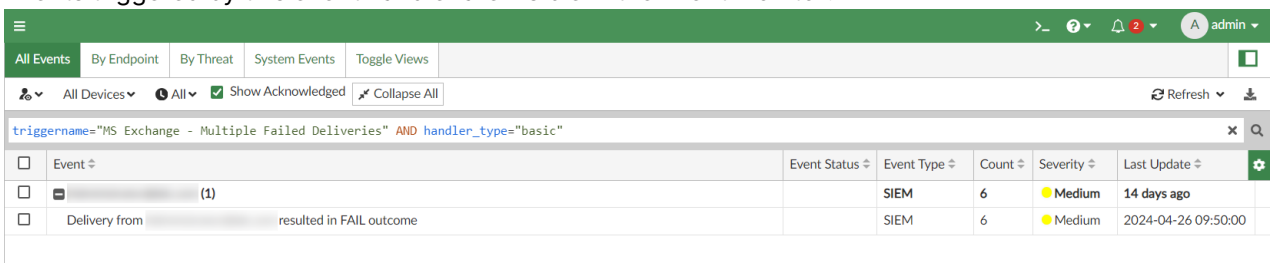
MS Exchange - Multiple Failed Deliveries is a basic event handler that uses MS Exchange Server logs to detect repeated delivery failures, including bounced messages, to the same recipient that exceeds a threshold. These events indicate potential issues with the recipient address or sender configuration.

This event handler uses the predefined data selector *Default Microsoft Exchange Transport Log* to ensure the proper devices and logs are used to trigger events.

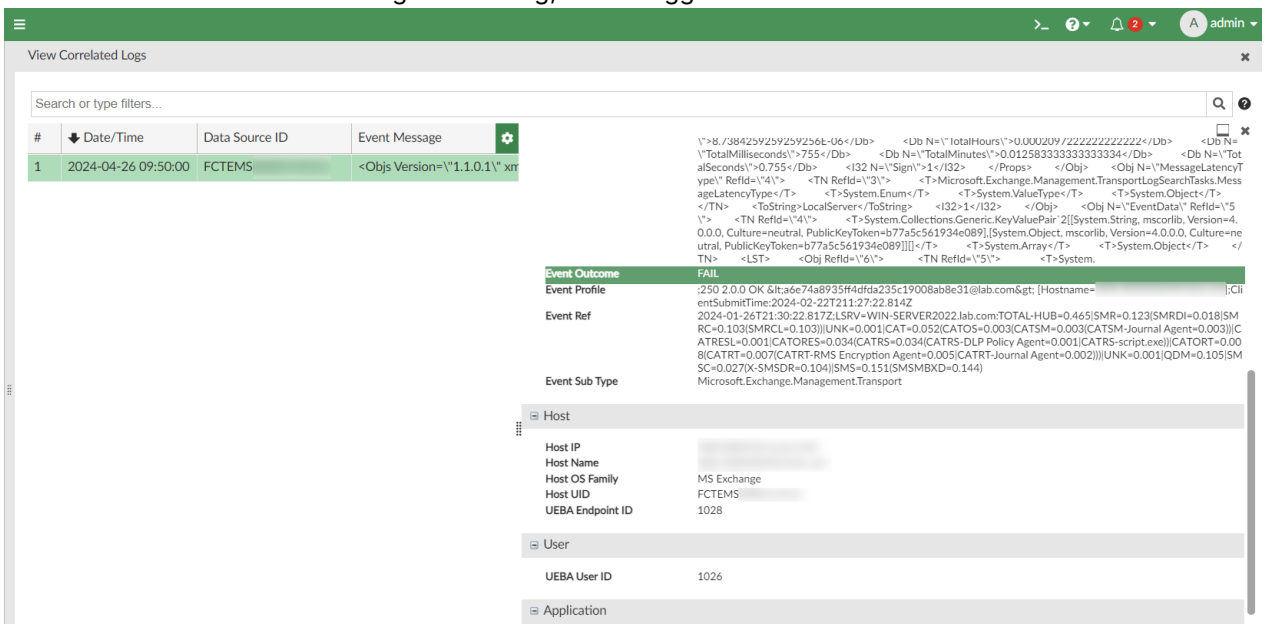
Rule details:

Rule	Description
Large Email Attachment Detected	Triggers an event when there are five or more failed or bounced deliveries in the MS Exchange Server within one hour. Event Severity: Medium Log Field: Mail From, Event Outcome Log Filter by Text: `event_outcome='FAIL' or event_outcome='DSN'` Event Message: Delivery from $groupby1 resulted in $groupby2 outcome Tags: MSExchange

Events triggered by this event handler are visible in the *Event Monitor*:



You can double-click an event to view the related logs. An email delivery is indicated as `FAIL` according to the event outcome in the MS Exchange Server log, which triggered the event.



MS Exchange - Suspicious Email Activity

MS Exchange - Suspicious Email Activity is a correlation event handler that detects five failed login attempts followed by email activity. These events may suggest that an attacker has successfully accessed the user account and is attempting to exploit access to the email system, possibly for data exfiltration, spreading malware, or conducting phishing attacks from a legitimate account.

This event handler uses the predefined data selector *Default Microsoft Windows Security and Exchange Transport Log* to ensure the proper devices and logs are used to trigger events.

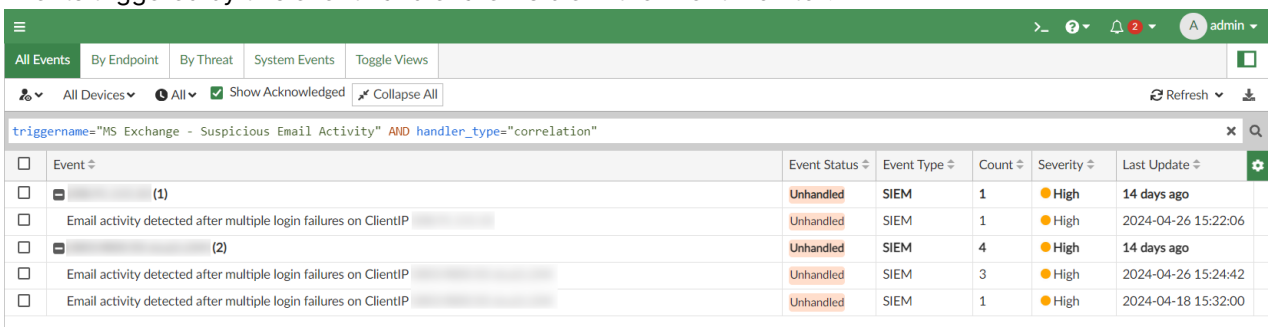
- Correlation: This event handler triggers an event when the rule *Login Failed 5 Times* is followed by *Email Activity Detected* within 10 minutes with a matching source IP.
- Rule details:

Rules	Description
Login Failed 5 Times	Triggered when there are five failed login attempts from the same source IP. Log Field: Source IP Logs that match all of the following filters:

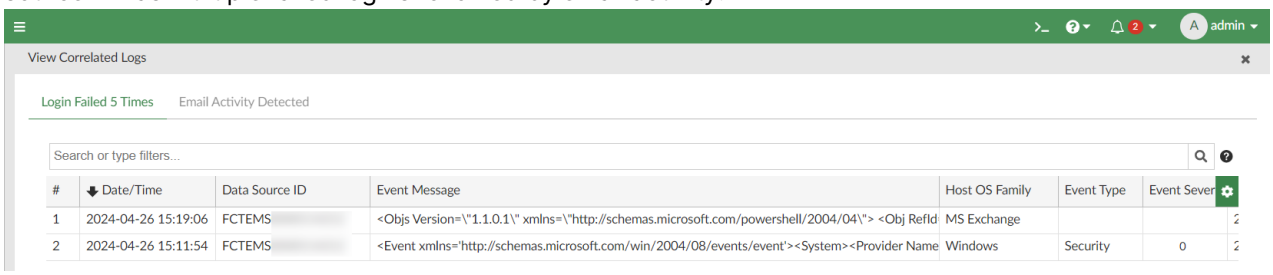
Rules	Description
	• `Event ID (event_id) = 4625`
Email Activity Detected	Triggered when there is email activity from the matching source IP within 10 minutes of the previous rule being triggered. Log Field: Source IP Logs that match all of the following filters: • `Event Outcome (event_outcome) = SEND`

- Event message: Email activity detected after multiple login failures on ClientIP ${Login Failed 5 Times.groupby1}
- Event Severity: High
- Tags: MSExchange, CredentialAccess, LateralMovement

Events triggered by this event handler are visible in the *Event Monitor*:



You can double-click an event to view the related logs. The logs that triggered each rule in the correlation sequence can be viewed in the respective tabs: *Login Failed 5 Times* and *Email Activity Detected*. The same source IP has multiple failed logins followed by email activity.



Geo-alerting event handlers

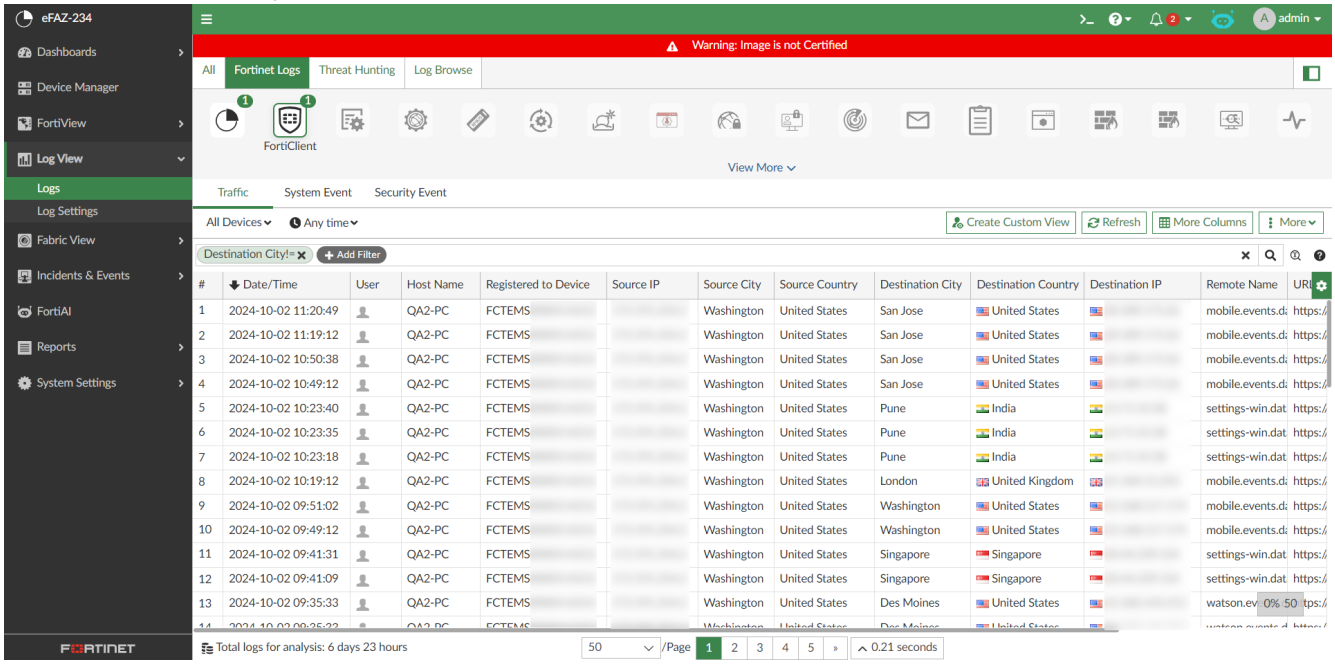
This topic describes the related logs and predefined event handlers that can be used for geo-alerting. These can be helpful for threat detection in scenarios such as multiple authentications to the same account from different geo locations or impossible travel between logins, indicating a likely breach.

The predefined event handler rules that are created for geo-alerting rely on the following fields, which are available for all log types:

- Source City (`srccity`)
- Destination City (`dstcity`)

- Source Country (`srccountry`)
- Destination Country (`dstcountry`)

These fields depend on the IP. When the IP is a public IP, the related city and country will display in the fields listed above. For example, see below.

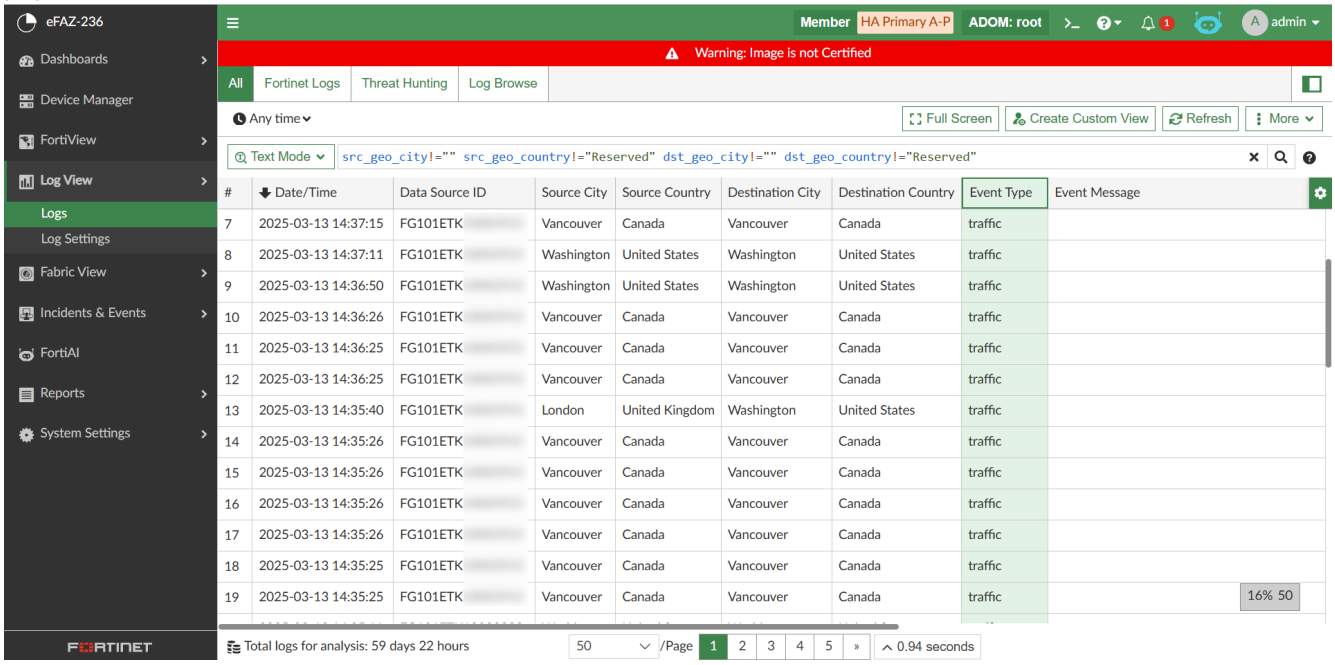


In other scenarios, the fields are displayed as follows:

- When the IP is invalid, these fields are empty.
- When there is no IP, these fields are empty.
- When the IP is a private IP, these fields display *Reserved*.

These source and destination fields can also be parsed to Fabric logs in the SIEM database. All predefined log parsers are updated to parse the `srccity`, `dstcity`, `srccountry`, and `dstcountry` fields into the normalized SIEM fields `src_geo_city`, `src_geo_country`, `dst_geo_city`, and `dst_geo_country` in Fabric logs.

For example, see the Fabric logs with *Source City*, *Source Country*, *Destination City*, and *Destination Country* populated in the table view.



The following predefined event handler includes multiple rules to detect suspicious login activities from different IPs/Countries:

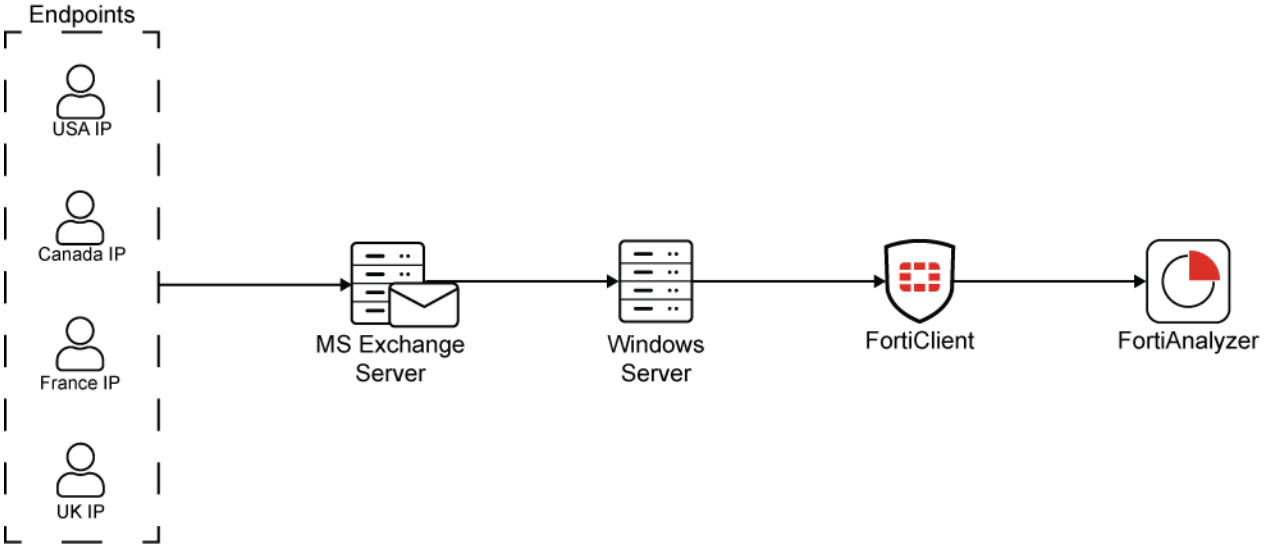
- Default-Multiple-Authentications-to-the-Same-Account

In addition to the event handler above, the following predefined event handler includes one rule for geo alerting as well:

- ZTNA Login Anomaly Detection: Impossible Travel Login Detection

These event handlers are enabled by default. They use normalized Fabric logs to detect events.

The following topology was used for the examples below.



Default-Multiple-Authentications-to-the-Same-Account

Default-Multiple-Authentications-to-the-Same-Account is a basic event handler detects multiple failed or successful authentication attempts to the same network device or domain using the same account but originating from different IP addresses or geo locations.

This event handler uses the predefined data selector *Default Microsoft Windows Security Auditing Log* to ensure the proper devices and logs are used to trigger events.

MITRE coverage:

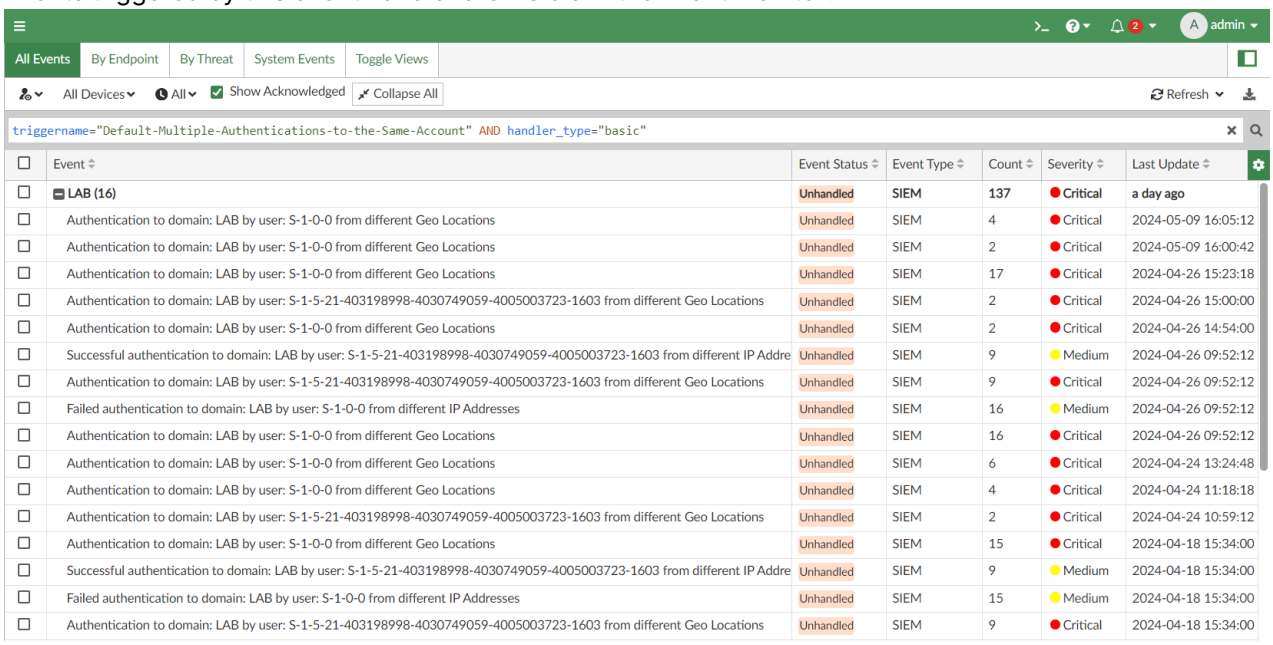
- MITRE Tech ID = T1078 Valid Accounts.

Rule details:

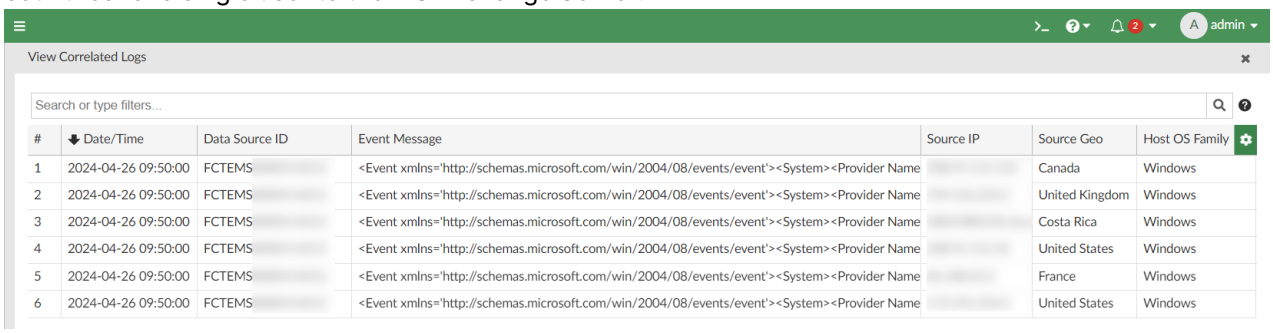
Rules	Description
Authentication to the Same Device from Different Public IPs	Triggers an event when a user has four failed or successful authentications to the same device from different public IPs within 30 minutes. Event Severity: Medium Log Field: Host Name, User Name Log Filter by Text: `(event_id = '4624' or event_id = '4625') and src_geo != '0' and src_geo != '1000000000'` Event Message: Authentication attempts on host: $groupby1 by user: $groupby2 from different public IP addresses Tags: ValidAccounts Additional Info: Authentication for application: ${app_ref}  Using Windows logs, event ID 4624 indicates a successful login and event ID 4625 indicates a failed login.
Authentication to the Same Domain from Different Public IPs	Triggers an event when a user has four failed or successful authentications to the same domain from different public IPs within 30 minutes. Event Severity: Medium Log Field: Destination Domain, User Name Log Filter by Text: `(event_id = '4624' or event_id = '4625') and src_geo != '0' and src_geo != '1000000000'` Event Message: Authentication attempts to domain: $groupby1 by user: $groupby2 from different public IP Addresses Tags: ValidAccounts Additional Info: Authentication for application: ${app_ref}
Authentication to the Same Device from Different Geo Locations	Triggers an event when a user has three failed or successful authentications to the same device from different countries within one hour.

Rules	Description
	Event Severity: Critical Log Field: Host Name, User Name Log Filter by Text: `(event_id = '4624' or event_id = '4625') and src_geo != '0' and src_geo != '1000000000'` Event Message: Authentication attempts on host: $groupby1 by user: $groupby2 from different Geo Locations Tags: ValidAccounts Additional Info: Authentication for application: ${app_ref}
Authentication to the Same Domain from Different Geo Locations	Triggers an event when a user has three failed or successful authentications to the same domain from different countries within one hour. Event Severity: Critical Log Field: Destination Domain, User Name Log Filter by Text: `(event_id = '4624' or event_id = '4625') and src_geo != '0' and src_geo != '1000000000'` Event Message: Authentication attempts to domain: $groupby1 by user: $groupby2 from different Geo Locations Tags: ValidAccounts Additional Info: Authentication for application: ${app_ref}

Events triggered by this event handler are visible in the *Event Monitor*:



You can double-click an event to view the related logs. In this example, there is login activity from multiple countries for a single user to the MS Exchange Server.



ZTNA Login Anomaly Detection: Impossible Travel Login Detection

You can find the *Impossible Travel Login Detection* rule in the predefined *ZTNA Login Anomaly Detection* event handler.

For this rule to trigger events, you must also have a FortiAuthenticator configured in your network and logging to FortiAnalyzer.

Rule details:

Rule	Description

Impossible Travel Login Detection	Event Severity: High
	Log Field: UEBA User ID
	Log Filter by Text:
	`data_sourcetype='FortiAuthenticator' and euid>1024 and app_state='Success' and event_subtype='Authentication' and event_action='Authentication'`
	Trigger an event when (*Advanced Mode*):
	`GEO_DISTANCE(1, 'km') alias geo_distance > TIME_DIFF(1, 'hour') alias time_diff * (geo_distance > 400 ? then 1400 else 100) and geo_distance > 200 and time_diff > 0.1 and not logins_with_mfa and not logins_from_usual_ip`
	Event Type Override: Auth
	Event Message: Impossible travel login detected for user: ${event.user_name}
	Event Status: Unhandled
	Tags: ZTNA, Login, Geo, ImpossibleTravel, Auth
	Indicators:

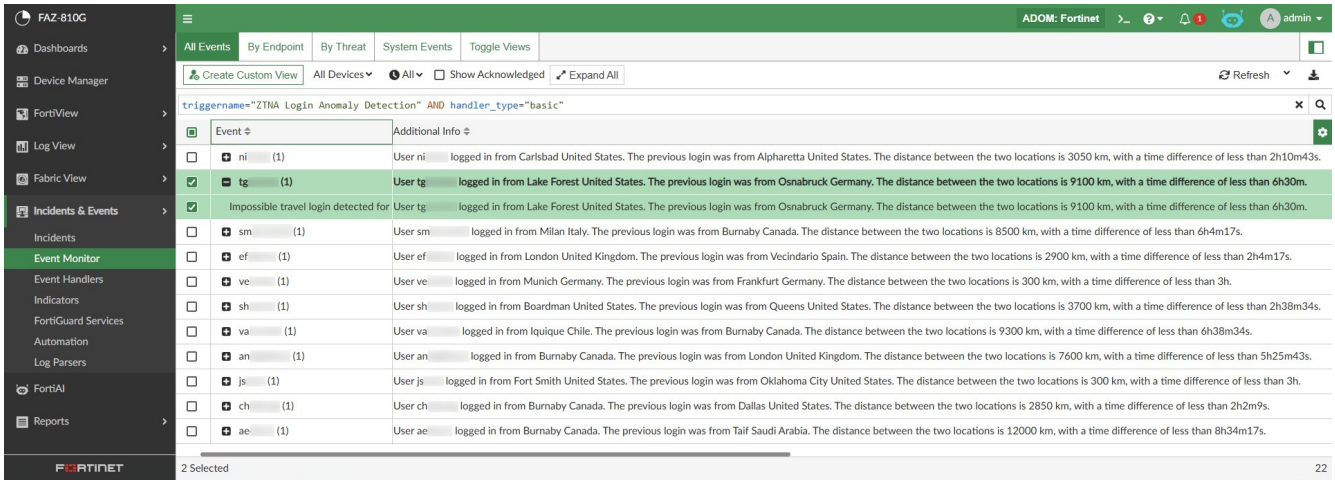
Rule	Description
	<table><tr><th>Log field</th><th>Indicator Type</th><th>Count</th></tr><tr><td>${src_geo_city} ${src_geo_country}</td><td>Others</td><td>6</td></tr><tr><td>Source IP (src_ip)</td><td>IP</td><td>6</td></tr></table> Additional Info: User ${event.user_name} logged in from ${event.src_geo_city} ${event.src_geo_country}. The previous login was from ${last_event.src_geo_city} ${last_event.src_geo_country}. The distance between the two locations is ${rule.alias.geo_distance}, with a time difference of less than ${event.time_diff_threshold}.

The table below describes the individual conditions set in *Advanced Mode* to trigger an event. All of the conditions must be met to trigger an event.

Condition	Description
Geo Distance vs. Speed Threshold	Criteria: `geo_distance > time_diff * (geo_distance > 400 ? then 1400 else 100)` The geo distance between two logins (geo_distance) must exceed the product of the time difference (time_diff) and an adaptive speed threshold: • If geo_distance greater than 400km, then the allowed speed is up to 1400 km/h. • If geo_distance less than or equal to 400km, then the allowed speed is up to 100 km/h. You can clone and edit the event handler to change the following: • The distance unit (default = km). This can be changed to mile. • The velocity_distance threshold integer (default = 400). If larger than <integer>, use velocity_high, otherwise use velocity_low. • The velocity_high integer (default = 1400). • The velocity_low integer (default = 100).
Minimum Geo Distance	Criteria: `geo_distance > 200` To avoid triggering events for short-range travel, the geo distance must be greater than 200km. This integer (200) can be edited in a cloned event handler.
Minimum Time Difference	Criteria: `time_diff > 0.1` The time difference between the two login events must be greater than 0.1 hour (approximately 6 minutes). This float (0.1) can be edited in a cloned event handler.
Not logins with token	Criteria: `not logins_with_mfa` Logins using a token will not be considered. This criteria can be removed in a cloned event handler.
Not from a usual IP	Criteria: `not logins_from_usual_ip`

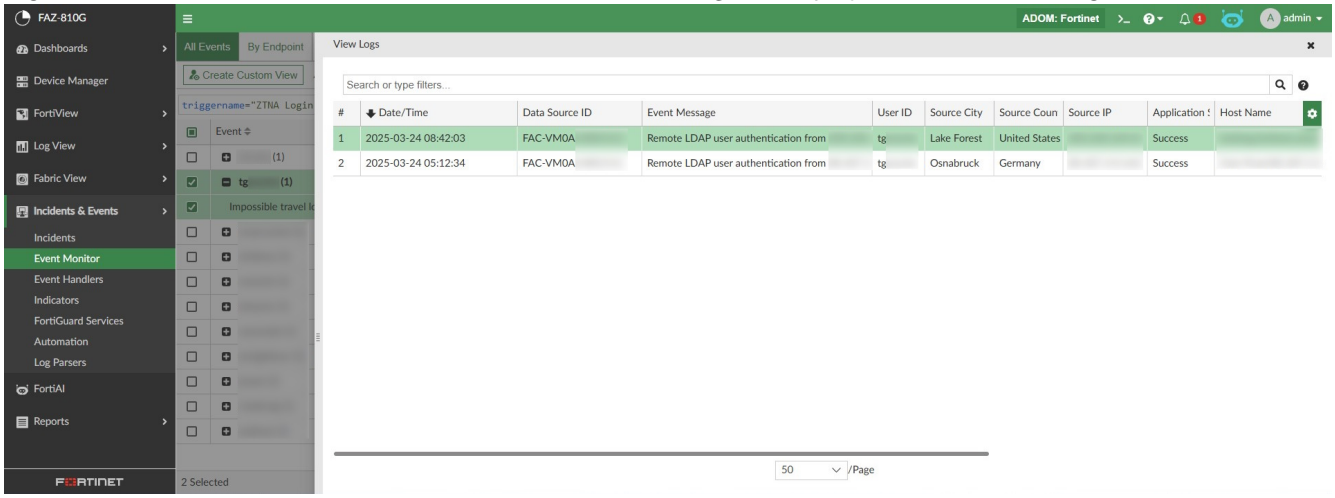
Condition	Description
	Logins from a usual IP will not be considered. This crtieria can be removed in a cloned event handler.

You can find the related events in the *Event Monitor*:

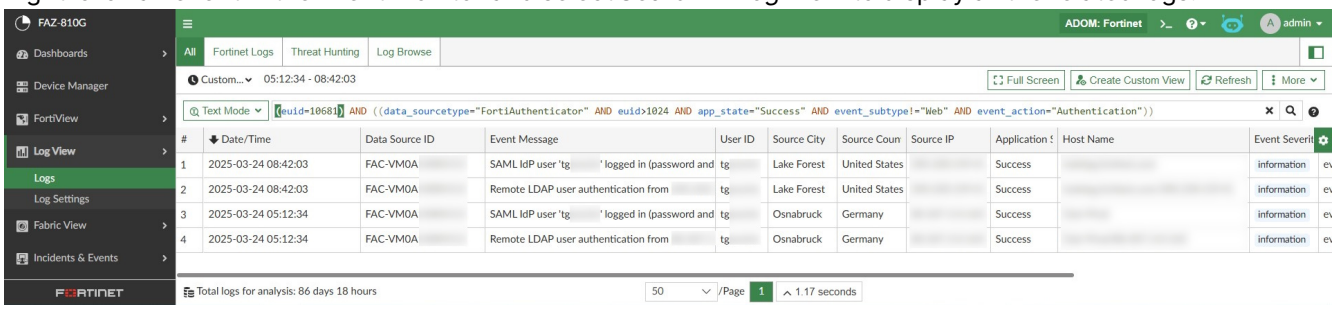


The *Event Monitor* displays the customized event message, including the username in the *Event* column. The event status, severity, type, and tags are also included in their respective columns. Additionally, using the additional info configured in the rule, the *Additional Info* column provides further information about the event at a glance.

Right-click an event in the *Event Monitor* and select *View Logs* to display the consecutive logs:

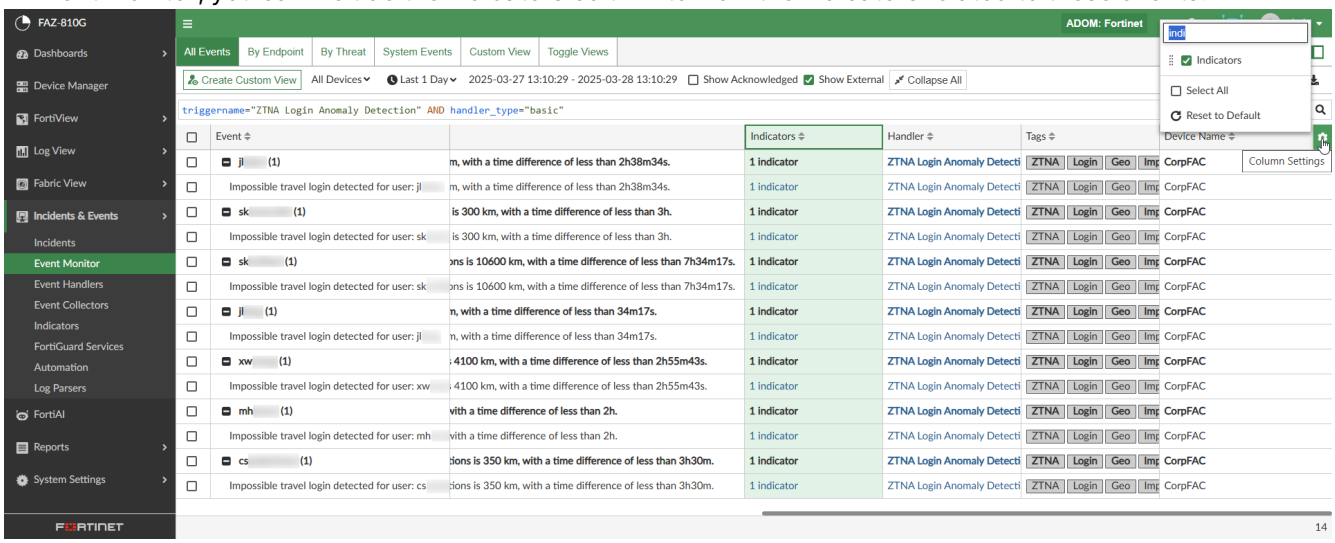


Right-click an event in the *Event Monitor* and select *Search in Log View* to display all the related logs:

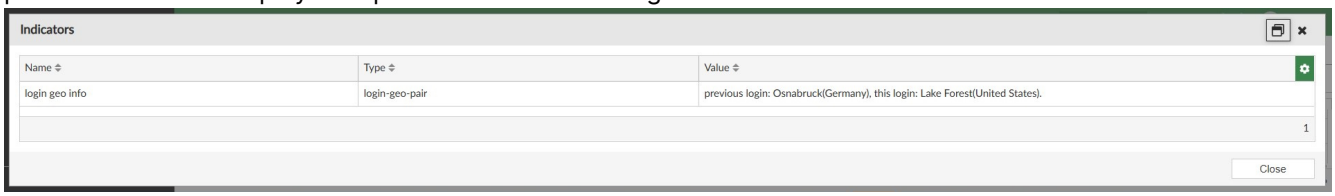


This rule is also configured to create indicators to display the previous login and new login location. If the alert is updated, you can also see the new geo-login information in the indicator as well.

In *Event Monitor*, you can include the *Indicators* column to view the indicators related to these events.



Click a link in this column to display the *Indicators* pane with more information. For example, see the *Indicators* pane below which displays the previous and current login:



To enable, disable, and troubleshoot the geo location function in the FortiAnalyzer CLI:

You can use the following commands to enable, disable, and troubleshoot the geo location function in FortiAnalyzer.

Command to enable the geo location function:

```
diagnose test application sqllogd 231 .geolocation enable
```

Command to disable the geo location function:

```
diagnose test application sqllogd 231 .geolocation disable
```

Other related commands:

```
# diagnose test application sqllogd 231

  Geo-Location diag usage:
  info                      geoip cache info
  countrylist               list all country names
  ip4dump                   dump ip4 ranges
  ip6dump                   dump ip6 ranges
  ip                        find IP's country
  fgt-cfg-cache             dump fgt-geo-cfg-cache info
```

ZTNA login event handlers

The following basic event handlers are included to detect ZTNA login anomalies and brute force logins:

- ZTNA Brute Force Login
- ZTNA Login Anomaly Detection

These event handlers use FortiAuthenticator logs for detection.

ZTNA Brute Force Login

This basic event handler detects various brute force login attempts in ZTNA environments.

MITRE Tech IDs:

- T1110.001 Password Guessing
- T1110.002 Password Cracking
- T1110.003 Password Spraying
- T1110.004 Credential Stuffing

For all rules in the event handler, the log device type is *Fabric* and the log type is *Normalized*.

You can review the resulting event messages in the *Event Monitor* pane to determine the details of the event, such as the user ID or host name according to the rule that triggered the event.

Rule	Description
High Volume of Failed Authentications from Multiple Non-Existing Users	Triggers an event when 100 or more non-existing users have failed authentications to a host name within 10 minutes. Event Severity: Medium Log Field: Host Name Logs that match all of the following filters: • Data Source Type = FortiAuthenticator • Event Sub Type = Authentication • Event ID = 20101 Event Message: High volume of failed authentications from multiple non-existing users to host: $groupby1 Tags: ZTNA, Login, AccountDiscovery, BruteForce, CredentialSurfing

Rule	Description
Authentication Failed from Multiple Geo Locations	Triggers an event when an existing account fails to authenticate from three or more different geo locations within five minutes. Event Severity: High Log Field: User ID Logs that match all of the following filters: • Data Source Type = FortiAuthenticator • Event Sub Type = Authentication • Event Profile contains AUTH_FAIL • UEBA User ID > 1024 Event Message: Authentication failed from multiple geo locations for user: $groupby1 Tags: ZTNA, Login, Geo, BruteForce
Brute Force Login Attack	Triggers an event when and existing user has 10 or more failed authentications with an event profile containing AUTH_FAIL_LOCK within 10 minutes. Event Severity: Medium Log Fields: User ID, Event Profile Logs that match all of the following filters: • Data Source Type = FortiAuthenticator • Event Sub Type = Authentication • Event Profile contains AUTH_FAIL • UEBA User ID > 1024 Event Message: Brute force login attack for user: $groupby1 Tags: ZTNA, Login, BruteForce
High Volume of Failed Authentications to Same Non-Existing User	Triggers an event when a non-existing user has at least 100 or more failed authentications within 1440 minutes (one day). Event Severity: Medium Log Field: User ID Logs that match all of the following filters: • Data Source Type = FortiAuthenticator • Event Sub Type = Authentication • Event ID = 20101 Event Message: High volume of failed authentications for non-existing user: $groupby1 Tags: ZTNA, Login, BruteForce, DoS
Low and Slow Brute Force Login Attack to Same User	Event Severity: High Log Field: UEBA User ID Log Filter by Text: `data_sourcetype='FortiAuthenticator' and euid>1024 and event_subtype='Authentication' and event_action='Authentication'`

Rule	Description
	Trigger an event when (*Advanced Mode*): `AVG(WINDOW_COUNT('daily', 'app_state="Failed"') alias daily_failed < 10? then daily_failed else 10) alias avg_daily_failed > 1 and (COUNT (daily_failed > WINDOW_COUNT('daily', 'app_state="Success"') * 1.0 ? then 1 else 0)) alias days_with_high_failed_ratio > 15 and not logins_from_usual_ip` Event Type Override: Auth Event Message: Possible low and slow brute force login attack to user: ${event.user_name} Event Status: Unhandled Tags: ZTNA, Login, BruteForce, SlowAttack, Auth Additional Info: User ${event.user_name}'s average daily login failure count is ${rule.alias.avg_daily_failed}, with ${rule.alias.days_with_high_failed_ratio} days having high failed login ratio.

Note that the *Low and Slow Brute Force Login Attack to Same User* rule uses *Advanced Mode* to trigger events. According to the default configuration, this rule triggers an event if either of the following two conditions are met within the last 30 days:

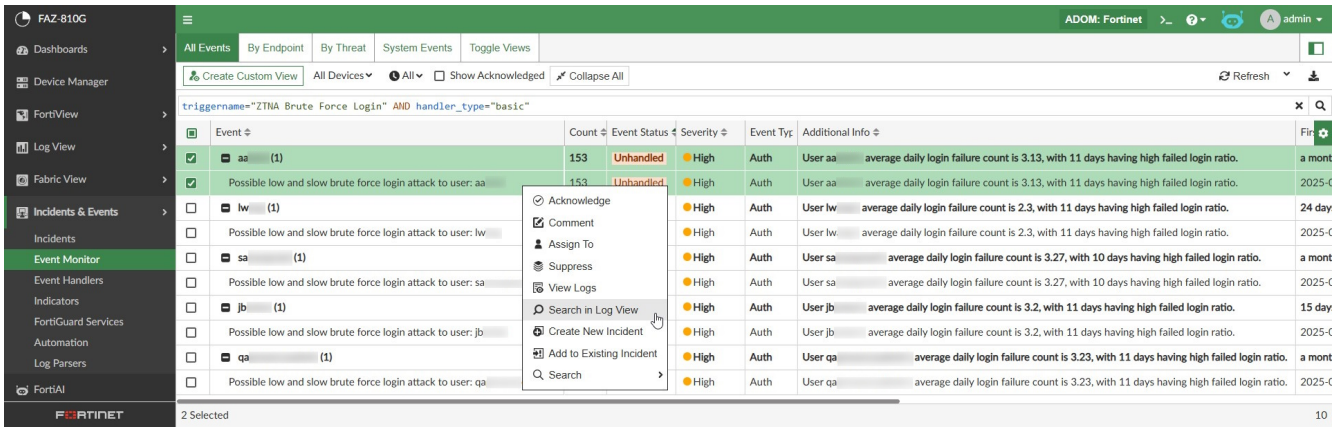
- If the average number of daily failed logins is greater than 1.

  To avoid false positive cases, the daily failed logins are capped at 10. The actual count is used if it is less than 10 failed logins.
- For more than 15 days within the last 30 day period, the number of failed logins has exceeded successful logins.

You can clone this event handler to edit the configuration of the rule, if needed. See below for a description of the criteria and values that can be edited:

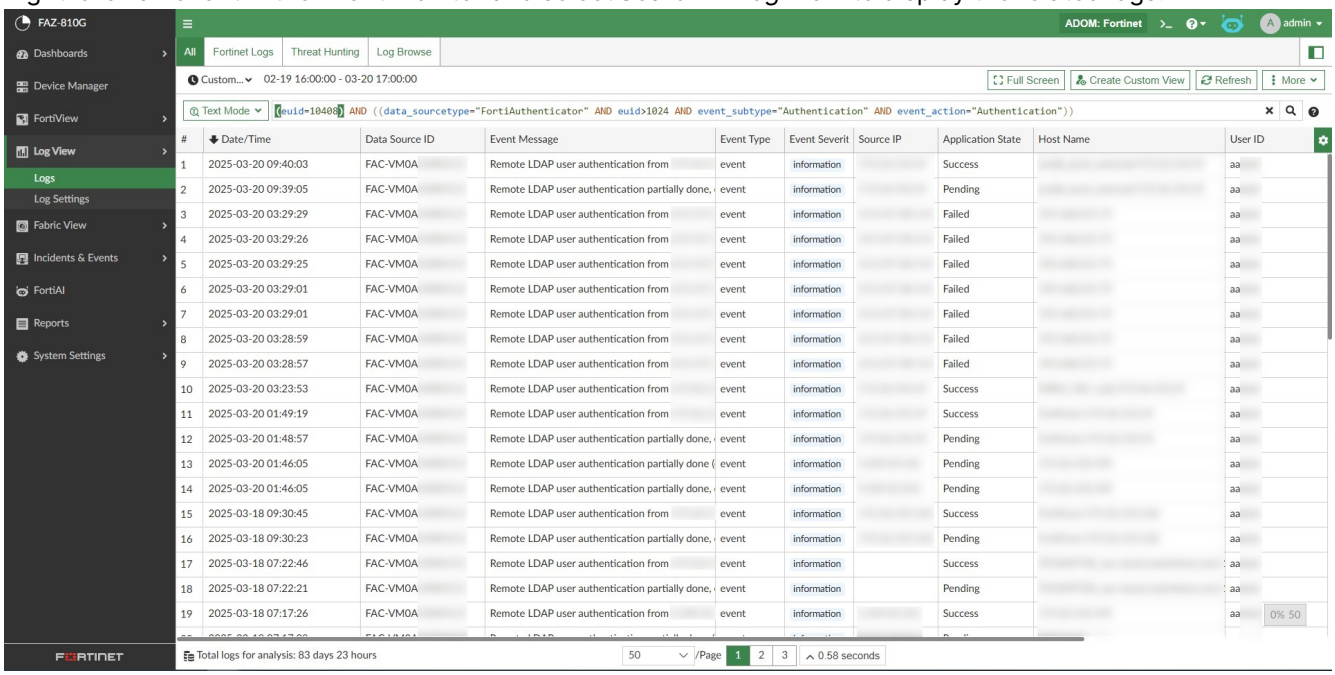
Criteria	Description
`daily_failed < 10? then daily_failed else 10)`	The maximum number for daily failed logins (default = 10). If daily failed logins is less than <integer>, the actual number will be counted. Otherwise, <integer> will be used as the daily failed logins number.
`avg_daily_failed > 1`	The average daily failed logins' number threshold (default = 1). If daily failed number is larger than <integer>, the day will be counted.
`(COUNT(daily_failed > WINDOW_COUNT('daily', 'app_state="Success"') * 1.0 ? then 1 else 0))`	The failed_ratio (login failed number / login success number) threshold (default = 1.0). If the failed_ratio is larger than <float>, the day will be counted.
`days_with_high_failed_ratio > 15`	The total failed login days' threshold (default = 15; must be less than 30). If, in 30 days, the total failed days is larger than <integer> there would be alert.
`and not logins_from_usual_ip`	Logins from usual IPs will not be considered. This criteria can be removed.

You can find the related events in the *Event Monitor*. This example uses the *Low and Slow Brute Force Login Attack to Same User* rule.



The *Event Monitor* displays the customized event message, including the username in the *Event* column. The event status, severity, type, and tags are also included in their respective columns. Additionally, using the additional info configured in the rule, the *Additional Info* column provides further information about the event at a glance.

Right-click an event in the *Event Monitor* and select *Search in Log View* to display the related logs:



ZTNA Login Anomaly Detection

This basic event handler detects various suspicious login scenarios in ZTNA environments.

MITRE Tech IDs:

- T1078.001 Default Accounts
- T1078.002 Domain Accounts
- T1078.003 Local Accounts

- T1078.004 Cloud Accounts

For all rules in the event handler, the log device type is *Fabric* and the log type is *Normalized*.

You can review the resulting event messages in the *Event Monitor* pane to determine the details of the event, such as the user ID, service, or sanctioned country according to the rule that triggered the event.

Rule	Description
Authentication to Multiple Services Failed	Triggers an event when a user has failed authentications to three or more services within 10 minutes. Event Severity: Medium Log Field: User ID Logs that match all of the following filters: • Data Source Type = FortiAuthenticator • Event Sub Type = Authentication • Event Profile contains AUTH_FAIL • UEBA User ID > 1024 Event Message: Authentication to multiple services failed for user: $groupby1 Tags: ZTNA, Login, PrivilegeEscalation
Successful Authentication from Multiple Geo Locations	Triggers an event when a user has successful authentication from three or more unique geo locations within 10 minutes. Event Severity: Critical Log Field: User ID Log Filter by Text: • `data_sourcetype = 'FortiAuthenticator' and euid > 1024 and ((event_subtype = 'User' and event_profile = 'SAML_IDP_PORTAL_LOGIN') or (event_subtype = 'Authentication' and event_profile ~ 'AUTH_OK'))` Event Message: Suspicious successful authentication from multiple geo locations for user: $groupby1 Tags: ZTNA, Login, Geo, ImpossibleTravel
Successful Authentication from Multiple Endpoints	Triggers an event when a user has successful authentication from five or more different host_IPs within 10 minutes. Event Severity: High Log Field: User ID, Host Name Log Filter by Text: • `data_sourcetype = 'FortiAuthenticator' and euid > 1024 and ((event_subtype = 'User' and event_profile = 'SAML_IDP_PORTAL_LOGIN') or (event_subtype = 'Authentication' and event_profile ~ 'AUTH_OK'))` Event Message: Suspicious successful authentication from multiple endpoints for user: $groupby1 to host $groupby2 Tags: ZTNA, Login, LateralMovement

Rule	Description
Successful Authentication from Sanctioned Countries	Triggers an event when a user has at least one successful authentication from sanctioned countries within 10 minutes. Event Severity: Medium Log Field: User ID Log Filter by Text: • `data_sourcetype='FortiAuthenticator' and euid>1024 and ((event_subtype='User' and event_profile='SAML_IDP_PORTAL_LOGIN') or (event_subtype='Authentication' and event_profile~'AUTH_OK')) and (src_geo_country='Russian Federation' or src_geo_country='Belarus' or src_geo_country='Iraq' or src_geo_country='Sri Lanka' or src_geo_country='Central African Republic' or src_geo_country='Syrian Arab Republic' or src_geo_country='Libyan Arab Jamahiriya' or src_geo_country='Korea, Democratic People\'s Republic of' or src_geo_country='Nicaragua' or src_geo_country='China' or src_geo_country~'Iran' or src_geo_country='Venezuela' or src_geo_country='Yemen' or src_geo_country='Lebanon' or src_geo_country='Myanmar' or src_geo_country~'Sudan' or src_geo_country~'Moldova' or src_geo_country~'Congo' or src_geo_country='Guatemala' or src_geo_country='Ukraine' or src_geo_country='Haiti' or src_geo_country='Somalia' or src_geo_country='Zimbabwe')` Event Message: Successful authentication from sanctioned countries for user: $groupby1 Tags: ZTNA, Login, Geo, PolicyViolation, Compliance
Impossible Travel Login Detection	For more information, see Geo-alerting event handlers on page 275.

Excessive email sending event handler

The predefined *FortiMail - Excessive Outbound Emails* basic event handler enhances email traffic visibility using FortiMail logs, especially in scenarios where email accounts may be misused to send spam, phishing, or malware at scale. It provides proactive detection of high-volume and suspicious email behavior without requiring manual configuration. It is enabled by default.

This event handler uses normalized fabric logs from FortiMail to generate events. It includes the following rules:

Rules	Description
Excessive rejected outbound emails	Triggers an event when there are 300 or more rejected outbound emails from a single sender in one day. Event Severity: Medium Log Field: Mail From

<table>
<tr><th>Rules</th><th>Description</th></tr>
<tr><td></td><td>Log Filter by Text: <code>event_outcome="Reject" and data_sourcetype="FortiMail" and event_type="statistics" and (net_direction!="in") and mail_from!="" and event_cat!="Session Limit" and mail_to!=''</code>
Trigger an event when a group contains 300 or more log occurences within one day.
Event Type Override: EmailAnomaly
Event Message: Excessive emails from ${groupby1} have been rejected
Event Status: Mitigated
Tags: Email, SpamRisk, FortiMail
Indicators:<table><tr><th>Log field</th><th>Indicator Type</th><th>Count</th></tr><tr><td>Mail To</td><td>Email Address</td><td>10</td></tr></table>Additional Info: Excessive rejected outbound emails sent from: ${mail_from} with srcip: ${src_ip} and srccountry: ${src_geo_country} to: ${mail_to} dstip: ${dst_ip}, with disposition: ${event_outcome}, direction: ${net_direction}.</td></tr>
<tr><td>Excessive outbound emails</td><td>Triggers an event when a single user has sent outbound emails to 500 or more unique recipients in one day. The rule ensures only meaningful cases are considered by excluding replies and requiring specific log categories and outcomes.
This rule is disabled by default.
Event Severity: High
Log Field: Mail From
Log Filter by Text: <code>event_outcome!="Reject" and data_sourcetype="FortiMail" and event_type="statistics" and net_direction!="in" and mail_from!=""and (mail_from !~ "reply" and mail_from !~ "Reply") and mail_to!=''</code>
Trigger an event when, within a group, the log field Mail To (mail_to) has 500 or more unique values within one day.
Event Type Override: EmailAnomaly
Event Message: Excessive outbound emails from ${groupby1} have been detected
Event Status: Unhandled
Tags: Email, SpamRisk, FortiMail
Indicators:<table><tr><th>Log field</th><th>Indicator Type</th><th>Count</th></tr><tr><td>Mail To</td><td>Email Address</td><td>10</td></tr></table></td></tr>
</table>

<table>
<tr><th>Rules</th><th>Description</th></tr>
<tr><td></td><td>Additional Info: Excessive outbound emails from: ${mail_from} with srcip: ${src_ip} and srccountry: ${src_geo_country} to: ${mail_to} dstip: ${dst_ip} with disposition: ${event_outcome}, direction: ${net_direction}.</td></tr>
<tr><td>Outbound emails originating from multiple countries</td><td>Triggers an event when a single user sends emails from three or more unique geographical locations (countries or IPs) within one day.
Event Severity: High
Log Field: Mail From
Log Filter by Text: <code>data_sourcetype="FortiMail" and event_type="statistics" and src_geo_country!="Reserved" and (mail_from !~ "reply" and mail_from !~ "Reply") and mail_from !='' and (event_outcome!="Reject" and event_outcome!="Discard") and net_direction!= "in" and mail_to!=''</code>
Trigger an event when, within a group, the log field Source Country (src_geo_country) has three or more unique values within one day.
Event Type Override: EmailAnomaly
Event Message: Outbound emails from ${groupby1} have been sent from multiple countries
Event Status: Unhandled
Tags: Email, Geo, FortiMail
Indicators:
<table>
<tr><th>Log field</th><th>Indicator Type</th><th>Count</th></tr>
<tr><td>Source Country</td><td>Others</td><td>10</td></tr>
<tr><td>Source IP</td><td>IP</td><td>10</td></tr>
</table>
Additional Info: Emails orignated from multiple countries from ${mail_from} with srcip ${src_ip} and srccountry: ${src_geo_country} to: ${mail_to} dstip: ${dst_ip} with disposition: ${event_outcome}, direction: ${net_direction}.</td></tr>
<tr><td>Excessive outbound emails with same subject</td><td>Triggers an event when a single user sends 500 or more emails with the same subject to unique recipients within one day.
Event Severity: High
Log Field: Mail From, Mail Subject
Log Filter by Text: <code>event_outcome!="Reject" and data_sourcetype="FortiMail" and event_type="statistics" and net_direction!="in" and mail_from!=""and (mail_from !~ "reply" and mail_from !~ "Reply") and mail_to!=''</code>
Trigger an event when, within a group, the log field Mail To (mail_to) has 500 or more unique values within one day.
Event Type Override: EmailAnomaly
Event Message: Excessive outbound emails with the subject "${groupby2}" from ${groupby1} have been detected
Event Status: Unhandled</td></tr>
</table>

Rules	Description
	Tags: Email, SpamRisk, FortiMail Indicators: **Log field** / **Indicator Type** / **Count** Mail To / Email Address / 10 Additional Info: Excessive outbound emails with same subject sent from: ${mail_from} with srcip: ${src_ip} and srccountry: ${src_geo_country} to: ${mail_to} dstip: ${dst_ip} with disposition: ${event_outcome}, direction: ${net_direction}.

If there are internal email addresses that normally send a high volume of emails per day and it is not suspicious, you can exclude these email addresses to reduce false positive alerts. These addresses can be excluded by editing the rules, cloning and editing the event handler, or adding a data selector for the event handler. These addresses can be excluded by adding a data selector for the event handler, or by cloning the event handler and editing the rules.

For example, you can create a data selector with the following criteria and assign it to the event handler:

Log Device Type	Fabric
Log Type	Normalized Log
Logs match	All **Log Field** / **Match Criteria** / **Value** Mail From (mail_from) / Not Equal To / <known email address>

Add further email addresses to the data selector, as needed. Alternatively, you can use the *Generic Text Filter* in the data selector to list the exclusions.

This event handler is associated with the following MITRE Tech IDs:

- T1078.001 Default Accounts
- T1078.002 Domain Accounts
- T1078.003 Local Accounts
- T1078.004 Cloud Accounts
- T1566.001 Spearphishing Attachment
- T1114.001 Local Email Collection
- T1585.002 Email Accounts

Malicious IP intrusion event handler

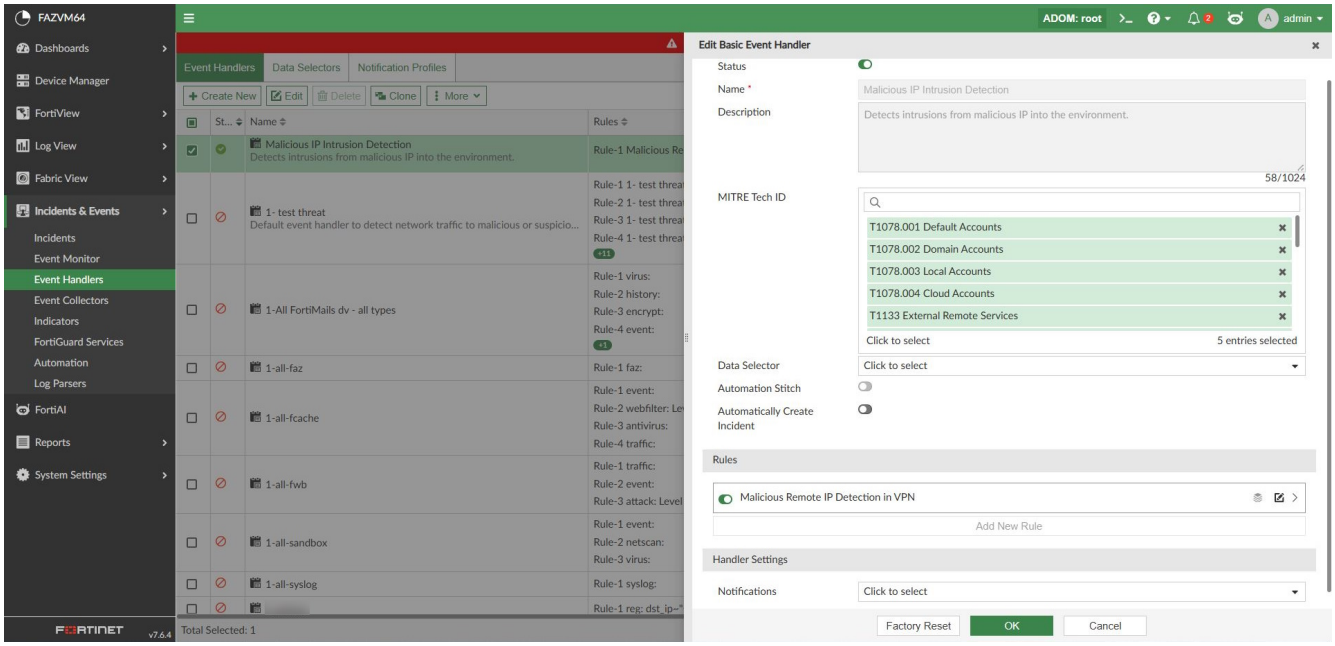
The *Malicious IP Intrusion Detection* event handler and *Automated Correlation Threat Hunting* playbook are used to detect malicious IP intrusion, trace lateral movement, and correlate related events. These features provide the following benefits:

- Faster detection and triage of correlated threats.
- Reduced manual effort in linking related events.
- Better visibility into attack paths and lateral movements.
- Proactive incident enrichment, with follow-up scans to capture new threats as they unfold.

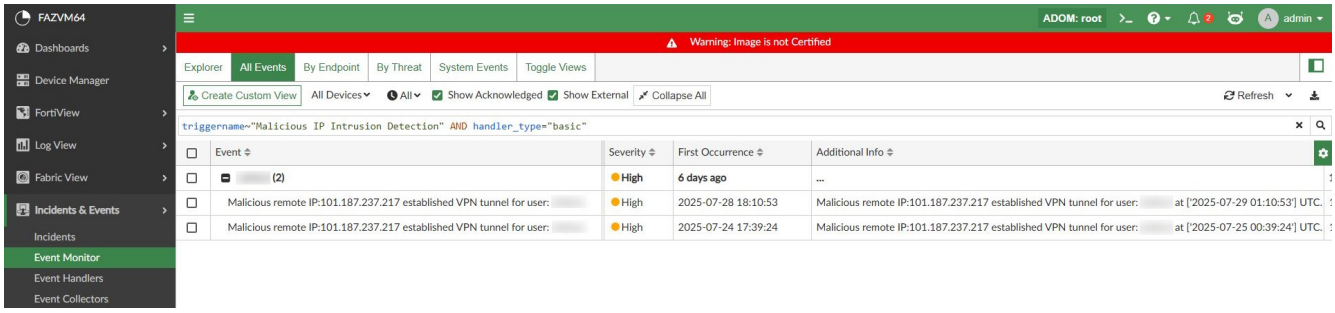
The event handler is triggered when a VPN log is received with `event_action = tunnel-up` and the `net_remote_server.ip` matches a malicious IP. There is a tag, `AutoCorrHuntTrigger`, in the event handler configuration that, when the handler is triggered, launches the playbook. The playbook traces lateral movement depth, correlates related events, identifies compromised devices, and creates an incident with contextual evidence. See below for further details about these objects.

Malicious IP Intrusion Detection event handler

The *Malicious IP Intrusion Detection* event handler can be found in *Incidents & Events > Event Handlers > Event Handlers*.



This event handler generates an event when a log meets the following conditions: `data_sourcetype='FortiGate' and euid>1024 and event_type='event' and event_subtype='vpn' and event_action='tunnel-up'`



The event handler is enabled by default, and it references the following MITRE Tech IDs:

- T1133: External Remote Services
- T1078.001: Default Accounts
- T1078.002: Domain Accounts
- T1078.003: Local Accounts
- T1078.004: Cloud Accounts

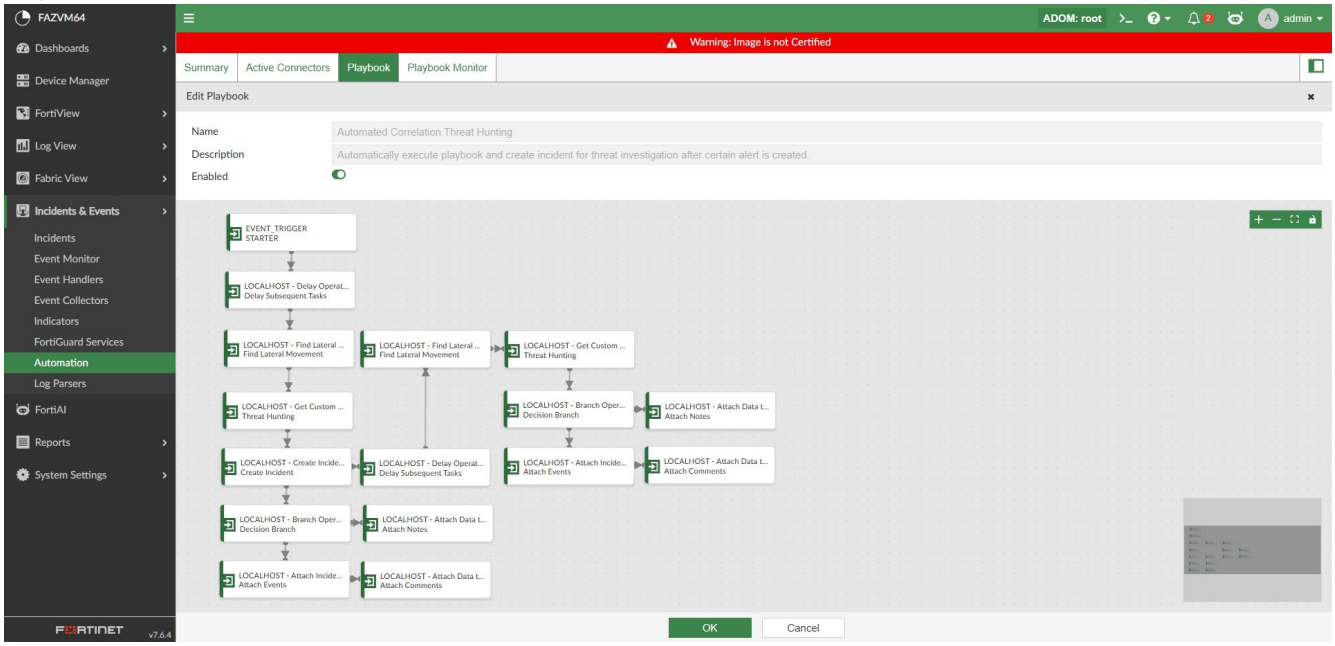
The event handler's one rule, *Malicious Remote IP Detection in VPN*, has the following configuration.

Rule option	Configuration
Name	Malicious Remote IP Detection in VPN
Status	Enabled
Event Severity	High
Log Device Type	Fabric
Log Type	Normalized Log
Log Field	End User, Net Remote Server (net_remote_server)
Log Filter by Text	`data_sourcetype='FortiGate' and euid>1024 and event_type='event' and event_subtype='vpn' and event_action='tunnel-up'`
Trigger an event when	Advanced Mode: `ioc_malicious_ip_detected(1h, 'net_remote_server.ip') or ioc_deltascan_malicious_ip_detected(7d,'net_remote_server.ip')` All logs we generated within a duration of `1d`.  The SQL check logic checks `time_now -10min` to ensure the data is stored in the database. Thus, you need to wait at least 10 minutes for handler to be triggered by logs that meet the rule conditions.
Event Type Override	network_malicious_ip_detected
Event Message	Malicious remote IP:${net_remote_server.ip} established VPN tunnel for user: ${groupby1}.
Event Status	Unhandled
Tags	VPN, Malicious, AutoCorrHuntTrigger  The `AutoCorrHuntTrigger` tag launches the *Automated Correlation Threat Hunting* playbook when the event handler is triggered.
Indicators	<table><tr><th>Log Field</th><th>Indicator Type</th><th>Count</th></tr><tr><td>net_remote_server.ip</td><td>IP</td><td>1</td></tr></table>

Rule option	Configuration
	<table><tr><th>Log Field</th><th>Indicator Type</th><th>Count</th></tr><tr><td>(net_remote_server.ip)</td><td></td><td></td></tr><tr><td>net_tunnel.ip (net_tunnel.ip)</td><td>IP</td><td>6</td></tr></table>
Additional Info	Use custom message: Malicious remote IP:${net_remote_server.ip} established VPN tunnel for user: ${groupby1} at ${event_time}.

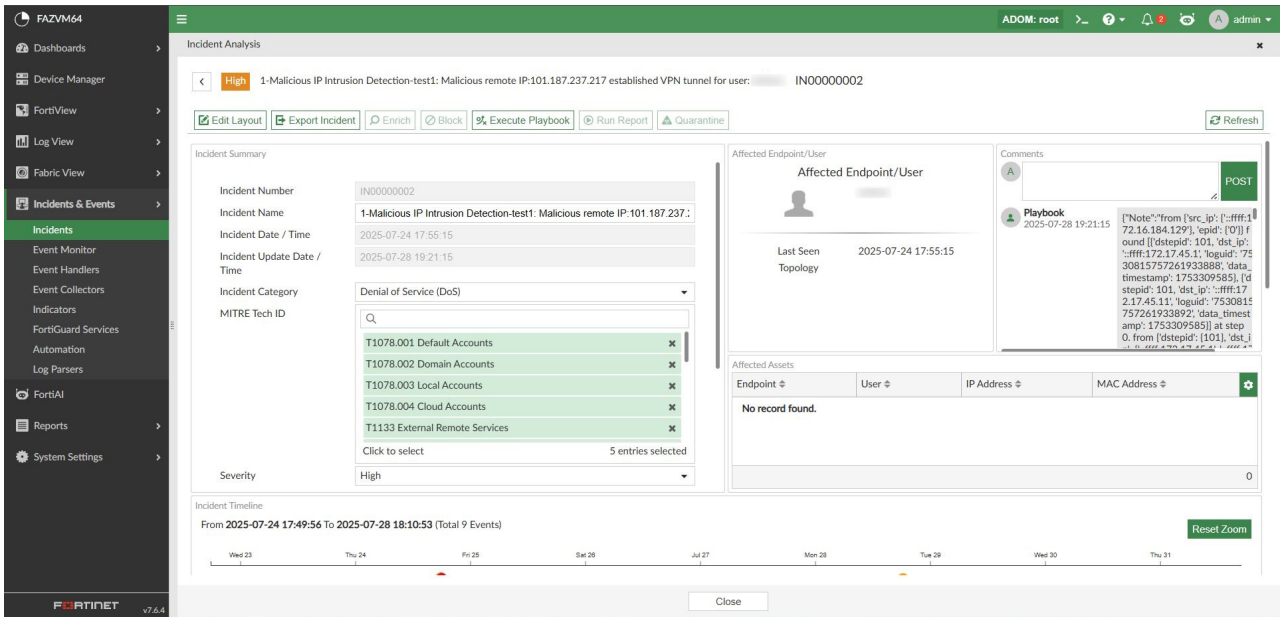
Automated Correlation Threat Hunting playbook

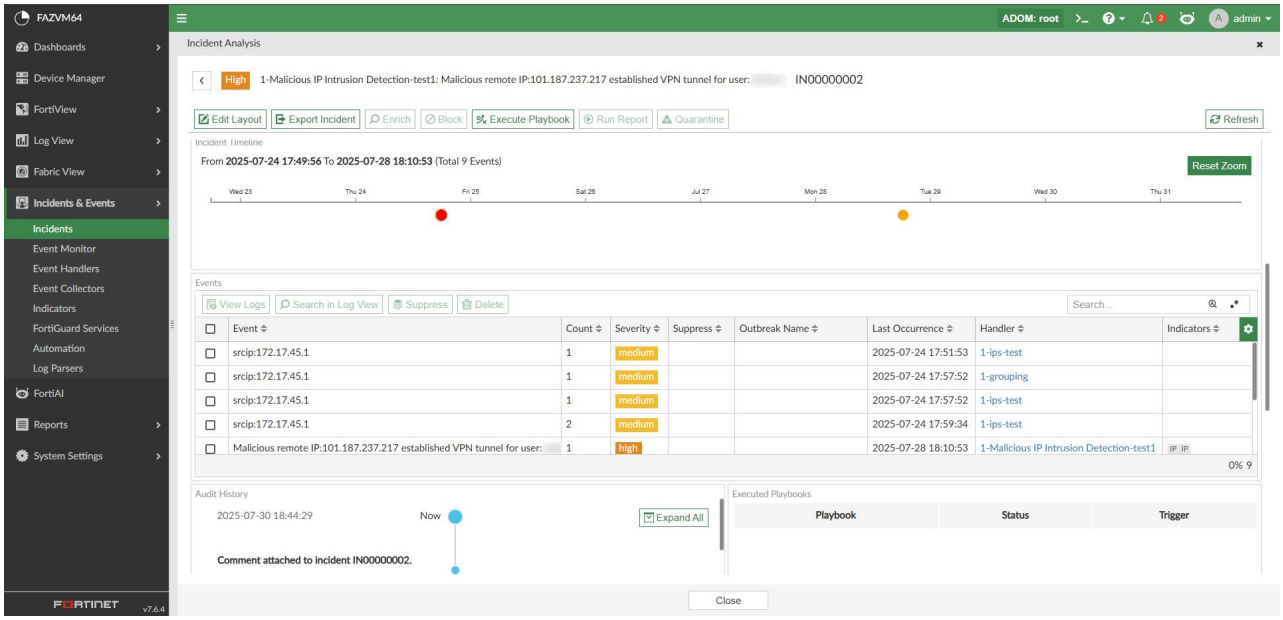
The *Automated Correlation Threat Hunting* playbook can be viewed in *Incidents & Events* > *Automation* > *Playbook*.

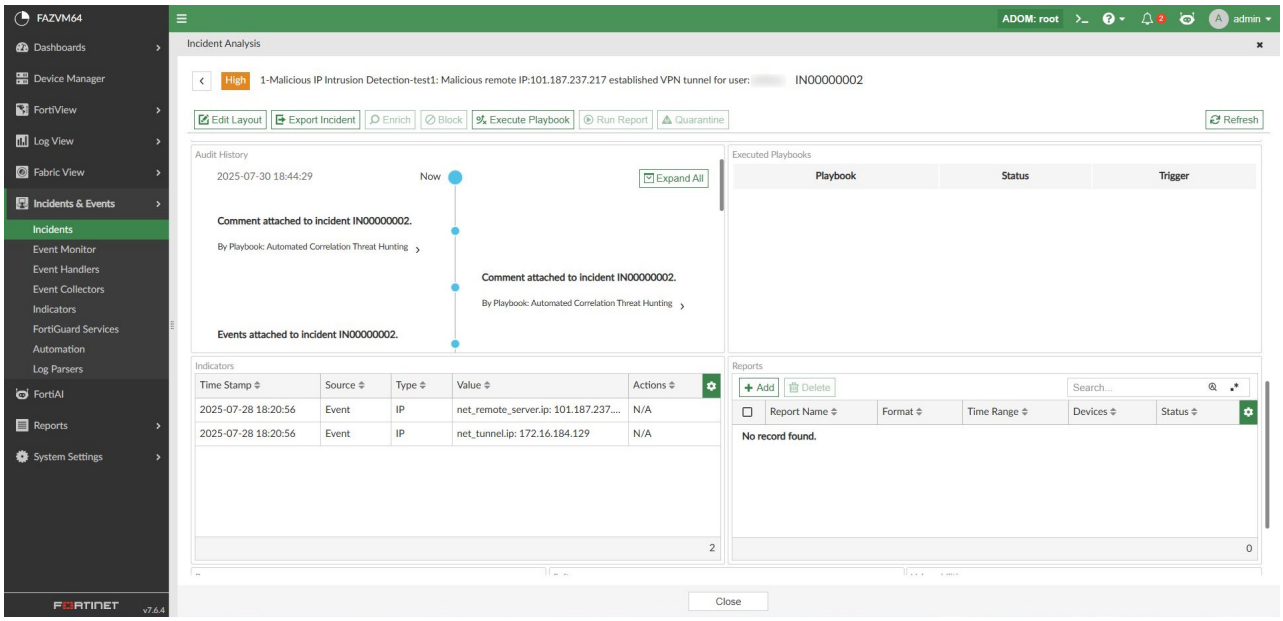


The playbook runs automatically when the *Malicious IP Intrusion Detection* is triggered, and does the following:

1. Traces lateral movement depth based on VPN sessions and log history (SSH, RDP, etc.).
2. Correlates related events and identifies compromised devices.
3. Creates an incident with contextual evidence and threat path analysis.

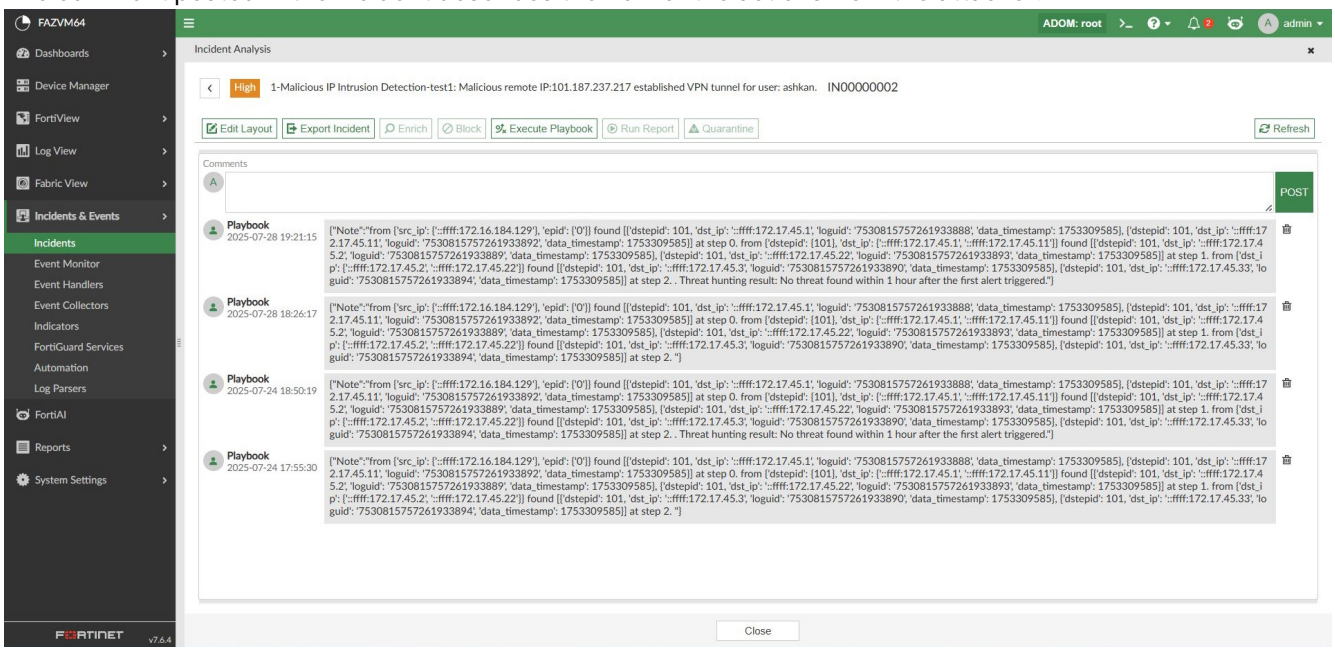

FAZVM64
ADOM: root
admin
Dashboards
Device Manager
FortiView
Log View
Fabric View
Incidents & Events
Incidents
Event Monitor
Event Handlers
Event Collectors
Indicators
FortiGuard Services
Automation
Log Parsers
FortiAI
Reports
System Settings
Incident Analysis
High
1-Malicious IP Intrusion Detection-test1: Malicious remote IP:101.187.237.217 established VPN tunnel for user:
IN00000002
Edit Layout
Export Incident
Enrich
Block
Execute Playbook
Run Report
Quarantine
Refresh
Incident Summary
Incident Number
Incident Name
Incident Date / Time
Incident Update Date / Time
Incident Category
Denial of Service (DoS)
MITRE Tech ID
T1078.001 Default Accounts
T1078.002 Domain Accounts
T1078.003 Local Accounts
T1078.004 Cloud Accounts
T1133 External Remote Services
Click to select
5 entries selected
Severity
High
Affected Endpoint/User
Affected Endpoint/User
Last Seen
2025-07-24 17:55:15
Topology
Comments
POST
Playbook
2025-07-28 19:21:15
Affected Assets
Endpoint
User
IP Address
MAC Address
No record found.
0
Incident Timeline
From 2025-07-24 17:49:56 To 2025-07-28 18:10:53 (Total 9 Events)
Reset Zoom
Wed 23
Thu 24
Fri 25
Sat 26
Jul 27
Mon 28
Tue 29
Wed 30
Thu 31
Close
FORTINET
v7.6.4


FAZVM64
ADOM: root
admin
Incident Analysis
High
1-Malicious IP Intrusion Detection-test1: Malicious remote IP:101.187.237.217 established VPN tunnel for user:
IN00000002
Edit Layout
Export Incident
Enrich
Block
Execute Playbook
Run Report
Quarantine
Refresh
Incident Timeline
From 2025-07-24 17:49:56 To 2025-07-28 18:10:53 (Total 9 Events)
Reset Zoom
Wed 23
Thu 24
Fri 25
Sat 26
Jul 27
Mon 28
Tue 29
Wed 30
Thu 31
Events
View Logs
Search in Log View
Suppress
Delete
Search...
Event
Count
Severity
Suppress
Outbreak Name
Last Occurrence
Handler
Indicators
srcip:172.17.45.1
1
medium
2025-07-24 17:51:53
1-ips-test
srcip:172.17.45.1
1
medium
2025-07-24 17:57:52
1-grouping
srcip:172.17.45.1
1
medium
2025-07-24 17:57:52
1-ips-test
srcip:172.17.45.1
2
medium
2025-07-24 17:59:34
1-ips-test
Malicious remote IP:101.187.237.217 established VPN tunnel for user:
1
high
2025-07-28 18:10:53
1-Malicious IP Intrusion Detection-test1
0% 9
Audit History
2025-07-30 18:44:29
Now
Expand All
Comment attached to incident IN00000002.
Executed Playbooks
Playbook
Status
Trigger
Close
FORTINET
v7.6.4



4. Re-runs the analysis after one hour to update the incident if new events are found.
5. Posts a comment with the alert hunting and lateral movement in the created incident.

The comment posted in the incident describes the flow of the actions from the attacker.



For example, the comment describes the attacker performing the following actions:

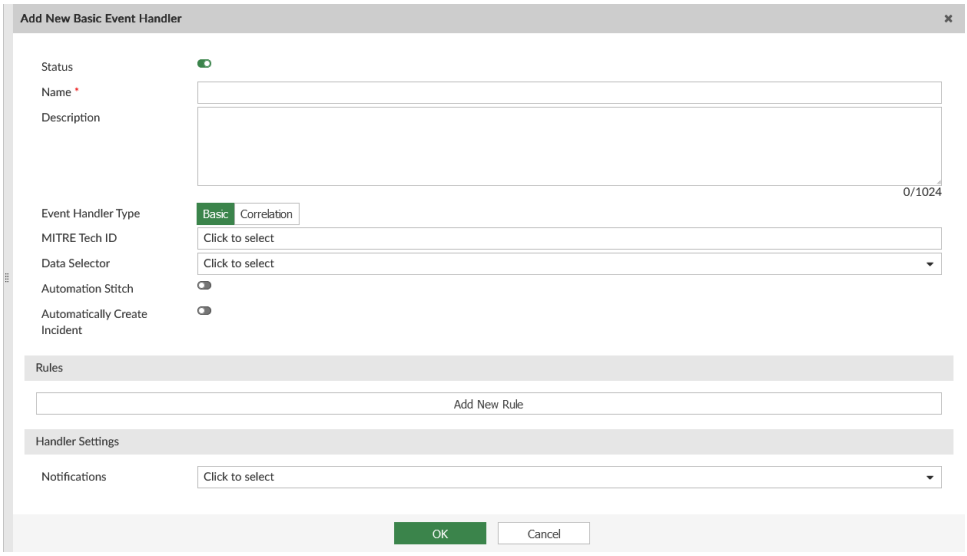
1. Attacker gets an assigned IP.
2. Lateral movement to another endpoint with SSH.
3. Lateral movement to another endpoint with RDP.
4. Lateral movement continues (see comment below).

{"Note":"from {'src_ip': {'::ffff:172.16.184.129'}, 'epid': {'0'}} found [{'dstepid': 101, 'dst_ip': '::ffff:172.17.45.1', 'loguid': '7530815757261933888', 'data_timestamp': 1753309585}, {'dstepid': 101, 'dst_ip': '::ffff:172.17.45.11', 'loguid': '7530815757261933892', 'data_timestamp': 1753309585}] at step 0. from {'dstepid': {101}, 'dst_ip': {'::ffff:172.17.45.1', '::ffff:172.17.45.11'}} found [{'dstepid': 101, 'dst_ip': '::ffff:172.17.45.2', 'loguid': '7530815757261933889', 'data_timestamp': 1753309585}, {'dstepid': 101, 'dst_ip': '::ffff:172.17.45.22', 'loguid': '7530815757261933893', 'data_timestamp': 1753309585}] at step 1. from {'dst_ip': {'::ffff:172.17.45.2', '::ffff:172.17.45.22'}} found [{'dstepid': 101, 'dst_ip': '::ffff:172.17.45.3', 'loguid': '7530815757261933890', 'data_timestamp': 1753309585}, {'dstepid': 101, 'dst_ip': '::ffff:172.17.45.33', 'loguid': '7530815757261933894', 'data_timestamp': 1753309585}] at step 2. . Threat hunting result: No threat found within 1 hour after the first alert triggered."}

Creating a custom event handler

You can create a custom event handler from scratch or clone a predefined basic event handler and customize its settings. See Cloning event handlers on page 314.

To create a basic event handler, select *Basic* for the *Event Handler Type* when creating the event handler.



Configuring an event handler includes defining the following main sections in the GUI:

Option	Description
Event handler attributes	The status, name, description, event handler type (basic), MITRE techniques, data selector, and automation stitch for the event handler. You can also enable the event handler to automatically create an incident, if needed.
Rules	The rules for event generation. 1. *Choose Your Logs*: Start by selecting the device and log type that you want to monitor for events. Choose log fields to categorize logs into smaller groups.

Option	Description
	2. *Refine Your Logs*: Once logs are grouped, you can refine the data within each group by applying filters with other log fields. Logs that match the filters will be retained within each group. 3. *Define Event Conditions*: Once you've organized and filtered the logs, set up criteria that enables the system to automatically initiate events when log records reoccur within each group. 4. *Advanced Settings*: Optional configuration for the event type override, event message, event status, tags, and indicators.
Handler Settings	The notification profile for the event handler.

To create a new event handler:

1. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.
2. In the toolbar, click *Create New*.
3. For *Event Handler Type*, select *Basic*. For more information, see the table below.
4. Configure the following options, and click *OK* to save the event handler.

Option	Description
Status	Enable or disable the event handler. Enabled event handlers show a icon in the *Status* column. Disabled event handlers show a icon in the *Status* column.
Name	Enter a name for the event handler.
Description	(Optional) Enter a description for the event handler.
Event Handler Type	Select one of the following: • *Basic*: an event is generated when one of the rules in the event handler is met. Each rule in the basic event handler has an OR relationship with the others. • *Correlation*: an event is generated when a set of rules are met in correlation sequence. For correlation handlers, you can define both the rules and the operators (AND, AND_NOT, OR, FOLLOWED_BY, and NOT_FOLLOWED_BY). Once the event handler is saved, you cannot edit the *Event Handler Type*. You must instead recreate the event handler with the correct event handler type. In this case, select *Basic*.
MITRE Tech ID	Select the MITRE ATT&CK technique ID(s) that the event handler provides coverage for. For more information, see MITRE ATT&CK® on page 213.
Data Selector	Select a data selector for the event handler. This selects devices, subnets, and filters used for the event handler. See Creating data selectors on page 316.

Option		Description
Automation Stitch		Enable or disable automation stitch. When enabled, FortiAnalyzer sends a notification to FortiGate when events are generated by the event handler. The events are available in the FortiAnalyzer GUI as well. For more information, see Using the Automation Stitch for event handlers on page 310.
Automatically Create Incident		Enable or disable if incidents are automatically created through this event handler. When enabled, once the handler triggers an alert, a new incident is created with the name as `<Handler Name>: <Event Subject>`. If there are new events with same subject, they will be directly attached to the same incident. A new incident is created if the event has a new subject, or if the existing incident's status has changed to *Closed*. The incidents created from event handlers can be identified in *Incident & Events > Incidents > Incidents*. The automatically created incidents display `<alertid>/Auto-Raised` in the *Incident Reporter* column .
Rules		
Add New Rule		Click to add a rule. The *Add New Rule* pane displays. Configure the options below, and then click *OK* to save the rule. You can add multiple rules to the event handler. Each rule has an OR relationship with other rules enabled in the event handler. When editing an existing event handler, you will see an *Edit* icon and a *Suppression* icon for each rule. For more information about event suppression, see Suppressing events on page 227.
	Status	Enable or disable the rule. If the rule is disabled, it will not be used to generate events.
	Name	Enter a name for the rule.
	Event Severity	Select the severity from the dropdown list: *Critical*, *High*, *Medium*, or *Low*.
	Choose Your Logs	
	Log Device Type	If you are in a Security Fabric ADOM, select the log device type from the dropdown list. If you are not in a Security Fabric ADOM, you cannot change the *Log Device Type*. The *Fabric* log device type can be used to generate alerts from SIEM logs when SIEM logs are available.
	Log Type	Select the log type from the dropdown list. When *Devices* is set to *Local Device*, you cannot change the *Log Type* or *Log Subtype*. If generating alerts from SIEM (Fabric) logs, select *Normalized Log*.
	Log Subtype	Select the category of event that this event handler monitors. The available options depend on the platform type.

Option	Description
	This option is only available when the *Log Type* has a subtype. For example, *Event Log* and *Traffic Log* have log subtypes which can be selected from the dropdown.
Log Field	Select the log fields for the system to categorize logs into smaller groups. For example, consider the scenario where the *Log Field* is set using `Source IP (srcip)`. When log entries are recorded with source IPs such as 192.168.1.1, 192.168.1.2, and 192.168.1.3, the system will categorize these logs into distinct groups: • Group 1: Logs with the source IP 192.168.1.1 • Group 2: Logs with the source IP 192.168.1.2 • Group 3: Logs with the source IP 192.168.1.3 This grouping mechanism allows analysis of log data based on the specified source IP addresses.  If you are using SIEM logs to generate alerts, you can find available log fields for existing log parsers using the Fabric Normalization Reference on the Fortinet Document Library.
Refine Your Logs	
Log Filters	Select *All Filters* or *Any One of the Filters*. Configure the filter(s): • **Log Field**: Select a log field from the dropdown. After the log device and log type are selected, the *Log Field* dropdown list will only include log fields that belong to the specified log type. For example, the *Botnet IP* log field is available when the *Log Type* is *DNS*, but not available when the *Log Type* is *Event Log*. • **Match Criteria**: Select an operator from the dropdown. The available options depends on the selected log field. Some log fields, such as *Source Port*, will provide a variety of operators in the dropdown list, such as *Equal To*, *Not Equal To*, *Greater Than or Equal To*, *Less Than or Equal To*, *Greater Than*, and *Less Than*. Other log fields, such as *Log Description*, will be limited to *Equal To* and *Not Equal To*. • **Value**: Select a value from the dropdown list or enter a value in the text box. The available options depends on the selected log field. If there is no dropdown list provided by FortiAnalyzer, you must manually enter a value to find in the raw log. If a dropdown list is provided, you can select a value from the list. For some log fields, such as *Level*, the dropdown list also allows you to enter a custom value. If there is no textbox to enter a custom value in the dropdown list, you must use the *Generic Text Filter* instead.

Option	Description

	In the **Action** column, click plus (**+**) to insert a new filter below. You can insert multiple filters. To delete a filter, click the **x** next to the filter.
	When generating alerts from SIEM logs, you must include the *Data Source Type* is *Equal To* each of the supported third-party logs. For example, if using Windows and Ubuntu log sources, you may configure the following:
	• *Log Filters = Any One of the Filters*
	  • *Data Source Type Equal To Windows*
	  • *Data Source Type Equal To Ubuntu*
	To view the available third-party log parsers, go to *Incidents & Events > Log Parsers > Log Parsers*.

Log Filter by Text	Enter a generic text filter. See Using the Generic Text Filter on page 311. For information on text format, hover the cursor over the help icon. The operator ~ means contains and !~ means does not contain.
Define Event Conditions	
Trigger an event when:	Select the radio button for one of the following options and configure the criteria: • A group contains `<integer>` or more log occurences • Within a group, the log field `<log field>` has `<integer>` or more unique values • Click the toggle icon to change to "[...] has fewer than `<integer>` unique values" • The sum of `<measure>` is greater than or equal to `<integer>` • Safeguard Risk Score is more than `<value>` • Advanced Mode: This field is used for specialized configuration in select predefined event handler rules. For example, see Geo-alerting event handlers on page 275 and ZTNA login event handlers on page 284.  The "sum" option is used for data exfiltration detection. This option is only supported in Fabric ADOMs. It is not available when using Web Filter, Application Control, or Email Filter log types. The "Safeguard Risk Score" option is only available when using Web Filter, Application Control, or Email Filter log types. For an example of a predefined event handler using this trigger, see Safeguarding event handler on page 350. Additionally, configure the following in relation to your selection: • All logs were generated within a duration of `<string>` The string must include days, hours, and minutes. For example, `1d12h30m`.

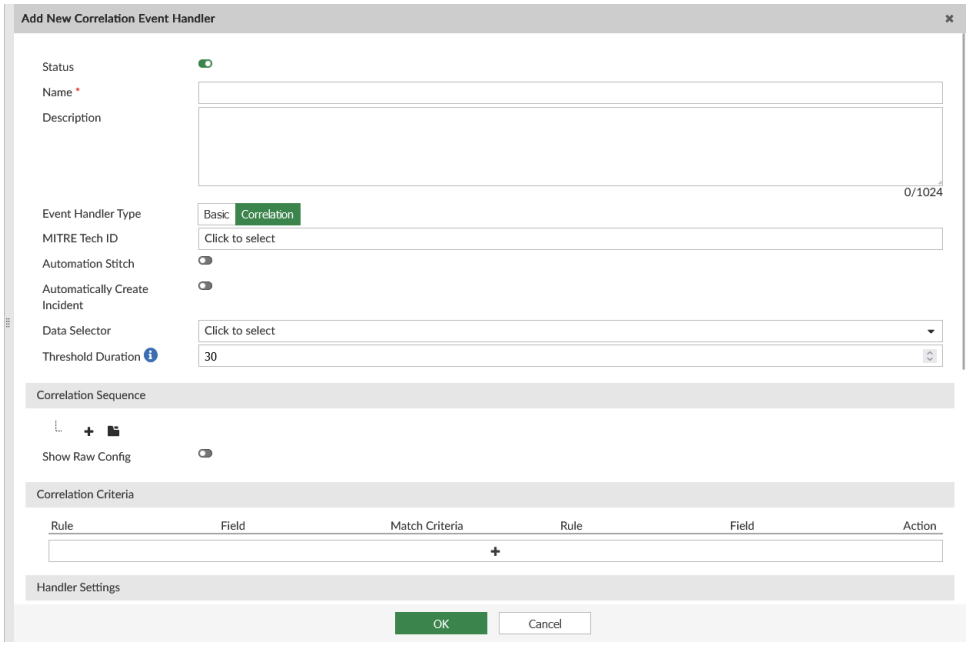
Option		Description
	Advanced Settings	
	Event Type Override	Specify a custom event type, or leave this field blank to use the default value.
	Event Message	(Optional) Enter a custom event message. By default, `Group by key-value pair(s)` will be displayed as the event message in *Event Monitor*. Examples: • `Virus:JS/Runfile.B!tr` • `Endpoint:172.17.58.118 Virus:BlackMoon` You can customize event messages by using Group By variables: $groupby1 and $groupby2 Examples: • `Virus $groupby1 found in traffic` • `Endpoint $groupby1 infected with virus $groupby2`
	Event Status	Select *Allow FortiAnalyzer to choose* or select a status from the dropdown list: *Unhandled*, *Mitigated*, *Contained*, *(Blank)*. You can use a custom event status by clicking the plus (**+**) that appears in the *Event Status* dropdown. Event statuses, including custom statuses, are displayed in the *Event Status* column in the *Event Monitor*.
	Tags	(Optional) Enter custom tags. Tags can be used as a filter when using default or custom views.
	Indicators	(Optional) Add indicators by clicking the plus (**+**). You can configure the *Log Field*, *Indicator Type*, and *Count* for each indicator created in an event handler. Use the buttons in the *Action* column to add (**+**) or remove (**x**) indicators. Up to five indicators can be created. When *Indicators* is selected in *Event Monitor > Display Options*, the *Indicators* column displays indicator types for detected events. You can see additional details when clicking on an indicator. See Event Monitor on page 218. If an incident is raised from an event that includes indicators, they can be viewed in the *Indicators* tab of the incident analysis page. See Analyzing an incident on page 208.
	Additional Info	Specify what to show in the *Additional Info* column of the *Event Monitor*. Select *Use system default* or *Use custom message*. A custom message can include variables and log field names. For more information, hover over the help icon. You can decode the attackcontext in IPS logs in alert notifications by including the following in the custom message: `${b64_decode (attackcontext)}`. For more information, see Decode the attackcontext field in IPS on page 318.

Option	Description
Handler Settings	
Notifications	Select a notification profile for the event handler. See Creating notification profiles on page 317.

Creating a custom correlation handler

You can create a custom correlation event handler from scratch or clone a predefined correlation event handler and customize its settings. See Cloning event handlers on page 314.

To create a basic event handler, select *Correlation* for the *Event Handler Type* when creating the event handler.



Configuring an correlation handler includes defining the following main sections in the GUI:

Option	Description
Correlation event handler attributes	The name, description, event handler type (correlation), MITRE techniques, automation stitch, data selector, and threshold duration for the correlation handler. You can also enable the event handler to automatically create an incident, if needed.
Correlation Sequence	The rules for event generation in sequence and logic group. 1. *Choose Your Logs*: Start by selecting the device and log type that you want to monitor for events. Choose log fields to categorize logs into smaller groups. 2. *Refine Your Logs*: Once logs are grouped, you can refine the data within each group by applying filters with other log fields. Logs that match the filters will be retained within each group.

Option	Description
	3. *Define Event Conditions*: Once you've organized and filtered the logs, set up criteria that enables the system to automatically initiate events when log records reoccur within each group.
Correlation Criteria	The correlation criteria to specify the type of logs that the event handler will look for. The criteria is applied to two rules on a field from each rule.
Handler Settings	The event fields, including the event type override, event message, event status, event severity, indicators, and tags. This section also includes the notification profile for the correlation handler.

To create a new correlation event handler:

1. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.
2. In the toolbar, click *Create New*.
3. For *Event Handler Type*, select *Correlation*. For more information, see the table below.
4. Configure the following options, and click *OK* to save the event handler.

Option	Description
Status	Enable or disable the event handler. Enabled event handlers show a  icon in the *Status* column. Disabled event handlers show a  icon in the *Status* column.
Name	Enter a name for the event handler.
Description	(Optional) Enter a description for the event handler.
Event Handler Type	Select one of the following: • *Basic*: an event is generated when one of the rules in the event handler is met. Each rule in the basic event handler has an OR relationship with the others. • *Correlation*: an event is generated when a set of rules are met in correlation sequence. For correlation handlers, you can define both the rules and the operators (AND, AND_NOT, OR, FOLLOWED_BY, and NOT_FOLLOWED_BY). Once the event handler is saved, you cannot edit the *Event Handler Type*. You must instead recreate the event handler with the correct event handler type. In this case, select *Correlation*.
MITRE Tech ID	Select the MITRE ATT&CK technique ID(s) that the event handler provides coverage for. For more information, see MITRE ATT&CK® on page 213.
Automation Stitch	Enable or disable automation stitch.

Option	Description
	When enabled, FortiAnalyzer sends a notification to FortiGate when events are generated by the event handler. The events are available in the FortiAnalyzer GUI as well. For more information, see Using the Automation Stitch for event handlers on page 310.
Automatically Create Incident	Enable or disable if incidents are automatically created through this event handler. When enabled, once the handler triggers an alert, a new incident is created with the name as `<Handler Name>: <Event Subject>`. If there are new events with same subject, they will be directly attached to the same incident. A new incident is created if the event has a new subject, or if the existing incident's status has changed to *Closed*. The incidents created from event handlers can be identified in *Incident & Events > Incidents > Incidents*. The automatically created incidents display `<alertid>/Auto-Raised` in the *Incident Reporter* column .
Data Selector	Select a data selector for the event handler. This selects devices, subnets, and filters used for the event handler. See Creating data selectors on page 316.
Threshold Duration	Enter the threshold duration for the correlation handler in minutes. The logs must match the criteria in correlation sequence within this time to generate an event.
Correlation Sequence	
Add Rule	Click the plus icon (**+**) to add a rule. The *Add New Rule* pane displays. Configure the options below and click *OK* to save the rule. After creating the rules, make sure they are in the correct correlation sequence. You can drag and drop the rules to re-order them, if needed. Select the correlation between each of the rules: • *AND* • *AND_NOT* • *OR* • *FOLLOWED_BY* (if selected, enter a time limit for the correlation to occur in) • *NOT_FOLLOWED_BY* (if selected, enter a time limit for the correlation to occur in) The rules must be met in the correlation sequence for the event handler to generate an event. Click the trash icon to delete a rule.
Name	Enter a name for the rule.
Choose Your Logs	
Log Device Type	If you are in a Security Fabric ADOM, select the log device type from the dropdown list. If you are not in a Security Fabric ADOM, you cannot change the *Log Device Type*.

Option	Description
	The *Fabric* log device type can be used to generate alerts from SIEM logs when SIEM logs are available.
Log Type	Select the log type from the dropdown list. When *Devices* is set to *Local Device*, you cannot change the *Log Type* or *Log Subtype*. If generating alerts from SIEM (Fabric) logs, select *Normalized Log*.
Log Subtype	Select the category of event that this event handler monitors. The available options depend on the platform type. This option is only available when the *Log Type* has a subtype. For example, *Event Log* and *Traffic Log* have log subtypes which can be selected from the dropdown.
Log Field	Select the log fields for the system to categorize logs into smaller groups. For example, consider the scenario where the *Log Field* is set using `Source IP (srcip)`. When log entries are recorded with source IPs such as 192.168.1.1, 192.168.1.2, and 192.168.1.3, the system will categorize these logs into distinct groups: • Group 1: Logs with the source IP 192.168.1.1 • Group 2: Logs with the source IP 192.168.1.2 • Group 3: Logs with the source IP 192.168.1.3 This grouping mechanism allows analysis of log data based on the specified source IP addresses.  If you are using SIEM logs to generate alerts, you can find available log fields for existing log parsers using the Fabric Normalization Reference on the Fortinet Document Library.
Log Filters	Select *All* or *Any of the following conditions*. Configure the condition(s): • **Log Field**: Select a log field from the dropdown. After the log device and log type are selected, the *Log Field* dropdown list will only include log fields that belong to the specified log type. For example, the *Botnet IP* log field is available when the *Log Type* is *DNS*, but not available when the *Log Type* is *Event Log*. • **Match Criteria**: Select an operator from the dropdown. The available options depends on the selected log field. Some log fields, such as *Source Port*, will provide a variety of operators in the dropdown list, such as *Equal To*, *Not Equal To*, *Greater Than or Equal To*, *Less Than or Equal To*, *Greater Than*, and *Less Than*. Other log fields, such as *Log Description*, will be limited to *Equal To* and *Not Equal To*.

Option	Description

	• **Value**: Select a value from the dropdown list or enter a value in the text box. The available options depends on the selected log field. If there is no dropdown list provided by FortiAnalyzer, you must manually enter a value to find in the raw log. If a dropdown list is provided, you can select a value from the list. For some log fields, such as *Level*, the dropdown list also allows you to enter a custom value. If there is no textbox to enter a custom value in the dropdown list, you must use the *Generic Text Filter* instead.
	In the **Action** column, click plus (**+**) to insert a new filter below. You can insert multiple filters. To delete a filter, click the **x** next to the filter.
	When generating alerts from SIEM logs, you must include the *Data Source Type* is *Equal To* each of the supported third-party logs. For example, if using Windows and Ubuntu log sources, you may configure the following:
	• *Log Filters = Any One of the Filters*
	  • *Data Source Type Equal To Windows*
	  • *Data Source Type Equal To Ubuntu*
	To view the available third-party log parsers, go to *Incidents & Events > Log Parsers > Log Parsers*.

Generic Text Filter	Enter a generic text filter. See Using the Generic Text Filter on page 311. For information on text format, hover the cursor over the help icon. The operator ~ means contains and !~ means does not contain.
Define Event Conditions	
Trigger an event when:	Select the radio button for one of the following options and configure the criteria: • A group contains `<integer>` or more log occurences • Within a group, the log field `<log field>` has `<integer>` or more unique values • Click the toggle icon to change to "[...] has fewer than `<integer>` unique values" • The sum of `<measure>` is greater than or equal to `<integer>` • Safeguard Risk Score is more than `<value>` • Advanced Mode: This field is used for specialized configuration in select predefined event handler rules. For example, see Geo-alerting event handlers on page 275 and ZTNA login event handlers on page 284.  The "sum" option is used for data exfiltration detection. This option is only supported in Fabric ADOMs. It is not available when using Web Filter, Application Control, or Email Filter log types.

Option	Description
	The "Safeguard Risk Score" option is only available when using Web Filter, Application Control, or Email Filter log types. For an example of a predefined event handler using this trigger, see Safeguarding event handler on page 350.
Add Logic Group	Click the folder icon to add a logic group. You must select a correlation between groups (*AND*, *AND_NOT*, *OR*, *FOLLOWED_BY*, or *NOT_FOLLOWED_BY*). All groups must be met in correlation sequence for the correlation event handler to generate an event. Click the trash icon to delete a logic group.
Show Raw Config	Enable to display the raw config of the correlation sequence. Edits made to the raw config will appear above in the correlation sequence fields. If there is an error in the text, the fields will not display and you will not be able to save the changes.
Correlation Criteria	Specify the fields that the event handler will look for to correlate the rules. Each correlation criteria is applied to two rules, using a field from each rule. Configure the following options for each correlation criteria: • *Rule*: Select two rules to create a correlation criteria for. • *Field*: Select a field for each rule in the correlation criteria. The fields available in the dropdown are determined by the *Group By* field in the rule. • *Match Criteria*: Select an operator from the dropdown. The available options depends on the selected fields. Use the buttons in the *Action* column to add (**+**) or remove (**x**) correlation criteria.
Handler Settings	
Event Type Override	Specify a custom event type, or leave this field blank to use the default value.
Event Message	(Optional) Enter a custom event message. By default, `Group by key-value pair(s)` will be displayed as the event message in *Event Monitor*. Examples: • `Virus:JS/Runfile.B!tr` • `Endpoint:172.17.58.118 Virus:BlackMoon` You can customize event messages by using Group By variables: $groupby1 and $groupby2 Examples: • `Virus $groupby1 found in traffic` • `Endpoint $groupby1 infected with virus $groupby2`

Option	Description
Event Status	Select *Allow FortiAnalyzer to choose* or select a status from the dropdown list: *Unhandled*, *Mitigated*, *Contained*, *(Blank)*. You can use a custom event status by clicking the plus (**+**) that appears in the *Event Status* dropdown. Event statuses, including custom statuses, are displayed in the *Event Status* column in the *Event Monitor*.
Event Severity	Select the severity from the dropdown list: *Critical*, *High*, *Medium*, or *Low*.
Tags	(Optional) Enter custom tags. Tags can be used as a filter when using default or custom views.
Indicators	(Optional) Add indicators by clicking the plus (**+**). You can configure the *Log Field*, *Indicator Type*, and *Count* for each indicator created in an event handler. Use the buttons in the *Action* column to add (**+**) or remove (**x**) indicators. Up to five indicators can be created. When *Indicators* is selected in *Event Monitor > Display Options*, the *Indicators* column displays indicator types for detected events. You can see additional details when clicking on an indicator. See Event Monitor on page 218. If an incident is raised from an event that includes indicators, they can be viewed in the *Indicators* tab of the incident analysis page. See Analyzing an incident on page 208.
Additional Info	Specify what to show in the *Additional Info* column of the *Event Monitor*. Select *Use system default* or *Use custom message*. A custom message can include variables and log field names. For more information, hover over the help icon. You can decode the attackcontext in IPS logs in alert notifications by including the following in the custom message: `${b64_decode (attackcontext)}`. For more information, see Decode the attackcontext field in IPS on page 318.
Notifications	Select a notification profile for the event handler. See Creating notification profiles on page 317.

Using the Automation Stitch for event handlers

All FortiGates added to FortiAnalyzer use a default event handler on the FortiAnalyzer side to receive high severity events such as Botnet Communication, IPS Attack Pass Through, and Virus Pass Through AntiVirus. This basic event handler, *Default-Botnet-Communication-Detection*, has automation stitch enabled in FortiAnalyzer.

Automation Stitch can also be enabled for any custom event handler. See Creating a custom event handler on page 298 and Creating a custom correlation handler on page 304.

To determine if an event handler has automation stitch enabled, review the *Automation Stitch* column in *Incidents & Events* > *Event Handlers* > *Event Handlers*.

When an event is generated by a handler with automation stitch enabled, FortiAnalyzer sends a notification to the FortiGate automation framework. If an automation stitch is configured on the FortiGate, the notification will trigger the related automation stitch and activate an action in response. For example, the FortiGate could send a custom email notification, execute a CLI script, and/or perform a system action in response to the trigger. For more information about automation stitches, including their triggers and actions, see the FortiGate/FortiOS Administration Guide.

The events generated by handlers with the automation stitch enabled can also be viewed in the FortiAnalyzer GUI through *Incidents & Events* > *Event Monitor*.



To receive the notifications from FortiAnalyzer on the FortiGate device, you must configure FortiAnalyzer logging on the FortiGate device.

To use the notifications as part of an automation stitch, you must configure a trigger on the FortiGate device for each event handler that has automation stitch enabled. This includes the predefined event handlers with automation stitch enabled, such as *Default-Botnet-Communication-Detection*.

For more information about configuring FortiAnalyzer logging and automation stitch triggers, see the FortiGate/FortiOS Administration Guide.

Using the Generic Text Filter

The *Generic Text Filter* field is available when creating filters for data selectors and rules for event handlers. When creating an event handler, this field is known as *Log Filter by Text*.

The generic text filter uses the glibc regex library for values with operators that support regular expression (~, !~, and not =, !=), using the POSIX standard. Filter string syntax is parsed by FortiAnalyzer, and both upper and lower case characters are supported (for example, "and" is the same as "AND"). You must use an escape character when needed. For example, `cfgpath=firewall.policy` is the wrong syntax because it is missing an escape character. The correct syntax is `cfgpath=firewall\.policy`.

Operator	Description
=	Exact match. Alternatively, you can use ==.
!=	Does not match.
<	Less than.
<=	Less than or equal to.
>	Greater than.
>=	Greater than or equal to.
~	Matches the regular expression.
!~	Does not match the regular expression.

Tokens:

- (
-)
- &
- |
- and
- or

Example:

```
dstip==192.168.1.168 and hostname ~ "facebook" dstip==192.168.1.168 and ( dstport == 514 or dstport
      == 515 )
```

To create an event handler using the Log Filter by Text to match raw log data:

1. Go to *Log View*, and select a log type.
2. In the toolbar, click *Tools* > *Raw Log*.
   The easiest method is to copy the text string you want from the raw log and paste it into the *Generic Text Filter* or *Log Filter by Text* field. Ensure you insert an escape character when necessary, for example, `cfgpath=firewall\.policy`.
3. Locate and copy the text in the raw log.
4. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers* and click *Create New*.
5. Click *Add New Rule*.
   You can also use the *Log Filter by Text* when creating a rule for a correlation event handler. See Creating a custom correlation handler on page 304.
6. In the *Log Filter by Text* box, paste the text you copied or type the text you want. Ensure you use the raw log field names, for example, `mem` (not memory) and `setuprate` (not setup-rate).
   For information on text format and operators, hover the cursor over the help icon. The operator ~ means contains and !~ means does not contain.
7. Configure other settings for the rule, and click *OK*. For a description of the fields, see Creating a custom correlation handler on page 304.
   You can also use the *Generic Text Filter* in data selectors, which can be assigned to event handlers. For more information, see Creating data selectors on page 316.

Managing event handlers

To manage event handlers, go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.

This pane includes the predefined and custom event handlers. An icon in the *Status* column indicates if the event handler is enabled or disabled.

The following options are available:

Option	Description
Create New	Create a new event handler.
Edit	Edit the selected event handler.

Option	Description
	Some fields in predefined event handlers cannot be modified, such as the name, description and filter settings. However, you can clone the predefined event handler to create a custom event handler and modify its settings according to your needs. You cannot edit the *Event Handler Type*. An icon in the *Name* column indicates if an event handler is a basic event handler or a correlation event handler.
Delete	Delete the selected event handler. You cannot delete predefined event handlers.
Clone	Clone the selected event handler. You can clone a predefined event handler and modify it to create a custom event handler. The cloned event handler will maintain all the settings, including the *Event Handler Type*, which cannot be edited. If you need to change the *Event Handler Type*, you must instead recreate the event handler.
Enable / Disable	Enable or disable the selected event handler to start or stop generating events. The current status is indicated by an icon in the *Status* column. Generated events are displayed on the *Incidents & Events > Event Monitor > All Events* pane.
Show Predefined	Show or hide predefined event handlers in the list.
Show Custom	Show or hide custom event handlers in the list.
Import / Export	Export the selected event handlers or import a event handler that you have exported. You can export event handlers and import them into another ADOM or FortiAnalyzer.
Factory Reset	If you have modified a predefined event handler, return the selected predefined event handler to its factory default settings.

Enabling event handlers

For both predefined and custom event handlers, you must enable the event handler to generate events. The *Status* column displays an icon to indicate which event handlers are enabled. The icon indicates enabled event handlers and the icon indicates disabled event handlers.

To enable event handlers:

1. Go to *Incidents & Events > Event Handlers > Event Handlers*.
2. Select one or more event handlers and click *More > Enable*.
   You can also right-click the event handler and select *Enable*.

Cloning event handlers

Cloning an event handler allows you to build a custom event handler by using an existing one as a template.

Most attributes in a predefined event handler cannot be modified, such as the name, description, and rule settings. You can, however, clone a predefined event handler to customize its settings and give it a meaningful name to show its function.

The cloned event handler will maintain all the settings, including the *Event Handler Type*, which cannot be edited. If you need to change the *Event Handler Type*, you must instead recreate the event handler.

To clone an event handler:

1. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.
2. Select an event handler and in the toolbar and click *Clone*.
   You can also right-click the event handler and select *Clone*.
3. Configure the cloned event handler.
   For a description of the fields, see Creating a custom event handler on page 298 or Creating a custom correlation handler on page 304.
4. Use a descriptive name so it is not confused with the event handler it was cloned from.
5. Click *OK* save the cloned event handler.

Resetting predefined event handlers to factory defaults

You can change some settings in predefined event handlers as needed. If required, you can restore those predefined event handlers to their factory default settings.

To reset predefined event handlers:

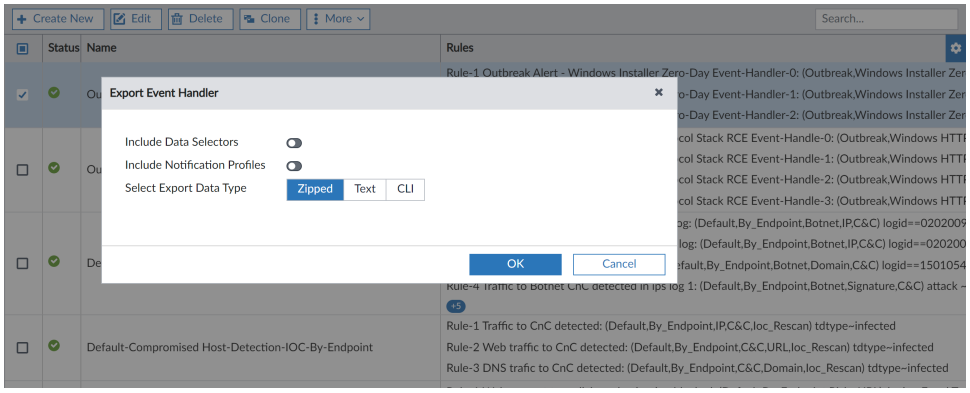
1. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.
2. In the *More* menu, select *Show Predefined*.
3. Select one or more predefined event handlers and click *More* > *Factory Reset*.
   You can also right-click the event handler and select *Factory Reset*.
   If the predefined event handler has not been changed from the factory default settings, this option will be grayed-out.

Importing and exporting event handlers

You can import and export event handlers. This feature allows you to develop custom event handlers and deploy them in bulk to other ADOMs or FortiAnalyzer units. To do so, export the custom event handlers, and then import them into the ADOMs or FortiAnalyzer units where you want them deployed. You can also export event handlers as part of your backup procedure, if needed.

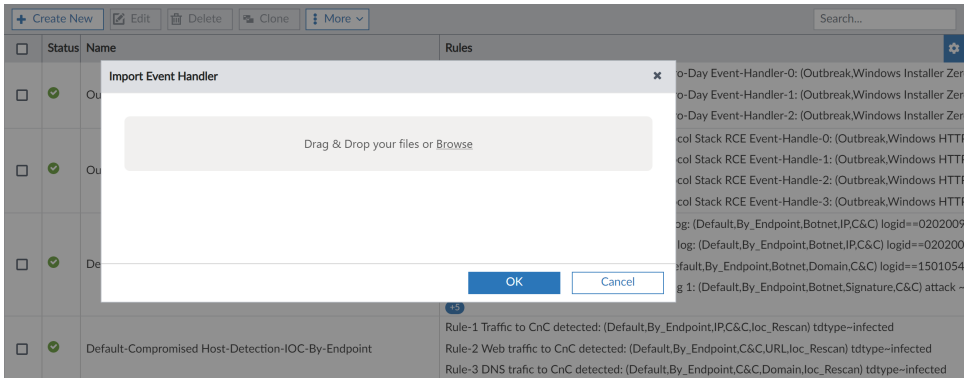
To export event handlers:

1. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.
2. Select the event handler(s) to export, and click *More* > *Export*.
   You can also right-click the event handler and select *Export*.
   If you are exporting basic event handlers and correlation event handlers simultaneously, they will be downloaded in two spearate files: one for basic event handlers and one for correlation event handlers.
3. Enable *Include Data Selectors*, if needed.
4. Enable *Include Notification Profiles*, if needed.
5. In the *Select Export Data Type* field, select *Zipped*, *Text*, or *CLI*.
   If the data type is *Zipped* or *Text*, it will be saved as a JSON file. If the data type is *CLI*, it will be saved as CONF file.
6. Click *OK* to save the export file.



To import handlers:

1. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.
2. Click *More* > *Import*.
   The *Import Event Handler* dialog displays.



3. Drag and drop the exported event handler JSON or CONF file into the import dialog, or click *Browse* to locate the file on the management computer.
   You can import multiple event handlers at a time.
4. Click *OK* to import the event handler(s).

If the imported event handler's name already exists, you will be asked if you want to *Rename*, *Replace*, or *Skip*.

If you select *Rename*, the Unix epoch timestamp will be automatically appended to the imported event handler's name. For example, *App Ctrl Event'1544644459276775*. The name can be edited as required after importing.

If the imported file is the wrong format or has an error, the system will report an error.

Creating data selectors

Data selectors are used to select devices, subnets, and filters for event handlers. You can create, edit, clone, and delete data selectors in *Incidents & Events > Event Handlers > Data Selectors*.

To assign a data selector to a basic event handler, see Creating a custom event handler on page 298.

To assign a data selector to a correlation handler, see Creating a custom correlation handler on page 304.

The filters in the data selector are applied before every rule configured in the event handler. This means the filter criteria does not need to be added individually within each rule of the event handler(s) that the data selector is assigned to.

The default data selectors are used in some of the predefined handlers, and they cannot be edited or deleted.

To create a data selector:

1. Go to *Incidents & Events > Event Handlers > Data Selectors*.
2. Click *Create New*.
   The *Add New Data Selector* pane displays.
3. Configure the following options, and click *OK* to save the data selector.

Option	Description
Name	Enter a name for the data selector.
Devices	Select one of the following: • *All Devices*. • *Specify*: Select the devices to include. • *Local Device*: Select if the event handler is for local FortiAnalyzer event logs. This option is only available in the root ADOM and is used to query FortiAnalyzer event logs. For *Local Device*, the *Log Type* must be *Event Log* and *Log Subtype* must be *Any*.
Subnets	Select *All Subnets* to include all subnets, or select *Specify* to choose which subnet(s) or subnet group(s) will be included or

Option		Description
		excluded from triggering events. For more information, see Subnets on page 191.
Filters		Click plus (**+**) to insert a new filter in the list. The *Filter* dialog displays. Configure the options and click *OK* to save. To delete a filter from the list, click the **x** next to the filter.
	Name	Enter a name for the filter.
	Log Device Type	Select the device type from the dropdown.
	Log Type	Select a log type from the dropdown. The log types will vary depending on the device type.
	Log Subtype	Select a log subtype from the dropdown. The log subtype is not available for all device types.
	Logs match	Select *All* or *Any of the following conditions*. Click plus (**+**) to insert a new condition. You can insert multiple conditions. Configure the condition(s): • *Log Field*: Select a log field from the dropdown. • *Match Criteria*: Select an operator from the dropdown. • *Value*: Select the event type from the dropdown. To delete a condition, click the *delete* icon next to the condition.
	Generic Text Filter	(Optional) Enter a filter string. For more information, see Using the Generic Text Filter on page 311.

Creating notification profiles

Notification profiles are used to send alert notifications when an event is generated by an event handler. You can configure the notification profile to send the alert to an email address, SNMP community, and/or syslog server. You can also configure the notification profile to send the alert through a fabric connector.

You can create, edit, clone, and delete notification profiles in *Incidents & Events > Event Handlers > Notification Profiles*.

To assign a notification profile to a basic event handler, see Creating a custom event handler on page 298.

To assign a notification profile to a correlation handler, see Creating a custom correlation handler on page 304.

To create a notification profile:

1. Go to *Incidents & Events > Event Handlers > Notification Profiles*.
2. Click *Create New*.
   The *Add New Notification Profile* pane displays.

3. Configure the following options, and click *OK* to save the notification profile.

Option	Description
Name	Enter a name for the notification profile.
Send Alert through Fabric Connectors	Send an alert through one or more fabric connectors selected from the dropdown. Click the plus (**+**) to add fabric connectors. For more information, see Connector actions on page 364.
Send Alert Email	Send an alert to one or more email addresses. Specify the email parameters, including the mail server. For more information, see Mail Server on page 537.
To	Enter the email address(es) to send the alert to. Use a semicolon (**;**) to separate multiple email addresses.
From	Enter a from address for the alert email.
Subject	Enter a subject line for the alert email.
Email Server	Select the mail server for the alert email.
Send SNMP(...) Trap	Send an alert to an SNMP community or user selected from the dropdown. For more information, see SNMP on page 483.
Send Alert to Syslog Server	Send an alert to the syslog server selected from the dropdown. For more information, see Syslog Server on page 539.
Send Each Alert Separately	Enable to send each alert individually instead of in a group.
Schedule	Enable to send notifications only during a specified time period.
Days	Select *All* to allow notifications for all days. Select *Specify* to select the days to allow notifications. By default, Monday to Friday are selected.
Time	Select *All* to allow notifications at all times during the specified days. Select *Specify* to configure a time range to allow notifications during. See *Start Time* and *Stop Time* options below. By default, the *Start Time* is *09:00 AM* and the *Stop Time* is *05:00 PM*.
Start Time	From the dropdown, select the start of the time range to allow notifications.
Stop Time	From the dropdown, select the end of the time range to allow notifications.

Decode the attackcontext field in IPS

The attackcontext field in IPS logs can be decoded within alert notifications and forwarded logs. This can help you to better understand the nature of the threats, such as the specific type of attack and its potential impact.

This feature is only for decoding attackcontext in IPS logs; no other fields and log types are supported for this feature.

To decode the attackcontext field in IPS logs for alert notifications:

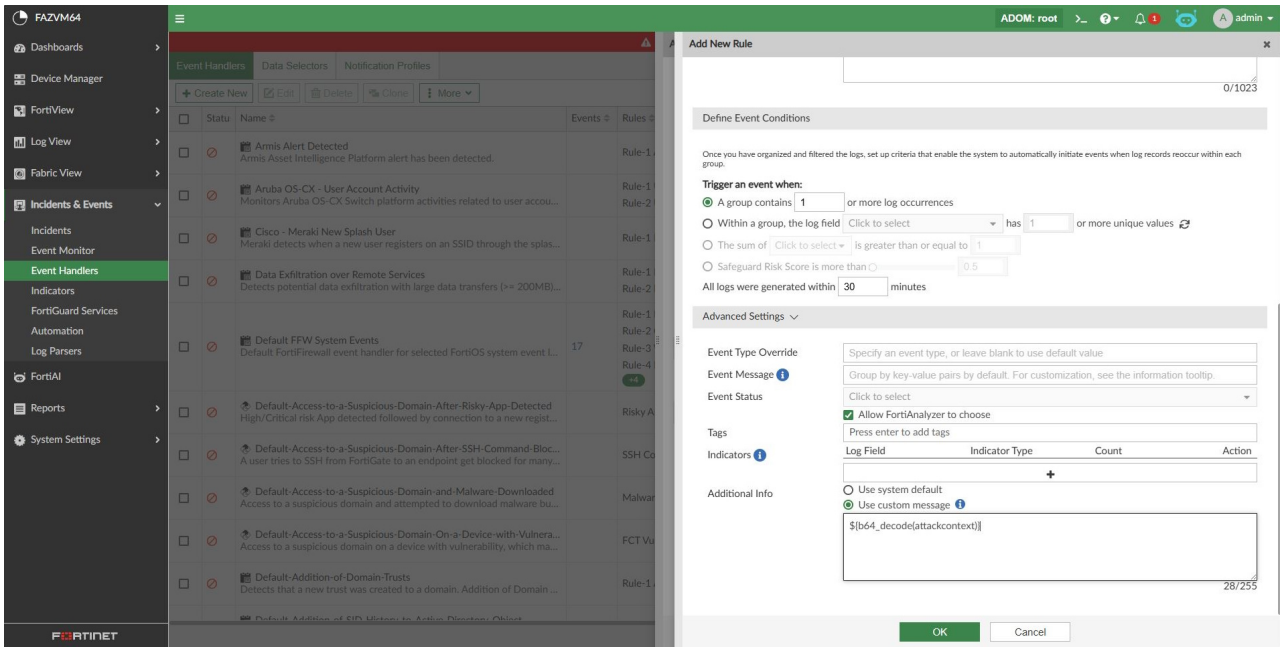
1. In *Incidents & Events > Event Handlers > Notification Profiles*, configure a notification profile for email and/or syslog notifications.

Send Alert Email	Enable and specify the email parameters, including the mail server.
Send Alert to Syslog Server	Enable and select the syslog server from the dropdown.

2. In *Incidents & Events > Event Handlers > Event Handlers*, configure an event handler to use this notification profile.
3. In the new event handler, configure an event handler rule for IPS logs:

Log Device Type	*FortiGate*
Log Type	*IPS (ips)*
Log Field	*Attack Name (attack)*

4. For the event handler rule, configure the custom message to include the following:
   `${b64_decode(attackcontext)}`



This ensures the attackcontext is decoded in the notification alerts to syslog and email servers.

To decode the attackcontext field when forwarding logs to a syslog server:

Configure log forwarding to a syslog server with `fwd-syslog-decode-b64` enabled:

```
config system log-forward
   edit <id>
      set mode forwarding
      set fwd-server-type syslog
      set fwd-syslog-decode-b64 enable
```

Variable	Description
fwd-syslog-decode-b64 {enable | disable}	Enable/disable base64 decoding when forwarding logs to syslog server. This command is only available when the mode is set to `forwarding` and `fwd-server-type` is `syslog`.

For example:

```
config system log-forward

    edit 1

        set mode forwarding

        set fwd-max-delay realtime

        set server-name "xxxxx"

        set server-addr "xxxxx"

        set fwd-server-type syslog

        set fwd-reliable enable

        set fwd-syslog-decode-b64 enable

            config device-filter

                edit 1

                    set adom "root"

                    set device "FGVMxxxxx"

                next

            end

end
```

Reduce delay and improve notification performance

FortiAnalyzer can support a high volume of alert notifications (for example, 25000+) with minimum delay.

In previous versions, there can be cache related delays in multiple steps before writing to the database or sending a high volume of notifications:

1. The fortilogd could take more than three seconds to write to files after logs are received.
2. Once logs are written to files, the sqllogd worker can have a more than three second delay before processing.
3. Once alerts are generated, the sqllogd worker secondary can cache these alerts for up to five seconds before writing them to Redis.

4. When the fazalertd retrieves alerts from Redis, it may cache for up to five seconds before writing to the database or sending notifications.

In addition, there were faznotify capacity and Redis performance limitations in previous versions. The faznotify would only allow one thread and one connection to send notification messages, and Redis, on port 6380, was unable to handle 25000 notification messages per second.

Beginning in FortiAnalyzer 7.6.4, the caching times are reduced to 20-50 milliseconds. The faznotify is also enhanced with the following:

- the faznotify connector supports multiple threads with parallel processing.
- synchronous HTTP requests are converted to asynchronous, allowing each faznotify worker to manage up to 30 concurrent connections.

A new Redis instance is also introduced on port 6390 to store notification messages, distributing the load between 6380 and 6390 at a 1:2 ratio respectively. Notification messages are bundled and compressed before sending to Redis, with each package containing up to 30 individual notifications.

To send a high volume of notifications (for example, 25000+) using more workers in the webhook connector:

1. In the FortiAnalyzer CLI, enable `log-process-fast-mode`.
   ```
   config system log settings
      set log-process-fast-mode enable
   end
   ```
   This option is not mandatory and it is disabled by default, but enabling it will reduce the delay time.
2. Create a generic webhook connector, including the intended number of workers in the connector name: `<name>${worker:<number of workers>}`
   For example, the connector name `webhook-${worker:1}` means one worker is running. You can update this name to indicate `2`, `3`, `4`, or more workers according to your needs.
   For more information about creating a generic connector, see Configuring ITSM connectors on page 378.

   The connector should be HTTP-based.

3. Create a notification profile to send alerts through the new connector.
   The notification profile should include the following option:

Send Alert through Fabric Connectors	Enabled. Select the generic webhook connector created in the previous step.

   For more information about creating a notification profile, see Creating notification profiles on page 317.
4. Create or edit an event handler that will use the connector to send notifications.
   For more information about creating an event handler, see Creating a custom event handler on page 298.
   a. From the *Notifications* dropdown, select the notification profile created in the previous step.
   b. Configure the other event handler settings as needed.
   c. Edit or create a rule.
   d. In the *Tags* field, include `MonitorAndNotifyOnly`.
      With this tag set, no alert is generated in FortiAnalyzer; the handler will only send notifications.

e. Configure the other rule settings as needed.
f. Configure other rules with the `MonitorAndNotifyOnly` tag as needed.
g. Save the rule and the event handler.

Notifications will be sent according to the rule(s) in the event handler. FortiAnalyzer will support sending a high volume of alerts with minimum delay.

CLI troubleshooting commands

In the FortiAnalyzer CLI, you can use the following diagnose commands to check and troubleshoot delays for alert generation.

To show Send rate, Message-queue stats, Sender stats, and Sender total connections with server:

```
diagnose test application faznotify 2 speed
```

To clear all stat data:

```
diagnose test application faznotify 2 clear
```

To show all connecters and workers:

```
diagnose test application faznotify 3 * *
```

To reset all connectors' counter:

```
diagnose test application faznotify 3 * * reset
```

To clear message queue buffer when server is not reachable:

```
diagnose test application faznotify 29 root *
```

To reset all notification related counter:

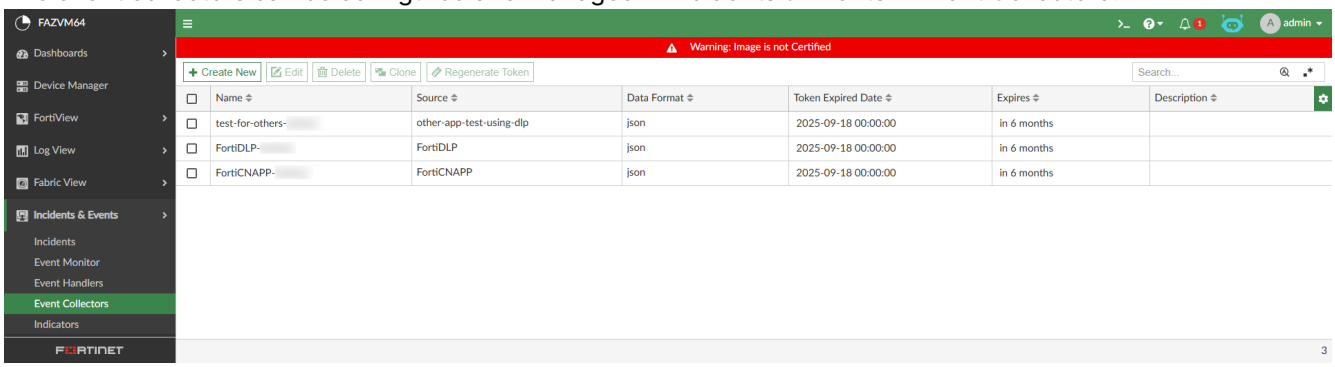
```
diagnose test application fazalertd 200 stat reset
```

Event collectors

FortiAnalyzer includes an HTTP-based event ingestion service called Fabric Event Collector (FEC). This service listens on specified ports, such as 8443, and accepts incoming alerts in JSON format. The events are parsed, normalized, enriched, and then displayed in *Event Monitor* and *Log View*. The system also handles throttling, logging, and supports filtering and suppression. Previously, FortiAnalyzer could not receive or interpret event data directly from FortiDLP, FortiCNAPP, or similar external systems through HTTP POST/webhook.

This feature improves integration between FortiAnalyzer and other security products. It eliminates the need for external log forwarding systems and provides a centralized, real-time view of multi-product alerts. This enhances event response, compliance monitoring, and threat correlation capabilities for customers using multiple products.

The event collectors can be configured and managed in *Incidents & Events > Event Collectors*.

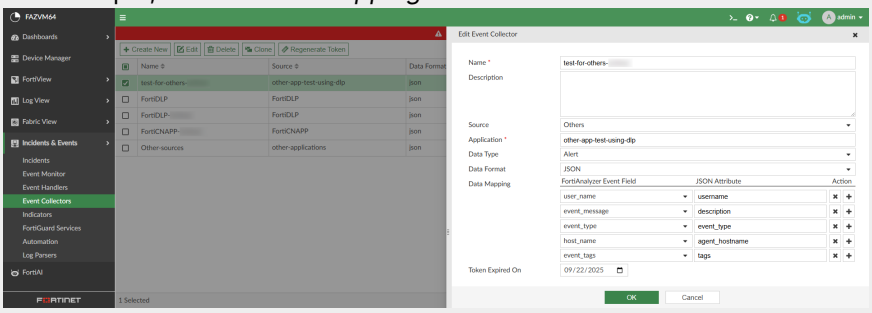


Once the event collector is configured, you will generate an access token that can be configured in the webhook for the related application to grant access to FortiAnalyzer. After the webhook is configured, the event collector will ingest logs that can be viewed in *Log View*. These logs will also be used to generate events that will be visible in the *Event Monitor*.

To create an event collector:

1. Go to *Incidents & Events > Event Collectors*.
2. Click *Create New*.
   The *Add New Event Collector* pane displays.
3. Configure the following options:

Name	Enter a name for the event collector.
Description	Enter a description for the event collector (optional).
Source	Select one of the following sources: • *FortiDLP* • *FortiCNAPP* • *Others*
Application	This option is only available when the *Source* is *Others*. Enter the application that will be used as the source. This will be displayed as the *Device Type*, *Data Source Type*, and *Data Source Name* for ingested logs.
Data Type	Select the data type to be received by the event collector, such as *Alert*.
Data Format	Select the data format to be received by the event collector, such as *JSON*.
Data Mapping	This option is only available when the *Source* is *Others*. Configure the data mapping for FortiAnalyzer event fields to related JSON attributes. Add and map FortiAnalyzer event fields as needed.

	For example, see the *Data Mapping* below. 
Token Expired On	Enter the expiry date for the token. By default, the token expiry is six months after the event collector is configured.

4. Click *Generate Token*.

   The *Access Token* displays.

   This token grants access to the FortiAnalyzer. This is the only chance to copy and save the token, so it is important to copy it now before proceeding to configure the webhook in FortiDLP, FortiCNAPP, or the other application.
5. Copy the access token and proceed to configure the webhook in the related application for the event collector.

   See Configuring the webhook on page 325.

Once the event collector is created, it can be edited, deleted, or cloned from the *Event Collectors* pane.

To regenerate an access token:

1. Go to *Incidents & Events > Event Collectors*.
2. Select the event collector and click *Regenerate Token*.

   The *Regenerate Token* pane displays.
3. Enter the *Token Expiration Date*.
4. From the *Last Token Time To Live* dropdown, select the amount of time the previous token should remain valid.

   The *Last Token Time To Live* is how long the previous token remains valid before a new token is generated, but it cannot extend beyond its original expiration time.
5. Copy the access token and proceed to replace the previous access token in the webhook configuration.

   See Configuring the webhook on page 325.

To troubleshoot using the CLI:

1. In the FortiAnalyzer CLI, enter the following command to show how many messages have been forwarded to fortilogd. This includes FEC data and other types as well.

   ```
   diagnose test app oftpd 7
   ```
2. In the FortiAnalyzer CLI, enter the following command to show how many FEC messages have been received from oftpd if there is a line starting with FEC.

   ```
   diagnose test app fortilogd 2
   ```

Configuring the webhook

Once you have generated the access token for the FortiAnalyzer event collector, you must configure the webhook in the related application.

This topic includes instructions to configure the webhook URL in FortiDLP and Lacework FortiCNAPP. To configure the webhook URL when the source for the event collector is *Others*, see documentation for the application that you are using.

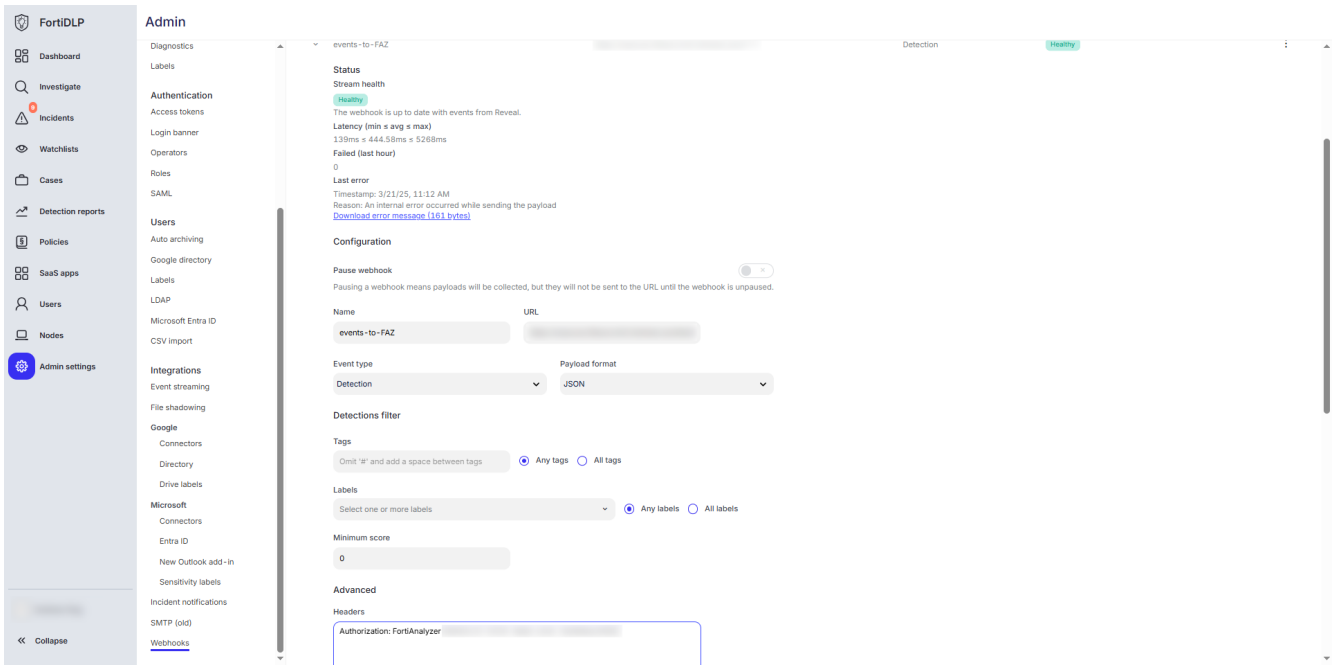


When configuring a webhook in FortiDLP or FortiCNAPP, the endpoint URL must use https. Thus, FortiAnalyzer must allow access for https and have a valid certificate to enable the connection.

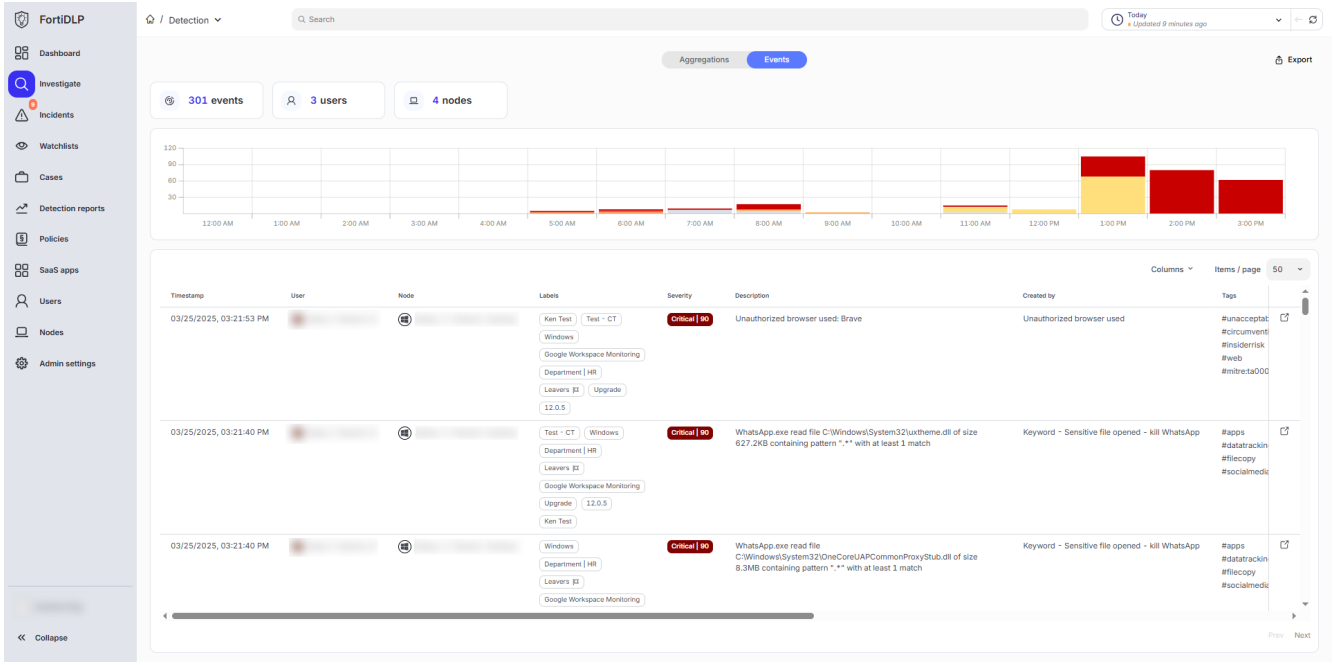
To configure the webhook in FortiDLP:

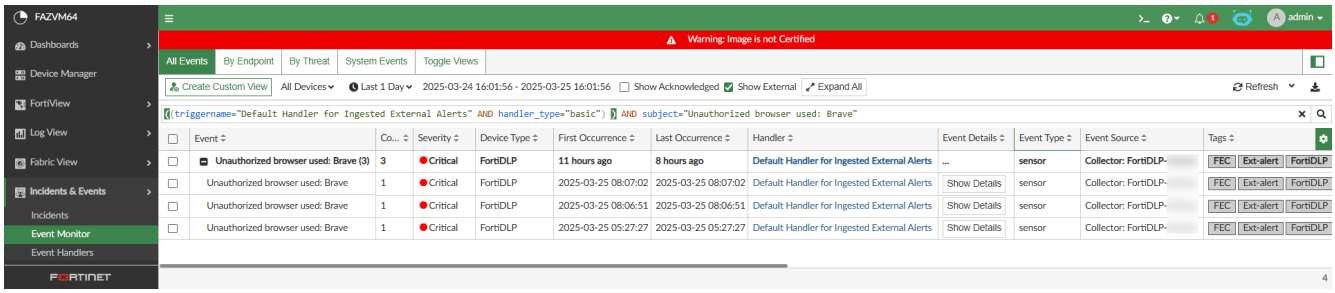
1. In FortiDLP, go to *Admin Setting* > *Webhooks*.
2. Click *Create new webhook*.
3. In the *Name* field, enter a name for the webhook.
4. In the *URL* field, enter the FortiAnalyzer URL with `/fazfec` added to the end.
   For example, `https://faz.fortinet.net/fazfec`.
5. From the *Event Type* dropdown, select *Detection*.
6. From the *Payload format* dropdown, select *JSON*.
7. In the *Headers* field, enter the following pattern, replacing `<token>` with the access token for the event collector:
   `Authorization: FortiAnalyzer <token>`
8. Configure the other options according to your needs and save the webhook.

For more information about configuring webhooks in FortiDLP, see the FortiDLP Administration Guide on the Fortinet Document Library.



The events can now be viewed in both FortiDLP and the FortiAnalyzer *Event Monitor*. For example, see the images below.

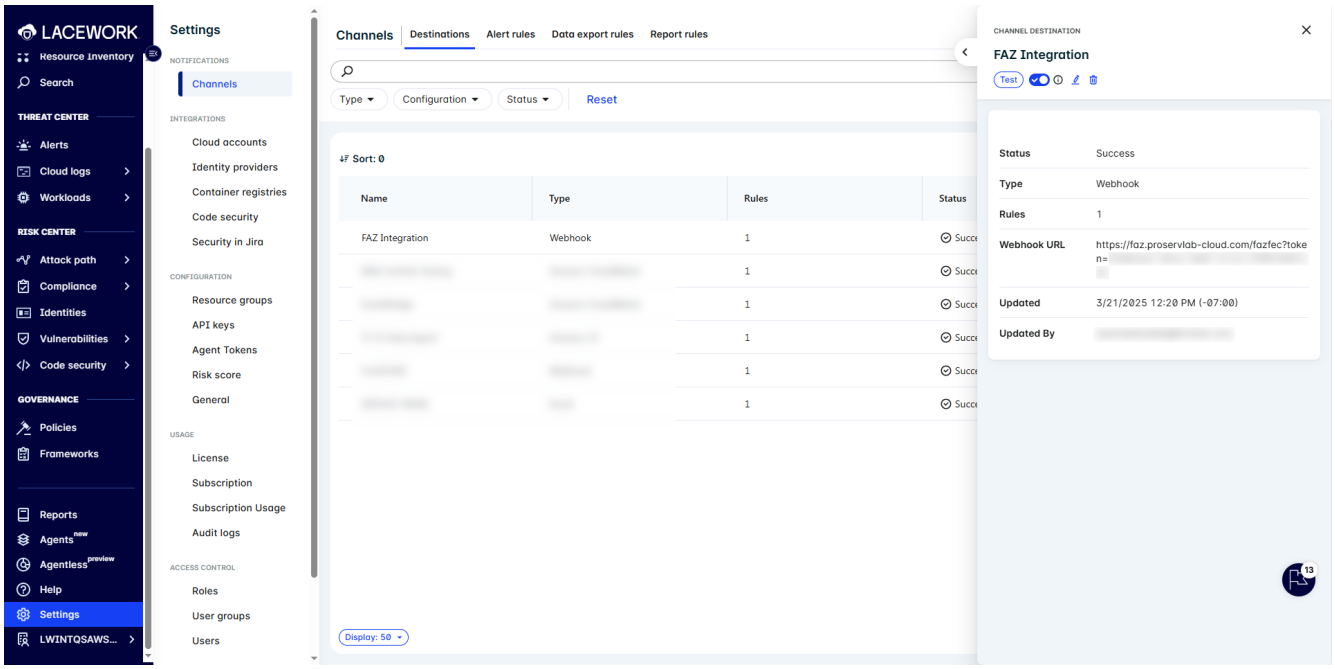




To configure the webhook in FortiCNAPP:

1. In FortiCNAPP, go to *Settings* > *Channels* > *Destinations*.
2. Add a destination and set the *Webhook URL* as follows, replacing `<token>` with the access token for the event collector:
   `https://faz.proservlab-cloud.com/fazfec?token=<token>`

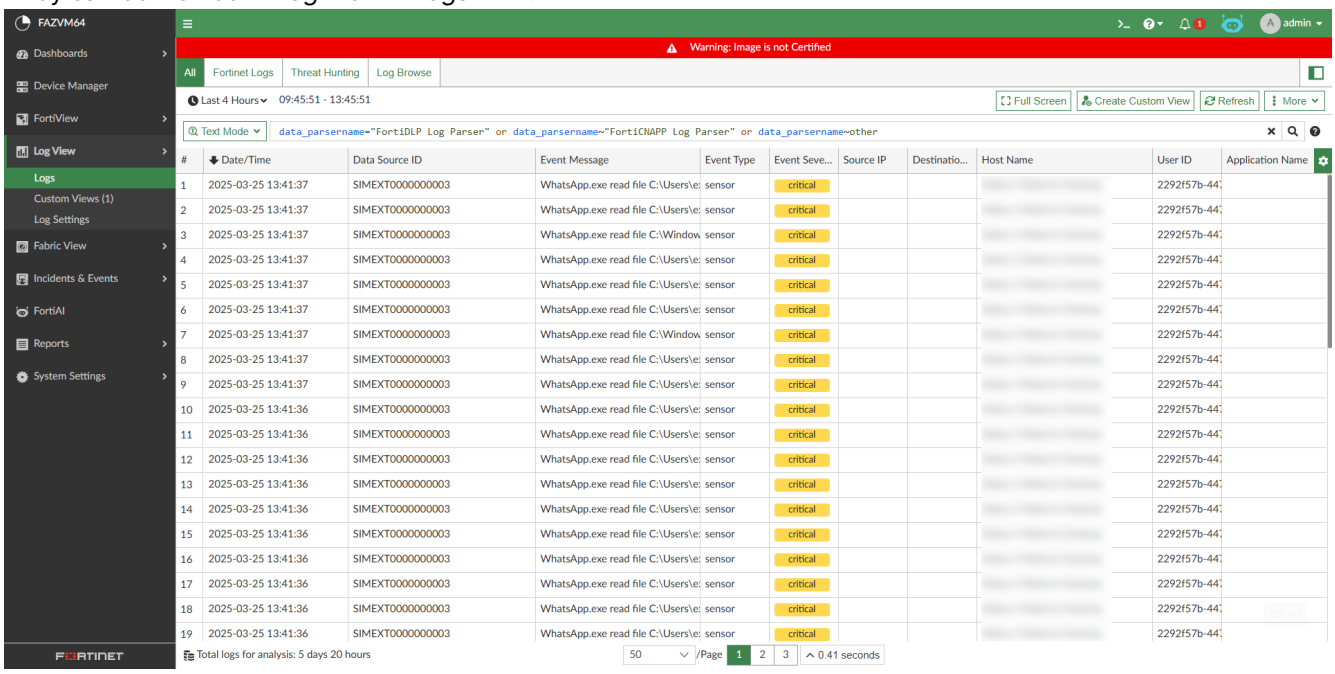
For more information about configuring the webhook URL in FortiCNAPP, see the Lacework FortiCNAPP Administration Guide on the Fortinet Document Library.



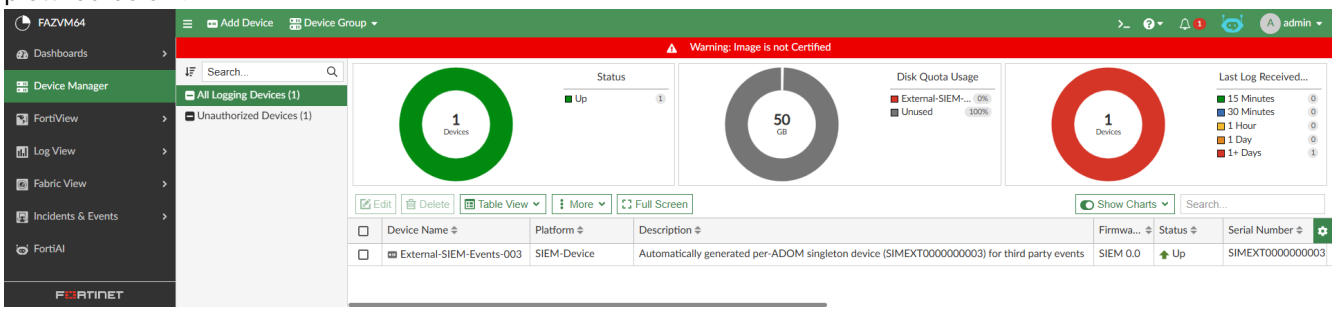
Event collector logs

Once the event collector and webhook have been configured, the relevant external alerts can be seen in FortiAnalyzer.

These ingested alerts are parsed and normalized using predefined and automatically generated log parsers. They can be viewed in *Log View* > *Logs* > *All*.



As seen in the *Log View* image above, all ingested alerts are displayed under the SIEM device, which is an automatically generated per-ADOM singleton device for third-party events. An example of the SIEM device is pictured below.



The predefined and automatically generated log parsers for event collectors can be found in *Incidents & Events* > *Log Parsers* > *Log Parsers* with the category *Fabric Event Collector* (FEC).

Log Parser	Description
FortiCNAPP Log Parser	Automatically available and used to parse logs ingested by the event collectors with FortiCNAPP as the source.
FortiDLP Log Parser	Automatically available and used to parse logs ingested by the event collectors with FortiDLP as the source.
FEC_<event collector Name>	Automatically created when an event collector is configured with *Others* as the source. The log parser is named after the related event collector and uses the data mapping to parse and normalize the logs.

Event collector events

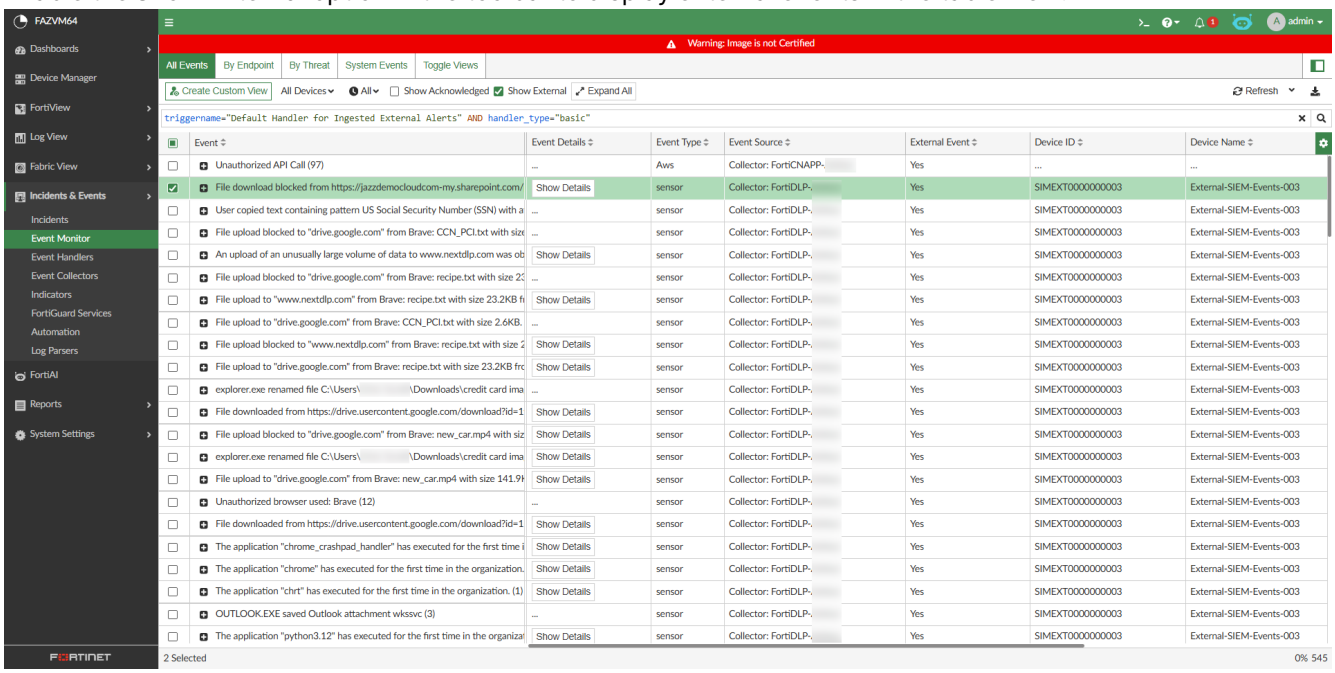
To support event collector configuration, there is a predefined basic event handler that will generate events based on the alerts ingested by the event collectors. This allows you to view the events within *Incidents & Events > Event Monitor* so you can review details and document incident reports conveniently within FortiAnalyzer.

In *Incidents & Events > Event Handlers > Event Handlers*, the predefined *Default Handler for Ingest External Events* is enabled by default to generate events using alerts ingested by the event collectors.

There are three rules in this event handler corresponding to the three source options for event collectors:

Rule	Description
FortiDLP Ingested Event	Triggers events for external alerts from FortiDLP. Event Severity: Low Log Field: Host Name, User Name, Log Unique ID Log Filter by Text: `data_sourcetags~"ext-alert" and data_sourcename="FortiDLP"` Triggers an event when a group contains 1 or more log occurences. All logs were generated within a duration of 1 minute. Tags: FEC, Ext-alert, FortiDLP
FortiCNAPP Ingested Event	Triggers events for external alerts from FortiCNAPP. Event Severity: Low Log Field: Host Name, User Name, Log Unique ID Log Filter by Text: `data_sourcetags~"ext-alert" and data_sourcename="FortiCNAPP"` Triggers an event when a group contains 1 or more log occurences. All logs were generated within a duration of 1 minute. Tags: FEC, Ext-alert, FortiCNAPP
Default Ingested Event	Triggers events for external alerts from other applications with event collectors configured in FortiAnalyzer. Event Severity: Low Log Field: Host Name, User Name, Log Unique ID Log Filter by Text: `data_sourcetags~"ext-alert" and data_sourcename!="FortiDLP" and data_sourcename!="FortiCNAPP"` Triggers an event when a group contains 1 or more log occurences. All logs were generated within a duration of 1 minute. Tags: FEC, Ext-alert

Events generated by this event handler can be viewed in *Incidents & Events* > *Event Monitor* > *All Events*. Enable the *Show External* option in the toolbar to display external events in the table view.



The following columns in *Event Monitor* can be used to help you track and review external events:

Column	Description
Event Source	Displays the collector name that ingested the related event.
Tags	Displays the tags in the FEC alerts as well as the tags configured in the event handler rules.
Event Details	Displays *Show Details* when applicable. Click *Show Details* to display the *Event Details* pane.
External Event	Displays *Yes* when the event is ingested through an event collector.

For more information about using the Event Monitor and creating incidents, see All Events on page 221.

Indicators

The *Incidents & Events* > *Indicators* pane consolidates all detected indicators for centralized analysis. This streamlines threat evaluation and enables SOC analysts to take swift action to mitigate risks.

Managing indicators

Indicators can be found in *Incidents & Events* > *Indicators*. This pane contains a chart view and table view of the indicators.

There are four charts in the chart view:

- *Indicator Type*
- *Reputation*
- *Enrichment Status*
- *Block Status*

By default, all the charts are displayed. From the *Show Charts* dropdown, you can toggle which charts display. You can also toggle *Show Charts* to hide all charts, when needed.

Select a value in any of the charts to apply the filter to all charts and the table view. To remove the filter, click the chart title.

The following actions are available in the toolbar:

Action	Description
Create New	Create a new indicator. Once the indicator is created, the *Source* column will display the admin that created it. Indicators cannot be edited. Instead, you can delete the indicator and create a new indicator if needed.
Delete	Delete the indicator.
Enrich	Enrich the indicator.
Block	Block the indicator.

The following columns are available in the table view:

Column	Description
Indicator	The indicator name.
Type	The indicator type: • *IP* • *URL* • *Domain*
Block Status	The block status for the indicator: • *TBD* • *Blocked (Pending)* • *Blocked* • *Unblocked* By default, new indicators are saved with the status as *TBD*.
Rating Confidence	The rating confidence from FortiGuard.

Column	Description
Reputation	The reputation from VirusTotal: • *Malicious* • *Suspicious* • *Harmless* • *Undetected*
Enrichment Status	The enrichment status: • *Enriched (completed)* • *No enrichment* • *No data*
Source	The source of the enrichment: • *<administrator name>* • *auto-created*

To create an indicator:

1. Go to *Incidents & Events* > *Indicators*.
2. Click *Create New*.
3. From the *Indicator* dropdown, select the indicator type.
4. In the *Indicator Value* field, enter the appropriate value for the indicator type (IP, URL, or domain).
5. Click *Create*.

To delete an indicator:

1. Go to *Incidents & Events* > *Indicators*.
2. Select and indicator, and click *Delete*.
3. To confirm the deletion, click *OK*.

To enrich an indicator:

1. Go to *Incidents & Events* > *Indicators*.
2. Select and indicator, and click *Enrich*.
   Alternatively, you can double-click the indicator or right-click the indicator and click *Enrich*.
   The *Enrich* pane displays.
3. Review the details in the *Enrich* pane.
4. Click *Save Enrichment* or *Cancel* according to the review.
   The indicator will only be processed and enriched after clicking *Save Enrichment*.

For more information about indicator enrichment, see Indicator enrichment on page 333.

To block an indicator:

If there the FortiAnalyzer does not have an authorized FortiManager connector, the *Block* option will be grayed out.

1. Go to *Incidents & Events* > *Indicators*.
2. Select a suspicious indicator, and click *Block*.

   When an indicator is blocked, the *Block Status* column will initially display *Blocked (Pending)*. In the backend, a playbook called *Block_indicator* runs every five minutes to send the information to FortiManager. After the playbook is run, the status for the indicator will change to *Blocked*.

   If a blocked indicator must be unblocked, select the blocked indicator and click *Unblock*.

For more information about blocking and unblocking indicators, see Blocking indicators on page 334.

Indicator enrichment

The indicator enrichment feature empowers security analysts by providing them with comprehensive threat intelligence on identified IP addresses, domains, and URLs. This enriched context allows for a deeper understanding of security incidents, leading to more informed and effective response decisions.

FortiAnalyzer uses FortiGuard and VirusTotal enrichment services to evaluate the risk possessed by the indicators. These services are used by means of a predefined playbook in FortiAnalyzer: *Indicator Enrichment*. This playbook is enabled by default and is read-only. It can be found in *Incidents & Events* > *Automation* > *Playbook*.

The FortiGuard enrichment services are built-in and ready to use, but VirusTotal requires an API Key in the fabric connector.

To setup the VirusTotal Connector:

1. Go to *Incidents & Events* > *Automation* > *Active Connectors*.
2. Double-click the *VirusTotal* connector.
3. In the *API Key* field, update the API key.
4. Click *OK*.
5. Enable the *VirusTotal* connector.

   When this connector is enabled, indicator enrichment will provide the VirusTotal information.

You can enrich indicators from the *Indicator* pane, or from an incident that contains the indicator. When an incident is raised from an event, the event's indicators are attached to the incident.

To enrich an indicator from and incident:

1. Go to *Incident & Events* > *Incidents* > *Incidents*.
2. Select the related incident and click *Analysis*.

   You can also enrich the indicator from the toolbar in the table view.

   The *Enrich* option is only available when there are indicators that can be enriched. Private IP addresses are not valid IP indicators.

3. Click *Enrich*.

   The *Enrich* pane displays.
4. Review the details in the *Enrich* pane.

5. Click *Save Enrichment* or *Cancel* according to the review.
   The indicator will only be processed and enriched after clicking *Save Enrichment*.

When indicators are enriched, FortiAnalyzer will display the following information:

Section	Description
FortiGuard CTS	Displays the indicator confidence, IOC tags, IOC, antivirus, and web filter categories.
VirusTotal Summary	Displays a Risk Summary, a *Detection* tab, and a *Details* tab.
Risk Summary	Displays detailed security vendor analysis, presenting a comprehensive list indicating whether each vendor has detected the indicator, along with their assigned risk category if detected.
Detection	Displays detailed security vendor analysis, presenting a comprehensive list indicating whether each vendor has detected the indicator, along with their assigned risk category if detected.
Details	Displays the *Whois Summary* and *Whois Lookup*, providing essential information such as organization details, address, data source, and contact information.



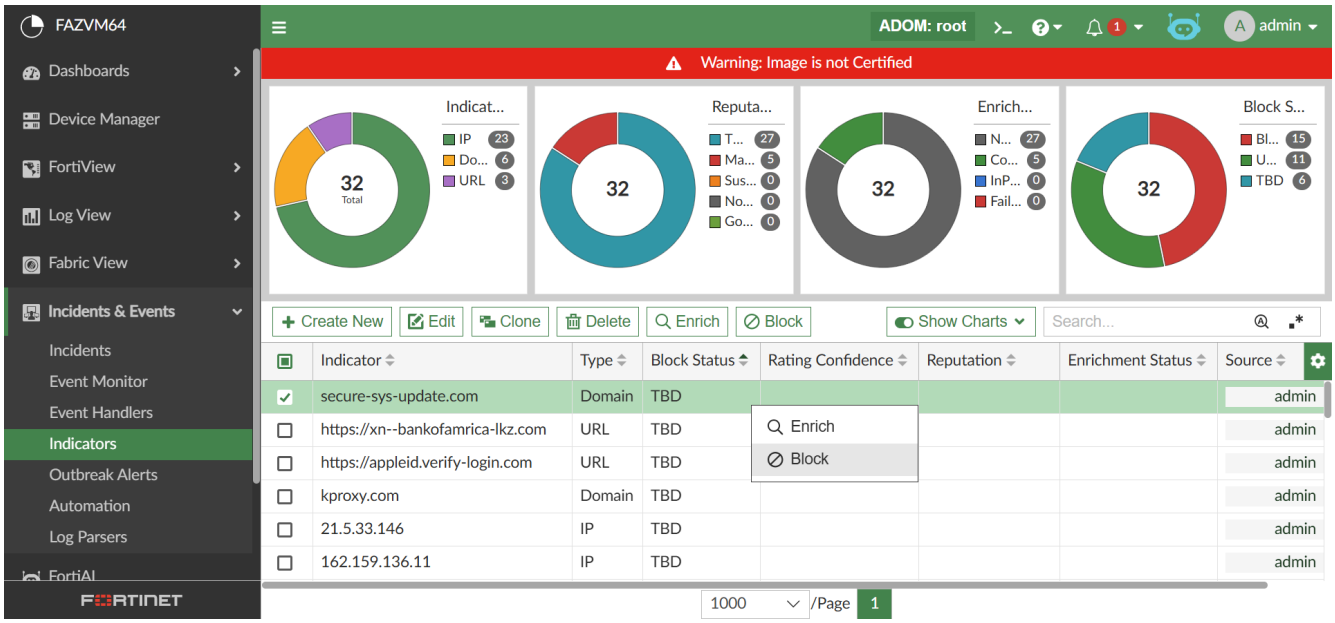
Saving the same enrichment would update the existing entry in the history. A new entry will only be created when there are changes in the enrichment.

Blocking indicators

You can block suspicious indicators directly from FortiAnalyzer. This can help you to reduce potential risks and quickly respond to known threats by blocking suspicious IPs, URLs, or domains.



To block indicators, you must setup an authorized FortiManager connector for the FortiAnalyzer. See To setup the FortiManager connector on FortiAnalyzer:.



The *Block* indicator option is available in:

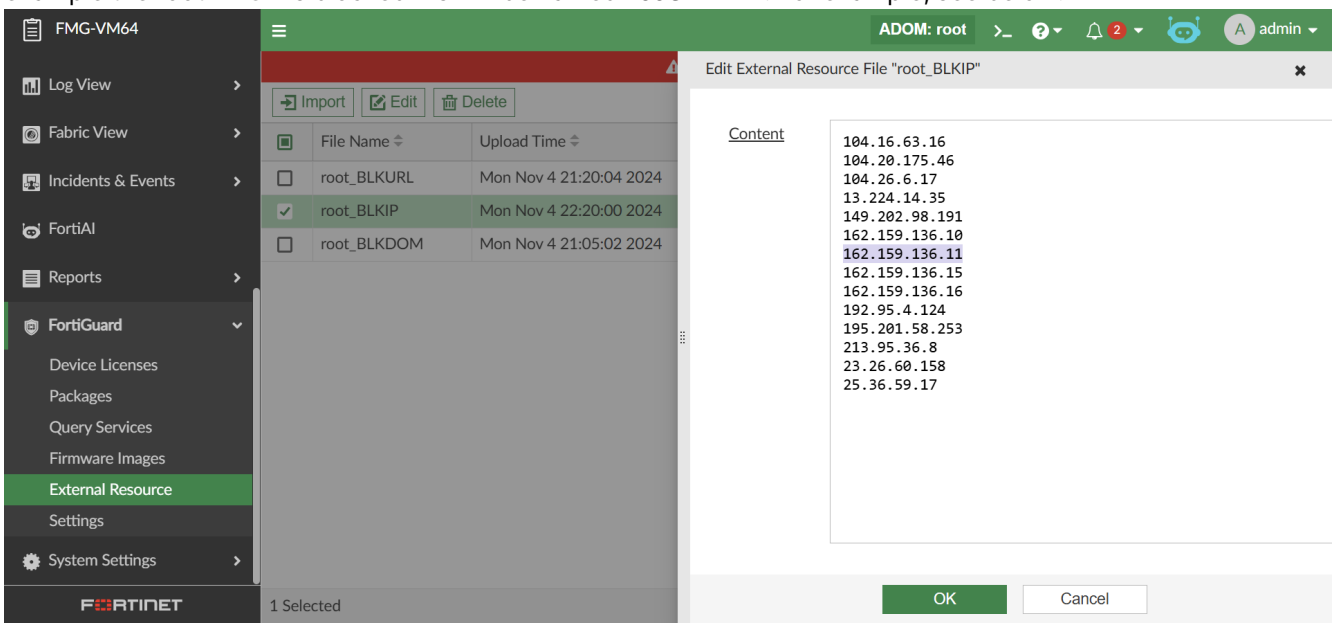
- *Incidents & Events > Indicators*
- *Incidents & Events > Incidents > Incidents*
- *Incidents & Events > Incidents > Incidents > Incident Analysis*

In *Incidents & Events > Indicators*, there is a pie chart and column to display the *Block Status* of the indicators: *TBD*, *Blocked*, and *Unblocked*.

When an indicator is blocked, the *Block Status* column will initially display *Blocked (Pending)*. In the backend, a playbook called *Block_indicator* runs every five minutes to send the information to FortiManager. After the playbook is run, the status for the indicator will change to *Blocked*. The *Blocked* status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to the FortiGate.

When the *Block_indicator* playbook is successfully run, the blocked indicator will be pushed to FortiManager's *External Resource* list. This list will be used to create threat feeds, security profiles, and policy blocks on FortiManager to push the policies to the identified FortiGate. It can also be used to update all FortiGates to block the suspicious indicators.

The *External Resource* is saved in FortiManager as "`<FortiAnalyzer ADOM name>-BLK<indicator-type>`". For example the root ADOM's blocked IPs will be named `root-BLKIP`. For example, see below.



The FortiManager firmware version must be the same as FortiAnalyzer for the block list to be pushed to FortiGates.

Indicators can also be unblocked from the FortiAnalyzer GUI. When a blocked indicator is selected in *Incidents & Events > Indicators*, the *Unblock* action becomes available in the toolbar and shortcut menu. Unblocking the indicator updates the *External Resource* on FortiManager by removing the unblocked indicator information. Once complete, the status of the indicator changes to *Unblocked*.

To setup the FortiManager connector on FortiAnalyzer:

The following configuration is required in the FortiManager CLI before adding a FortiAnalyzer using a fabric connection:

```
config system csf
   set status enable
   set accept-auth-by-cert enable
end
```

In both the FortiAnalyzer and FortiManager CLI, under `config system interface`, the port's `allowaccess` setting must include `fabric`.

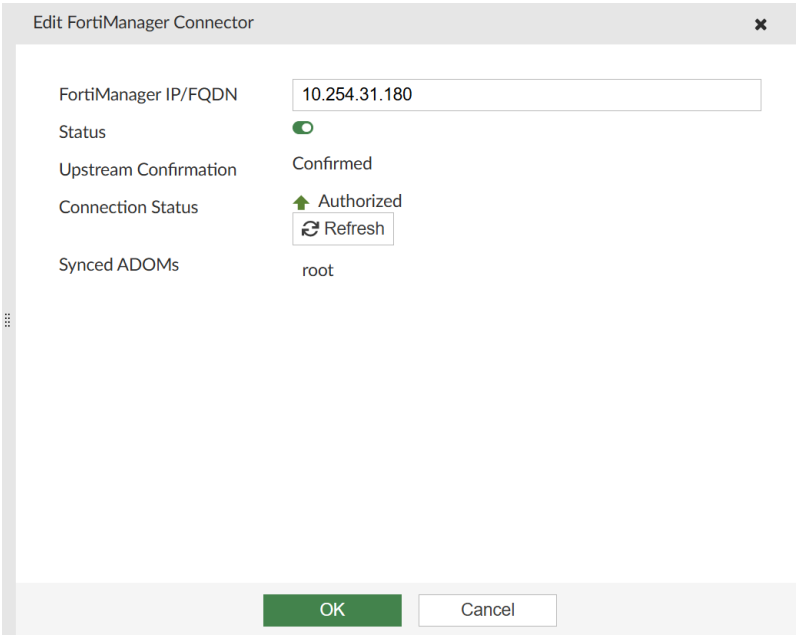
For more information, see the FortiManager Administration Guide.

1. In the FortiAnalyzer, go to *Incidents & Events > Automation > Active Connectors*.
2. Double-click the *FMG Connector*.
   The *Edit FortiManager Connector* pane displays.
3. In the *FortiManager IP/FQDN* field, enter the IP of the FortiManager.
4. Toggle the *Status* to *Enabled*.
5. Click *OK* and wait for the connection.

6. Once the connection status is *Pending Authorization*, click *Authorize*.
7. In the authorization page, select the ADOM to add the FortiAnalyzer to and click *Next*.
8. After authorizing, the FortiAnalyzer is added to FortiManager under *Device Manager* > *Device & Groups* > *Managed FortiAnalyzer*.

   Alternatively, you can authorize the FortiAnalyzer from the FortiManager GUI.

If the FortiManager connector is not setup or if the status is down, the *Block* option will be grayed out in the *Incidents* and *Indicators* panes.



FortiGuard Services

The *Incidents & Events* > *FortiGuard Services* pane displays content from FortiGuard, including SOC automation content packs, safeguarding keywords, and Outbreak Alerts. To receive this information from FortiGuard, FortiAnalyzer must be connected to the FortiGuard Distribution Servers (FDS) and have a valid license for the following FortiGuard services depending on the use case:

- Security Automation Service
- Security Rating Update
- Industrial Security Service
- Outbreak Detection Service

The Security Automation Service provides content packs from FortiGuard; however, the Security Rating Update and Industrial Security Service may be required for certain reports. The Outbreak Detection Service is required to receive information about outbreak alerts, including predefined event handlers and reports from FortiGuard.

The *Incidents & Events > FortiGuard Services* pane displays information about the objects provided by these services, which can be used to support threat hunting, incident investigation, and incident response. The related event handlers, reports, playbooks, and connectors received from FortiGuard can be found in their respective panes in FortiAnalyzer.

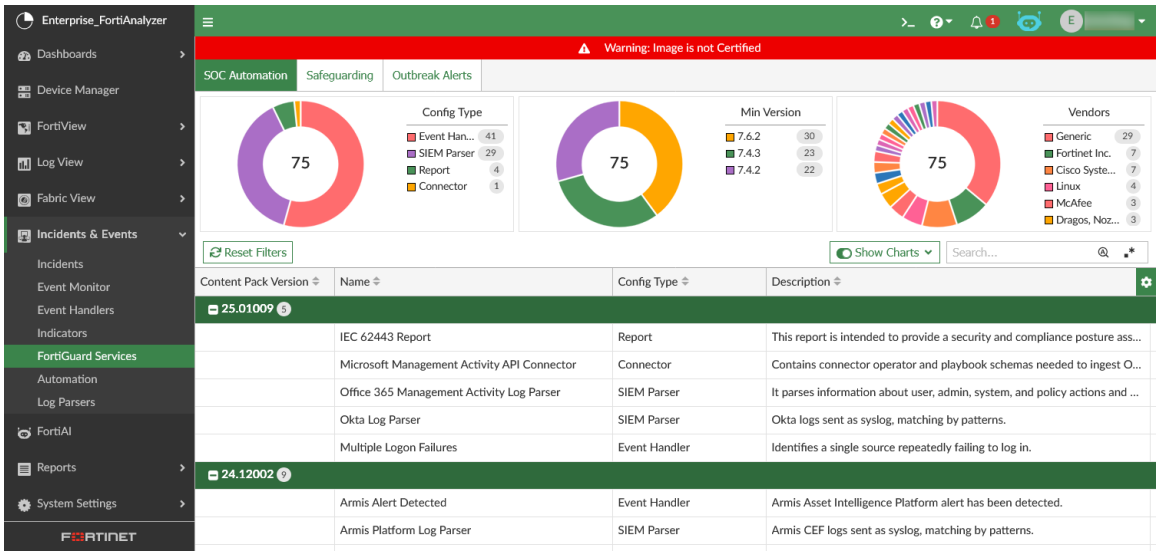
SOC Automation

The FortiAnalyzer Security Automation Service is a license that provides content packs released from FortiGuard on a monthly basis. The content packs include premium reports, event handlers, advanced correlation rules, third-party log parsers, and more. These tools are designed to help you detect, investigate, and respond to security incidents. For more information about this service, see *FortiAnalyzer Security Automation Service* on the FortiGuard website.

To confirm you have a valid Security Automation Service license in FortiAnalyzer, see the License Information widget on page 63.

With a valid Security Automation Service license, the content pack release is applied automatically in FortiAnalyzer when it is available from the FortiGuard Distribution Server (FDS). The details of the content pack, including the list of log parsers, event handlers, and/or reports, are available on the FortiGuard website and in the FortiAnalyzer GUI.

To view the content packs that have been applied in your FortiAnalyzer, go to *Incidents & Events > FortiGuard Services > SOC Automation*.



The objects applied by the Security Automation Service are listed in a table view. In this pane you can only review what objects are available. To find review the object configuration and make changes within your licensed FortiAnalyzer, see Finding Security Automation Service objects on page 340.

By default, three charts display above the table to summarize the number of objects by:

- *Config Type*
- *Min Version*
- *Vendors*

Toggle *Show Charts* to enable or disable these charts. Alternatively, you can enable or disable select charts from the *Show Charts* dropdown.

The table provides a complete list of objects organized by content pack. You can expand or collapse the content packs according to your needs. You can use the *Search* field to find an object in the table.

The following columns are available for the table. You can use the settings icon above the table to add or remove columns according to your needs.

Column	Description
Content Pack Version	The version the content pack was released or modified on. For more information, see the FortiGuard website.
Name	The name of the object.
Config Type	The type of object: *Report*, *SIEM Parser*, *Event Handler*, or *Connector*. You will be able to find the object in the FortiAnalyzer GUI according to the config type. For more information, see Finding Security Automation Service objects on page 340.
Description	A brief description for the object and its use case.
Status	The status update for that object in the content pack: *New* or *Modified*.
Release Date	The date the object was released or modified as part of the content pack.
Vendor	The vendor the object type was created to integrate with.
Min Version	The minimum required version of FortiAnalyzer to use the object.

You can set filters for the table using the column headers.

To set filters for the table:

1. Mouse over the column header and click the filter icon.
2. Select the type of filter:
   - *Contains*
   - *Exact Match*
3. Toggle *NOT* to enable, if needed.
   When enabled, the filter will be does *NOT* contain or is *NOT* an exact match according to your selection for the filter type.
4. Use the *Search* field to find the appropriate terms for your filter.
   To add a new term for the filter, type the string and click the plus icon.
5. From the available list, select the appropriate filter(s).
   You can also use the *Select all* or *Deselect all* buttons to help make your selection.
6. Click *Apply*.
   The table is now filtered according to the results for this column. You can add filters to other columns as well, if needed.
   A filter icon displays in the column header.

To remove a filter for the table:

To quickly remove all filters for the table, click *Reset Filters* above the table. To remove only select filters, follow the steps below.

1. Click the filter icon in the column header.
2. Remove the filters individually, or click *Remove* to remove all the filters applied using that column.
3. If you removed the filters individually, click *Apply* to save your changes.

Finding Security Automation Service objects

The FortiAnalyzer Security Automation Service includes support for the *RHSP* FortiGuard package which is used to share updated reports, event handlers, SIEM parsers, and connectors as content packages. RHSP FortiGuard package objects are only applied with a valid Security Automation Service license.

To review the list of objects, go to *Incidents & Events > FortiGuard Services > SOC Automation*. Based on the *Config Type* for the object, you can find the objects in the following panes in the FortiAnalyzer GUI:

- **Reports**: Go to *Reports > Report Definitions > All Reports*.
  Reports included in the RHSP package are stored on the global level. They are displayed in the global *Security Automation Reports* folder. The global folder and global reports are identified with the system theme's color applied to the icon. Reports delivered by the RHSP package are displayed with *Origin = FortiGuard*.
- **Event handlers**: Go to *Incidents & Events > Event Handlers > Event Handlers*.
  Event handlers delivered by the RHSP package are displayed with *Origin = FortiGuard*.
- **SIEM parsers**: Go to *Incidents & Events > Log Parsers > Log Parsers*.
  Log parsers delivered by the RHSP package are displayed with *Origin = FortiGuard*.
- **Connectors**: Go to *Incidents & Events > Automation > Active Connectors*.
  You will need to create and configure the connector for your environment. For example, see Microsoft management activity API connector on page 340.

Microsoft management activity API connector

The Microsoft Management Activity API connector is available as part of version 25.01009 content pack.

When configured to connect to your Microsoft Management Activity API, this connector can be used to perform the following actions:

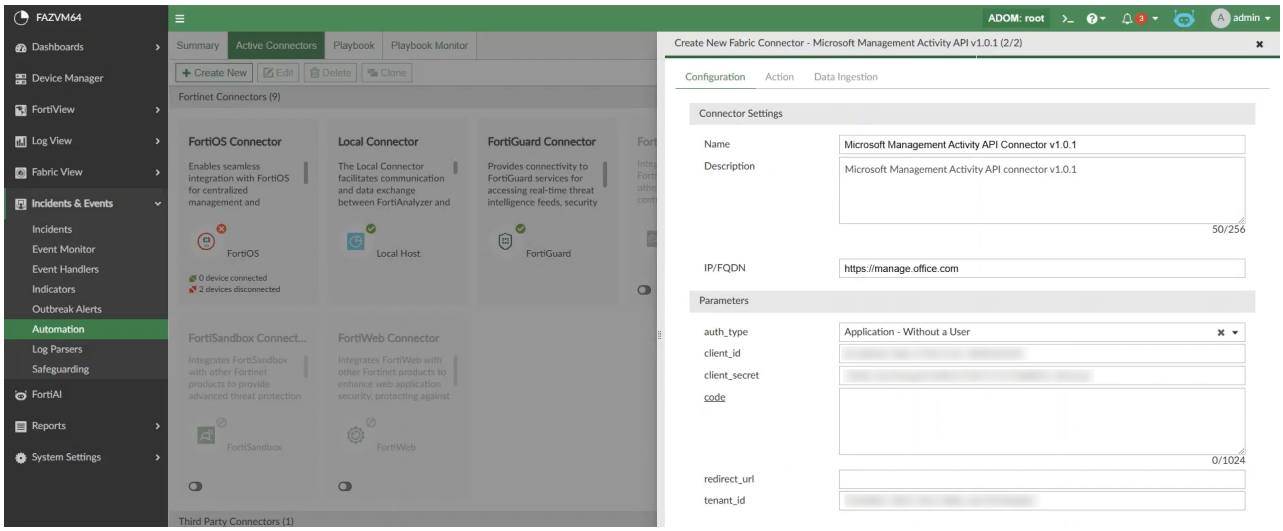
Action	Description
Ingest Microsoft Management Activity API Logs	Ingest Office 365 and Azure AD activity logs from the Microsoft Management Activity API. When this action is run for the first time, it will automatically create an authorized device and assign it to the Office 365 Management Activity Log Parser. For this first run of the action, all logs from the last 24 hours will be ingested. In subsequent runs of this action, only new logs since the last fetch will be ingested and added to FortiAnalyzer.

Action	Description
	To use this action successfully, you must enable the *Office 365 Management Activity Log Parser*, which is also introduced in the version 25.01009 content pack. See To enable the Office 365 Management Activity Log Parser:. To use this action as part of a playbook, see To use the Microsoft Management Activity API connector in a playbook:.
MS Management Activity Start Subscription	Starts a subscription in Microsoft.
MS Management Activity Stop Subscription	Stops a subscription in Microsoft.
MS Management Activity List Subscription	Retrieves a current list of subscriptions in Microsoft.
MS Management Activity List Content	Retrieves content from Microsoft.

To configure the Microsoft Management Activity API connector:

1. Go to *Incidents & Events* > *Automation* > *Active Connectors*, and click *Create New*.
2. For the connector type, select *Microsoft Management Activity API v1.0.1* and click *Next*.
3. In the *Configuration* tab, configure the following options:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Microsoft Management Activity API.
auth_type	Select one of the following: • *Application - Without a User* • *Delegated - On behalf of User*
client_id	Enter the client ID for the Microsoft Management Activity API.
client_secret	Enter the client secret for the Microsoft Management Activity API.
code	Enter the code. This field is only required when the *auth_type = Delegated - On behalf of User*.
redirect_url	Enter the redirect URL. This field is only required when the *auth_type = Delegated - On behalf of User*.
tenant_id	Enter the tenant ID for the Microsoft Management Activity API.



4. In the *Action* tab, view the actions available with the connector.
5. In the *Data Ingestion* tab, enable or disable the *Status* according to your needs.
   This feature allows you to define schedules for when to pull the logs from the external resource.
   When enabled, configure the following:

Option	Description
Schedule Selection	Select *Single Schedule* or *Custom Schedule*. • *Single Schedule*: configure the data ingestion schedule for all available enabled actions. • *Custom Schedule*: select each enabled action and click *Edit* to configure its data ingestion schedule.
The start time of the schedule	Select the date and time to begin the data ingestion schedule.
The end time of the schedule	Select the date and time to end the data ingestion schedule.
The interval unit of the schedule	Select the unit to set the interval for the schedule: • *N-MINUTES* • *N-HOURS* • *N-DAYS* • *CRON*
The interval value of the schedule	Set the integer. This is the interval for data ingestion according to *The interval unit of the schedule*. For example: • *The interval unit of the schedule* = N-HOURS • *The interval value of the schedule* = 5 Data ingestion is scheduled for every 5 hours.
Actions	Enable the *Actions* that should perform data ingestion at the set schedule.

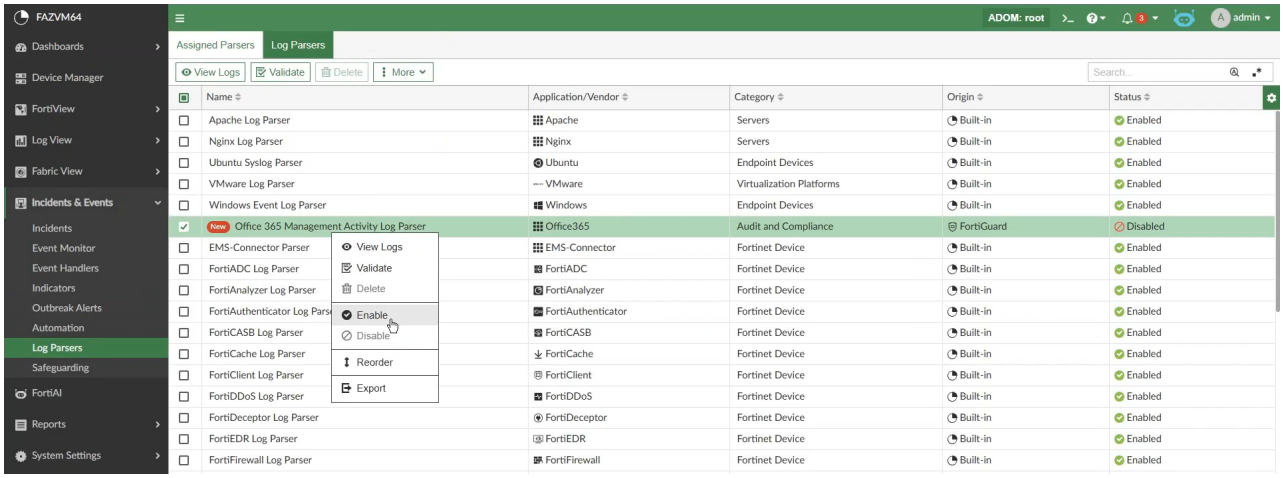
Option	Description
	Data ingestion schedules can only be configured for some actions; these actions are indicated in the *Actions* tab for the connector.

6. To save the configuration, click *OK*.
   This connector and its status is now visible in the *Active Connectors* pane. It can be used as part of playbooks to perform the actions that were visible in the *Actions* tab.

To enable the Office 365 Management Activity Log Parser:

This log parser is disabled by default. It must be enabled to properly ingest and parse logs using the Microsoft Management Activity API connector.

1. Go to *Log Parsers > Log Parsers* and select the *Office 365 Management Activity Log Parser*.
2. From the *More* dropdown, select *Enable*.
   Alternatively, you can right-click the log parser and select *Enable* from the shortcut menu.

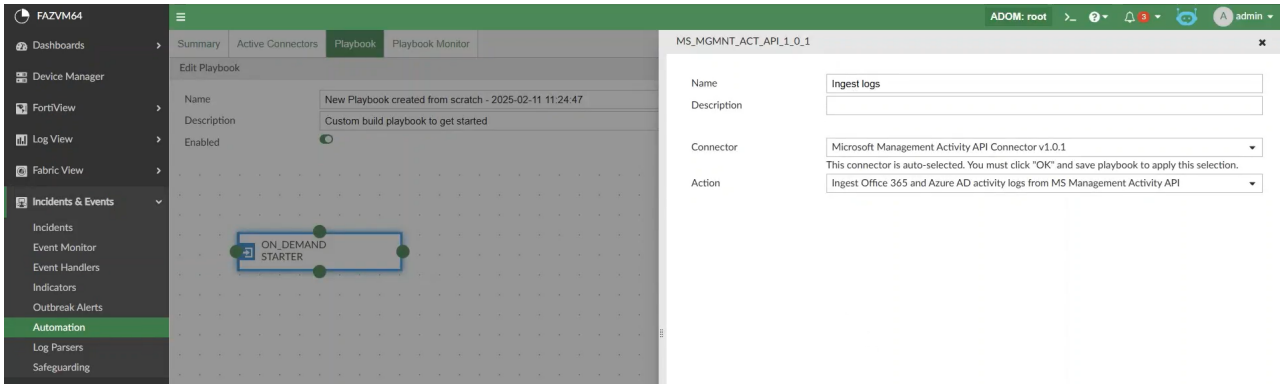


To use the Microsoft Management Activity API connector in a playbook:

1. Go to *Incidents & Events > Automation > Playbook*, and click *Create New*.
2. Select *New Playbook created from scratch*.
3. Select a trigger for the playbook. In this example, the playbook will be triggered *ON_DEMAND*.
4. Drag-and-drop any connector point from the trigger to add a new task.
   The *Tasks* pane displays available connectors.
5. Select the Microsoft Management Activity API connector.
6. Configure the automated action for the connector, and then click *OK*:

Option	Description
Name	Enter a name for the action
Description	Enter a description for the action.
Connector	The connector is automatically selected.

Option	Description
Action	Select the action for the connector to perform as part of this playbook. In this example, the *Ingest Office 365 and Azure activity logs from MS Management Activity API* action is used.

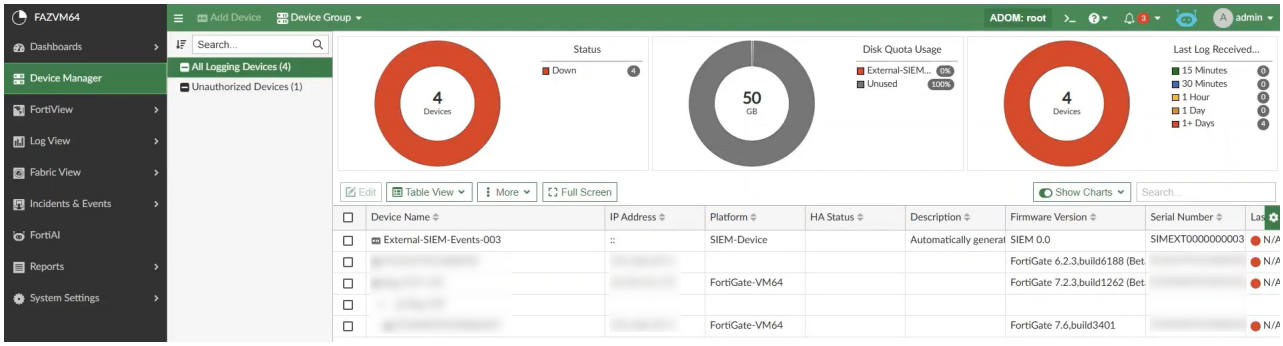


7. Enter a *Name* and *Description* for the playbook.
8. Save the playbook.

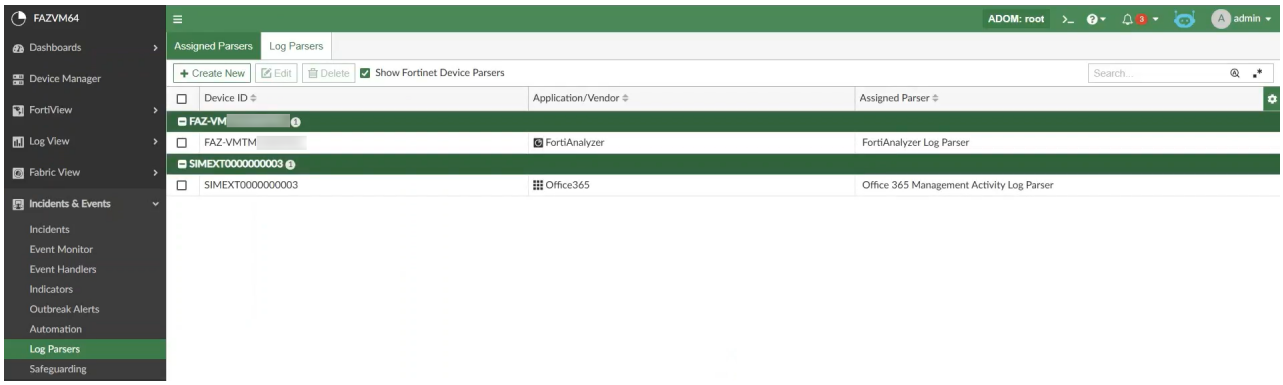
The *Office 365 Management Activity Log Parser* must be enabled to parse the logs ingested by this playbook. See To enable the Office 365 Management Activity Log Parser:..

This playbook can now be run to ingest activity logs through the Microsoft Management Activity API connector.

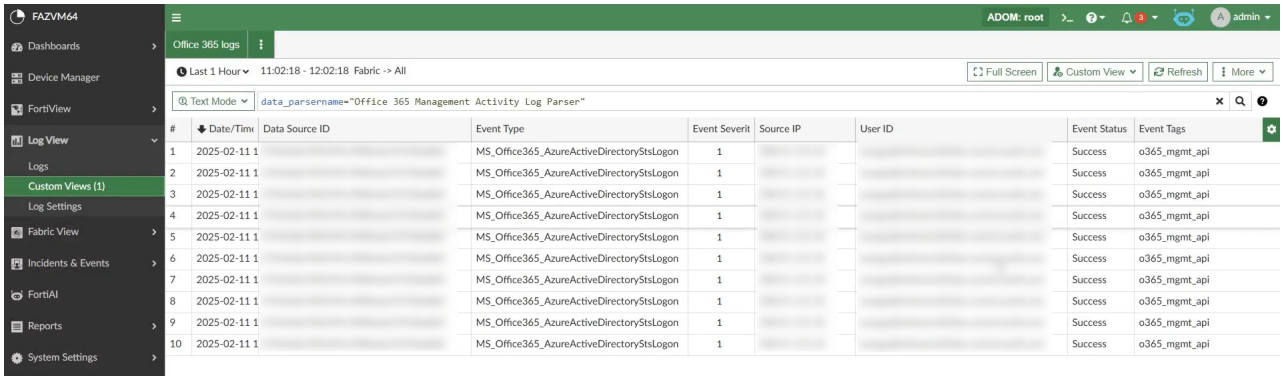
When this playbook is run for the first time, a new device is automatically created and authorized in *Device Manager*.



This device is also automatically assigned to the related *Office 365 Management Activity Log Parser* in *Incidents & Events > Log Parsers > Assigned Parsers*.



The ingested logs can be viewed in *Log View* > *Logs* > *Log Browse* or *Log View* > *Logs* > *All*. The logs can also quickly be found using the following filter: `data_parsername="Office 365 Management Activity Log Parser"`. For example, see the *Custom View* below filtered for the ingested logs.



Microsoft 365 Defender connector

The Microsoft 365 Defender connector is available as part of version 25.05005 content pack.

This connector facilitates the automation of operations related to files, machines, IP, domain, actor, etc., and supports the ingestion of Microsoft 365 Defender incidents into FortiAnalyzer. For more information, see Supported Microsoft Defender XDR APIs in the Microsoft documentation.

When configured to connect to your Microsoft 365 Defender, this connector can be used to perform the following actions:

Action	Description
Advanced Hunting	Retrieves data from the past 30 days based on the query that you have specified.
Get Incident Details	Retrieves the details of a specific incident based on the incident ID that you have specified.
Get Incidents List	Retrieves a list of flagged network incidents with their status, allowing users to filter by time range, owner, and other details to support informed cybersecurity response. This action is configurable with *Data Ingestion*.

Action	Description
	You must enable the Microsoft 365 Defender Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Get Incidents List (Microsoft 365 Defender Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Microsoft 365 Defender Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *Microsoft 365 Defender Log Parser* assignment. On this first run of the playbook, the connector will ingest incidents from the last seven days. In subsequent runs, it will ingest only new or updated incidents since the last run. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="Microsoft 365 Defender Log Parser"`.
Update Incident	Updates the owner, status, comments, and other details of existing incidents based on the incident ID that you have specified.

To enable the Microsoft 365 Defender Log Parser:

This log parser is disabled by default. It must be enabled to properly ingest and parse logs using the Microsoft 365 Defender connector.

1. Go to *Incidents & Events* > *Log Parsers* > *Log Parsers* and select the *Microsoft 365 Defender Log Parser*.
2. From the *More* dropdown, select *Enable*.
   Alternatively, you can right-click the log parser and select *Enable* from the shortcut menu.

To configure the Microsoft 365 Defender connector:

1. Go to *Incidents & Events* > *Automation* > *Active Connectors*, and click *Create New*.
2. For the connector type, select *Microsoft 365 Defender v1.0.0* and click *Next*.
3. In the *Configuration* tab, configure the following options:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Microsoft 365 Defender.
auth_type	Select one of the following: • *Application - Without a User* • *Delegated - On behalf of User*

Option	Description
client_id	Enter the client ID for the Microsoft 365 Defender.
client_secret	Enter the client secret for the Microsoft 365 Defender.
code	Enter the code. This field is only required when the *auth_type = Delegated - On behalf of User*.
redirect_url	Enter the redirect URL. This field is only required when the *auth_type = Delegated - On behalf of User*.
tenant_id	Enter the tenant ID for the Microsoft 365 Defender.

4. In the *Action* tab, view the actions available with the connector.
5. In the *Data Ingestion* tab, enable or disable the *Status* according to your needs.
   This feature allows you to define schedules for when to ingest logs from the external resource.
   When enabled, configure the following:

Option	Description
Schedule Selection	Select *Single Schedule* or *Custom Schedule*. • *Single Schedule*: configure the data ingestion schedule for all available enabled actions. • *Custom Schedule*: select each enabled action and click *Edit* to configure its data ingestion schedule.
The start time of the schedule	Select the date and time to begin the data ingestion schedule.
The end time of the schedule	Select the date and time to end the data ingestion schedule.
The interval unit of the schedule	Select the unit to set the interval for the schedule: • *N-MINUTES* • *N-HOURS* • *N-DAYS* • *CRON*
The interval value of the schedule	Set the integer. This is the interval for data ingestion according to *The interval unit of the schedule*. For example: • *The interval unit of the schedule* = N-HOURS • *The interval value of the schedule* = 5 Data ingestion is scheduled for every 5 hours.
Actions	Enable the *Actions* that should perform data ingestion at the set schedule. Data ingestion schedules can only be configured for some actions; these actions are indicated in the *Actions* tab for the connector.

6. To save the configuration, click *OK*.
   This connector and its status is now visible in the *Active Connectors* pane. It can be used as part of playbooks to perform the actions that were visible in the *Actions* tab.

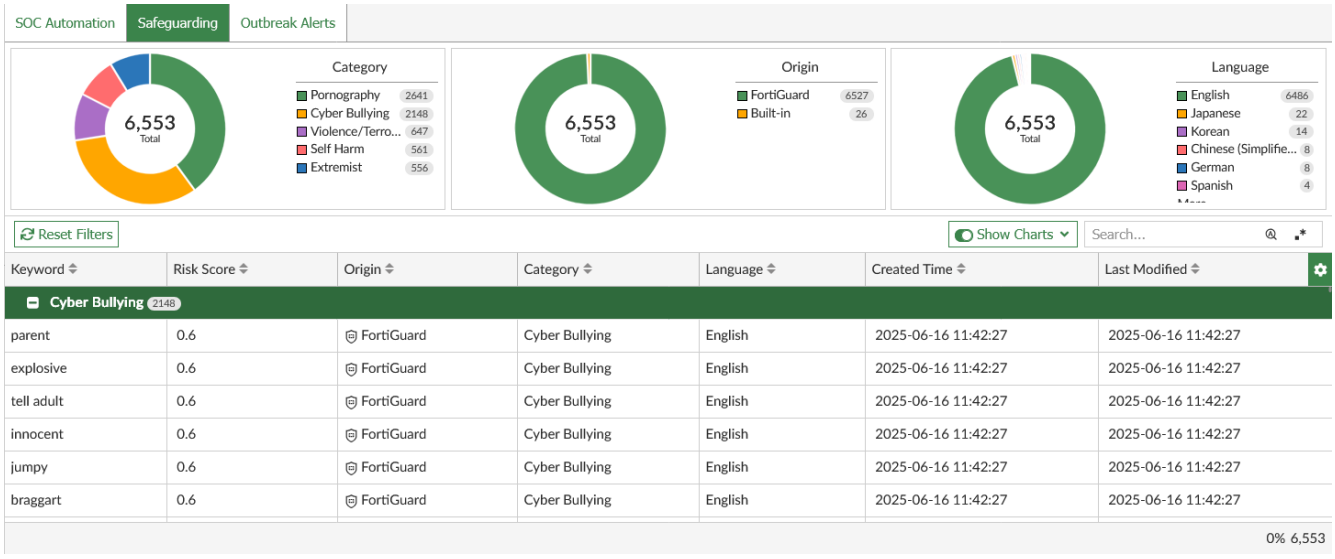
To use the Microsoft 365 Defender connector in a playbook:

1. Go to *Incidents & Events* > *Automation* > *Playbook*, and click *Create New*.
2. Select *New Playbook created from scratch*.
3. Select a trigger for the playbook.
4. Drag-and-drop any connector point from the trigger to add a new task.
   The *Tasks* pane displays available connectors.
5. Select the Microsoft 365 Defender connector.
6. Configure the automated action for the connector, and then click *OK*:
7. Enter a *Name* and *Description* for the playbook.
8. Save the playbook.

Safeguarding

The *Safeguarding* feature in FortiAnalyzer can help you to identify keywords for harmful content on your network. These keywords are used in reports and event handlers so you can respond accordingly.

To view the complete list of safeguarding keywords, go to *Incidents & Events* > *FortiGuard Services* > *Safeguarding*. While there are some built-in keywords, FortiAnalyzer must have a connection to the FortiGuard Distribution Servers (FDS) to display all the safeguarding keywords in this pane.



The keywords are automatically updated from FortiGuard. To check when the object was last updated from FortiGuard, enter the following command in the FortiAnalyzer CLI:

```
diagnose fmupdate fds-getobject objid 07000000ESDB00103
```

By default, three charts display above the table to summarize the number of keywords by:

- *Category*
- *Origin*
- *Language*

Toggle *Show Charts* to enable or disable these charts. Alternatively, you can enable or disable select charts from the *Show Charts* dropdown.

The table provides a complete list of safeguarding keywords organized by category. You can expand or collapse the categories according to your needs. You can use the *Search* field to find a keyword in the table.

The following columns are available for the table. You can use the settings icon above the table to add or remove columns according to your needs.

Column	Description
Keyword	The safeguarding keyword.
Risk Score	The risk score for the keyword.
Origin	The origin of the keyword, such as built-in or FortiGuard.
Category	The category for the keyword, such as cyber bullying or self harm.
Language	The language the keyword is in.
Created Time	The date and time the keyword was added to FortiAnalyzer.
Last Modified	The date and time the keyword was last updated in FortiAnalyzer.

You can set filters for the table using the column headers.

To set filters for the table:

1. Mouse over the column header and click the filter icon.
2. Select the type of filter:
   - *Contains*
   - *Exact Match*
3. Toggle *NOT* to enable, if needed.
   When enabled, the filter will be does *NOT* contain or is *NOT* an exact match according to your selection for the filter type.
4. Use the *Search* field to find the appropriate terms for your filter.
   To add a new term for the filter, type the string and click the plus icon.
5. From the available list, select the appropriate filter(s).
   You can also use the *Select all* or *Deselect all* buttons to help make your selection.
6. Click *Apply*.
   The table is now filtered according to the results for this column. You can add filters to other columns as well, if needed.
   A filter icon displays in the column header.

To remove a filter for the table:

To quickly remove all filters for the table, click *Reset Filters* above the table. To remove only select filters, follow the steps below.

1. Click the filter icon in the column header.
2. Remove the filters individually, or click *Remove* to remove all the filters applied using that column.
3. If you removed the filters individually, click *Apply* to save your changes.

Safeguarding event handler

A predefined event handler is available to detect safeguarding keywords in logs for web traffic, application control (social media), and email. This event handler supports consistent monitoring for harmful content, allowing timely intervention.

This predefined event handler is named *Sensitive Keyword Detection for Safeguarding* and can be found in *Incidents & Events > Event Handlers > Event Handlers*. This event handler and all of its rules are enabled by default. For all events created by this event handler, the event status is *Unhandled*, indicating that they require follow up from the admin.

By default, events are triggered when the risk score for the safeguarding keyword is greater than 0.8. This can be changed in the event handler rules according to your needs. To review the safeguarding keywords, see *Incidents & Events > Safeguarding*. For more information, see Safeguarding on page 348.

The following predefined rules are configured for the *Sensitive Keyword Detection for Safeguarding* event handler:

Rule	Description
Web traffic sensitive keyword detection	Generates an event when the safeguard risk score is more than 0.8 in webfilter logs. Event Severity: High Log Device Type: FortiGate Log Type: Web Filter Log Fields: • Source End User • Safeguard Category Trigger event when the Safeguard Risk Score is more than 0.8. All logs were generated within 1 day. Event Message: Sensitive keywords detected in web traffic from user ${groupby1} under category "${groupby2}" Tags: By_Enduser, Violation, SafeGuard, SensitiveContent, RiskQuery, Webfilter.
App traffic sensitive keyword detection	Generates an event when safeguard risk score is more than 0.8 in the app-ctrl logs. Event Severity: High Log Device Type: FortiGate Log Type: Application Control

Rule	Description
	Log Fields: • Source End User • Safeguard Category Trigger event when the Safeguard Risk Score is more than 0.8. All logs were generated within 1 day. Event Message: Sensitive keywords detected in app traffic from user ${groupby1} under category "${groupby2}" Tags: By_Enduser, Violation, SafeGuard, SensitiveContent, RiskQuery, AppCtrl.
Email sensitive keyword detection	Generates an event when safeguard risk score is more than 0.8 in the emailfilter logs. Event Severity: High Log Device Type: FortiGate Log Type: Email Filter Log Fields: • Source End User • Safeguard Category Trigger event when the Safeguard Risk Score is more than 0.8. All logs were generated within 1 day. Event Message: Sensitive keywords detected in emails from user ${groupby1} under category "${groupby2}" Tags: By_Enduser, Violation, SafeGuard, SensitiveContent, RiskQuery, EmailFilter.

To find events created by this event handler:

1. Go to *Incidents & Events* > *Event Handlers* > *Event Handlers*, and find the event handler.
2. In the *Event* column for *Sensitive Keyword Detection for Safeguarding*, click the number.

   The *Event Monitor* displays, filtered by `triggername="Sensitive Keyword Detection for Safeguarding"`. The events are organized by user. You can expand the users to view all related events from that user.

Safeguarding report

The predefined *Safeguarding Report* is available to help identify high-risk users that show rising trends in searches, posts, or messages related to inappropriate topics like self-harm or cyberbullying. The report also highlights noticeable users who are not as high risk, but still show an increase in inappropriate content.

This report uses web filter, email filter, and application control logs to populate the charts. The safeguarding keywords are used to identify risky terms, which are visible in *Incidents & Events*. Many of these keywords require a connection to the FortiGuard Distribution Servers (FDS) to remain up-to-date. For more information, see Safeguarding on page 348.

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
2. Select the checkbox for *Template - Safeguarding Report*.
3. From the *More* dropdown, click *Create Report*.
4. In the *Name* field, enter a name for the report.
   If you did not make any changes, consider naming the report `Safeguarding Report`. The GUI notifies you if a duplicate name already exists.
5. Make other changes to the report, if needed.
   You can review the charts used in the report to confirm the information will be valuable to your processes.
6. From the *Save to Folder* dropdown, select a folder for the report.
   If needed, you can save the report to multiple folders. To create a report folder, see Organizing reports into folders on page 445.
7. Click *OK*.
   The report is now available to be run, as needed, from *Reports* > *Report Definitions* > *All Reports*.

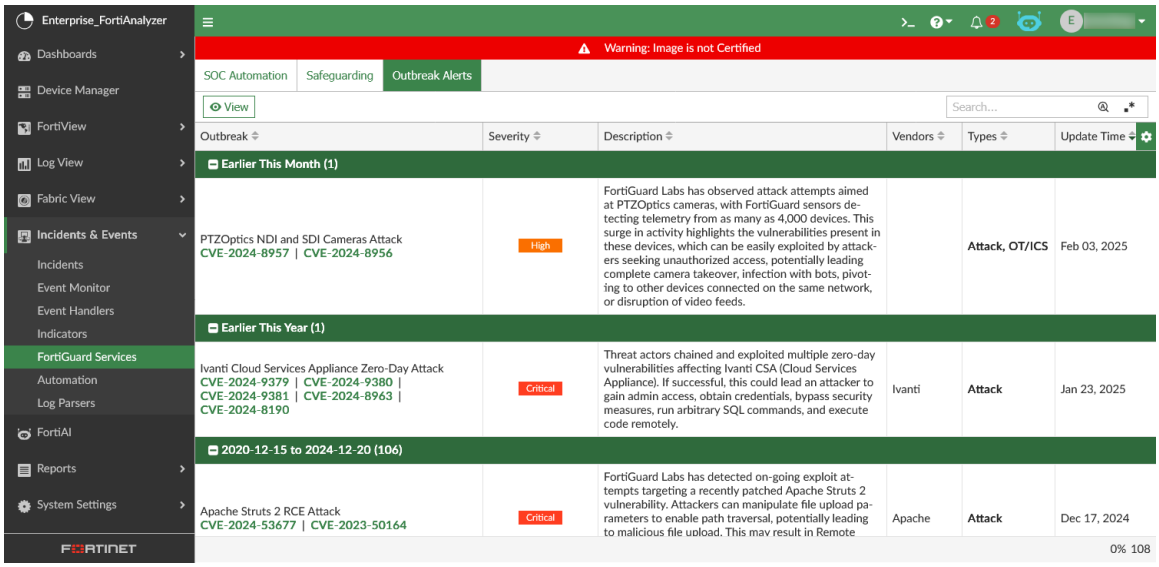
To run the report:

1. Go to *Reports* > *Report Definitions* > *All Reports*, and double-click the row for the *Safeguarding Report*.
   The *Edit: Safeguarding Report* pane displays.
2. In the *Generated Reports* tab, click *Run Report*.
3. When the report is available, click the *Format* to open the report in.

Outbreak Alerts

The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows FortiAnalyzer administrators to view Outbreak Alerts and automatically download related event handlers and reports from FortiGuard.

When FortiAnalyzer has a valid license for the Outbreak Detection Service, Outbreak Alert from Fortinet are displayed in the *Incidents & Events* > *FortiGuard Services* > *Outbreak Alerts* pane. Outbreak Alerts can be viewed from any ADOM.



An Outbreak Alert is a comprehensive report that provides in-depth insights into cybersecurity threats serving as a vital tool for organizations to stay informed about critical and or emerging cybersecurity risks that may compromise sensitive data, disrupt business operations, and pose significant risks to the organization's overall security.

Each report provides the background of the attack, the timeline of events, affected technologies, and related threat intelligence such as Indicators of Compromise (IoCs), Tactics, Techniques, and Procedures (TTPs), and Attack sequence used by the adversaries.

Without a valid license for the Outbreak Detection Service, *Outbreak Alerts* displays a default alert page, and Outbreak Alert event handlers and reports are not available from FortiGuard. To obtain a valid license for FortiAnalyzer Outbreak Detection Service, contact Fortinet FortiCare.

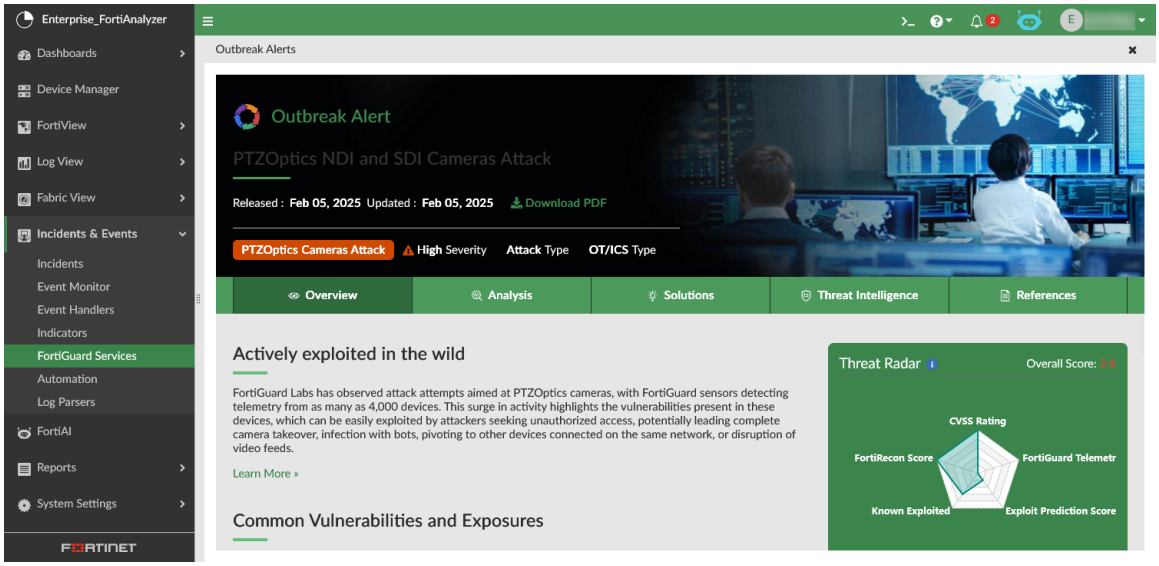
The following columns are available for the table in *Outbreak Alerts*:

Column	Description
Outbreak	The outbreak name and the related CVE numbers.
Severity	The severity of the outbreak.
Description	A description of the outbreak.
Vendor	The vendor affected by the outbreak.
Types	The type of outbreak, such as vulnerability, ransomware, or attack.
Publish Time	The publish date from FortiGuard for the Outbreak Alert.
Update Time	The latest update from FortiGuard for the Outbreak Alert.

You can sort and filter the table by each column. To filter the table by a column, mouse-over the column header and click the filter icon. You can filter by *Contains*, *Exact Match*, and *NOT*. Enter the filter and click *Apply*. You can apply multiple filters at once. To remove a filter, mouse-over the column header and click the filter icon; delete the filter or click *Remove* to remove all filters for that column and click *Apply*.

You can use the *Search* field to find Outbreak Alerts in the table.

You can review the complete details of the Outbreak Alert by double-clicking a record in the table. Alternatively, you can select the Outbreak Alert in the table and click *View*. The Outbreak Alert details from FortiGuard display within the FortiAnalyzer GUI.



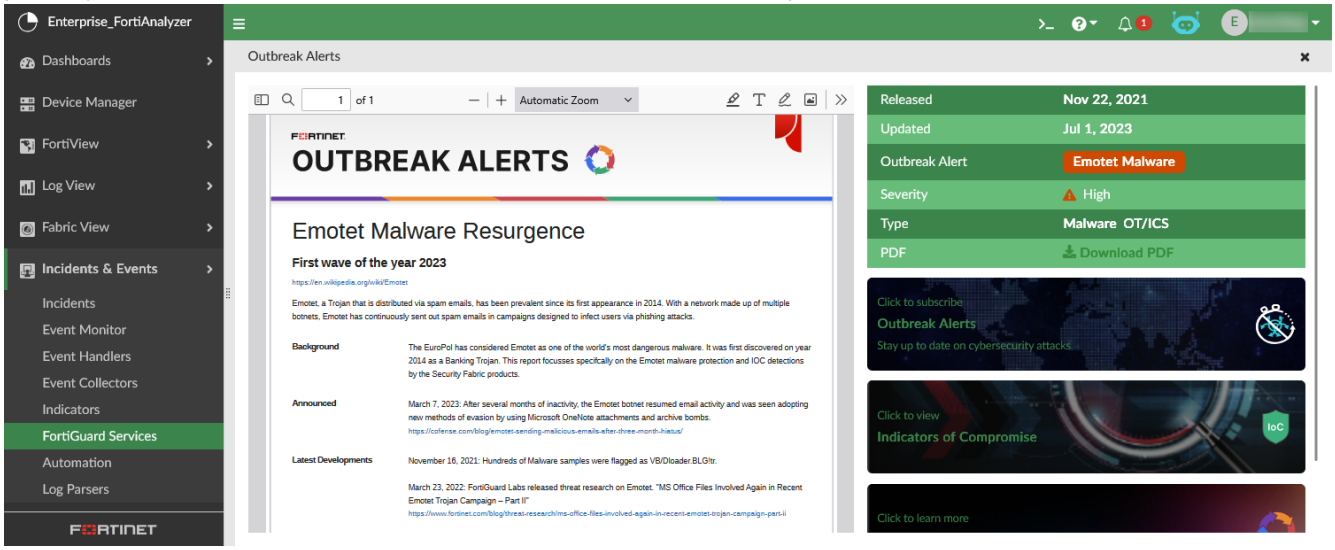
The header for the Outbreak Alert includes the alert name, release date, most recent update, severity, and type. You can click *Download PDF* to save the Outbreak Alert information as a PDF.

Click the tabs to review the related information. Outbreak Alerts typically include the following information:

Tab	Description
Overview	Includes a brief description of the outbreak, its background, and the related CVE numbers. The overview also includes a Threat Radar, which displays threat ratings from different sources.
Analysis	Displays the latest developments for the outbreak organized in a timeline. If applicable, this section may also include an attack sequence, which is a simple diagram of the cyber-attack and its components when deployed to compromise a target system or network.
Solutions	Includes relevant links for FortiGuard services to help mitigate the outbreak. This information is typically organized by services that will help to: • Protect • Detect • Respond • Recover • Identify
Threat Intelligence	Includes information gathered from analyzing ongoing cybersecurity events including threat actors, their tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), malware, and related vulnerabilities. The information is organized into widgets that display tables and charts. If there is MITRE ATT&CK® information for the outbreak, you can click the widget to review the related matrix.

Tab	Description
References	Links to sources for supporting information in relation to the Outbreak Alert.

In some cases, the Outbreak Alert may not have charts available. In this case, it will display the information in a print layout with the overview information in the sidebar. For example, see below:



Event handlers and reports are created in real-time by Fortinet to detect and respond to emerging outbreaks. With a valid license for the Outbreak Detection Service, these event handlers and reports are automatically downloaded so that they are available in your environment. To find these reports in your FortiAnalyzer GUI, see Viewing imported event handlers and reports on page 355.

Viewing imported event handlers and reports

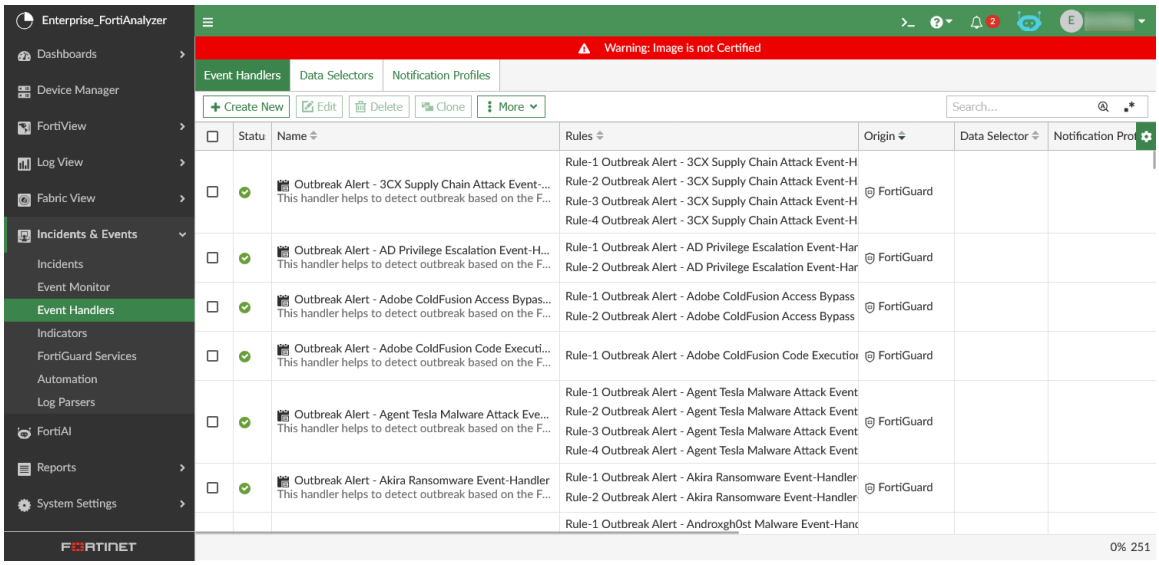
With a valid license, the FortiAnalyzer Outbreak Detection Service automatically downloads event handlers and reports created by Fortinet in response to known outbreaks. Handlers and reports are downloaded from FortiGuard as part of the FOAS package. This section includes information on how to view downloaded Outbreak Alert event handlers and reports.

To view Outbreak Alert event handlers:

1. Go to a Fabric ADOM. Outbreak Alert event handlers are only available in Fabric ADOMs.
2. To view the event handlers, go to *Incidents & Events* > *Event Handlers* > *Event Handlers*.

   Event handlers created by the FortiAnalyzer Outbreak Detection Service are displayed with the `Outbreak Alert` prefix and their *Origin* is *FortiGuard*. See Event handlers on page 231.

   In FortiAnalyzer 7.6.0 and later, these event handlers will also have the *Automatically Create Incident* option enabled. The incidents generated by these event handlers can be found in *Incidents & Events* > *Incidents* > *Incidents*.



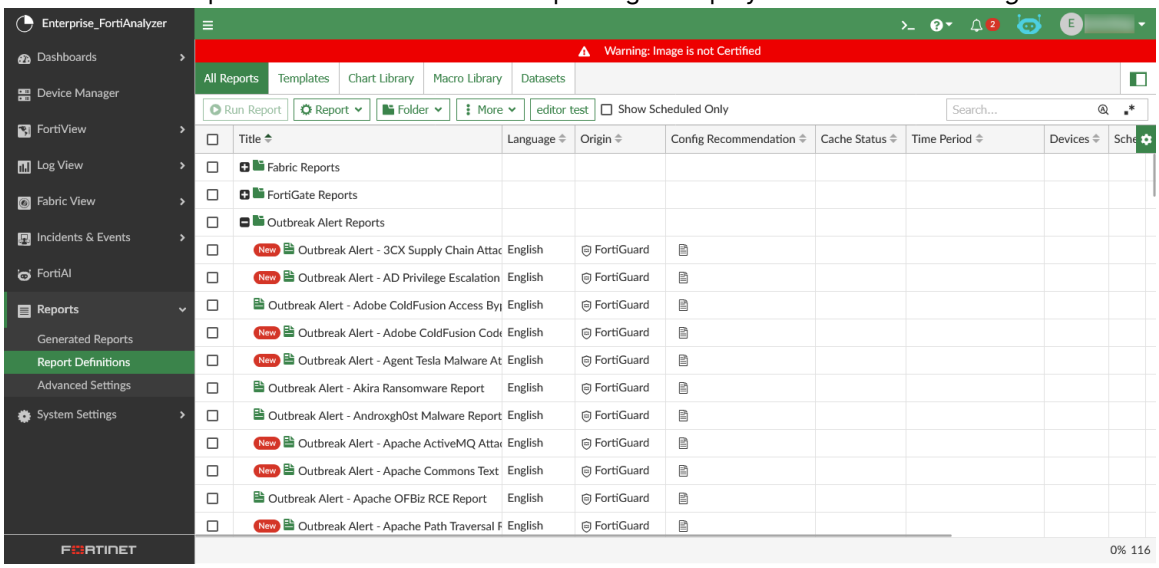
To view Outbreak Alert reports:

1. To view the reports, go to *Reports* > *Report Definitions* > *All Reports*.

   The *Outbreak Alert Reports* folder includes available reports from the FortiAnalyzer Outbreak Detection Service. Reports can be run in HTML, PDF, XML, CSV, and JSON output formats. See Generating reports on page 430.

   In FortiAnalyzer 7.4.2 and later, new reports included in the FOAS package are displayed in the global *Outbreak Alert Reports* folder. Outbreak Alert reports released prior to this release remain at the ADOM level. The global folder and global reports are identified with the system theme's color applied to the icon.

   Outbreak Alert reports received as FortiGuard packages display *FortiGuard* in the *Origin* column.



Security rating update

The Security Rating Update license allows FortiAnalyzer to generate reports using security rating information from FortiGate devices. This includes compliance information for Fortinet Security Best Practices (FSBP) and Center for Internet Security (CIS) standards. When FortiAnalyzer has a valid license for Security Rating Update, predefined reports and report templates will be available to review security posture according to these standards. The reports help security teams to design, implement, and maintain their security posture; they provide actionable configuration recommendations as well as key performance and risk indicators.

For example, the Security Rating Update provides the following FortiAnalyzer reports:

- *CIS Controls Security Rating Report*
- *FSBP Security Rating Report*
- *HIPAA Compliance Security Rating Report*
- *ISO 27001:2022 Compliance Security Rating Report*
- *NERC CIP Compliance Security Rating Report*
- *PCI DSS Security Rating Update Report*
- *SOC 2 Compliance Report*

Additional compliance reports can also be received from FortiGuard through the Security Automation Service license. See SOC Automation on page 338.

The *FortiGate Security Rating Log Parser* is used to parse security rating data from FortiGate devices and store it in the FortiAnalyzer SIEM database (siemdb). The FortiGate devices must be licensed for Security Rating & CIS Compliance as well.

FortiTIP service integration

The FortiTIP service is a licensed feature on FortiAnalyzer. This feature is only supported on FortiAnalyzer hardware models.

Powered by FortiGuard, FortiTIP provides real-time insights into threat adversaries, indicators of compromise (IOCs), malware hashes, and phishing domains and URLs. FortiTIP streamlines threat investigation and response by leveraging vast FortiGuard intelligence, escalated outbreak alerts, and automated workflows. This comprehensive cloud-based platform accelerates detection, response, and mitigation of advanced threats, while enhancing visibility and strengthening the security of digital ecosystems. You can provision the FortiTIP instance on FortiCloud.

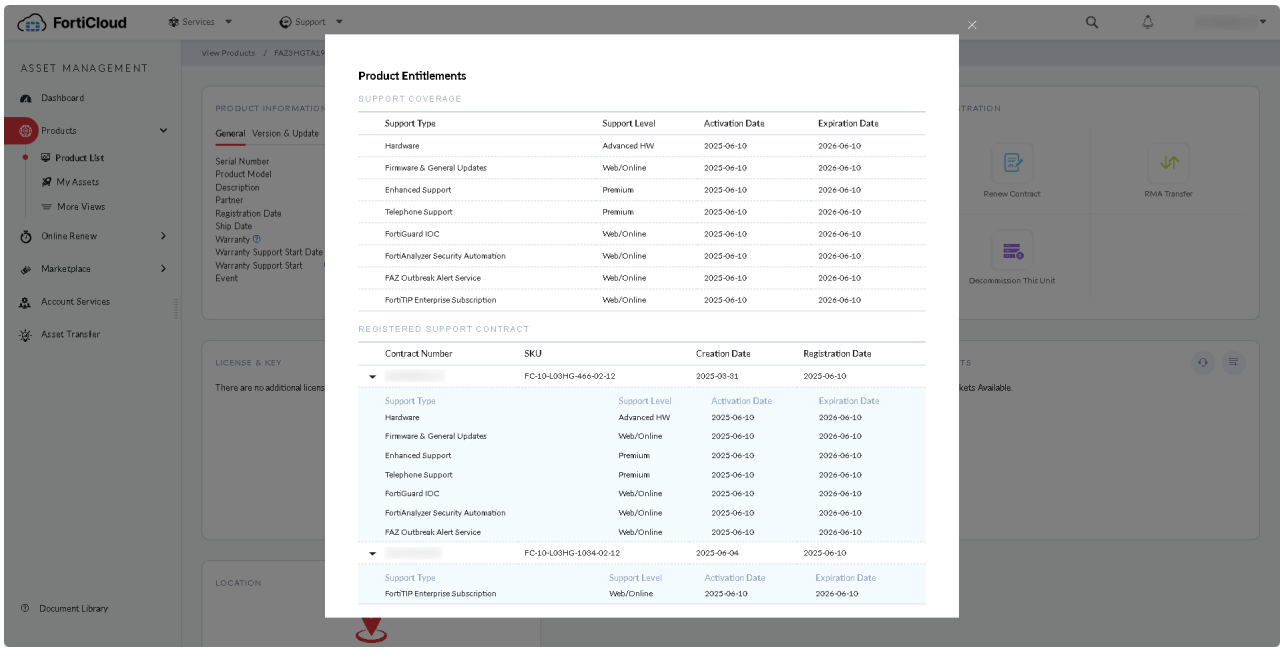
When the FortiTIP service is licensed on FortiAnalyzer, hyperlinks for threat intel and outbreak information are available in the FortiAnalyzer GUI. These hyperlinks redirect to the provisioned FortiTIP instance to display the related threat information.

FortiAnalyzer pane	FortiTIP hyperlink
Indicators of Compromise	Drill-down to view the threat details for a particular endpoint (*Blocklist* or *Suspicious* table). In the *Detect Pattern* column, click a hyperlink to view more information about the threat in the FortiTIP instance. See Working with IOC information on page 113.

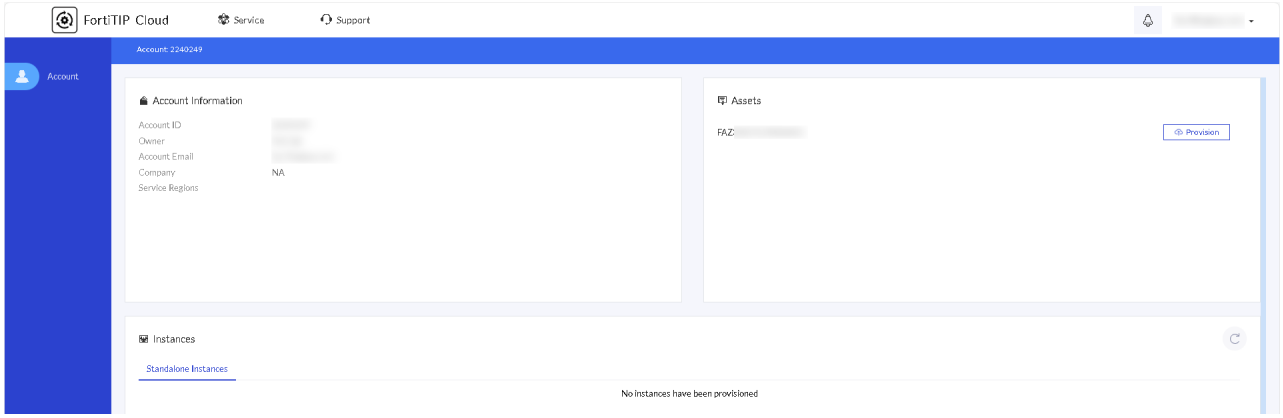
FortiAnalyzer pane	FortiTIP hyperlink
Event Monitor	In the *Outbreak Name* column, click a hyperlink to view the outbreak information in the FortiTIP instance. See All Events on page 221.
Incident Analysis	Similar to the *Event Monitor*, the *Outbreak Name* column is included in the *Events* widget in the *Incident Analysis* pane. Click a hyperlink to view the outbreak information in the FortiTIP instance. See Analyzing an incident on page 208.

To provision the FortiTIP instance:

1. In FortiCloud, register the FortiTIP contract.

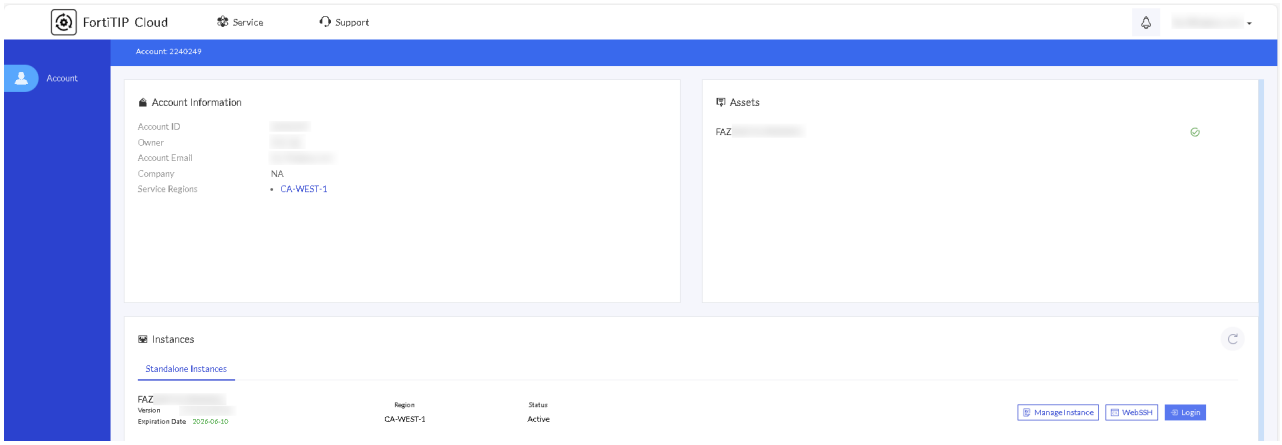


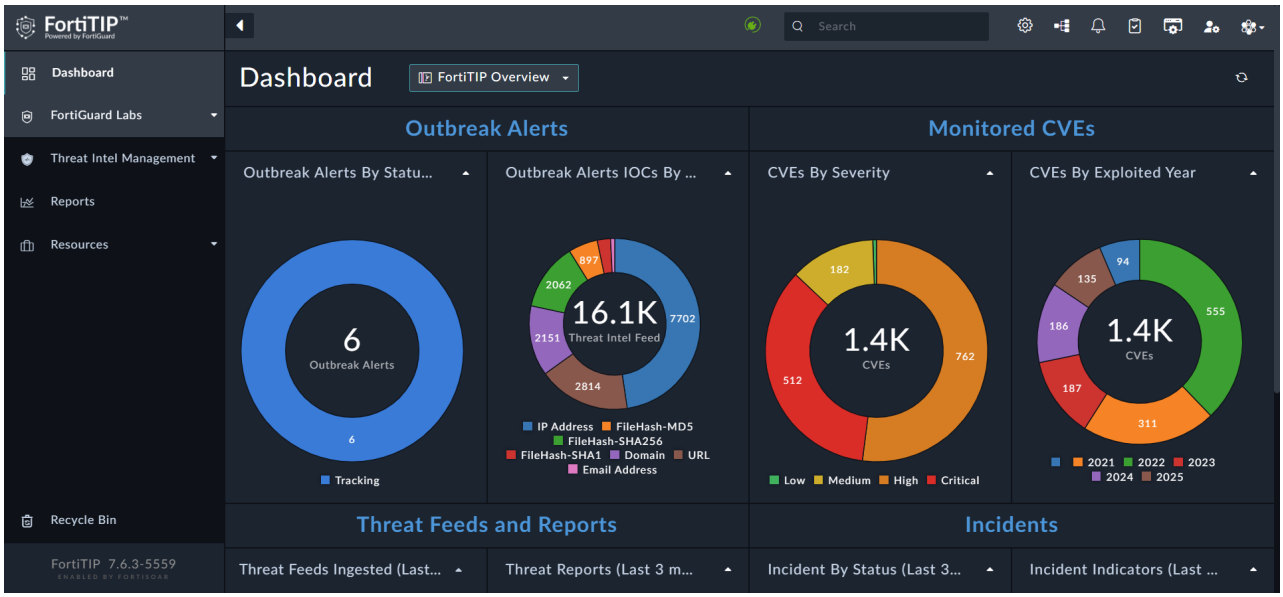
2. In the FortiTIP cloud portal, provision the instance.



During provisioning, you must select the region and agree to the terms and policies.

3. Once provisioning is complete, you can log into the FortiTIP instance from the cloud portal.





In FortiAnalyzer, the FortiTIP license status displays in *Dashboards > Status > License Information widget*.

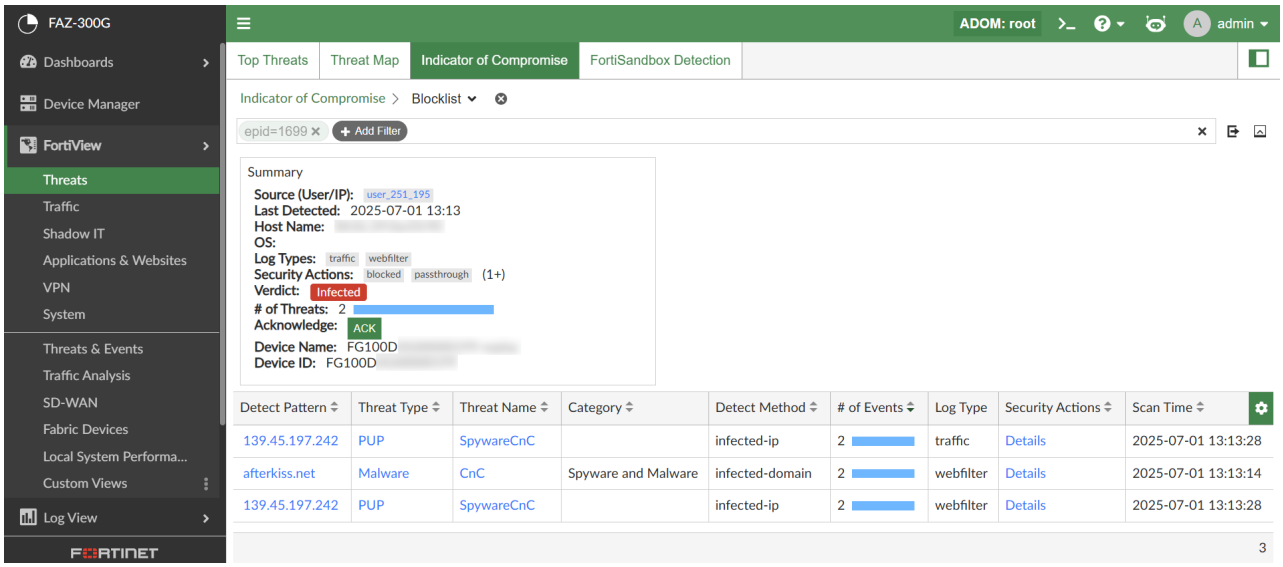
You can also find the `TIPE FortiTIP Service` license status using the following command in the FortiAnalyzer CLI:

```
diagnose license list
```

To view threat intel about a detect pattern:

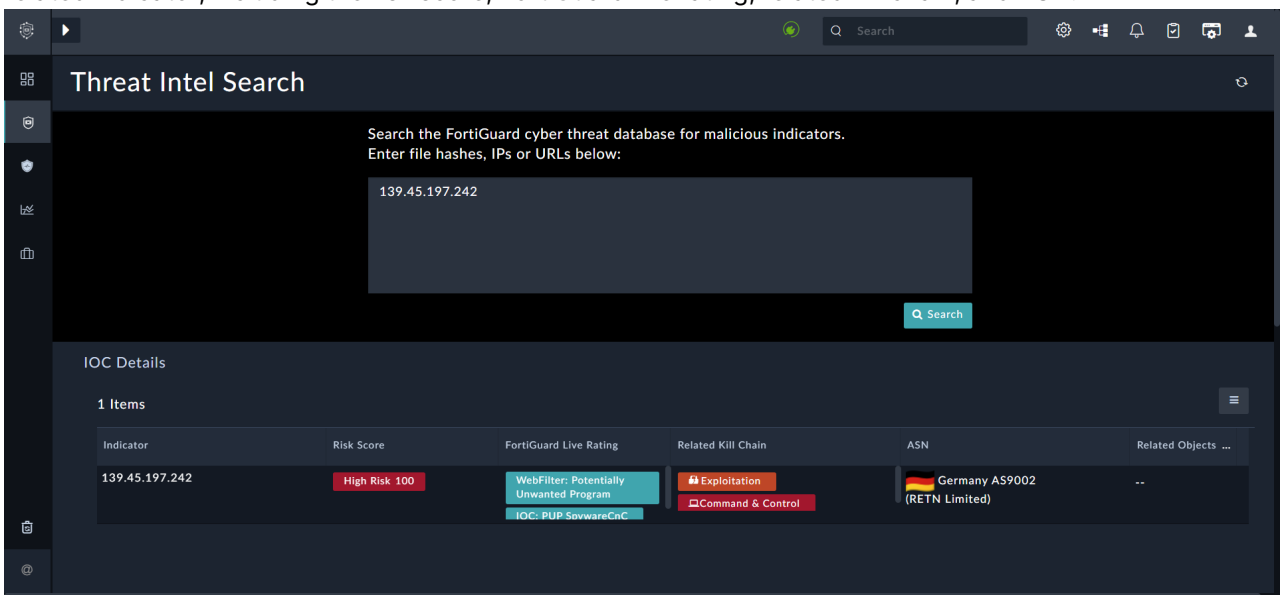
1. In FortiAnalyzer, go to *FortiView > Threats > Indicators of Compromise*.
2. To drill down and view threat details for a particular endpoint, right-click a row and select *Blocklist* or *Suspicious*. Alternatively, double-click a row to open the *Blocklist*.

   The *Blocklist* and *Suspicious* table views list all unique threats detected for the end user. A summary of the end user is provided above the table. You can toggle between *Blocklist* and *Suspicious* from this view.

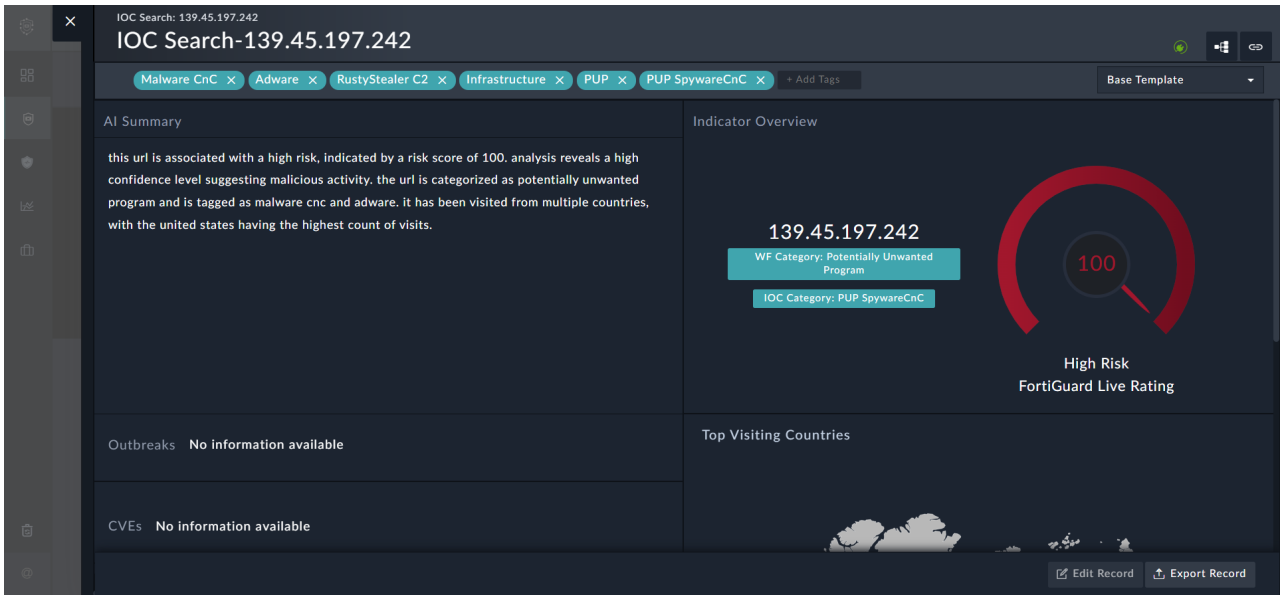


3. Click a hyperlink for a *Detect Pattern* in the table view. This column is available in both the *Blocklist* and *Suspicious* table views.

   FortiTIP displays the *Threat Intel Search*, filtered by the indicator. This view provides an overview of the related indicator, including the risk score, FortiGuard live rating, related kill chain, and ASN.

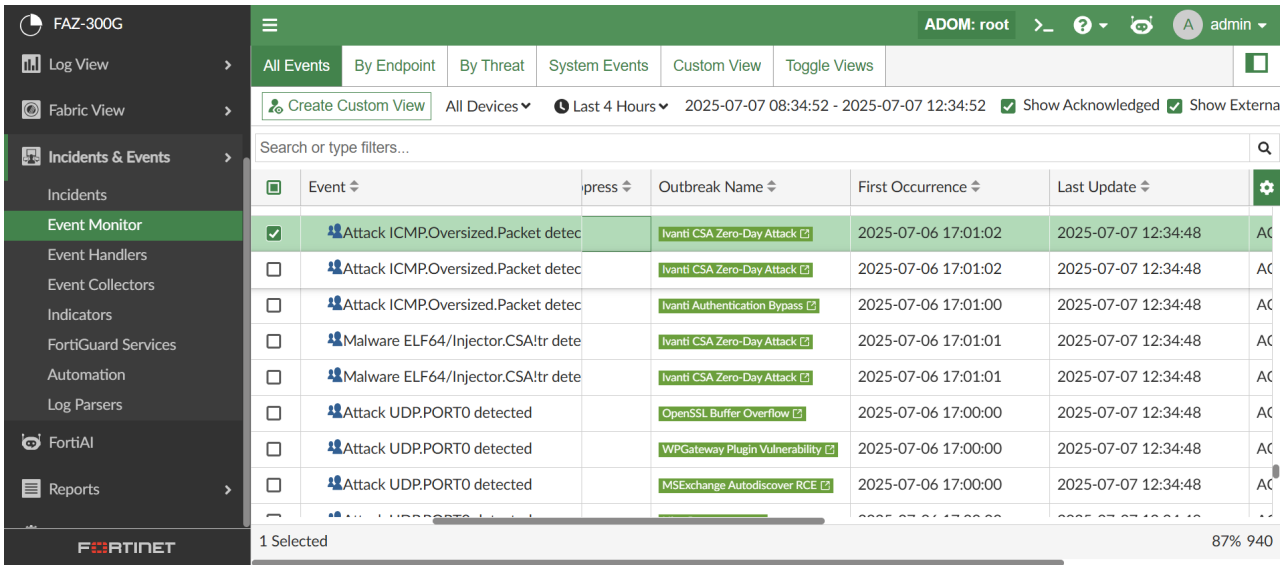


4. You can drilldown further in FortiTIP for more information about this indicator, including a descriptive summary of the indicator.



To view outbreak details:

1. In FortiAnalyzer, go to *Incidents & Events* > *Event Monitor* > *All Events*.

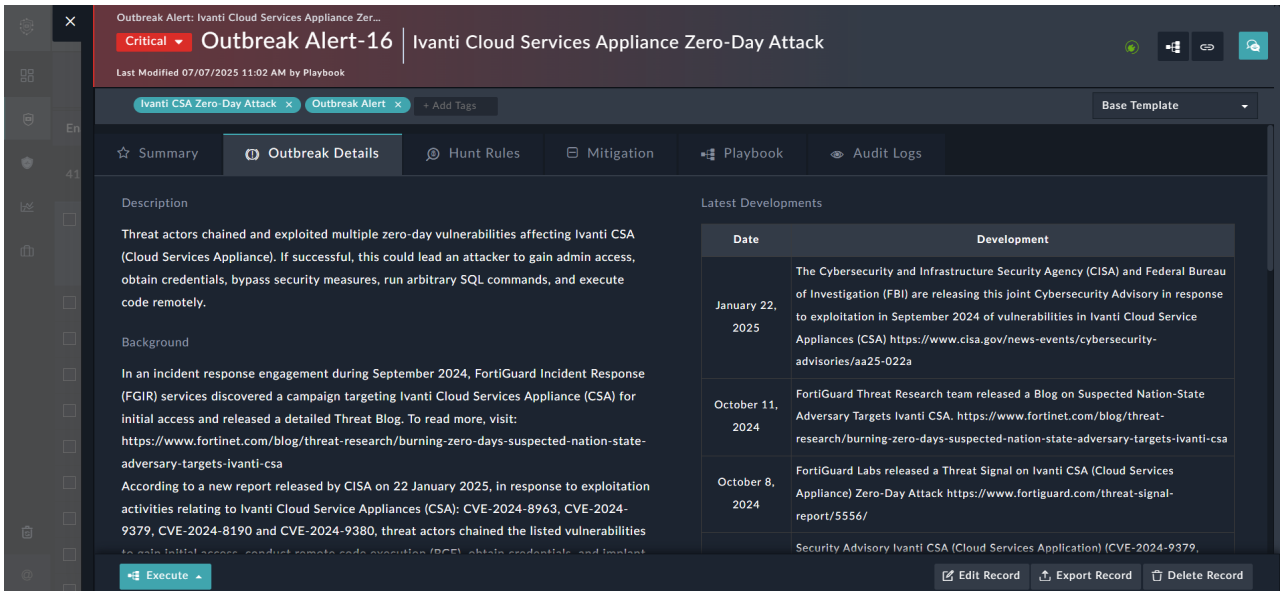


   You can also find the *Outbreak Name* column and hyperlinks the other event monitors and in *Incidents & Events* > *Incidents* > *Incident Analysis* > *Events widget*.

2. Click a hyperlink in the *Outbreak Name* column.

   CTRL+click the hyperlinks to open the FortiTIP instance in a new tab.

   FortiTIP displays the outbreak information, including a summary, the outbreak details, hunt rules, mitigation, playbooks, and audit logs.



If the outbreak alert is not yet available in FortiTIP, it will display Resource Not Found.

The hyperlinks are not accessible without a provisioned FortiTIP instance or FortiTIP license registered to FortiAnalyzer. The hyperlinks will instead return errors that the FortiTIP service is not reachable. For example, you may encounter the following errors:

- If the license is registered, but the FortiTIP instance is not provisioned: "FortiTIP service not reachable at https://auth.fortitip.forticloud.com/jsonrpc. Please check your network connection or availability of service".
- If the asset is not synced from FortiCloud: "Your entitlement is not qualified to use this service".

Automation

You can configure playbooks to automate tasks from *Incidents & Events > Automation*.

A Security Automation subscription is required to run at full capacity. For additional information about licensing, please see support.fortinet.com.

Summary

Incidents & Events > Automation > Summary provides a dashboard to review playbook performance at a glance.

This dashboard includes the following widgets:

Playbook Summary	The total number of playbooks executed and plabook actions (tasks) executed.

Playbooks Executed	The total number of playbooks executed by playbook name in a donut chart.
Total Executed Playbooks and Actions Trend	The total number of playbooks executed and actions (tasks) executed in a line chart timeline.

Active connectors

Incidents & Events > *Automation* > *Active Connectors* displays connectors and the automated actions that they can perform in playbooks.

The following connectors are available:

- FortiOS
- Local (FortiAnalyzer)
- FortiGuard
- FortiManager
- FortiAuthenticator
- FortiCASB
- FortiClient EMS / FortiClient EMS Cloud
- FortiEDR
- FortiMail
- FortiSandbox
- FortiWeb
- FortiAnalyzer Cloud
- ServiceNow
- Slack
- MS Teams
- Generic webhook
- VirusTotal

Connectors can be used for automation in playbooks, and they can also be used in incident settings and notification profiles.

Some connectors are available by default, such as the Local, FortiGuard, and VirusTotal connectors. These connectors are used in default playbooks. Other connectors are not visible in the dashboard unless they are created, such as the ServiceNow, Slack, and MS Teams connectors.

Additional connectors are also available from FortiGuard when FortiAnalyzer has a valid license for the Security Automation Service. For more information about this service, see SOC Automation on page 338.

The status of each connector is indicated by a colored icon:

- **Green**: The API connection is successful.
- **Orange**: The API connection is unknown.
- **Red**: The API connection is down.

FortiOS devices are organized by standalone, Cooperative Security Fabric (CSF), and high availability (HA). Click the device information on the FortiOS Connector card to view a tree breakdown of the devices.

Connector actions

This topic provides details for the following connectors:

- Local Connector
- FortiOS Connector
- FortiGuard Connector
- FortiManager Connector
- EMS Connector
- FortiEDR Connector
- FortiMail Connector
- FortiCASB Connector
- FortiAuthenticator Connector
- FortiWeb Connector
- FortiSandbox Connector
- FortiAnalyzer Cloud Connector
- VirusTotal Connector
- vSphere Connector

For more information about the uses of ITSM connectors, see Configuring ITSM connectors on page 378.

Local Connector

The local connector is the default connector for FortiAnalyzer and is available automatically. The local connector displays a set of predefined FortiAnalyzer actions to be used within playbooks.

Local connectors include the following actions:

Name	Description
Update Asset and Identity	Update FortiAnalyzer's *Asset and Identity*.
Get Events	Get events.
Get Endpoint Vulnerabilities	Get endpoint vulnerabilities.
Create Incident	Create a new incident.
Update Incident	Update an existing incident.
Attach Data to Incident	Attach the specified data to an existing incident.
Run Report	Run the specified FortiAnalyzer report.
Get EPEU from incidents	Get the EPEU from an incident.
Enrich Start	Start indicator enrichment workflow.
Enrich Aggregate	Aggregate indicator enrichment results.

Name	Description
Enrich Save	Save indicator enrichment.
Get Disk Usage	Get FortiAnalyzer's disk usage.
Get Virtual Memory	Get FortiAnalyzer's virtual memory.
Get CPU Usage	Get FortiAnalyzer's CPU usage.

FortiOS Connector

The FortiOS connector is added after the first FortiGate has been authorized on an ADOM. Additional devices authorized to the ADOM are displayed as separate entries within the same connector. FortiOS connectors are available in FortiGate and Fabric ADOMs.

Enabling FortiOS actions

The actions available with FortiOS connectors are determined by automation rules configured on each FortiGate. Automation rules using the *Incoming Webhook* trigger must be created in FortiOS before they are shown as actions in FortiAnalyzer. FortiOS automation rules are configured on FortiOS in *Security Fabric > Automation*. For information on creating FortiOS automation rules, see the FortiOS administration guide.

Rules for FortiOS actions:

- Automation rules must use the *Incoming Webhook* trigger.
- Automation rules are configured on FortiGate devices individually.
- When multiple FortiOS connectors are configured, FortiAnalyzer decides which device to call based on the *devid* (serial number) identified in the task. FortiGate serial numbers can be manually entered or supplied by a preceding task.
- Automation rules must have unique names to be displayed in the task's *Action* dropdown menu. Rules sharing the same name will appear only once, as they are considered to be the same automation rule configured on multiple FortiGate devices.
- FortiOS automation rules are only displayed in *Incidents & Events > Automation > Active Connectors* when they are enabled in FortiOS.

FortiGuard Connector

The FortiGuard connector is automatically configured when a valid license has been applied to FortiAnalyzer.

FortiGuard connectors include the following actions:

Name	Description
Lookup Indicator	Lookup indicators in FortiGuard to get threat intelligence.
FGD Enrich	Get the reputation report for indicator enrichment.



The FortiGuard connector cannot be used in an air-gap environment.

FortiManager Connector

Using this connector establishes a fabric connection to FortiManager, providing accessibility to certain FortiAnalyzer features on FortiManager.

For more information, see FortiAnalyzer Features and Adding FortiAnalyzer devices using a fabric connection in the FortiManager Administration Guide.

EMS Connector

FortiClient EMS connectors are configured as Security Fabric connectors. See Configuring security fabric connectors on page 372. Individual FortiClient EMS connector actions can be toggled on and off while editing the connector.

FortiClient EMS connectors include the following actions:

Name	Description
Get Endpoints	Retrieve list of endpoints and all of the related information to enrich FortiAnalyzer asset and identity views.
Quarantine	Quarantines an endpoint.
Unquarantine	Unquarantines an endpoint.
Vulnerability Scan	Run a vulnerability scan on endpoints.
AV Quick Scan	Run a quick antivirus scan on endpoints.
AV Full Scan	Run a full antivirus scan on endpoints.
Get Software Inventory	Retrieve list of software and apps installed on an endpoint to enrich FortiAnalyzer asset view.
Get Process List	Retrieve list of running process on endpoints OS.
Get Vulnerabilities	Retrieve list of endpoint vulnerabilities on endpoints OS.
Tag Endpoints	Tag endpoints.
Untag Endpoints	Untag endpoints.

FortiEDR Connector

FortiEDR connectors include the following actions:

Name	Description
Create Exception	Creates a new exception in Fortinet FortiEDR based on the event ID and other input parameters you have specified.
Create IPSet	Creates an IPSet in Fortinet FortiEDR using the set of IP addresses and other parameters you have specified.
Delete IPSet	Deletes specific IPSets from Fortinet FortiEDR based on the IPSet names and other input parameters you have specified.

Name	Description
Get Agent Groups	Retrieves a list of all agent group lists from Fortinet FortiEDR.
Get Collector List	Retrieves the list of the collectors from Fortinet FortiEDR based on the device names or IDs, and other input parameters you have specified.
Get Event By ID	Retrieves a specific event from Fortinet FortiEDR based on the event ID you have specified.
Get Event Count	Retrieves the event count from Fortinet FortiEDR based on the filter parameters you have specified.
Get Event Exceptions	Retrieves the list of event exceptions from Fortinet FortiEDR based on the event ID and other input parameters you have specified.
Get Event List Extended	Retrieves archived/unarchived events together from Fortinet FortiEDR based on the filter parameters you have specified. Note: If none of the input parameters that you specify match the events in Fortinet FortiEDR, then an empty result set is returned.
Get Events	Retrieves all the events from Fortinet FortiEDR that match the condition(s) you have specified. Note: If none of the input parameters that you specify match the events in Fortinet FortiEDR, then an empty result set is returned. This action can be configured for data ingestion.
Get Exception List	Retrieves the list of all exceptions or specific exceptions from Fortinet FortiEDR based on the input parameters you have specified.
Get IPSet List	Retrieves a list of IPSets from Fortinet FortiEDR based on the IP address and other input parameters you have specified.
Get Raw Data Items	Retrieves the raw data items from Fortinet FortiEDR based on the event ID and other input parameters you have specified.
Get Raw JSON Event Data	Retrieve the raw data of specific events from Fortinet FortiEDR based on the event ID and other input parameters you have specified.
Get System Summary	Retrieves a summary of the environment from Fortinet FortiEDR.
Isolate Collector	Isolates a collector from the Fortinet FortiEDR network based on the list of device IDs or names, and other input parameters you have specified.
Move Collectors	Move collectors between organizations based on the collectors, target collectors group, and other input parameters that you have specified.
Remediate Device	Takes remedial actions on Fortinet FortiEDR such as killing a process, deleting a file and/or cleaning persistent data on which malware was detected based on the device type, device name/ID, and other input parameters you have specified.
Unisolate Connector	Unisolates a collector from the Fortinet FortiEDR network based on the device ID and other input parameters you have specified.

Name	Description
Update Events	Updates events in Fortinet FortiEDR that match the condition(s) you have specified. Note: If none of the input parameters that you specify match the events in Fortinet FortiEDR, then an empty result set is returned.
Update Exception	Updates a specific exception in Fortinet FortiEDR based on the event ID, exception ID, and other input parameters you have specified.
Update IPSet	Updates IP addresses in the specific IPSet in Fortinet FortiEDR using the set of IP addresses, the IPSet name, and other parameters you have specified.

FortiMail Connector

FortiMail connectors are configured as Security Fabric connectors. See Configuring security fabric connectors on page 372.

FortiMail connectors include the following actions:

Name	Description
Get Email Statistics	Query a given email address.
Get Sender Reputation	Query a given sender's reputation information.
Add Sender to Blocklist	Update system and domain level blocklist.
Get Session Profile	Get the session profile from FortiMail.
Delete Session Profile	Delete the session profile from FortiMail.
Get Sender Block List	Get the list of blocked senders' email addresses from a session profile.
Get Sender Safe List	Get the list of safelisted senders' email addresses from a session profile.
Get Recipient Block List	Get the list of blocked recipients' email adddresses from a session profile.
Get Recipient Safe List	Get the list of safelisted recipients' email adddresses from a session profile.
Block Sender Email with Session Profile	Block sender's email address with a session profile.
Unblock Sender Email with Session Profile	Unblock sender's email address with a session profile.
Block Recipient Email with Session Profile	Block recipient's email address within a session profile.
Unblock Recipient Email with Session Profile	Unblock recipient's email address within a session profile.

FortiCASB Connector

FortiCASB connectors are configured as Security Fabric connectors. See Configuring security fabric connectors on page 372.

Creating a FortiCASB connector will automatically create the *Get Cloud Service Data (FortiCasb Connector)* playbook, which must be enabled to use the predefined Default-Shadow-IT-Events event handler. For more information, see Predefined basic event handlers on page 232.

FortiCASB connectors include the following actions:

Name	Description
Get Cloud Data from FCASB	Retrieve cloud application, user, and file information.

FortiAuthenticator Connector

The FortiAuthenticator connector includes the following actions:

Name	Description
Get Schema	Retrieves a report for all the endpoint actions within FortiAuthenticator.
Get User List	Retrieves a list of users from FortiAuthenticator.
Get User	Retrieves details of a specific user from FortiAuthenticator based on the user ID, username, or email you have specified.
Update User Status	Updates the user status of a specific user in FortiAuthenticator based on the user ID and status you have specified.
Get User Lockout Policy	Retrieves User Lockout Policy details from FortiAuthenticator.

FortiWeb Connector

The FortiWeb connector includes the following actions:

Name	Description
Get Anomaly Policy	Retrieves the domain information of a specific Anomaly Detection policy from FortiWeb based on the policy name you have specified.
Get Blocked IPs	Retrieves all the blocked IPs from the FortiWeb server.
Unblock IPs	Release all IPs from the blocked IP list under a specific policy in FortiWeb or release one IP from the blocked IP list under a specific policy in FortiWeb based on the policy name and other input parameters you have specified.
Get Blocked Users	Retrieves all blocked users or specific blocked users from FortiWeb based on the input parameters you have specified.
Unblock Users	Releases users from the blocked user list in a server policy in FortiWeb based on the input parameters you have specified.
Get Active Users	Retrieves a list of active users by user tracking or site publish type from FortiWeb based on the input parameters you have specified.
Delete Active Users	Deletes active users from a specific policy from FortiWeb based on the policy ID and other input parameters you have specified.

Name	Description
Get Client Info	Retrieves client information in Client Management in FortiWeb based on the input parameters you have specified.
Delete Client Information	Deletes information for a specific client from Client Management in FortiWeb based on the client ID you have specified.
Restore Client Threat Score	Restores the threat score of a specific client to 0 in FortiWeb based on the client ID you have specified.
Get All Virtual Servers	Retrieves all virtual servers, virtual IP, and interfaces in each virtual server sub-table in the JSON format from FortiWeb.
Get All Physical Servers	Retrieves the IP addresses in the server pool of all physical servers in the JSON format from FortiWeb.
Get Server Policy Status	Retrieves the details including the status of a server policy from FortiWeb.
Get Server Policy Traffic	Retrieves traffic information for traffic on all the system server policies from FortiWeb, or traffic information for a specific system server policy based on the policy name you have specified from FortiWeb.

FortiSandbox Connector

The FortiSandbox connector includes the following actions:

Name	Description
Get System Status	Retrieves the status of the system from FortiSandbox.
Get Scan Status	Retrieves the scan stats for the last 7 days from FortiSandbox.
Get Submission Job List	Retrieves all job IDs associated with the submission ID you have specified from FortiSandbox.
Get Job Verdict	Retrieves job verdict detail for job ID you have specified from FortiSandbox.
Get File Rating	Retrieves file rating for the file type and filehash you have specified from FortiSandbox.
Get URL Rating	Get rating details for the URL you have specified from FortiSandbox.
Get Job Behavior	Retrieves job behavior details associated with the file type and filehash you have specified from FortiSandbox.
Toggle FPN State	Marks specified sample based on the Job ID you have specified as false negative or false positive in FortiSandbox.
Get AV Rescan Result	Retrieves AV-Rescan results for the time duration you have specified from FortiSandbox.
Get File Verdict	Retrieves the file verdict details for the file type and filehash you have specified from FortiSandbox.

Name	Description
Get All Installed VM	Retrieves the names and the clone numbers of all installed VMs on FortiSandbox.
List Filehash or URL From Malware Package or URL Package	Retrieves a list of file hashes or URLs based on the type you have specified from the Malware Package or URL Package in FortiSandbox.

FortiAnalyzer Cloud Connector

The *FortiAnalyzer Cloud Connector* can be configured to securely forward logs to FortiAnalyzer Cloud, allowing you to use FortiAnalyzer Cloud for centralized logging for third-party applications.

You can only configure one *FortiAnalyzer Cloud Connector* per on-premise FortiAnalyzer. This connector can only be enabled in the root ADOM of the on-premise FortiAnalyzer.

The *FortiAnalyzer Cloud Connector* requires an access token from FortiAnalyzer Cloud. To create the access token, see the FortiAnalyzer Cloud Deployment Guide on the Fortinet Document Library.

The *FortiAnalyzer Cloud Connector* can query FortiAnalyzer Cloud with the access token. This token cannot be created or renewed when the FortiAnalyzer Cloud account does not have an add on storage license. FortiAnalyzer Cloud will disconnect from the on-premise FortiAnalyzer when the token is expired or invalid.

The *FortiAnalyzer Cloud Connector* includes the following actions:

Name	Description
Forward Logs	Forward logs to FortiAnalyzer Cloud. Edit this action to set the forwarding frequency for the connector.

Once configured and enabled, all non-FortiGate logs, such as FortiMail, FortiClient EMS, or third-party logs in the root ADOM will be forwarded to the FortiAnalyzer Cloud. FortiAnalyzer will not connect to FortiAnalyzer Cloud when the token is expired. You must update the access token for the connector once it is expired.

If the non-FortiGate devices have not yet been added in FortiAnalyzer Cloud, they will appear in the FortiAnalyzer Cloud *Device Manager* to be authorized. Once authorized, the logs can be viewed in the FortiAnalyzer Cloud *Log View*.

You can view the status of the connector from the *Dashboards > Status > FortiAnalyzer Cloud Status* widget. See FortiAnalyzer Cloud Status widget on page 75.

VirusTotal Connector

The VirusTotal connector is used as part of the indicator enrichment feature through the *Indicator Enrichment* playbook. To enable this connector, you must double-click the connector and add the API key. For more information, see Indicator enrichment on page 333.

The VirusTotal connector includes the following actions:

Name	Description
Query IP	Retrieves a report from VirusTotal for the IP address submitted to determine if it is suspicious based on the IP address you have specified.
Query Domain	Retrieves a report from VirusTotal for the domain submitted to determine if it is suspicious based on the domain name you have specified.
Query URL	Retrieves a report from VirusTotal for the URL submitted to determine if it is suspicious based on the URL you have specified.
VIRUSTOTAL Enrich	Enrich the indicator.

vSphere Connector

The vSphere connector includes the following actions:

Name	Description
Ingest vSphere Server Event Logs	Retrieves event logs from vSphere and ingests into FortiAnalyzer.

When you save a vSphere connector, a new playbook will automatically be added in the backend named, *Ingest vSphere Server Event Logs*. This playbook is run as per the schedule defined in the *Data Ingestion* tab. To configure *Data Ingestion*, see Configuring security fabric connectors on page 372. This playbook is not visible in the GUI, however its logs are available for troubleshooting under *Playbook Monitor* .

After the first time the playbook is run, it will pull all the logs from the vSphere server to FortiAnalyzer. It will also create a new *External-SIEM-Events* device in *Device Manager*; the device is automatically authorized and only one of such device is created per ADOM for all of the third-party connectors. Then the logs pulled from the server can be seen in *Log View* > *Logs* > *All* alongside other Fabric/SIEM logs; the logs are parsed by the predefined VMware Log Parser and assigned to the new external SIEM device. In *Log Browse*, the logs files will be available from the new device. The next time the playbook runs, only the new logs after the previous pull will be fetched and added to *Log View*.

The FortiAnalyzer CLI command "`diagnose test application fazwatchd 10`" can be used to check the ingestion stats or to manually trigger a playbook:

```
diagnose test application fazwatchd 10
Airflow Diag Usage:
info show generic airflow information
scheduler show airflow scheduler status
global-monitor show global monitor status
health-check-stat show health check status
ingestion-stat show data ingestion status
trigger-playbook execute a playbook
reset reset airflow database
logging-level set airflow logging level
reset-log-dir reset airflow log directory
```

Configuring security fabric connectors

You can use the *Active Connectors* pane to create the following types of security fabric connectors:

- FortiClient EMS
- FortiMail
- FortiCASB
- FortiAuthenticator
- FortiWeb
- FortiSandbox
- vSphere
- FortiEDR
- FortiAnalyzer Cloud

The following connectors cannot be created from the *Create New* action. However, they can be viewed and/or edited from the *Active Connectors* pane.

- Local Connector: The local connector is the default connector for FortiAnalyzer and is available automatically.
- FortiOS Connector: The FortiOS connector is added after the first FortiGate has been authorized on an ADOM. Additional devices authorized to the ADOM are displayed as separate entries within the same connector.
- FortiGuard Connector: The FortiGuard connector is automatically configured when a valid license has been applied to FortiAnalyzer.
- FMG Connector: You can edit and enable this connector to establish a fabric connection to FortiManager. See Adding FortiAnalyzer devices using a fabric connection in the FortiManager Administration Guide.

Further connectors may be available from FortiGuard with a license for the FortiAnalyzer Security Automation Service. See SOC Automation on page 338

Once configured, Security Fabric connectors enrich incident response related actions available in playbooks.

To create a Security Fabric connector:

1. Go to *Incidents & Events* > *Automation* > *Active Connectors*, and click *Create New*.
   Alternatively, if a card for the connector that you want to create, you can *Edit* to configure and enable the connector.
   The *Create New Fabric Connector* pane displays.
2. Under *Security Fabric*, select one of the available connector types.
3. In the *Configuration* tab, configure the following options for:
   FortiClient EMS

Option	Description
Type	Select *FortiClient EMS* or *FortiClient EMS Cloud*.
Name	Type a name for the Security Fabric connector.
Description	(Optional) Type a description for the Security Fabric connector.

Option		Description
FortiClient EMS	IP/FQDN	Type the IP address or FQDN for the Security Fabric device.
	Username	Type the username for the Security Fabric device.
	Password	Type the password for the Security Fabric device.
	Verify SSL	Enable to verify SSL.
FortiClient EMS Cloud	Account ID	Super users can type the account ID of the FortiClient EMS Cloud instance. For non-super users, the field is automatically populated with the default account ID. The FortiAnalyzer device must be registered with FortiCloud to create and update the connector as a non-super user. The FortiClient EMS must be v7.0 or later. After the FortiClient EMS Cloud connector is created, the connector's health-check sends an authentication request with SNI (the account ID) to the EMS instance. The authentication request from the FortiAnalyzer device must be approved in EMS: *Administration > Fabric Devices*. For more information, see *FortiClient* on the Fortinet Document Library.
	Verify SSL	Enable to verify SSL.
Site		If sites are enabled in EMS, enter the site.

FortiMail

Option	Description
Name	Type a name for the Security Fabric connector.
Description	(Optional) Type a description for the Security Fabric connector.
IP/FQDN	Type the IP address or FQDN for the Security Fabric device.
Username	Type the username for the Security Fabric device.
Password	Type the password for the Security Fabric device.

FortiCASB

Option	Description
Name	Type a name for the Security Fabric connector.
Description	(Optional) Type a description for the Security Fabric connector.
IP/FQDN	Type the IP address or FQDN for the Security Fabric device. Use the FortiCASB FQDN for your chosen server location. The server location is selected when creating your FortiCASB account. Use `forticasb.com` for global servers or `eu.forticasb.com` for EU based servers.
Account ID	Enter the credentials token used for authentication.

Option	Description
	To create a FortiCASB credentials token, log in to FortiCASB with your account, go to *Home* > *Manage Company* > *API Setting*, and click *Generate New*. For more information, see *FortiCASB* on the Fortinet Docs Library.

FortiAuthenticator

Option	Description
Name	Type a name for the Security Fabric connector.
Description	(Optional) Type a description for the Security Fabric connector.
IP/FQDN	Type the IP address or FQDN for the Security Fabric device.
User Name	Type the username for the Security Fabric device.
API Key	Enter the API key for the FortiAuthenticator device.

FortiWeb

Option	Description
Name	Type a name for the Security Fabric connector.
Description	(Optional) Type a description for the Security Fabric connector.
IP/FQDN	Type the IP address or FQDN for the Security Fabric device.
User Name	Type the username for the Security Fabric device.
Password	Type the password for the Security Fabric device.
FortiWeb ADOM	Enter the FortiWeb ADOM that the device is in.

FortiSandbox

Option	Description
Name	Type a name for the Security Fabric connector.
Description	(Optional) Type a description for the Security Fabric connector.
IP/FQDN	Type the IP address or FQDN for the Security Fabric device.
User Name	Type the username for the Security Fabric device.
Password	Type the password for the Security Fabric device.
FortiSandBox Version	Enter the version of the FortiSandbox device.
FortiSandBox Instance Type	Select the FortiSandbox instance type: On Premise or Cloud.

vSphere

Option	Description
Name	Type a name for the Security Fabric connector.

Option	Description
Description	(Optional) Type a description for the Security Fabric connector.
IP/FQDN	Type the IP address or FQDN for the data source.
User Name	Type the username for the data source.
Password	Type the password for the data source.

FortiEDR

Option	Description
Name	Type a name for the FortiEDR connector.
Description	(Optional) Type a description for the FortiEDR connector.
IP/FQDN	Type the IP address or FQDN for the FortiEDR device.
User Name	If the user on FortiEDR is configured for all organizations, type the user name. If the user on FortiEDR is configured with access for a specific organization, type the organization and user name. Use the following format: <organization>\<user name>.
Password	Type the password for the FortiEDR user.

FortiAnalyzer Cloud



The *FortiAnalyzer Cloud Connector* must be added in the root ADOM. See Connector actions on page 364.

Option	Description
Name	Type a name for the FortiAnalyzer Cloud Connector.
Description	(Optional) Type a description for the FortiAnalyzer Cloud Connector.
Access Token	Type the *Access Token* created in FortiAnalyzer Cloud.
Token Expiry Date	Populated based on the *Access Token*. Displays the expiry date for the access token.
FortiAnalyzer Cloud SN	Populated based on the *Access Token*. Displays the FortiAnalyzer Cloud serial number.
Region	Populated based on the *Access Token*. Displays the region for the FortiAnalyzer Cloud.
Token Type	Populated based on the *Access Token*. Displays the token type.

4. In the *Action* tab, view the actions available with the Security Fabric connector.
   For the *FortiAnalyzer Cloud Connector*, edit the *Forward Logs* action and set the following:

- *Status*: Toggle to enabled (default) or disabled.
- *Sending Frequency*: Select *Real-time*, *Every 1 Minute*, or *Every Five Minutes* (default).

5. If available, in the *Data Ingestion* tab, enable or disable the *Status* according to your needs.

   This feature allows you to define schedules for when to pull the logs from the external resource. This feature is only available for applicable connectors and it is disabled by default.

   If enabled, configure the following:

Option	Description
Schedule Selection	Select *Single Schedule* or *Custom Schedule*. • *Single Schedule*: configure the data ingestion schedule for all available enabled actions. • *Custom Schedule*: select each enabled action and click *Edit* to configure its data ingestion schedule.
The start time of the schedule	Select the date and time to begin the data ingestion schedule.
The end time of the schedule	Select the date and time to end the data ingestion schedule.
The interval unit of the schedule	Select the unit to set the interval for the schedule: • *N-MINUTES* • *N-HOURS* • *N-DAYS* • *CRON*
The interval value of the schedule	Set the integer. This is the interval for data ingestion according to *The interval unit of the schedule*. For example: • *The interval unit of the schedule* = N-HOURS • *The interval value of the schedule* = 5 Data ingestion is scheduled for every 5 hours.
Actions	Enable the *Actions* that should perform data ingestion at the set schedule. Data ingestion schedules can only be configured for some actions; these actions are indicated in the *Actions* tab for the connector.

6. To save the connector, click *OK*.

   After the connector is saved, it is visible in *Incidents & Events > Automation > Active Connectors* with a toggle to enable or disable the connector.

7. Toggle the status of the connector to disabled or enabled according to your needs.

After the Security Fabric connector is created, playbooks configured in *Incidents & Events > Automation > Playbook* can use the connector to execute automated actions. For a list of connector actions available in playbooks, see Connector actions on page 364.

Default playbooks are automatically created when configuring some Security Fabric connectors. For more information on playbooks, see Playbooks on page 382.

To edit a Security Fabric connector:

1. Go to *Incidents & Events* > *Automation* > *Active Connectors*.
2. Select a Security Fabric connector, and click *Edit*.
   The *Edit Connectors* pane displays.
3. Edit the settings, and click *OK*.

Configuring ITSM connectors

You can use the *Active Connectors* tab to create the following types of ITSM connectors:

- MS Teams
- ServiceNow
- Slack
- Webhook, a generic connector

You can create ITSM connectors for ServiceNow, Slack, MS Teams, and Webhook.

To create an ITSM connector:

1. Go to *Incidents & Events* > *Automation* > *Active Connectors*, and click *Create New*.
2. Under *ITSM*, select one of the available connector types.

3. Configure the following options, and click *OK*:

Property	Description
Name	Type a name for the fabric connector.
Description	(Optional) Type a description for the fabric connector.
Protocol	Select *HTTPS*. For Slack connectors and Generic connectors, you can also select *HTTP*.
Port	Specify the port FortiAnalyzer uses to communicate with the external platform.
Method	For ServiceNow and MS Teams connectors, select *POST*. For Slack connectors, select *POST* or *PUT*. For Generic connectors, select one of the following: • *POST* • *PUT* • *GET* • *PATCH* • *DELETE*
Title	Type a title for the fabric connector.
URL	Type the URL of the external platform. This option is not available for the MS Teams Connector. Using ServiceNow as an example, copy and paste the URL from *ServiceNow API URL* in the *Connection to ServiceNow API* section in *ServiceNow > FortiAnalyzer System Properties*.
Custom HTTP Header	Enable to use custom HTTP headers. This option is only available for Generic connectors. These headers store information in the form of key-value pairs. They can be used for communcation control, content description, authentication, session management, caching, and more. If enabled, add any number of *HTTP Headers* by clicking the plus sign (+). Enter the key-value pairs.  When *Custom HTTP Header* is enabled, *HTTP Authentication* is no longer available for the connector. This is because you can use the custom HTTP headers for HTTP authentication instead.
Teams Webhook URL	Type the incoming webhook URL created in MS Teams. This option is only available for the MS Teams Connector.
HTTP Body	Type the HTTP body of the message that should be sent by the connector. This option is only available for Generic and MS Teams connectors.

Property	Description
	For example, `{ \"text\": \"<message to send>\" }`. You also use `${}` for macros in the message. For a list of supported macros, see Supported macros for the MS Teams Connector.
HTTP Authentication	Enable or disable HTTP authentication. This option is not available for the *MS Teams Connector*. If enabled, select *Basic* or *OAuth2* authentication type. Using ServiceNow with *Basic* authenictation as an example, enter the username and password from the *Connection to ServiceNow API* section in *ServiceNow > FortiAnalyzer System Properties*. Using a Generic webhook connector with *OAuth2* authentication as an example, enter the URL of the token service as well as the client ID and client secret for authentication.
Status	Enable or disable the fabric connector.

To use a generic connector:

Generic webhook connectors can be used to send notifications about incidents and events. After it is created, the connector can be added in the incident settings or in notification profiles for event handlers. They can also be used as part of a playbook; for example, see Playbook examples on page 386.

- Configuring incident settings on page 212
- Creating notification profiles on page 317
- Playbooks on page 382

To use a ServiceNow connector:

ServiceNow connectors can be used to post incident change notices. After it is created, the ServiceNow connector can be added in the incident settings or as part of a playbook.

- Configuring incident settings on page 212
- Playbooks on page 382

To use a Slack connector:

Slack connectors can be used to send messages in Slack about incidents and events. After it is created, the Slack connector can be added in the incident settings or notification profiles for event handlers.

- Configuring incident settings on page 212
- Creating notification profiles on page 317

To use an MS Teams connector:

MS Teams connectors can be used to send messages in MS Teams about incidents and events. After it is created, the MS Teams connector can be added in the incident settings, notification profiles for event handlers, or as part of a playbook.

- Configuring incident settings on page 212
- Creating notification profiles on page 317
- Playbooks on page 382

To edit an ITSM connector:

1. Go to *Incidents & Events* > *Automation* > *Active Connectors*.
2. Select an ITSM connector, and click *Edit*.
   The *Edit Connectors* pane displays.
3. Edit the settings, and click *OK*.

Supported macros for the MS Teams Connector

Category	Variable	Macro	Description
Global	type	${type}	Notification type
Global	adom	${adom}	Adom name
Global	from	${from}	FAZ SN
Global	timestamp	${timestamp}	Notification timestamp
Event	event	${event}	All event fields
Event	eventid	${event.eventid}	Event id
Event	alertid	${event.alertid}	Alert id (same with eventid, but name consistent with previous notification format)
Event	logtype	${event.logtype}	Log type
Event	devtype	${event.devtype}	Device type
Event	eventtime	${event.eventtime}	Event time
Event	alerttime	${event.alerttime}	Alert time (same with eventtime, but name consistent with previous notification format)
Event	firstlogtime	${event.firstlogtime}	First log time
Event	lastlogtime	${event.lastlogtime}	Last log time
Event	devid	${event.devid}	Device id
Event	devname	${event.devname}	Device name
Event	eventtype	${event.eventtype}	Event type
Event	groupby1	${event.groupby1}	groupby1
Event	groupby2	${event.groupby2}	grouby2
Event	groupby3	${event.groupby3}	grouby3

Category	Variable	Macro	Description
Event	indicator	${event.indicator}	indicator
Event	severity	${event.severity}	severity
Event	subject	${even.subject}	subject
Event	tag	${event.tag}	tag
Event	triggername	${event.triggername}	Trigger name
Event	vdom	${event.vdom}	vdom
Event	epid	${event.epid}	epid
Event	euid	${event.euid}	euid
Event	epip	${event.epip}	epip
Event	epname	${event.epname}	epname
Event	euname	${event.euname}	euname
Event	extrainfo	${event.extrainfo}	Additional info
Event	log-length	${event.log-length}	Log length
Event	log-detail	${event.log-detail}	Log detail
Incident	incident	${incident}	All incident fields
Incident	incid	${incident.incid}	Incident ID
Incident	type	${incident.type}	Notification type
Incident	revision	${incident.revision}	revision
Incident	attach_revision	${incident.attach_ revision}	attach revision

Playbooks

Playbooks include a starter event (a trigger) and one or more tasks configured with automated actions. A task is run as soon as the playbook is triggered and all connected tasks preceding it are complete.



To manage playbooks, administrators must be assigned an administrator profile with *Read-Write* permissions for *Incidents & Events*. See Administrator profiles on page 566.

To manage playbooks, go to *Incidents & Events* > *Automation* > *Playbook*. The following options are available:

Create New	Create a new playbook. Playbooks can be created from scratch or by using playbook templates.
Run	Run selected playbooks that are configured with the *ON_DEMAND* trigger.

	When you run a playbook, you will be asked to configure the parameters in the *Manually Run Playbook* dialog. Once run, the *Playbook Tasks* dialog displays the live progress of the job, including the following information: • Job details, including Job ID, Playbook name, Trigger, Start Time, End Time, and Status. • Timeline for each task in the playbook. • Raw logs for each task in the playbook; select the task in the timeline to display the related raw log.  You can run playbooks directly from an incident, when appropriate. See Analyzing an incident on page 208.
Edit	Edit the selected playbook.
Clone	Clone the selected playbook.
Delete	Delete the selected playbook.
Enable	Enable the selected playbook.
Disable	Disable the selected playbook.
Import	Import a playbook. For more information, see Importing and exporting playbooks on page 394.
Export	Export the selected playbook. For more information, see Importing and exporting playbooks on page 394.
Column Settings	Choose which columns are displayed in the playbook table.
Search	Perform a text search for the playbook name, description, created time, and modified time.

Creating a playbook

When creating or editing a playbook, you can click and drag to pan the view of the playbook editor. View controls are also available in the top right of the pane to zoom in, zoom out, and fit view.

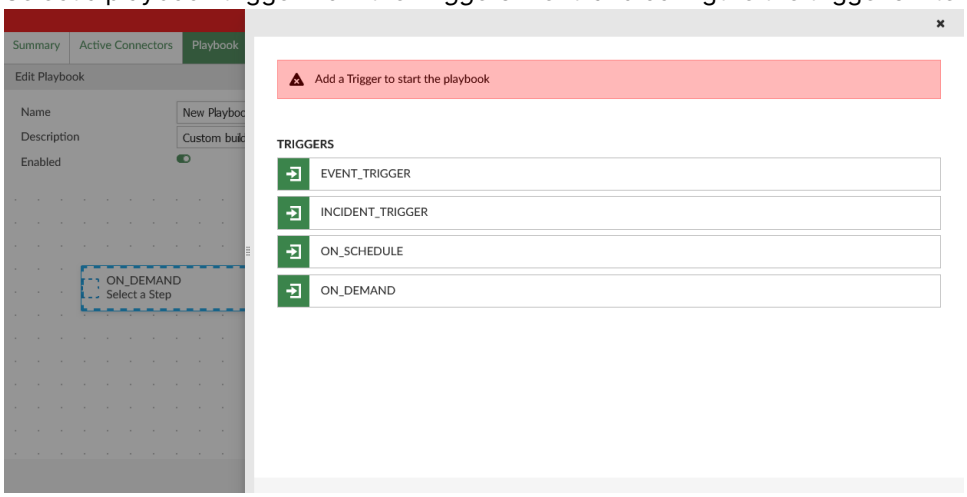
To create a playbook:

1. Go to *Incidents & Events* > *Automation* > *Playbook*, and click *Create New*.
   Select a playbook template or choose *New Playbook created from scratch*.
   The playbook editor opens.

    When a playbook template is selected, the playbook designer is automatically populated with a trigger and one or more tasks. You can configure trigger filter conditions and add or remove tasks to customize the playbook. See Playbook templates on page 390.

2. Click within the playbook's title field to change its name and description.

3. Select a playbook trigger from the *Triggers* menu and configure the trigger's filter conditions.

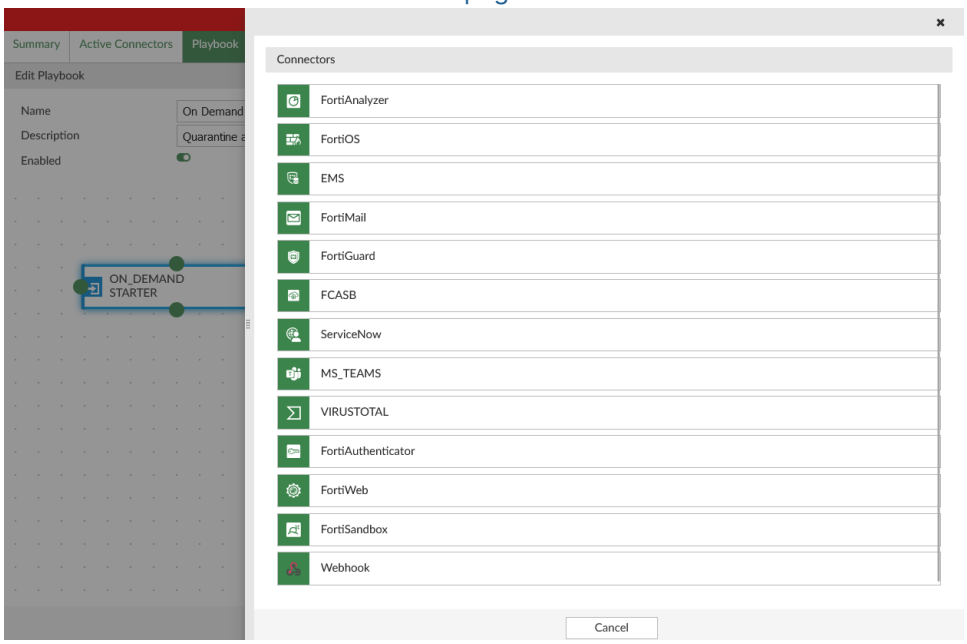


Once the trigger is created, it is displayed in the playbook editor with highlighted connector points.

For more information on the available playbook triggers, see Playbook triggers and tasks on page 391.

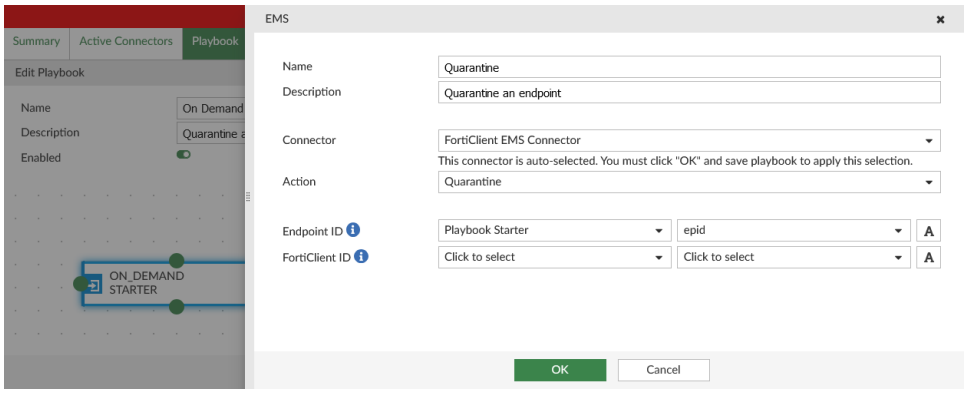
4. Add playbook tasks.

Drag-and-drop any connector point to add a new task. The *Tasks* window is displayed showing available connectors. See Connector actions on page 364.



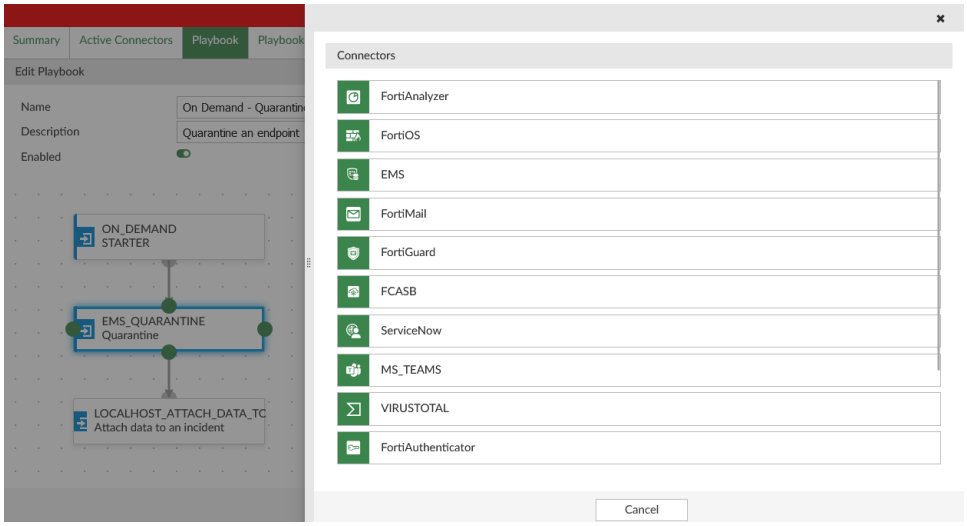
5. Select a connector type and configure an automated action:

Name	Enter a name for the task.
Description	Enter a description of the task.
Connector	Select a connector to use from the dropdown menu. See Connector actions on page 364.
Action	Select the automated action to be performed.
Parameters	Configure the parameters for the selected action.



6. Connect playbook tasks.

   Additional connector points can be added to connect this task to other tasks in the playbook. A task automatically begins once *all* preceding tasks connected to it have been completed. A playbook ends when there are no additional tasks to run.



7. (Optional) Manage your playbook by clicking on one of the options displayed when hovering your mouse over the trigger or task:
   - **Edit**: Edit the trigger or task.
   - **Delete**: Delete the task.
8. Click *Save Playbook*.

Enabling and disabling playbooks

Once created, playbooks can be enabled or disabled through the playbook editor. Enabled playbooks will run as soon as their trigger conditions are met. Playbooks configured with the *On_Demand* trigger start when manually initiated by the administrator in *Incidents & Events > Automation > Playbook* or an Incident's *Analysis* page.

To enable or disable a playbook:

1. Go to *Incidents & Events > Automation > Playbook*.
2. Edit a previously configured playbook.

3. In the playbook designer, toggle *Enabled*, as needed.
4. Click *Save Playbook*.
   Alternatively, you can select the playbook and click *Enable* or *Disable* in the toolbar.

Playbook examples

This topic includes the following playbook examples:

- Example: Using a FortiGuard connector
- Example: Using generic connectors in a playbook

Example: Using a FortiGuard connector

The FortiGuard connector is automatically configured when a valid *Indicators of Compromise Service* license has been applied to FortiAnalyzer. For more information about this license, see Viewing Indicators of Compromise on page 112.

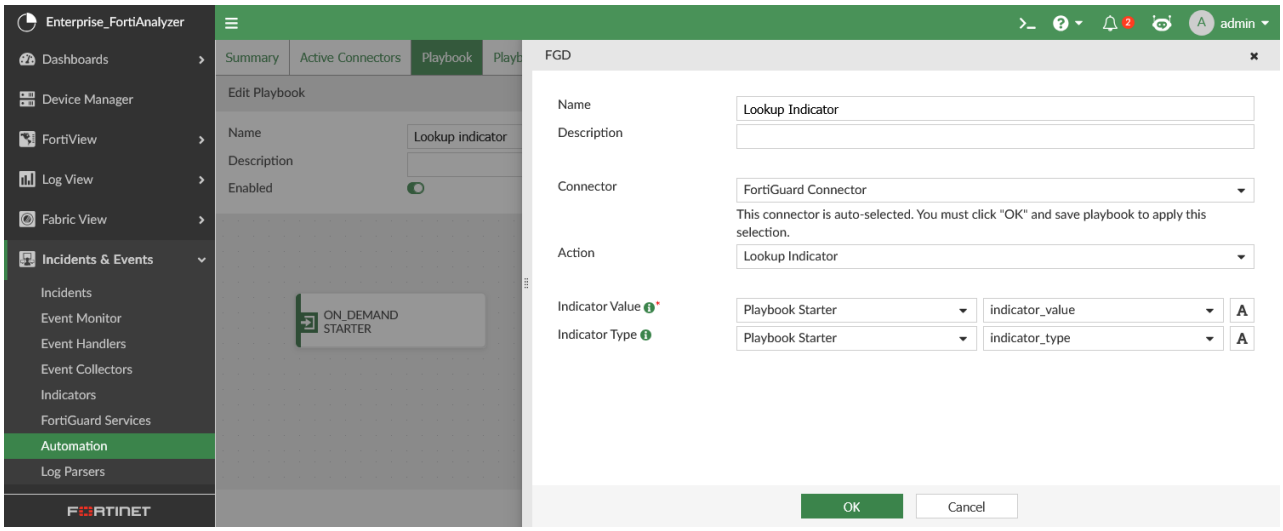
The FortiGuard connector can be used to perform an indicator lookup, which is used to determine the related threat information for the indicator value (IP, URL, or domain).

For example, an admin investigating an incident in FortiAnalyzer notices some traffic with unknown URLs. With the help of the FortiGuard real-time threat intelligence service, the admin can determine the enrichment information of the URL and then conclude if it is suspicious or not.

In the below example, a playbook is created to manually perform the indicator lookup and attach the data to an existing incident.

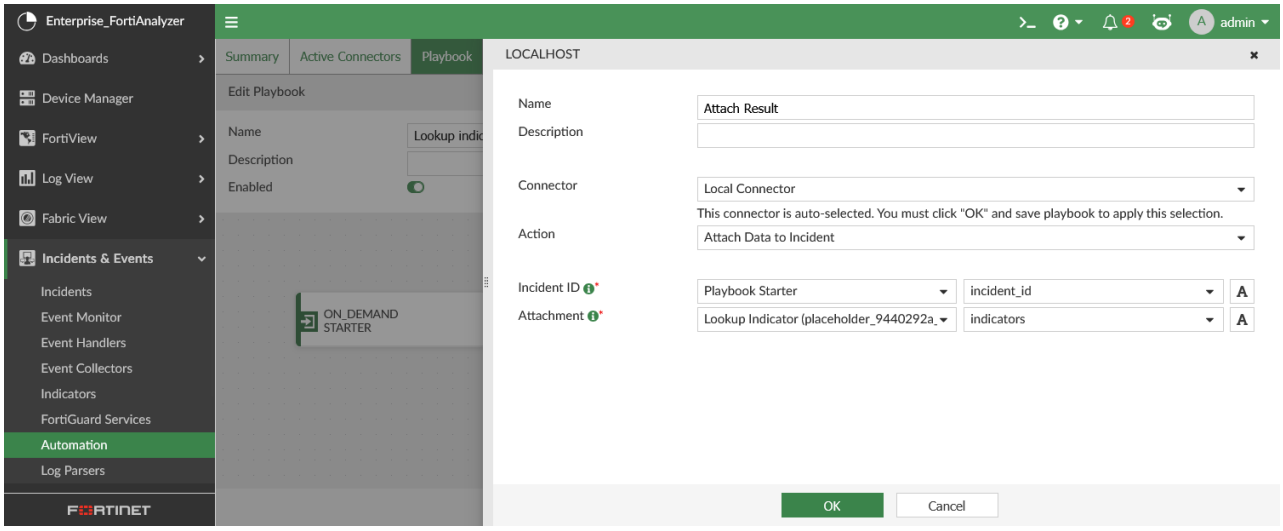
1. In *Incidents & Events* > *Automation* > *Playbook*, create a new playbook from scratch.
2. For *Triggers*, select *ON_DEMAND*.
3. Create a task using the FortiGuard connector with the following configuration:

Name	Enter a name for the connector.
Description	Optionally, enter a description for the connector.
Connector	Select *FortiGuard Connector*.
Action	Select *Lookup Indicator*. The *Indicator Value* field displays.
Indicator Value	Select *Playbook Starter* and *indicator_value*.
Indicator Type	Select *Playbook Starter* and *indicator_type*.

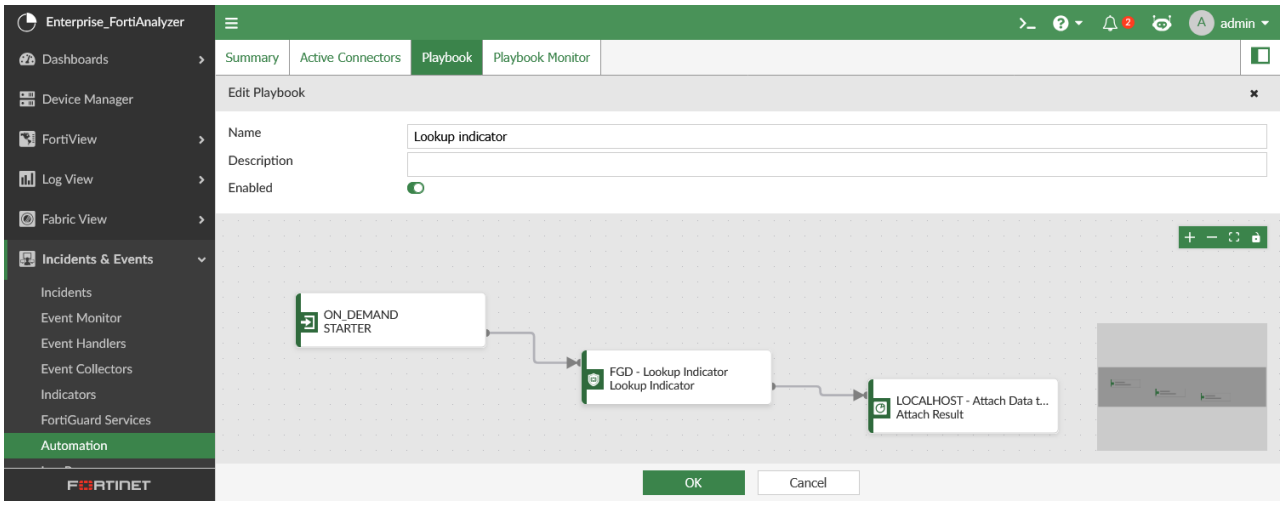


4. Create a task using the FortiAnalyzer (local) connector with the following configuration:

Name	Enter a name for the connector.
Description	Optionally, enter a description for the connector.
Connector	Select *Local Connector*.
Action	Select *Attach Data to Incident*. The *Incident ID* and *Attachment* fields display.
Incident ID	Select *Playbook Starter* and *incident_id*.
Attachment	Select *Lookup Indicator* and *indicators*.

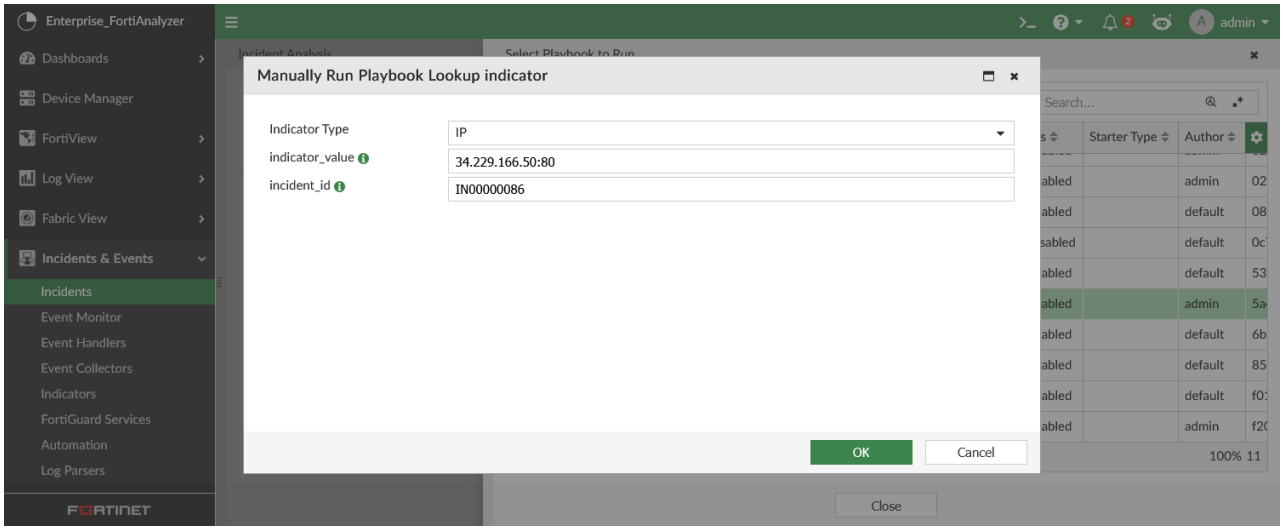


5. Save the playbook.



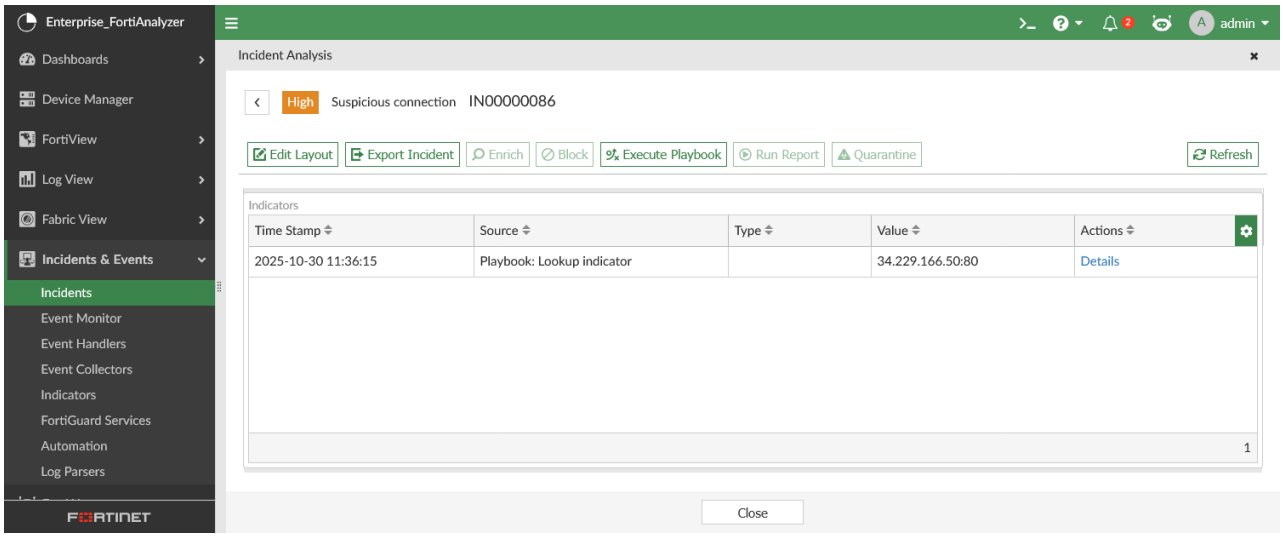
6. When you run the playbook, you will enter the indicator type and value.

You can run the playbook directly from the incident to automatically populate the incident ID. Otherwise, you can manually enter the ID when running the playbook.

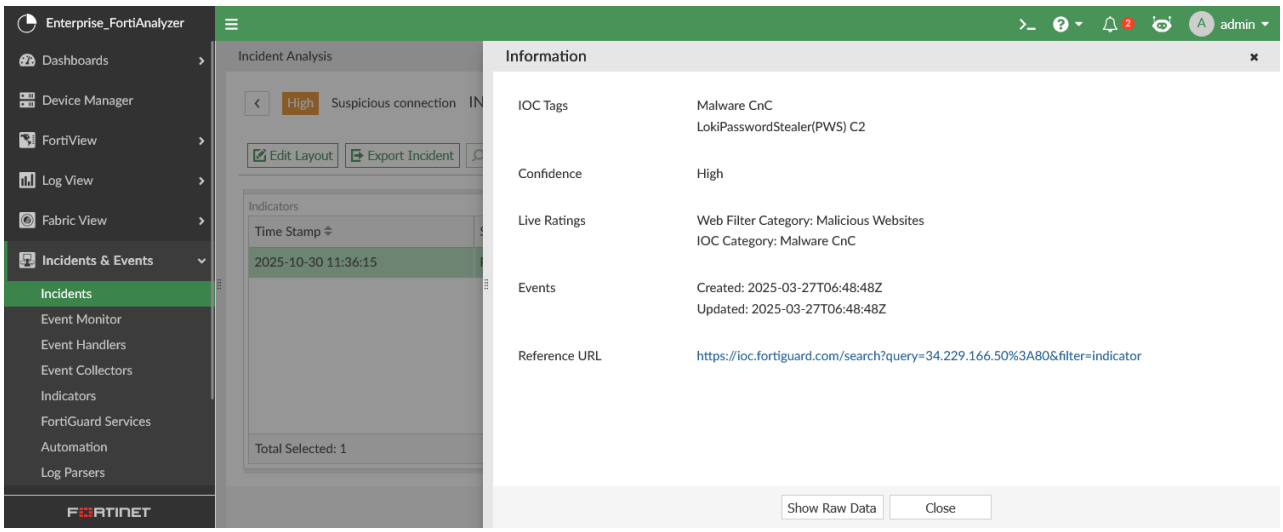


The *indicator_value* is a malicious IP, URL, or domain. The FortiGuard connector checks the FortiGuard threat database for information related to the indicator. If there is a match for the entered IP, URL, or domain in the threat database, the information from FortiGuard will be attached to the incident.

7. In *Incidents & Events* > *Incidents*, open the *Incident Analysis* pane for the incident.
8. To view the attached results from the playbook, go to the *Indicators* widget.



9. To view the threat details pulled from FortiGuard, click *Details* in the *Actions* column.

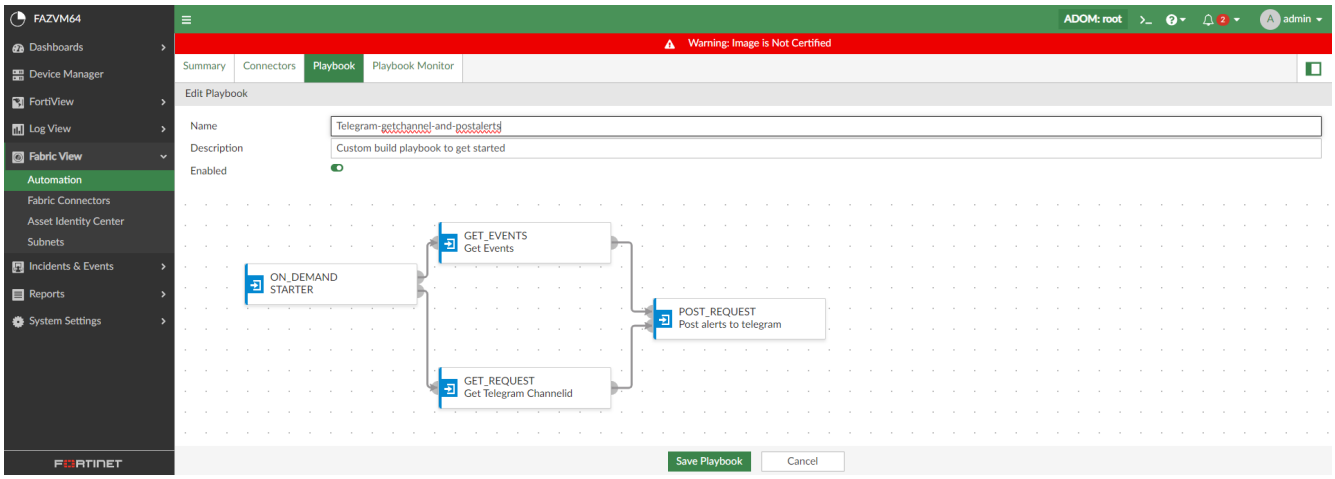


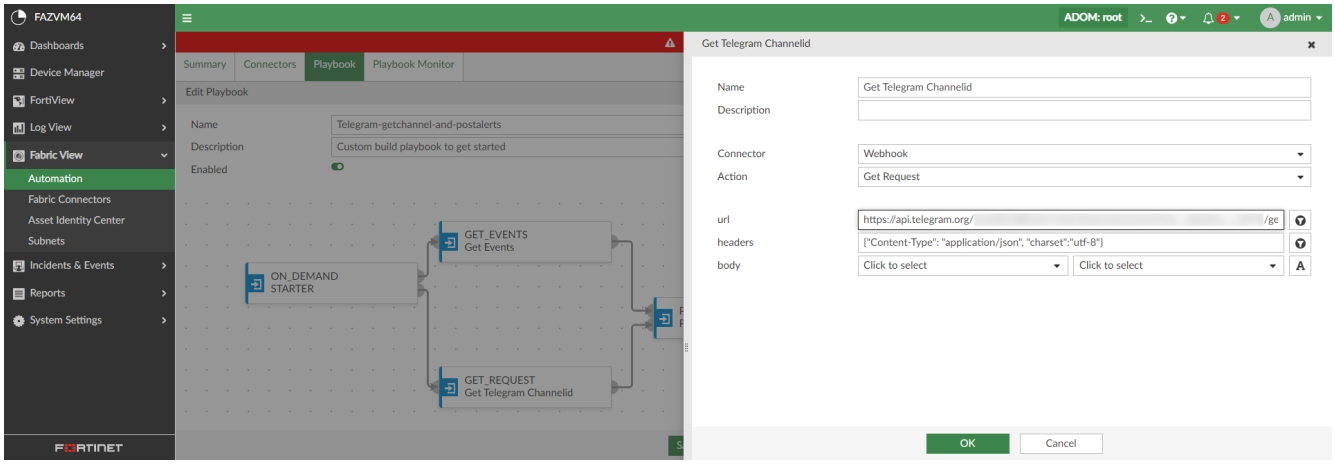
Example: Using generic connectors in a playbook

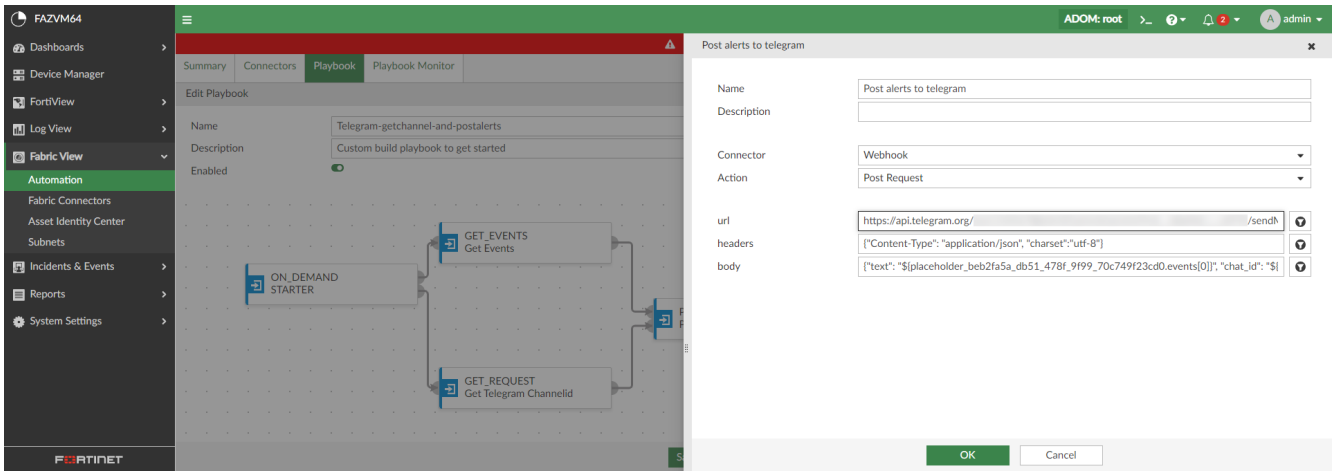
The below playbook is configured to get the channel ID from one task and then use it in another task to send the alerts to a protected server.

This example uses generic webhook connectors. For information about configuring generic connectors, see Configuring ITSM connectors on page 378.

While the URL is included when configuring a generic connector, you will be required to enter the URL again when using the generic webhook connector in the playbook. See the *url* field in the example below.







Playbook templates

When a playbook template is selected, the playbook designer is automatically populated with a trigger and one or more tasks. You can configure, add, or remove tasks to customize the playbook.

When creating a new playbook, the following predefined templates are available:

Connector	Name	Description
FAZ Localhost	**Compromised Host Incident**	Playbook to create an incident on FortiAnalyzer compromised hosts detected by the IoC feature.
	Critical Intrusion Incident	Playbook to create an incident on FortiAnalyzer for critical intrusions detected by IPS.
	Attach Endpoint Vulnerability List to Incident	Playbook to collect the list of endpoint vulnerabilities from logs and attach it to an incident.
FortiOS	**Quarantine Endpoint by FortiOS**	Playbook to quarantine an endpoint by FOS connector providing the MAC address or FortiClient UID.
FortiClient EMS	**Update Asset and Identity Database**	Playbook to automatically update FortiAnalyzer Asset and Identity database with endpoint and user information from EMS.
	Run AV Scan on Endpoint	Playbook to run AV scan on an endpoint by EMS Connector.
	Run Vulnerability Scan on Endpoint	Playbook to run a vulnerability scan on an endpoint.
	Quarantine Endpoint by EMS	Playbook to quarantine an endpoint by EMS connector.
	Unquarantine Endpoint by EMS	Playbook to unquarantine an endpoint by EMS connector.
	Enrich Incident with Process List	Playbook to get running processes on endpoint by EMS connector and attach to an incident.
	Enrich Incident with Vulnerability List	Playbook to collect the list of endpoint vulnerabilities from logs and attach to an incident.
	Enrich Incident with Software Inventory	Playbook to get software inventory from endpoint by EMS connector and attach to an incident.

Playbook triggers and tasks

Triggers

Triggers determine when a playbook is to be executed. Triggers are always the first step in a playbook, and each playbook can only include one trigger. Once a playbook has been triggered, it flows through the remaining tasks as defined by the routes in the playbook using the trigger as a starting point.

The following playbook triggers are available:

Trigger	Description
EVENT_TRIGGER	The playbook is run when an event is created that matches the configured filters. You can configure filters that require *All of the following conditions* to be met or *Any of the following conditions* to be met. When no filters are set, all events will trigger the playbook.
INCIDENT_TRIGGER	The playbook is run when an incident is created that matches the configured filters. You can configure filters that require *All of the following conditions* to be met or *Any of the following conditions* to be met. When no filters are set, all incidents will trigger the playbook.
ON_SCHEDULE	The playbook is run during the configured schedule. You can define the start time, end time, interval type, and interval frequency for the schedule.
ON_DEMAND	The playbook is run when manually started by an administrator. You can run playbooks configured with the *ON_DEMAND* trigger from *Incidents & Events* > *Automation* > *Playbook* or within an incident's *Incident Analysis* page.

Tasks

Tasks include automated actions that take place on FortiAnalyzer or devices with configured connectors. See Connector actions on page 364.

Tasks can be linked together in sequences. A task's automated action will only begin once the playbook is triggered and all preceding connected tasks are complete.

Tasks can be configured with default input values or take inputs from the trigger or preceding tasks. For more information about linking and configuring tasks in a playbook, see Playbooks on page 382.



FortiOS actions are configured using automation rules created on FortiGate. For more information on enabling FortiOS actions in tasks, see Connector actions on page 364.

Configuring tasks using variables

Variables can be used when configuring playbook tasks. There are two types of playbook variables, including output variables and trigger variables.

For a list of trigger and output variables that can be used when configuring playbook tasks, see FortiAnalyzer Playbook Variables on the Fortinet Docs Library.

Output variables

Output variables allow you to use the output from a proceeding task as an input to the current task. For example, the report generated in one task can be attached to an incident in a second task. For a list of output types, see *Incidents & Events > Automation > Connectors*. A task ID is created automatically for each task added to the playbook.

Output variables use the following format:

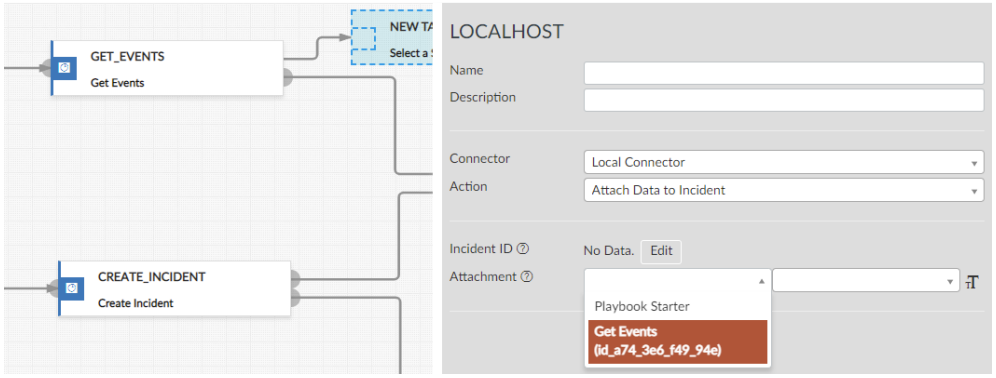
Format: `${<task_id>.<output>}`

Example: `${id_2c7_84b_2c5_f47.vulnerabilities}`

Obtaining task IDs

Task IDs are not currently displayed within a task. To view a task ID, the following workaround can be used.

1. Create a new task in the playbook using the Local Connector action *Attach Data to Incident*.
2. In the *Attachment* dropdown, select a preceding task to view its task ID. You can switch to text mode to copy the value after selection.



Trigger (incident and event) variables

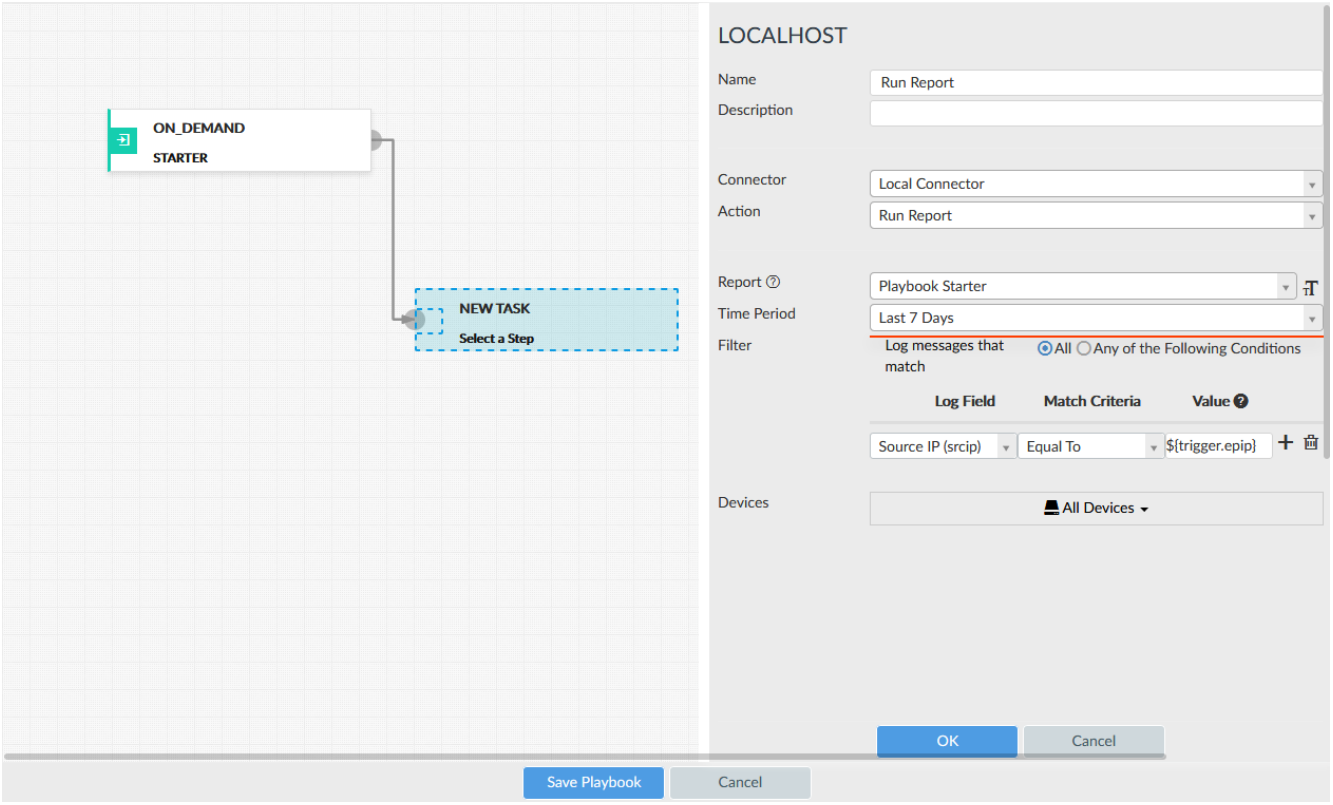
Trigger variables allow you to use information from the trigger (starter) of a playbook when it has been configured with an incident or event trigger.

For example, the *Run Report* action can include a filter for the endpoint IP address from the event that triggered the playbook.

Trigger variables use the following format:

Format: `${trigger.<variable>}`

Example: `${trigger.epip}`



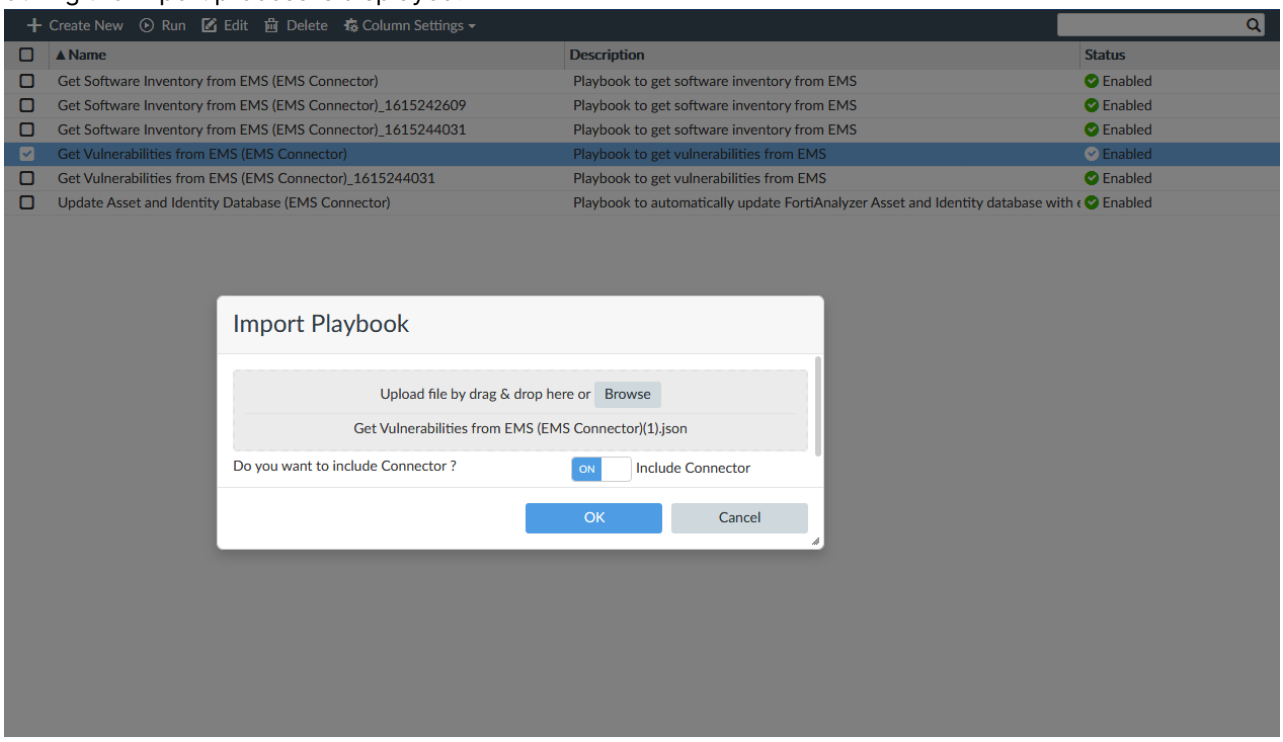
Importing and exporting playbooks

You can import or export playbooks, including the connectors required to support the playbook, by using the right-click context menu in the playbook dashboard.

To import a playbook:

1. Go to *Incidents & Events* > *Automation* > *Playbook*.
2. Right-click in the playbook dashboard, and click *Import*.
   The *Import Playbook* dialog appears.
3. Click *Browse* and select the playbook file to be imported.
   When the playbook file includes connectors, a toggle allowing you to include or exclude the connectors

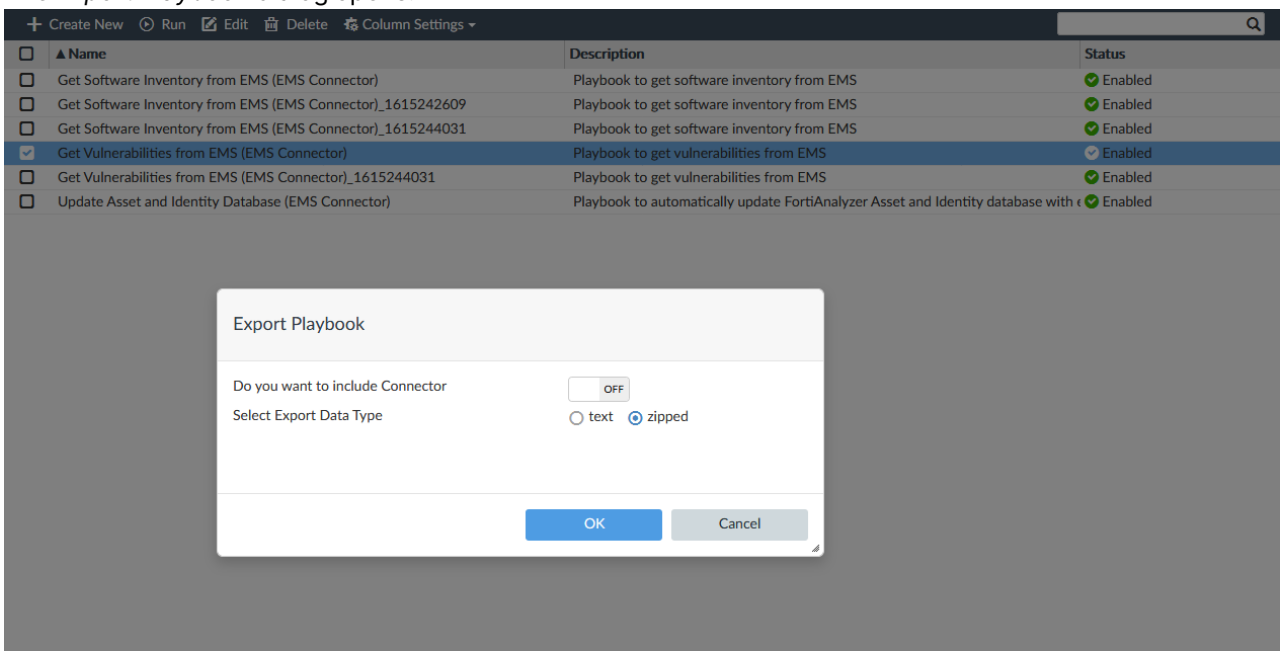
during the import process is displayed.



4. Click *OK*.
   A message is displayed confirming that the playbook was imported successfully.

To export a playbook:

1. Go to *Incidents & Events* > *Automation* > *Playbook*.
2. Highlight the playbook(s) that you want to export, then right-click in the dashboard and click *Export*.
   The *Export Playbook* dialog opens.



3. Configure the settings for exporting the selected playbook:
   a. *Do you want to include Connector*: When enabled, connectors required to run this playbook will be included in the exported file.
   b. *Select Export Data Type*: Select the export file type as either plain text JSON or zipped/base 64 encoded JSON.
4. Click *OK*.



When an imported playbook has the same name as an existing playbook, FortiAnalyzer will automatically create a new name which includes the import timestamp to avoid a conflict.

Playbook Monitor

You can view the status of playbook jobs in *Incidents & Events* > *Automation* > *Playbook Monitor*.

You can perform the following actions on the *Playbook Monitor* table:

- Click *Refresh* to refresh the table view.
- Select the checkbox for playbook jobs and click *Delete* to remove them from the table view.
- Use the *Search* field to find specific playbook jobs.

The *Playbook Monitor* table includes the following columns:

Column	Description
Job ID	The unique ID of the playbook job. The ID includes the date and time that the job began as well as a unique number.
Playbook	The name of the playbook as configured in *Incidents & Events* > *Automation* > *Playbook* .
User	Displays the name of the administrator who started the playbook job when configured with the *On Demand* trigger.
Start Time	The date and time that the job began.
End Time	The date and time that the job ended.
Status	The current status of the job. Statuses include: • **Running**: The job is currently running. • **Success**: The job has finished with all tasks completed successfully. • **Failed**: The job has finished with one or more tasks failing to complete successfully.
Details	Clicking the *Details* icon shows the status of each task run by the playbook. After double-clicking a record in the table or clicking the *Details* icon for a playbook job, the *Playbook Tasks* dialog displays. This dialog includes the live or historical progress of the job, including the following information: • Job details, including Job ID, Playbook name, Trigger, Start Time, End

Column	Description
	Time, and Status. • Timeline for each task in the playbook. • Raw logs for each task in the playbook; select the task in the timeline to display the related raw log.

Task statuses include:

Task status	Description
Scheduled	Scheduled to run.
Success	Completed successfully.
Failed	Failed to complete.
Upstream_failed	Failed because the task could not connect with an upstream device.

Playbook jobs that include one or more failed tasks are labeled as *Failed* in Playbook Monitor, however, individual actions may have been completed successfully.

SIEM log parsers

FortiAnalyzer's SIEM capabilities parse, normalize, and correlate logs from Fortinet products as well as third-party applications. For example, there are built-in log parsers for Apache and Nginx web servers, and the security event logs of Windows and Linux hosts (with Fabric Agent integration). Additionally, more log parsers for other third-party applications can also be added from FortiGuard when FortiAnalyzer has a valid license for the Security Automation Service.

The SIEM logs parsed by these log parsers are displayed in *Log View > Logs > All* and can be used when generating reports or creating event handlers.

Parsing from the built-in log parsers and FortiGuard log parsers is predefined by FortiAnalyzer and does not require manual configuration by administrators. The predefined SIEM log parsers can be managed in *Incidents & Events > Log Parsers*. This pane includes predefined log parsers, log parsers from FortiGuard, and any custom log parsers that you have imported.

The *Incidents & Events > Log Parsers* pane is only available in Fabric ADOMs.

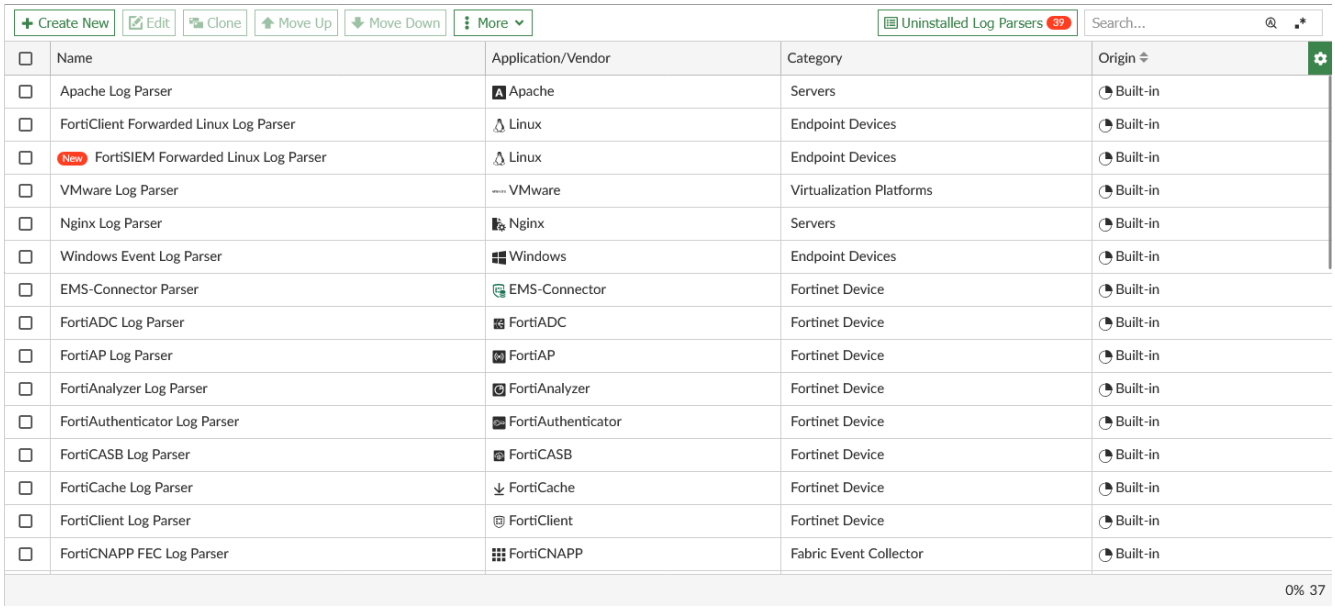
This topic includes information about:

- Log Parsers on page 398
- Assigned Parsers on page 400

For more information about normalized fabric logs, including the normalized log fields, see the Fabric Normalization Reference on the Fortinet Document Library.

Log Parsers

Go to *Incidents & Events* > *Log Parsers* > *Log Parsers* to view available log parsers in the table view.



The log parsers are listed in order of priority; they can be moved up or down in the table to change priority. You cannot sort the table using the column headers.

The table view includes the following columns:

Column	Description
Name	The name of the SIEM log parser.
Application/Vendor	The application of the log parser.
Category	The category of the log parser.
Origin	The origin of the log parser. Predefined log parsers indicate the origin is *Built-in*. Log parsers delivered in content packages will indicate the origin is *FortiGuard*. For more information, see Finding Security Automation Service objects on page 340.
Status	The status of the log parser: *Enabled* or *Disabled*.
Priority	The priority of the log parser. To change the priority of a log parser, select the parser and click *Move Up* or *Move Down*. Alternatively, you can click and hold the checkbox column for the row to drag and drop the log parser to the appropriate priority in the table.



You can also view the SIEM logs from *Log View* > *Logs* > *All*. Filter the log view by `Data Parser Name = name of the log parser` to display the related logs. For example, filter by `Data Parser Name = FortiGate Log Parser` to display logs related to the FortiGate Log Parser.

You can perform the following actions from *Incidents & Events* > *Log Parsers* > *Log Parsers*:

Action	Description

Create New	Create a new log parser from within the GUI.
	Log parsers must include the following three sections:
	• header: Basic information, including name, category, and application.
	• data_source: Checks if patterns in logs match the device.
	• parser: Includes two sub parts:
	  • rules: Includes the trigger and the subsequent actions. In other words, if "trigger", then do "actions".
	  • field_map: Value to fields in the siemdb.
	For more information, see Custom Log Parsers on the Fortinet Document Library.

View	View the selected log parser configuration. Click *text* or *tree* to toggle the view of the configuration. In both views, you can use the search function to find text within the configuration. In the *text* view, you can enable or disable the following search features: • *match case* • *regexp* • *by word* In the *tree* view, you can collapse and expand sections for readability. You can also use the breadcrumb feature to expand and highlight an individual section or line. The tree view also provides a copy button to copy highlighted text.
Clone	Clone the selected log parser.
Move Up / Move Down	Increase (*Move Up*) or decrease (*Move Down*) the priority of a log parser. Alternatively, you can click and hold the checkbox column for the row to drag and drop the log parser to the appropriate priority in the table.
View Logs	Open the *Log View for Log Parser* pane to display all related SIEM logs in a table view.
Disable	Disable a log parser. You cannot disable a log parser if it is assigned and in use. Once disabled, the log parser will be included in the *Uninstalled Parsers* pane.
Validate	Validate a raw log with the selected log parser. You cannot perform the *Validate* action with more than one log parser at a time.
Delete	Delete a custom log parser. You cannot delete a predefined log parser.
Import	Import a custom log parser. The log parser must be in JSON format. If needed, you can select *Overwrite custom parser*; you cannot overwrite predefined parsers.

Action	Description
	For more information, see Custom Log Parsers on the Fortinet Document Library.
Export	Export a log parser in the JSON format. Select a location to save the JSON file locally.
Uninstalled Log Parsers	This button includes the number of uninstalled log parsers. Click to open the *Uninstalled Parsers* pane. The *Uninstalled Parsers* pane lists all the currently uninstalled (disabled) log parsers. Sort the columns or use the search bar to find a specific log parser in the list. To install (enable) log parsers, select the checkbox for the log parser(s) and, in the tool bar, click *Install*. Clicking *Install* in the *Install* column will only install that individual log parser.

Third-party logs can be parsed in JSON format.

Assigned Parsers

Devices are assigned automatically according to the log matching patterns (data_source) defined in the parser.

Go to *Incidents & Events* > *Log Parsers* > *Assigned Parsers* to view the devices/applications and their current log parser assignments in a table view.



In some cases, a `SIEM-Device` is automatically created for third-party application log parsers, such as those from FortiGuard. These devices are automatically assigned according to the matched patterns on the raw logs. For example, see Microsoft management activity API connector on page 340.

If the raw logs are not matched to any log parser, the Generic SYSLOG parser will be automatically assigned to the device.

To assign a log parser to a device/application:

1. In *Incidents & Events* > *Log Parsers* > *Assigned Parsers*, click *Create New*.
   The *Assign Parser* pane displays.
2. From the *Device ID* dropdown, select a device for the log parser assignment.
3. From the *Application* dropdown, select an application for the log parser assignment.
4. From the *Current Parser* dropdown, select the log parser.
   The log parser must use the selected *Application*. See *Incidents & Events* > *Log Parsers* > *Log Parsers* to determine which application is used by the log parser.
5. Click *OK*.

To edit a log parser assignment:

1. In *Incidents & Events* > *Log Parsers* > *Assigned Parsers*, click *Create New*.
   The *Change Parser* pane displays.
2. From the *Current Parser* dropdown, select the log parser.
   The log parser must use the selected *Application*. See *Incidents & Events* > *Log Parsers* > *Log Parsers* to determine which application is used by the log parser.
3. Click *OK*.

FortiAI

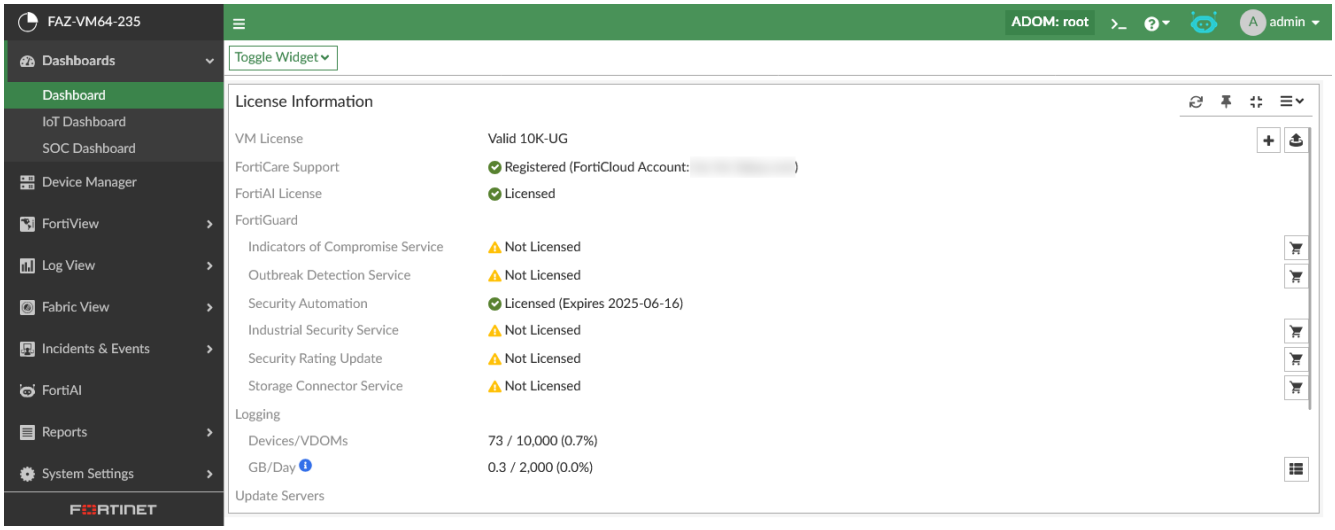
FortiAI is a generative AI security assistant that uses FortiGuard lab's high-fidelity security data and is continuously monitored and improved by FortiGuard Security experts. Administrators can use the FortiAI Assistant to answer questions and get help with configurations using FortiAI's advanced natural language processing capabilities.

FortiAI can be used in FortiAnalyzer for incident investigation, response, and threat hunting. The assistant can interpret security events, generate detailed summaries, identify potential impacts, and make remediation recommendations. FortiAI can also simplify platform usage with natural language prompts. For example, the assistant can create complex database queries, generate reports, write event handler and correlation rules, and execute many other FortiAnalyzer functions during typical workflow. For more information, see Using FortiAI on page 403.

FortiAI can be accessed from the following areas in the FortiAnalyzer GUI:

- The FortiAI icon in the banner from any page in the GUI.
- The FortiAI module in the FortiAnalyzer tree menu.

In order to use FortiAI, FortiAnalyzer must have a valid FortiAI license. FortiAI license information can be viewed in *Dashboards* > *Status* in the *License Information* widget. See the FortiAnalyzer Datasheet and FortiAI tokens on page 409 for more information about licensing.



In a FortiAnalyzer Fabric, you cannot use FortiAI on the FortiAnalyzer Fabric supervisor.

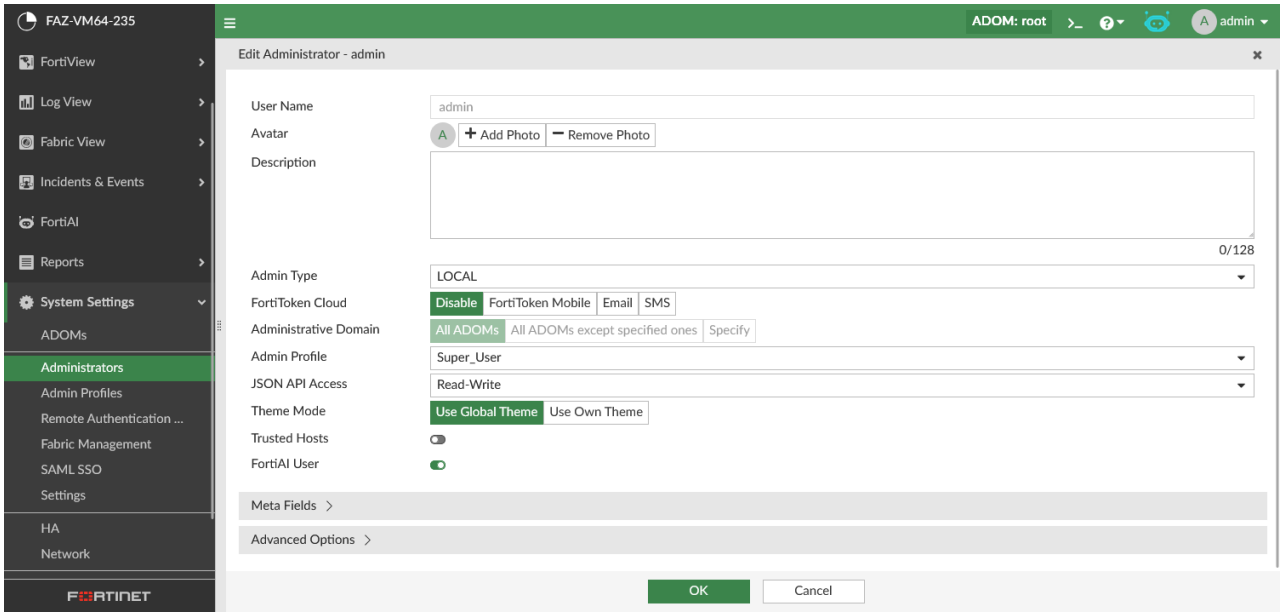
When licensed, FortiAI can be accessed by up to a maximum of three local administrators on the FortiAnalyzer. You can configure which administrators can use the FortiAI service using the FortiAnalyzer CLI. See Enabling administrator access to FortiAI on page 403.

Enabling administrator access to FortiAI

You can enable administrator access to FortiAI using the GUI or the CLI. FortiAI capabilities can only be enabled for local administrators.

To enable administrator access to FortiAI:

1. Ensure that you have a valid license for FortiAI.
2. Go to *System Settings* > *Administrators* and create or edit a local administrator.
3. Set the *FortiAI User* field to the *ON* position, and click *OK* to save the changes.



When attempting to enable FortiAI access on more than three administrators or on a non-local user, an error message is displayed.

To configure administrator access to FortiAI in the CLI:

1. In the FortiAnalyzer CLI, use the following commands to enable or disable this feature for an admin:

```
config system admin user
   edit <administrator>
      set fortiai {disable | enable}
```

Using FortiAI

The FortiAI assistant can be used to navigate the GUI and perform actions. It can also be used to answer questions and query data.

The FortiAI assistant is operated using prompts. You can use natural language to request actions or information from the FortiAI assistant. If you enter a prompt that the FortiAI assistant does not understand, it will ask for more details to clarify your request. Responses from the FortiAI assistant may also include suggestions and requests for you to consider. For example, after responding to a query for information, the FortiAI assistant may ask if you would like help performing a related action, such as filtering log view or creating an event handler.

The FortiAI assistant's responses can include text, images, widgets, and data retrieved directly from your FortiAnalyzer environment.



If you log out, close, or reload your session, you will not be able to continue your current thread with the FortiAI assistant. For example, you will not be able to reference a chart created by the FortiAI assistant in the current thread after reloading.

The following information is available in this topic:

- FortiAI capabilities on page 404
- FortiAI uses by pane on page 405
- FortiAI prompts on page 406
- The FortiAI pane on page 407

FortiAI capabilities

Capabilities of FortiAI in FortiAnalyzer can be categorized into the following areas:

Category	Description
Incident detection	FortiAI can help to create event handlers and event handler rules for incident detection. The event handlers can be created automatically according to your prompts from any pane, and the rules are customized to your environment. FortiAI is capable of creating these event handlers using the SIEM database. For example, during log analysis, if you find a suspicious log and want to get informed of similar occurrences, you can send the following prompt to FortiAI: "Keep me updated with same log happening again." FortiAI will automatically help to create an event handler for this kind of log.
Incident investigation	FortiAI can help to gather relevant information from multiple places in the FortiAnalyzer GUI. In addition, FortiAI can provide the context for the information, such as the threat information and the affected assets. Using these queries, you can perform an interactive investigation with FortiAI by asking follow-up questions, refining queries for information, and exploring different aspects of the incident to discover correlations within a single thread.
Incident response	FortiAI is integrated with playbooks and connectors for incident response automation. FortiAI can also support with post-incident reviews and compliance by generating detailed incident reports.

Category	Description
	Using these queries, you can collect many details related to the incident, including targeted endpoint information, event details, critical incident information, and the impact explanations. This information can be used to determine the root cause of the security threat and to initiate response measures.
Visibility and insights	FortiAI can generate custom charts and reports from the available log data. You can specify data sources, parameters, and choose the visualization type through a guided process with FortiAI.

In addition to the categories above, FortiAI can also be used to support use of your FortiAnalyzer device by providing product knowledge and performance monitoring.

For product knowledge of FortiAnalyzer, FortiAI can respond to your prompts with smart summaries, including information about the product and instructions for use. For example, you can use the following prompts to gain insight:

- How can I setup an HA Cluster in the GUI or CLI?
- What is the asset and identity center?
- How can I create a read-only user with restricted permission in the GUI or CLI?

While FortiAI cannot currently perform any of these actions on your behalf (creating a HA cluster or a read-only user), it will provide summaries and instructions according to your requests.

For performance monitoring, FortiAI can provide a summary of the FortiAnalyzer device, including overall performance details, storage utilization, and significant bottlenecks observed. For example, you can use the following prompts to gain insight:

- How is my FAZ performing?
- What is the current performance status of FortiAnalyzer?

FortiAI uses by pane

The table below provides a brief summary of the actions that can be performed with FortiAI in select FortiAnalyzer panes:

Pane	Description
Device Manager	FortiAI currently cannot navigate to or perform actions in *Device Manager*. FortiAI can guide you through actions in *Device Manager*, if needed.
FortiView	FortiAI can navigate to some *FortiView* panes, such as *FortiView* > *Threats* > *Top Threats*. In these panes, FortiAI can apply filters and create event handlers based on the results. You can use FortiAI to analyze the logs in these panes as well. FortiAI can navigate to the following *FortiView* panes: Top Threats, Top Source, Top Destination, Top Country, Top Policy Hit, Top Applications, and Top Website Domains.

Pane	Description

Log View	FortiAI can navigate to *Log View* and apply filters. FortiAI can analyze the logs to provide insights, render charts to visualize the log data, and create reports based on the logs for further analysis. You can make follow-up queries to gain further insights about the filtered information, as needed. For example:
	• Initial prompt: Show me the top 5 threats identified from last 24 hours
	  • Follow-up 1: Can you tell me more about the first threats?
	  • Follow-up 2: Are there any users under this threat?
	  • Follow-up 3: What is the destination IP associated with this threat?
	FortiAI also supports incident response from the *Log View* pane. You can use FortiAI to view logs related to a specific event or incident, and you can take action with FortiAI to quarantine compromised endpoints.
	FortiAI can navigate to *Log View* > *Threat Hunting* and apply filters. In addition, FortiAI can provide an analysis of the related logs in this pane.

Fabric View	FortiAI currently cannot navigate to or perform actions in *Fabric View*. FortiAI can guide you through actions in *Fabric View*, if needed.
Incidents & Events	FortiAI can navigate to *Event Handlers* and create event handlers according to your prompts. Note that these event handlers can also be created when using FortiAI to filter *FortiView* and *Log View*. FortiAI can also navigate to *Event Monitor* and apply filters; FortiAI can create event handlers using these filters as well. FortiAI can navigate to *Incidents*. You can use FortiAI to provide a list of incidents, and to create and save incident reports. FortiAI can display an event summary from any pane in the GUI.
Reports	FortiAI currently cannot navigate to reports; however, you can use FortiAI to render charts from *Log View*. These charts can be saved for future reference or used to create event handlers.
System Settings	FortiAI currently cannot navigate to or perform actions in *System Settings*. FortiAI can guide you through actions in *System Settings*, if needed.

In addition to the actions described in the table above, FortiAI can also to perform certain actions in any pane. For example, FortiAI can perform the following actions from anywhere in the GUI:

- Perform security reputation checks on suspicious IPs, domains, and URLs.
- Gather system process information for investigation purposes.
- Provide analysis and recommendations for data filtered/gathered in a FortiAI thread.
- Create event handlers.

For examples of FortiAI being used in FortiAnalyzer, see FortiAI example tasks on page 413.

FortiAI prompts

When using FortiAI, your prompts should be directly related to the information the assistant is programmed to access, enabling efficient and effective data retrieval.

A valid prompt is a clear, well-defined question that the FortiAI assistant can easily interpret and process. It should be specific and relevant to the data or queries the FortiAI assistant is designed to handle. A valid prompt can be translated into precise SQL queries to retrieve accurate results.

Example of valid prompts:

- Can you provide a summary of the latest security incidents detected?
- Could you assist in identifying any anomalies in our network traffic?
- Is there any unusual behavior observed from specific user accounts we should investigate?
- Are there any known exploits or vulnerabilities that we need to remediate immediately?
- Is there any unusual outbound network traffic that could indicate data exfiltration?

An invalid prompt is one that cannot be easily interpreted or processed by the FortiAI assistant. This typically includes prompts that are ambiguous, lack sufficient detail, or are outside the scope of the FortiAI assistant's capabilities.

Example of invalid prompts:

- "How many attacks will I receive tomorrow based on past trends?"

  This prompt is asking for information that requires FortiAI to make assumptions. Instead, consider prompting for an analysis of the current trends, and then following up to determine possible next steps to mitigate attacks according to those trends.
- "Give me a report of PCI compliance for my infrastructure."

  This prompt is too vague and FortiAI will likely ask for clarification, requiring more tokens. Instead, consider making the initial prompt more specific by including the related logs, devices, and/or a timeline. For more suggested best practices regarding tokens, see FortiAI tokens on page 409.



The above examples use full sentences. However, in general, using more text means using more tokens. To more efficiently use tokens, keep your prompts concise.

For more information about tokens, see FortiAI tokens on page 409.

The FortiAI pane

The FortiAI assistant pane includes the following:

Section		Description
Toolbar		Click an icon to perform the related action or open the related dialog.
	Restart Thread	Restart the FortiAI chat thread.
	Download Chat History	Download the current chat thread in HTML or PNG format.
	Close	Close the FortiAI pane. This does not clear the current thread. You can continue the chat thread by re-opening the FortiAI assistant in the same session.
Thread		Displays your prompts and the FortiAI assistant's responses for the current thread. At the bottom of responses from the FortiAI assistant, click the help icon to display the function callback results.

Section	Description
Prompt	Enter a prompt for the FortiAI assistant, and then click send. Alternatively, you can click the microphone icon to speak a prompt for the FortiAI assistant. When available, suggested prompts display above the text box. You can click these suggestions to prompt the FortiAI assistant.
Monthly token usage	Displays the percentage of monthly tokens used for the current month. For more information, see FortiAI tokens on page 409.

FortiAI data privacy

FortiAnalyzer and FortiAI protects your data using a multi-layered approach of function callbacks, data masking, and a secure proxy.

Function Callback: Your prompts are sent to the large language model (LLM), which generates a query that FortiAnalyzer can understand. This query is then executed on your local host, ensuring that results are processed locally.

Data Masking: Sensitive information such as IP addresses, MAC addresses, and usernames are automatically masked before being sent to the LLM, as the model does not need this data to form the query. When the function call returns to the local host, the data is unmasked.

For example:

- Prompt from Admin: "Give me the statistics of malware activities detected today from endpoint **`192.168.50.20`**?"
- Masked data sent from FortiAnalyzer: "Give me the statistics of malware activities detected today from endpoint **`12.198.37.2`**?"

In this example, **`12.198.37.2`** is an auto-generated, irrelevant IP address based on the session cookie.

Note that different values are masked using different methods within FortiAnalyzer; for instance, IP addresses are masked differently than usernames. The masked values also depend on the session cookie, ensuring that every session uses a different key to mask and protect data.

FortiAI Proxy: All FortiAI prompts pass through the Fortinet FortiAI proxy before reaching the cloud, where additional checks are performed to ensure your data is protected.

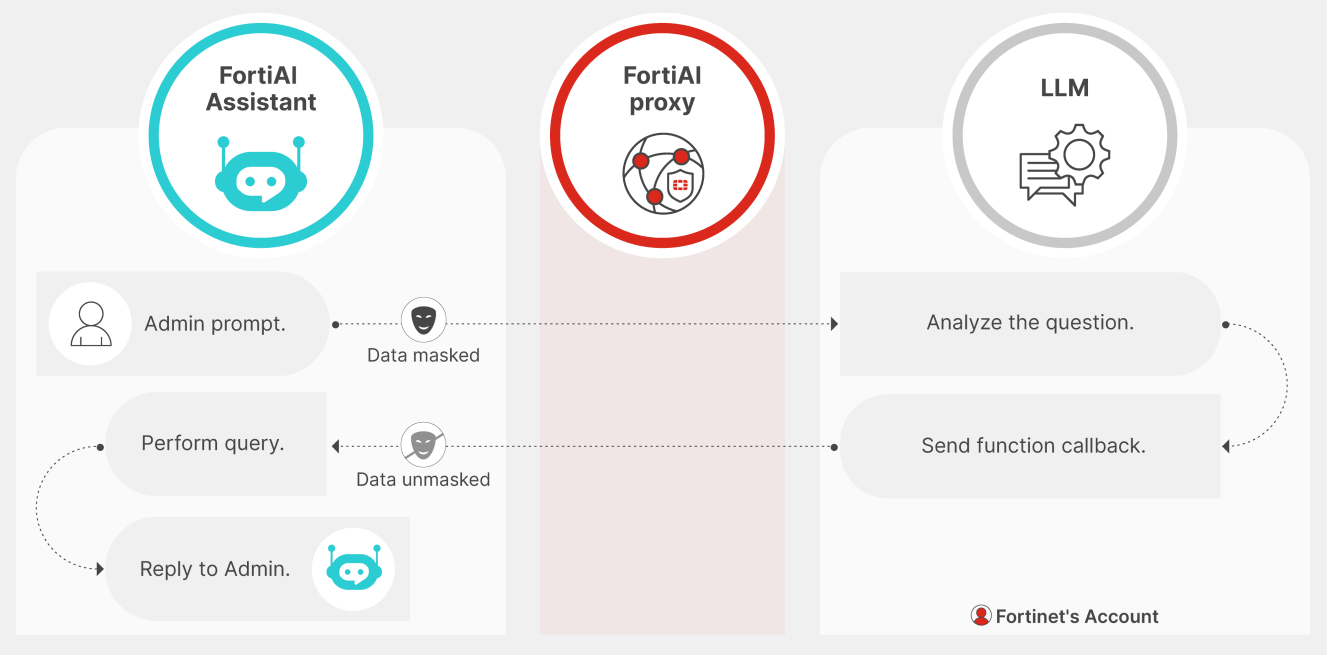
Example

1. The Admin enters a prompt in the FortiAnalyzer FortiAI Assistant.
   For example: "How much YouTube did 192.168.4.199 watch today?"
   The question is passed through the FortiAI proxy. Sensitive data, such as the IP, is automatically masked before it leaves FortiAnalyzer.
2. The LLM analyzes the question, determining the correct function to answer the prompt.
3. The LLM sends the function callback through the FortiAI proxy to FortiAnalyzer.
4. FortiAnalyzer unmasks the data and queries the database according to the function callback.
5. FortiAnalyzer replies to the Admin in the FortiAI Assistant.

For example:

"Here are today's statistics for IP 192.168.4.199 access to YouTube based on the logs:

- Log Count: 1803
- Percentage of Total: 99.83%
- Total Sent Bytes: 10.5 MB
- Average Session Duration: 00h 01m 52s



If there is further need to protect data from administrators, including the FortiAI users, you can also use the *Privacy Masking* feature in administrator profiles. This feature allows you to encrypt and anonymize data for administrators, further protecting user privacy according to your requirements. For more information, see Privacy Masking on page 568.

FortiAI tokens

When FortiAnalyzer is licensed for FortiAI, the license will include a monthly entitlement for tokens that is shared by all FortiAI users.

How token usage is calculated

Tokens are used in large language models (LLMs) to process text and quantify usage. Tokens usage is calculated using the following guidelines:

- When you use the FortiAI assistant, the text in both the prompt (input) and the response (output) is processed as tokens.

- While there is not a one-to-one relationship between words or characters and tokens, in general, more text in the query and response means using more tokens.
- Because the FortiAI assistant uses session history to inform it's responses, queries that are a part of a long session will use more tokens than new conversations.

Consider the following two queries:

- Can you show me all the log entries for the endpoint 10.10.10.10?
- Show logs for 10.10.10.10 (Past week).

The total amount of tokens used in the above examples is based on input (prompt) plus output (response). The first prompt uses more text, which means it will use more tokens in the input. The first prompt will also generate a larger response from FortiAI because it asks for "all log entries" rather than limiting the response to logs from the "Past week" only. Thus, the first prompt will use a greater number of tokens in the output as well.

For example, see below for a simple calculation of tokens used for each query. Note that the number of tokens are for the example, and do not reflect actual amounts to be used by these queries.

- Tokens used by first query = 20 (input) + 2000 (output)
- Tokens used by second query = 10 (input) + 1000 (output)

It would also be important to consider how long the thread is when these queries are made. The longer the thread gets, the more the number of tokens will be consumed.

Best practices

To ensure you are using your monthly allocation of tokens effectively, consider implementing best practices for FortiAI users. For example:

- Make your prompts concise and specific. In terms of token usage, the prompt "Can you show me all the log entries for endpoint 10.10.10.10 from the past week?" is less effective than "Show recent logs for 10.10.10.10 (Past week)" because the former prompt uses more text than the latter.
- Use filters in your prompts to receive concise and specific responses. For example, include time ranges or specify a limit for the number of results.
- Use words that relate to functions existing in FortiAnalyzer. For example, using "apply filter" or "generate report" concisely tells the FortiAI assistant what action is required.
- Leverage predefined datasets, charts, reports, and event handlers whenever possible. You can more efficiently use FortiAI by referencing existing tools in your prompts.
- Reference details in the existing thread when possible. This reduces redundancy and allows you to be concise and specific as you build upon previous prompts. However, note that the FortiAI assistant will not remember previous threads.
- Restart the AI assistant after 10 conversations if you don't need to keep the historical context.

Viewing token usage

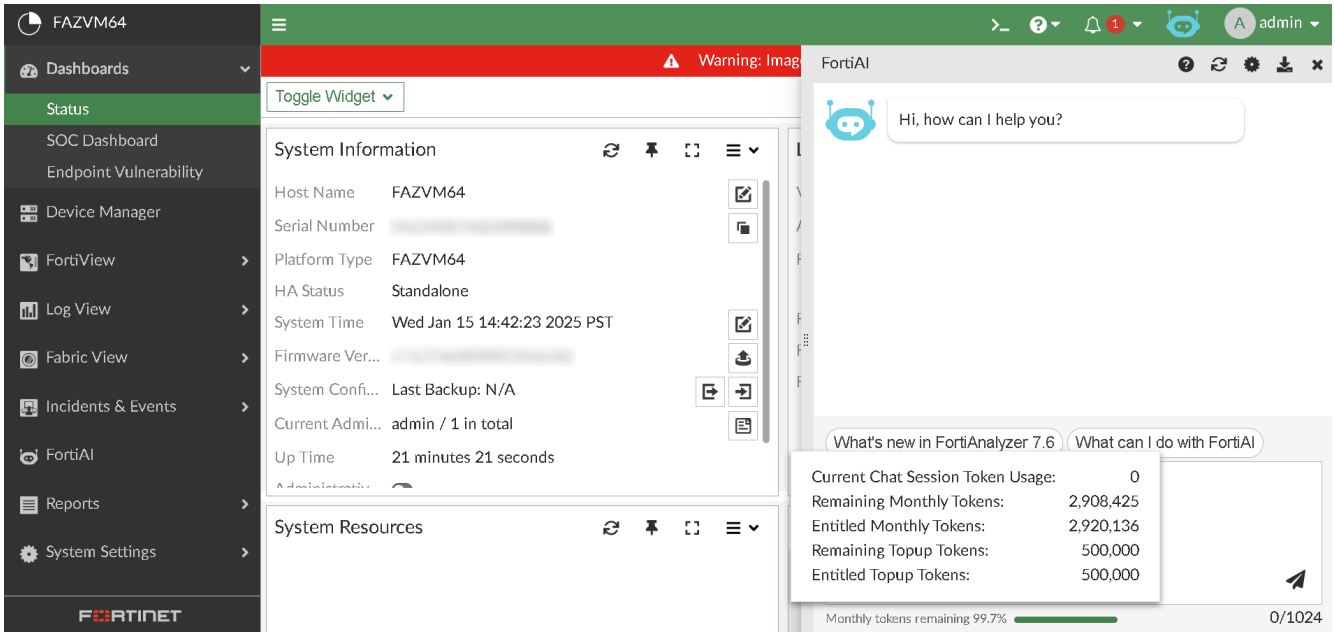
The monthly token usage is displayed at the bottom of the *FortiAI* pane in FortiAnalyzer. Mouse over the *Monthly tokens remaining* to view the following in a tooltip:

- *Current Chat Session Token Usage*
- *Remaining Monthly Tokens*

- *Entitled Monthly Tokens*

The following fields are also available in the tooltip when FortiAnalyzer has a FortiAI Token Top-up license:

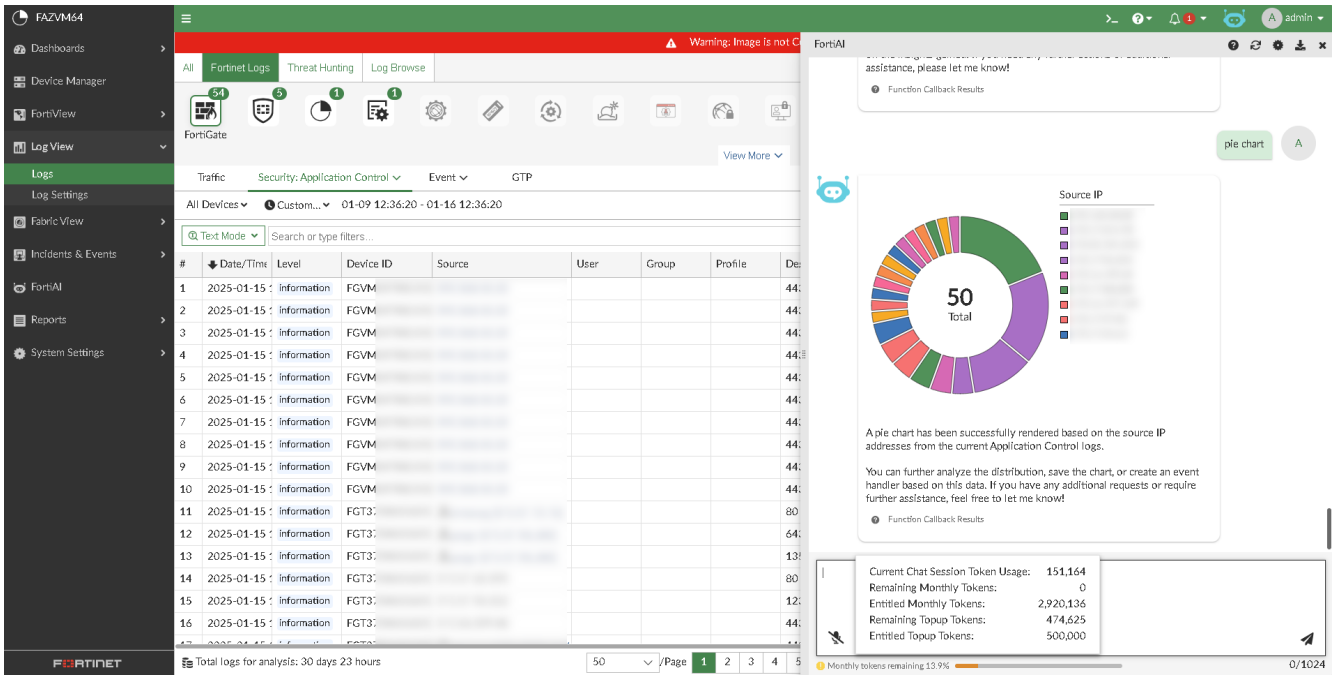
- *Remaining Topup Tokens*
- *Entitled Topup Tokens*



The monthly entitled tokens included with your FortiAI license varies by FortiAnalyzer platform. For additional tokens, you can purchase the FortiAI Token Top-up license. See Appendix D - FortiAI token entitlements for FortiAnalyzer on page 629.

You cannot add a FortiAI Token Top-Up license without already applying the FortiAI license to your FortiAnalyzer.

The top-up tokens will not be used when there are remaining monthly entitled tokens. Once the *Remaining Monthly Tokens* reaches `0`, the *Entitled Topup Tokens* will be used until the monthly entitlement resets.



You can confirm the FortiAI Token Top-up contract is applied using the following command in the CLI:

```
diagnose fmupdate dbcontract
```

The FortiAI Token Top-up contract and its expiration date is listed under `AITK` in the output. For example:

```
diagnose fmupdate dbcontract
FAZVMSTM******* [SERIAL_NO]
  AccountID: *****
  Industry:
  Company:   Fortinet Technologies (Canada) ULC.
  Contract:  11
        AISN-1-06-20260207
        AITK-1-06-20260207
        COMP-1-20-20260130
        ENHN-1-20-20260130
        FMWR-1-06-20260130
        FOAS-1-06-20260130
        FRVS-1-06-20260130
        PBDS-1-06-20260130
        SOAR-1-06-20260130
        SPRT-1-20-20260130
        VMLS-1-06-20260130
  Contract Raw Data:
        Contract=AISN-1-06-20260207:0:500:500:0*AITK-1-06-20260207:0:2:2:0*COMP-1-20-
20260130:0:1:1:0*ENHN-1-20-20260130:0:1:1:0*FMWR-1-06-20260130:0:1:1:0*FOAS-1-06-
20260130:0:1:1:0*FRVS-1-06-20260130:0:1:1:0*PBDS-1-06-20260130:0:1:1:0*SOAR-1-06-
20260130:0:1:1:0*SPRT-1-20-20260130:0:1:1:0*VMLS-1-06-
20260130:0:500:500:0|AccountID=*****|Company=Fortinet Technologies (Canada) ULC.|UserID=1272266
```

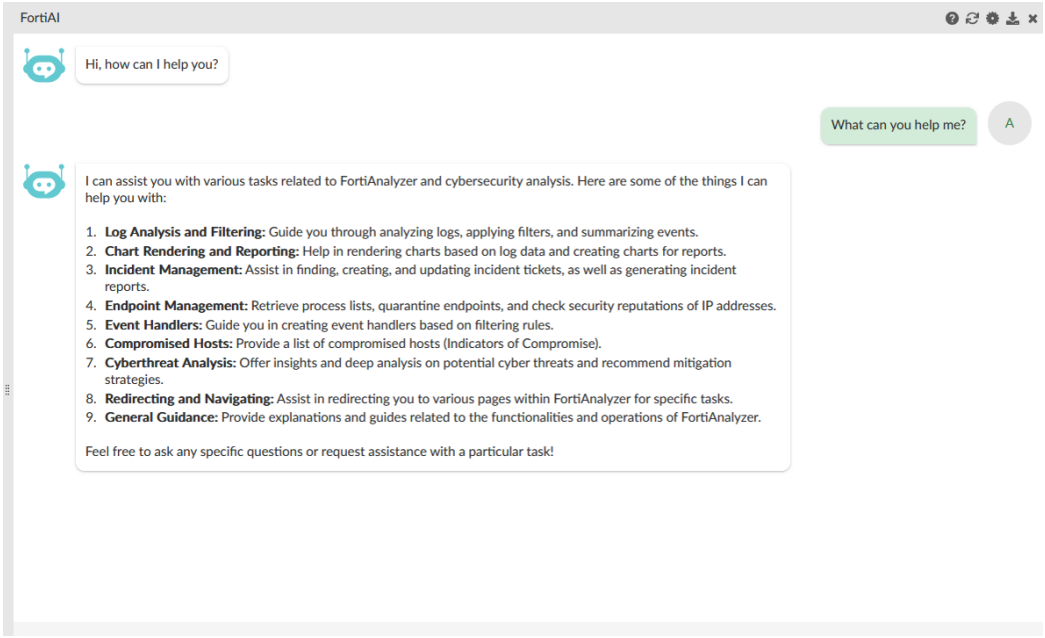
The FortiAI Token Top-up license is also visible in the *License Information* widget in *Dashboards* > *Status*. See License Information widget on page 63.

FortiAI example tasks

The following are examples using the FortiAI assistant in FortiAnalyzer.

- Example 1: Performing log analysis and filtering on page 413
- Example 2: Performing security reputation checks on page 416
- Example 3: Rendering charts on page 417
- Example 4: Creating an event handler on page 418
- Example 5: Identifying incidents and compromised hosts on page 420
- Example 6: Gathering system process information on page 421
- Example 7: Generating an incident report on page 424

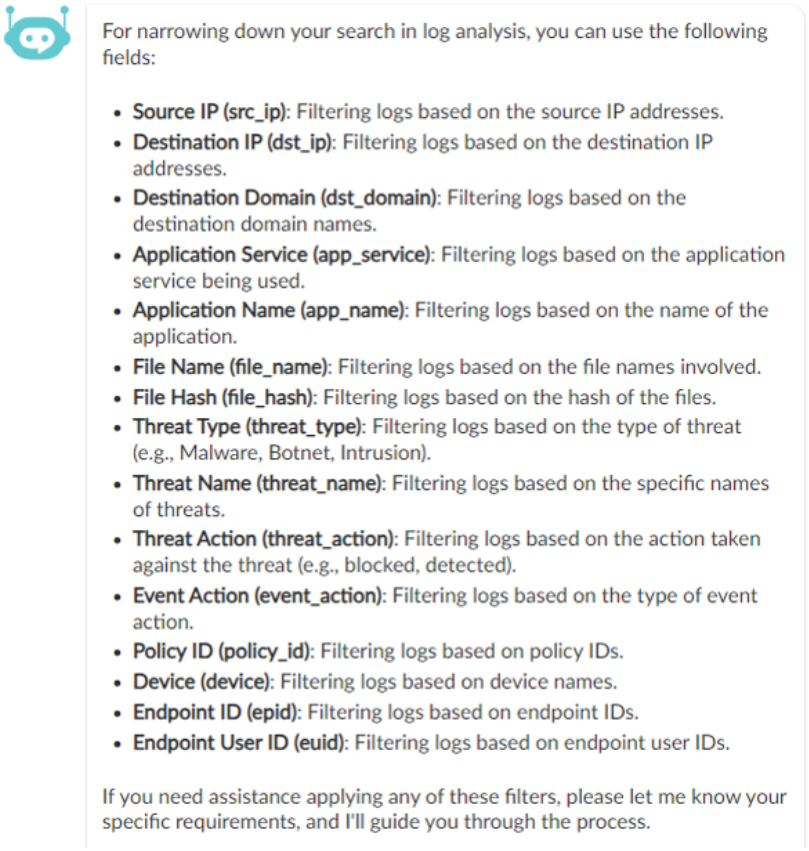
You can prompt FortiAI for suggestions and with questions when needed. For example, you can prompt FortiAI to list what tasks it can help with:



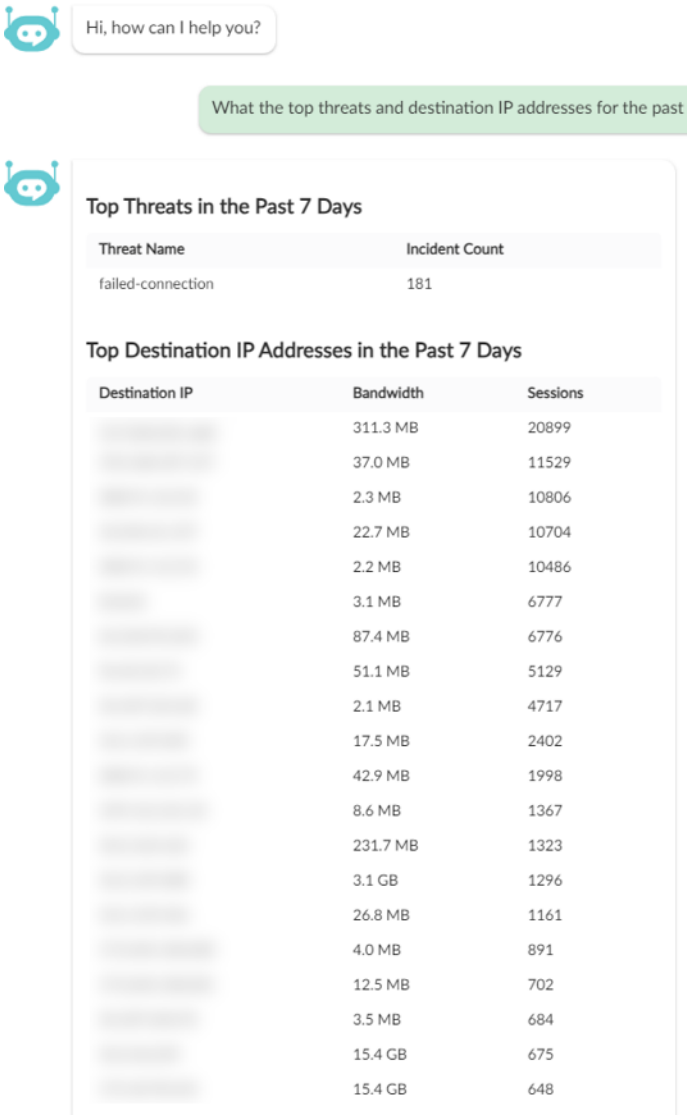
Example 1: Performing log analysis and filtering

FortiAI can guide you through analyzing logs and applying filters to refine your search. You can filter using specific criteria such as IP addresses, event actions, threat types, and more. You can also apply filters based on

time ranges.


For narrowing down your search in log analysis, you can use the following fields:
Source IP (src_ip): Filtering logs based on the source IP addresses.
Destination IP (dst_ip): Filtering logs based on the destination IP addresses.
Destination Domain (dst_domain): Filtering logs based on the destination domain names.
Application Service (app_service): Filtering logs based on the application service being used.
Application Name (app_name): Filtering logs based on the name of the application.
File Name (file_name): Filtering logs based on the file names involved.
File Hash (file_hash): Filtering logs based on the hash of the files.
Threat Type (threat_type): Filtering logs based on the type of threat (e.g., Malware, Botnet, Intrusion).
Threat Name (threat_name): Filtering logs based on the specific names of threats.
Threat Action (threat_action): Filtering logs based on the action taken against the threat (e.g., blocked, detected).
Event Action (event_action): Filtering logs based on the type of event action.
Policy ID (policy_id): Filtering logs based on policy IDs.
Device (device): Filtering logs based on device names.
Endpoint ID (epid): Filtering logs based on endpoint IDs.
Endpoint User ID (euid): Filtering logs based on endpoint user IDs.
If you need assistance applying any of these filters, please let me know your specific requirements, and I'll guide you through the process.

1. Prompt FortiAI to list the destination IP addresses for top threats in the past 7 days.



The FortiAI assistant responds with a list of the addresses, as well as a brief analysis and mitigation recommendations.

Professional Cybersecurity Concern

Given that "failed-connection" tops the threats, there might be legitimate reasons (e.g., network issues or misconfigurations) that caused these connection failures. However, high volumes of failed connections can also indicate scanning activities, potential attacks or attempts to communicate with blocked or filtered hosts, which should be further investigated.

Also, several of the destination IPs have high session counts and bandwidth usage. This could indicate normal operation, but also could be related to data exfiltration or other malicious activities if combined with suspicious behavior.

Mitigation Recommendations

1. **Further Investigation of Failed Connections**: Determine the root cause of the high number of failed connections.
2. **IP Traffic Monitoring**: Continuously monitor the high-traffic destination IPs for unusual activity.
3. **Enhance Logging and Alerting**: Set up event handlers and logging to alert on abnormal activities for these IPs.
4. **Security Controls**: Consider quarantining suspicious IPs and strengthening firewall rules.

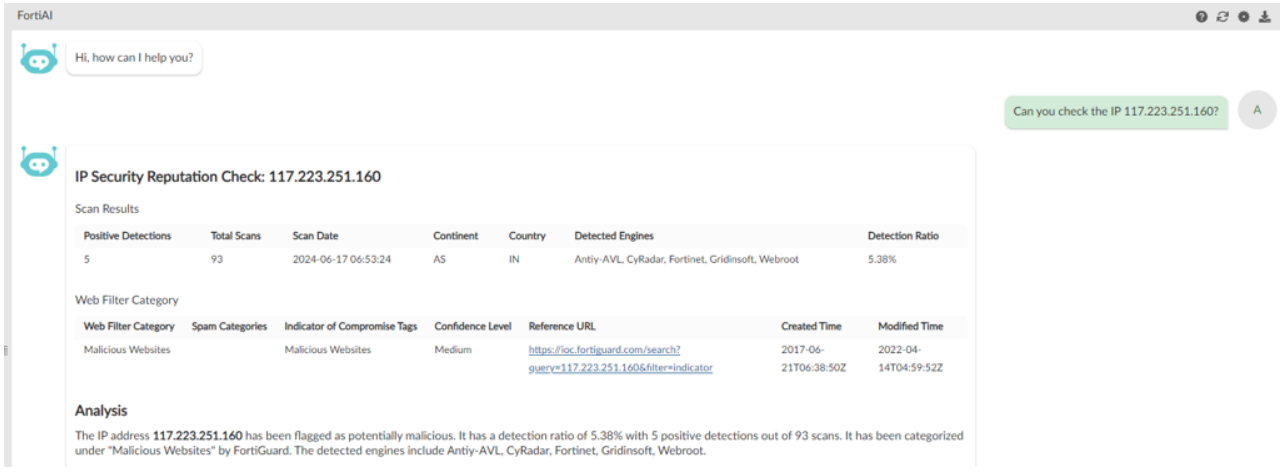
If you need further assistance, I can help you create event handlers or take a closer look at specific logs.

Function Callback Results

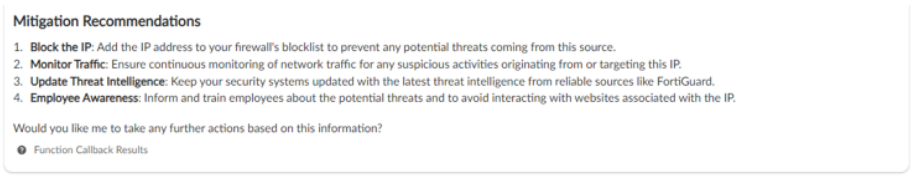
Example 2: Performing security reputation checks

FortiAI can investigate external IP addresses for their security reputation using FortiGuard and VirusTotal.

1. Prompt FortiAI to perform a security reputation check for an IP address.

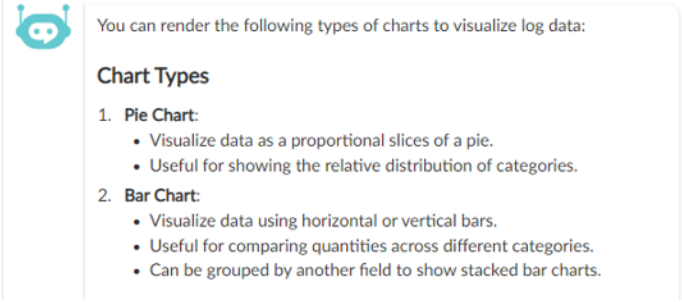


2. If it is not provided in the initial response, you can then prompt FortiAI to provide mitigation recommendations.

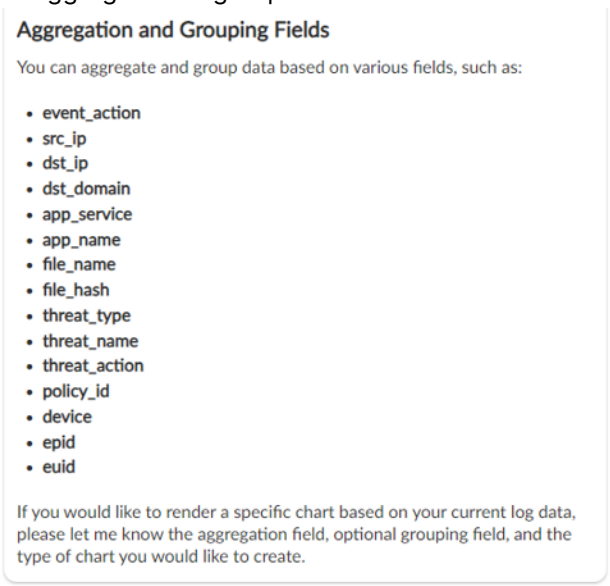


Example 3: Rendering charts

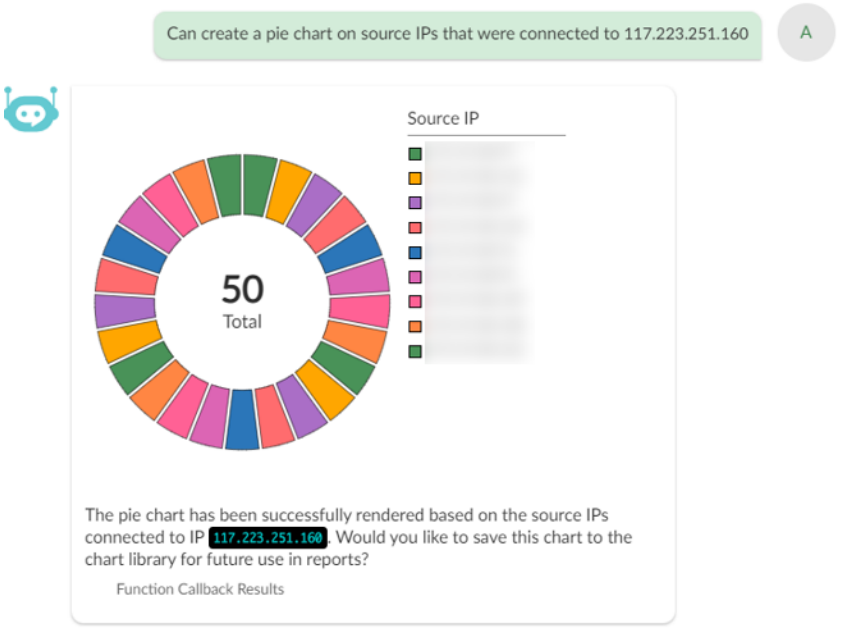
FortiAI can render charts to create visual representations of the log data. This can be done using pie charts or bar charts.



You can aggregate and group data in these charts based on various fields in FortiAnalyzer. For example:

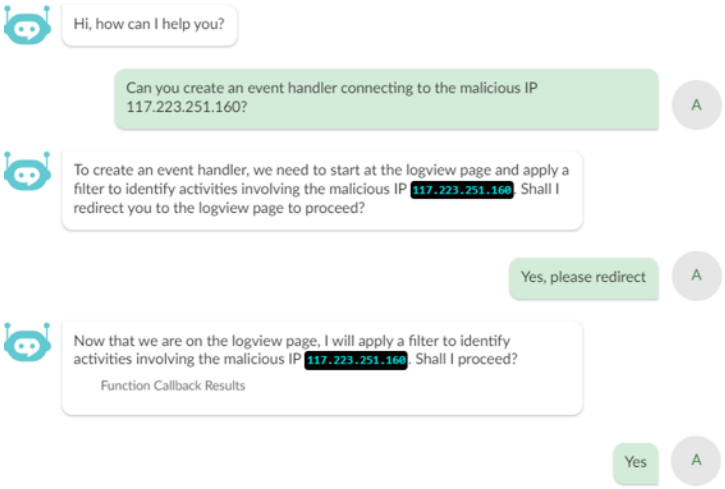


1. Prompt FortiAI to generate a pie chart based on source IPs that were connected to the malicious IP identified above.

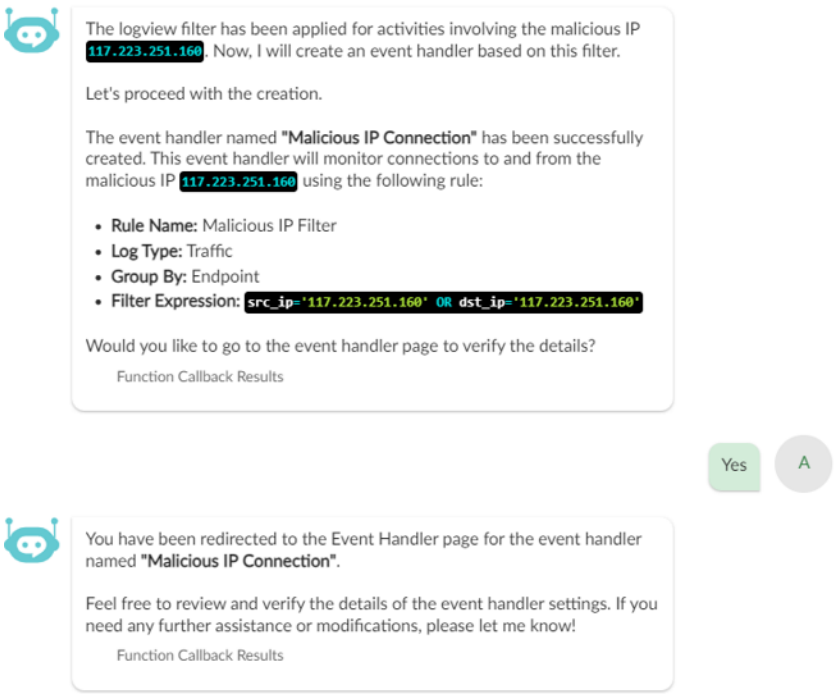


Example 4: Creating an event handler

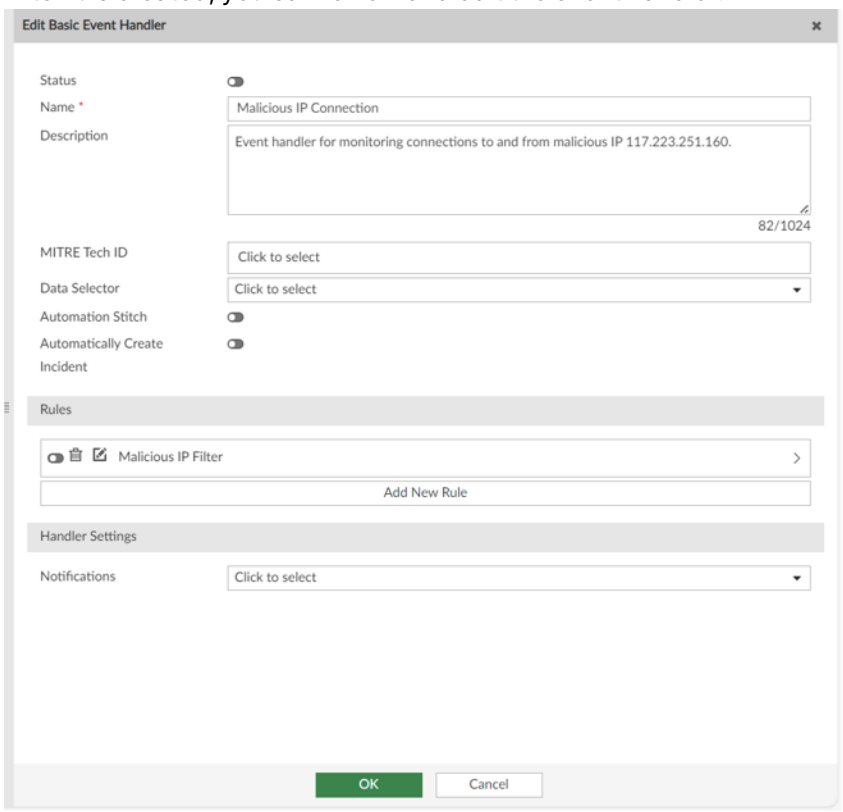
1. Prompt FortiAI to create an event handler connecting to the malicious IP identified above.
   Prompt FortiAI to continue with the task, as needed.



   When the FortiAI assistant creates the event handler, it provides the event handler name and a summary of the rule configuration.



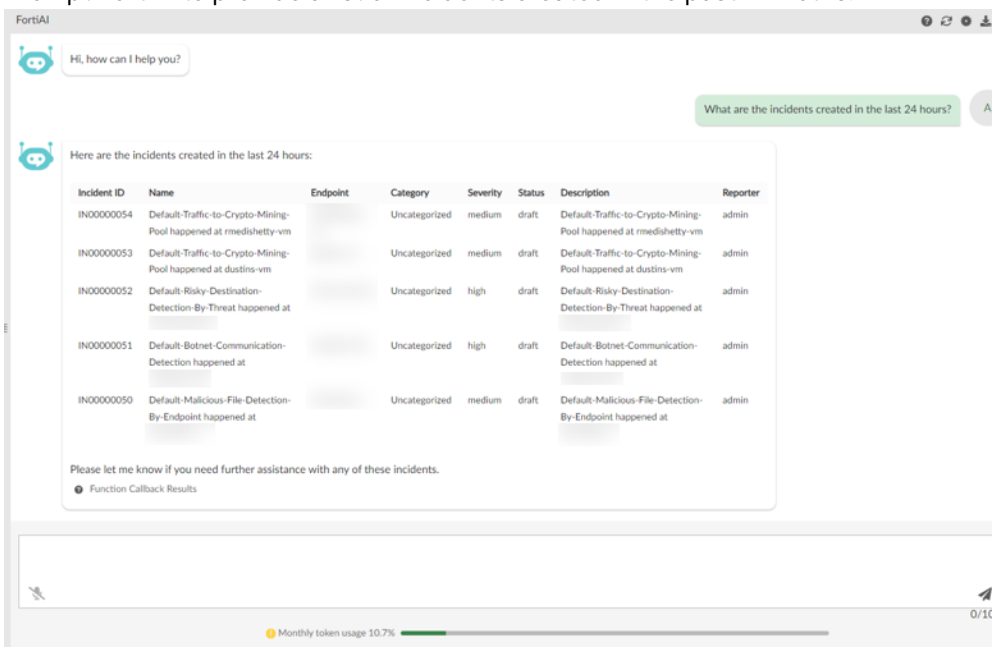
2. After it is created, you can review and edit the event handler.



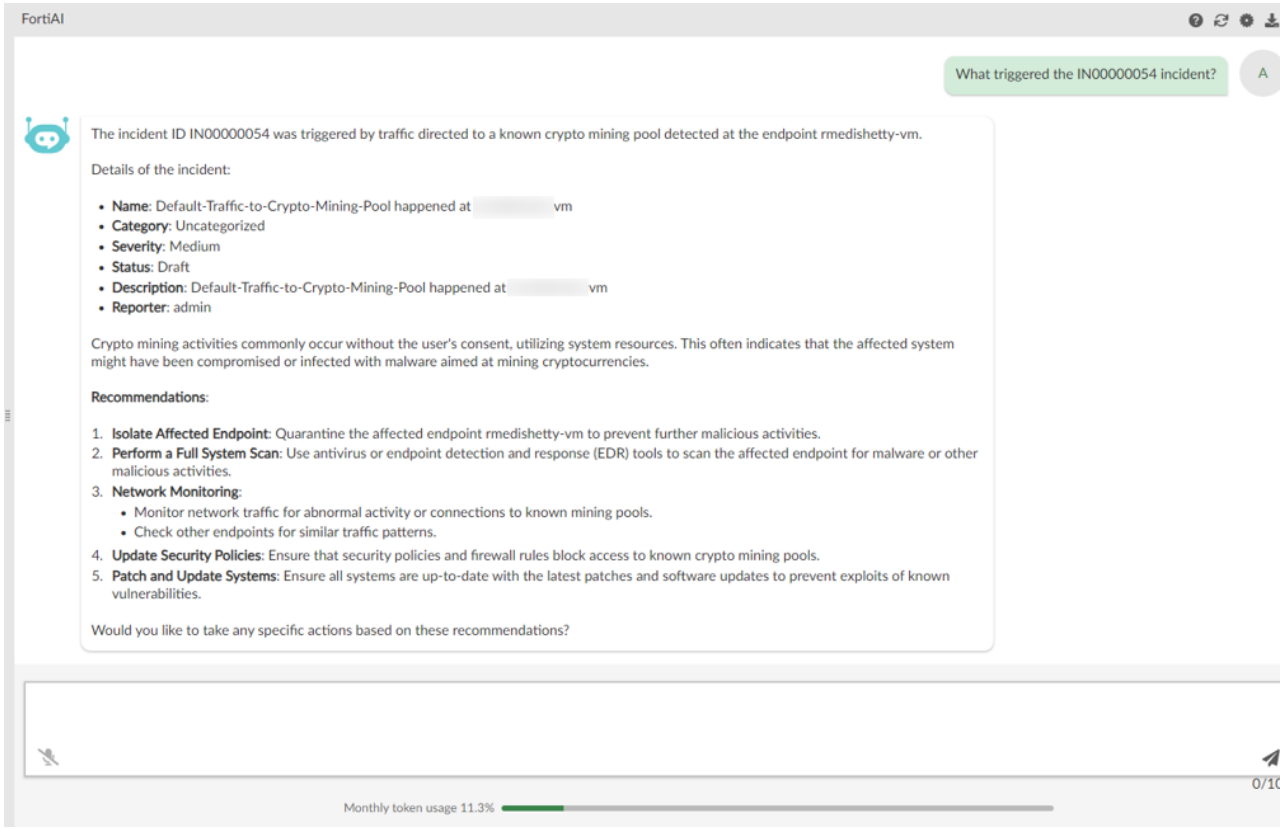
Example 5: Identifying incidents and compromised hosts

FortiAI can create, update, and track incidents, including generating reports and adding notes to existing incidents. FortiAI can also identify the compromised hosts.

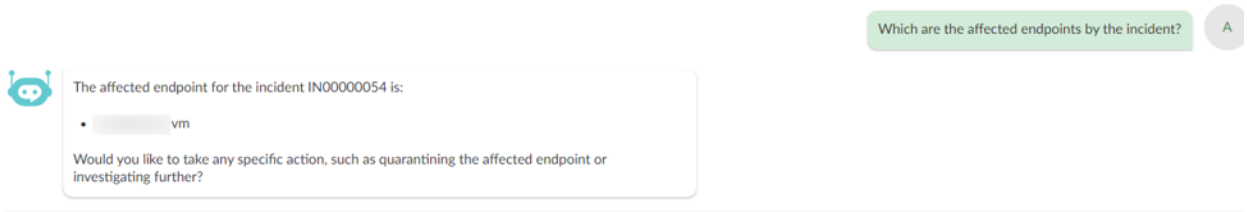
1. Prompt FortiAI to provide a list of incidents created in the past 24 hours.



2. Prompt FortiAI to provide more details about a specific incident in the list.



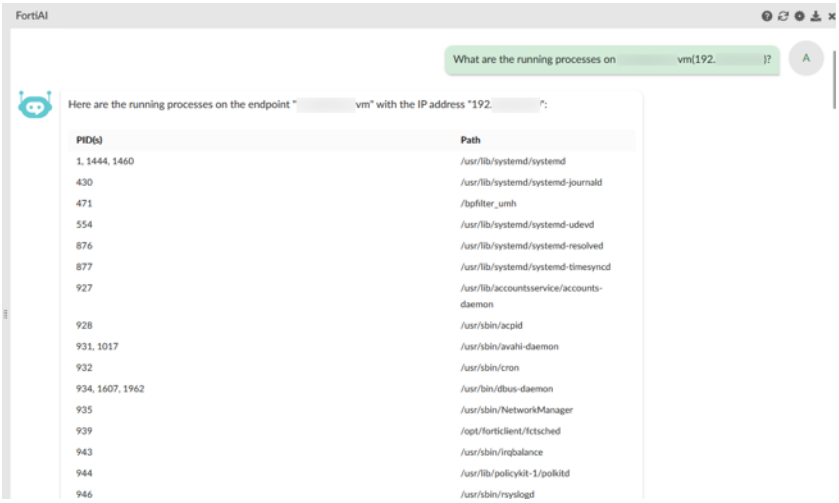
3. Prompt FortiAI to list the affected endpoints for the incident.



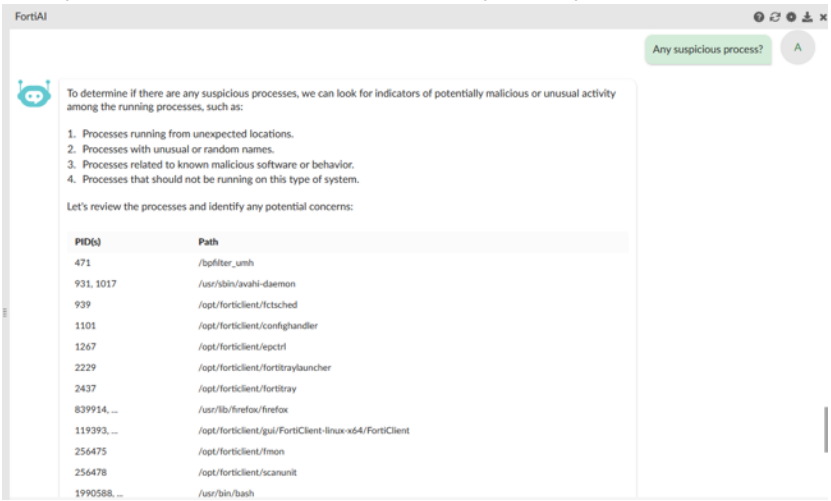
Example 6: Gathering system process information

FortiAI can get a list of running processes on the server for investigation purposes. As in the example below, you can prompt FortiAI to help with the analysis.

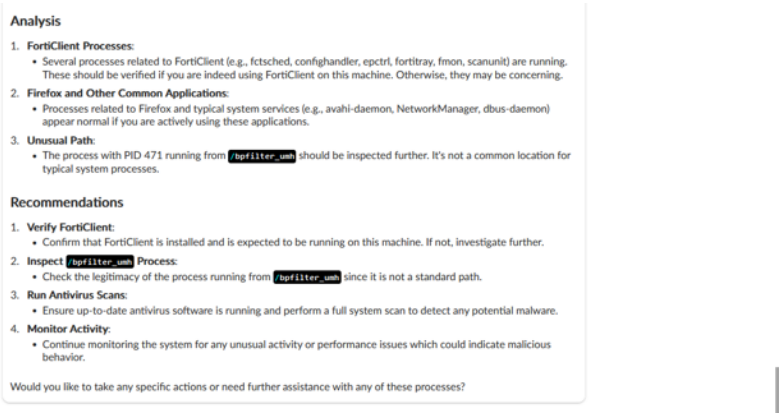
1. Prompt FortiAI for the running processes on a specific endpoint.



2. Prompt FortiAI to review the list for a suspicious process.



3. If the analysis is not included in the previous response, prompt FortiAI for a analysis of the suspicious process(es).



Example 6: Quarantining an endpoint

FortiAI can help prevent and mitigate threats by quarantining endpoints using IP addresses.

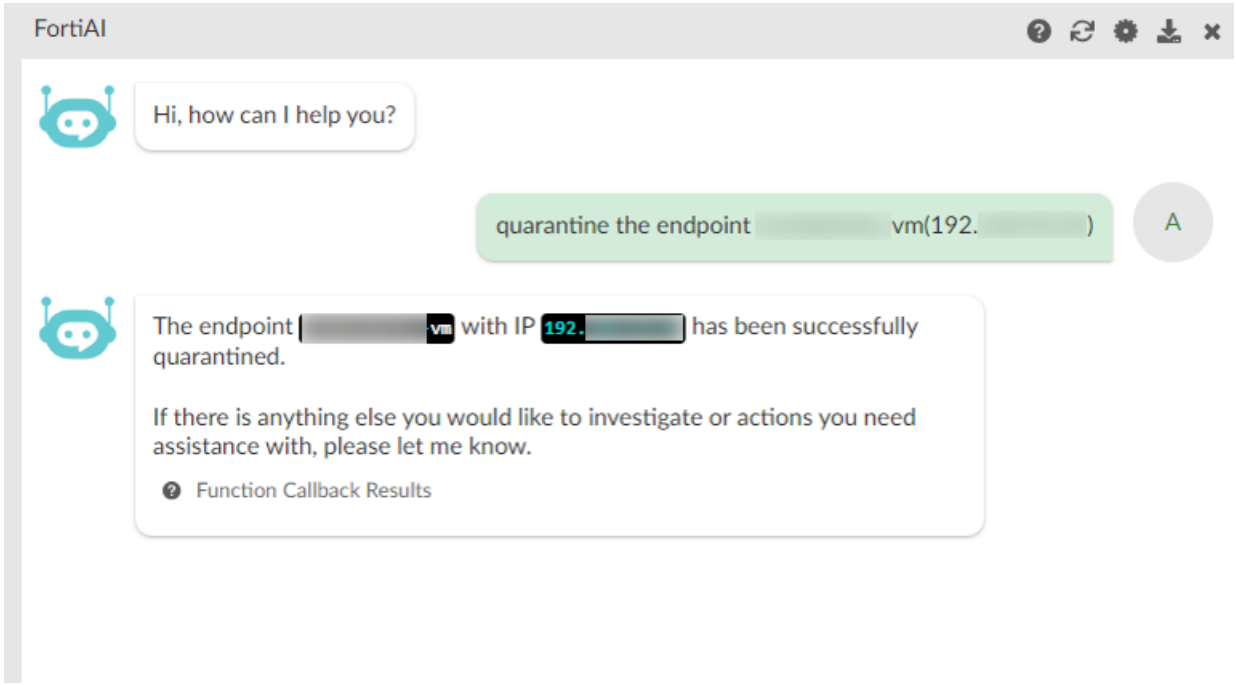
To execute quarantine actions on an endpoint, you can use the `action_quarantine_endpoint` function. Here's what it requires:

- **IP Address**: The IP address of the endpoint that you wish to quarantine.

Upon specifying the IP address of the suspicious or compromised endpoint, FortiAI will isolate this endpoint from the network, reducing the risk of further malicious activity.

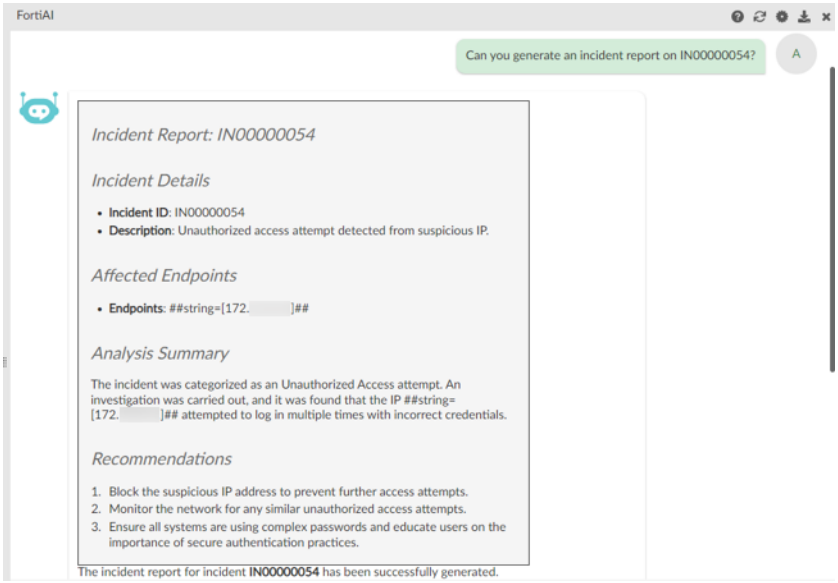
If you need assistance with quarantining a specific endpoint, please provide the IP address of the endpoint you wish to quarantine.

1. Prompt FortiAI to quarantine an endpoint using the IP address.

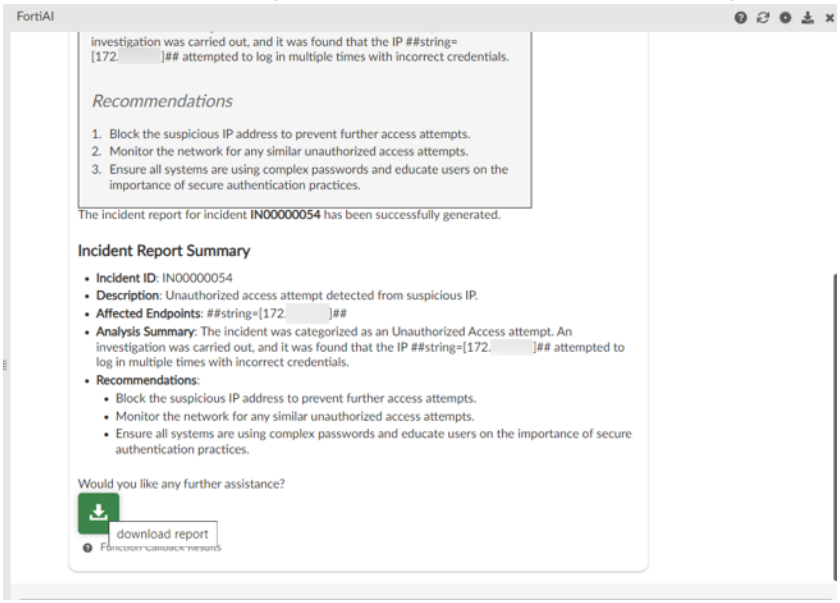


Example 7: Generating an incident report

1. Prompt FortiAI to produce an incident report for a specific incident number.



2. To save the incident report, click the download icon in the response.



Reports

You can generate data reports from logs by using the *Reports* feature. You can do the following:

- Use predefined reports. Predefined report templates, charts, and macros are available to help you create new reports.
- Create custom reports.

Report files are stored in the reserved space for the FortiAnalyzer device. See Automatic deletion on page 172.

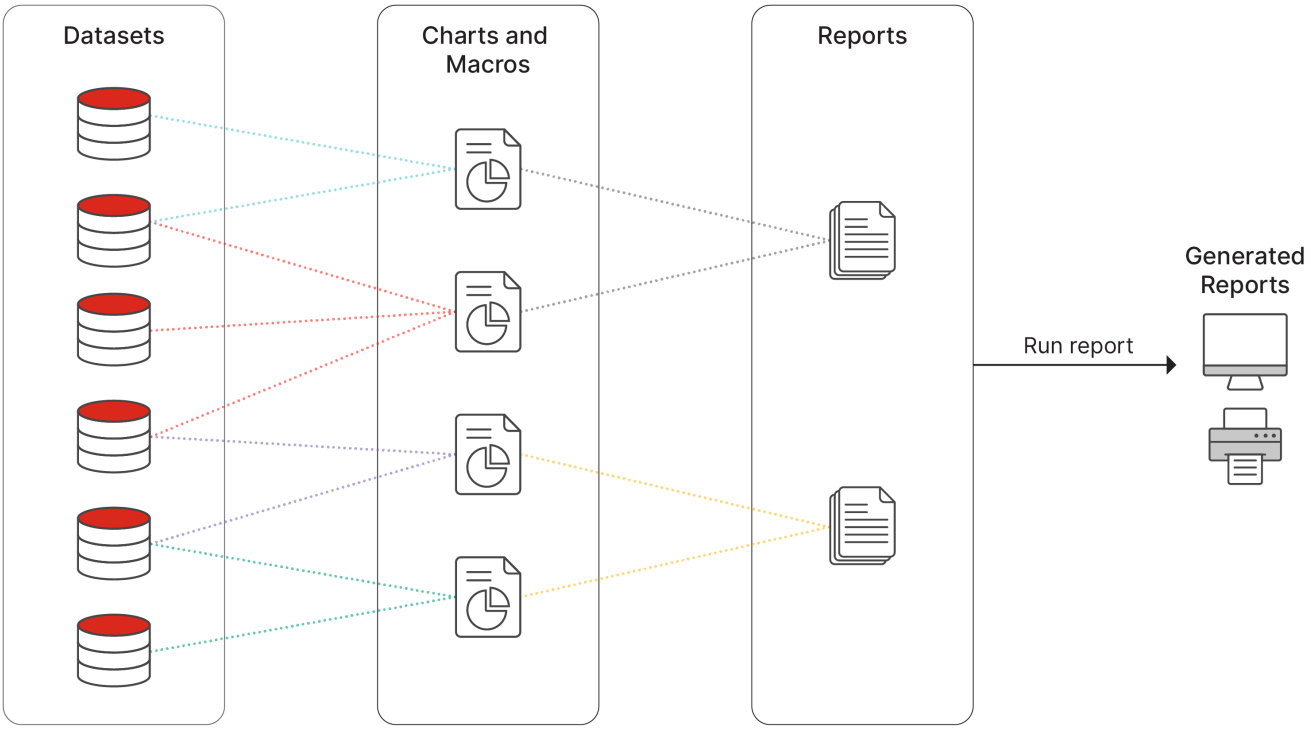


When rebuilding the SQL database, *Reports* are not available until the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

For more information on FortiAnalyzer report technology and troubleshooting report performance issues, see the *FortiAnalyzer Report Performance Troubleshooting Guide*.

How reports are populated

Reports are generated using logs and data stored in FortiAnalyzer. The type of logs used in the report are determined by datasets configured in FortiAnalyzer. These datasets are included in charts and macros, which are then added to reports alongside cover pages, images, and text to explain content for the user. When the report is run, the report is generated according to the available analytics logs and other relevant data in FortiAnalyzer. For more information about the logs used in reports, see Logs used for reports on page 428.



As demonstrated in the image above, reports rely on the following objects configured in FortiAnalyzer:

- **Datasets**: Determine the log type or data source tables to query from the database. For example, a dataset that queries FortiGate logs for botnet events.
- **Charts**: Reference a dataset to visualize queried data in a selected chart type, such as table, bar chart, pie chart, line chart, and more. For example, a line chart that displays number of botnet events over time.
- **Macros**: Reference a dataset to include queried data as text, bandwidth, counter, duration, or a percentage. For example, a macro that displays the total number of botnet events.

When a report is run, the generated report is populated using the charts and macros configured in the report. The data is included according to the datasets referenced in the charts and macros. You can use the *Report Guidance* feature to make sure the appropriate analytics logs are available for the report. This feature can help you to troubleshoot the report when it shows `No Data`, or to confirm you have the required logs after creating a custom report. For more information, see Report guidance on page 429.

There are many predefined datasets, charts, and macros used in predefined reports and report templates. If the data (logs) are available, you can generate these predefined reports. You can also clone and customize these predefined reports to alter them according to your unique needs. Alternatively, you can create reports from scratch using custom or predefined datasets, charts, and macros.

If you are using ADOMs, it is important to remember that each ADOM has its own reports, datasets, charts, and macros. For example, ADOMs can only support importing datasets that use the device types supported by that ADOM. Fabric ADOMs, however, can support all reports, regardless of the device type used in the datasets. Fabric ADOMs also support datasets that use the SIEM database (siemdb) to generate the report. Make sure you are in the correct ADOM before creating, editing, or generating a report. For more information, see How ADOMs affect reports on page 427.

When you generate a report, it can take days to assemble the required dataset and produce the report, depending on the required datasets. Instead of assembling datasets at the time of report generation, you can

enable the auto-cache feature to assemble the report with the help of an "hcache". This can reduce report generation time significantly. For more information, see How auto-cache works on page 429.

How ADOMs affect reports

When ADOMs are enabled, each ADOM has its own reports, libraries, and advanced settings. Make sure you are in the correct ADOM before selecting a report. See Switching between ADOMs on page 34.

Some reports are available only when ADOMs are enabled. For example, ADOMs must be enabled to access FortiCarrier, FortiCache, FortiClient, FortiDDoS, FortiMail, FortiSandbox, and FortiWeb reports. In a Security Fabric ADOM, all reports are displayed.

You cannot import reports to ADOMs that do not match the device type used in the charts and datasets for the report. Fabric ADOMs support all reports, regardless of the device type used in the charts and datasets. For example, a FortiGate report cannot be imported to an ADOM for a different device type; it can only be imported to a FortiGate or Fabric ADOM.

You can configure and generate reports for these devices within their respective default ADOM or a Security Fabric ADOM. These devices also have device-specific charts and datasets.

ADOM limits for reports

The following table identifies FortiAnalyzer ADOM limits for reports.

Report object	Per ADOM limit
Chart	5000
Dataset	5000
Macro	5000
Layout	2000
Schedule	2000
Layout-folder	100
Output	2000

Predefined reports, templates, charts, and macros

FortiAnalyzer includes a number of predefined elements you can use to create and/or build reports.

Predefined...	GUI Location	Purpose
Reports	*Reports* > *Report Definitions* > *All Reports*	You can generate reports directly or with minimum setting configurations. Predefined reports are actually report templates with basic default setting configurations.
Templates	*Reports* > *Report Definitions* > *Templates*	You can use directly or build upon. Report templates include charts and/or macros and specify the layout of the report. A template populates the *Layout* tab of a report that is to be created. See List of report templates on page 449.
Charts	*Reports* > *Report Definitions* > *Chart Library*	You can use directly or build upon a report template you are creating, or in the *Layout* tab of a report that you are creating. Charts specify what data to extract from logs.
Macros	*Reports* > *Report Definitions* > *Macro Library*	You can use directly or build upon a report template that you are creating, or in the *Layout* tab of a report that you are creating. Macros specify what data to extract from logs.

Logs used for reports

Reports uses Analytics logs to generate reports. Archive logs are not used to generate reports. For more information, see Data policy and automatic deletion on page 47.

For reports about users, the FortiGate needs to populate the `user` field in the logs sent to FortiAnalyzer.

Reports can use the SIEM database (siemdb) to generate reports. Logs in the siemdb are parsed and normalized by predefined log parsers in Fabric ADOMs. This allows the reports to include more information from third-party products and Fortinet products. For example, the data query for the *Endpoint Security Vulnerability Report* is based on the siemdb, and it uses SIEM normalized logs and the fct_mdata. For more information about log parsers, see SIEM log parsers on page 397.

You can use the *Report Guidance* feature to make sure the appropriate Analytics logs are available for a custom or predefined report. For more information, see Report guidance on page 429.

The logs used to generate reports is determined by the chart, datasets, and macros. These can be found in the following panes:

- *Reports* > *Report Definitions* > *Chart Library*
- *Reports* > *Report Definitions* > *Macro Library*
- *Reports* > *Report Definitions* > *Datasets*

How charts and macros extract data from logs

Reports include charts and/or macros. Each chart and macro is associated with a dataset. When you generate a report, the dataset associated with each chart and macro extracts data from the logs and populates the charts

and macros. Each chart requires a specific log type.

FortiAnalyzer includes a number of predefined charts and macros. You can also create custom charts and macros.

Report guidance

You can use the *Report Guidance* feature to determine if FortiAnalyzer has the appropriate Analytics logs available for a report.

If Analytics logs are not available for a chart or macro used in the report, it will display `No Data` in the report output. For example, the Analytics logs may not be available if;

- logging is not enabled correctly on the device,
- the log requires a FortiGuard license and you do not have one,
- or there are no matching logs at that time.

To use Report Guidance:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Click the icon in the *Config Recommendation* column for the report.
   The *Report Guidance* pane dispays for that report. The information in the *Report Guidance* pane is organized by `Item Title` (chart or macro name), `Device Type`, and `Log Type`. The pane indicates the relevant `Log Fields` and if the Analytics logs are available.
   See below for a partial example from *Report Guidance* for the 360-Degree Security Review report:

```
Item Title: 360 Degree Application Visibility and Control
Device Type: FortiGate
Log Type: app-ctrl
Log Fields: app, appcat
Analytics logs available: Yes
-----------------------------------------------------
Item Title: 360 Degree Threats Detection and Prevention
Device Type: FortiGate
Log Type: app-ctrl
Log Fields: app, appcat
Analytics logs available: Yes
----------------------------
Device Type: FortiGate
Log Type: attack
Log Fields: attack, severity
Analytics logs available: Yes
```

How auto-cache works

When you generate a report, it can take days to assemble the required dataset and produce the report, depending on the required datasets. Instead of assembling datasets at the time of report generation, you can enable the *auto-cache* feature for the report. *Auto-cache* is a setting that tells the system to automatically generate *hcache*.

hcache is a proprietary FortiAnalyzer caching system that stays on the disk in the form of a database table. Unlike other caches, *hcache* tables are persistent and are not removed based on a set period of time.

When a database table is rolled, it becomes "mature", meaning the table will not grow any more. Because the tables will not grow, it is unnecessary to query the database table each time for the same SQL query. *hcache* runs queries on these matured database tables in advance and caches the interim results of each query. When it is time to generate the report, much of the datasets are already assembled, and the system only needs to merge the results from *hcaches*. This reduces report generation time significantly.

The *auto-cache* process uses system resources to assemble and cache the datasets and it takes extra space to save the query results. You should only enable *auto-cache* for reports that require a long time to assemble datasets.

Generating reports

You can generate reports by using one of the predefined reports or by using a custom report that you created. You can find all the predefined reports and custom reports listed in *Reports > Report Definitions > All Reports*.



Click the icon in the *Config Recommendation* column to determine if the appropriate Analytics logs are available for the report. For more information, see Report guidance on page 429.

To generate a report:

1. Go to *Reports > Report Definitions > All Reports*.
2. In the content pane, select a report from the list.
3. (Optional) Click *Edit* in the toolbar and edit settings on the *Settings* and *Layout* tabs. For a description of the fields in the *Settings* and *Layout* tabs, see Reports Settings tab on page 435 and Creating charts on page 457 and Macro library on page 460.
4. In the toolbar, click *Run Report*.

Generated reports can be attached to incidents. See Adding reports to an incident on page 212.

Viewing completed reports

After you generate reports, you can view completed reports in *Reports > Generated Reports* or *Reports > Report Definitions > All Reports*. You can view reports in the following formats: HTML, PDF, XML, CSV, and JSON.

To view completed reports in Generated Reports:

1. Go to *Reports > Generated Reports*.
   This view shows all generated reports for the specified time period.
2. To sort the report list by date, click *Order by Time*.To sort the report list by report name, click *Order by Name*.

3. To stop showing status updates for reports as they are generating, click *Pause*.
   This prevents the table from changing while in the pane, if needed, so you can more easily select or view the reports.
   To resume the auto-update, click *Play*.
4. Locate the report and click the format in which you want to view the report to open the report in that format.

   For example, if you want to review the report in HTML format, click the *HTML* link.

To view completed reports in All Reports:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. On the report list, double-click a report to open it.
3. In the *View Report* tab, locate the report and click the format in which you want to view the report to open the report in that format.
   For example, if you want to review the report in HTML format, click the *HTML* link.

Enabling auto-cache

You can enable auto-cache to reduce report generation time for reports that require a long time to assemble datasets. For information about auto-cache and hcache, see How auto-cache works on page 429.

You can see the status of building the cache in *Reports* > *Report Definitions* > *All Reports* in the *Cache Status* column.

To enable auto-cache:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Select the report from the list, and click *Edit* in the toolbar.
3. In the *Settings* tab, select the *Enable Auto-cache* checkbox.
4. Click *Apply*.

Grouping reports

If you are running a large number of reports which are very similar, you can significantly improve report generation time by grouping the reports. Grouping reports has these advantages:

- Reduce the number of *hcache* tables.
- Improve *auto-hcache* completion time.
- Improve report completion time.

Step 1: Configure report grouping

For example, to group reports with titles containing string `Security_Report` by device ID and VDOM, enter the following CLI commands:

```
config system report group
   edit 0
      set adom root
      config group-by
         edit devid
         next
         edit vd
         next
   end
   set report-like Security_Report
   next
end
```

Notes:

- The `report-like` field specifies the string in report titles that is used for report grouping. This string is case-sensitive.
- The `group-by` value controls how cache tables are grouped.
- To view report grouping information, enter the following CLI command, then check the Report Group column of the table that is displayed.
  `execute sql-report list-schedule <ADOM>`

Step 2: Initiate a rebuild of hcache tables

To initiate a rebuild of hcache tables, enter the following CLI command:

```
diagnose sql hcache rebuild-report <start-time> <end-time>
```

Where `<start-time>` and `<end-time>` are in the format: `<yyyy-mm-dd hh:mm:ss>`.

Retrieving report diagnostic logs

Once you start to run a report, FortiAnalyzer creates a log about the report generation status and system performance. Use this diagnostic log to troubleshoot report performance issues. For example, if your report is very slow to generate, you can use this log to check system performance and see which charts take the longest time to generate.

For information on how to interpret the report diagnostic log and troubleshoot report performance issues, see the *FortiAnalyzer Report Performance Troubleshooting Guide*.

To retrieve report generation logs:

1. In *Reports* > *Generated Report*, right-click the report and select *Retrieve Diagnostic* to download the log to your computer.
2. Use a text editor to open the log.

Auto-Generated Reports

The *Daily Summary Report* is automatically generated. By default, this report will run daily at 3:00AM. You can update this schedule in the report settings for the *Daily Summary Report*. For more information, see Scheduling reports on page 433.

The complete schedule for report generation can be viewed in the *Report Calendar*. See Report calendar on page 473.



This will only affect newly installed FortiAnalyzers or newly created ADOMs. In upgraded FortiAnalyzers, the calendar will be kept as is.

Scheduling reports

You can configure a report to generate on a regular schedule. Schedules can be viewed in the *Report Calendar*. See Report calendar on page 473.

To schedule a report:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Select a report and click *Edit* in the toolbar.
3. Click *Settings* in the toolbar.
4. Select the *Enable Schedule* checkbox and configure the schedule.
5. Click *Apply*.

Creating reports

You can create reports from report templates, by cloning and editing predefined/existing reports, or start from scratch.

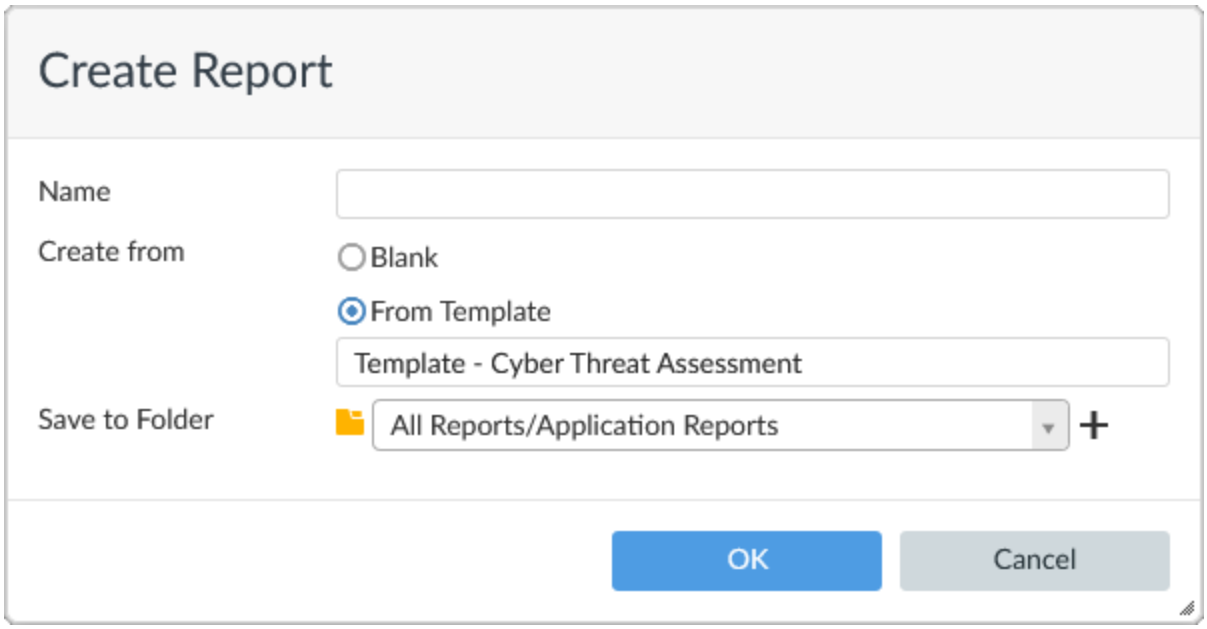
Creating reports from report templates

You can create a new report from a template. The template populates the *Layout* tab of the report. The template specifies what text, charts, and macros to use in the report and the layout of the content. Report templates do not contain any data. Data is added to the report when you generate the report.

To create a new report from a template:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.

3. In the toolbar, click *Report* > *Create New*. The *Create Report* dialog box opens.



4. In the *Name* box, type a name for the new report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % $ +
5. Select *From Template* for the *Create from* setting, then select a template from the dropdown list. The template populates the *Layout* tab of the report.
6. Select the folder that the new report will be saved to from the dropdown list. You can click the add button to include additional folder locations. See Organizing reports into folders on page 445
7. Select *OK* to create the new report.
8. On the *Settings* tab, configure the settings as required. For a description of the fields, see Reports Settings tab on page 435.
9. Optionally, go to the *Layout* tab to customize the report layout and content. For a description of the fields, see Reports Editor tab on page 440.
10. Click *Apply* to save your changes.

Creating reports by cloning and editing

You can create reports by cloning and editing predefined and/or existing reports.

To create a report by cloning and editing:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the content pane, select the report from the list, then click *Report* > *Clone* in the toolbar.
4. In the *Clone Report* dialog box, type a name for the cloned report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % $ +
5. Select the folder that the new report will be saved to from the dropdown list. See Organizing reports into folders on page 445
6. Select *OK* to create the new report.

7. On the *Settings* tab, configure the settings as required. For a description of the fields, see Reports Settings tab on page 435.
8. Optionally, go to the *Layout* tab to customize the report layout and content. For a description of the fields, see Reports Editor tab on page 440.
9. Click *Apply* to save your changes.

Creating reports without using a template

To create a report without using a template:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the toolbar, click *Report* > *Create New*. The *Create New Report* dialog box opens.
4. In the *Name* box, type a name for the new report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % $ +
5. Select the *Blank* option for the *Create from* setting.
6. Select the folder that the new report will be saved to from the dropdown list. You can click the add button to include additional folder locations. See Organizing reports into folders on page 445
7. Select *OK* to create the new report.
8. On the *Settings* tab, you can specify a time period for the report, what device logs to include in the report, and so on. You can also add filters to the report, add a cover page to the report, and so on. For a description of the fields, see Reports Settings tab on page 435.

   To create a custom cover page, you must select *Print Cover Page* in the *Advanced Settings* menu.

9. On the *Layout* tab, you can specify the charts and macros to include in the report, as well as report content and layout.
   For a description of the fields, see Reports Editor tab on page 440.
   For information about creating charts and macros, see Creating charts on page 457 and Creating macros on page 461.
10. Click *Apply* to save your changes.

Reports Settings tab

The following options are available in the *Settings* tab:

Field	Description
Name	The report name.
Time Zone	The time zone to use for data in the report. The *Default* time zone is the time zone set for the FortiAnalyzer. For more information, see Configuring the system time on page 53.

Field	Description
Time Period	The time period the report covers. Available report filter time periods include *Previous 7 Days*, *Previous 14 Days*, *Previous 30 Days*, *This Week*, *Previous Week*, *Previous 2 Weeks*, *Previous N Hours*, *Previous N Days*, *Previous N Weeks*, *This Month*, *Previous Month*, *This Quarter*, *Previous Quarter*, *This Year*, *Today*, *Yesterday*, and *Custom*. Select a time period or select *Custom* to manually specify the start and end date and time. The specific range of time included for your report is displayed below the selected *Time Period*.  *Previous* time period filters can include up to the *previous* days data at the latest, and do not include data from the current day. This ensures that data is not missed during report generation and that scheduled reports using these filters include a consistent time period.
Devices	The devices to include in the report. Select either *All Devices* or *Specify* to add specific devices. Select the add icon to select devices.
Subnets	Select *All Subnets* to include all subnets, or select *Specify* to include/exclude subnets as a filter for this report. See Subnets on page 191.
Type	Select either *Single Report (Group Report)* or *Multiple Reports (Per-Device)*. This option is only available if multiple devices are selected.
Enable Schedule	Select to enable report template schedules.
Enable Notification	Select to enable notifications to the selected output profile.
Output Profile	Select the output profile from the dropdown list, or click *Create New* to create a new output profile. See Output profiles on page 469.
Enable Auto-Cache	Select to assemble datasets before generating the report and as the data is available. This process uses system resources and is recommended only for reports that require days to assemble datasets. Disable this option for unused reports and for reports that require little time to assemble datasets.
Extended Log Filtering	Enable to cache the following log fields for faster filtering. • Device • Source IP • Destination IP • Endpoint ID • Source End User ID Use the *Additional Log Fields* dropdown to select additional log fields.
Generate PDF Report Every	Select when the report is generated. Enter a number for the frequency of the report based on the time period selected from the dropdown list.
Start time	Enter a starting date and time for the file generation.

Field	Description
End time	Enter an ending date and time for the file generation, or set it to never ending.

Filters section of Reports Settings tab

See Filtering report output on page 442.

Advanced Settings section of Reports Settings tab

The following options are available in the *Advanced Settings* section of the *Settings* tab.

Field	Description
Language	Select the report language.
Bundle rest into "Others"	Select to bundle the uncategorized results into an *Others* category.
Print Orientation	Set the print orientation to portrait or landscape.
Chart Heading Level	Set the heading level for the chart heading.
Default Font	Set the default font.
Hide # Column	Select to hide the column numbers.
Layout Header	Enter header text and select the header image. Accept the default Fortinet image or click *Browse* to select a different image.
Layout Footer	Select either the default footer or click *Custom* to enter custom footer text in the text field.
Print Cover Page	Select to print the report cover page. Click *Customize* to customize the cover page. See Customizing report cover pages on page 438.
Print Table of Contents	Select to include a table of contents.
Print Device List	Select to print the device list. Select *Compact*, *Count*, or *Detailed* from the dropdown list.
Display Device Name	Select to display devices *By Device Name* or *By Device ID*.
Print Report Filters	Select to print the filters applied to the report.
Obfuscate User	Select to hide user information in the report.
Resolve Hostname	Select to resolve hostnames in the report.
Date Format	Select the date format to display.
Allow save maximum	Select a value between 1-10000 for the maximum number of reports to save.

Field	Description
Color Code	The color used to identify the report on the calendar. Select a color code from the dropdown list to apply to the report schedule. Color options include: *Bold Blue*, *Blue*, *Turquoise*, *Green*, *Bold Green*, *Yellow*, *Orange*, *Red*, *Bold Red*, *Purple*, and *Gray*.
Report Owner	Select a report owner.
Enable Report Filter Caching	Select to accelerate processing speed when generating multiple reports. In this case, all filters are applied when querying the hcache table. This is the default. De-select to improve report accuracy. In this case, the filters are put inside the hcache to increase data accuracy. However, this will also impact performance.

Enable High Accuracy Caching	Select to increase the maximum hcache rows, increasing data accuracy.
	You can show, set, or reset the maximum number of rows for high-accuracy hcache by entering the following command in the FortiAnalyzer CLI:
	`diagnose sql config hcache-max-high-accu-row [reset | set <integer>]`
	De-select to use the default number of hcache rows, increasing system performance. This is the default.
	You can show, set, or reset the default number of hcache rows by entering the following command in the FortiAnalyzer CLI:
	`diagnose sql config hcache-max-rpt-row [reset | set <integer>]`

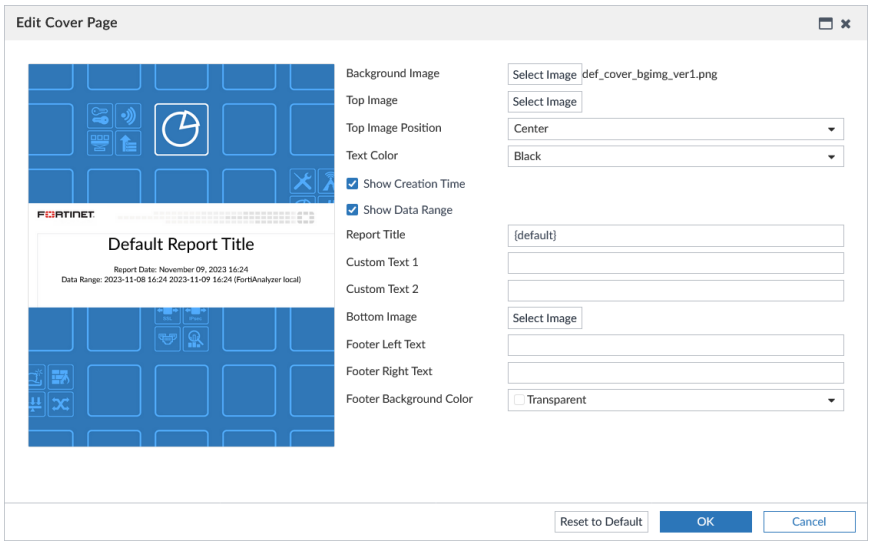
Customizing report cover pages

A report cover page is only included in the report when enabled on the *Settings* tab in the *Advanced Settings* section.

When enabled, the cover page can be customized to contain the desired information and imagery.

To customize a report cover page:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the content pane, select the report from the list, and click *Report* > *Edit* in the toolbar.
4. Select the *Settings* tab and then click *Advanced Settings*.
5. Select the *Print Cover Page* checkbox, then click *Customize* next to the checkbox. The *Edit Cover Page* pane opens.



6. Configure the following settings:

Background Image	Click *Select Image* to open the *Select Image?* dialog. Select an image or click *Browse* to find an image on the management computer, then click *OK* to add the image as the background image of the cover page. Alternatively, you can select *No Image*.
Top Image	Click *Select Image* to open the *Select Image?* dialog. Select an image or click *Browse* to find an image on the management computer, then click *OK* to add the image at the top of the cover page. Alternatively, you can select *No Image*.
Top Image Position	Select the top image position from the dropdown menu. Select one of the following: *Left*, *Center*, *Right*.
Text Color	Select a text color from the dropdown list.
Show Creation Time	Select to print the report date on the cover page.
Show Data Range	Select to print the data range on the cover page.
Report Title	Accept the default title or type another title in the *Report Title* field.
Custom Text 1	If you want, enter custom text for the *Custom Text 1* field.
Custom Text 2	If you want, enter custom text for the *Custom Text 2* field.
Bottom Image	Click *Select Image* to open the *Select Image?* dialog. Select an image or click *Browse* to find an image on the management computer, then click *OK* to add the image to the bottom of the cover page.
Footer Left Text	If you want, enter custom text to be printed in the left footer of the cover page.
Footer Right Text	If you want, enter custom text to be printed in the right footer of the cover page.

Footer Background Color	Select the cover page footer background color from the dropdown list.
Reset to Default	Select to reset the cover page settings to their default settings.

7. Click *OK* to save the configurations and return to the *Settings* tab.

Reports Editor tab



Because the cut, copy, and paste functions need access to the clipboard of your operating system, some Internet browsers either block it when called from the layout editor toolbar, or ask you to explicitly agree to it. If you're blocked from accessing the clipboard by clicking the respective cut, copy, and paste buttons from the toolbar or context menu, you can always use keyboard shortcuts.

The following options are available in the *Editor* tab (layout editor):

Field	Description
Insert Chart or Edit Chart	Click to insert a FortiAnalyzer chart. Charts are associated with datasets that extract data from logs for the report. In the *Insert Chart* or *Chart Properties* dialog box, you can specify a custom title, width, and filters for the chart. For information on setting filters, see Filtering report output on page 442. You can edit a chart by right clicking the chart in the layout editor and selecting *Chart Properties* or by clicking the chart to select it and then clicking *Edit Chart*.
Insert Macro	Click to insert a FortiAnalyzer macro. Macros are associated with datasets that extract data from logs for the report.
Image	Click the *Image* button in the toolbar to insert an image into the report layout. Right-click an existing image to edit image properties.
Table	Click the *Table* button in the toolbar to insert a table into the report layout. Right-click an existing table to edit a cell, row, column, table properties, or delete the table.
Insert Horizontal Line	Click to insert a horizontal line.
Insert Page Break for Printing	Click to insert a page break for printing.
Link	Click the *Link* button in the toolbar to open the *Link* dialog box. You can select to insert a URL, a link to an anchor in the text, or an email address.
Anchor	Click the *Anchor* button in the toolbar to insert an anchor in the report layout.
Cut	To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods: • Click the cut button in the toolbar • Use the *CTRL+X* shortcut on your keyboard.

Field	Description
Copy	To copy a text fragment, start with selecting it. When the text is selected, you can copy it using one of the following methods: • Click the copy button in the toolbar • Use the *CTRL+C* shortcut on your keyboard.
Paste	To paste text, start with cutting or copying from within the editor or from another source. Once the text is cut or copied, you can paste it in the editor using one of the following methods: • Click the paste button in the toolbar • Use the *CTRL+V* shortcut on your keyboard.
Undo	Click to undo the last action. Alternatively, use the *CTRL+Z* keyboard shortcut to perform the undo operation.
Redo	Click to redo the last action. Alternatively, use the *CTRL+Y* keyboard shortcut to perform the redo operation.
Find	Type text in the search field, and then click *Find* to highlight instances of that text in the editor. The instances of that text will be highlighted one at a time, starting at the top of the editor. The search field is not case-sensitive.
Replace	This is only actionable when text has been highlighted using the *Find* button. Type the replacement text in the replace field, and then click *Replace* to put it in place of the highlighted text.
Replace All	This is only actionable when text has been highlighted using the *Find* button. Type the replacement text in the replace field, and then click *Replace All* to put it in place of all instances of the text in the *Find* field.
Save as Template	Click to save the layout as a template.
Paragraph Format	Select the paragraph format from the dropdown list. Select one of the following: *Normal*, *Heading 1*, *Heading 2*, *Heading 3*, *Heading 4*, *Heading 5*, *Heading 6*.
Font Name	Select the font from the dropdown list.
Font Size	Select the font size from the dropdown list. Select a size ranging from 8 to 72.
Bold	Select the text fragment and then click the *Bold* button in the toolbar. Alternatively, use the *CTRL+B* keyboard shortcut to apply bold formatting to a text fragment.
Italic	Select the text fragment and then click the *Italic* button in the toolbar. Alternatively, use the *CTRL+I* keyboard shortcut to apply italics formatting to a text fragment.
Underline	Select the text fragment and then click the *Underline* button in the toolbar. Alternatively, use the *CTRL+U* keyboard shortcut to apply underline formatting to a text fragment.

Field	Description
Strike Through	Select the text fragment and then click the *Strike Through* button in the toolbar.
Subscript	Select the text fragment and then click the *Subscript* button in the toolbar.
Superscript	Select the text fragment and then click the *Superscript* button in the toolbar.
Text Color	You can change the color of text in the report by using a color palette. To choose a color, select a text fragment, click the *Text Color* button in the toolbar, and select a color.
Background Color	You can also change the color of the text background.
Insert/Remove Numbered List	Click to insert or remove a numbered list.
Insert/Remove Bulleted List	Click to insert or remove a bulleted list.
Decrease Indent	To decrease the indentation of the element, click the *Decrease Indent* toolbar button. The indentation of a block-level element containing the cursor will decrease by one tabulator length.
Increase Indent	To increase the indentation of the element, click the *Increase Indent* toolbar button. The block-level element containing the cursor will be indented with one tabulator length.
Block Quote	Block quote is used for longer quotations that are distinguished from the main text by left and right indentation. It is recommended to use this type of formatting when the quoted text consists of several lines or at least 100 words.
Align Left	When you align your text left, the paragraph is aligned with the left margin and the text is ragged on the right side. This is usually the default text alignment setting for the languages with left to right direction.
Center	When you center your text, the paragraph is aligned symmetrically along the vertical axis and the text is ragged on the both sides. This setting is often used in titles or table cells.
Align Right	When you align your text right, the paragraph is aligned with the right margin and the text is ragged on the left side. This is usually the default text alignment setting for the languages with right to left direction.
Justify	When you justify your text, the paragraph is aligned to both the left and right margins and the text is not ragged on either side..
Remove Format	Click to remove formatting.

Filtering report output

You can apply log message filters to reports and charts.

To filter output in a report:

Click the *Settings* tab and scroll to the *Filters* section.

To filter output in a chart:

1. Click the *Layout* tab.
2. Filter a new or existing chart:
   - Click *Insert Chart* and scroll to the *Filters* section.
   - Right-click a chart in the layout and select *Chart Properties*. Scroll to the *Filters* section.

In the *Filters* section, the following options are available.

Field	Description
Log messages that match	Available in the *Settings* tab only. Select *All* to filter log messages based on all of the added conditions, or select *Any of the Following Conditions* to filter log messages based on any one of the conditions.
Add Filter	Click to add filters. For each filter, select a log field and operator from the dropdowns, and then enter or select the value(s). • **Log Field**: Select a log field from the dropdown. The available log fields depend on the device type. • **Match Criteria**: Select an operator from the dropdown. The available options depend on the selected log field. • **Value**: Select a value from the dropdown list or enter a value in the text box. The available options depend on the selected log field. If there is no dropdown list provided by FortiAnalyzer, you must manually enter a value to find in the raw log. The *Value* field is case sensitive. In the **Action** column, click plus (**+**) to insert a new filter below. You can insert multiple filters. To delete a filter, click the **x** next to the filter.  You cannot create multiple filters using the same *Log Field*. If multiple entries for the same field are required, use a comma without a space as a separator in the *Value* field. For example, • **Log Field**: `Interface (intf)` • **Match Criteria**: `Equal To` • **Value**: `port1,port2` If there is a comma used within the values, enclose each value in double quotations. For example, • **Log Field**: `Sequence Number (seq)` • **Match Criteria**: `Equal To` • **Value**: `"1,2","2,1"`

Field	Description
	 The *Settings* and *Layout* tabs use the same *Log Field* list to filter output; however, some log fields are not used in charts. The *Log Field* you use to filter a report may not apply to the log fields in a chart.
LDAP Query	Available in the *Settings* tab only. Click to add an LDAP query, then select the *LDAP Server* and the *Case Change* value from the dropdown lists. Use this option to query an LDAP server for group membership. The results of this query is used to filter the report to only match logs for users belonging to that group. You must specify the group name in the filter definition. If you enable *LDAP Query*, the group name is not used to match the group field in logs. The group name is only used for the LDAP query to determine group membership.  The query will not retrieve the `userPrincicpalName` if the *Distinguished Name* in the *System Settings* does not contain an organization unit (ou). To retrieve the UPN, add the *Distinguished Name* as it appears in the *System Settings* to your query.

 If both chart and report filters are selected for the same report, the chart filter will be used instead of the report filter.

Managing reports

You can manage reports by going to *Reports* > *Report Definitions* > *All Reports*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a report to display the menu.

Option	Description
Run report	Generates a report.
Report	See below for report options.
Create New	Creates a new report. You can choose whether to base the new report on a report template.
Edit	Edit the selected report.

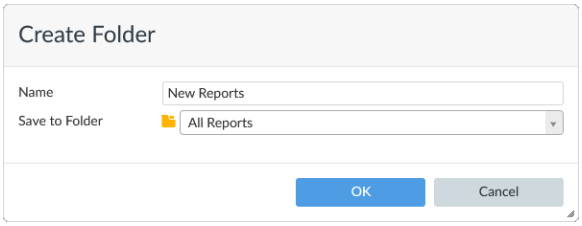
Option		Description
	Clone	Clones the selected report.
	Disable Schedule	Disable the schedule for the selected report. You can enable schedules, if needed, by editing the report.
	Delete	Deletes the selected report.
	Remove from Folder	Remove the selected report from its current folder.
	Move	Move the report to a new folder location.
	Assign to Folder	Assign the selected report(s) to a folder. From the dropdown menu, select an existing report folder. Click the add icon to add an additional folder. When multiple folders are selected, reports are included in both folders.
Folder		See below for folder options.
	Create New Folder	Create a new folder. Folders can be nested.
	Rename Folder	Rename the currently selected folder.
	Delete Folder	Delete the currently selected folder. Folders which include reports cannot be deleted.
More		See below for more options.
	Import	Imports a report from a management computer.
	Export	Exports a report to a management computer.
Show Scheduled Only		Filters the list to include only reports that have been run or are scheduled to be run. This setting is only available in the toolbar.

Organizing reports into folders

FortiAnalyzer reports are organized into default folders. You can create additional folders to organize reports. Reports can be assigned to multiple folders, and folders can be nested.

To organize reports into folders:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. Click *Folder* in the toolbar, and select *Create New Folder*.



4. Specify the folder name and location and click *OK*. The folder is now displayed in the report list.
5. You can now drag-and-drop, move, assign, create, clone, or import reports into this folder. See Managing reports on page 444.

To move folder locations:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. Highlight an existing folder, and select *Report* > *Move* from the right-click menu.
4. Select the target folder location, and click *OK*.

Importing and exporting reports

You can transport a report between FortiAnalyzer units and ADOMs. You can export a report from the FortiAnalyzer unit to the management computer. The report is saved as a .dat file on the management computer. You can then import the report file to another FortiAnalyzer unit or ADOM.

To export reports:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. Select a report, and click *More* > *Export*.
   The *Export Report* pane displays.
4. Use the toggles to *Backup Other Dependent Settings* in the exported file, as needed:
   - *Subnets*
   - *LDAP Server* (the export will remove the ADOM setting from the LDAP configuration)
   - *Output Profile*
   - *Email*

   By default, all of these options are disabled.
5. Click *OK* to export the report.
   The report configuration is saved as a .dat file on the management computer. This includes the charts, datasets, images, and report settings.

To import reports:

1. If using ADOMs, ensure that you are in the correct ADOM.
   If the device type used in the charts and datasets for the report does not match the ADOM type, the import will be rejected with an error. For more information, see How ADOMs affect reports on page 427.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. Click *More* > *Import*.
   The *Import Report* pane displays.
4. In the *File* field, drag and drop the .dat report file, or click *Browse* and select the file.
5. From the *Save to Folder* dropdown, select the folder to save the report in.
6. Select the *Action in Case of Conflict*:

- *Keep Current Settings* (default)
- *Reject with Error*
- *Overwrite*

7. Click *OK* to import the report.

Report template library



Because the cut, copy, and paste functions need access to the clipboard of your operating system, some Internet browsers either block it when called from the layout editor toolbar, or ask you to explicitly agree to it. If you're blocked from accessing the clipboard by clicking the respective cut, copy and paste buttons from the toolbar or context menu, you can always use keyboard shortcuts.

A report template defines the charts and macros that are in the report, as well as the layout of the content.

You can use the following items to create a report template:

- Text
- Images
- Tables
- Charts that reference datasets
- Macros that reference datasets

Datasets for charts and macros specify what data are used from the Analytics logs when you generate the report. You can also create custom charts and macros for use in report templates.

Creating report templates

You can create a report template by saving a report as a template or by creating a totally new template.

To create a report template:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to the *Reports* > *Report Definitions*> *Templates*.
3. In the toolbar of the content pane, click *Create New*.
4. Set the following options:
   a. Name.
   b. Description.
   c. Category. If you are in a Security Fabric ADOM, the *Category* must be *SecurityFabric*.
   d. Language.
5. Use the toolbar to insert and format text and graphics for the template. In particular, use the *Insert Chart* and *Insert Macro* buttons to insert charts and macros into the template.

For a description of the fields, see Reports Editor tab on page 440. For information about creating charts and macros, see Creating charts on page 457 and Creating macros on page 461.

6. Click *OK*.
   The new template is now displayed on the template list.

To create a report template by saving a report:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the content pane, select the report from the list, and click *Edit* in the toolbar.
4. In the *Layout* tab, click the *Save As Template* button in the toolbar.
5. In the *Save as Template* dialog box, set the following options, and click *OK*:
   a. Name.
   b. Description.
   c. Category. If you are in a Security Fabric ADOM, the *Category* must be *SecurityFabric*.
   The new template is now displayed on the template list.

Viewing sample reports for predefined report templates

You can view sample reports for predefined report templates to help you visualize how the reports would look.

To view sample reports:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to the *Reports* > *Report Definitions* > *Templates*.
3. In the content pane, click the *HTML* or *PDF* link in the *Preview* column of a template to view a sample report based on the template.

Managing report templates

You can manage report templates in *Reports* > *Report Definitions*> *Templates*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a template to display the menu.

Option	Description
Create New	Creates a new report template
Edit	Edits a report template. You can edit report templates that you created. You cannot edit predefined report templates.
View	Displays the settings for the predefined report template. You can copy elements from the report template to the clipboard, but you cannot edit a predefined report template.

Option	Description
Delete	Deletes the selected report template. You cannot delete predefined report templates.
Clone	Clones the selected report template.
Create Report	Creates the selected report template.
Install Template Pack	Upload and install a template pack.

List of report templates

FortiAnalyzer includes report templates you can use as is or build upon when you create a new report. FortiAnalyzer provide different templates for different devices.

You can find report templates in *Reports* > *Report Definitions* > *Templates*.

Application report templates

Template - Application Risk and Control	Template - Safeguarding Report
Template - Bandwidth and Applications Report	Template - Self-Harm and Risk Indicators Report
Template - Bandwidth and Applications Report (SIEM)	Template - Shadow IT Report
Template - Cyber-Bullying Indicators Report	Template - Social Media Usage Report
Template - Detailed Application Usage and Risk	Template - Top 20 Categories and Applications (Bandwidth)
Template - High Bandwidth Application Usage Report	Template - Top 20 Categories and Applications (Session)
Template - SaaS Application Usage Report	Template - Top Allowed and Blocked with Timestamps

Assets report templates

Template - Asset and Identity Report

Fabric report templates

Template - Fortinet Email Risk Assessment
Template - FortiPortal User Summary Report

FortiADC report templates

Template - FortiADC Report

FortiCache report templates

Template - FortiCache Default Report
Template - FortiCache Security Analysis
Template - FortiCache Web Usage Report

FortiClient report templates

Template - FortiClient Default Report
Template - FortiClient Vulnerability Scan Report

FortiDDoS report templates

Template - FortiDDoS Default Report

FortiDeceptor report templates

Template - FortiDeceptor Default Report

FortiEDR report templates

Template - FortiEDR Report

FortiFirewall report templates

Template - FortiFirewall Bandwidth and Applications Report

FortiMail report templates

Template - FortiMail Analysis Report

Template - FortiMail Default Report
Template - FortiMail Summary Report

FortiNAC report templates

Template - FortiNAC Endpoints and Network Report

FortiNDR report templates

Template - FortiNDR Breach Prevention Report
Template - FortiNDR Network Anomalies Report

FortiProxy report templates

Template - FortiProxy Default Report
Template - FortiProxy Security Analysis
Template - FortiProxy Web Usage Report

FortiSandbox report templates

Template - Endpoint Sandbox Detections Report
Template - FortiSandbox CTAP Report
Template - FortiSandbox Default Report

FortiWeb report templates

Template - FortiWeb Default Report
Template - FortiWeb Web Application Analysis Report

Security report templates

Template - 360-Degree Security Review	Template - ISO 27001:2022 Compliance Security Rating Report

Template - 360 Security Report	Template - NERC CIP Compliance Security Rating Report (OT)
Template - CIS Security Rating Report	Template - Operational Technology (OT) Security Risk Report
Template - Cyber Threat Assessment	Template - PCI-DSS Compliance Review
Template - Daily Summary Report	Template - Security Analysis
Template - Data Loss Prevention Detailed Report	Template - Security Events and Incidents Summary
Template - Default ZTNA Report	Template - Situation Awareness Report
Template - DLP Report	Template - SOC 2 Compliance Report
Template - DNS Security Report	Template - SOC Incident Report
Template - Email Report	Template - Threat Report
Template - Endpoint Security Vulnerability Report	Template - VPN Report
Template - FortiClient Default Report from FortiGate	Template - Web Usage Report
Template - FortiClient Vulnerability Scan Report from FortiGate	Template - Web Usage Summary Report
Template - FSBP Security Rating Report	Template - What is New Report
Template - HIPAA Compliance Security Rating Report	Template - WiFi Network Summary
Template - IPS Report	

System report templates

Template - 360 Protection Report	Template - NGFW Assessment Report
Template - Admin and System Events Report	Template - Secure SD-WAN Assessment Report
Template - C-Suite SD-WAN Insights Report	Template - Secure SD-WAN Report
Template - DNS Report	Template - Throughput Utilization Billing by Device and Interface Report
Template - FortiGate Performance Statistics Report	Template - Throughput Utilization Billing Report
Template - GTP Report	

User report templates

Template - Client Reputation
Template - User Detailed Browsing Log
Template - User Security Analysis

Template - User Top 500 Websites by Bandwidth
Template - User Top 500 Websites by Session

Web report templates

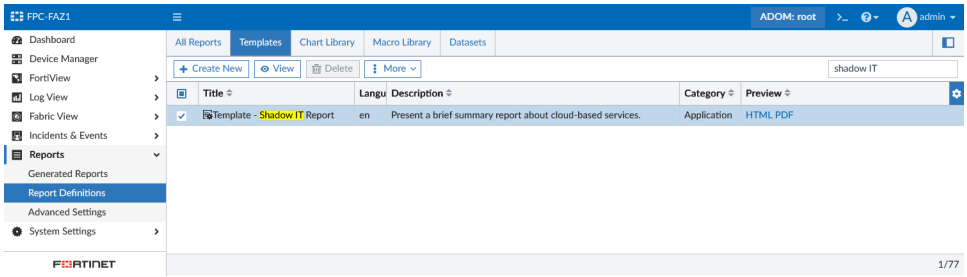
Template - Hourly Website Hits
Template - Top 20 Category and Websites (Bandwidth)
Template - Top 20 Category and Websites (Session)
Template - Top 500 Sessions by Bandwidth

Using the template - Shadow IT Report

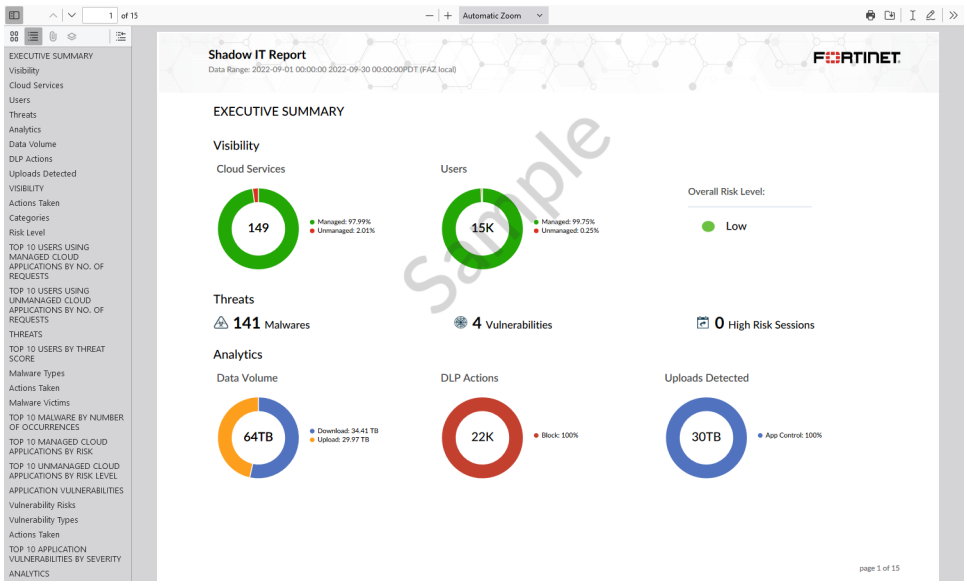
This topic provides an example for creating a report from a template. This topic also provides a brief explanation of the report used in the example: the *Shadow IT Report*.

To view a sample of the report:

1. Go to *Reports* > *Report Definitions* > *Templates*.
2. In the *Search* field, type `Shadow IT Report`.
   The table will filter and display the *Template - Shadow IT Report*.



3. In the *Preview* column for the report, click *HTML* or *PDF* to view the sample report in that format.
   For example, see page 1 of the report in PDF below.



The *Shadow IT Report* provides enhanced visibility and control for cloud based applications.

Detected applications are classified as:

- `Managed`: Allowed applications.
- `Unmanaged`: Blocked, quarantined, or reset applications.

Information about the applications, including their Category and Compliance Standard, is provided by the Shadow IT database (SIDB).

Application risk is determined by a numerical score provided by the SIDB for each application. The Risk Levels in the report are as follows:

- `Low`: Score is 1 to 15.
- `Guarded`: Score is 16 to 30.
- `Elevated`: Score is 31 to 50.
- `High`: Score is 51 to 70.
- `Severe`: Score is 71 to 100.

The `Overall Risk Level` is the average application risk score for all detected managed applications.

The `High Risk Sessions` are the number of sessions from managed applications with a risk score of `High` or `Severe`.

To create the report from the template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
2. Select the checkbox for *Template - Shadow IT Report*.
3. From the *More* dropdown, click *Create Report*.
4. In the *Name* field, enter a name for the report.

   If you did not make any changes, consider naming the report `Shadow IT Report`. The GUI notifies you if a duplicated name already exists.
5. From the *Save to Folder* dropdown, select a folder for the report.

   If needed, you can save the report to multiple folders. To create a report folder, see Organizing reports into folders on page 445.
6. Click *OK*.

The report is now available to be run, as needed, from *Reports > Report Definitions > All Reports*.

To run the report:

1. Go to *Reports > Report Definitions > All Reports*, and double-click the row for the *Shadow IT Report*. The *Edit: Shadow IT Report* pane opens.
2. In the *Generated Reports* tab, click *Run Report*.
3. When the report is available, click the Format to open the report in.

Using the template - Endpoint security vulnerability report

This topic describes a template report that uses logs from the SIEM database (siemdb).

The *Endpoint Security Vulnerability Report* provides a comprehensive security rating overview and historical trends specifically for all managed endpoints based on the vulnerabilities. This report utilizes retrieved data from FortiClient EMS and FortiGuard, including the outbreak alert and endpoint vulnerability information.

FortiClient EMS connector(s) must be created and enabled to generate this report with data. The EMS connector can insert the data into FortiAnalyzer Fabric SIEM logs. For more information about configuration, see below.

1. In FortiAnalyzer, go to a Fabric ADOM.
2. In *Incidents & Events > Automation > Active Connectors*, create a new FortiClient EMS Connector. See Configuring security fabric connectors on page 372.

   Once the FortiClient EMS Connector is configured, the *Update Asset, Identity and Vulnerability in Sequence* playbook is automatically created in *Incidents & Events > Automation > Playbook* . This default playbook gets the endpoints and their vulnerabilities from EMS. It is scheduled to run once per day, but it can be edited according your needs.
3. In *Incidents & Events > Automation > Playbook*, enable the *Update Asset, Identity and Vulnerability in Sequence* playbook for the FortiClient EMS Connector. See Playbooks on page 382.
4. In *Fabric View > Asset Identity Center > Asset Identity List*, add the FortiClient EMS Connector as a data source.
   a. In *Fabric View > Asset Identity Center > Asset Identity List*, click *More > Data Sources*. The *Data Source Selection* dialog displays.
   b. Click *Create New*.
   c. From the *Data Source* dropdown, select *EMS Connector*.
   d. Enable the *Status*.
   e. For the *Connectors* field, select the EMS connector that you have created.
   f. Click *OK*.
5. In *Device Manager*, add the FortiClient EMS as an authorized device.
   a. In *Device Manager*, click *Add Device*. The *Add Device* dialog displays.
   b. In the *Name* field, enter a name for the FortiClient EMS.
   c. For *Link Device By*, select *Serial Number*.
   d. In the Serial Number field, enter the serial number for the FortiClient EMS. The *Device Model* field automatically populated with *FortiClient-EMS*.

e. Click *Next*.

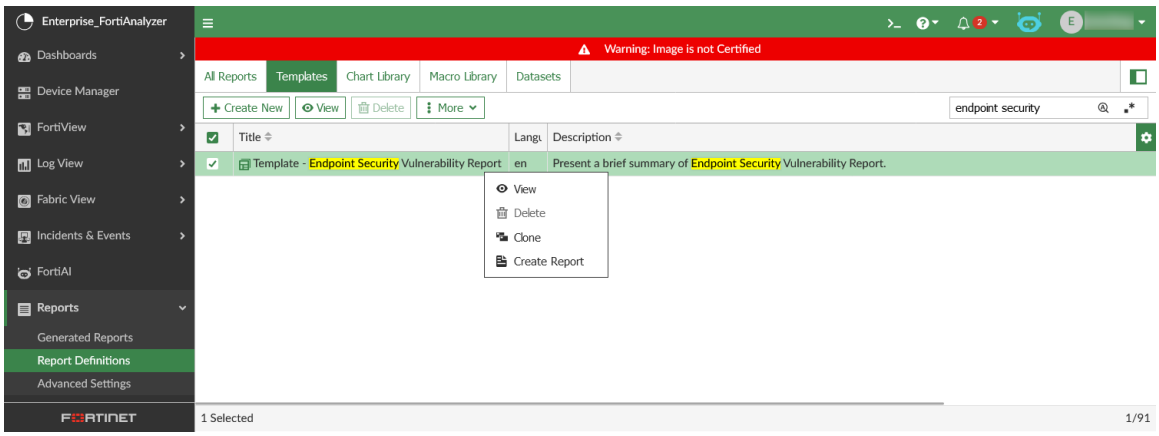
The dialog displays the status for adding the device and confirms when the device is succesfully added.

The FortiClient EMS will receive the related endpoint vulnerabilities logs.

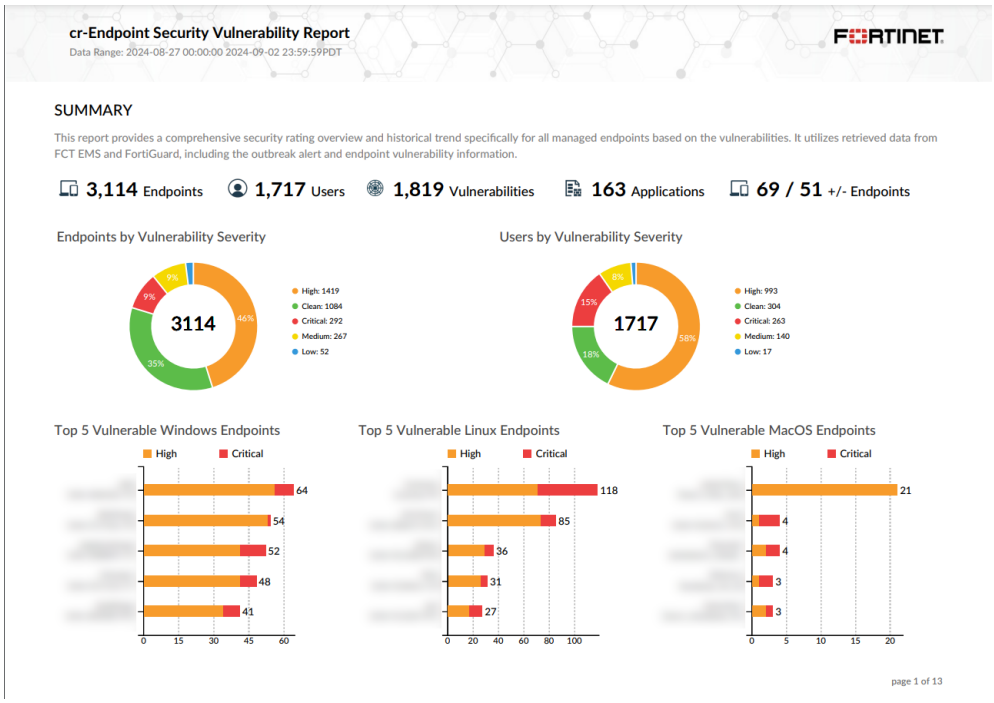
When the *Update Asset, Identity and Vulnerability in Sequence* playbook is run, it will call the EMS API to get all endpoints and vulnerabilities data, and it will be inserted as Fabric (SIEM) logs. The predefined EMS-Connector Log Parser is automatically assigned to the device to parse the logs; you can find this parser and confirm its assignment in *Incidents & Events > Log Parser*.

Multiple EMS connectors are supported. If needed, repeat the steps to create another EMS connector.

The report can be created from the template in *Reports > Report Definitions > Templates*.



See below for an example of page 1 from the *Endpoint Security Vulnerability Report*.



The data query for the *Endpoint Security Vulnerability Report* is based on the SIEM database (siemdb), and it uses SIEM normalized logs and the fct_mdata.

The following fields have been added in FortiAnalyzer 7.6.2 for this report:

- `event_subtype=endpoint-vuln` is added in the siemdb
- `release_data` and `detection_product` are added to fct_mdata

Chart library

Use the Chart library to create, edit, and manage your charts.

In a Security Fabric ADOM, you can insert charts from all device types into a single report.

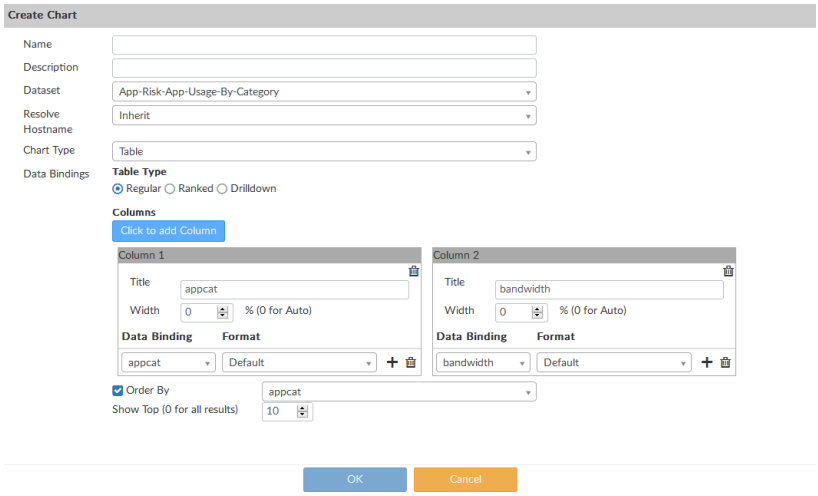
Creating charts



You can also create charts using the *Log View* Chart Builder. See Creating charts with Chart Builder on page 164.

To create charts:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *Chart Library*.
3. Click *Create New* in the toolbar.



4. Configure the settings for the new chart, the click *OK*.

Name	Enter a name for the chart.
Description	Enter a description of the chart.

Dataset		Select a dataset from the dropdown list. For more information, see Datasets on page 462. Options vary based on device type.
Resolve Hostname		Select to resolve the hostname. Select one of the following: *Inherit*, *Enabled*, or *Disabled*.
Chart Type		Select a graph type from the dropdown list; one of: *Table*, *Bar*, *Pie*, *Line*, *Area*, *Donut*, or *Radar*. This selection affects the rest of the available selections.
Data Bindings		The data bindings vary depending on the chart type selected.
Table		
	Table Type	Select *Regular*, *Ranked*, or *Drilldown*.
	Add Column	Select to add a column. Up to 15 columns can be added for a *Regular* table. *Ranked* tables have two columns, and *Drilldown* tables have three columns.
	Columns	The following column settings must be set: • *Column Title*: Enter a title for the column. • *Width*: Enter the column width as a percentage. • *Data Binding*: Select a value from the dropdown list. The options vary depending on the selected dataset. • *Format*: Select a value from the dropdown list.All formats are available regardless of the data binding selected for the column. Select a format to display the data according to your needs.  Some formats will only work with select data bindings. For example, the *Icon-IP Country/Region* format only displays the correct flag icon when the *Data Binding* is *dstcountry*. • *Add Data Binding*: Add data bindings to the column. Every column must have at least one data binding. The maximum number varies depending on the table type.
	Order By	Select what to order the table by. The available options vary depending on the selected dataset.
	Show Top	Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the *Others* category for *Ranked* and *Drilldown* tables.
	Drilldown Top	Enter a numerical value. Only the first 'X' items are displayed. This options is only available for *Drilldown* tables.
Bar		
	X-Axis	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Label*: Enter a label for the axis.

		• *Show Top*: Enter a numerical value. Only the first 'X' items are displayed. Other items are bundled into the *Others* category.
	Y-axis	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Format*: Select a format from the dropdown list: *Bandwidth*, *Counter*, *Default*, *Percentage*, or *Severity*. • *Label*: Enter a label for the axis.
	Bundle rest into "Others"	Select to bundle the rest of the results into an *Others* category.
	Group By	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Show Top*: Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the *Others* category.
	Order By	Select to order by the X-Axis or Y-Axis.
Pie, Donut, or Radar		
	Category	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Label*: Enter a label for the axis. • *Show Top*: Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the *Others* category.
	Series	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Format*: Select a format from the dropdown list: *Bandwidth*, *Counter*, *Default*, *Percentage*, or *Severity*. • *Label*: Enter a label for the axis.
	Bundle rest into "Others"	Select to bundle the rest of the results into an *Others* category.
Line or Area		
	X-Axis	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Format*: Select a format from the dropdown list: *Default*, or *Time*. • *Label*: Enter a label for the axis.
	Lines	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Format*: Select a format from the dropdown list: *Bandwidth*, *Counter*, *Default*, *Percentage*, or *Severity*. • *Type*: Select the type from the dropdown list: *Line Up* or *Line Down*. • *Legend*: Enter the legend text for the line.
	Add line	Select to add more lines.

Managing charts

Manage your charts in *Reports > Report Definitions > Chart Library*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a chart to display the menu.

Option	Description
Create New	Creates a new chart.
Edit	Edits a chart. You can edit charts that you created. You cannot edit predefined charts.
View	Displays the settings for the selected predefined chart. You cannot edit a predefined chart.
Delete	Deletes the selected chart. You can delete charts that you create. You cannot delete predefined charts.
Clone	Clones the selected chart.
Import	Imports a previously exported FortiAnalyzer chart.
Export	Exports one or more FortiAnalyzer charts.
View Options	Select or deselect the checkboxes to show or hide FortiGuard, Built-in, and Custom charts in the table view.
Search	Lets you search for a chart name. You can toggle to match case and use regular expression according to your needs.

Viewing datasets associated with charts

To view datasets associated with charts:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports > Report Definitions > Chart Library*.
3. Select a chart, and click *View* in the toolbar.
4. In the *View Chart* pane, find the name of the dataset associated with the chart in the *Dataset* field.
5. Go to *Reports > Report Definitions > Datasets*.
6. In the *Search* box, type the name of the dataset.
7. Select the dataset that is found, and click *View* in the toolbar to view it.

Macro library

Use the Macro library to create, edit, and manage your macros.

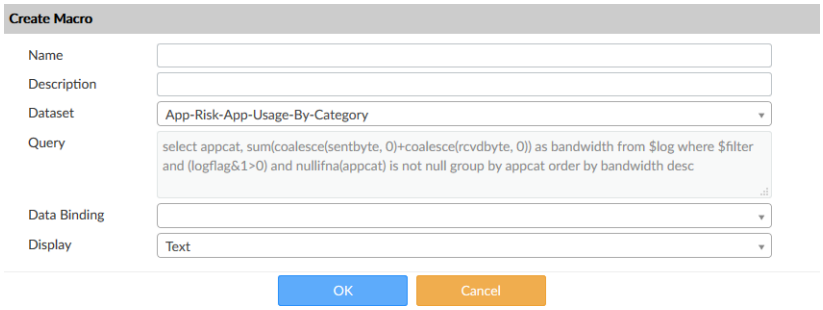
Creating macros

FortiAnalyzer includes a number of predefined macros. You can also create new macros, or clone and edit existing macros.

Macros are predefined to use specific datasets and queries. They are organized into categories, and can be added to, removed from, and organized in reports.

To create a new macro:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *Macro Library*, and click *Create New*. The *Create Macro* pane is displayed.



3. Provide the required information for the new macro.

Name	Enter a name for the macro.
Description	Enter a description of the macro.
Dataset	Select a dataset from the dropdown list. The options will vary based on device type.
Query	Displays the query statement for the dataset selected.
Data Binding	The data bindings vary depending on the dataset selected. Select a data binding from the dropdown list.
Display	Select a value from the dropdown list.

4. Click *OK*. The newly created macro is shown in the Macro library.

Managing macros

You can manage macros by *Reports* > *Report Definitions* > *Macro Library*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a macro to display the menu.

Option	Description
Create New	Creates a new macro.
Edit	Edit the selected macro. You can edit macros that you created.

Option	Description
View	Displays the settings for the selected macro. You cannot edit predefined macros.
Delete	Deletes the selected macro. You can delete macros that you create. You cannot delete predefined macros.
Clone	Clones the selected macro.
View Options	Select or deselect the checkboxes to show or hide FortiGuard, Built-in, and Custom macros in the table view.
Search	Lets you search for a macro name. You can toggle to match case and use regular expression according to your needs.

Viewing datasets associated with macros

To view datasets associated with macros:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *Macro Library*.
3. Select a macro, and click *View* (for predefined macros) or *Edit* (for custom macros) in the toolbar.
4. In the *View Macro* or *Edit Macro* pane, find the name of the dataset associated with the macro in the *Dataset* field.
5. Go to *Reports* > *Report Definitions*> *Datasets*.
6. In the *Search* box, type the name of the dataset.
7. Double-click the dataset to view it.

Datasets

Use the Datasets pane to create, edit, and manage your datasets.

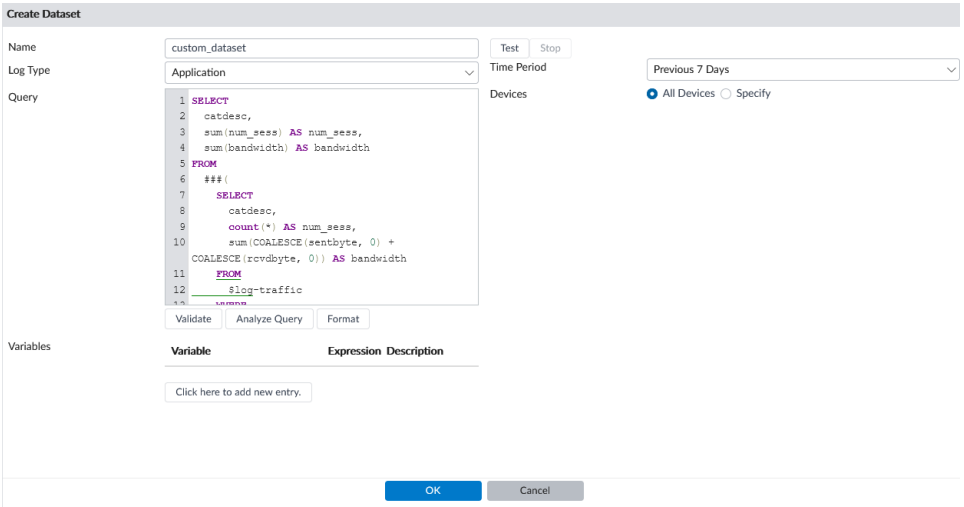
Creating datasets

FortiAnalyzer datasets are collections of data from logs for monitored devices. Charts and macros reference datasets. When you generate a report, the datasets populate the charts and macros to provide data for the report.

FortiAnalyzer has many predefined datasets that you can use right away. You can also create your own custom datasets. An easy way to build a custom query is to copy and modify a predefined dataset's query.

To create a new dataset:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
3. In the *Create Dataset* pane, provide the required information for the new dataset.



Name	Enter a name for the dataset.
Log Type	Select a log type from the dropdown list. Below is a list of the available log types based on device. • **FortiGate**: *Application Control*, *Intrusion Prevention*, *Content* , *Data Loss Prevention*, *DNS*, *Email Filter*, *Event*, *FortiClient System Event*, *FortiClient Security Event*, *FortiClient Traffic*, *File Filter*, *GTP*, *Vulnerability Scan*, *Protocol*, *Security*, *SSH*, *SSL*,*Traffic*, *Antivirus*, *VoIP*, *Web Application Firewall*, *Web Filter*, and *Local Event*. • **FortiMail**: *Email Filter*, *Event*, *History*, and *Antivirus*. • **FortiAnalyer**: *Application*, *Event*, and *Local Event*. • **FortiWeb**: *Attack* , *Event*, and *Traffic*. • **FortiCache**: *Application Control*, *Intrusion Prevention*, *Content* , *Data Loss Prevention*, *Email Filter*, *Event*, *Vulnerability Scan*, *Traffic*, *Antivirus*, *VoIP*, and *Web Filter*. • **FortiClient**: *FortiClient System Event*, *FortiClient Security Event*, *FortiClient Traffic*, and *SIEM*. • **Syslog**: *Syslog*. • **FortiManager**: *Application* and *Event*. • **FortiSandbox**: *Event*, *Malware*, and *Network Alerts*. • **FortiDDoS**: *Intrusion Prevention* and *Event*. • **FortiAuthenticator**: *Event*. • **FortiProxy**: *Application Control*, *Intrusion Prevention*, *Data Loss Prevention*, *DNS*, *Email Filter*, *Event*, *File Filter*, *Protocol*, *SSH*, *SSL*, *Traffic*, *Antivirus*, *VoIP*, *Web Application Firewall*, and *Web Filter*. • **FortiNAC**: *Asset* and *Event*. • **FortiFirewall**: *DNS*, *Event*, *File Filter*, *GTP*, *SSH*, *SSL*, and *Traffic*. • **FortiSOAR**: *Event*

	• **FortiADC**: *Intrusion Prevention*, *Event*, and *Traffic*. • **FortiDeceptor**: *Event*. • **FortiAP**: *Application Control*, and *Web Filter*. • **FortiNDR**: *Attack*, *Event*, and *NDR*. • **FortiIsolator**: *Event* and *Traffic*. • **FortiEDR**: *Event*. • **FortiPAM**: *Data Loss Prevention*, *Event*, *Protocol*, *Secret Events & Videos*, *SSH*, *Traffic*, *Antivirus*, *Zero-Trust Network Access*. • **FortiCASB**: *Data Loss Prevention*. • **FortiToken**: *Event*. • **FortiSRA**: *Data Loss Prevention*, *Event*, *Protocol*, *Secret*, *SSH*, *Traffic*, *Antivirus*, *Zero-Trust Network Access*. • **Fabric**: *Normalized*.
Query	Enter the SQL query used for the dataset. While entering SQL in the query field, automatic suggestions are provided that offer a list of possible commands, table names, log fields, and more to use in your query.
Validate	Click *Validate* to validate the entered SQL query. If any errors are present in the query, the details of the error are displayed below, otherwise the message will display *OK*.
Analyze Query	Click *Analyze Query* to perform a detailed analysis on the SQL query. *Analyze Query* displays the original SQL query, the transformed SQL query (if applicable), and the SQL validation results. This function also allows users to view the hcache query that is used when a report using this dataset has enabled the auto-cache option for faster report generation. For more information on hcache, see How auto-cache works on page 429
Format	Click *Format* to automatically format the entered SQL query, making it easier to read, update, and detect errors.
Variables	Click the *Add* button to add variable, expression, and description information. If added, the expression for the variable will be used when configuring filters for reports that use this dataset. For example, if *Variable = User (user)* and *Expression = coalesce(nullifna(`user`), ipstr(`srcip`))*, then the expression will be used when *User (user)* is selected as the *Log Field* in a report's filter. See Filtering report output on page 442.
Test	Click to test the SQL query before saving the dataset configuration. Click *Stop* to end a test in progress.
Time Period	Use the dropdown list to select a time period. When selecting *Custom*, enter the start date and time, and the end date and time.
Devices	Select *All Devices* or *Specify* to select specific devices to run the SQL query against. Click the *Select Device* button to add multiple devices to the query.

4. Click *Test*.
   The query results are displayed. If the query is not successful, an error message appears in the *Test Result* pane.
5. Click *OK*.

Viewing the SQL query of an existing dataset

You can view the SQL query for a dataset, and test the query against specific devices or all devices.

To view the SQL query for an existing dataset:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *Datasets*.
3. Hover the mouse cursor over the dataset on the dataset list. The SQL query is displayed as a tooltip.
   You can also open the dataset to view the *Query* field.



The SQL dataset test function can be used to determine if any errors are present in the SQL format. It should not be used to test returned values as those may be different than the ones used in reports.

SQL query functions

In addition to standard SQL queries, the following are some SQL functions specific to FortiAnalyzer. These are based on standard SQL functions.

`root_domain(hostname)`	The root domain of the FQDN. An example of using this function is: `select devid, root_domain(hostname) as website FROM $log WHERE'user'='USER01' GROUP BY devid, hostname ORDER BY hostname LIMIT 7`
`nullifna(expression)`	This is the inverse operation of `coalesce` that you can use to filter out `n/a` values. This function takes an expression as an argument. The actual SQL syntax this is base on is `select nullif(nullif(expression, 'N/A'), 'n/a')`. In the following example, if the user is n/a, the source IP is returned, otherwise the username is returned. `select coalesce(nullifna('user'), nullifna('srcip')) as user_src, coalesce(nullifna(root_domain(hostname)),'unknown') as domain FROM $log WHERE dstport='80' GROUP BY user_src, domain ORDER BY user_src LIMIT 7`
`email_domain` `email_user`	`email_domain` returns the text after the `@` symbol in an email address. `email_user` returns the text before the `@` symbol in an email address. An example of using this function is: `select 'from' as source, email_user('from') as e_user, email_domain ('from') as e_domain FROM $log LIMIT 5 OFFSET 10`

`from_dtime` `from_itime`	`from_dtime(bigint)` returns the device timestamp without time zone. `from_itime(bigint)` returns FortiAnalyzer's timestamp without time zone. An example of using this function is: `select itime, from_itime(itime) as faz_local_time, dtime, from_dtime (dtime) as dev_local_time FROM $log LIMIT 3`

`get_devtype()`	Returns the source device type. An example of using this function is:
	`select get_devtype(srcswversion, osname, devtype) as devtype_new, coalesce(nullifna(`srcname`),nullifna(`srcmac`), ipstr (`srcip`)) as dev_src, sum(crscore%65536) as scores from $log where $filter and (logflag&1>0) and crscore is not null group by devtype_new, dev_src having sum(crscore%65536)>0 order by scores desc`
	This function may return null values. To replace null values with "Unknown", you can add the following outer query:
	`select coalesce(nullifna(`devtype_new`), 'Unknown') as devtype_ new1,dev_src, scores from ###(select get_devtype(srcswversion, osname, devtype) as devtype_new, coalesce(nullifna(`srcname`),nullifna(`srcmac`), ipstr(`srcip`)) as dev_src, sum(crscore%65536) as scores from $log where $filter and (logflag&1>0) and crscore is not null group by devtype_new, dev_src having sum(crscore%65536)>0 order by scores desc )### t`

Managing datasets

You can manage datasets by going to *Reports* > *Report Definitions* > *Datasets*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a dataset to display the menu.

Option	Description
Create New	Creates a new dataset.
Edit	Edit the selected dataset. You can edit datasets that you created.
View	Displays the settings for the selected dataset. You cannot edit predefined datasets.
Delete	Deletes the selected dataset. You can delete datasets that you create. You cannot delete predefined datasets.
Clone	Clones the selected dataset. You can edit cloned datasets.
Validate	Validate selected datasets.
Validate All Custom	Validates all custom datasets.
View Options	Select or deselect the checkboxes to show or hide FortiGuard, Built-in, and Custom datasets in the table view.
Search	Lets you search for a dataset name. You can toggle to match case and use regular expression according to your needs.

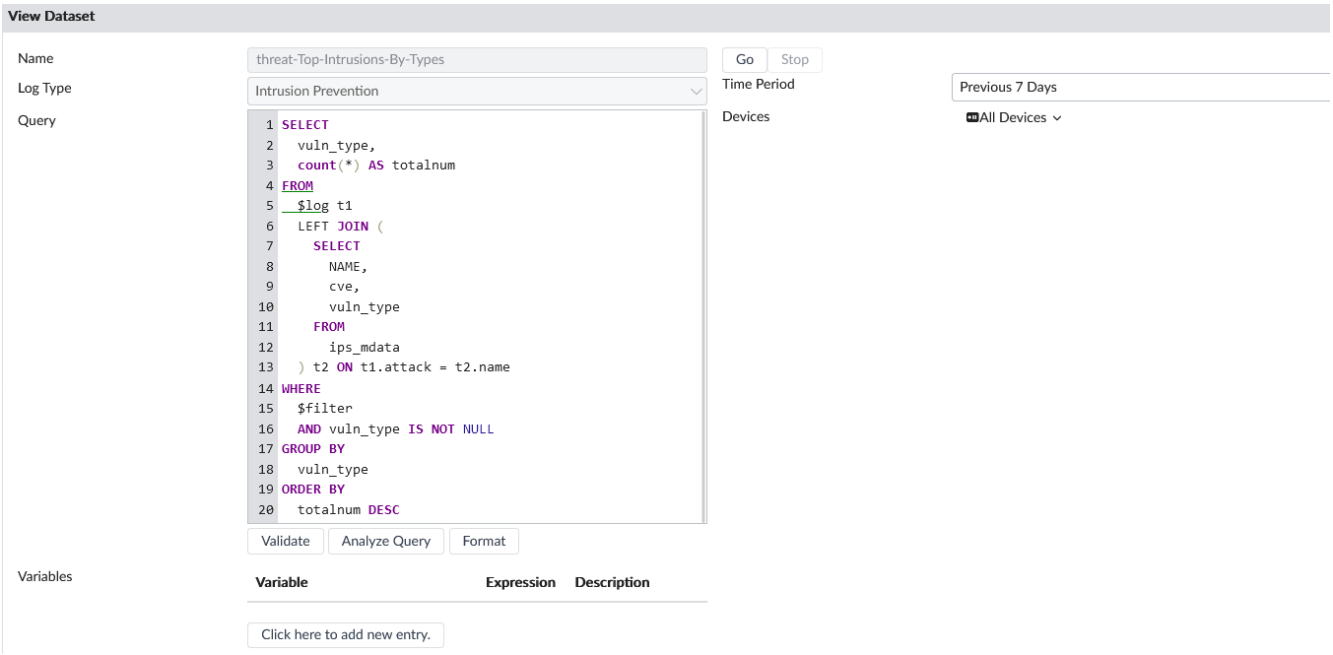
Aliases and metadata tables

Aliases in predefined datasets

Some predefined FortiAnalyzer datasets make use of aliases which are labeled as `t1`, `t2`, etc. These temporary names can only be referenced within the dataset in which they are created.

As an example, the `t1` and `t2` aliases are used in the *threat-Top-Intrusions-By-Types* dataset to define the following tables:

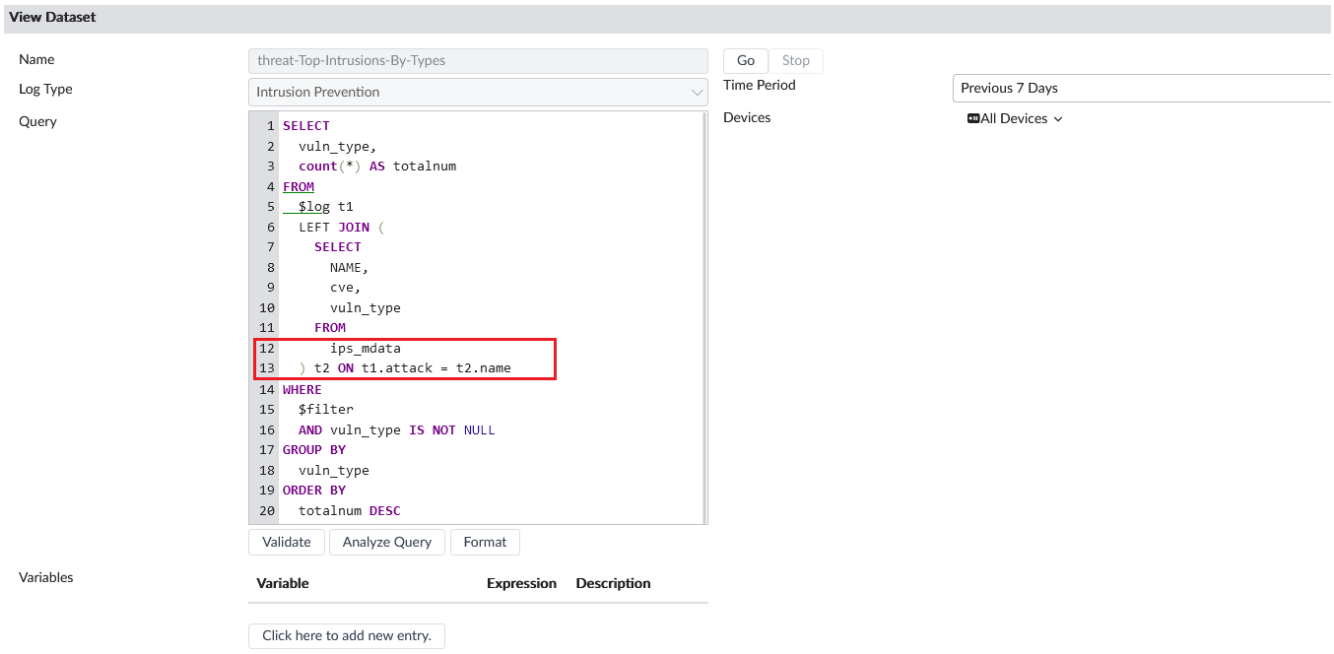
- `t1`: Intrusion Prevention log data.
- `t2`: The *name*, *CVE*, and *vuln_type* from the *IPS_mdata* table.



Metadata tables

FortiAnalyzer has access to metadata tables which are used in some predefined datasets to enrich a chart's data by complementing log fields with information from FortiGuard. This is typically accomplished through the use of the SQL JOIN clause.

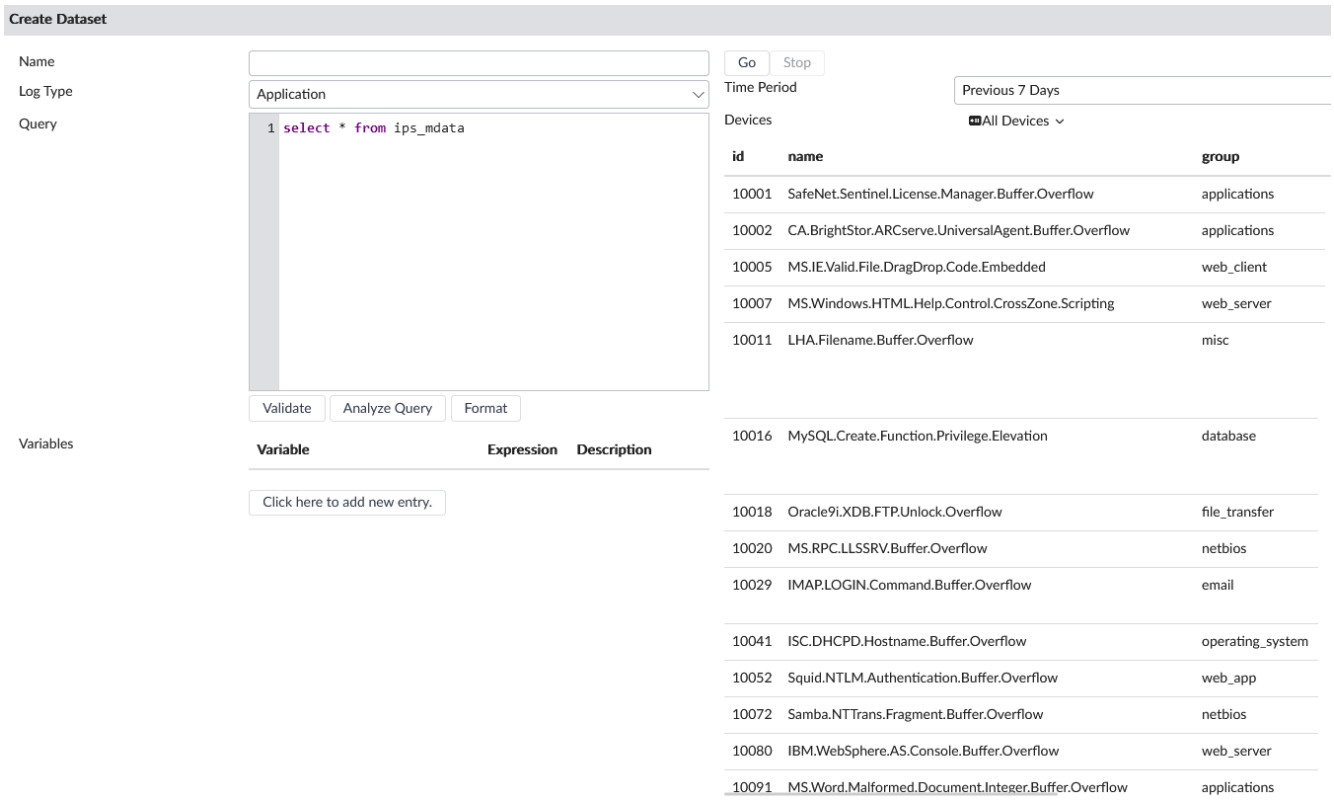
As an example, in the *threat-Top-Intrusions-By-Type* dataset, the *ips_mdata* metadata table is referenced. The *ips_mdata* table is a collection of intrusion prevention related metadata from FortiGuard that is used by this dataset to add information about vulnerability types, vulnerability names, and CVE data to intrusion prevention logs.



You can view the information contained in the metadata tables (as well as other tables) using the following custom dataset. An asterisk can be used to select all applicable fields.

```
select <field> from <table name>
```

For example, the custom dataset below displays all fields retrieved from the IPS metadata table.



Metadata tables from FortiGuard are also available to be used in custom dataset queries. The following metadata tables are available:

- ips_mdata
- app_mdata
- fct_mdata
- pci_dss_mdata
- td_threat_name_mdata

Output profiles

Output profiles allow you to define email addresses to which generated reports are sent and provide an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.

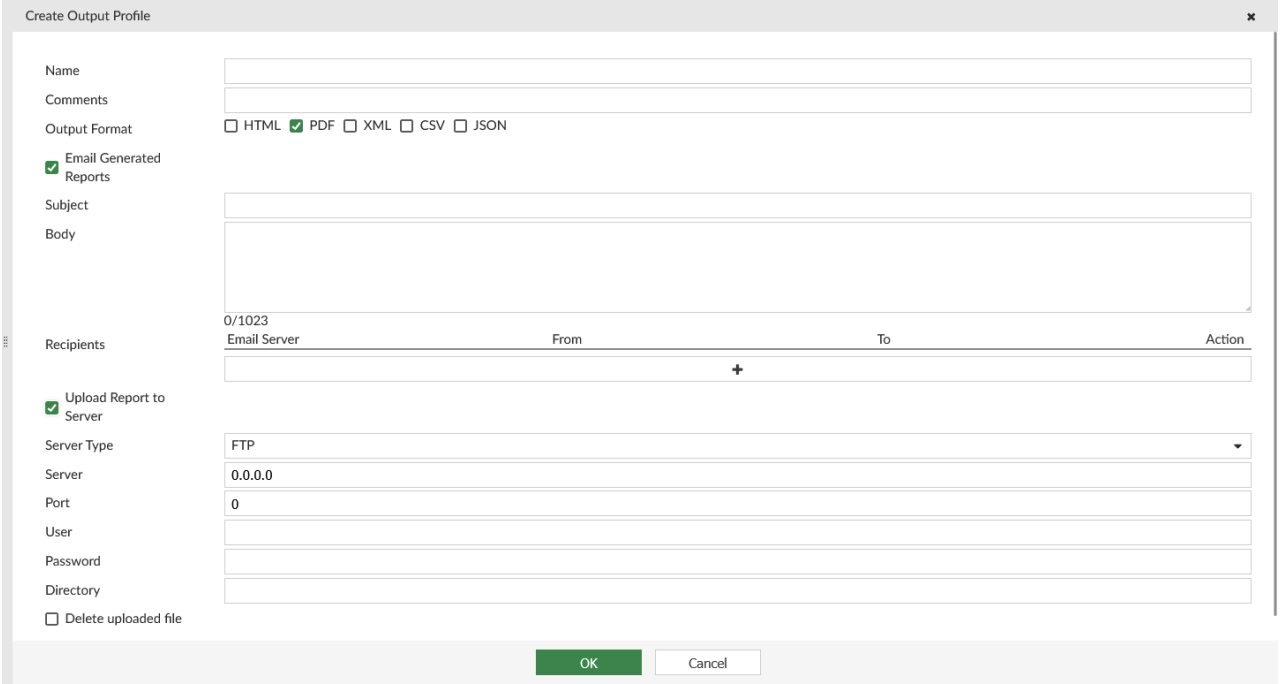
Creating output profiles



You must configure a mail server before you can configure an output profile. See Mail Server on page 537.

To create output profiles:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Advanced Settings* > *Output Profile*.
3. Click *Create New*. The *Create Output Profile* pane is displayed.



4. Provide the following information, and click *OK*:

Name	Enter a name for the new output profile.
Comments	Enter a comment about the output profile (optional).
Output Format	Select the format or formats for the generated report. You can choose *HTML*, *PDF*, *XML*, *CSV*, or *JSON* format.
Email Generated Reports	Enable emailing of generated reports.
Subject	Enter a subject for the report email.
Body	Enter body text for the report email.
Recipients	Select the email server from the dropdown list and enter to and from email addresses. Click *Add* to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading of generated reports to a server.
Server Type	Select *FTP*, *SFTP*, or *SCP* from the dropdown list.
Server	Enter the server IP address.
Port	Enter a custom port. Enter 0 or null for the default port.
User	Enter the username.
Password	Enter the password.
Directory	Specify the directory where the report will be saved.
Delete uploaded file	Select to delete the generated report after it has been uploaded to the selected server.

Managing output profiles

You can manage output profiles by going to *Reports* > *Advanced Settings* > *Output Profile*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click an output profile to display the menu.

Option	Description
Create New	Create a new output profile.
Edit	Edit the selected output profile.
Clone	Clone the selected output profile.
Delete	Delete the selected output profile.

Report languages

The languages available for reports can be found in *Reports* > *Advanced Settings* > *Language*. In this pane, you can export and import language files to be used in reports. If a custom language file is no longer needed, it can be deleted from this pane.

You can specify the language when creating a report. Select the language from the *Language* dropdown in the *Report Settings* tab. For more information, see Reports Settings tab on page 435.

This topic includes:

- Exporting and modifying a language on page 471
- Importing a language on page 472
- Deleting a language on page 472

Exporting and modifying a language

You can export a language file to modify the language or text.

Once the exported language file is modified, it can be imported to override a system language or to add a custom language.

To export and modify a language:

1. Go to *Reports* > *Advanced Settings* > *Language*.
2. Select the checkbox for a language to export.
3. From the *More* dropdown, click *Export*.
4. Extract the zip file and use a text editor to modify it.
5. Change the text after the equal sign (=) to a different language or text.
   For example, `rpt_name=[text to be changed]`. Do not change text on the left-side of the equal sign.

6. Save and zip the modified file.
   You can change the title of the language file, or you can leave the title unchanged. You will select the language name when importing the modified file.
   There should only be one language file in the zipped folder.

The language file is ready to be imported into FortiAnalyzer.

Importing a language

After exporting and modifying a language file, you can import it to use in reports.

You can override a system language with the import, or you can import a custom language.

To import a language file:

1. Go to *Reports* > *Advanced Settings* > *Language*.
2. From the *More* dropdown, click *Import*.
   The *Import Language* pane displays.
3. In the *Language File* field, drag and drop or select the zip file.
4. Select a *Language Name* from the dropdown.
   You can select a system language to override it.
5. Click *OK*.

The language is now available in the table view. The *Date Imported* column indicates when the language file was imported, and the *Status* column indicates that it is `User defined`.

The language can now be used in reports. To use this imported language, select it from the *Language* dropdown in the *Report Settings* tab. See Reports Settings tab on page 435.



If the import was to override a system language, such as `English`, the *Status* column changes from `System` to `User defined`. You can delete this row to restore the original system language. See Deleting a language on page 472.

Deleting a language

You can delete custom languages that have been imported in *Reports* > *Advanced Settings* > *Language*.

You cannot delete system languages unless they have been overridden by an import. Deleting the overridden language will restore the original system language. For example, if you imported a language file with modified text to override `English`, you can delete it to restore the system `English` language.

To delete a language:

1. Go to *Reports* > *Advanced Settings* > *Language*.
2. Select the checkbox for a language to delete.
3. Click *Delete*.

If you delete custom language, it is no longer available in the table view.

If you delete an overridden system language, the *Status* column changes from `User defined` to `System`. The original system language is restored.

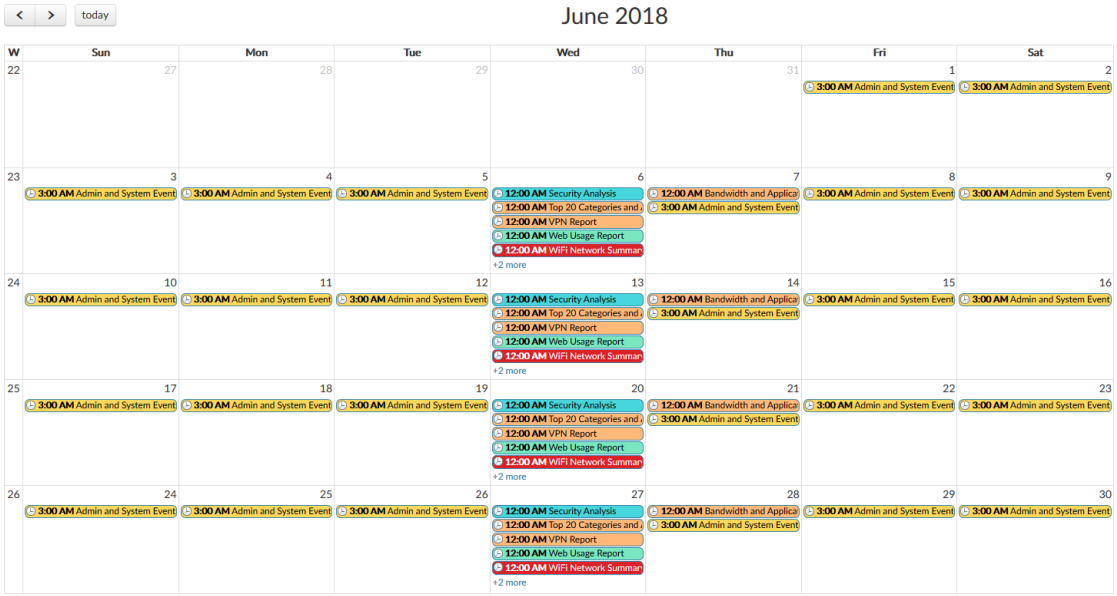
Report calendar

You can use the report calendar to view all the reports that are scheduled for the selected month. You can edit or disable upcoming report schedules, as well as delete or download completed reports.

Viewing all scheduled reports

To view all scheduled reports:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Advanced Settings* > *Report Calendar*.



3. Hover the mouse cursor over a calendar entry to display the name, status, and device type of the scheduled report.
4. Click a generated report to download it.
5. Click a scheduled report to go to the *Settings* tab of the report.
6. Click the left or right arrow at the top of the *Report Calendar* pane to change the month that is displayed. Click *Today* to return to the current month.

Managing report schedules

You can manage report schedules in *Reports* > *Advanced Settings* > *Report Calendar*.

To edit a report schedule:

1. In *Report Calendar*, right-click an upcoming calendar entry, and select *Edit*.
2. In the *Settings* tab of the report that opens, edit the corresponding report schedule.

To disable a report schedule:

In *Report Calendar*, right-click an upcoming calendar entry, and select *Disable*. All scheduled instances of the report are removed from the report calendar. Completed reports remain in the report calendar.

To delete or download a completed report:

In *Report Calendar*, right-click a past calendar entry, and select *Delete* or *Download*. The corresponding completed report will be deleted or downloaded.



You can only delete or download scheduled reports that have a *Finished* status. You cannot delete scheduled reports with a *Pending* status.

System Settings

System Settings allows you to manage system options for your FortiAnalyzer device.



Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the GUI page to access these options.

This section contains the following topics:

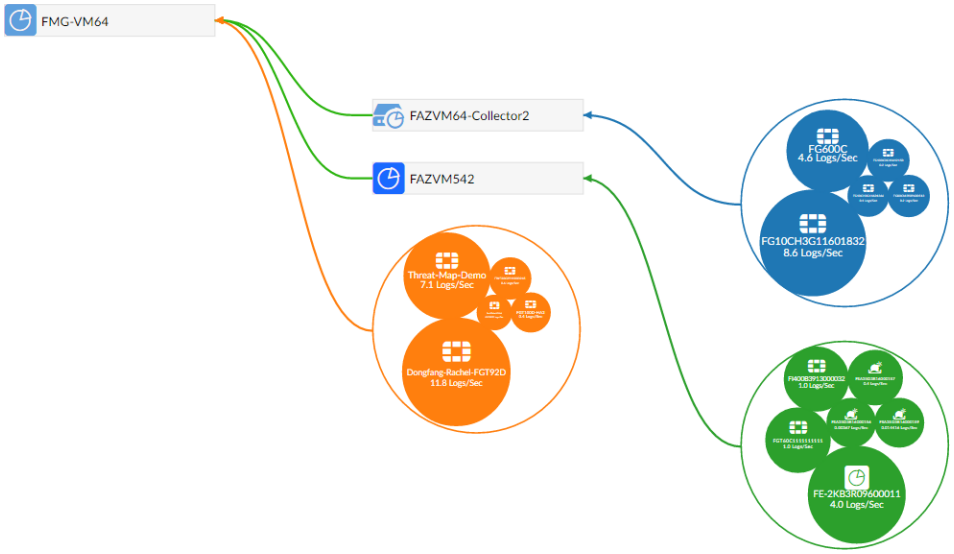
- Logging Topology on page 475
- Network on page 476
- RAID Management on page 493
- Administrative Domains (ADOMs) on page 498
- Fabric Management on page 509
- Certificates on page 511
- Log Forwarding on page 518
- Log Fetching on page 529
- Event Log on page 534
- Task Monitor on page 536
- Mail Server on page 537
- Syslog Server on page 539
- Meta Fields on page 541
- Device logs on page 542
- Miscellaneous Settings on page 547

Logging Topology

The *System Settings* > *Advanced* > *Logging Topology* pane shows the physical topology of devices in the Security Fabric. Click, hold, and drag to adjust the view in the content pane, and double-click or use the scroll wheel to change the zoom.

The visualization can be filtered to show only FortiAnalyzer devices or all devices by device count or traffic.

Hovering the cursor over a device in the visualization will show information about the device, such as the IP address and device name. Right-click on a device and select *View Related Logs* to go to the *Log View* pane, filtered for that device.



Network

The network settings are used to configure ports for the FortiAnalyzer unit. You should also specify what port and methods that an administrators can use to access the FortiAnalyzer unit. If required, static routes can be configured.

The default port for FortiAnalyzer units is port 1. It can be used to configure one IP address for the FortiAnalyzer unit, or multiple ports can be configured with multiple IP addresses for improved security.

You can configure administrative access in IPv4 or IPv6 and include settings for HTTPS, HTTP, PING, SSH, SNMP, Web Service, and FortiManager.

FortiAnalyzer supports SSHv2.

You can prevent unauthorized access to the GUI by creating administrator accounts with trusted hosts. With trusted hosts configured, the administrator can only log in to the GUI when working on a computer with the trusted host as defined in the administrator account. For more information, see Trusted hosts on page 554 and Managing administrator accounts on page 555.

Configuring network interfaces

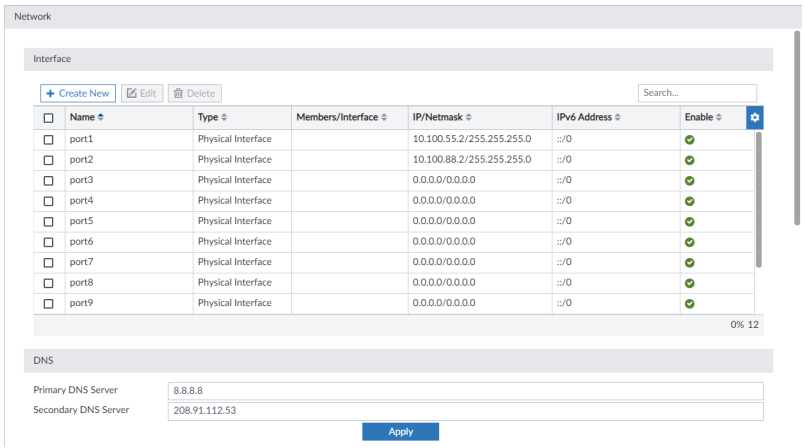
Fortinet devices can be connected to any of the FortiAnalyzer unit's interfaces. The DNS servers must be on the networks to which the FortiAnalyzer unit connects, and should have two different IP addresses.

The following port configuration is recommended:

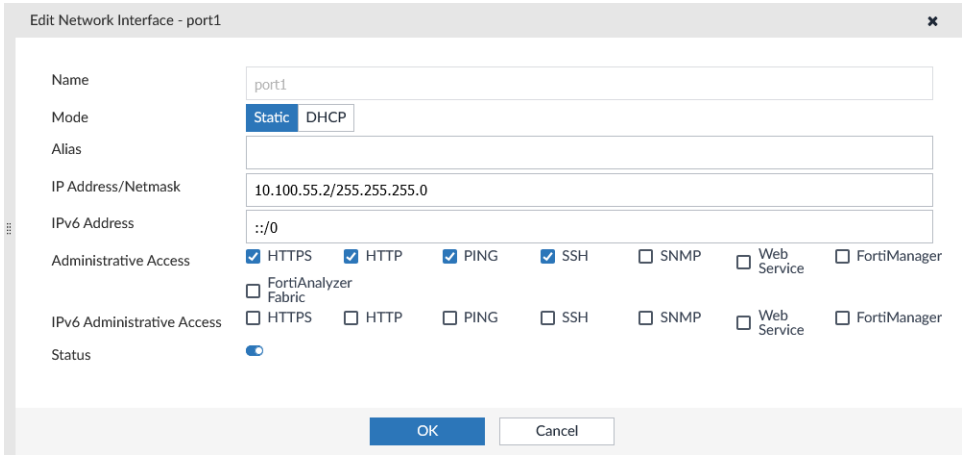
- Use port 1 for device log traffic, and disable unneeded services on it, such as SSH, Web Service, and so on.
- Use a second port for administrator access, and enable HTTPS, Web Service, and SSH for this port. Leave other services disabled.

To configure port 1:

1. Go to *System Settings* > *Network*.The *Interface* pane is displayed at the top of the page.



2. In the *Interface* pane, double-click *Port1*. The *Edit System Interface* pane is displayed.



3. Configure the following settings for *port1*, then click *OK* to apply your changes.

Name	Displays the name of the interface.
IP Address/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.

Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, Web Service, FortiManager, and FortiAnalyzer Fabric.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, SNMP, Web Service, and FortiManager.
Status	Select *Enable* or *Disable*.

4. Configure the DNS settings, and click *Apply*.

Primary DNS Server	The primary DNS server IP address.
Secondary DNS Server	The secondary DNS server IP address.

To configure additional ports:

1. Go to *System Settings* > *Network*. The *Interface* pane is displayed at the top of the page.
2. In the *Interface* pane, double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Configure the settings as required.
4. Click *OK* to apply your changes.



The port name, default gateway, and DNS servers cannot be changed from the *Edit System Interface* pane. The port can be given an alias if needed.

Disabling ports

Ports can be disabled to prevent them from accepting network traffic

To disable a port:

1. Go to *System Settings* > *Network*. The *Interface* list is displayed.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. In the *Status* field, click *Disable*
4. Click *OK* to disable the port.

Changing administrative access

Administrative access defines the protocols that can be used to connect to the FortiAnalyzer through an interface. The available options are: HTTPS, HTTP, PING, SSH, SNMP, Web Service, FortiManager, and FortiAnalyzer Fabric.

To change administrative access:

1. Go to *System Settings* > *Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Select one or more access protocols for the interface for *Administrative Access* and *IPv6 Administrator Access*, as required.
4. Click *OK* to apply your changes.

The following access protocols are available on FortiAnalyzer:

Protocol	Description when access is enabled
HTTPS `https`	Allows secure HTTPS connections to the FortiAnalyzer GUI through this interface.
HTTP `http`	Allows HTTP connections to the FortiAnalyzer GUI through this interface.
PING `ping`	The interface responds to pings. Use this setting to verify your installation and for testing.
SSH `ssh`	Allows SSH access through the interface.
SNMP `snmp`	Allows a remote SNMP manager to request SNMP information by connecting to this interface.
Web Service `webservice`	Allows FortiAnalyzer to be accessed by the XML API through the interface. The FortiManager XML API can be used to retrieve information about managed devices and perform actions such as modifying device configurations using the API.
FortiManager `fgfm`	Allows the FortiAnalyzer to be remotely managed by a FortiManager.
FortiAnalyzer Fabric `soc-fabric`	Allows FortiAnalyzer Fabric access through the interface. This access must be enabled in order for the FortiAnalyzer to join a Fabric of FortiAnalyzer as either a member or supervisor. See Fabric Management on page 509.

The following access protocols are only available to configure using the FortiAnalyzer CLI:

Protocol	Description when access is enabled
`fabric`	Allows for FortiManager and FortiAnalyzer to establish a fabric connection. This protocol must also be enabled on the FortiAnalyzer to establish the connection.
`https-logging`	Allows FortiAnalyzer to receive logs from FortiClient EMS over HTTPS. See FortiClient support and ADOMs on page 500.

Static routes

Static routes can be managed from the routing tables for IPv4 and IPv6 routes. The routing tables can be accessed by going to *System Settings* > *Network*.

To add a static route:

1. From the network routing table, click *Create New* in the toolbar. The *Create New Network Route* pane opens.
2. Select the *IP Type* as either IPv4 or IPv6.
3. Enter the destination IP address and netmask, or IPv6 prefix, and gateway in the requisite fields.
4. Select the network interface that connects to the gateway from the dropdown list. Ports, aggregate links, and VLANs are available.
5. Click *OK* to create the new static route.

To edit a static route:

1. From the network routing table: double-click on a route, right-click on a route then select *Edit* from the pop-up menu, or select a route then click *Edit* in the toolbar. The *Edit Network Route* pane opens.
2. Edit the configuration as required. The route ID cannot be changed.
3. Click *OK* to apply your changes.

To delete a static route or routes:

1. From the newtork routing table, right-click on a route then select *Delete* from the pop-up menu, or select a route or routes then click *Delete* in the toolbar.
2. Click *OK* in the confirmation dialog box to delete the selected route or routes.

Packet capture

Packets can be captured on configured interfaces by going to *System* > *Network* > *Packet Capture*.

The following information is available:

Interface	The name of the configured interface for which packets can be captured. For information on configuring an interface, see Configuring network interfaces on page 477.
Filter Criteria	The values used to filter the packet.
# Packets	The number of packets.
Maximum Packet Count	The maximum number of packets that can be captured on a sniffer.
Progress	The status of the packet capture process.
Actions	Allows you to start and stop the capturing process, and download the most recently captured packets.

To start capturing packets on an interface, select the *Start capturing* button in the *Actions* column for that interface. The *Progress* column changes to *Running*, and the *Stop capturing* and *Download* buttons become available in the *Actions* column.

To add a packet sniffer:

1. From the *Packet Capture* table, click *Create New* in the toolbar. The *Create New Sniffer* pane opens.
2. Configure the following options:

Interface	The interface name (non-changeable).
Max. Packets to Save	Enter the maximum number of packets to capture, between 1-10000. The default is 4000 packets.
Include IPv6 Packets	Select to include IPv6 packets when capturing packets.
Include Non-IP Packets	Select to include non-IP packets when capturing packets.
Enable Filters	You can filter the packet by *Host(s)*, *Port(s)*, *VLAN(s)*, and *Protocol*.

3. Click *OK*.

To download captured packets:

1. In the *Actions* column, click the *Download* button for the interface whose captured packets you want to download.
   If no packets have been captured for that interface, click the *Start capturing* button.
2. When prompted, save the packet file (*sniffer_[interface].pcap*) to your management computer.
   The file can then be opened using packet analyzer software.

To edit a packet sniffer:

1. From the *Packet Capture* table, click *Edit* in the toolbar. The *Edit Sniffer* pane opens.
2. Configure the packet sniffer options
3. Click *OK*.

Aggregate links

Link aggregation enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces.

To configure aggregate links:

1. Go to *System Settings* > *Network*.
2. In the *Interface* toolbar, click *Create New*. The *Create New Interface* page is displayed.
3. In the *Name* field, enter a name for the interface.
4. In the *Type* field, select *Aggregate*.

5. In the *Members* field, select the ports you want to include in the aggregate.
6. In the *IP Addess/Netmask* field, enter the IP address for the aggregate link.
7. In the *Administrative Access* field, select the access protocol.
8. In the *IPv6 Administrative Access* area, select the access protocol.
9. Set the *LACP Speed* to *Slow* or *Fast*.
10. In the *Minimum Links Up* field, enter the number of aggregated ports that must be up.



You must enter a minimum value of *2* for the aggregate links to work.

11. Set *Minimum Links Down* to *Operational* or *Administrative*.
12. In the *Links up Delay*, set the number of milliseconds to wait before considering the link is up.
13. Click *OK*.

To enable the interface with the GUI:

1. Go to *System Settings* > *Network*.
2. In the *Interface* pane, double-click the aggregate interface to edit it. The *Edit System Interface* window opens.
3. Set the *Status* to *Enable*.

To enable the interface with the CLI:

```
# config system interface
(interface)# edit Aggregation1
(Aggregation1)# set status up
(Aggregation1)# end
```

VLAN interfaces

You can configure a VLAN interface in FortiAnalyzer by going to *System Settings* > *Network*.

To configure a VLAN interface:

1. Go to *System Settings* > *Network*.
2. In the *Interface* toolbar, click *Create New*. The *Create New Network Interface* page is displayed.
3. In the *Name* field, enter a name for the VLAN.
4. In the *Type* field, select *VLAN*.
5. In the *VLAN ID* field, enter a VLAN ID. You can use a range between 1 and 4094.
6. In the *Interface* field, select the interface to which the VLAN will be bound.
7. In the *Protocol* field, select either *IEEE 802.1Q*. or *IEEE 802.1AD*.
8. In the *IP Address/Netmask* field, enter the IP address for the VLAN.
9. Optionally, add an *IPv6 Address*.
10. In the *Administrative Access* field, select the access protocol.

11. Optionally, configure the *IPv6 Administrative Access*.
12. In the *Service Access* field, select which services can be accessed in this VLAN.
13. In the *Status* field, select the VLAN status.
14. Click *OK*.
15. If required, you can create a static route with the VLAN interface. See Static routes on page 480.

SNMP

Enable the SNMP agent on the FortiAnalyzer device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiAnalyzer with an SNMP manager.

SNMP has two parts - the SNMP agent that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on monitored FortiGate devices are hard coded and configured by the FortiAnalyzer system - they are not user configurable.

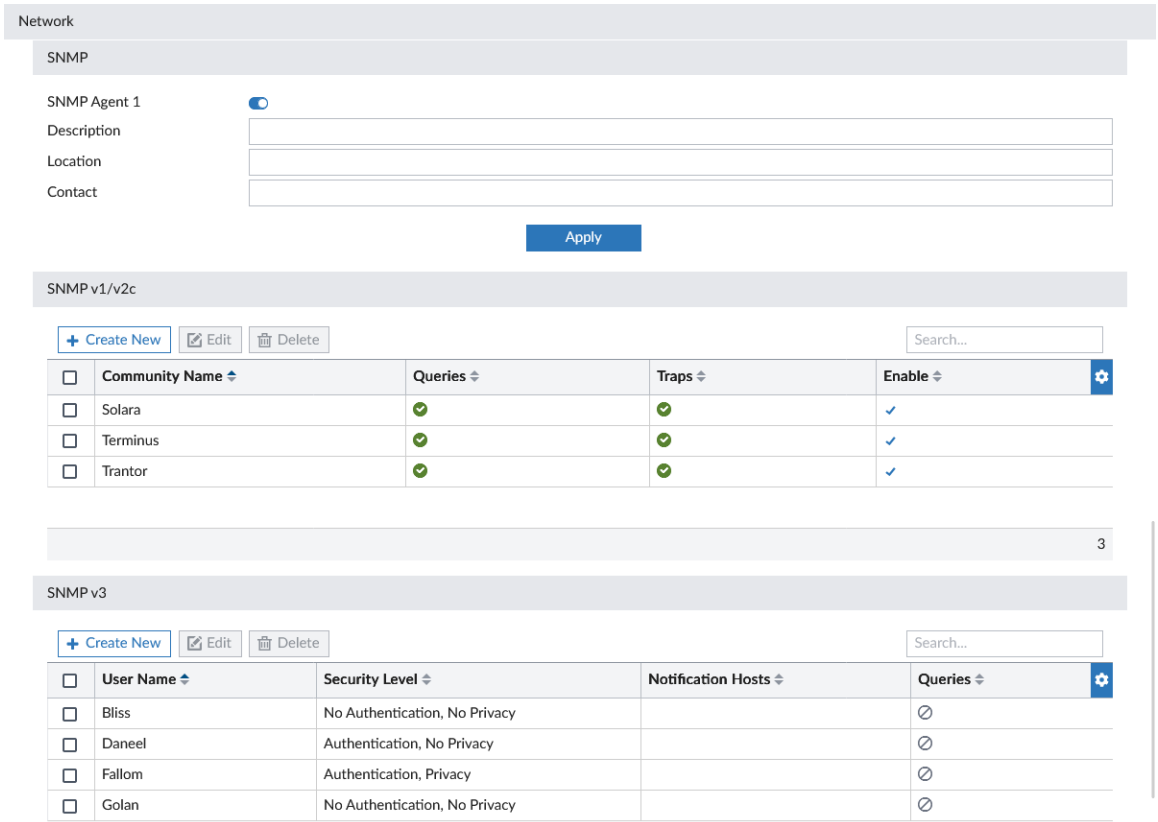
The FortiAnalyzer SNMP implementation is read-only — SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiAnalyzer system information and can receive FortiAnalyzer system traps.

SNMP agent

The SNMP agent sends SNMP traps originating on the FortiAnalyzer system to an external monitoring SNMP manager defined in a SNMP community. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiAnalyzer system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiAnalyzer system will be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiAnalyzer system requires attention.

Go to *System Settings* > *Network* and scroll to the *SNMP* section to configure the SNMP agent.



The following information and options are available:

SNMP Agent	Select to enable the SNMP agent. When this is enabled, it sends FortiAnalyzer SNMP traps.
Description	Optionally, type a description of this FortiAnalyzer system to help uniquely identify this unit.
Location	Optionally, type the location of this FortiAnalyzer system to help find it in the event it requires attention.
Contact	Optionally, type the contact information for the person in charge of this FortiAnalyzer system.
SNMP v1/2c	The list of SNMP v1/v2c communities added to the FortiAnalyzer configuration.
Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v1/v2c communities on page 485.
Edit	Edit the selected SNMP community.
Delete	Delete the selected SNMP community or communities.
Community Name	The name of the SNMP community.

	Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
	Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
	Enable	Enable or disable the SNMP community.
SNMP v3		The list of SNMPv3 users added to the configuration.
	Create New	Select *Create New* to add a new SNMP user. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v3 users on page 488.
	Edit	Edit the selected SNMP user.
	Delete	Delete the selected SNMP user or users.
	User Name	The user name for the SNMPv3 user.
	Security Level	The security level assigned to the SNMPv3 user.
	Notification Hosts	The notification host or hosts assigned to the SNMPv3 user.
	Queries	The status of SNMP queries for each SNMP user. The enabled icon indicates queries are enabled. The disabled icon indicates they are disabled.

SNMP v1/v2c communities

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiAnalyzer to belong to at least one SNMP community so that community's SNMP managers can query the FortiAnalyzer system information and receive SNMP traps from it.

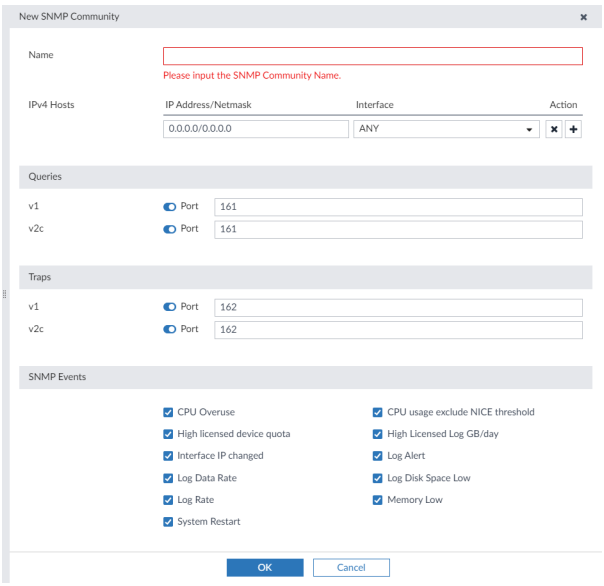


These SNMP communities do not refer to the FortiGate devices the FortiAnalyzer system is managing.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to eight hosts to each community. Hosts can receive SNMP device traps and information.

To create a new SNMP community:

1. Go to *System Settings* > *Network*.
2. In the *SNMP* section, ensure the SNMP agent is enabled.
3. In the *SNMP v1/v2c* section, click *Create New* in the toolbar. The *New SNMP Community* pane opens.



4. Configure the following options, then click *OK* to create the community.

Name		Enter a name to identify the SNMP community. This name cannot be edited later.
Hosts		The list of hosts that can use the settings in this SNMP community to monitor the FortiAnalyzer system. When you create a new SNMP community, there are no host entries. Select *Add* to create a new entry that broadcasts the SNMP traps and information to the network connected to the specified interface.
	IP Address/Netmask	Enter the IP address and netmask of an SNMP manager. By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community. Hosts configured with a /31 or larger subnet can poll SNMP but will not be sent any SNMP traps. To ensure traps are sent, configure the host with a /32 subnet (for example, `10.1.1.1/32` or `10.1.1.1/255.255.255.255`)
	Interface	Select the interface that connects to the network where this SNMP manager is located from the dropdown list. This must be done if the SNMP manager is on the Internet or behind a router.
	Delete	Click the delete icon to remove this SNMP manager entry.
	Add	Select to add another entry to the Hosts list. Up to eight SNMP manager entries can be added for a single community.

Queries	Enter the port number (161 by default) the FortiAnalyzer system uses to send v1 and v2c queries to the FortiAnalyzer in this community. Enable queries for each SNMP version that the FortiAnalyzer system uses.
Traps	Enter the remote port number (162 by default) the FortiAnalyzer system uses to send v1 and v2c traps to the FortiAnalyzer in this community. Enable traps for each SNMP version that the FortiAnalyzer system uses.
SNMP Event	Enable the events that will cause SNMP traps to be sent to the community. • *Interface IP changed* • *Log disk space low* • *CPU Overuse* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* (only available on supported hardware devices) • *Fan Speed Out of Range* • *Temperature Out of Range* • *Voltage Out of Range* • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate* FortiAnalyzer feature set SNMP events:

To edit an SNMP community:

1. Go to *System Settings > Network*.
2. In the *SNMP v1/v2c* section, double-click on a community, right-click on a community then select *Edit*, or select a community then click *Edit* in the toolbar. The *Edit SNMP Community* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP community or communities:

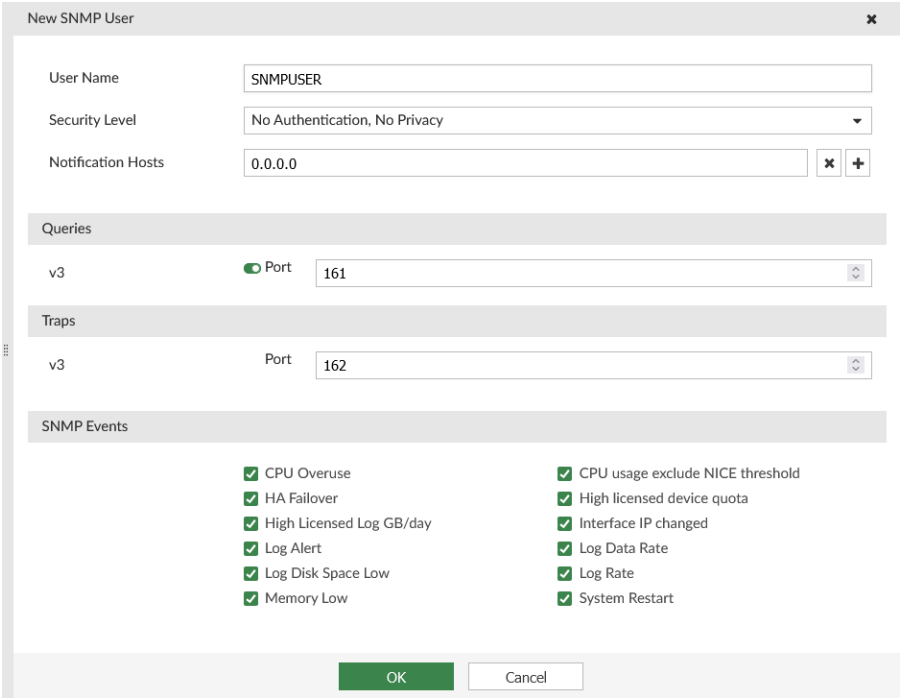
1. Go to *System Settings > Network*.
2. In the *SNMP v1/v2c* section, select the community or communities you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected community or communities.

SNMP v3 users

The FortiAnalyzer SNMP v3 implementation includes support for queries, traps, authentication, and privacy. SNMP v3 users can be created, edited, and deleted as required.

To create a new SNMP user:

1. Go to *System Settings* > *Network*.
2. In the *SNMP* section, ensure the SNMP agent is enabled.
3. In the *SNMP v3* section, click *Create New* in the toolbar. The *New SNMP User* pane opens.



4. Configure the following options, then click *OK* to create the community.

User Name	The name of the SNMP v3 user.
Security Level	The security level of the user. Select one of the following: • *No Authentication, No Privacy* • *Authentication, No Privacy*: Select the *Authentication Algorithm* (MD5, SHA, SHA224, SHA256, SHA384, SHA512) and enter the password. • *Authentication, Privacy*: Select the *Authentication Algorithm* (MD5, SHA, SHA224, SHA256, SHA384, SHA512), the *Private Algorithm* (AES, AES256, AES256CISCO, DES), and enter the passwords.
Queries	Select to enable queries then enter the port number. The default port is 161.
Traps	Configure the SNMPv3 trap remote port. The default port is 162.

Notification Hosts	The IP address or addresses of the host. Click the add icon to add multiple IP addresses.
SNMP Event	Enable the events that will cause SNMP traps to be sent to the SNMP manager. • *Interface IP changed* • *Log disk space low* • *CPU Overuse* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* (only available on supported hardware devices) • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Log Data Rate* • *Fan Speed Out of Range* • *Temperature Out of Range* • *Voltage Out of Range*

To edit an SNMP user:

1. Go to *System Settings > Network*.
2. In the *SNMP v3* section, double-click on a user, right-click on a user then select *Edit*, or select a user then click *Edit* in the toolbar. The *Edit SNMP User* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP user or users:

1. Go to *System Settings > Network*.
2. In the *SNMP v3* section, select the user or users you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected user or users.

SNMP MIBs

The Fortinet and FortiAnalyzer MIBs, along with the two RFC MIBs, can be obtained from Customer Service & Support (https://support.fortinet.com). You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib* MIB file in the firmware image file folder. The *FORTINET-CORE-MIB.mib* file is located in the main FortiAnalyzer 5.00 file folder.

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

To be able to communicate with the SNMP agent, you must include all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer. Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet and FortiAnalyzer proprietary MIBs to this database.

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiAnalyzer MIB includes system information and trap information for FortiAnalyzer units.
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception. No support for the dot3Tests and dot3Errors groups.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device type. For example FortiAnalyzer units have FortiAnalyzer specific SNMP traps. To receive Fortinet device SNMP traps, you must load and compile the FORTINET-CORE-MIB into your SNMP manager.

Traps sent include the trap message as well as the unit serial number (fnSysSerial) and host name (sysName). The Trap Message column includes the message that is included with the trap, as well as the SNMP MIB field name to help locate the information about the trap.

Event	Trap Name	Description
High Licensed Log GB/day `lic-gbday`	fmTrapLicGbDayThreshold	Indicates that the used log has exceeded the licensed GB/Day.
Log Alert `log-alert`	fmTrapLogAlert	Trap is sent when a log based alert has been triggered. Alert description included in trap.
CPU usage exclude NICE threshold	fmTrapCpuThresholdExcludeNice	Indicates that the CPU usage excluding nice processes has exceeded the threshold. This threshold can be set in the CLI using the following commands:

Event	Trap Name	Description

`cpu-high-exclude-nice`		`config system snmp sysinfo`
		`set trap-cpu-high-exclude-nice-threshold <percentage value>`
		`end`

High licensed device quota `lic-dev-quota`	fmTrapLicDevQuotaThreshold	Indicates that the used device quota has exceeded the licensed device quota.
Log Data Rate `log-data-rate`	fmTrapLogDataRateThreshold	Indicates that the incoming log data rate has exceeded the threshold. The peak data rate is calculated using the peak log rate x 512 bytes (average log size).
Log Rate `log-rate`	fmTrapLogRateThreshold	Indicates that the incoming log rate has exceeded the threshold. To determine the peak log rate, use the following CLI command: `get system loglimits`
System Restart `sys_reboot`	fmTrapPowerStateChange	Trap is sent when there is a change in the status of the power supply, if present.

CPU Overuse
`cpu_high`
	fnTrapCpuThreshold	Indicates that the CPU usage has exceeded the configured threshold.
		This threshold can be set in the CLI using the following commands:
		`config system snmp sysinfo`
		`set trap-high-cpu-threshold <percentage value>`
		`end`

Memory Low
`mem_low`
	fnTrapMemThreshold	Indicates memory usage has exceeded the configured threshold.
		This threshold can be set in the CLI using the following commands:
		`config system snmp sysinfo`
		`set trap-low-memory-threshold <percentage value>`
		`end`

Log Disk Space Low `disk_low`	fnTrapLogDiskThreshold	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Interface IP changed `intf_ip_chg`	fnTrapIpChange	Indicates that the IP address of the specified interface has been changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.

Fortinet & FortiAnalyzer MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The below tables list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the `fortinet.3.00.mib` file into your SNMP manager and browsing the Fortinet MIB fields.

System MIB fields:

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Administrator accounts:

MIB field	Description	
fnAdminNumber	The number of administrators on the Fortinet unit.	
fnAdminTable	Table of administrators.	
	fnAdminIndex	Administrator account index number.
	fnAdminName	The user name of the administrator account.
	fnAdminAddr	An address of a trusted host or subnet from which this administrator account can be used.
	fnAdminMask	The netmask for fnAdminAddr.

Custom messages:

MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

MIB fields and traps

MIB field	Description
fmModel	A table of all FortiAnalyzer models.

RAID Management

RAID helps to divide data storage over multiple disks, providing increased data reliability. For FortiAnalyzer devices containing multiple hard disks, you can configure the RAID array for capacity, performance, and/or availability.



The *RAID Management* tree menu is only available on FortiAnalyzer devices that support RAID.

Supported RAID levels

FortiAnalyzer units with multiple hard drives can support the following RAID levels:



See the FortiAnalyzer datasheet to determine your devices supported RAID levels.

Linear RAID

A Linear RAID array combines all hard disks into one large virtual disk. The total space available in this option is the capacity of all disks used. There is very little performance change when using this RAID format. If any of the drives fails, the entire set of drives is unusable until the faulty drive is replaced. All data will be lost.

RAID 0

A RAID 0 array is also referred to as striping. The FortiAnalyzer unit writes information evenly across all hard disks. The total space available is that of all the disks in the RAID array. There is no redundancy available. If any single drive fails, the data on that drive cannot be recovered. This RAID level is beneficial because it provides better performance, since the FortiAnalyzer unit can distribute disk writing across multiple disks.

- Minimum number of drives: 2
- Data protection: No protection



RAID 0 is not recommended for mission critical environments as it is not fault-tolerant.

RAID 1

A RAID 1 array is also referred to as mirroring. The FortiAnalyzer unit writes information to one hard disk, and writes a copy (a mirror image) of all information to all other hard disks. The total disk space available is that of only one hard disk, as the others are solely used for mirroring. This provides redundant data storage with no single point of failure. Should any of the hard disks fail, there are backup hard disks available.

- Minimum number of drives: 2
- Data protection: Single-drive failure



One write or two reads are possible per mirrored pair. RAID 1 offers redundancy of data. A re-build is not required in the event of a drive failure. This is the simplest RAID storage design with the highest disk overhead.

RAID 1s

A RAID 1 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure the hot spare is substituted for the failed drive, integrating it into the RAID array and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 5

A RAID 5 array employs striping with a parity check. Similar to RAID 0, the FortiAnalyzer unit writes information evenly across all drives but additional parity blocks are written on the same stripes. The parity block is staggered for each stripe. The total disk space is the total number of disks in the array, minus one disk for parity storage. For example, with four hard disks, the total capacity available is actually the total for three hard disks. RAID 5 performance is typically better with reading than with writing, although performance is degraded when one disk has failed or is missing. With RAID 5, one disk can fail without the loss of data. If a drive fails, it can be replaced and the FortiAnalyzer unit will restore the data on the new disk by using reference information from the parity volume.

- Minimum number of drives: 3
- Data protection: Single-drive failure

RAID 5s

A RAID 5 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure, the hot spare is substituted for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 6

A RAID 6 array is the same as a RAID 5 array with an additional parity block. It uses block-level striping with two parity blocks distributed across all member disks.

- Minimum number of drives: 4
- Data protection: Up to two disk failures.

RAID 6s

A RAID 6 with hot spare array is the same as a RAID 5 with hot spare array with an additional parity block.

RAID 10

RAID 10 (or 1+0), includes nested RAID levels 1 and 0, or a stripe (RAID 0) of mirrors (RAID 1). The total disk space available is the total number of disks in the array (a minimum of 4) divided by 2, for example:

- 2 RAID 1 arrays of two disks each,
- 3 RAID 1 arrays of two disks each,
- 6 RAID1 arrays of two disks each.

One drive from a RAID 1 array can fail without the loss of data; however, should the other drive in the RAID 1 array fail, all data will be lost. In this situation, it is important to replace a failed drive as quickly as possible.

- Minimum number of drives: 4
- Data protection: Up to two disk failures in each sub-array.



Alternative to RAID 1 when additional performance is required.

RAID 50

RAID 50 (or 5+0) includes nested RAID levels 5 and 0, or a stripe (RAID 0) and stripe with parity (RAID 5). The total disk space available is the total number of disks minus the number of RAID 5 sub-arrays. RAID 50 provides increased performance and also ensures no data loss for the same reasons as RAID 5. One drive in each RAID 5 array can fail without the loss of data.

- Minimum number of drives: 6
- Data protection: Up to one disk failure in each sub-array.



Higher fault tolerance than RAID 5 and higher efficiency than RAID 0.



RAID 50 is only available on models with 9 or more disks. By default, two groups are used unless otherwise configured via the CLI. Use the `diagnose system raid status` CLI command to view your current RAID level, status, size, groups, and hard disk drive information.

RAID 60

A RAID 60 (6+ 0) array combines the straight, block-level striping of RAID 0 with the distributed double parity of RAID 6.

- Minimum number of drives: 8
- Data protection: Up to two disk failures in each sub-array.

High read data transaction rate, medium write data transaction rate, and slightly lower performance than RAID 50.

Configuring the RAID level

Changing the RAID level will delete all data.

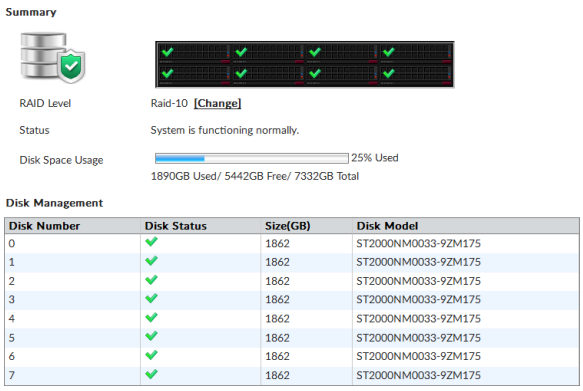
To configure the RAID level:

1. Go to *System Settings* > *RAID Management*.
2. Click *Change* in the *RAID Level* field. The *RAID Settings* dialog box is displayed.
3. From the *RAID Level* list, select a new RAID level, then click *OK*.
   The FortiAnalyzer unit reboots. Depending on the selected RAID level, it may take a significant amount of time to generate the RAID array.

Monitoring RAID status

To view the RAID status, go to *System Settings* > *RAID Management*. The RAID Management pane displays the RAID level, status, and disk space usage. It also shows the status, size, and model of each disk in the RAID array.

The *Alert Message Console* widget, located in *Dashboards* > *Status*, provides detailed information about RAID array failures. For more information see Alert Messages Console widget on page 72.



Summary	Shows summary information about the RAID array.

	Graphic	Displays the position and status of each disk in the RAID array. Hover the cursor over each disk to view details.
	RAID Level	Displays the selected RAID level. Click *Change* to change the selected RAID level. When you change the RAID settings, all data is deleted.
	Status	Displays the overall status of the RAID array.
	Disk Space Usage	Displays the total size of the disk space, how much disk space is used, and how much disk space is free.
Disk Management		Shows information about each disk in the RAID array.
	Disk Number	Identifies the disk number for each disk.
	Disk Status	Displays the status of each disk in the RAID array. • *Ready*: The hard drive is functioning normally. • *Rebuilding*: The FortiAnalyzer unit is writing data to a newly added hard drive in order to restore the hard drive to an optimal state. The FortiAnalyzer unit is not fully fault tolerant until rebuilding is complete. • *Initializing*: The FortiAnalyzer unit is writing to all the hard drives in the device in order to make the array fault tolerant. • *Verifying*: The FortiAnalyzer unit is ensuring that the parity data of a redundant drive is valid. • *Degraded*: The hard drive is no longer being used by the RAID controller. • *Inoperable*: One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system. Data on an inoperable drive cannot be accessed.
	Size (GB)	Displays the size, in GB, of each disk.
	Disk Model	Displays the model number of each disk.

Swapping hard disks

If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running - known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget. See Alert Messages Console widget on page 72.



Electrostatic discharge (ESD) can damage FortiAnalyzer equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiAnalyzer chassis.



When replacing a hard disk, you need to first verify that the new disk is the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiAnalyzer unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.

The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

To hot swap a hard disk on a device that supports hardware RAID:

1. Remove the faulty hard disk.
2. Install a new disk.
   The FortiAnalyzer unit automatically adds the new disk to the current RAID array. The status appears on the console. The *RAID Management* pane displays a green checkmark icon for all disks and the *RAID Status* area displays the progress of the RAID re-synchronization/rebuild.

Adding hard disks

Some FortiAnalyzer units have space to add more hard disks to increase your storage capacity.



Fortinet recommends you use the same disks as those supplied by Fortinet. Disks of other brands will not be supported by Fortinet. For information on purchasing extra hard disks, contact your Fortinet reseller.

To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiAnalyzer unit.
   You can also migrate the data to another FortiAnalyzer unit, if you have one. Data migration reduces system down time and the risk of data loss.
3. Install the disks in the FortiAnalyzer unit.
   If your unit supports hot swapping, you can do so while the unit is running. Otherwise the unit must be shut down first. See Unit Operation widget on page 71 for information.
4. Configure the RAID level. See Configuring the RAID level on page 496.
5. If you backed up the log data, restore it.

Administrative Domains (ADOMs)

Administrative domains (ADOMs) enable administrators to manage only those devices that they are specifically assigned, based on the ADOMs to which they have access. When the ADOM mode is advanced, FortiGate

devices with multiple VDOMs can be divided among multiple ADOMs.

Administrator accounts can be tied to one or more ADOMs, or denied access to specific ADOMs. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. Super user administrator accounts, such as the `admin` account, can see and maintain all ADOMs and the devices within them.

Each ADOM specifies how long to store and how much disk space to use for its logs. You can monitor disk utilization for each ADOM and adjust storage settings for logs as needed.

The maximum number of ADOMs you can add depends on the FortiAnalyzer system model. Please refer to the FortiAnalyzer data sheet for more information.

When the maximum number of ADOMs has been reached, you will be unable to create a new ADOM.

When upgrading to FortiAnalyzer 6.2.1 or later, you will continue to have access to any ADOMs exceeding the limit, however, no additional ADOMs can be created, and an alert will be issued in the *Alert Message Console* in *Dashboards* > *Status*.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by administrators with the *Super_User* profile. See Administrators on page 554.

The root ADOM and Security Fabric ADOMs are available for visibility into all Fabric devices. See Security Fabric ADOMs on page 199.



Non-FortiGate devices are automatically located in specific ADOMs for their device type. They cannot be moved to other ADOMs, except for FortiClient devices, which can be promoted to Fabric ADOMs if needed.



ADOMs must be enabled to support the logging and reporting of non-FortiGate devices.

Root ADOM

When ADOMs are enabled, the default *root ADOM* type is *Fabric*. Fabric ADOMs show combined results from all Security Fabric devices in the *Device Manager*, *Log View*, *FortiView*, *Incidents & Events* and *Reports* panes. For more information on Fabric ADOMs, see Security Fabric ADOMs on page 199.

In FortiAnalyzer 6.2.0 and earlier, the root ADOM is a *FortiGate* ADOM. When upgrading to FortiAnalyzer 6.2.1 and later, the root ADOM type will *not* be changed to *Fabric*. Resetting the FortiAnalyzer settings through a factory reset will cause the root ADOM to become a Fabric ADOM.

Default device type ADOMs

When ADOMs are enabled, FortiAnalyzer includes default ADOMs for specific types of devices. When you add one or more of these devices to FortiAnalyzer, the devices are automatically added to the appropriate ADOM, and the ADOM becomes selectable. When a default ADOM contains no devices, the ADOM is not selectable.

For example, when you add a FortiClient EMS device to the FortiAnalyzer, the FortiClient EMS device is automatically added to the default FortiClient ADOM. After the FortiClient ADOM contains a FortiClient EMS device, the FortiClient ADOM is selectable when you log into FortiAnalyzer or when you switch between ADOMs.

You can view all of the ADOMs, including default ADOMs without devices, on the *System Settings > ADOMs* pane.

Organizing devices into ADOMs

You can organize devices into ADOMs to allow you to better manage these devices. Devices can be organized by whatever method you deem appropriate, for example:

- Firmware version: group all devices with the same firmware version into an ADOM.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a different region into another ADOM.
- Administrative users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.

FortiClient support and ADOMs

FortiClient logs are stored in the device that the FortiClient endpoint is registered to.

For example, when endpoints are registered to a FortiGate device, FortiClient logs are viewed on the FortiGate device. When endpoints are registered to a FortiClient EMS, FortiClient logs are viewed in the FortiClient ADOM that the FortiClient EMS device is added to.

ADOMs must be enabled to support FortiClient EMS devices.

Merge FortiAnalyzer Logging Support for FortiClient EMS for Chromebooks

1. Add `https-logging` to the `allowaccess` list using the following CLI command:
```
config system interface
   edit "port1"
      set allowaccess https ssh https-logging
   next
end
```
2. Add SSL certificate to enable communication.
   An SSL certificate is required to support communication and send logs between FortiClient Web Filter extension and FortiAnalyzer. If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer.
   However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiAnalyzer, and you must push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient EMS Chromebook Web Filter extension and FortiAnalyzer will not work. The common name of the certificate must be the FortiAnalyzer IP address.

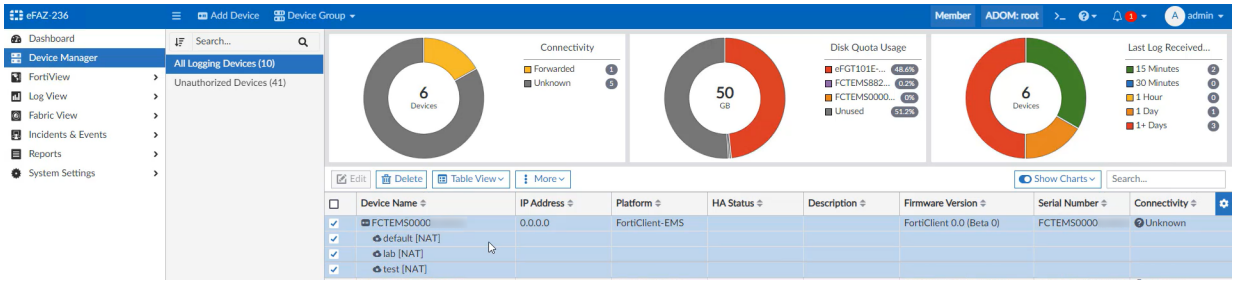
a. In FortiAnalyzer, go to *System Settings* > *Certificates*.
b. Click *Create New/Import* > *Certificate*. The *Import Local Certificate* dialog box appears.
c. In the *Type* list, select *Certificate*. Or,
In the *Type* list, select *PKCS#12 Certificate* to upload the certificate in PK12 format.
d. Beside the *Certificate File* field, click *Browse* to select the certificate.
e. Enter the *password* and *certificate name*.
f. Click *OK*.

3. Select certificates for HTTPS connections:
a. In FortiAnalyzer, go to *System Settings* > *Settings*.
b. In the *HTTPS & Web Service Certificate* box, select the certificate you want to use for HTTPS connections, and click *Apply*.
4. Enable the FortiClient ADOM using the following CLI command:
```
conf sys global
   set adom-status enable
end
```
5. Add FortiClient EMS for Chromebooks as a device to the FortiClient ADOM:
Go to *Device Manager* > *click the + Add Device button* to add FortiClient EMS for Chromebooks as a FortiClient ADOM device.
6. Enable logging in FortiClient EMS for Chromebooks:
You will need to enable logging in FortiClient EMS for Chromebooks, see the *FortiClient EMS for Chromebooks Administration Guide* for more information.

FortiClient EMS multitenancy support in FortiAnalyzer

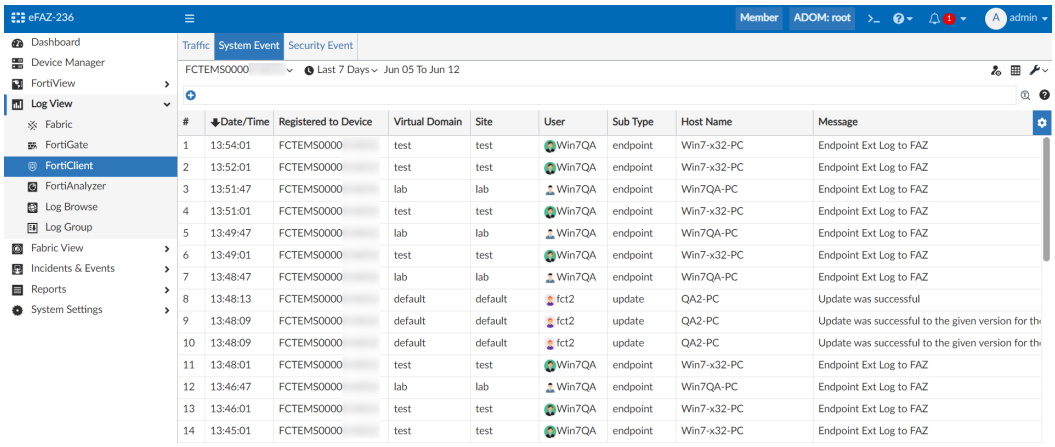
With FortiClient EMS multitenancy, you can create multiple sites to provide granular access to different sites and to separate endpoint data and configurations.

On FortiAnalyzer, the FortiClient EMS device can be authorized to Fabric or FortiClient ADOM, as needed. When sites are configured as part of multitenancy, they will be nested under the device in *Device Manager* on FortiAnalyzer. For example, see below.

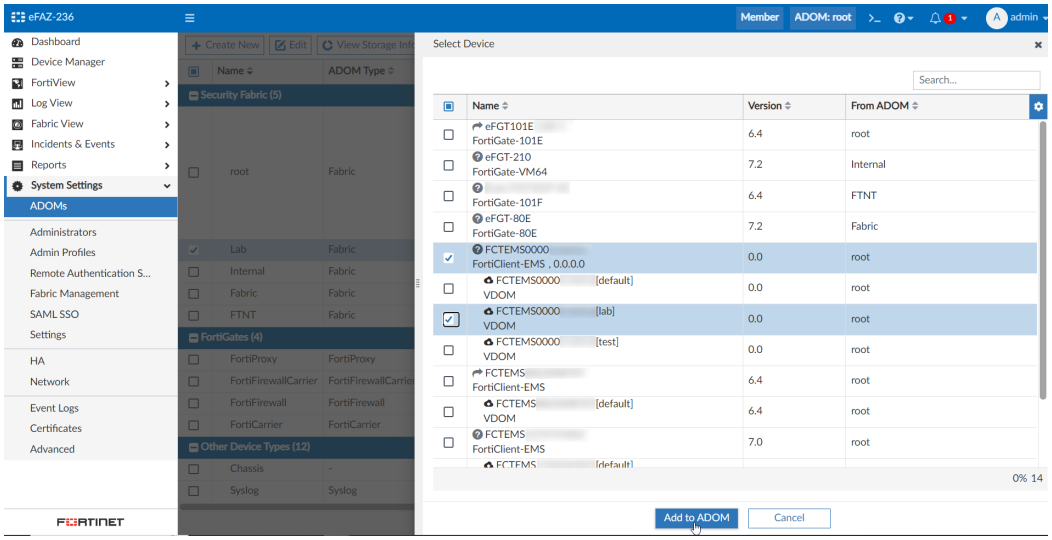


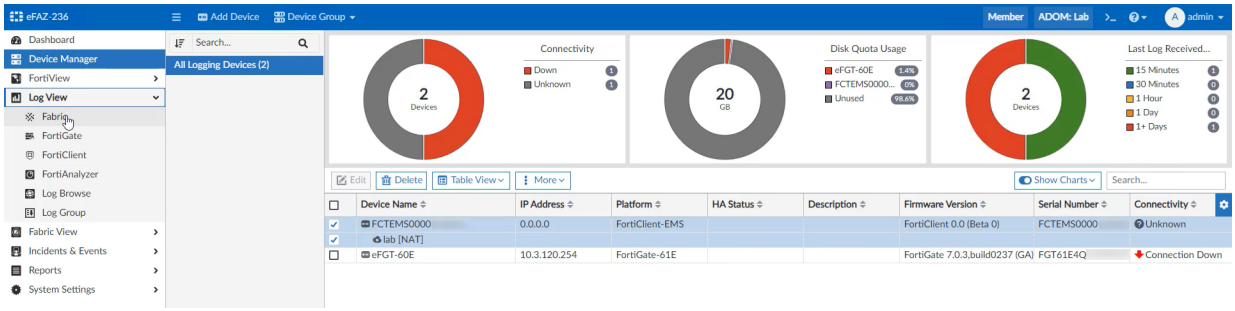
In *Log View* > *FortiClient*, multitenancy logs can be identified using the following two columns:

- *Registered to Device* = the FortiClient device
- *Virtual Domain* = the site name



When the *ADOM Mode* is set to *Advanced*, the sites can be assigned to different ADOMs, as needed. For example, see below. The lab site (VDOM) is assigned to the Lab ADOM in FortiAnalyzer. To set ADOM Mode to advanced, see ADOM device modes on page 503.





Enabling and disabling the ADOM feature

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by super user administrators.

When ADOMs are enabled, the *Device Manager*, *FortiView*, *Log View*, *Incidents & Events*, and *Reports* panes are displayed per ADOM. You select the ADOM you need to work in when you log into the FortiAnalyzer unit. See Switching between ADOMs on page 34.



ADOMs must be enabled to support FortiMail and FortiWeb logging and reporting. When a FortiMail or FortiWeb device is authorized, the device is added to the respective default ADOM and is visible in the left-hand tree menu.



FortiGate and FortiCarrier devices cannot be grouped into the same ADOM. FortiCarrier devices are added to a specific default FortiCarrier ADOM.

To enable the ADOM feature:

1. Log in to the FortiAnalyzer as a super user administrator.
2. Go to *Dashboards* > *Status*.
3. In the *System Information* widget, toggle the *Administrative Domain* switch to *ON*.
   You will be automatically logged out of the FortiAnalyzer and returned to the log in screen.

To disable the ADOM feature:

1. Remove all the devices from all non-root ADOMs. That is, add all devices to the root ADOM.
2. Delete all non-root ADOMs. See Deleting ADOMs on page 509.
   Only after removing all the non-root ADOMs can ADOMs be disabled.
3. Go to *Dashboard*.
4. In the *System Information* widget, toggle the *Administrative Domain* switch to *OFF*.
   You will be automatically logged out of the FortiAnalyzer and returned to the log in screen.



The ADOMs feature cannot be disabled if ADOMs are still configured and have managed devices in them.

ADOM device modes

ADOM deployment can have two device modes: *Normal* (default) and *Advanced*.

- In *Normal* mode, you cannot assign different FortiGate VDOMs to different ADOMs. The FortiGate unit can only be added to a single ADOM.
- In *Advanced* mode, you can assign a VDOM from a single device to a different ADOM. This allows you to analyze data for individual VDOMs, but will result in more complicated management scenarios. It is recommended only for advanced users.

FortiAnalyzer does not support splitting FortiGate VDOMs between multiple ADOMs in different ADOM modes (normal/backup).

To change from *Advanced* mode back to *Normal* mode, you must ensure no FortiGate VDOMs are assigned to an ADOM.

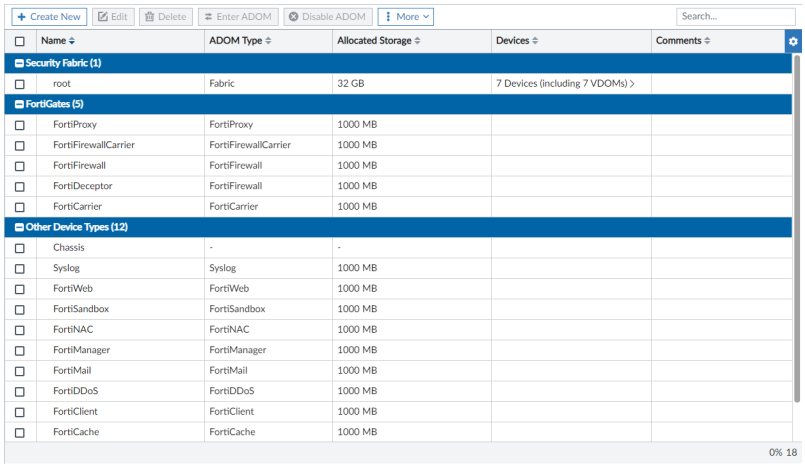
To change the ADOM device mode:

1. Go to *System Settings* > *Advanced* > *Misc Settings*.
2. In the *ADOM Mode* field, select either *Normal* or *Advanced*.
3. Select *Apply* to apply your changes.

Managing ADOMs

The ADOMs feature must be enabled before ADOMs can be created or configured. See Enabling and disabling the ADOM feature on page 502.

To create and manage ADOMs, go to *System Settings* > *ADOMs*.



Create New	Create a new ADOM. See Creating ADOMs on page 505.
Edit	Edit the selected ADOM. This option is also available from the right-click menu. See Editing an ADOM on page 508.
Delete	Delete the selected ADOM or ADOMs. You cannot delete default ADOMs. This option is also available from the right-click menu. See Deleting ADOMs on page 509.
Enter ADOM	Switch to the selected ADOM. This option is also available from the right-click menu.
Disable ADOM	Disable the selected ADOM. This option is also available from the right-click menu.

More	Select *Expand Devices* to expand all of the ADOMs to show the devices in each ADOM. Select *Collapse Devices* to collapses the device lists. Some of these options are also available from the right-click menu.
Search	Enter a search term to search the ADOM list.
Name	The name of the ADOM. ADOMs are listed in the following groups: *Security Fabric*, *FortiGates* and *Other Device Types*. A group can be collapsed or expanded by clicking the triangle next to its name.
Firmware Version	The firmware version of the ADOM. Devices in the ADOM should have the same firmware version.
Devices	The number of devices and VDOMs that the ADOM contains. The device list can be expanded or by clicking the triangle.

Creating ADOMs

ADOMs must be enabled, and you must be logged in as a super user administrator to create a new ADOM.

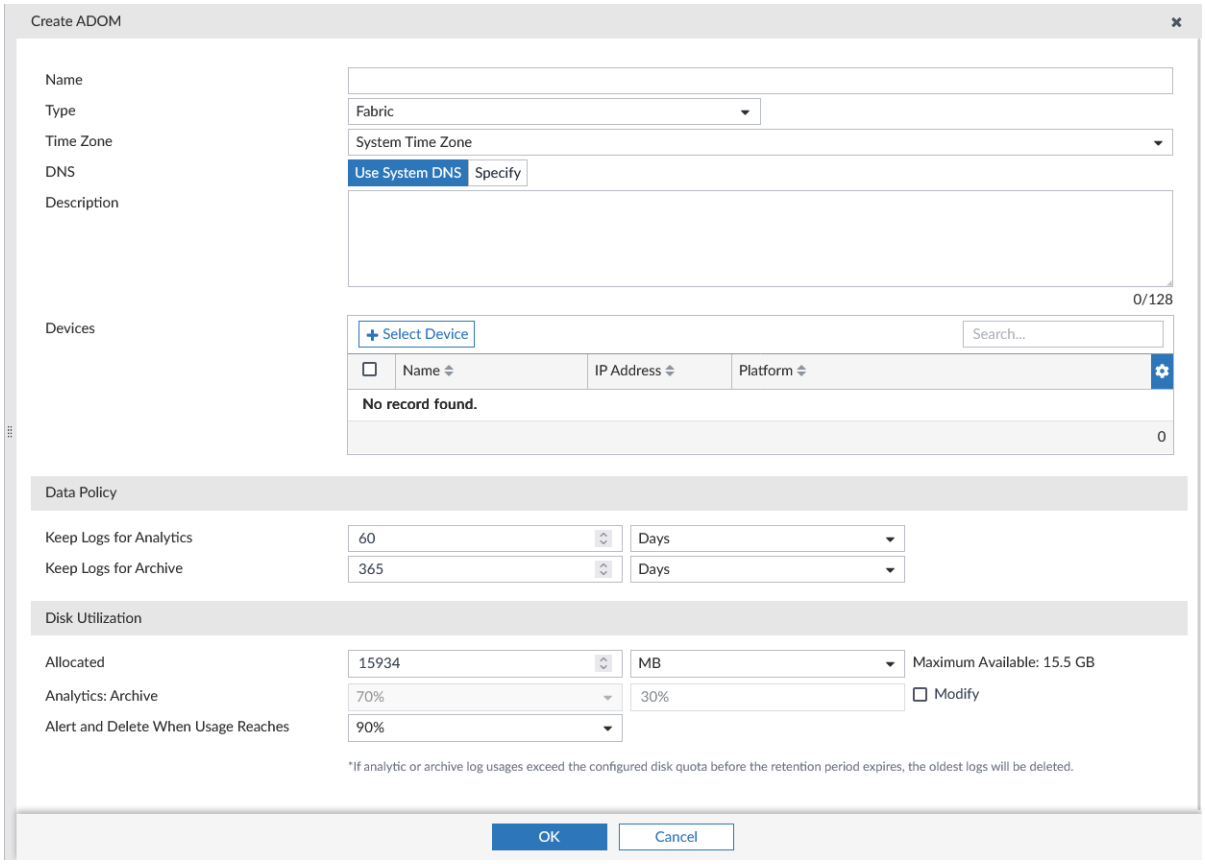
Consider the following when creating ADOMs:

- The maximum number of ADOMs that can be created depends on the FortiAnalyzer model. For more information, see the FortiAnalyzer data sheet at https://www.fortinet.com/products/management/fortianalyzer.html.
  When the maximum number of ADOMs has been exceeded, an alert will be issued in the *Alert Message Console* in *Dashboards* > *Status*.
- You must use an administrator account that is assigned the *Super_User* administrative profile.
- You can add a device to only one ADOM. You cannot add a device to multiple ADOMs.
- You cannot add FortiGate and FortiCarrier devices to the same ADOM. FortiCarrier devices are added to a specific, default FortiCarrier ADOM.
- You can add one or more VDOMs from a FortiGate device to one ADOM. If you want to add individual VDOMs from a FortiGate device to different ADOMs, you must first enable advanced device mode. See ADOM device modes on page 503.
- You can configure how an ADOM handles log files from its devices. For example, you can configure how much disk space an ADOM can use for logs, and then monitor how much of the allotted disk space is used. You can also specify how long to keep logs in the SQL database and how long to keep logs stored in compressed format.

To create an ADOM:

1. Ensure that ADOMs are enabled. See Enabling and disabling the ADOM feature on page 502.
2. Go to *System Settings* > *ADOMs*.

3. Click *Create New* in the toolbar. The *Create New ADOM* pane is displayed.



4. Configure the following settings, then click *OK* to create the ADOM.

Name	Type a name that allows you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
Type	Select the type of device that you are creating an ADOM for. The ADOM type cannot be edited. For Security Fabric ADOMs, select *Fabric*. Although you can create a different ADOM for each type of device, FortiAnalyzer does not enforce this setting.
Time Zone	Select the time zone for the ADOM. This time zone will be used when displaying data in *Log View* and *FortiView*. The *Default* time zone is the time zone set for the FortiAnalyzer. For more information, see Configuring the system time on page 53.
DNS	Select *Use System DNS* or specify a unique DNS server for the ADOM. When a unique DNS server is specified for the ADOM, all the resolution of IP address to hostnames in the ADOM are queried to the specified DNS server instead of the system DNS server in *Log View*, *FortiView*, *Reports*, and so on. To configure the system DNS, see Configuring network interfaces on page 477.

Devices		Add a device or devices with the selected versions to the ADOM. The search field can be used to find specific devices. See Assigning devices to an ADOM on page 507.
Data Policy		Specify how long to keep logs in the indexed and compressed states.
	Keep Logs for Analytics	Specify how long to keep logs in the indexed state. During the indexed state, logs are indexed in the SQL database for the specified amount of time. Information about the logs can be viewed in the *FortiView*, *Incidents & Events*, and *Reports* modules. After the specified length of time expires, Analytics logs are automatically purged from the SQL database.
	Keep Logs for Archive	Specify how long to keep logs in the compressed state. During the compressed state, logs are stored in a compressed format on the FortiAnalyzer unit. When logs are in the compressed state, information about the log messages cannot be viewed in the *FortiView*, *Incidents & Events*, or *Reports* modules. After the specified length of time expires, Archive logs are automatically deleted from the FortiAnalyzer unit.
Disk Utilization		Specify how much disk space to use for logs.
	Maximum Allowed	Specify the maximum amount of FortiAnalyzer disk space to use for logs, and select the unit of measure. The total available space on the FortiAnalyzer unit is shown. For more information about the maximum available space for each FortiAnalyzer unit, see Disk space allocation on page 170.
	Analytics : Archive	Specify the percentage of the allotted space to use for Analytics and Archive logs. Analytics logs require more space than Archive logs. For example, a setting of 70% and 30% indicates that 70% of the allotted disk space will be used for Analytics logs, and 30% of the allotted space will be used for Archive logs. Select the *Modify* checkbox to change the setting.
	Alert and Delete When Usage Reaches	Specify at what data usage percentage an alert messages will be generated and logs will be automatically deleted. The oldest Archive log files or Analytics database tables are deleted first.

Assigning devices to an ADOM

To assign devices to an ADOM you must be logged in as a super user administrator. Devices cannot be assigned to multiple ADOMs.

To assign devices to an ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select the *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Click *Select Device*. The *Select Device* list opens on the right side of the screen.

4. Select the devices that you want to add to the ADOM. Only devices with the same version as the ADOM can be added. The selected devices are displayed in the *Devices* list.
   If the ADOM mode is *Advanced* you can add separate VDOMs to the ADOM as well as units.
5. When done selecting devices, click *Close* to close the *Select Device* list.
6. Click *OK*.
   The selected devices are removed from their previous ADOM and added to this one.

Assigning administrators to an ADOM

Super user administrators can create other administrators and either assign ADOMs to their account or exclude them from specific ADOMs, constraining them to configurations and data that apply only to devices in the ADOMs they can access.



By default, when ADOMs are enabled, existing administrator accounts other than *admin* are assigned to the *root* domain, which contains all devices in the device list. For more information about creating other ADOMs, see Creating ADOMs on page 505.

To assign an administrator to specific ADOMs:

1. Log in as a super user administrator. Other types of administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings* > *Administrators*.
3. Double-click on an administrator, right-click on an administrator and then select the *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
4. Edit the *Administrative Domain* field as required, either assigning or excluding specific ADOMs.
5. Select *OK* to apply your changes.



The *admin* administrator account cannot be restricted to specific ADOMs.

Editing an ADOM

To edit an ADOM you must be logged in as a super user administrator. The ADOM type and version cannot be edited. For the default ADOMs, the name cannot be edited.

To edit an ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting ADOMs

To delete an ADOM, you must be logged in as a super-user administrator (see Administrator profiles on page 566), such as the *admin* administrator.

Prior to deleting an ADOM:

- All devices must be removed from the ADOM. Devices can be moved to another ADOM, or to the root ADOM. See Assigning devices to an ADOM on page 507.

To delete an ADOM:

1. Go to *System Settings* > *ADOMs*.
2. Ensure that the ADOM or ADOMs being deleted have no devices in them.
3. Select the ADOM or ADOMs you need to delete.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
5. Click *OK* in the confirmation box to delete the ADOM or ADOMs.
6. If there are users or policy packages referring to the ADOM, they are displayed in the *ADOM References Detected* dialog. Click *Delete Anyway* to delete the ADOM or ADOMs. The references to the ADOMs are also deleted.



Default ADOMs cannot be deleted.

Fabric Management

In *System Settings* > *Fabric Management*, you can create and manage a FortiAnalyzer Fabric and storage connectors.

Use the FortiAnalyzer Fabric tab to create or join a FortiAnalyzer Fabric. For more information, see the FortiAnalyzer Fabric Deployment Guide.

Use the *Fabric Connectors* tab to create storage connectors.

Storage connectors

You can use the *Fabric Connectors* tab to create the following types of storage connectors:

- Amazon S3
- Azure Blob Container
- Google Cloud Storage

Creating or editing storage connectors

You can create storage connectors for Amazon S3, Azure Blob, and Google Cloud. Once you have created a storage connector, you can upload FortiAnalyzer logs to cloud storage. You must also import the CA certificate from the cloud service provider. See Upload logs to cloud storage on page 546

To create a storage connector:

1. Go to *Fabric View* > *Fabric Connectors*, and click *Create New*.
2. Under *Storage*, click *Amazon S3*, *Azure Blob*, or *Google*, and click *Next*.
3. Configure the following options, and click *OK*.

Property		Description
Name		Type a name for the fabric connector.
Description		(Optional) Add a description for the fabric connector.
Title		Type a title for the fabric connector.
Status		Toggle *On* to enable the fabric connector. Toggle *Off* to disable the fabric connector.
Amazon S3	Provider	Type AWS.
	Region	Select a region.
	Access Key ID	Paste the access key from the IAM user account.
	Secret Access Key	Paste the secret access key from the IAM user account. Click the eye icon to Show or Hide the key.
Azure Blob	Storage Account Name	Paste the storage account name from the Microsoft Azure account.
	Account Key	Paste the account key from the Microsoft Azure account.
Google	Cloud Project Number	Paste the project number from the Google account.
	Service Account Credentials	Paste the entire Google account JSON key into the field. Click the eye icon to Show or Hide the key.
	Cloud Location	Select a Google Cloud location. For information about Google locations, visit the product help.

4. Advanced options will differ between the various types of storage connectors.

To edit a storage connector:

1. Go to *System Settings* > *Fabric Management* > *Fabric Connectors*.
2. Right-click a storage connector, and select *Edit*.
   The *Edit Connectors* dialog box is displayed.
3. Edit the settings, and click *OK*.

Certificates

The FortiAnalyzer generates a certificate request based on the information you entered to identify the FortiAnalyzer unit. After you generate a certificate request, you can download the request to a management computer and then forward the request to a CA.

Local certificates are issued for a specific server, or website. Generally they are very specific, and often for an internal enterprise network.

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to an entire company.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and include the date and time when the next CRL will be issued, as well as a sequence number to help ensure you have the most current versions.

Local certificates

The FortiAnalyzer unit generates a certificate request based on the information you enter to identify the FortiAnalyzer unit. After you generate a certificate request, you can download the request to a computer that has management access to the FortiAnalyzer unit and then forward the request to a CA.

The certificate window also enables you to export certificates for authentication, importing, and viewing.

The FortiAnalyzer has one default local certificate: *Fortinet_Local*.

You can manage local certificates from the *System Settings > Certificates* page. Some options are available in the toolbar and some are also available in the right-click menu.



In order to safeguard against compromise, in FortiAnalyzer 7.6.4, FAZ-VM license files contain a unique certificate which is tied to the device's serial number.

Creating a local certificate

To create a certificate request:

1. Go to *System Settings > Certificates*.
2. Click *Create New/Import > Generate CSR* in the toolbar. The *Generate Certificate Signing Request* pane opens.
3. Enter the following information as required, then click *OK* to save the certificate request:

Certificate Name	The name of the certificate.

Subject Information		Select the ID type from the dropdown list: • *Host IP*: Select if the unit has a static IP address. Enter the public IP address of the unit in the *Host IP* field. • *Domain Name*: Select if the unit has a dynamic IP address and subscribes to a dynamic DNS service. Enter the domain name of the unit in the *Domain Name* field. • *Email*: Select to use an email address. Enter the email address in the *Email Address* field.
Optional Information		
	Organization Unit (OU)	The name of the department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icons.
	Organization (O)	Legal name of the company or organization.
	Locality (L)	Name of the city or town where the device is installed.
	State/Province (ST)	Name of the state or province where the FortiGate unit is installed.
	Country (C)	Select the country where the unit is installed from the dropdown list.
	E-mail Address (EA)	Contact email address.
	Subject Alternative Name	Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma. A name can be: • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) You must precede the name with the name type. Examples: • IP:1.1.1.1 • email:test@fortinet.com • email:my@other.address • URI:http://my.url.here/
Key Type		The key type can be *RSA* or *Elliptic Curve*.
Key Size		Select the key size from the dropdown list: *512 Bit*, *1024 Bit*, *1536 Bit*, or *2048 Bit*. This option is only available when the key type is *RSA*.
Curve Name		Select the curve name from the dropdown list: *secp256r1* (default), *secp384r1*, or *secp521r1*. This option is only available when the key type is *Elliptic Curve*.
Enrollment Method		The enrollment method is set to *File Based*.

Importing local certificates

To import a local certificate:

1. Go to *System Settings* > *Certificates*.
2. Click *Create New/Import* > *Local Certificate* in the toolbar.
3. Enter the following information as required, then click *OK* to import the local certificate:

Type	Select the certificate type from the dropdown list: *Local Certificate*, *PKCS #12 Certificate*, or *Certificate*.
Certificate File	Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
Key File	Click *Browse...* and locate the key file on the management computer, or drag and drop the file onto the dialog box. This option is only available when *Type* is *Certificate*.
Password	Enter the certificate password. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.
Certificate Name	Enter the certificate name. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.

Deleting local certificates

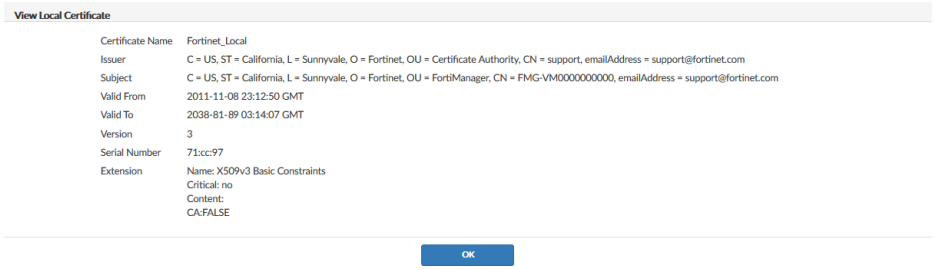
To delete a local certificate or certificates:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.

Viewing details of local certificates

To view details of a local certificate:

1. Go to *System Settings* > *Certificates*.
2. Select the certificates that you would like to see details about, then click *View Certificate Detail* in the toolbar or right-click menu. The *View Local Certificate* page opens.



3. Click *OK* to return to the local certificates list.

Downloading local certificates

To download a local certificate:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate that you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.

When an object is added to a policy package and assigned to an ADOM, the object is available in all devices that are part of the ADOM. If the object is renamed on a device locally, FortiManager automatically syncs the renamed object to the ADOM.

Using a local certificate for OFTP connection

You can configure FortiAnalyzer to use an externally signed local (custom) certificate for OFTP connection between FortiGate and FortiAnalyzer for logging.

The below example uses FortiGate as the logging device; however, you can use the same process to import a certificate for syslog devices logging over TLS. Make sure to complete the config and check connection according to the syslog device you are using.

To generate a certificate signing request from FortiAnalyzer:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Create New/Import* > *Generate CSR*.
3. Enter the relevant information in the certificate signing request, and then click *OK*.

   If certificate validation is enabled on FortiGate, you must enter the FortiAnalyzer serial number in the *Domain Name* field.

4. Select the newly created CSR and click *Download*.
5. To generate the certificate, sign the CSR with either a public CA or private CA.

   For example, you can use a FortiAuthenticator to sign the CSR. For more information, see the FortiAuthenticator Administration Guide.
6. After signing the CSR, export and download the certificate.

7. In FortiAnalyzer, import the signed certificate:
   a. Go to *System Settings > Certificates > Local Certificates*.
   b. Click *Create New/Import > Certificate*.
   c. In the *Type* field, select *Local Certificate*.
   d. In the *Certificate File* field, drag and drop or select the signed certificate.
   e. Click *OK*.
8. The certificate status will change from *PENDING* to *OK* once the certificate is uploaded correctly.

To configure the use of the local certificate and restart the OFTP daemon:

1. Once the certificate has been imported, enter the following command in the FortiAnalyzer CLI to use the local certificate:
   ```
   config system certificate oftp
      set mode local
      set local "<name of the certificate>"
   end
   ```
2. In the FortiAnalyzer CLI, enter the following command to restart the OFTP daemon:
   ```
   diagnose test application oftpd 99
   ```
3. If a private CA was used, you must import the CA certificate in the FortiGate.
4. Validate the connection status to FortiAnalyzer in the FortiGate.
   In the FortiGate GUI, you can validate the connection in *Security Fabric > Fabric Connectors > Logging & Analytics > FortiAnalyzer*.
   In the FortiGate CLI, you can run the following command to validate the connection:
   ```
   execute log fortianalyzer test-connectivity
   ```
   For example:

   ```
   FGT-kvm2 # execute log fortianalyzer test-connectivity
   FortiAnalyzer Host Name: FAZ-kvm1
   FortiAnalyzer Adom Name: root
   FortiGate Device ID: FGVM########
   Registration: registered
   Connection: allow
   Adom Disk Space (Used/Allocated): 39960108B/53687091200B
   Analytics Usage (Used/Allocated): 37919829B/37580963840B
   Analytics Usage (Data Policy Days Actual/Configured): 60/60 Days
   Archive Usage (Used/Allocated): 2040279B/16106127360B
   Log: Tx & Rx (33 logs received since 11:08:11 09/27/22)
   IPS Packet Log: Tx & Rx
   Content Archive: Tx & Rx
   Quarantine: Tx & Rx

   Certificate of Fortianalyzer valid and serial number is:FAZ-VM####
   ```

   For more information, see the FortiGate / FortiOS Administration Guide.

CA certificates

The FortiAnalyzer has one default CA certificate, *Fortinet_CA*. In this sub-menu you can delete, import, view, and download certificates.

Importing CA certificates

To import a CA certificate:

1. Go to *System Settings* > *Certificates*.
2. Click *Create New/Import* > *CA Certificate* in the toolbar.
3. Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the certificate.

Viewing CA certificate details

To view a CA certificate's details:

1. Go to *System Settings* > *Certificates*.
2. Select the certificates you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *View CA Certificate* page opens.
4. Click *OK* to return to the CA certificates list.

Downloading CA certificates

To download a CA certificate:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.

Deleting CA certificates

To delete a CA certificate or certificates:

1. Go to *System Settings* > *Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.



The *Fortinet_CA* certificate cannot be deleted.

Certificate revocation lists

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and Certificate Revocation List (CRL) from the issuing CA.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiAnalyzer unit according to the procedures given below.

Importing a CRL

To import a CRL:

1. Go to *System Settings* > *Certificates*.
2. Click *Create New/Import* > *CRL* in the toolbar.
3. Click *Browse...* and locate the CRL file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the CRL.

Viewing a CRL

To view a CRL:

1. Go to *System Settings* > *Certificates*.
2. Select the CRL you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *Result* page opens.
4. Click *OK* to return to the CRL list.

Deleting a CRL

To delete a CRL or CRLs:

1. Go to *System Settings* > *Certificates*.
2. Select the CRL or CRLs you need to delete.

3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

Log Forwarding

You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server when you use the default forwarding mode in log forwarding. You can also forward logs via an output plugin, connecting to a public cloud service.

The *client* is the FortiAnalyzer unit that forwards logs to another device. The *server* is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs.

In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. See Log storage on page 45 for more information.



To see a graphical view of the log forwarding configuration, and to see details of the devices involved, go to *System Settings* > *Logging Topology*. For more information, see Logging Topology on page 475.

Modes

FortiAnalyzer supports two log forwarding modes: forwarding (default), and aggregation.

Forwarding

Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

This mode can be configured in both the GUI and CLI.

Aggregation

As FortiAnalyzer receives logs from devices, it stores them, and then forwards the collected logs at a specified time every day. To avoid duplication, the client only sends logs that are not already on the server.

FortiAnalyzer supports log forwarding in aggregation mode only between two FortiAnalyzer units. Syslog and CEF servers are not supported.



The client must provide super user log in credentials to get authenticated by the server to aggregate logs.

Aggregation mode can only be configured with the `log-forward` and `log-forward-service` CLI commands. See the *FortiAnalyzer CLI Reference* for more information.

The following table lists the differences between the two modes:

	Log Forwarding	Log Aggregation
Configuration Portal	GUI or CLI	CLI
Remote Server Type	FortiAnalyzer Syslog/CEF/Forward via Output Plugin	FortiAnalyzer
Device Filter Support	Yes	Yes
Log Filter Support	Yes	No
Log Archive Support	Yes	Yes
Server Port customization	Yes (Except for FortiAnalyzer)	No
Compression	Yes (FortiAnalyzer only)	No
Log Field Exclusion	Yes	No
Log Delay	Real-time (max 5 minutes delay)	Max 1 day
Log Data Masking	Yes	No
Meta-data synchronization	Yes	No
Secure channel support	Yes (SSL as reliable connection)	Yes (rsync + SSH)
Network bandwidth	Normal (as log traffic received)	Peak hour as aggregation starts to finish
Impact on remote FortiAnalyzer	Normal (as log volume received)	Potentially large table (If there is a mix of incoming real-time and real-time logs.)

Configuring log forwarding

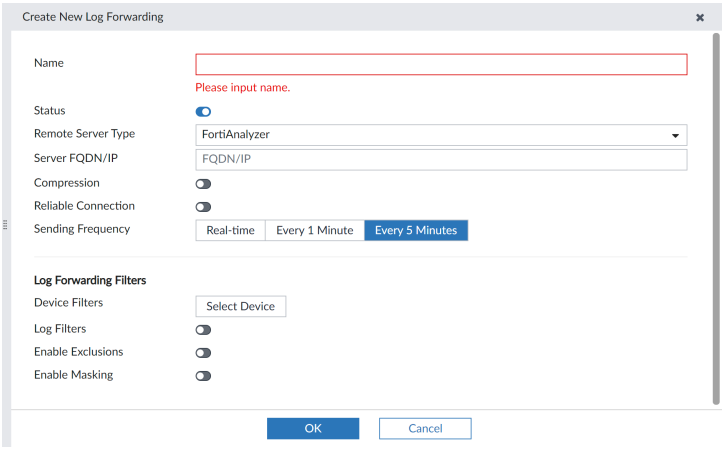
Forwarding mode only requires configuration on the client side. No configuration is needed on the server side. In aggregation mode, accepting the logs must be enabled on the FortiAnalyzer that is acting as the server.

Forwarding mode

Forwarding mode can be configured in the GUI. No configuration is required on the server side.

To configure the client:

1. Go to *System Settings* > *Advanced* > *Log Forwarding* > *Settings*.
2. Click *Create New* 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.

Name	Enter a name for the remote server.
Status	Set to *On* to enable log forwarding. Set to *Off* to disable log forwarding.
Remote Server Type	Select the type of remote server to which you are forwarding logs: • *FortiAnalyzer* • *Syslog* (this option can be used to foward logs to FortiSIEM and FortiSOAR) • *Syslog Pack* • *Common Event Format (CEF)* • *Forward via Output Plugin*
Output Profile	Select the output profile. You must configure output profiles to appear in the dropdown. For more information, see Output profiles on page 523. This option is only available when the server type is *Forward via Output Plugin*.
Server FQDN/IP	Enter the fully qualified domain name or IP for the remote server. This option is not available when the server type is *Forward via Output Plugin*.
Server Port	Enter the server port number. Default: 514. This option is only available when the server type is *Syslog*, *Syslog Pack*, or *Common Event Format (CEF)*.
Compression	Turn on to enable log message compression when the remote FortiAnalyzer also supports this format. If the remote FortiAnalyzer does not support compression, log messages will remain uncompressed. This option is only available when the server type is *FortiAnalyzer*.
Reliable Connection	Turn on to use TCP connection. Turn off to use UDP connection.

	If you want to forward logs to a Syslog or CEF server, ensure this option is supported. RELP is not supported. If the connection goes down, logs are buffered and automatically forwarded when the connection is restored. The buffer limit is 12GB. This option is not available when the server type is *Forward via Output Plugin*.
Sending Frequency	Select when logs will be sent to the server: *Real-time*, *Every 1 Minute*, or *Every 5 Minutes* (default). This option is only available when the server type is *FortiAnalyzer*.
Log Forwarding Filters	
Device Filters	Click *Select Device*, then select the devices whose logs will be forwarded.
Log Filters	Turn on to configure filter on the logs that are forwarded. Select *All* or *Any of the Following Conditions* in the *Log messages that match* field to control how the filters are applied to the logs. Add filters to the table by selecting the *Log Field*, *Match Criteria*, and *Value* for each filter.
Enable Exclusions	Turn on to configure filter on the logs that are forwarded. Add exclusions to the table by selecting the *Device Type* and *Log Type*. Then, add *Log Fields* to the *Exclusion List* by clicking *Fields* and specifying the excluded log fields in the *Select Log Field* pane.
Enable Masking	Turn on to enable log field masking. In the *Masking Data Fields*, select any data fields that should be masked during log forwarding. The remote server will receive logs with the selected field values masked. Configure a *Data Mask Key*.

When configuring *Log Forwarding Filters*, FortiAnalyzer does not support wildcard or subnet values for IP log field filters when using the *Equal to* and *Not equal to* operators.

If wildcards or subnets are required, use *Contain* or *Not contain* operators with the regex filter. For example, the following text filter excludes logs forwarded from the 172.10.0.0/16 subnet:

```
srcip !~ "172\.10\.[0-9]+\.[0-9]+
```

Devices whose logs are being forwarded to another FortiAnalyzer device are added to the server as unauthorized devices. To authorize devices, see Authorizing devices on page 89.

When log forwarding to a syslog server, you can decode the attackconext field for IPS logs. This can only be done in the CLI by enabling `fwd-syslog-decode-b64` in the log forward configuration.

See Decode the attackcontext field in IPS on page 318

Aggregation mode

Aggregation mode can only be configured using the CLI. Aggregation mode configurations are not listed in the GUI table, but still use a log forwarding ID number.



Use the following CLI command to see what log forwarding IDs have been used:
`get system log-forward`

To configure the server:

1. If required, create a new administrator with the *Super_User* profile. See Creating administrators on page 557.
2. Enable log aggregation and, if necessary, configure the disk quota, with the following CLI commands:
```
config system log-forward-service
   set accept-aggregation enable
   set aggregation-disk-quota <quota>
end
```

To configure the client:

1. Open the log forwarding command shell:
```
config system log-forward
```
2. Create a new, or edit an existing, log forwarding entry:
```
edit <log forwarding ID>
```
3. Set the log forwarding mode to aggregation:
```
set mode aggregation
```
4. Set the server display name and IP address:
```
set server-name <string>
set server-ip <xxx.xxx.xxx.xxx>
```
5. Enter the user name and password of the super user administrator on the server:
```
set agg-user <string>
set agg-password <string>
```
6. If required, set the aggregation time from 0 to 23 hours (default: 0, or midnight):
```
set agg-time <integer>
```
7. Enter the following to apply the configuration and create the log aggregation:
```
end
```
The following line will be displayed to confirm the creation of the log aggregation:
```
check for cfg[<log forwarding ID>] svr_disp_name=<server-name>
```



For more information, see the *FortiAnalyzer CLI Reference*.

Output profiles

You can use output profiles to configure log forwarding to public cloud services.

You can create and manage these output profiles in *System Settings > Advanced > Log Forwarding > Output Profile*. Once created, you can use the output profile when configuring a client for log forwarding. See Configuring log forwarding on page 519.

To create an output profile:

1. Go to *System Settings > Advanced > Log Forwarding > Output Profile*.
2. Click *Create New*.
   The *Create Output Profile* pane displays.
3. Configure the following options:

Name	Enter a name for the output profile.
Type	Select the public cloud service for the output profile.
Configuration	Click *Use Default* to use the default Fluentd configuration for the selected public cloud service. Alternatively, copy and paste the Fluentd configuration into this field for the selected public cloud service.
Field	Fields will automatically be added into the configuration if a keyword matches the placeholder in the configuration to provide encryption for you to hide the credentials. For example, a password placeholder in the configuration would be "`${password}`". In the field, you can define *Field*: `password`, *Value*: `actual_password`.

4. Click *Validate and Save*.

To edit an output profile:

1. Go to *System Settings > Advanced > Log Forwarding > Output Profile*.
2. Select the checkbox for the output profile.
3. Click *Edit*.
4. Edit the options as needed.
5. Click *Validate and Save*.

To clone an output profile:

1. Go to *System Settings > Advanced > Log Forwarding > Output Profile*.
2. Select the checkbox for the output profile.
3. Click *Clone*.
4. Edit the options to create the new output profile.
5. Click *Validate and Save*.

To export and import an output profile:

1. In the FortiAnalyzer that you are exporting the output profile from, go to *System Settings > Advanced > Log Forwarding > Output Profile*.
2. Select the checkbox for the output profile.
3. Click *More > Export*.
4. Select the export data type and click *OK*.
5. In the FortiAnalyzer that you are imorting the output profile to, go to *System Settings > Advanced > Log Forwarding > Output Profile*.
6. Click *More > Import*.
7. Drag and drop or select the output profile file saved on the management computer.
   If there is a conflict with an existing output profile, you can select if the import file should be skipped, renamed, or if it should replace the existing output profile.
8. Click *OK* to complete the import.



You can enable and troubleshoot Fluentd logging from the FortiAnalyzer CLI using the following commands:

```
diagnose sql fluentd log-tail
diagnose sql fluentd log-view
diagnose test application fwdplugind
```

For more information, see the FortiAnalyzer CLI Reference on the Fortinet Documents Library.

Managing log forwarding

Log forwarding mode server entries can be edited and deleted using both the GUI and the CLI. Aggregation mode server entries can only be managed using the CLI. Entries cannot be enabled or disabled using the CLI.

To enable or disable a log forwarding server entry:

1. Go to *System Settings > Advanced > Log Forwarding > Settings*.
2. Double-click on a server entry, right-click on a server entry and select *Edit*, or select a server entry then click *Edit* in the toolbar. The *Edit Log Forwarding* pane opens.
3. Set the *Status* to *Off* to disable the log forwarding server entry, or set it to *On* to enable the server entry. Only the name of the server entry can be edited when it is disabled.
4. Click *OK* to apply your changes.

To edit a log forwarding server entry using the GUI:

1. Go to *System Settings > Advanced > Log Forwarding > Settings*.
2. Double-click on a server entry, right-click on a server entry and select *Edit*, or select a server entry then click *Edit* in the toolbar. The *Edit Log Forwarding* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To edit a log forwarding server entry using the CLI:

1. Open the log forwarding command shell:
   ```
   config system log-forward
   ```
2. Enter an existing entry using its log forwarding ID:
   ```
   edit <log forwarding ID>
   ```
3. Edit the settings as required. See the *FortiAnalyzer CLI Reference* for information.
4. Enter the following command to apply your changes:
   ```
   end
   ```

To delete a log forwarding server entry or entries using the GUI:

1. Go to *System Settings* > *Advanced* > *Log Forwarding* > *Settings*.
2. Select the entry or entries you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected entry or entries.

To delete a log forwarding server entry using the CLI:

1. Open the log forwarding command shell:
   ```
   config system log-forward
   ```
2. Delete an entry using its log forwarding ID:
   ```
   delete <log forwarding ID>
   ```
   The log forwarding server entry is immediately deleted. There is no confirmation.

To delete all log forwarding entries using the CLI:

1. Enter the following CLI command:
   ```
   config system log-forward
      purge
   ```
2. Enter y to delete all the entries.
   ```
   This operation will clear all table!
   Do you want to continue? (y/n)y
   ```

Log forwarding buffer

When log forwarding is configured, FortiAnalyzer reserves space on the system disk as a buffer between the *fortilogd* and *logfwd* daemons. In the event of a connection failure between the log forwarding client and server (network jams, dropped connections, etc.), logs are cached as long as space remains available. When storage space is exceeded, older logs are deleted in favor of new logs.

The default log forward buffer size is 30% of the system reserved disk size, and can be increased to use up to 80% of the available reserved disk. Additional storage space is available by using the disk space reserved for ADOMs. When configuring the log forward buffer size above 80% of the reserved disk size, the space available for ADOMs is reduced.

For example, in a scenario where the FortiAnalyzer has a total disk size of 275 GB for the entire system, with a system reserved disk size of 50 GB and an ADOM disk space of 50 GB, the log forwarding buffer can be

configured up to a maximum of 90 GB (80% of the 50 GB reserved disk size = 40 GB + 50 GB disk reserved for ADOMs = 90 GB total).

The size of the system reserved disk varies by platform and total available storage. See Disk space allocation on page 170.



The log forward buffer is shared between *fortilogd* for all *logfwd* servers.

When changes are made to the log forward cache size, each server individually resets the log reading position to the latest one, and all logs currently in the log-forward disk cache are dropped.

To change the log forward cache size:

1. In the FortiAnalyzer CLI, enter the following commands:
   ```
   config system global (global)#
   set log-forward-cache-size [number (GB)]
   ```
2. When prompted, enter `Y` to confirm the change.
   - When entering a number outside of the valid cache size range, an error with the valid range is displayed.
   - When entering a number that uses storage from both the reserved disk size and available ADOM disk, a message displays to indicate that the cache will be allocated from the available disk quota and reserved space.
     ```
     (global)# set log-forward-cache-size 50
     Log-forward disk cache will be allocated from available disk quota and reserved space.
     All logs currently in log-forward disk cache will be dropped.
     Do you want to continue? (y/n)
     ```



The `diagnose test application logfwd 3` CLI command can be used to display log positions for the last log buffered and last log sent, as well as determine the buffer lag-behind. See the FortiAnalyzer CLI Reference.

Log forwarding to SOCaaS

FortiCloud SOCaaS provides scalable security operations services designed to help you maintain continuous Cyber Awareness and control of your Fortinet Security Fabric network. For more information, see SOCaaS in the Fortinet Document Library.

You can configure FortiAnalyzer to forward logs to SOCaaS. When the Fortinet SOC team is setting up the service, they will provide you with the server IP and port numbers that you need for the configuration.

In case of abrupt disconnection between your FortiAnalyzer and SOCaaS, logs will only be cached for the amount of time allowed based on the cache size available. Logs exceeding the available cache storage time are dropped. To avoid log dropping in such cases, we recommended that you configure a log buffer cache size that accommodates 24 hours of logs in your FortiAnalyzer using the following formula:

Average Lograte * 200 * seconds in 1 day (86400) * 1.2 = Cache Size logfwd

To configure log forwarding to SOCaaS:

1. Go *System Settings > Advanced > Log Forwarding*, and click *Create New*.
   The *Create New Log Forwarding* dialog displays.
2. Configure the following mandatory settings:

Remote Server Type	FortiAnalyzer
Server FQDN/IP	Enter the FQDN provided by the Fortinet SOC team.  FQDNs are supported for log forwarding in FortiAnalyzer 7.0.0 and later. If you are using an earlier version of FortiAnalyzer, you can use the resolved IP address of the FQDN instead.
Reliable Connection	On
Sending Frequency	Real-time

3. (Optional) Configure the device filters.
   a. Under *Log Forwarding Filters*, click *Select Device*.
   b. Select the devices from the list and click *OK*.
4. (Optional) Configure the log filters. This step is optional but is strongly recommended.
   a. Enable *Log Filters*.
   b. For *Log messages that match*, select *Any of the Following Conditions* and configure the following:

Log Field	Select *Log Type* from the dropdown.
Match Criteria	Select *Equal to* from the dropdown.
Value	Select *Traffic*, *Event*, or *UTM* from the dropdown.

5. (Optional) Toggle *Enable Exclusions* to *ON*.



To exclude fields related to user privacy, create individual filters for the *Any* and *Traffic* log types, and one for each UTM subtype (*Antivirus*, *Application*, *DNS*, *Data Leak Prevention*, *Web Application Firewall*, *Email Filter*, *File Filter*, *Intrusion Prevention*, *SSH*, *SSL*, and *Web Filter*).

a. Configure the following exclusion criteria:

Device Type	Log Type	Exclusion List (Fields)
FortiGate	Any	User
FortiGate	Traffic	Destination Unauthenticated User (dstunauthuser) Destination User (dstuser) Unauthenticated User (unauthuser)
FortiGate	Antivirus	Unauthenticated User (unauthuser)
FortiGate	Application	Unauthenticated User (unauthuser)
FortiGate	DNS	Unauthenticated User (unauthuser)
FortiGate	Data Leak Prevention	Unauthenticated User (unauthuser)
FortiGate	Email Filter	Unauthenticated User (unauthuser)
FortiGate	File Filter	Unauthenticated User (unauthuser)
FortiGate	Intrusion Prevention	Unauthenticated User (unauthuser)
FortiGate	SSH	Unauthenticated User (unauthuser)
FortiGate	SSL	Unauthenticated User (unauthuser)
FortiGate	Web Application Firewall	Unauthenticated User (unauthuser)
FortiGate	Web Filter	Unauthenticated User (unauthuser)

b. Click *OK*.

6. Repeat the step above for each exclusion filter type.
7. Verify the settings are configured properly using the following command:
   ```
   show system log-forward
   ```
8. To avoid log dropping in case of abrupt disconnection between your FortiAnalyzer and SOCaaS, configure a log buffer cache size that accommodates 24 hours of logs in your FortiAnalyzer device. See To configure the log buffer cache size:.

For more information about the log forwarding options, see Configuring log forwarding on page 519.

To configure the log buffer cache size:

1. Go to *Dashboards* > *Status*.
2. Open the *Settings* for the *Insert Rate vs. Receive Rate* widget.
3. From the *Time Period* dropdown, select *Last 24 Hours*.
4. Click *OK*.
5. View the graph details, and use the peak log rate as the number for the average lograte count. Use this average log rate to calculate the buffer cache size.

   The following table provides three example scenarios for calculating the log forwarding buffer cache size for a small, medium, and enterprise business:

Customer size	Average log rate	Calculation	Buffer cache size
Small	100 logs/sec	`100 * 200 * 86400 * 1.2`	2GB
Medium	1000 logs/sec	`1000 * 200 * 86400 * 1.2`	20GB
Enterprise	10000 logs/sec	`10000 * 200 * 86400 * 1.2`	200GB

For more information about sizing, see the FortiAnalyzer Architecture Guide.

6. In the FortiAnalyzer CLI, set the log buffer cache size in GB using the following command:
```
config system global
   set log-forward-cache-size <integer>
```
7. When prompted, enter `Y` to confirm the change.

   For more information about log forwarding buffers and how log forwarding space allocation works, see Log forwarding buffer on page 525.

Log Fetching

Log fetching is used to retrieve archived logs from one FortiAnalyzer device to another. This allows administrators to run queries and reports against historic data, which can be useful for forensic analysis.

The fetching FortiAnalyzer can query the server FortiAnalyzer and retrieve the log data for a specified device and time period, based on specified filters. The retrieved data are then indexed, and can be used for data analysis and reports.

Log fetching can only be done on two FortiAnalyzer devices running the same firmware. A FortiAnalyzer device can be either the fetch server or the fetching client, and it can perform both roles at the same time with different FortiAnalyzer devices. Only one log fetching session can be established at a time between two FortiAnalyzer devices.

The basic steps for fetching logs are:

1. On the client, create a fetching profile. See Fetching profiles on page 529.
2. On the client, send the fetch request to the server. See Fetch requests on page 531.
3. If this is the first time fetching logs with the selected profile, or if any changes have been made to the devices and/or ADOMs since the last fetch, on the client, sync devices and ADOMs with the server. See Synchronizing devices and ADOMs on page 532.
4. On the server, review the request, then either approve or reject it. See Request processing on page 532.
5. Monitor the fetch process on either FortiAnalyzer. See Fetch monitoring on page 533.
6. On the client, wait until the database is rebuilt before using the fetched data for analysis.

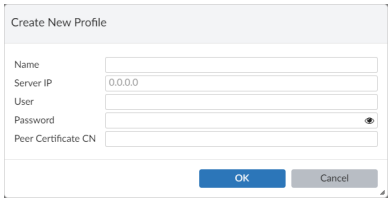
Fetching profiles

Fetching profiles can be managed from the *Profiles* tab on the *System Settings > Advanced > Log Fetch* pane.

Profiles can be created, edited, and deleted as required. The profile list shows the name of the profile, as well as the IP address of the server it fetches from, the server and local ADOMs, and the administrator name on the fetch server.

To create a new fetching profile:

1. On the client, go to *System Settings > Advanced > Log Fetch*.
2. Select the *Profiles* tab, then click *Create New* in the toolbar, or right-click and select *Create New* from the menu. The *Create New Profile* dialog box opens.



3. Configure the following settings, then click *OK* to create the profile.

Name	Enter a name for the profile.
Server IP	Enter the IP address of the fetch server.
User	Enter the username of an administrator on the fetch server, which, together with the password, authenticates the fetch client's access to the fetch server.
Password	Enter the administrator's password, which, together with the username, authenticates the fetch client's access to the fetch server.
Peer Certificate CN	Enter the certificate common name of the server.

The fetch server administrator user name and password must be for an administrator with either a *Standard_User* or *Super_User* profile.

To edit a fetching profile:

1. Go to *System Settings > Advanced > Log Fetch > Profiles*.
2. Double-click on a profile, right-click on a profile then select *Edit*, or select a profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete a fetching profile or profiles:

1. Go to *System Settings > Advanced > Log Fetch > Profiles*.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected profile or profiles.

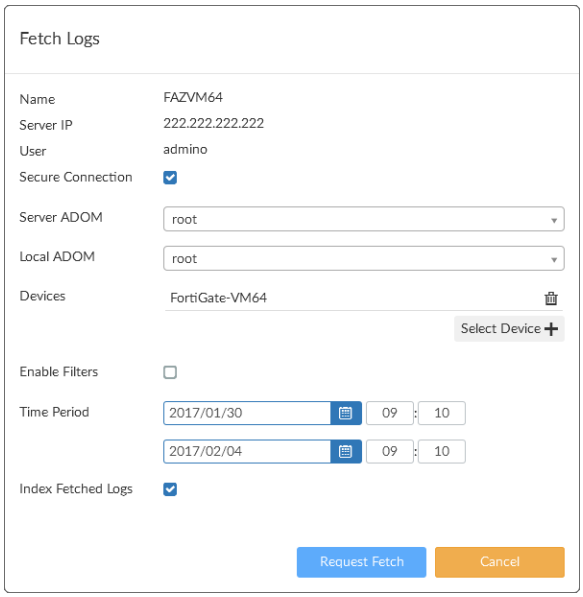
Fetch requests

A fetch request requests archived logs from the fetch server configured in the selected fetch profile. When making the request, the ADOM on the fetch server the logs are fetched from must be specified. An ADOM on the fetching client must be specified or, if needed, a new one can be created. If logs are being fetched to an existing local ADOM, you must ensure the ADOM has enough disk space for the incoming logs.

The data policy for the local ADOM on the client must also support fetching logs from the specified time period. It must keep both archive and analytics logs long enough so they will not be deleted in accordance with the policy. For example: Today is July 1, the ADOM's data policy is configured to keep analytics logs for 30 days (June 1 - 30), and you need to fetch logs from the first week of May. The data policy of the ADOM must be adjusted to keep analytics and archive logs for at least 62 days to cover the entire time span. Otherwise, the fetched logs will be automatically deleted after they are fetched.

To send a fetch request:

1. On the fetch client, go to *System Settings* > *Advanced* > *Log Fetch* > *Profiles*.
2. Select the profile then click *Request Fetch* in the toolbar, or right-click and select *Request Fetch* from the menu. The *Fetch Logs* dialog box opens.



3. Configure the following settings, then click *Request Fetch*.
The request is sent to the fetch server. The status of the request can be viewed in the *Sessions* tab.

Name	Displays the name of the fetch server you have specified.
Server IP	Displays the IP address of the server you have specified.
User	Displays the username of the server administrator you have provided.
Secure Connection	Select to use SSL connection to transfer fetched logs from the server.
Server ADOM	Select the ADOM on the server the logs will be fetched from. Only one ADOM can be fetched from at a time.

Local ADOM	Select the ADOM on the client where the logs will be received. Either select an existing ADOM from the dropdown list, or create a new ADOM by entering a name for it into the field.
Devices	Add the devices and/or VDOMs that the logs will be fetched from. Up to 256 devices can be added. Click *Select Device*, select devices from the list, then click *OK*.
Enable Filters	Select to enable filters on the logs that will be fetched. Select *All* or *Any of the Following Conditions* in the *Log messages that match* field to control how the filters are applied to the logs. Add filters to the table by selecting the *Log Field*, *Match Criteria*, and *Value* for each filter.
Time Period	Specify what date and time range of log messages to fetch.
Index Fetch Logs	If selected, the fetched logs will be indexed in the SQL database of the client once they are received. Select this option unless you want to manually index the fetched logs.

Synchronizing devices and ADOMs

If this is the first time the fetching client is fetching logs from the device, or if any changes have been made the devices or ADOMs since the last fetch, then the devices and ADOMs must be synchronized with the server.

To synchronize devices and ADOMs:

1. On the client, go to *System Settings* > *Advanced* > *Log Fetch* > *Profiles*.
2. Select the profile then click *Sync Devices* in the toolbar, or right-click and select *Sync Devices* from the menu. The *Sync Server ADOM(s) & Device(s)* dialog box opens and shows the progress of the process. Once the synchronization is complete, you can verify the changes on the client. For example, newly added devices in the ADOM specified by the profile.



If a new ADOM is created, the new ADOM will mirror the disk space and data policy of the corresponding server ADOM. If there is not enough space on the client, the client will create an ADOM with the maximum allowed disk space and give a warning message. You can then adjust disk space allocation as required.

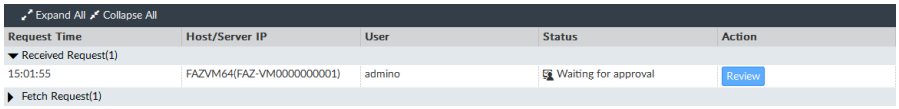
Request processing

After a fetching client has made a fetch request, the request will be listed on the fetch server in the *Received Request* section on the *System Settings* > *Advanced* > *Log Fetch* > *Sessions* pane. It will also be available from the notification center in the GUI banner.

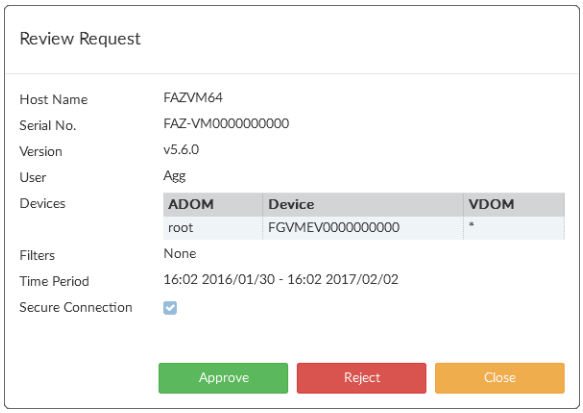
Fetch requests can be approved or rejected.

To process the fetch request:

1. Go to the notification center in the GUI banner and click the log fetcher request, or go to *System Settings* > *Advanced* > *Log Fetch* > *Sessions*.



2. Find the request in the *Received Request* section. You may have to expand the section, or select *Expand All* in the content pane toolbar. The status of the request will be *Waiting for approval*.
3. Click *Review* to review the request. The *Review Request* dialog box will open.



4. Click *Approve* to approve the request, or click *Reject* to reject the request.
   If you approve the request, the server will start to retrieve the requested logs in the background and send them to the client. If you reject the request, the request will be canceled and the request status will be listed as *Rejected* on both the client and the server.

Fetch monitoring

The progress of an approved fetch request can be monitored on both the fetching client and the fetch server.

Go to *System Settings* > *Advanced* > *Log Fetch* > *Sessions* to monitor the fetch progress. A fetch session can be paused by clicking *Pause*, and resumed by clicking *Resume*. It can also be canceled by clicking *Cancel*.

Once the log fetching is completed, the status changes to *Done* and the request record can be deleted by clicking *Delete*. The client will start to index the logs into the database.



It can take a long time for the client to finish indexing the fetched logs and make the analyzed data available. A progress bar is shown in the GUI banner; for more information, click on it to open the *Rebuild Log Database* dialog box.

Log and report features will not be fully available until the rebuilding process is complete.

You may need to rebuild the ADOM after the transfer is complete depending on the Log Fetch settings.

To perform post fetch actions:

Is *Index Fetched Logs* enabled in the *Log Fetch* settings?	Yes	The ADOM is rebuilt automatically and the log fetch workflow is complete.
	No	You will need to rebuild ADOM manually from the CLI.

Event Log

The *Event Log* pane provides an audit log of actions made by users on FortiAnalyzer. It allows you to view log messages that are stored in memory or on the internal hard disk drive. You can use filters to search the messages and download the messages to the management computer.

See the *FortiAnalyzer Log Message Reference*, available from the Fortinet Document Library, for more information about the log messages.

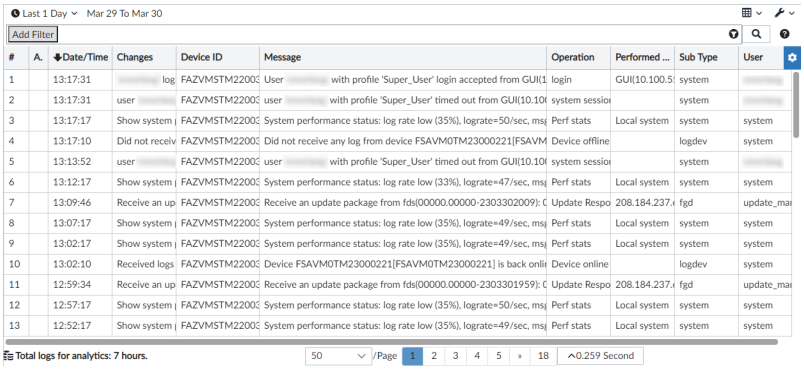


The event log includes logs for modify, request, and response API calls.

You can disable or enable JSON API request and response logging in the FortiAnalyzer CLI:

```
config system global
   set jsonapi-log {all | disable | request | response}
      all - logging for both jsonapi request & response.
      disable - disable jsonapi logging for both request & response.
      request - logging for jsonapi request only.
      response - logging for jsonapi response only.
```

Go to *System Settings* > *Event Log* to view the local log list.



The following options are available:

Last...	Select the amount of time to show from the available options, or select a custom time span or any time.
Add Filter	Filter the event log list based on the log level, user, sub type, or message. See Event log filtering on page 535.

Column Settings		Select which columns are enabled or disabled in the Event Log table.
Tools		
	Display Raw / Formatted Log	Click on *Display Raw* to view the logs in their raw state. Click *Formatted Log* to view logs formatted into a table.
	Real-time Log / Historical Log	Click to view the real-time or historical logs list.
	Download	Download the event logs in either CSV or the normal format to the management computer.
	Case Sensitive Search	Enable or disable case sensitive searching.
Pagination		Browse the pages of logs and adjust the number of logs that are shown per page.

The following information is shown:

#	The log number.
Date/Time	The date and time that the log file was generated.
Device ID	The ID of the related device.
Level	The severity level of the message. For a description of severity levels, see the Log Message Reference.
User	The user that the log message relates to.
Sub Type	The event log subtype. For a description of the subtypes for event logs, see the Log Message Reference.
Description	A description of the event.
Operation	The change or operation that triggered the event.
Performed On	Entity affected by the change or operation. For example, when you log out of the FortiAnalyzer GUI, the operation is performed on the local FortiAnalyzer GUI.
Changes	Details of the change.
Message	Log message details. A *Session ID* is added to each log message. The *username* of the administrator is added to log messages wherever applicable for better traceability.

Event log filtering

The event log can be filtered using the *Add Filter* box in the toolbar.

To filter event log results using the toolbar:

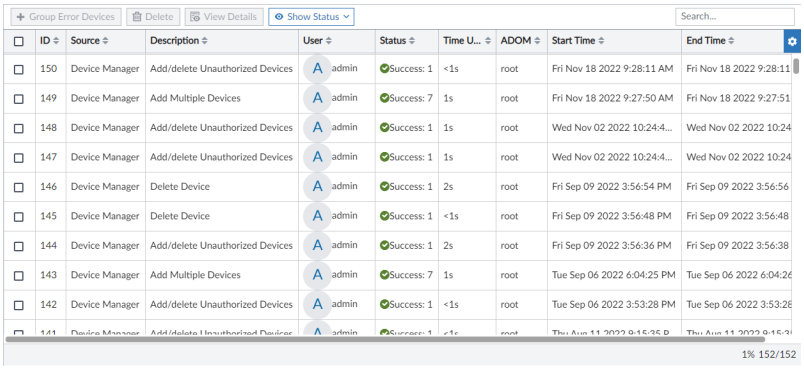
1. Specify filters in the *Add Filter* box.
   - **Filter mode**: Click in the *Add Filter* box, select a filter from the dropdown list, then type a value.
   - **Text Mode**: Click the *Switch to Text Mode* icon at the right end of the *Add Filter* box to switch to text mode. In this mode, you can type in the whole search criteria.
     Click the *Switch to Filter Mode* icon to return to filter mode.
     Additional search operators such as "And", "Or", and "Not" can be used in event log filtering. Click the help icon next to the filter bar in the GUI for additional information.
2. Click *Go* to apply the filter.

Task Monitor

Use the task monitor to view the status of the tasks you have performed.

Go to *System Settings* > *Advanced* > *Task Monitor* to view the task monitor. The task list size can also be configured; see Miscellaneous Settings on page 547.

To filter the information in the monitor, enter a text string in the search field.



The following options are available:

Group Error Devices	Create a group of the failed devices, allowing for re-installations to be done only on the failed devices.
Delete	Remove the selected task or tasks from the list. This changes to *Cancel Running Task(s)* when *View* is *Running*.
View Task Detail	View the task *Index*, *Name*, *Status*, *Time Used*, and *History*, in a new window. Click the icons in the *History* column to view the following information: • History • Promotion of device in FortiAnalyzer with autolink • Upgrade remote device firmware • Retrieve remote device configuration • Installation of device templates

	• Installation of policy packages • Execution of additional scripts To filter the information in the task details, enter a text string in the search field. This can be useful when troubleshooting warnings and errors.
Show Status	Select which tasks to view from the dropdown list, based on their status. The available options are: *All*, *Pending*, *Running*, *Canceling*, *Canceled* , *Done*, *Error*, *Aborting*, *Aborted*, and *Warning*.
Column Settings	Select the columns you want to display from the dropdown.

The following information is available:

ID	The identification number for a task.
Source	The platform from where the task is performed.
Description	The nature of the task. Double-click the task to display the specific actions taken under this task.
User	The user or users who performed the tasks.
Status	The status of the task: • *Success*: Completed with success. • *Error*: Completed without success. • *Canceled*: User canceled the task. • *Canceling*: User is canceling the task. • *Aborted*: The FortiAnalyzer system stopped performing this task. • *Aborting*: The FortiAnalyzer system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column. • *Pending* • *Warning*
Time Used	The number of seconds to complete the task.
ADOM	The ADOM associated with the task.
Start Time	The time that the task was started.
End Time	The time that the task was completed.

Mail Server

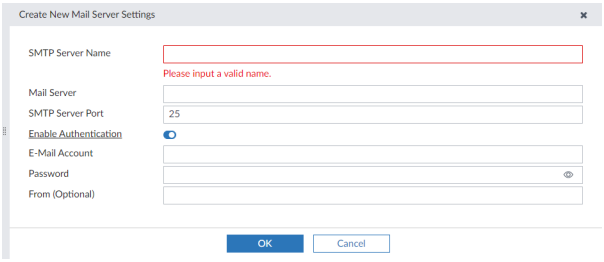
A mail server allows the FortiAnalyzer to sent email messages, such as notifications when reports are run or specific events occur. Mail servers can be added, edited, deleted, and tested.

Go to System *Settings* > *Advanced* > *Mail Server* to configure SMTP mail server settings.

If an existing mail server is in use, the delete icon is removed and the mail server entry cannot be deleted.

To add a mail server:

1. Go to *System Settings > Advanced > Mail Server*.
2. Click *Create New* in the toolbar. The *Create New Mail Server Settings* pane opens.



3. Configure the following settings and then select *OK* to create the mail server.

SMTP Server Name	Enter a name for the SMTP server.
Mail Server	Enter the mail server information.
SMTP Server Port	Enter the SMTP server port number. The default port is 25.
Enable Authentication	Enable or disable authentication.
Email Account	Enter an email account. This option is only accessible when authentication is enabled.
Password	Enter the email account password. This option is only accessible when authentication is enabled.
From (Optional)	Optionally, set the default username for sending.

To edit a mail server:

1. Go to *System Settings > Advanced > Mail Server*.
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 Mail Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

To test the mail server:

1. Go to *System Settings > Advanced > Mail Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
4. Type the email address you would like to send a test email to and click *OK*. A confirmation or failure message will be displayed.
5. Click *OK* to close the confirmation dialog box.

To delete a mail server or servers:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the server.

Syslog Server

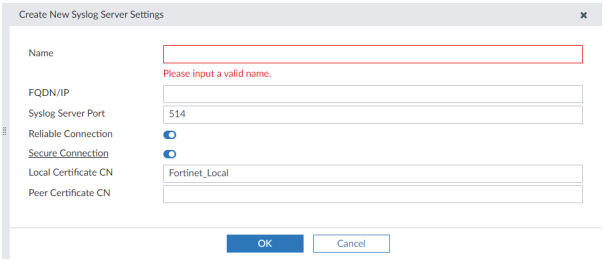
Go to *System Settings* > *Advanced* > *Syslog Server* to configure syslog server settings. Syslog servers can be added, edited, deleted, and tested.

After adding a syslog server, you must also enable FortiAnalyzer to send local logs to the syslog server. See Send local logs to syslog server on page 540.

If an existing syslog server is in use, the delete icon is removed and the server entry cannot be deleted.

To add a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Click *Create New* in the toolbar. The *Create New Syslog Server Settings* pane opens.



3. Configure the following settings and then select *OK* to create the syslog server.

Name	Enter a name for the syslog server.
IP address (or FQDN)	Enter the IP address or FQDN of the syslog server. FortiAnalyzer supports IPv4 and IPv6 addresses.
Syslog Server Port	Enter the syslog server port number. The default port is 514.
Reliable Connection	Enable or disable a reliable connection with the syslog server. The default is *disable*.
Secure Connection	Enable/disable connection secured by TLS/SSL. The default is *disable*. This option is only available when *Reliable Connection* is enabled.

Local Certificate CN	Enter one of the available local certificates used for secure connection: *Fortinet_Local* or *Fortinet_Local2*. The default is *Fortinet_Local*. This option is only available when *Secure Connection* is enabled.
Peer Certificate CN	Enter the certificate common name of syslog server. Null means no certificate CN for the syslog server. This option is only available when *Secure Connection* is enabled.

To edit a syslog server:

1. Go to *System Settings > Advanced > Syslog Server*.
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.

To test the syslog server:

1. Go to *System Settings > Advanced > Syslog Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
   A confirmation or failure message will be displayed.

To delete a syslog server or servers:

1. Go to *System Settings > Advanced > Syslog Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the server or servers.

Send local logs to syslog server

After adding a syslog server to FortiAnalyzer, the next step is to enable FortiAnalyzer to send local logs to the syslog server. See Syslog Server on page 539.

You can only enable these settings by using the CLI.

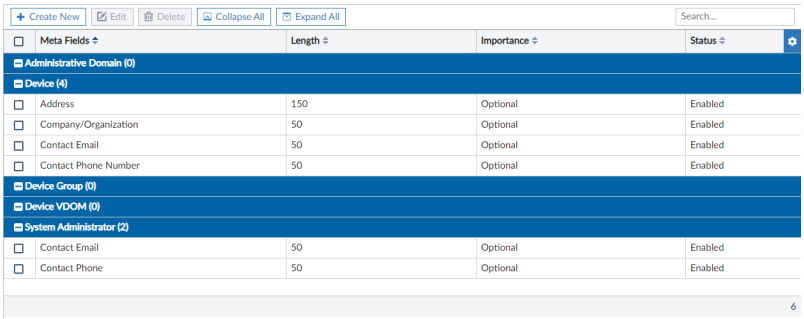
```
config system locallog syslogd setting
   set severity information
   set status enable
   set syslog-name <syslog server name>
end
```

Meta Fields

Meta fields allow administrators to add additional attributes to objects and administrators. You can make meta fields required or optional.

When meta fields are required, administrators must supply additional information when they create an associated object. For example, if you create a required meta field for a device object, administrators must define a value for that meta field for all devices.

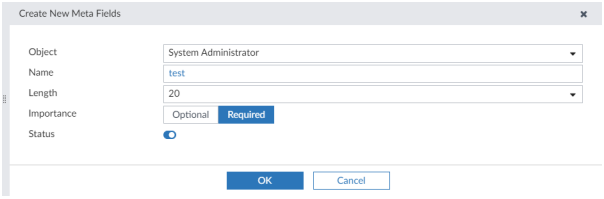
Go to *System Settings* > *Advanced* > *Meta Fields* to configure meta fields. Meta fields can be added, edited, and deleted.



Select *Expand All* or *Collapse All* from the toolbar or right-click menu to view all or none of the meta fields under each object.

To create a new meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Click *Create New* in the toolbar. The *Create New Meta Field* pane opens.



3. From the *Object* field, select an object.
   Some objects also allow you to define a value for the meta field for each device.

Object	The object this metadata field applies to: *Administrative Domains*, *Devices*, *Device Groups*, *Device VDOM*, or *System Administrator*.

4. Configure the following settings:

Name	Enter the label to use for the field. When you type the name, a variable name is automatically created.

Length	Select the maximum number of characters allowed for the field from the dropdown list: *20*, *50*, or *255*.
Importance	Select *Required* to make the field compulsory; otherwise, select *Optional*.
Status	Disable/enable the field. The default selection is *Enabled*.

5. Click *OK*.
   The meta field is created.

To edit a meta field:

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



The *Object* and *Name* fields cannot be edited.

To delete a meta field or fields:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Select the field or fields you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the field or fields.



The default meta fields cannot be deleted.

Device logs

The FortiAnalyzer allows you to log system events to disk. You can control device log file size and the use of the FortiAnalyzer unit's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiAnalyzer unit receives new log items, it performs the following tasks:

- Verifies whether the log file has exceeded its file size limit.
- Checks to see if it is time to roll the log file if the file size is not exceeded.

When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiAnalyzer unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog.1252929496.log`), where `x` is a letter indicating the log type and `N` is a unique number corresponding to the

time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called `tlog.log`. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the GUI, they are in the following format:

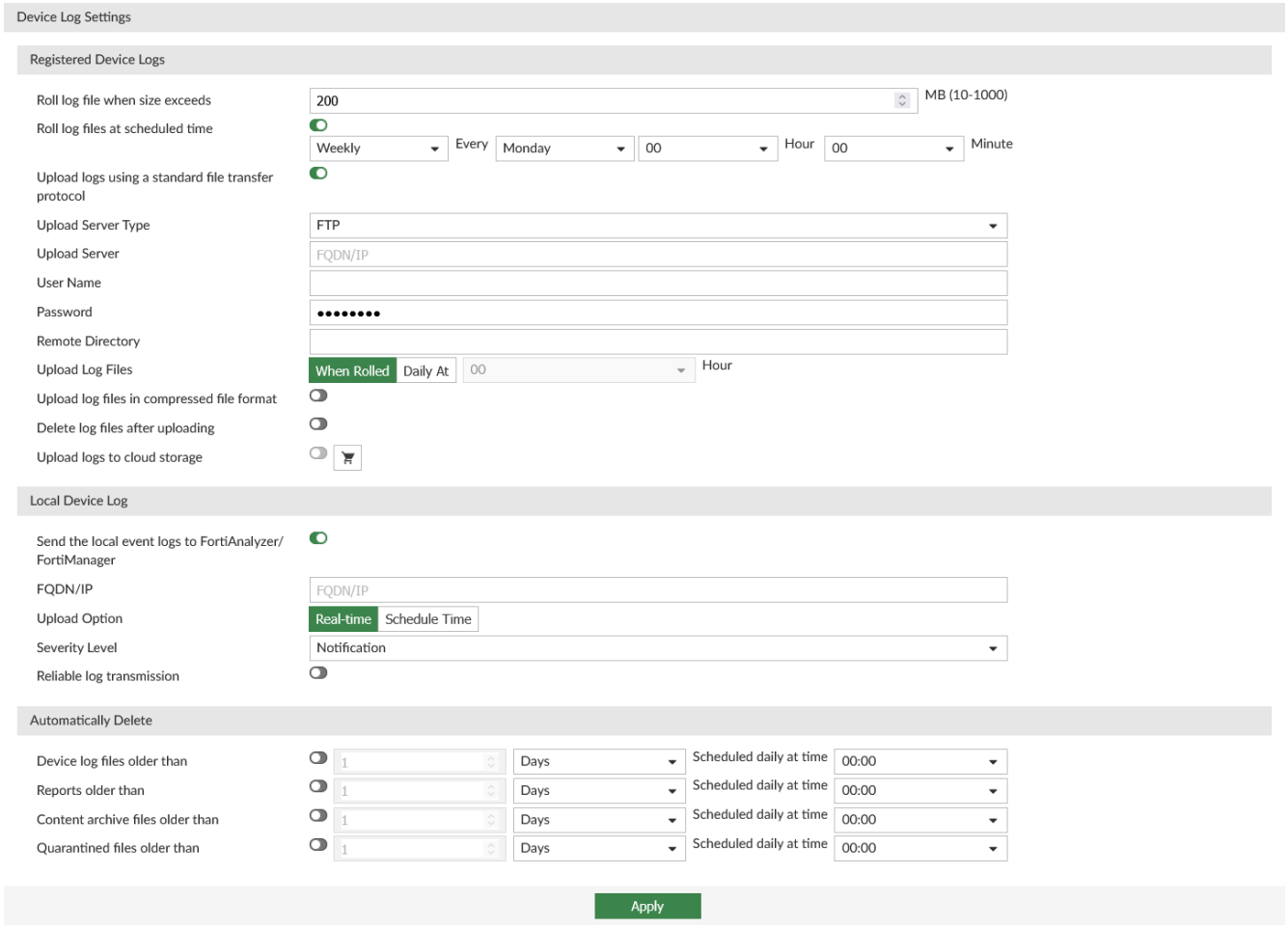
```
FG3K6A3406600001-tlog.1252929496.log-2017-09-29-08-03-54.zst
```

If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Log rolling and uploading can be enabled and configured using the GUI or CLI.

Configuring rolling and uploading of logs using the GUI

Go to *System Settings* > *Advanced* > *Device Log Setting* to configure device log settings.



Configure the following settings, and then select *Apply*:

Registered Device Logs	
Roll log file when size exceeds	Enter the log file size, from 10 to 1000MB. Default: 200MB.
Roll log files at scheduled time	Select to roll logs daily or weekly. • *Daily*: select the hour and minute value in the dropdown lists. • *Weekly*: select the day, hour, and minute value in the dropdown lists.
Upload logs using a standard file transfer protocol	Select to upload logs and configure the following settings.
Upload Server Type	Select one of *FTP*, *SFTP*, or *SCP*.
Upload Server IP	Enter the IP address of the upload server.
User Name	Enter the username used to connect to the upload server.
Password	Enter the password used to connect to the upload server.
Remote Directory	Enter the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs*, or daily at a specific hour.
Upload rolled files in compressed file format	Select to compress the logs before uploading. This will result in smaller logs and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiAnalyzer system after they have been uploaded to the Upload Server.
Upload logs to cloud storage	Configure to upload logs to cloud storage. For more information, see Upload logs to cloud storage on page 546.
Local Device Log	
Send the local event logs to FortiAnalyzer / FortiManager	Select to send local event logs to another FortiAnalyzer or FortiManager device.
FQDN / IP	Enter the fully qualified domain name or IP address of the FortiAnalyzer or FortiManager.
Upload Option	Select to upload logs in real time or at a scheduled time. When selecting a scheduled time, you can specify the hour and minute to upload logs each day.
Severity Level	Select the minimum log severity level from the dropdown list. This option is only available when *Upload Option* is *Realtime*.
Reliable log transmission	Select to use reliable log transmission.
Secure connection	Select to use a secure connection for log transmission. This option is only available when *Reliable log transmission* is enabled.

Peer Certificate CN	Enter the certificate common name of syslog server. Null means no certificate CN for the syslog server. This option is only available when *Reliable log transmission* is enabled.
Automatically Delete	
	In the following settings, the time period you select determines how often the item is checked. If you select *Months*, then the item is checked once per month. If you select *Weeks*, then the item is checked once per week, and so on. For example, if you specify *Device log files older than 3 Months*, then on July 1, the logs for April, May, and June are kept and the logs for March and older are deleted.
Device log files older than	Select to enable automatic deletion of compressed log files. Enter a value in the text field, select the time period (*Days*, *Weeks*, or *Months*), and choose a time of day.
Reports older than	Select to enable automatic deletion of reports of data from compressed log files. Enter a value in the text field, select the time period, and choose a time of day.
Content archive files older than	Select to enable automatic deletion of IPS and DP archives from Archive logs. Enter a value in the text field, select the time period, and choose a time of day.
Quarantined files older than	Select to enable automatic deletion of compressed log files of quarantined files. Enter a value in the text field, select the time period, and choose a time of day.

Configuring rolling and uploading of logs using the CLI

Log rolling and uploading can be enabled and configured using the CLI. For more information, see the *FortiAnalyzer CLI Reference*.

Enable or disable log file uploads

Use the following CLI commands to enable or disable log file uploads.

To enable log uploads:

```
config system log settings
   config rolling-regular
      set upload enable
   end
```

To disable log uploads:

```
config system log settings
   config rolling-regular
```

```
      set upload disable
   end
```

Roll logs when they reach a specific size

Use the following CLI commands to specify the size, in MB, at which a log file is rolled.

To roll logs when they reach a specific size:

```
config system log settings
   config rolling-regular
      set file-size <integer>
   end
```

Roll logs on a schedule

Use the following CLI commands to configure rolling logs on a set schedule, or never.

To disable log rolling:

```
config system log settings
   config rolling-regular
      set when none
   end
```

To enable daily log rolling:

```
config system log settings
   config rolling-regular
      set upload enable
      set when daily
      set hour <integer>
      set min <integer>
   end
```

To enable weekly log rolling:

```
config system log settings
   config rolling-regular
      set when weekly
      set days {mon | tue | wed | thu | fri | sat | sun}
      set hour <integer>
      set min <integer>
   end
```

Upload logs to cloud storage

The FortiAnalyzer can be set to upload logs to cloud storage. Before enabling this feature, you must have a valid Storage Connector Service license. See License Information widget on page 63.

For information on setting up a storage fabric connector, see Creating or editing storage connectors on page 510.

To upload logs to cloud storage:

1. Go to *System Settings > Advanced > Device Log Settings*.
2. Enable *Upload logs to cloud storage* and configure the following:
   - Enter a name for the cloud storage.
   - From the *Cloud Storage Connector* dropdown, select a *Fabric Connector*.
   - In the *Remote Path* field, enter the bucket or container name from the storage account.
3. Click *Apply*.

Certificates required for cloud storage

Before logs can be uploaded to cloud storage using Amazon S3, Azure Blob, or Google connectors, the cloud provider's CA certificate(s) must be imported into FortiAnalyzer.

Third-party CA certificates, for example GlobalSign and CyberTrust, may be required. Check with your cloud storage provider to see which CA certificates are supported.

For information on how to import certificates into FortiAnalyzer, see CA certificates on page 516.

Miscellaneous Settings

Go to *System Settings > Advanced > Misc Settings* to view and configure advanced settings and download WSDL files.

Configure the following settings and then select *Apply*:

ADOM Mode	Select the ADOM mode, either *Normal* or *Advanced*. Advanced mode will allow you to assign a VDOM from a single device to a different ADOM, but will result in more complicated management scenarios. It is recommended only for advanced users.
Download WSDL file	Select the required WSDL functions then click the *Download* button to download the WSDL file to your management computer. When selecting *Legacy Operations*, no other options can be selected. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiAnalyzer will accept as well as the responses to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiAnalyzer unit and operate it or retrieve information, just as an administrator can from the GUI or CLI.
Task List Size	Set a limit on the size of the task list. Default: 2000.

FortiGuard

This section includes information on FortiGuard for FortiAnalyzer, and includes the following topics:

- Subscribing FortiAnalyzer to FortiGuard on page 548
- Licensing in an air-gap environment on page 548
- Enabling updates through a web proxy on page 552

Subscribing FortiAnalyzer to FortiGuard

To keep your FortiAnalyzer threat database up to date:

- Ensure your FortiAnalyzer can reach FortiGuard at `fds1.fortinet.com`.
- Purchase a FortiGuard Indicators of Compromise Service license and apply that license to the product registration. No change is needed on the FortiAnalyzer side.

To subscribe FortiAnalyzer to FortiGuard:

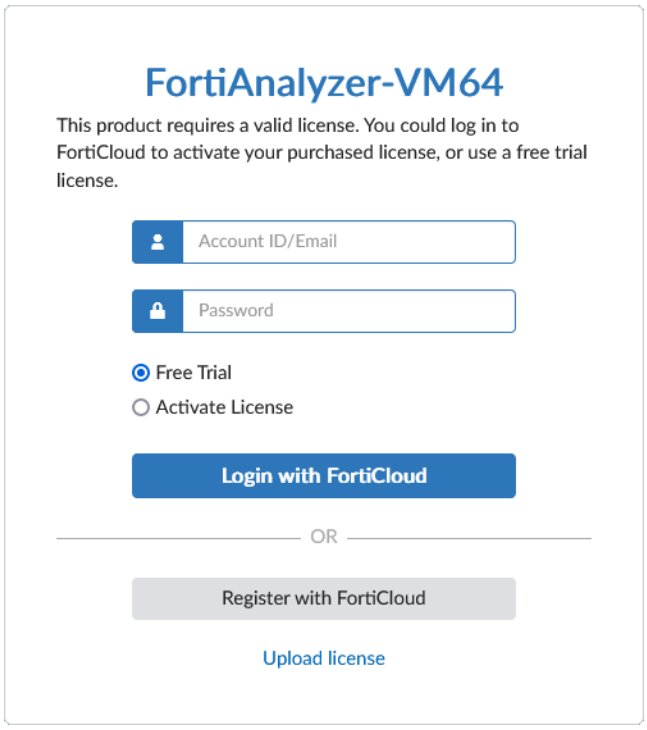
1. Go to *Dashboards* > *Status*.
2. In the *License Information* widget, find the *FortiGuard* > *Indicators of Compromise Service* field and click *Purchase*.
3. After purchasing the license, check that the *FortiGuard* > *Indicators of Compromise Service* is *Licensed* and shows the expiry date.

Licensing in an air-gap environment

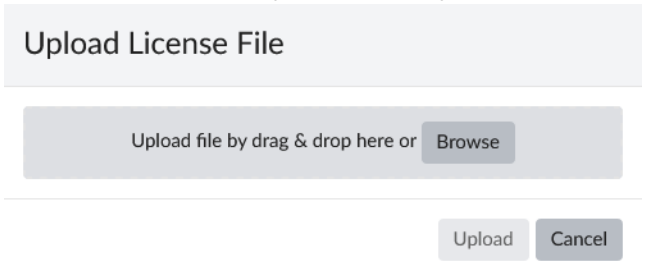
When performing the initial setup of FortiAnalyzer, you are required to register your FortiAnalyzer to FortiCare, which typically requires internet access. While operating in a closed network or air-gap environment, you must complete this step by uploading the entitlements file through the FortiAnalyzer GUI or CLI.

To register FortiAnalyzer in an air-gap environment:

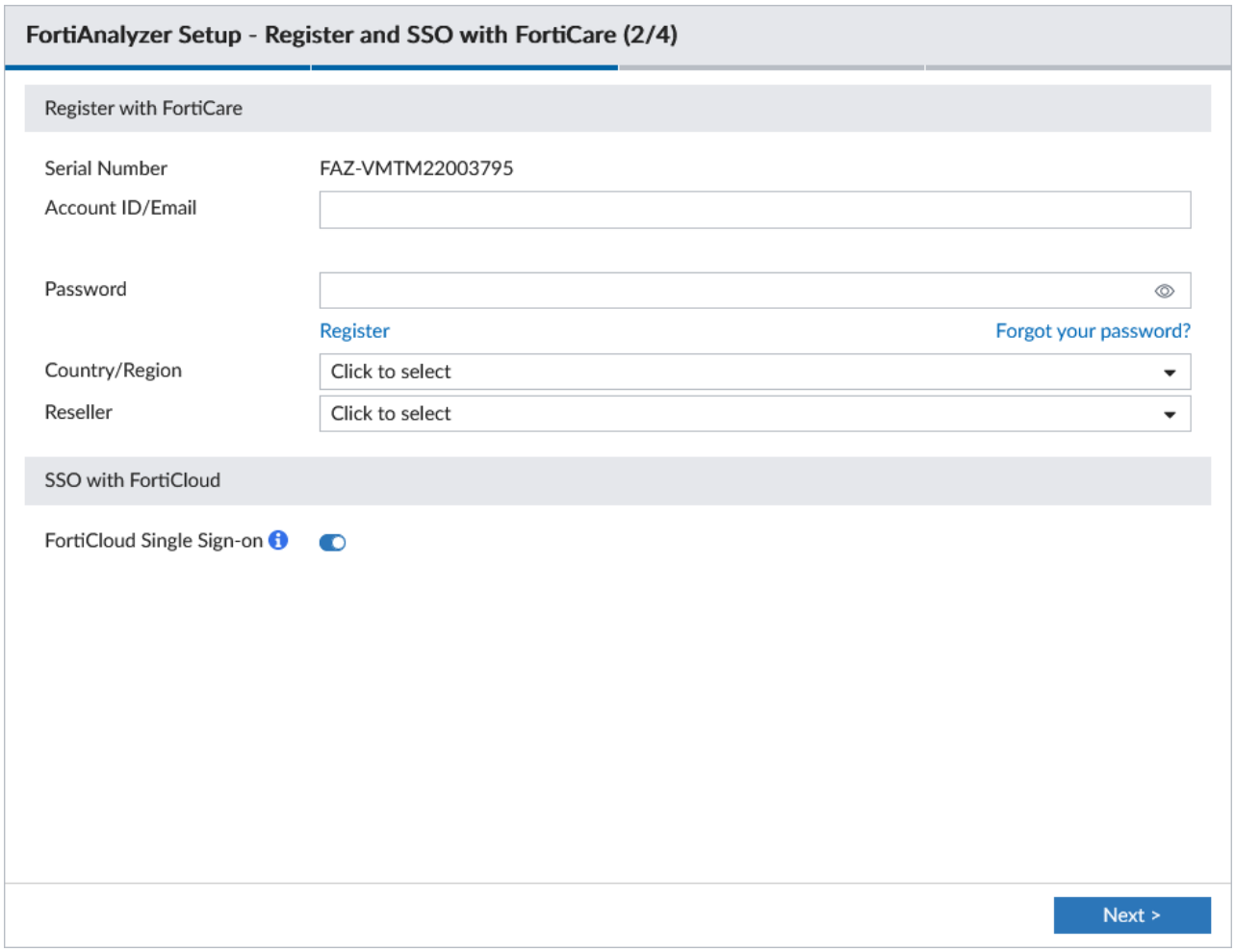
1. In FortiAnalyzer, disable access to the public FortiGuard Distribution Servers (FDS) using the following CLI commands:
```
config fmupdate publicnetwork
   set status disable
end
```
2. Connect to the FortiAnalyzer GUI, and on the FortiAnalyzer login screen, click *Upload License*.



3. Click *Browse* to select your FortiAnalyzer license or drag-and-drop the license file, and click *Upload*.



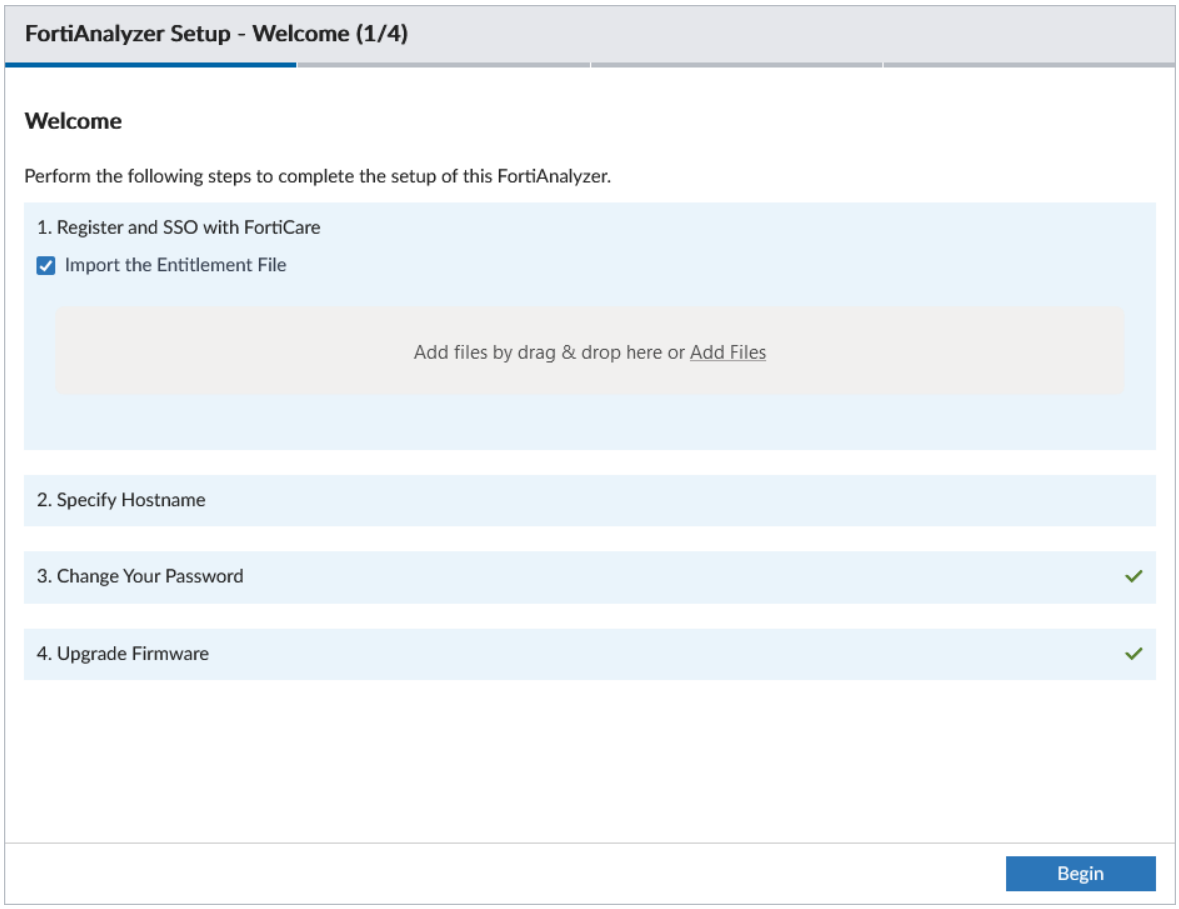
   The license file will be applied, and the FortiAnalyzer will be restarted in order to verify the license.
4. Sign in to FortiAnalyzer.
   The FortiAnalyzer Setup Wizard is displayed.



In order to access your FortiAnalyzer, it must be registered to FortiCare in the FortiAnalyzer Setup Wizard.

5. On FortiCloud, create a ticket for your FortiAnalyzer entitlements file, and Fortinet Customer Service will provide you with the file.
6. You can upload your entitlement file either through the setup wizard or through the FortiAnalyzer CLI.
   a. *Onboarding wizard*:
      i. Select *Import the Entitlement File* in the FortiAnalyzer Setup wizard.

ii. Drag and drop the entitlement file into the import area, or click *Add Files* to select the file location.



b. *Command line interface*:

i. Open the FortiAnalyzer CLI.

ii. Upload the entitlement file using the following command.

```
execute fmupdate <ftp | scp | tftp> import license <filename> <server> <port>
      <directory> <username> <password>
```

The <port> variable is only required when connecting to a remote SCP host. The <directory>, <username>, and <password> variables are only required for logging into a FTP server or SCP host to download the file. For more information, see the FortiAnalyzer CLI Reference.

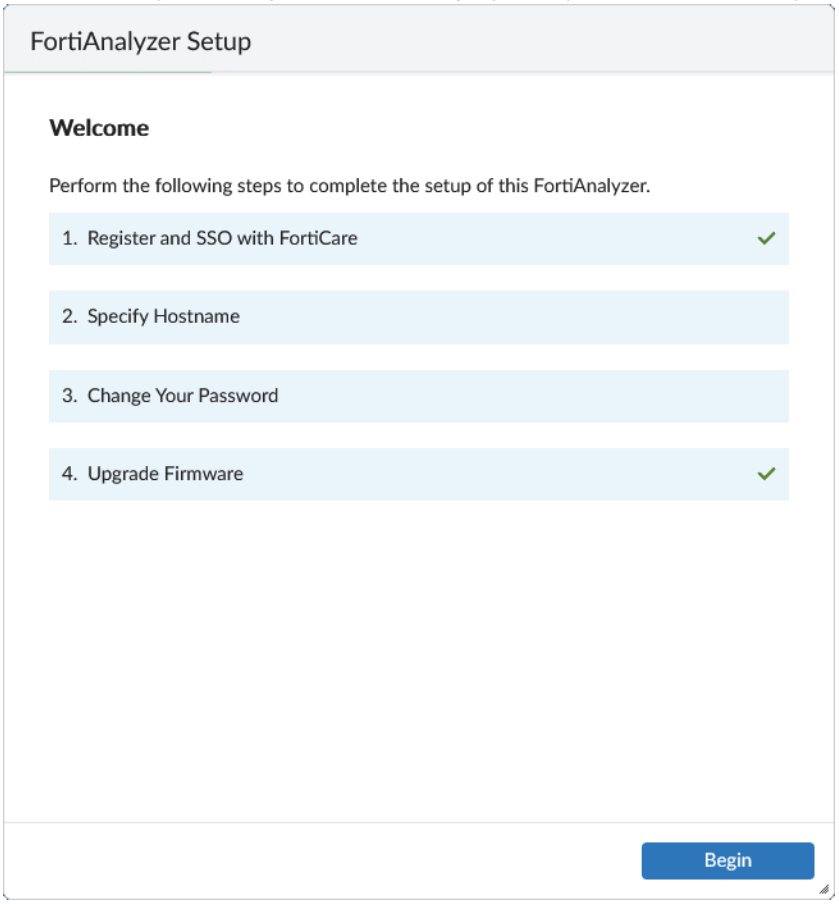
For example:

```
execute fmupdate ftp import license entitlement-file 172.10.1.10 /pub/place user1
      password1
This operation will replace the current package!
Do you want to continue? (y/n)y

Start getting file from FTP Server...
Transferred 0.001M of 0.001M in 0:00:00s (0.008M/s)
FTP transfer is successful.
Package installation is in process...
This could take some time.
```

```
Update successfully
```

7. The FortiAnalyzer Setup wizard will display that you are successfully registered with FortiCare.



Enabling updates through a web proxy

FortiAnalyzer is able to connect to the FDS/FGD server through a web proxy.

You can specify the IP address and port of the proxy server. If the proxy requires authentication, you can also specify a user name and password.

FortiAnalyzer can only have one proxy server configuration.

To enable updates to FortiAnalyzer through a proxy using the CLI:

Use the following command in the FortiAnalyzer CLI:

```
config system web-proxy
   set status enable
   set mode {proxy | tunnel} (default = tunnel)
   set address <string>
   set password <passwd>
   set port <integer>
   set username <string>
end
```

Tunnel mode (default) uses port `TCP/443`. Proxy mode uses port `TCP/80`.

For more information about the variables, see the FortiAnalyzer CLI Reference.

This feature cannot be configured in the FortiAnalyzer GUI.

Administrators

The *System Settings* administrator menus enable you to configure administrator accounts, access profiles, remote authentication servers, and adjust global administrative settings for the FortiAnalyzer unit.

Administrator accounts are used to control access to the FortiAnalyzer unit. Local and remote authentication is supported, as well as two-factor authentication. Administrator profiles define different types of administrators and the level of access they have to the FortiAnalyzer unit, as well as its authorized devices.

Global administration settings, such as the GUI language and password policies, can be configured on the *Admin Settings* pane. See Global administration settings on page 586 for more information.

This section contains the following topics:

- Trusted hosts on page 554
- Monitoring administrators on page 555
- Disconnecting administrators on page 555
- Managing administrator accounts on page 555
- Administrator profiles on page 566
- Authentication on page 572
- Global administration settings on page 586
- Multi-factor authentication on page 595

Trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative permissions. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiAnalyzer unit does not respond to administrative access attempts and cannot be pinged from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to both the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.



If you set trusted hosts and want to use the Console Access feature of the GUI, you must also set 127.0.0.1/255.255.255.255 as a trusted host.

Monitoring administrators

The *Admin Session List* lets you view a list of administrators currently logged in to the FortiAnalyzer unit.

To view logged in administrators:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button.
   The *Admin Session List* opens in the widget.
   The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, or SSH).
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).

Disconnecting administrators

Administrators can be disconnected from the FortiAnalyzer unit from the *Admin Session List*.

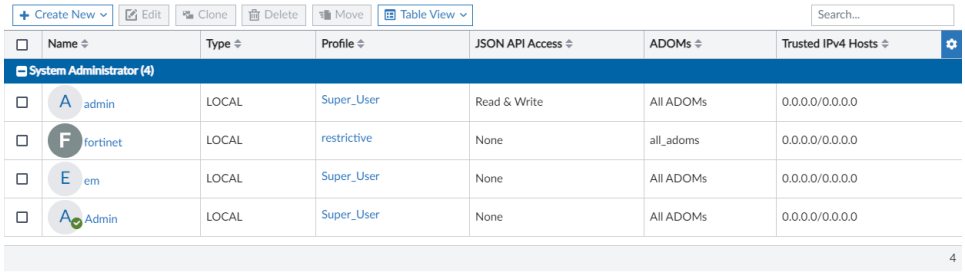
To disconnect administrators:

1. Go to *Dashboards* > *Status*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button.
   The *Admin Session List* opens in the widget.
3. Select the administrator or administrators you need to disconnect.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
   The selected administrators will be automatically disconnected from the FortiAnalyzer device.

Managing administrator accounts

Go to *System Settings* > *Administrators* to view the list of administrators and manage administrator accounts.

Only administrators with the *Super_User* profile can see the complete administrators list. If you do not have certain viewing permissions, you will not see the administrator list. When ADOMs are enabled, administrators can only access the ADOMs they have permission to access.



The following options are available:

Create New	Create a new administrator. See Creating administrators on page 557.
Edit	Edit the selected administrator. See Editing administrators on page 561.
Clone	Clone the selected administrator.
Move	Move the adminstrator to a different sequence in the table.
Delete	Delete the selected administrator or administrators. See Deleting administrators on page 562.
Table View/Tile View	Change the view of the administrator list. Table view shows a list of the administrators in a table format. Tile view shows a separate card for each administrator in a grid pattern.
Column Settings	Change the displayed columns.
Search	Search the administrators.
Change Password	Change the selected administrator's password. This option is only available from the right-click menu. See Editing administrators on page 561.

The following columns are available:

#	The sequence number.
Name	The name the administrator uses to log in.
Type	The user type, as well as if the administrator uses a wildcard.
Profile	The profile applied to the administrator. See Administrator profiles on page 566
JSON API Access	The administrators read/write privileges for JSON API.
ADOMs	The ADOMs the administrator has access to or is excluded from.
Comments	Comments about the administrator account. This column is hidden by default.
Trusted IPv4 Hosts	The IPv4 trusted host(s) associated with the administrator. See Trusted hosts on page 554.

Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator. See Trusted hosts on page 554. This column is hidden by default.
Contact Email	The contact email associated with the administrator. This column is hidden by default.
Contact Phone	The contact phone number associated with the administrator. This column is hidden by default.
FortiAI User	Indicates if the user has access to use the FortiAI assistant. This feature is only available with a valid FortiAI license. See FortiAI on page 402.

Creating administrators

To create a new administrator account, you must be logged in as a super user administrator.

You need the following information to create an account:

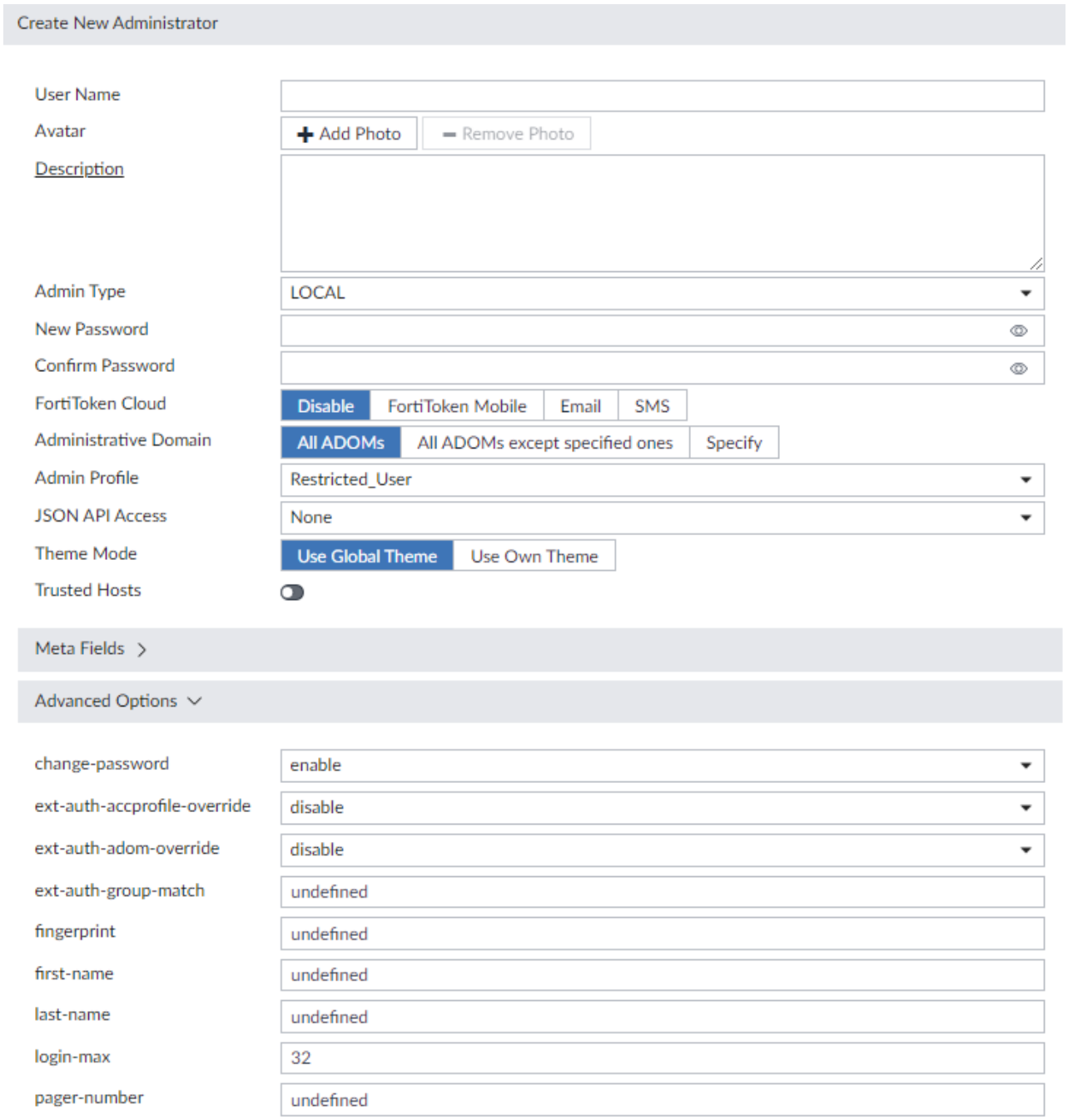
- Which authentication method the administrator will use to log in to the FortiAnalyzer unit. Local, remote, and Public Key Infrastructure (PKI) authentication methods are supported.
- What administrator profile the account will be assigned, or what system privileges the account requires.
- If ADOMs are enabled, which ADOMs the administrator will require access to.
- If using trusted hosts, the trusted host addresses and network masks.



For remote or PKI authentication, the authentication must be configured before you create the administrator. See Authentication on page 572 for details.

To create a new administrator:

1. Go to *System Settings* > *Administrators*.
2. In the toolbar, click *Create New* > *Administrator* to display the *Create New Administrator* pane.



3. Configure the following settings, and then click *OK* to create the new administrator.

User Name	Enter the name of the administrator will use to log in.
Avatar	Apply a custom image to the administrator. Click *Add Photo* to select an image already loaded to the FortiAnalyzer, or to load an new image from the management computer. If no image is selected, the avatar will use the first letter of the user name.

Comments	Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.
Admin Type	Select the type of authentication the administrator will use when logging into the FortiAnalyzer unit. One of: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, *PKI*, *Group*, or *SSO*. See Authentication on page 572 for more information.
Server or Group	Select the RADIUS server, LDAP server, TACACS+ server, or group, as required. The server must be configured prior to creating the new administrator. This option is not available if the *Admin Type* is *LOCAL* or *PKI*.
Match all users on remote server	Select this option to automatically add all users from a LDAP server specified in *Admin>Remote Authentication Server*. All users specified in the *Distinguished Name* field in the LDAP server will be added as FortiManager users with the selected Admin Profile. Select this option when the *Admin Type* is *SSO* to create one SAML SSO wildcard admin user to match all users on the identity provider (IdP) server. This FortiAnalyzer must be configured as a service provider (SP), added to the IdP, and have the same user profile and ADOM names as the IdP. If this is done, the user is assigned the same profile and ADOMs when logging in as an SSO user on this SP. See SAML admin authentication on page 581. If this option is not selected, the *User Name* specified must exactly match the LDAP user specified on the LDAP server. This option is not available if the *Admin Type* is *LOCAL* or *PKI*.
Subject	Enter a comment for the PKI administrator. This option is only available if the *Admin Type* is *PKI*.
CA	Select the CA certificate from the dropdown list. This option is only available if the *Admin Type* is *PKI*.
Required two-factor authentication	Select to enable two-factor authentication. This option is only available if the *Admin Type* is *PKI*.
New Password	Enter the password. This option is not available if *Match all users on remote server* is selected. If the *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selected. If the *Admin Type* is *RADIUS*, *LDAP*, or *TACACS+*, the password is only used when the remote server is unreachable.
Confirm Password	Enter the password again to confirm it. This option is not available if *Match all users on remote server* is selected. If the *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selected.

Force this administrator to change password upon next log on.	Force the administrator to change their password the next time that they log in to the FortiAnalyzer. This option is only available if *Password Policy* is enabled in *Admin Settings*. See Password policy on page 588.
FortiToken Cloud	Enable or disable multi-factor authentication with FortiToken Cloud, then select the token delivery method from the following options: • *FortiToken Mobile*: Use the FortiToken Mobile app to get tokens. The administrator is sent an email with a link to activate their token in the FortiToken Mobile app on their mobile device. • *Email*: Receive the token by email. • *SMS*: Receive the token by SMS message. This option is not available if Admin Type is set to *PKI* or *SSO*. For more information, see Multi-factor authentication with FortiToken Cloud on page 599.
Administrative Domain	Choose the ADOMs this administrator will be able to access. • *All ADOMs*: The administrator can access all the ADOMs. • *All ADOMs except specified ones*: The administrator cannot access the selected ADOMs. • *Specify*: The administrator can access the selected ADOMs. Specifying the ADOM shows the *Specify Device Group to Access* check box. Select the *Specify Device Group to Access* check box and select the Device Group this administrator is allowed to access. The newly created administrator will only be able to access the devices within the Device Group and sub-groups.In *Log View*, *Reports*, and so on, the administrator will only be able to view logs from the specified Device Group. If the *Admin Profile* is *Super_User*, then this setting is *All ADOMs*. This field is available only if ADOMs are enabled. See Administrative Domains (ADOMs) on page 498.
Admin Profile	Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features. See Administrator profiles on page 566. If the *Administrative Domain* is *Specify*, you can select *Single* or *Per-ADOM*. • *Single* (default): Select one admin profile to apply for all ADOMs the administrator can access. • *Per-ADOM*: Select a admin profile for each ADOM that the administrator can access. The administrator's access to the FortiAnalyzer's features will vary by ADOM according to the profiles selected.
JSON API Access	Select the permission for JSON API Access. Select *Read-Write*, *Read*, or None. The default is *None*.
Theme Mode	Select *Use Global Theme* to apply a theme to all administrator accounts.

	Select *Use Own Theme* to allow administrators to select their own theme.
Trusted Hosts	Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added. See Trusted hosts on page 554 for more information.
FortiAI User	When FortiAnalyzer has a valid FortiAI license, you can enable this field to enable access to the FortiAI assistant for this user.
Meta Fields	Optionally, enter the new administrator's email address and phone number.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced options, see the *FortiAnalyzer CLI Reference*.

Advanced options

Option	Description	Default
change-password	Enable or Disable changing password.	disable
ext-auth-accprofile-override	Enable or Disable overriding the account profile by administrators configured on a Remote Authentication Server.	disable
ext-auth-adom-override	Enable or Disable overriding the ADOM by administrators configured on a Remote Authentication Server. This will also override the *Admin Profile* configured for each ADOM.	disable
ext-auth-group-match	Specify the group configured on a Remote Authentication Server.	-
fingerprint	Specify the user certificate fingerprint based on MD5, SHA-1, or SHA-256 hash function. This option is only available if the *Admin Type* is *PKI*.	-
first-name	Specify the first name.	-
last-name	Specify the last name.	-
mobile-number	Specify the mobile number.	-
pager-number	Specify the pager number.	-
restrict-access	Enable or Disable restricted access.	disable

Editing administrators

To edit an administrator, you must be logged in as a super user administrator. The administrator's name cannot be edited. An administrator's password can be changed using the right-click menu, if the password is not a wildcard.

To edit an administrator:

1. Go to *System Settings* > *Administrators*.
2. Double-click on an administrator, right-click on an administrator and then select *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To change an administrator's password:

1. Go to *System Settings* > *Administrators*.
2. Right-click on an administrator and select *Change Password* from the menu. The *Change Password* dialog box opens.
3. If you are editing the *admin* administrator's password, enter the old password in the *Old Password* field.
4. Enter the new password for the administrator in the *New Password* and *Confirm Password* fields.
5. Select *OK* to change the administrator's password.



The current administrator's password can also be changed from the admin menu in the GUI banner. See GUI overview on page 30 for information.

Deleting administrators

To delete an administrator or administrators, you must be logged in as a super user administrator.



You cannot delete an administrator that is currently logged in to the device.



The *admin* administrator can only be deleted using the CLI.

To delete an administrator or administrators:

1. Go to *System Settings* > *Administrators*.
2. Select the administrator or administrators you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the administrator or administrators.

To delete an administrator using the CLI:

1. Open a CLI console and enter the following command:

```
config system admin user
   delete <username>
```

```
end
```

Override administrator attributes from profiles

FortiAnalyzer administrator accounts can be configured to use the *RPC Permit (JSON API Access)* and *Trusted Hosts* attributes that are defined by an administrator profile.

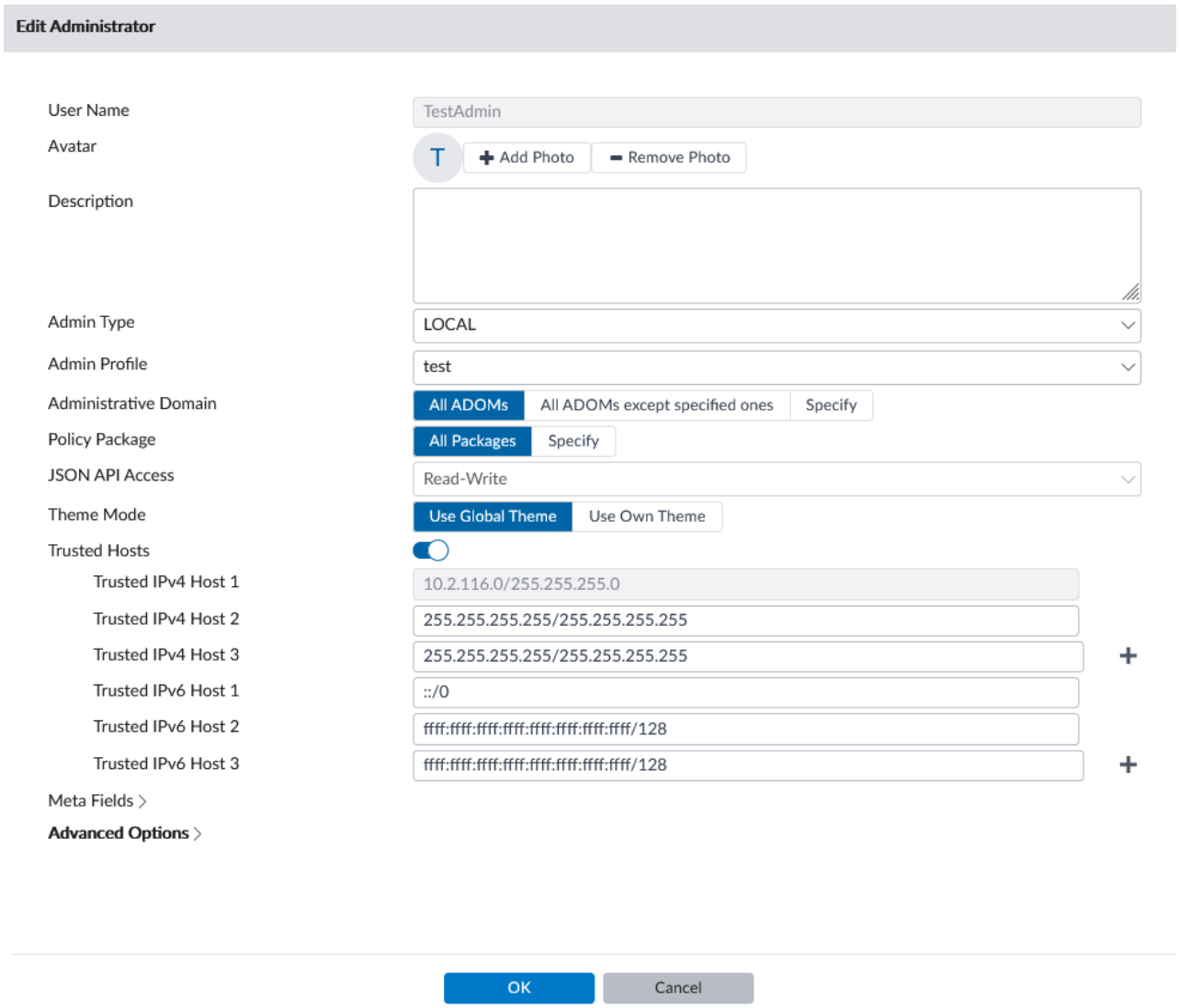
When an administrator has been configured to use the attributes from the profile, the attributes can no longer be changed by editing the administrator account.

This feature can only be configured from the FortiAnalyzer CLI.

For more information, see the FortiAnalyzer CLI Reference Guide on the Fortinet Document Library.

To use RPC Permit and Trusted Host administrator attributes from a profile:

1. Go to *System Settings* > *Administrators*, and create or edit an admin user.
2. In *Admin Profile* dropdown, select an administrator profile, and click *OK*.
3. Configure the settings for the `rpc-permit` and/or `trusthost1` attributes in the admin profile.
   Enter the following commands in the FortiAnalyzer CLI:
   ```
   config system admin profile
      edit <profile name>
         set rpc-permit {none | read | read-write}
         set trusthost1 <ip & netmask>
      end
   ```
4. Configure the admin user to use the `from-profile` option for the `rpc-permit` and/or `trusthost1` attributes.
   Enter the following commands in the FortiAnalyzer CLI:
   ```
   config system admin user
      edit <admin user>
         set rpc-permit from-profile
         set trusthost1 from-profile
   end
   ```
5. In the FortiAnalyzer GUI, go to *System Settings* > *Administrators* and view the administrator account. The attributes that were configured to use the `from-profile` setting can no longer be edited and display the settings defined in the administrator profile.



Creating administrators for the FortiAnalyzer API

In order to use the FortiAnalyzer JSON API, you must first create an administrator.

The type of administrator required depends on if you will be using a predefined API key or session-based authentication.

- **Predefined API key**: A REST API Admin is used to generate a permanent API key, which means the same user account will always share the same session and you do not need to use the login/logout endpoints. Because of this benefit, predefined API keys are useful for simplifying automation workflows.
- **Session-based authentication**: A regular FortiAnalyzer administrator with JSON API access is used with the login operation in order to get a session ID that is used in API requests.

Both types of administrators also require that you assign an *Admin Profile* with the appropriate permissions to complete the desired operations.

For more information on using the FortiAnalyzer JSON API, see the Fortinet Developer Network (FNDN).

To create REST API administrator with a predefined API key:

1. Go to *System Settings > Administrators*.
2. Click the *Create New* dropdown and choose *REST API Admin*.
3. Configure the following required information:

User Name	Enter a username.
Admin Profile	Select an admin profile that provides appropriate permissions required to complete the operations needed using the API.
JSON API Access	Select *Read* or *Read-Write* access, depending on your need.
PKI Group	(Optional) Certificate matching is supported as an extra layer of security. Both the client certificate and token must match to be granted access to the API.
CORS Allow Origin	(Optional) Cross Origin Resource Sharing (CORS) allows third-party web apps to make API requests to the FortiAnalyzer using the token.
Trusted Hosts	At least one trusted host must be configured. This trusted host should align with the IP range where the API requests will originate from.

4. Configure any remaining settings as required, such as additional role-based access control settings to restrict the administrator to specific ADOMs, policy packages, or policy blocks.
5. Click *OK* to create the REST API Admin.
   An API key is automatically generated for the REST API Admin. The API key is permanent and only shown once.
6. Copy the API key. The generated API key can be used in the request header using the bearer authentication scheme.
7. Optionally, you can generate a new API key by editing the REST API Admin and clicking *Regenerate API Key*.

To create an administrator for session-based authentication:

1. Go to *System Settings > Administrators*.
2. Click the *Create New* dropdown and choose *Administrator*.
3. Configure the following required information:

User Name	Enter a username.
New Password/Confirm Password	Enter a password.
Admin Profile	Select an admin profile that provides appropriate permissions required to complete the operations needed using the API.
JSON API Access	Select *Read* or *Read-Write* access, depending on your need.

4. Configure any remaining settings as required, such as additional role-based access control settings to restrict the administrator to specific ADOMs, policy packages, or policy blocks.
5. Click *OK* to create the administrator.

The username and password of this administrator will be used for the `login` operation on FortiAnalyzer which will generate a session ID which is used in API requests.

Administrator profiles

Administrator profiles are used to control administrator access privileges to devices or system features. Profiles are assigned to administrator accounts when an administrator is created. The profile controls access to both the FortiAnalyzer GUI and CLI.

There are the following predefined system profiles:

Restricted_User	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.
Standard_User	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.
Super_User	Super user profiles have all system and device privileges enabled. It cannot be edited.
No_Permission_User	No permission user profiles have no system or device privileges enabled.
Password_Change_User	Password change user profiles can only change passwords using the CLI or API and have no access to the FortiAnalyzer GUI or other features.

These profiles cannot be deleted, but standard and restricted profiles can be edited. New profiles can also be created as required. Only super user administrators can manage administrator profiles.

Go to *System Settings* > *Admin Profiles* to view and manage administrator profiles.

The following options are available:

Create New	Create a new administrator profile. See Creating administrator profiles on page 570.
Edit	Edit the selected profile. See Editing administrator profiles on page 571.
Clone	Clone the selected profile. See Cloning administrator profiles on page 572.
Delete	Delete the selected profile or profiles. See Deleting administrator profiles on page 572.
Search	Search the administrator profiles list.

The following information is shown:

Name	The name the administrator uses to log in.
Type	The profile type.
Description	A description of the system and device access permissions allowed for the selected profile.

Permissions

The below table lists the default permissions for the Super_User, Standard_User, and Restricted_User administrator profiles.

When *Read-Write* is selected, the user can view and make changes to the FortiAnalyzer system. When *Read-Only* is selected, the user can only view information. When *None* is selected, the user can neither view or make changes to the FortiAnalyzer system.

Setting	Predefined Administrator Profile		
	Super User	Standard User	Restricted User
System Settings `system-setting`	Read-Write	None	None
Administrative Domain `adom-switch`	Read-Write	Read-Write	None
Device Manager `device-manager`	Read-Write	Read-Write	Read-Only
Add/Delete/Edit Devices/Groups `device-op`	Read-Write	Read-Write	None
Log View/FortiView `log-viewer`	Read-Write	Read-Write	Read-Only
Incidents & Events `event-management`	Read-Write	Read-Write	Read-Only
Create & Update Incidents `update-incidents`	Read-Write	Read-Write	None
Triage Event `triage-events`	Read-Write	Read-Write	None
Execute Playbook `execute-playbook`	Read-Write	Read-Write	None
Reports `report-viewer`	Read-Write	Read-Write	Read-Only
Run Report `run-report`	Read-Write	Read-Write	None
Fabric View `fabric-viewer`	Read-Write	Read-Write	Read-Only
CLI only settings			
`device-wan-link-load-balance`	Read-Write	Read-Write	Read-Only

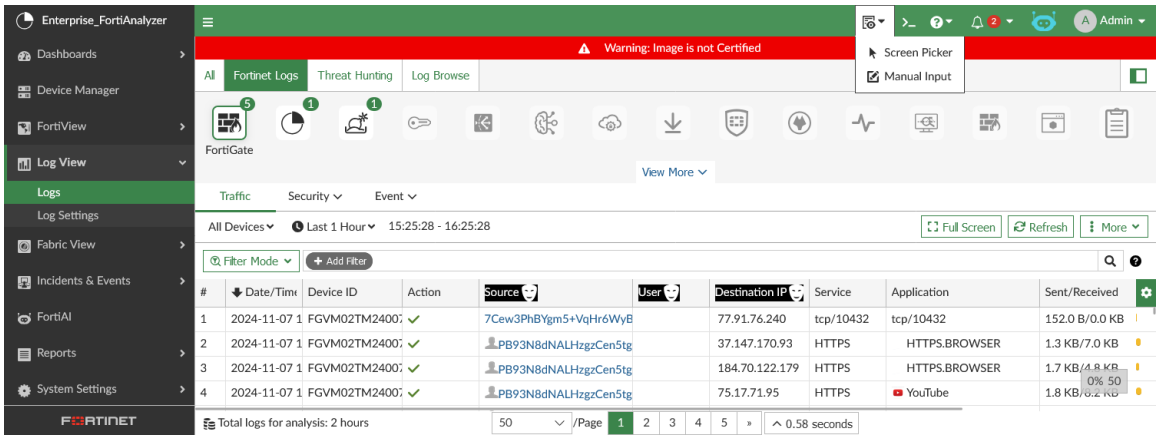
Setting	Predefined Administrator Profile		
	Super User	Standard User	Restricted User
device-ap	Read-Write	Read-Write	Read-Only
device-fortiswitch	Read-Write	Read-Write	Read-Only
adom-lock	Read-Write	Read-Write	Read-Only
device-policy-package-lock	Read-Write	Read-Write	Read-Only
extension-access	Read-Write	Read-Write	None
execute-playbook	Read-Write	Read-Write	None
script-access	Read-Write	Read-Write	None

For a description of each permission, see the FortiAnalyzer CLI Reference.

Privacy Masking

Use *Privacy Masking* to help protect user privacy by masking user information. You can select which fields to mask. Masked fields show anonymous data. You can unmask and see the original data by entering the *Data Mask Key* that you specify in the administrator profile.

When *Privacy Masking* is enabled in an administrator profile, the configured fields will be masked for those administrators. These administrators will have a *See Original Data* button in the banner, which they can use to unmask data when appropriate if they have the configured data mask key.



Administators with a *Privacy Masking*-enabled Admin Profile can download logs from *Log View*. However, the masked data is excluded from the output.

Privacy Masking and GDPR

Privacy masking can be used to support compliance to the General Data Protection Regulation (GDPR). An Admin Profile can be created that masks all fields that may contain personal data relevant to the definitions of GDPR. The administrators assigned this profile can view the fields to perform their work in FortiAnalyzer, but the data will be anonymized. The anonymized data is different for each administrator and the anonymization is changed at each login to prevent opportunity for identification. When the anonymized data is required for processing, the administrator can use a data mask key to unmask the data. Only the selected data is unmasked, leaving all other masked data anonymized.

To turn privacy masking on:

1. In *System Settings* > *Admin Profiles*, create or edit a profile.
2. Toggle *Privacy Masking* to *ON*.
3. In the *Masked Data Fields* section, select the fields you want to mask.

   The fields you select are masked in all modules that display those fields, including reports generated by the administrator.

   If fields that must be masked are not available to select, they can be manually added using the CLI. For more information, see the FortiAnalyzer CLI Reference.
4. In the *Data Mask Key* field, type the key that will allow users to unmask the data.
5. In the *Data Unmasked Time* field, type the number of days the data is initially unmasked.

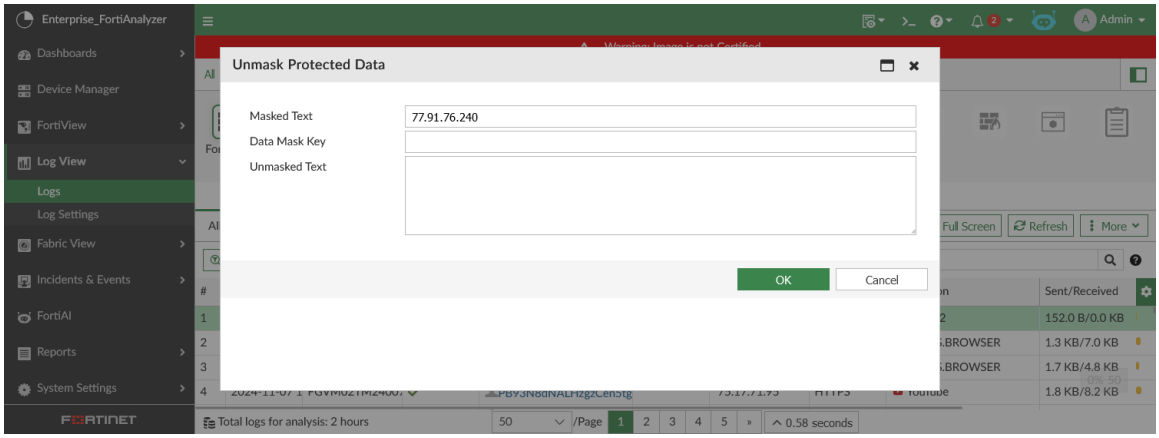
   You can enter a number between 0-365. Logs that are older than the number of days appear masked.

To see the original, unmasked data:

1. In any list showing masked data, click *See Original Data* in the banner and select *Screen Picker* or *Manual Input*.
2. If you select *Screen Picker*, click a masked field in the current pane.

   The *Unmask Protected Data* dialog displays with the field you clicked already entered.

   If you select *Manual Input*, enter the *Masked Text*.



3. Enter the *Data Mask Key* that was configured in the Admin Profile and click *OK*.

   The original data appears in the *Unmasked Text* field.

Creating administrator profiles

To create a new administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To create a custom administrator profile:

1. Go to *System Settings* > *Admin Profiles*.
2. Click *Create New* in the toolbar. The *New Profile* pane is displayed.
3. Configure the following settings:

Profile Name	Enter a name for this profile.
Description	Optionally, enter a description for this profile. While not a requirement, a description can help to know what the profiles is for, or the levels it is set to.
Permissions	Select *None*, *Read Only*, or *Read-Write* access for the categories as required.
Privacy Masking	Enable/disable privacy masking.
Masked Data Fields	Select the fields to mask: *Destination Name*, *Source IP*, *Destination IP*, *User*, *Source Name*, *Email*, *Message*, and/or *Source MAC*.
Data Mask Key	Enter the data masking encryption key. You need the *Data Mask Key* to see the original data.
Data Unmasked Time(0-365 Days)	Enter the number of days the user assigned to this profile can see all logs without masking. The logs are masked if the time period in the *Log View* toolbar is greater than the number of days in the *Data Masked Time* field. • Only integers between 0-365 are supported. • Time frame masking does not apply to real time logs. • Time frame masking applies to custom view and drill-down data.

4. Click *OK* to create the new administrator profile.

To apply a profile to an administrator:

1. Go to *System Settings* > *Administrators*.
2. Create a new administrator or edit an existing administrator. The *Edit Administrator* pane is displayed.
3. From the *Admin Profile* list, select a profile.

ADOM scoped admin profiles are only available when the *Administrative Domain* is *Specify* and the *Admin Profile* is *Single*.

Creating administrator profiles for incident & event management

Incident and event profile permissions allow security analysts to access the *Incidents & Events* module while preventing them from making changes to configurations that will affect the SLA.

To create an analyst profile:

1. Go to *System Settings* > *Admin Profiles*.
2. In the toolbar, click *Create New*.
3. In the *Profile Name* field, give the profile a distinctive name such as, *Analyst*.
4. Set *Incidents & Events* to *Read-Only*.
5. Set one or more of the following settings to *Read-Write*.

Permission	Description
Create & Update Incidents	Allows analysts to create and update incidents.
Triage Event	Allows analysts to acknowledge, comment, view logs, create new incidents, and add to existing incidents.
Execute Playbook	Allows analysts to view and run a playbook.
Run Report	Allows analysts to view, run, and export a report.

6. Configure the other settings as required, and click *OK*.

To apply a profile to an administrator:

1. Go to *System Settings* > *Administrators*.
2. Create a new administrator or edit an existing administrator. The *Edit Administrator* pane is displayed.
3. From the *Admin Profile* list, select a profile.

Editing administrator profiles

To edit an administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator. The profile's name cannot be edited. The *Super_User* profile cannot be edited, and the predefined profiles cannot be deleted.

To edit an administrator:

1. Go to *System Settings* > *Admin Profiles*.
2. Double-click on a profile, right-click on a profile and then select *Edit* from the menu, or select the profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.

3. Edit the settings as required, and then select *OK* to apply the changes.

Cloning administrator profiles

To clone an administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To edit an administrator:

1. Go to *System Settings* > *Admin Profiles*.
2. Right-click on a profile and select *Clone* from the menu, or select the profile then click *Clone* in the toolbar. The *Clone Profile* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting administrator profiles

To delete a profile or profiles, you must be logged in to an account with sufficient privileges, or as a super user administrator. The predefined profiles cannot be deleted.

To delete a profile or profiles:

1. Go to *System Settings* > *Admin Profiles*.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the profile or profiles.

Authentication

The FortiAnalyzer system supports authentication of administrators locally, remotely with RADIUS, LDAP, or TACACS+ servers, and using PKI. Remote authentication servers can also be added to authentication groups that administrators can use for authentication.

Security Assertion Markup Language (SAML) authentication can be enabled across all Security Fabric devices, enabling smooth movement between devices for the administrator. FortiAnalyzer can play the role of the identity provider (IdP) or the service provider (SP) when an external identity provider is available. See SAML admin authentication on page 581.

To use PKI authentication, you must configure the authentication before you create the administrator accounts. See Public Key Infrastructure on page 573 for more information.

To use remote authentication servers, you must configure the appropriate server entries in the FortiAnalyzer unit for each authentication server in your network. New LDAP remote authentication servers can be added and linked to all ADOMs or specific ADOMs. See LDAP servers on page 576, RADIUS servers on page 578, TACACS+ servers on page 579, and Remote authentication server groups on page 580 for more information.



If authentication fails, the FortiAnalyzer provides a generic error message indicating that there was an authentication error, and does not disclose which field contains the error.

Public Key Infrastructure

Public Key Infrastructure (PKI) authentication uses X.509 certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Administrators only need a valid X.509 certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. You will also need the following certificates:

- an X.509 certificate for the FortiManager administrator (administrator certificate)
- an X.509 certificate from the Certificate Authority (CA) which has signed the administrator's certificate (CA Certificate)

For more information on the CSR generation process, see Local certificates on page 511.

To get the CA certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
3. Select the certificate and select *Export* in the toolbar to save the `ca_fortinet.com` CA certificate to your management computer. The saved CA certificate's filename is `ca_fortinet.com.crt`.

To get the administrator certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management* > *End Entities* > *Users*.
3. Select the certificate and select *Export* in the toolbar to save the administrator certificate to your management computer. The saved CA certificate's filename is `admin_fortinet.com.p12`. This PCKS#12 file is password protected. You must enter a password on export.

To import the administrator certificate into your browser:

1. In Mozilla Firefox, go to *Options* > *Advanced* > *Certificates* > *View Certificates* > *Import*.
2. Select the file `admin_fortinet.com.p12` and enter the password used in the previous step.

To import the CA certificate into the FortiAnalyzer:

1. Log into your FortiAnalyzer.
2. Go to *System Settings* > *Certificates*.
3. Click *Create New/Import* > *CA Certificate*, and browse for the `ca_fortinet.com.crt` file you saved to your management computer, or drag and drop the file onto the dialog box. The certificate is displayed as *CA_Cert_1*.

To create a new PKI administrator account:

1. Go to *System Settings* > *Administrators*.
2. Click *Create New*. The *Create New Administrator* pane opens.
   See Creating administrators on page 557 for more information.
3. Select *PKI* for the *Admin Type*.
4. Enter a comment in the *Subject* field for the PKI administrator.
5. Select the CA certificate from the dropdown list in the *CA* field.
6. Click *OK* to create the new administrator account.

PKI authentication must be enabled via the FortiAnalyzer CLI with the following commands:

```
config system global
   set clt-cert-req enable
end
```

When connecting to the FortiAnalyzer GUI, you must use HTTPS when using PKI certificate authentication.

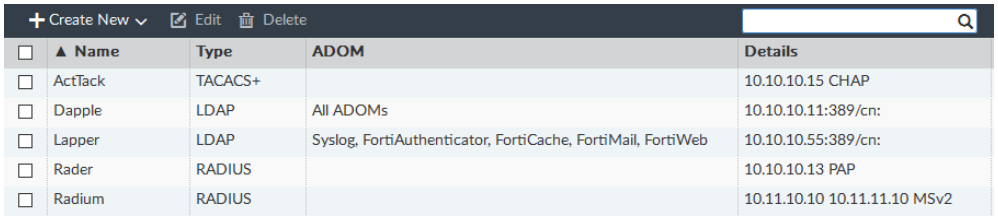
When `clt-cert-req` is set to optional, the user can use certificate authentication or user credentials for GUI login.

Managing remote authentication servers

The FortiAnalyzer system supports remote authentication of administrators using LDAP, RADIUS, and TACACS+ remote servers. To use this feature, you must configure the appropriate server entries for each authentication server in your network, see LDAP servers on page 576, RADIUS servers on page 578, and TACACS+ servers on page 579 for more information.

Remote authentication servers can be added, edited, deleted, and added to authentication groups (CLI only).

Go to *System Settings* > *Remote Authentication Server* to manage remote authentication servers.



The following options are available:

Create New	Add an LDAP, RADIUS, or TACACS+ remote authentication server. See LDAP servers on page 576, RADIUS servers on page 578, and TACACS+ servers on page 579.
Edit	Edit the selected remote authentication server. See Editing remote authentication servers on page 575.
Delete	Delete the selected remote authentication server or servers. See Deleting remote authentication servers on page 575.

The following information is displayed:

Name	The name of the server.
Type	The server type: *LDAP*, *RADIUS*, or *TACACS+*.
ADOM	The administrative domain(s) which are linked to the remote authentication server.
Details	Details about the server, such as the IP address.

Editing remote authentication servers

To edit a remote authentication server, you must be logged in to an account with sufficient privileges, or as a super user administrator. The server's name cannot be edited.

To edit a remote authentication server:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select the server then click *Edit* in the toolbar. The *Edit Server* pane for that server type opens.
3. Edit the settings as required, and then select *OK* to apply the changes.
   See LDAP servers on page 576, RADIUS servers on page 578, and TACACS+ servers on page 579 for more information.

Deleting remote authentication servers

To delete a remote authentication server or servers, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To delete a remote authentication server or servers:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the server or servers.

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiAnalyzer unit sends the administrator's credentials to the LDAP server for authentication. If the LDAP server can authenticate the administrator, they are successfully authenticated with the FortiAnalyzer unit. If the LDAP server cannot authenticate the administrator, the FortiAnalyzer unit refuses the connection.



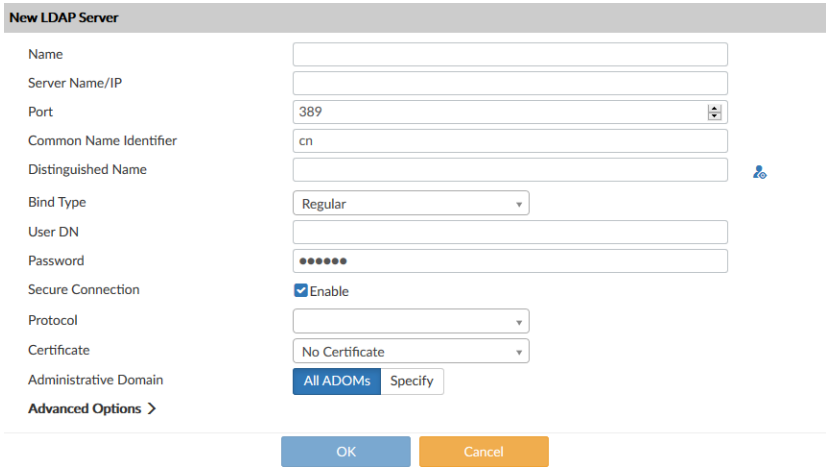
When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials.

- To secure this connection, use LDAPS on both the Active Directory server and FortiAnalyzer.
- Apply the principle of least privilege. For the LDAP regular bind operation, do not use credentials that provide full administrative access to the Windows server when using credentials.

To use an LDAP server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add an LDAP server:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Select *Create New* > *LDAP Server* from the toolbar. The *New LDAP Server* pane opens.



3. Configure the following settings, and then click *OK* to add the LDAP server.

Name	Enter a name to identify the LDAP server.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.

Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use `cn`. However, some servers use other common name identifiers such as `UID`.
Distinguished Name	The distinguished name is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Clicking the *query distinguished name* icon will query the LDAP server for the name and open the *LDAP Distinguished Name Query* window to display the results.
Bind Type	Select the type of binding for LDAP authentication: *Simple*, *Anonymous*, or *Regular*.
User DN	When the *Bind Type* is set to *Regular*, enter the user DN.
Password	When the *Bind Type* is set to *Regular*, enter the password.
Secure Connection	Select to use a secure LDAP server connection for authentication.  When configuring LDAP settings with a secure connection, certificates signed using the sha1RSA algorithm are not accepted; use supported algorithms such as sha256RSA instead.
Protocol	When *Secure Connection* is enabled, select either LDAPS or STARTTLS.
Certificate	When *Secure Connection* is enabled, select the certificate from the dropdown list.
Administrative Domain	Choose the ADOMs that this server will be linked to for reporting: *All ADOMs* (default), or *Specify* for specific ADOMs.
Advanced Options	
adom-attr	Specify an attribute for the ADOM.
attributes	Specify the attributes such as *member*, *uniquemember*, or *memberuid*.
filter	Specify the filter in the format `(objectclass=*)`
group	Specify the name of the LDAP group.
memberof-attr	Specify the value for this attribute. This value must match the attribute of the group in LDAP Server. All users part of the LDAP group with the attribute matching the *memberof-attr* will inherit the administrative permissions specified for this group.
profile-attr	Specify the attribute for this profile.
secondary-server	Specify a secondary server.
ssl-protocol	Set the lowest SSL protocol version for connection to LDAP server. By default, this will follow the global SSL protocol, which is configured in the CLI using the following command: `config system global`

```
set global-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 |
      tlsv1.2 | tlsv1.3}
end
```

For more information, see the FortiAnalyzer CLI Reference.

tertiary-server	Specify a tertiary server.

RADIUS servers

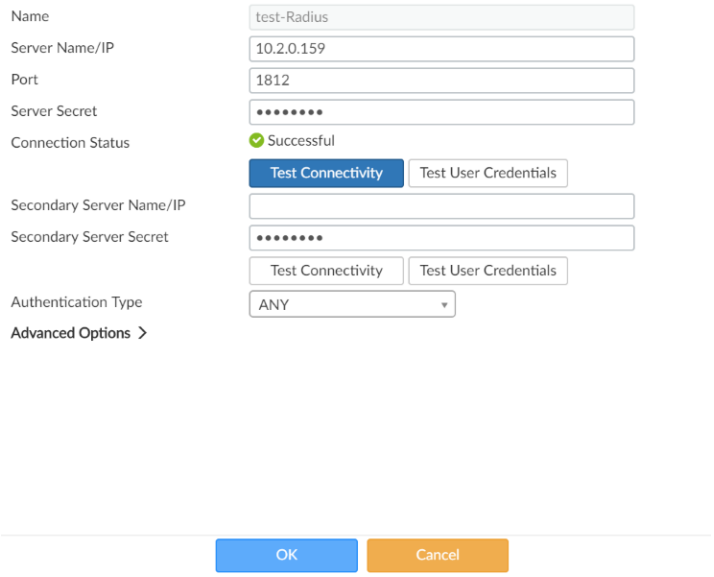
Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they type a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

You can create or edit RADIUS server entries in the server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiAnalyzer unit uses the RADIUS server to verify the administrator password at log on. The password is not stored on the FortiAnalyzer unit.

To use a RADIUS server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a RADIUS server:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Select *Create New* > *RADIUS Server* from the toolbar. The *New RADIUS Server* pane opens.



3. Configure the following settings, and then click *OK* to add the RADIUS server.

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.
Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.

Server Secret	Enter the RADIUS server secret. Click the eye icon to Show or Hide the server secret.
Test Connectivity	Click *Test Connectivity* to test the connectivity with the RADIUS server. Shows success or failure.
Test User Credentials	Click *Test User Credentials* to test the user credentials. Shows success or failure.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.
Authentication Type	Select the authentication type the RADIUS server requires. If you select the default *ANY*, FortiAnalyzer tries all authentication types.
Advanced Options	
nas-ip	Specify the IP address for the Network Attached Storage (NAS).

TACACS+ servers

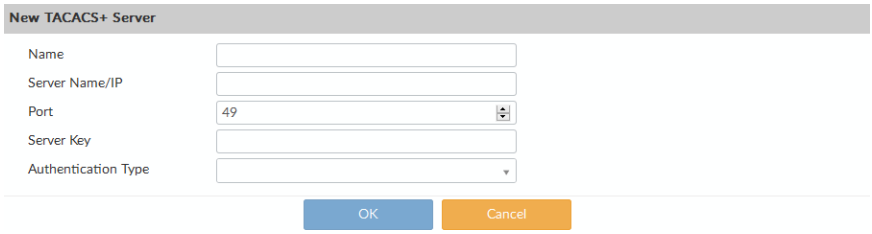
Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers. It allows a client to accept a user name and password and send a query to a TACACS authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS+ server is 49.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiAnalyzer unit contacts the TACACS+ server for authentication. If the TACACS+ server can authenticate the administrator, they are successfully authenticated with the FortiAnalyzer unit. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiAnalyzer unit.

To use a TACACS+ server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a TACACS+ server:

1. Go to *System Settings > Remote Authentication Server*.
2. Select *Create New > TACACS+ Server* from the toolbar. The *New TACACS+ Server* pane opens.



3. Configure the following settings, and then click *OK* to add the TACACS+ server.

Name	Enter a name to identify the TACACS+ server.

Server Name/IP	Enter the IP address or fully qualified domain name of the TACACS+ server.
Port	Enter the port for TACACS+ traffic. The default port is 49.
Server Key	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
Authentication Type	Select the authentication type the TACACS+ server requires. If you select the default *ANY*, FortiAnalyzer tries all authentication types.

Remote authentication server groups

Remote authentication server groups can be used to extend wildcard administrator access. Normally, a wildcard administrator can only be created for a single server. If multiple servers of different types are grouped, a wildcard administrator can be applied to all of the servers in the group.

Multiple servers of the same type can be grouped to act as backups - if one server fails, the administrator can still be authenticated by another server in the group.

To use a server group to authenticate administrators, you must configure the group before configuring the administrator accounts that will use it.

Remote authentication server groups can only be managed using the CLI. For more information, see the *FortiAnalyzer CLI Reference*.

To create a new remote authentication server group:

1. Open the admin group command shell:
   ```
   config system admin group
   ```
2. Create a new group, or edit an already create group:
   ```
   edit <group name>
   ```
3. Add remote authentication servers to the group:
   ```
   set member <server name> <server name> ...
   ```
4. Apply your changes:
   ```
   end
   ```

To edit the servers in a group:

1. Enter the following CLI commands:
   ```
   config system admin group
      edit <group name>
            set member <server name> <server name> ...
      end
   ```
   Only the servers listed in the command will be in the group.

To remove all the servers from the group:

1. Enter the following CLI commands:
   ```
   config system admin group
      edit <group name>
   ```

```
    unset member
  end
```

All of the servers in the group will be removed.

To delete a group:

1. Enter the following CLI commands:

```
config system admin group
   delete <group name>
end
```

SAML admin authentication

SAML can be enabled across devices, enabling smooth movement between devices for the administrator. FortiAnalyzer can play the role of the identity provider (IdP) or the service provider (SP) when an external identity provider is available.

When FortiGate is acting as the IdP in a Security Fabric, FortiAnalyzer can be configured to automatically connect as a Fabric SP, allowing for easy setup of SAML authentication. See Enabling SAML authentication in a Security Fabric on page 201.

Devices configured to the IdP can be accessed through the Quick Access menu which appears in the top-right corner of the main menu. The current device is indicated with an asterisk (currently only supported between FAZ/FMG).

Logging into an SP device will redirect you to the IdP login page. By default, it is a Fortinet login page. After successful authentication, you can access other SP devices from within the same browser without additional authentication.

When FortiAnalyzer is registered to FortiCloud, you can enable *Allow admins to login with FortiCloud*. This feature allows administrators to log in to FortiAnalyzer using their FortiCloud SSO account credentials. See FortiCloud SSO admin authentication on page 584.



The admin user must be created on both the IdP and SP, otherwise you will see an error message stating that the admin doesn't exist.

Alternatively, you can configure the ADOM and profile names in the SP to match the IdP. When this is done, you can create one SAML SSO wildcard admin user on the SP to match all users on the IdP server.



When accessing FortiGate from the *Quick Access* menu, if FGT is set up to use the default login page with SSO options, you must select the *via Single Sign-On* button to be automatically authenticated.

To configure FortiAnalyzer as the identity provider:

1. Go to *System Settings* > *SAML SSO*.
2. Select *Identity Provider (IdP)*.
3. In the *IdP Certificate* dropdown, choose a certificate where IdP is used.
4. Select *Download* to get the IdP certificate, used later to configure SPs.

5. (Optional) A custom login page can be created by moving the *Login Page Template* toggle to the *On* position and selecting *Customize*.
6. In the *SP Settings* table, select *Create New* to add a service provider.
7. In the *Edit Service Provider* window, configure the following information:

Name	Enter a name for the service provider.
IdP Prefix	Copy the IdP prefix. This will be required when configuring your service providers.
SP Type	Select *Fortinet* as the *SP Type*. If the SP is not a Fortinet product, select *Custom* as the *SP Type* and copy the *SP Entity ID*, *SP ACS (Login) URL*, and *SP SLS (Logout) URL* from your SPs configuration page.
SP Address	Enter the IP address of the service provider.
SAML Attributes	SAML attributes can be added to a service provider to specify ADOM and/or profile names. FortiAnalyzer acting as IdP supports the following SAML attributes: • Type: *Username*, Attribute: *username* • Type: *Profile Name*, Attribute: *profilename* • Type: *ADOM*, Attribute: *adoms* **SAML SSO Wildcard users** As long as the SP has the same user profile and ADOM names as the IdP, you do not need to re-create each user from the IdP on the SP. Instead, you can create one SAML SSO wildcard admin user on the SP with the *Match all users on remote server* setting enabled to match all users on the IdP server. When logging in as an SSO user on the SP, the user is assigned the same profile and ADOMs as are configured on the IdP. See Creating administrators on page 557.

8. Select *OK* to save changes to the service provider.
9. Click *Apply* to save the IdP configuration.

To configure FortiAnalyzer as a service provider:

1. Go to *System Settings* > *SAML SSO*.
2. Select *Service Provider (SP)*.
3. Enter the *Server Address* which is the browser accessible address for this device.
4. Optionally, configure the signing options:
   - *Authentication Request Signed*: Enable this setting to require that all authentication requests sent by the FortiAnalyzer service provider are signed. A valid SP certificate is required to enable this option.
   - *Require Assertions Signed from IdP*: Enable this setting to require that all assertions received from the IdP are signed.

5. Configure the IdP Settings:
   a. Select the IdP type as *Fortinet* or *Custom*.
   b. Enter the *IdP Address* and the *Prefix* that you obtained while configuring the IdP device.
   c. Select the IdP certificate. If this is a first-time set up, you can import the IdP certificate that you downloaded while configuring the IdP device.
6. Confirm that the information is correct and select *Apply*.
7. Repeat the steps for each FAZ/FMG that is to be set as a service provider.

For information on configuring FortiAnalyzer as an SP in a Security Fabric, see: Enabling SAML authentication in a Security Fabric on page 201.

Supported SAML attribute overrides

The following SAML attributes are accepted by FortiAnalyzer SAML service provider.

SAML Attribute	Description

username	The username of the local/SSO user. This attribute is mandatory.
	Example:
	`<Attribute Name="username">`
	`<AttributeValue>user1</AttributeValue>`
	`</Attribute>`

profilename	The *Profile* assigned to the user. If a matching profile exists on the FortiAnalyzer, it will be assigned to the user. This attribute is optional.
	Example:
	`<Attribute Name="profilename">`
	`<AttributeValue>SSOPROFILE</AttributeValue>`
	`</Attribute>`

adoms	The *ADOM(s)* to which the user will have access. Multiple ADOMs can be specified in the SAML assertion if supported by the IdP. This attribute is optional.
	Example:
	`<Attribute Name="adoms">`
	`<AttributeValue>ADOM1</AttributeValue>`
	`<AttributeValue>ADOM2</AttributeValue>`
	`</Attribute>`

You can use the following command in the CLI to verify the correct adoption of the SAML attributes by FortiAnalyzer.

```
diagnose system admin-session list
```

For example:

```
diagnose system admin-session list
*** entry 0 ***
   session_id: 57410 (seq: 0)
   username: user1
   admin template: SSO
   from: SSO(192.168.50.188) (type 7)
   profile: SSOPROFILE
   adom: adom1
   session length: 3 (seconds)
```

FortiCloud SSO admin authentication

When FortiAnalyzer is registered to FortiCloud, you can enable login to FortiAnalyzer using your FortiCloud SSO account.

By default, only the FortiCloud account ID which the FortiAnalyzer is registered to can be used to log into FortiAnalyzer. Additional SSO users can be configured as IAM users in FortiCloud. See IAM user account login on page 585.

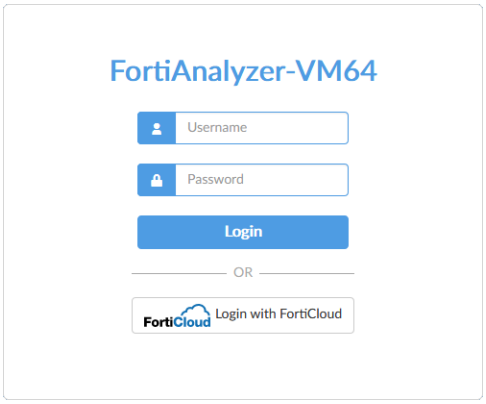
To enable login with FortiCloud:

1. Before enabling this feature, FortiAnalyzer must be registered to FortiCloud, and a FortiCloud account must be configured.
   You can check your FortiCloud registration status in *Dashboards* > *Status* in the *License Information* widget.

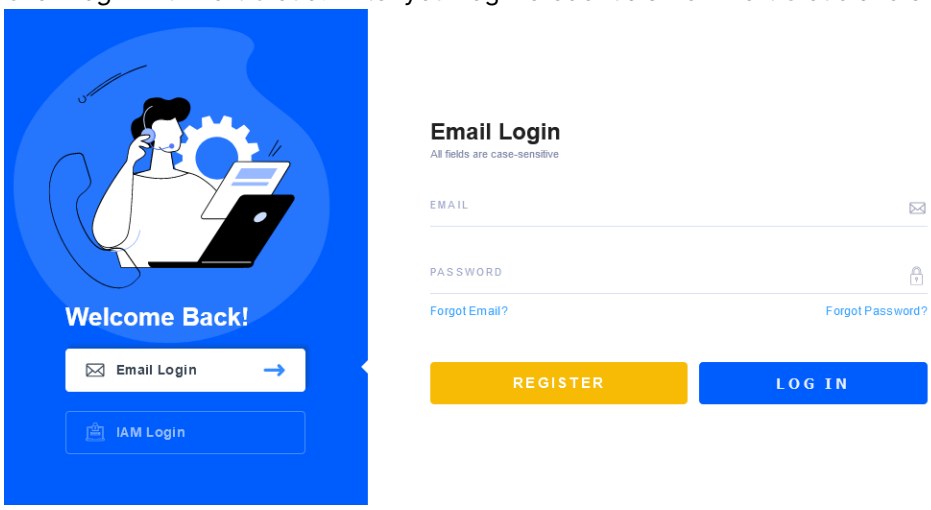
2. Go to *System Settings* > *SAML SSO*, and enable *Allow admins to login with FortiCloud*.



3. Sign out of FortiAnalyzer to return to the sign in screen.
   An option to *Login with FortiCloud* is now visible on the FortiAnalyzer login page.



4. Click *Login with FortiCloud*. Enter your login credentials from FortiCloud and click *LOGIN*.



You are signed in with your FortiCloud user account.

IAM user account login

FortiCloud supports the creation of additional users called IAM users. Once created, you can use the IAM user account to sign in to FortiAnalyzer.

To sign in using a FortiCloud IAM user:

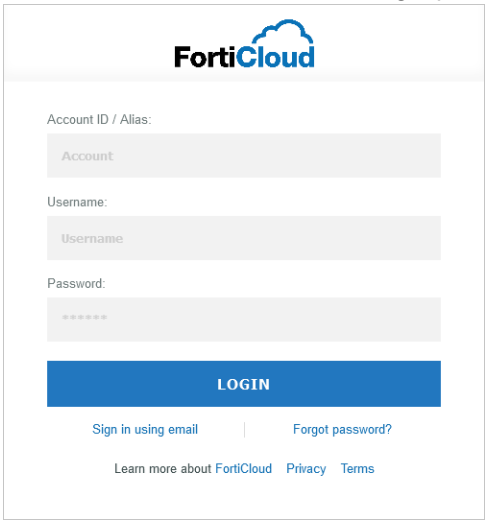
1. In FortiCloud, create one or more additional IAM user accounts. See Identity and Access Management (IAM).

The IAM users must have the following portal included in their *Permission Profile*:
- *FortiOS SSO*
  - *Access* = enabled
  - *Access Type* = *Admin*

---

2. In FortiAnalyzer, enable *Allow admins to login with FortiCloud* in *System Settings > SAML SSO*.
3. Sign out of FortiAnalyzer, return to the FortiAnalyzer sign on page, and click *Login with FortiCloud*.

4. At the bottom of the FortiCloud login portal, click *Sign in as IAM user*.



5. Enter your IAM user credentials.
   You are signed in using your FortiCloud IAM account.

Global administration settings

The administration settings page provides options for configuring global settings for administrator access to the FortiAnalyzer device. Settings include:

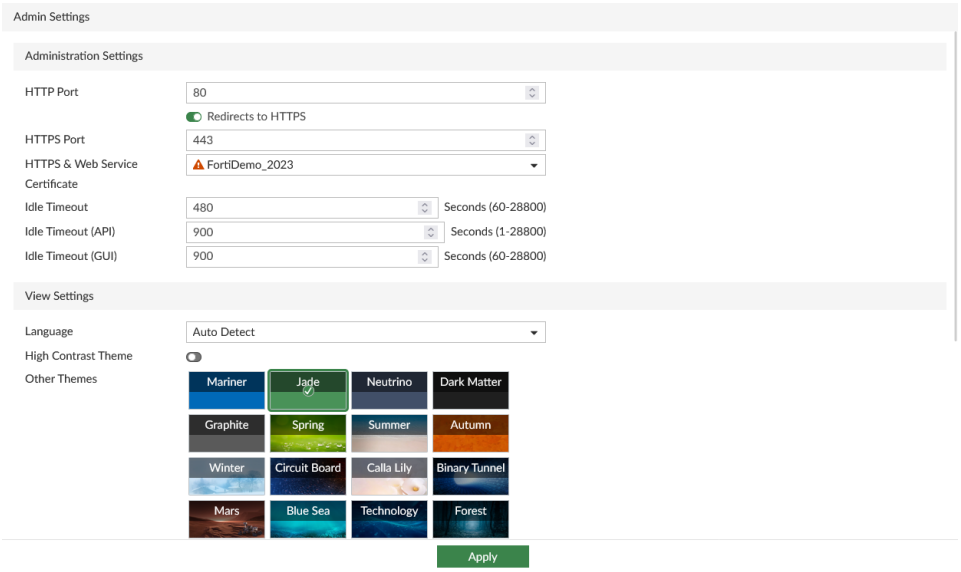
- Ports for HTTPS and HTTP administrative access
  To improve security, you can change the default port configurations for administrative connections to the FortiAnalyzer. When connecting to the FortiAnalyzer unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiAnalyzer unit using port 8080, the URL would be `https://192.168.1.99:8080`. When you change to the default port number for HTTP or HTTPS, ensure that the port number is unique.
- Idle timeout settings
  By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management computer is left unattended.
- GUI language
  The language the GUI uses. For best results, you should select the language used by the management computer.
- GUI theme
  The default color theme of the GUI is *Jade*. You can choose another color or an image.
- Password policy
  Enforce password policies for administrators.



Only super user administrators can access and configure the administration settings. The settings are global and apply to all administrators of the FortiAnalyzer unit.

To configure the administration settings:

1. Go to *System Settings* > *Settings*.



2. Configure the following settings as needed, then click *Apply* to save your changes to all administrator accounts:

Administration Settings		
	HTTP Port	Enter the TCP port to be used for administrative HTTP access. Default: 80. Select *Redirect to HTTPS* to redirect HTTP traffic to HTTPS.
	HTTPS Port	Enter the TCP port to be used for administrative HTTPS access. Default: 443.
	HTTPS & Web Service Server Certificate	Select a certificate from the dropdown list.
	Idle Timeout	Enter the number of seconds an administrative connection can be idle before the administrator must log in again, from 60 to 28800 (eight hours). See Idle timeout on page 593 for more information.
	Idle Timeout (API)	Enter the number of seconds an administrative connection to the API can be idle before the administrator must log in again, from 1 to 28800 (eight hours). Default: 900.
	Idle Timeout (GUI)	Enter the number of seconds an administrative connection to the GUI can be idle before the administrator must log in again, from 60 to 28800 (eight hours). Default: 900.
View Settings		
	Language	Select a language from the dropdown list. See GUI language on page 593 for more information.

	High Contrast Theme	Toggle *ON* to enable a high contrast dark theme in order to make the FortiAnalyzer GUI more accessible, and to aid people with visual disability in using the FortiAnalyzer GUI.
	Other Themes	Select a theme for the GUI. The selected theme is not applied until you click *Apply*, allowing to you to sample different themes. Default: Jade.
Password Policy		Click to enable administrator password policies. See Password policy on page 588 and Password lockout and retry attempts on page 592 for more information.
	Minimum Length	Select the minimum length for a password, from 8 to 32 characters. Default: 8.
	Must Contain	Select the types of characters a password must contain.
	Admin Password Expires after	Select the number of days a password is valid for, after which it must be changed.
	Enforce Password History	Enable to set the number of unique new passwords that must be used before an old password can be reused, from 1 to 20.
Fabric Authorization		Specifies the accessible management IP of FortiAnalyzer for FortiOS to retrieve and use for authorization of a Security Fabric connection to FortiAnalyzer. When you are using FortiOS to create a Security Fabric connection to FortiAnalyzer, a browser pop window is displayed and connects to FortiAnalyzer as part of the authorization process. FortiOS retrieves the information specified in FortiAnalyzer and provides it to the browser popup window to successfully connect to FortiAnalyzer. Without this information, the browser popup window cannot connect to FortiAnalyzer in certain topologies, such as when NAT is used. See also Security Fabric authorization information for FortiOS on page 594.
	Authorization Address	Type the accessible management IP for FortiAnalyzer.
	Authorization Port	If a non-default port is used for the management port of FortiAnalyzer, specify the custom port.

Password policy

You configure a password policy for local users from *System Settings* > *Settings*.

When setting up FortiAnalyzer 7.6.4 or later, a password policy is enabled and configured by default. However, existing password policy settings are maintained after upgrading. For example, if the password policy is disabled prior to upgrading to FortiAnalyzer 7.6.4 or later, it will remain disabled after the upgrade.



When a password policy is enabled, only the current password is remembered for each user in password reuse history.

To configure the password policy:

1. Go to *System Settings* > *Settings*.
2. Enable *Password Policy*.
3. Configure the following settings, then click *Apply* to apply to password policy.

Minimum Length	Specify the minimum number of characters that a password must be, from 8 to 32. Default: 8.
Must Contain	Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, and/or special characters. The following settings are selected by default: • *Uppercase Letters* • *Lowercase Letters* • *Numbers (0-9)* • *Special Characters*
Admin Password Expires after	Specify the number of days a password is valid for. When the time expires, an administrator will be prompted to enter a new password. Default: 0.
Enforce Password History	Enable to set the number of unique new passwords that must be used before an old password can be reused, from 1 to 20. Default: disabled.

Enhanced administrator password security

The PBKDF2 hashing scheme with randomized salts is now used to store system administrator passwords on the FortiAnalyzer to enhance security. Previously the SHA256 hashing algorithm was used.

With this change, a new command is available to maintain FortiAnalyzer downgrade:

```
config system password-policy
    set login-lockout-upon-downgrade {enable | disable}
end
```

`set login-lockout-upon-downgrade {enable | disable}`	Enable/disable system administrator login lockout after downgrade to FortiAnalyzer firmware that does not support safer passwords (default = disable). When disabled, system administrator passwords with SHA256 hash are kept after successfully converting to PBKDF2 hash. SHA256 hashed passwords are used after downgrading to a firmware version that does not support PBKDF2 hashed passwords. When enabled, system administrator passwords that are converted to PBKDF2 hash will immediately remove the SHA256 hashed password. Upon downgrading the FortiAnalyzer firmware to a lower version, where safer passwords are unsupported, the administrators will be locked out.

When creating a new administrative user in FortiAnalyzer 7.6.3 or later, the PBKDF2 hashing scheme is used to store the password. When displayed in the CLI, the password is encoded with a prefix of PB2:

```
# config system admin user
(user)# edit admin2
new entry 'admin2' added
(admin2)# set profileid Super_User
Super user profile selected, adom-access will be set to all
(admin2)# set password 123456
(admin2)# show
config system admin user
    edit "admin2"
        set password ENC
PB2q4Knobgbqda31z0OHOvc19fq5QhvXCuLqXqyaMK3k2iN3zgvyaLAxLKAThYl8U+teWCAeW2rOMYodqCtQi9rOjQkSEdZ1hH
TBMiZAqirRVA=
        set old-password ENC SH2ak0hUxGlkppXtwCaAz0wKZrHiFKTdjOO7XDDSoTQibDNyqfkFYKLLocCHz0=
        set profileid "Super_User"
            config meta-data
                edit "Contact Email"
                next
                edit "Contact Phone"
                next
            end
    next
end
```

Upgrade

To view system administrator passwords before and after upgrade to FortiAnalyzer 7.6.3:

1. Before upgrade to FortiAnalyzer 7.6.3 or later, view the encoded password. The encoded password shows a SH2 prefix because it was hashed with the SHA256 algorithm:

   ```
   (admin2)# show
   config system admin user
       edit "admin2"
           set password ENC SH2ak0hUxGlkppXtwCaAz0wKZrHiFKTdjOO7XDDSoTQibDNyqfkFYKLLocCHz0=
           set profileid "Super_User"
               config meta-data
                   edit "Contact Email"
                   next
                   edit "Contact Phone"
                   next
               end
       next
   end
   ```

2. Upgrade to FortiAnalyzer 7.6.3 or later. Each system administrator password hashed with SHA256 is stored on FortiAnalyzer until each system administrator successfully logs in to FortiAnalyzer.

   If a system administrator does not log in to FortiAnalyzer after upgrading to 7.6.3 or later, their password remains saved as the SHA256 hashed password.
3. Log in to FortiAnalyzer. The password is converted to a PBKDF2 hashed password.

4. View the encoded password. The encoded password shows a PB2 prefix because it was hashed with the PBKDF2 algorithm:

```
FAZ-VM64-HV # show system admin user
config system admin user
    ...
    edit "admin2"
        set password ENC
PB2q4Knobgbqda31z0OHOvc19fq5QhvXCuLqXqyaMK3k2iN3zgvyaLAxLKAThYl8U+teWCAeW2rOMYodqCtQi9rOjQkSEd
Z1hHTBMiZAqirRVA=
        set old-password ENC SH2ak0hUxGlkppXtwCaAz0wKZrHiFKTdjOO7XDDSoTQibDNyqfkFYKLLocCHz0=
        set profileid "Super_User"
            config meta-data
                edit "Contact Email"
                next
                edit "Contact Phone"
                next
            end
    next
end
```

Downgrade

To support downgrading to an older version that does not support the PBKDF2 hashed password, by default, the old SHA256 hashed password is still stored in the system after being converted to PBKDF2. This is controlled by the following setting that is disabled by default:

```
config system password-policy
    set login-lockout-upon-downgrade disable
end
```

The SHA256 hashed password will be removed from the system as soon as it is converted to a PBKDF2 hashed password upon a successful login.

During a downgrade operation, the system will display the following (see bold text below):

```
Downgrade FAZ_VM64 image from v7.6.3-b3481-250409(Interim) to v7.4.6-b2588-241218(GA.M)

Configure may be lost in a downgrade.

Warning: downgrade image from maturity Interim to GA.M

Image is GA Certified

You are downgrading to a version that does not support safer passwords.
After downgrade, some administrative user no longer will be able to login with local
authentication.

This operation will replace the current firmware version and reboot the system!
Do you want to continue? (y/n)y
```

Administrators can choose to proceed or abort this downgrade.

Finally, if an administrator wants to restore the SHA256 hashed password for a downgrade, they can do the following:

1. Disable the login-lockout-upon-downgrade option.
2. Log out the current administrator.
3. For each system administrator, log in to the FortiAnalyzer to generate the SHA256 hashed password.



After administrator passwords are converted to PBKDF2 hashed passwords, loading the config file to an older version that does not support safer passwords will lock out the administrators.

Password lockout and retry attempts

By default, the number password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts and the default wait time before the administrator can try to enter a password again can be customized. Both settings can be configured using the CLI.

To configure the lockout duration:

1. Enter the following CLI commands:
```
config system global
   set admin-lockout-duration <seconds>
end
```

To configure the number of retry attempts:

1. Enter the following CLI commands:
```
config system global
   set admin-lockout-threshold <failed_attempts>
end
```

Example

To set the lockout threshold to one attempt and set a five minute duration before the administrator can try to log in again, enter the following CLI commands:

```
config system global
   set admin-lockout-duration 300
   set admin-lockout-threshold 1
end
```

GUI language

The GUI supports multiple languages, including:

- English
- Simplified Chinese
- Traditional Chinese
- Japanese
- Korean
- Spanish
- French

By default, the GUI language is set to *Auto Detect*, which automatically uses the language used by the management computer. If that language is not supported, the GUI defaults to English. For best results, you should select the language used by the operating system on the management computer.

For more information about language support, see the FortiAnalyzer Release Notes.

To change the GUI language:

1. Go to *System Settings* > *Settings*.
2. Under the *View Settings*, in the *Language* field, select a language, or *Auto Detect*, from the dropdown list.
3. Click *Apply* to apply the language change.

Idle timeout

To ensure security, the idle timeout period should be short. By default, administrative sessions are disconnected if no activity takes place for 900 seconds (15 minutes). This idle timeout is recommended to prevent anyone from using the GUI on a PC that was logged in to the GUI and then left unattended.

There are multiple idle timeout settings, which allows you to control idle timeout for API, GUI, and SSO sessions individually. The *Idle Timeout* setting controls all other idle timeout, including the idle timeout for SSH and console.



The idle timeout for SSO can only be set in the CLI using the following command:

```
config system admin setting
   set idle_timeout_sso <integer>
end
```

For more information, see the FortiAnalyzer CLI Reference in the Fortinet Document Library.

To change the idle timeout:

1. Go to *System Settings* > *Settings*.
2. In the *Idle Timeout* field, enter the idle timeout in seconds (60 - 28800, default = 900).
3. In the *Idle Timeout (API)* field, enter the idle timeout for API sessions in seconds (1 - 28800, default = 900).
4. In the *Idle Timeout (GUI)* field, enter the idle timeout in seconds (60 - 28800, default = 900).

5. Click *Apply*.
   If you need to set the idle timeout for SSO sessions, you must use the FortiAnalyzer CLI.

Security Fabric authorization information for FortiOS

When using FortiOS to create a Security Fabric connection to FortiAnalyzer, the process includes device authorization. The authorization process uses a browser popup window that requires communication to FortiAnalyzer. Depending on the topology, communication might fail, unless you specify the accessible management IP address and/or port of FortiAnalyzer that the browser popup window in FortiOS can use to connect with FortiAnalyzer.

FortiOS retrieves this information from FortiAnalyzer and makes it available to the browser popup window used for the authorization process.

To specify the authorization address and/or port:

1. In FortiAnalyzer, go to *System Settings > Settings*.
2. Under *Fabric Authorization*, set the following options:

Authorization Address	Type the GUI-accessible URL for FortiAnalyzer.
Authorization Port	If a non-default port is used, type the port number used for GUI access to FortiAnalyzer.

3. Click *Apply*.

Control administrative access with a local-in policy

Administrative access to FortiAnalyzer can be controlled by a IPv4/IPv6 local-in policy. This feature can only be configured using the FortiAnalyzer CLI.

For more information, see the FortiAnalyzer CLI Reference Guide on the Fortinet Docs Library.

To create an IPv4 local-in policy to control administrator access to FortiAnalyzer:

1. Access the FortiAnalyzer CLI.
2. Enter the following command to create the IPv4 local-in policy:
```
config system local-in-policy
   edit <policy ID>
   new entry '<Policy ID>' added
```
3. Configure additional settings for the local-in policy using the `set` command.
   For example:
```
set
   action - Action performed on traffic matching this policy.
   dport - Destination port number (0 for all).
   dst - Destination IP and mask.
   intf - Incoming interface name.
   protocol - Traffic protocol.
   src - Source IP and mask.
```

To create an IPv6 local-in policy to control administrator access to FortiAnalyzer:

1. Access the FortiAnalyzer CLI.
2. Enter the following command to create the IPv6 local-in policy:
```
config system local-in-policy6
   (local-in-policy6)# edit <policy ID>
   new entry '<Policy ID>' added
```
3. Configure additional settings for the local-in policy using the `set` command.
   For example:
```
set
  action - Action performed on traffic matching this policy.
  dport - Destination port number (0 for all).
  dst - Destination IP and mask.
  intf - Incoming interface name.
  protocol - Traffic protocol.
  src - Source IP and mask.
```



FortiAnalyzer local-in policies support multiple entries when configuring ports, addresses, and interfaces. For example:
```
config system local-in-policy
   edit 1
      set description "IP group 123"
      set dport "22" "443" "80" "8080" "514"
      set dst "1.1.1.1/16" "2.2.2.2/24" "3.3.3.3/32"
      set intf "port1" "port2"
      set src "1.1.1.1/16" "2.2.2.2/24"
```

Multi-factor authentication

FortiAnalyzer supports the following two methods for multi-factor authentication:

- FortiAuthenticator
- FortiToken Cloud

Multi-factor authentication with FortiAuthenticator

To configure two-factor authentication for administrators with FortiAuthenticator you will need the following:

- FortiAnalyzer
- FortiAuthenticator
- FortiToken

Configuring FortiAuthenticator

On the FortiAuthenticator, you must create a local user and a RADIUS client.

Before proceeding, ensure you have configured your FortiAuthenticator, created a NAS entry for your FortiAnalyzer, and created or imported FortiTokens.

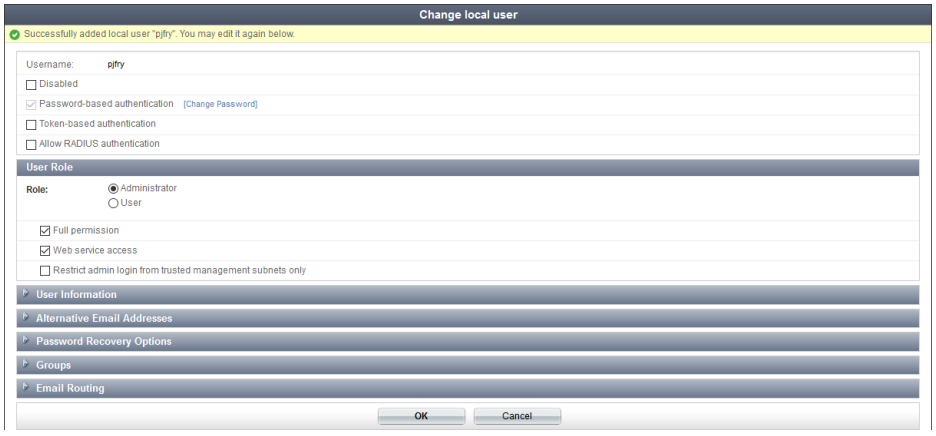
For more information, see the RADIUS Interoperability Guide and FortiAuthenticator Administration Guide in the Fortinet Document Library.

To create a local user:

1. Go to *Authentication > User Management > Local Users*.
2. Click *Create New* in the toolbar.
3. Configure the following settings:

Username	Enter a user name for the local user.
Password creation	Select Specify a password from the dropdown list.
Password	Enter a password. The password must be a minimum of 8 characters.
Password confirmation	Re-enter the password. The passwords must match.
Allow RADIUS authentication	Enable to allow RADIUS authentication.
Role	Select the role for the new user.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.

4. Click *OK* to continue to the *Change local user* page.



5. Configure the following settings, then click *OK*.

Disabled	Select to disable the local user.
Password-based authentication	Leave this option selected. Select *[Change Password]* to change the password for this local user.

Token-based authentication	Select to enable token-based authentication.
Deliver token code by	Select to deliver token by FortiToken, email, or SMS. Click *Test Token* to test the token.
Allow RADIUS authentication	Select to allow RADIUS authentication.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.
User Role	
Role	Select either *Administrator* or *User*.
Full Permission	Select to allow Full Permission, otherwise select the admin profiles to apply to the user. This option is only available when *Role* is *Administrator*.
Web service	Select to allow Web service, which allows the administrator to access the web service via a REST API or by using a client application. This option is only available when *Role* is *Administrator*.
Restrict admin login from trusted management subnets only	Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when *Role* is *Administrator*.
Allow LDAP Browsing	Select to allow LDAP browsing. This option is only available when *Role* is *User*.

Create a RADIUS client:

1. Go to *Authentication > RADIUS Service > Clients*.
2. Click *Create New* in the toolbar.
3. Configure the following settings, then click *OK*.

Name	Enter a name for the RADIUS client entry.
Client name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiAnalyzer.
Secret	Enter the server secret. This value must match the FortiAnalyzer RADIUS server setting at *System Settings > Remote Authentication Server*.
First profile name	See the *FortiAuthenticator Administration Guide*.
Description	Enter an optional description for the RADIUS client entry.
Apply this profile based on RADIUS attributes	Select to apply the profile based on RADIUS attributes.
Authentication method	Select *Enforce two-factor authentication* from the list of options.
Username input format	Select specific user name input formats.

Realms	Configure realms.
Allow MAC-based authentication	Optional configuration.
Check machine authentication	Select to check machine based authentication and apply groups based on the success or failure of the authentication.
Enable captive portal	Enable various portals.
EAP types	Optional configuration.



For more information, see the *FortiAuthenticator Administration Guide*, available in the Fortinet Document Library.

Configuring FortiAnalyzer

On the FortiAnalyzer, you need to configure the RADIUS server and create an administrator that uses the RADIUS server for authentication.

To configure the RADIUS server:

1. Go to *System Settings* > *Remote Authentication Server*.
2. Click *Create New* > *RADIUS Server* in the toolbar.
3. Configure the following settings, then click *OK*.

Name	Enter a name to identify the FortiAuthenticator.
Server Name/IP	Enter the IP address or fully qualified domain name of your FortiAuthenticator.
Port	Enter the port for FortiAuthenticator traffic.
Server Secret	Enter the FortiAuthenticator secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
Secondary Server Secret	Enter the secondary FortiAuthenticator secret, if applicable.
Authentication Type	Select the authentication type the FortiAuthenticator requires. If you select the default *ANY*, FortiAnalyzer tries all authentication types. **Note**: RADIUS server authentication for local administrator users stored in FortiAuthenticator requires the *PAP* authentication type.

To create the administrator:

1. Go to *System Settings* > *Administrators*.
2. Click *Create New* from the toolbar.

3. Configure the settings, selecting the previously added RADIUS server from the *RADIUS Server* dropdown list. See Creating administrators on page 557.
4. Click *OK* to save the settings.

To test the configuration:

1. Attempt to log in to the FortiAnalyzer GUI with your new credentials.
2. Enter your user name and password and click *Login*.
3. Enter your FortiToken pin code and click *Submit* to log in to the FortiAnalyzer.

Multi-factor authentication with FortiToken Cloud

FortiAnalyzer supports MFA with FortiToken Cloud.

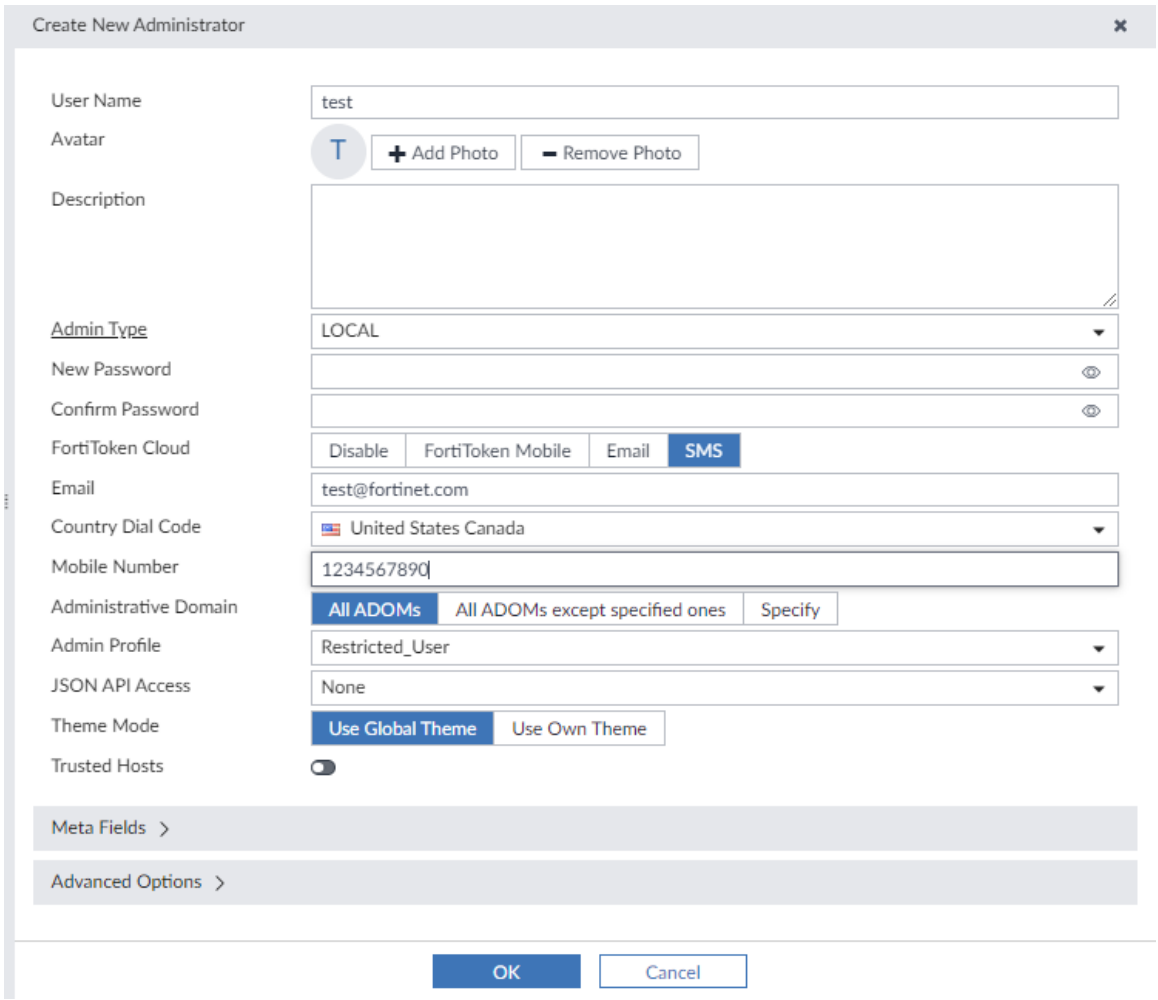
To use MFA with FortiToken Cloud, you must have an active FortiToken Cloud license registered on the same FortiCloud account as FortiAnalyzer. For more information about how to register your FortiToken license on FortiCloud, see How to register your FTC license and the FortiCloud Asset Management guide.

For information about licenses for FortiToken Cloud, see How to Add Licenses to FortiToken Cloud.

To configure an administrator to use MFA with FortiToken Cloud:

1. Register FortiToken Cloud and FortiAnalyzer to the same FortiCloud account.
2. In FortiAnalyzer, go to *System Settings > Admin > Administrators* and click *Create New* or edit an existing administrator.
3. In the *FortiToken Cloud* field, select the token delivery method from the following options:

FortiToken Mobile	Use the FortiToken Mobile app to get tokens. The following information must be provided: • **Email**: Provide the administrator's email address. The administrator is sent an email to the specified address with a link to activate their token in the FortiToken Mobile app on their mobile device. After FortiToken Mobile app is activated, they will receive their token codes through the app.
Email	Receive the token by email. The following information must be provided: • **Email**: Provide the administrator's email address. Token codes will be sent to the specified email address.
SMS	Receive the token by SMS message. The following information must be provided: • **Email**: Provide the administrator's email address. • **Country Dial Code**: Select a country code for the mobile number. • **Mobile Number**: Enter a valid mobile phone number for receiving SMS messages.

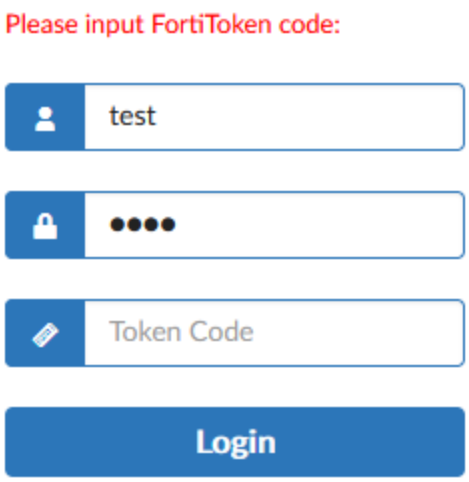


4. Edit other fields as needed and click *OK* to save the administrator configuration.

   When the FortiToken Cloud is registered to the same FortiCloud account as FortiAnalyzer and the license permits adding a new user, the administrator is automatically synchronized to FortiToken Cloud with the specified *FortiToken Cloud* MFA method. Otherwise, an error message is displayed.

   You can view the user in *FortiToken Cloud under User Management > Users*. For more information, see the FortiToken Cloud Administration Guide.

5. When the administrator logs in, they are prompted to enter the token code from their email, SMS, or FortiToken Mobile app.


Please input FortiToken code:
test
Token Code
Login

High Availability

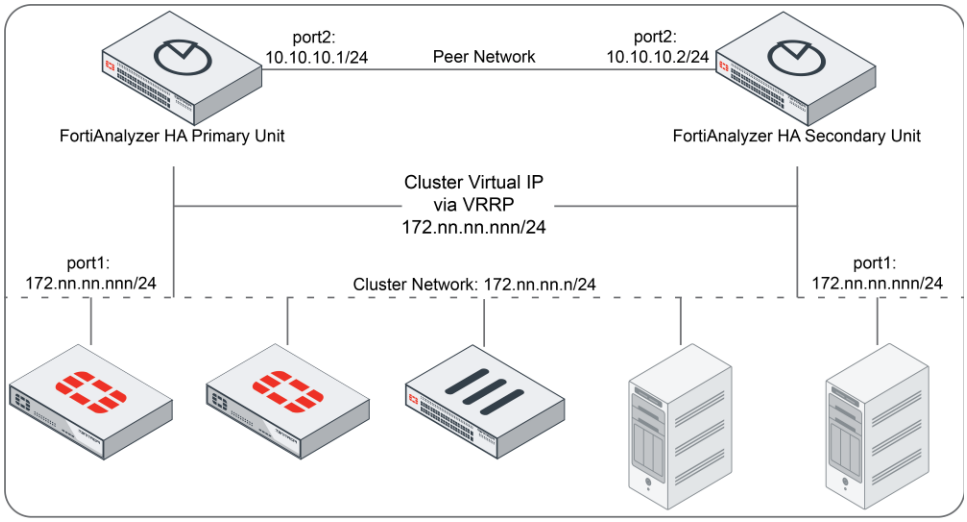
A FortiAnalyzer high availability (HA) cluster provides the following features:

- Provide real-time redundancy in case a FortiAnalyzer primary unit fails. If the primary unit fails, another unit in the cluster is selected as the primary unit. See If the primary unit fails on page 611.
- Synchronize logs and data securely among multiple FortiAnalyzer units. Some system and configuration settings are also synchronized. See Configuration synchronization on page 606.
- Alleviate the load on the primary unit by using secondary (backup) units for processes such as running reports.

A FortiAnalyzer HA cluster can have a maximum of four units: one primary unit with up to three secondary units. All units in the cluster must be of the same FortiAnalyzer series. All units are visible on the network.

All units must run in the same operation mode: Analyzer or Collector.

When devices with different licenses are used to create an HA cluster, the license that allows for the smallest number of managed devices is used.



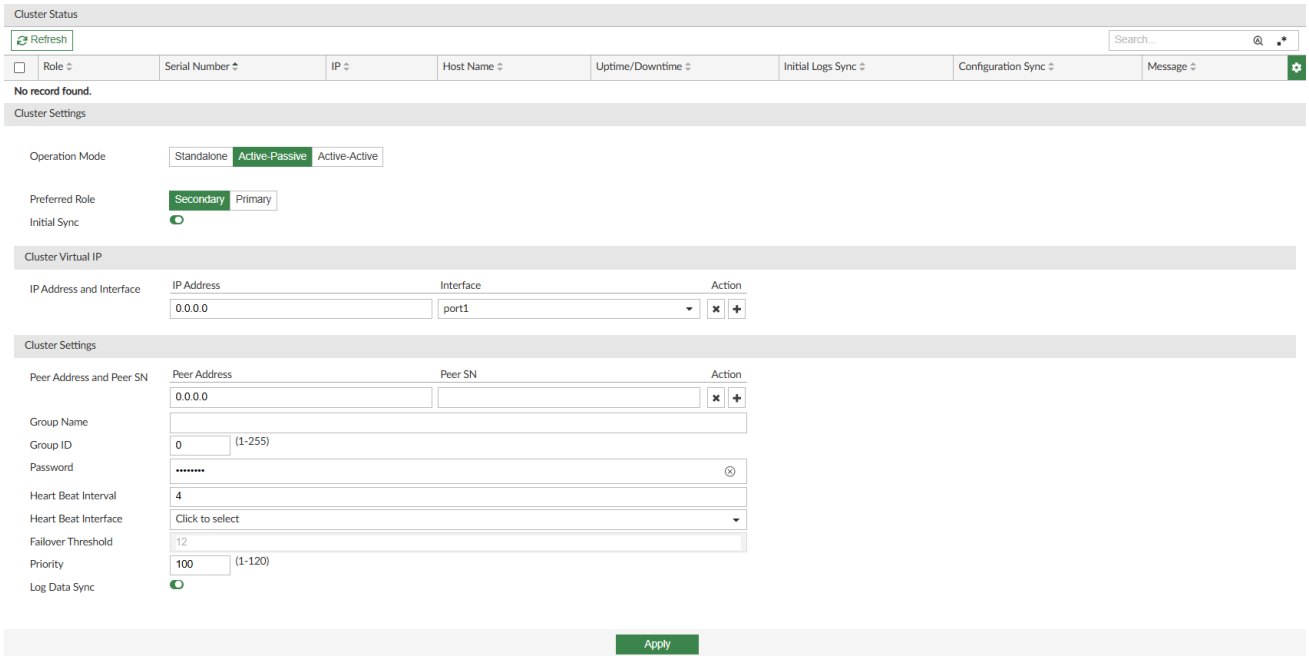
Configuring HA options

To configure HA options go to *System Settings > HA* and configure FortiAnalyzer units to create an HA cluster or change cluster configuration.

In *System Settings > HA*, use the *Cluster Settings* pane to create or change HA configuration, and use the *Cluster Status* pane to monitor HA status.

To configure a cluster, set the *Operation Mode* of the primary unit to *Active-Passive* or *Active-Active*. Then add the IP addresses and serial numbers of each secondary unit to the primary unit peer list. The IP address and serial number of the primary unit and all secondary units must be added to each secondary unit's HA configuration. The primary unit and all secondary units must have the same *Group Name*, *Group ID* and *Password*.

You can connect to the primary unit GUI to work with FortiAnalyzer. Using configuration synchronization, you can configure and work with the cluster in the same way as you work with a standalone FortiAnalyzer unit.



Configure the following settings:

Cluster Settings	
Operation Mode	Select *Active-Passive* or *Active-Active* to configure the FortiAnalyzer unit for HA. You can use *Active-Active* mode to create a geo-redundant solution. For more information, see Geo-redundant HA on page 607. Select *Standalone* to stop operating in HA mode.
Preferred Role	Select the preferred role when this unit first joins the HA cluster. If the preferred role is *Primary*, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit. The default is *Secondary* so that the unit can synchronize with the primary unit. A secondary unit cannot become a primary unit until it is synchronized with the current primary unit.
Initial Sync	Initial data sync from the primary node is required before the node is fully functional as an HA member.

	 During initial setup, at least one node must have *Initial Sync* disabled. If all nodes have *Initial Sync* enabled during initial setup, the cluster will get stuck trying to synchronize. During initial setup, any node with *Initial Sync* enabled will pull the initial data sync from the primary node. The primary node itself is elected from among the nodes that have *Initial Sync* disabled. Once the initial setup is complete, nodes added later can have *Initial Sync* enabled (default) without issue. They will sync to the current primary node.
Cluster Virtual IP	
IP Address	The IP address for which the FortiAnalyzer HA unit is to provide redundancy.
Interface	The interface the FortiAnalyzer HA unit uses to provide redundancy.
Action	Click the plus (+) to add another virtual IP. Click the x to remove a virtual IP from the list.
Cluster Settings	
Peer IP	Type the IP address of another FortiAnalyzer unit in the cluster.
Peer SN	Type the serial number of the FortiAnalyzer unit corresponding to the entered IP address.
Action	Click the plus (+) to add another FortiAnalyzer unit in the cluster. Click the x to remove a FortiAnalyzer unit from the cluster.
Group Name	Type a group name that uniquely identifies the FortiAnalyzer HA cluster. All units in a cluster must have the same *Group Name*, *Group ID* and *Password*.
Group ID	Type a group ID from 1 to 255 that uniquely identifies the FortiAnalyzer HA cluster.
Password	A password for the HA cluster. All members of the HA cluster must have the same password.
Heart Beat Interval	The time the primary unit waits between sending heartbeat packets, in seconds. The heartbeat interval is also the amount of time that secondary units waits before expecting to receive a heartbeat packet from the primary unit. By default, the *Heart Beat Interval* is set to 4.
Heart Beat Interface	Select the interface used to send heartbeat packets.
Failover Threshold	The number of seconds that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed. This value corresponds to *Heart Beat Interval* x 3 and it is automatically updated based on the configured *Heart Beat Interval*.

	For example, the failure is detected after 12 seconds with the default settings: • *Heart Beat Interval*: 4 • *Failover Threshold*: 12 The *Heart Beat Interval* can be increased or decreased to adapt to latency conditions of your network and to detect legitimate failures.
Priority	The priority or seniority of the secondary unit in the cluster.
Log Data Sync	This option is on by default. It provides real-time log synchronization among cluster members.

Log synchronization

To ensure logs are synchronized among all HA units, FortiAnalyzer HA synchronizes logs in two states: initial logs synchronization and real-time log synchronization.

Initial Logs Sync

When you add a unit to an HA cluster, the primary unit synchronizes its logs with the new unit. After initial sync is complete, the secondary unit automatically reboots. After the reboot, the secondary unit rebuilds its log database with the synchronized logs.

You can see the status in the *Cluster Status* pane *Initial Logs Sync* column.



During initial setup, at least one node must have *Initial Sync* disabled. If all nodes have *Initial Sync* enabled during initial setup, the cluster will get stuck trying to synchronize.

During initial setup, any node with *Initial Sync* enabled will pull the initial data sync from the primary node. The primary node itself is elected from among the nodes that have *Initial Sync* disabled.

Once the initial setup is complete, nodes added later can have *Initial Sync* enabled (default) without issue. They will sync to the current primary node.

Log Data Sync

After the initial log synchronization, the HA cluster goes into real-time log synchronization state.

Log Data Sync is turned on by default for all units in the HA cluster.

When *Log Data Sync* is turned on in the primary unit, the primary unit forwards logs in real-time to all secondary units. This ensures that the logs in the primary and secondary units are synchronized.

Log Data Sync is turned on by default in secondary units so that if the primary unit fails, the secondary unit selected to be the new primary unit will continue to synchronize logs with secondary units.

If you want to use a FortiAnalyzer unit as a standby unit (not as a secondary unit), then you don't need real-time log synchronization so you can turn off *Log Data Sync*.

Configuration synchronization

Configuration synchronization provides redundancy and load balancing among the cluster units. A FortiAnalyzer HA cluster synchronizes the configuration of the following modules to all cluster units:

- Device Manager
- Incidents & Events
- Reports
- Most System Settings

FortiAnalyzer HA synchronizes most *System Settings* in the HA cluster. The following table shows which *System Setting* configurations are synchronized:

System Setting	Configuration synchronized
***Dashboards* > *Status* > System Information**	Only *Administrative Domain* is synchronized. All other settings in the System Information widget are not synchronized.
ADOMs, including Storage Info	Yes
Administrators	Yes
Admin Profiles	Yes
Remote Authentication Server	Yes
Fabric Management	No
SAML SSO	Yes
Admin Settings	Yes
HA	No
Network > Interface	No
Network > DNS	No
Network > Routing Table	No
Network > Packet Capture	No
Network > SNMP	Yes
Event Logs	No
Certificates > Local Certificate	No
Certificates > CA Certificate	Yes
Certificates > CRL	Yes
Certificates > Remote CA Certificate	Yes
Advanced > Log Forwarding	Yes
Advanced > Logging Topology	Yes
Advanced > Device Log Settings	Yes

System Setting	Configuration synchronized
Advanced > Mail Server	Yes
Advanced > Syslog Server	Yes
Advanced > Meta Fields	Yes
Advanced > Log Fetch	Yes
Advanced > Task Monitor	Yes
Advanced > Misc Settings	Yes

Geo-redundant HA

The active-active mode for FortiAnalyzer HA helps to create a geo-redundant solution.

In FortiAnalyzer HA active-passive mode, a layer 2 connection is required between HA members in order to set up the HA cluster virtual IP. In active-active mode, however, a layer 2 connection is not required between data centers at different locations.

Below is a brief comparison between FortiAnalyzer HA in active-passive and active-active mode.

active-passive	active-active
Only the HA primary can receive logs and archive files from its directly connected device and forward them to HA secondary.	All HA members can receive logs and archive files from its directly connected device and forward logs and archive files to its HA peer.
Only the HA primary can forward data to the remote server.	All HA members can forward its directly received logs and archive file to the remote server.

In the examples below, the goal is to build an active-active geo-redundant layer 3 FortiAnalyzer HA cluster between two data centers. The FortiAnalyzer HA members are located in different places. They are communicating with each other via routers. There is no layer 2 connection.



Unicast must be enabled for the HA heartbeat in order for the cluster to operate in this mode. This setting can only be configured from the CLI. For more information on enabling the unicast heartbeat setting, see the FortiAnalyzer CLI Reference.

VRRP (IP protocol 112) must be allowed through any connecting firewalls between the cluster members.

To build a geo-redundant FortiAnalyzer HA via the GUI:

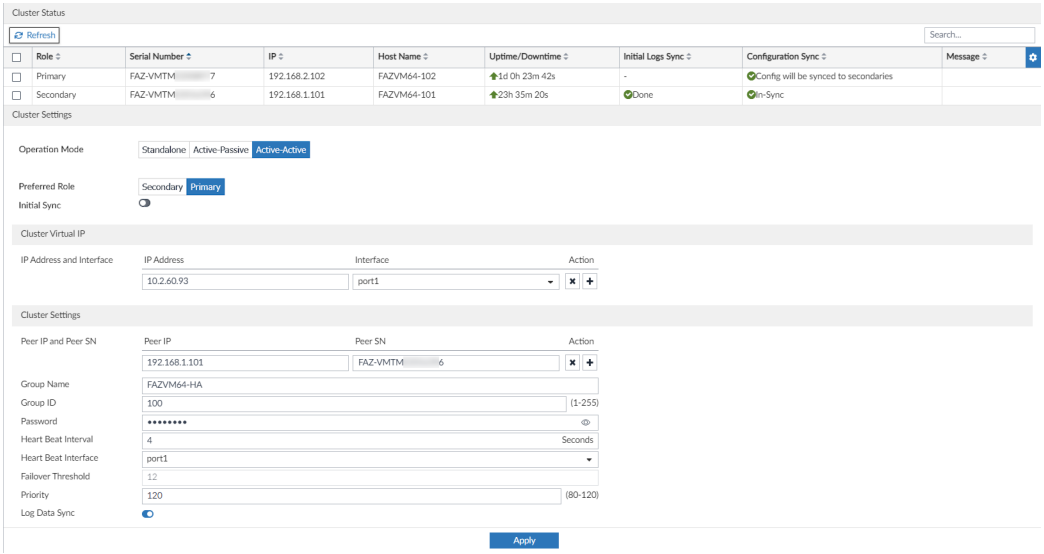
1. In the first FortiAnalyzer, configure the primary in *System Settings > HA*.
   - For *Operation Mode*, select *Active-Active*.
   - For *Preferred Role*, select *Primary*.
   - For *Initial Sync*, toggle to *Disabled*.

During initial setup, at least one node must have *Initial Sync* disabled. If all nodes have *Initial Sync* enabled during initial setup, the cluster will get stuck trying to synchronize.

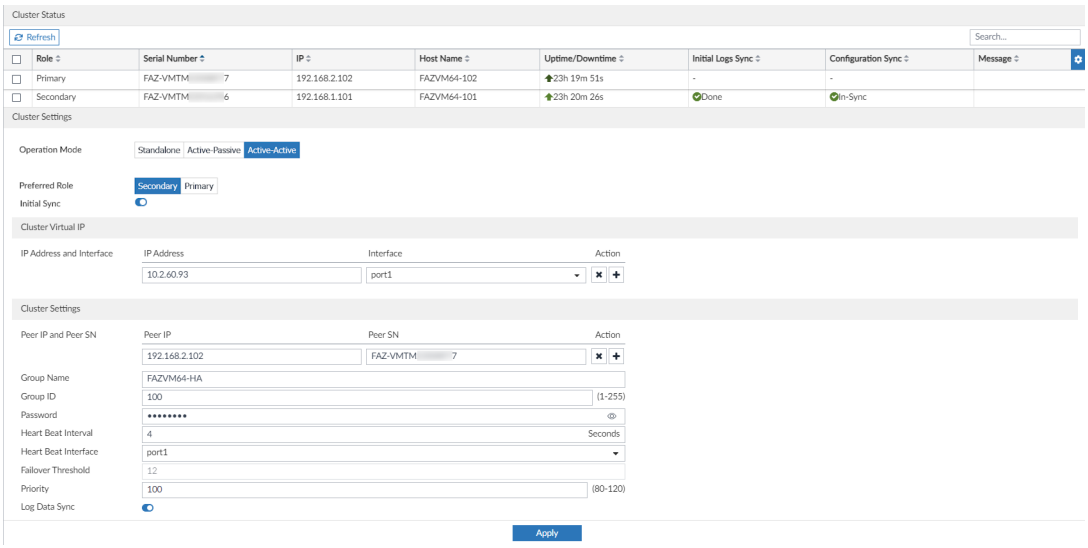
During initial setup, any node with *Initial Sync* enabled will pull the initial data sync from the primary node. The primary node itself is elected from among the nodes that have *Initial Sync* disabled.

Once the initial setup is complete, nodes added later can have *Initial Sync* enabled (default) without issue. They will sync to the current primary node.

- Complete the other fields, including *Peer IP* and *Peer SN*.
- Cluster Virtual IP (VIP) is optional. It requires a layer 2 connection between HA members. If VIP is not configured, select the interface which is used to communicate with the peer as *Heart Beat Interface*. You can click the *X* icon next to the VIP entry to remove it.



2. In the second FortiAnalyzer, configure the primary in *System Settings* > *HA*.
   - For *Operation Mode*, select *Active-Active*.
   - For *Preferred Role*, select *Secondary*.
   - For *Initial Sync*, you can leave it *Enabled*.
   - Complete the other fields, including *Peer IP* and *Peer SN*.
   - Cluster VIP is optional. It requires a layer 2 connection between HA members. If VIP is not configured, select the interface which is used to communicate with the peer as *Heart Beat Interface*. You can click the *X* icon next to the VIP entry to remove it.



To build a geo-redundant FortiAnalyzer HA via the CLI:

For more information about the FortiAnalyzer CLI commands, see the FortiAnalyzer CLI Reference.

1. Configure the FortiAnalyzer HA.

   When configuring the FortiAnalyzer `system ha`, set `mode` to `a-a`. The `vip` is optional; if there is no layer 2 connection between HA members, `vip` will not work. In this case, set `hb-interface` as the interface which is used to communicate with the peer.

   a. Configure the first FortiAnalyzer. In the CLI, enter the following commands:

```
config system ha
    set mode a-a
    set group-id 100
    set group-name "FAZVM64-HA"
    set hb-interface "port1"
    set initial-sync disable
    set unicast enable
    set password xxxxxx
        config peer
            edit 1
                set ip "192.168.1.101"
                set serial-number "FAZ-VMTM-----6"
            next
        end

    set preferred-role primary
    set priority 120
end
```

   b. Configure the second FortiAnalyzer. In the CLI, enter the following commands:

```
config system ha
    set mode a-a
    set group-id 100
```

```
    set group-name "FAZVM64-HA"
    set hb-interface "port1"
    set unicast enable
    set password xxxxxx
        config peer
            edit 1
                set ip "192.168.2.102"
                set serial-number "FAZ-VMTM-----7"
            next
        end
end
```

2. If the alternate FortiAnalyzer can be configured on FortiGate, `set server` to the HA primary and `set alt-server` to the HA secondary. In the FortiGate CLI, enter:

```
FGT# config log fortianalyzer setting
FGT (setting) # set status enable
set ?
...
*server                          The main remote FortiAnalyzer.
alt-server                      The alternate remote FortiAnalyzer.
...
set server 192.168.2.102
set alt-server 192.168.1.101
...
end
```

   The FortiGate CLI also includes a setting for automatic failover to the other active FortiAnalyzer. This setting is enabled by default:

```
config log fortianalyzer setting
    set fallback-to-primary enable
end
```

   For more information, see the FortiGate / FortiOS Administration Guide.

3. If the alternate FortiAnalyzer cannot be configured on FortiGate, `set server` to a HA member which is reachable from the FortiGate or to the VIP address of the FortiAnalyzer HA, if any. In the FortiGate CLI, enter:

```
FGT# config log fortianalyzer setting
FGT (setting) # set status enable
...
set server 192.168.2.102(or 10.2.60.93)
...
end
```

Monitoring HA status

In *System Settings* > *HA*, the *Cluster Status* pane shows the HA status. This pane displays information about the role of each cluster unit, the HA status of the cluster, and the HA configuration of the cluster.



You can use the CLI command `diagnose ha status` to display the same HA status information.

The *Cluster Status* pane displays the following information:

Role	Role of each cluster member.
Serial Number	Serial number of each cluster member.
IP	IP address of each cluster members including the host.
Host Name	Host name of the HA cluster.
Uptime/Downtime	Uptime or downtime of each cluster member.
Initial Logs Sync	Status of the initial logs synchronization.
Configuration Sync	Status of synchronizing configuration data.
Message	Status or error messages, if any.

If the primary unit fails

If the primary unit becomes unavailable, another unit in the cluster is selected as the primary unit using the following rules:

- All cluster units are assigned a priority from 1 – 120. The default priority is 100. If the primary unit becomes unavailable, an available unit with the highest priority is selected as the new primary unit. For example, a unit with a priority of 110 is selected over a unit with a priority of 100.
- If multiple units have the same priority, the unit whose primary IP address has the greatest value is selected as the new primary unit. For example, 123.45.67.124 is selected over 123.45.67.123.

After a secondary unit has been selected as the new primary in a failover scenario, new units can be added to the cluster and the old primary unit can rejoin when it is back online. The following rules apply in this scenario:

- If a new unit with *secondary* as the preferred role and a higher priority or a greater value IP address joins the cluster, the new unit does not replace (or preempt) the current primary unit. For example, when a new secondary unit is added to the cluster, it will not replace the current primary.
- If a new unit with *primary* as the preferred role joins the cluster, it will replace (or preempt) the current primary unit. For example, when the old primary unit rejoins the cluster, it will replace the current primary unit.

  This is due to the preferred role in the HA configuration for the unit. When the preferred role is primary, `preempt` is automatically set in the keepalived config and `120` added to the keepalived priority, ensuring the unit can be selected as the primary for the cluster.

Load balancing

Because FortiAnalyzer HA synchronizes logs among HA units, the HA cluster can balance the load and improve overall responsiveness. Load balancing enhances the following modules:

- Reports
- FortiView

When generating multiple reports, the loads are distributed to all HA cluster units in a round-robin fashion. When a report is generated, the report is synchronized with other units so that the report is visible on all HA units.

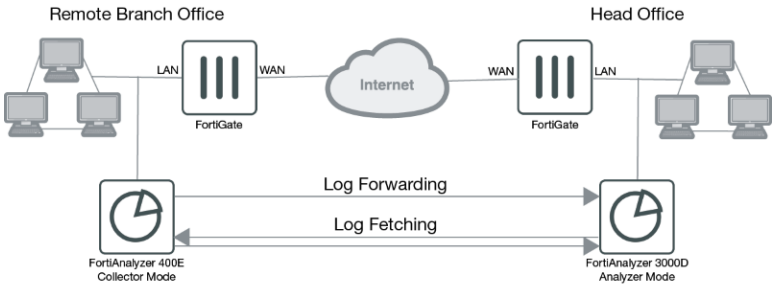
Similarly, for FortiView, cluster units share some of the load when these modules generate output for their widgets.

Upgrading the FortiAnalyzer firmware for an operating cluster

For information on upgrading the FortiAnalyzer firmware for an operating cluster, see the *FortiAnalyzer Upgrade Guide* on the Fortinet Docs Library.

Collectors and Analyzers

This topic describes how to configure two FortiAnalyzer units as the Analyzer and Collector and make them work together. In the scenario shown in the diagram below, Company A has a remote branch network with a FortiGate unit and a FortiAnalyzer 400E in Collector mode. In its head office, Company A has another FortiGate unit and a FortiAnalyzer 3000D in Analyzer mode. The Collector forwards the logs of the FortiGate unit in the remote branch to the Analyzer in the head office for data analysis and reports generation. The Collector is also used for log archival.



For related concepts, see Operation modes on page 41 and Analyzer–Collector collaboration on page 43. You need to complete the initial setup for your FortiAnalyzer units first. See Initial setup on page 39.

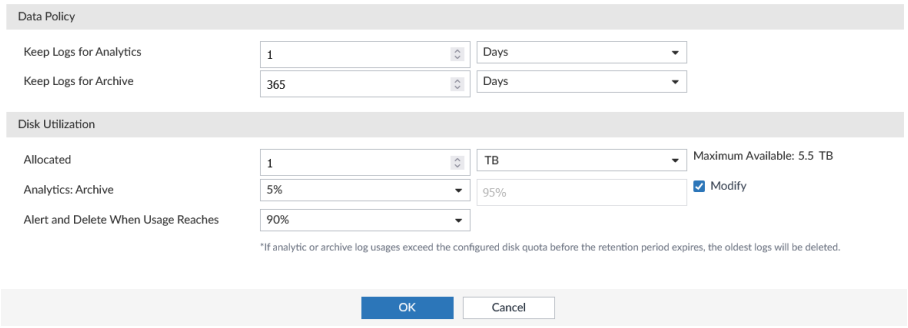
Configuring the Collector

To configure the Collector:

1. Ensure the FortiAnalyzer Operation Mode is *Collector*. See Configuring the operation mode on page 62.
2. Check and configure the storage policy for the Collector. See Log storage information on page 173.

For the Collector, you should allocate most of the disk space for Archive logs. You should keep the Archive logs long enough to meet the regulatory requirements of your organization. After this initial configuration, you can monitor the storage usage and adjust it as you go.

Following is a storage configuration example of the Collector.



If *Keep Logs for Analytics* is set to 0, the Analytics logs will be kept for unlimited days. For more information, see Configuring log storage policy on page 175.

3. Set up log forwarding to enable the Collector to forward the logs to the Analyzer. See Log Forwarding on page 518. In particular,
   - Set *Remote Server Type* to *FortiAnalyzer*.
   - Set *Server IP* to the IP address of the Analyzer that this Collector will forward logs to.
   - Click *Select Device* and select the FortiGate device that the Collector will forward logs for.

   For additional security, you can use the following command in the Analyzer's CLI:

```
config system log-forward-service
   set collector-auth enable
end
```

Variable	Description
collector-auth {enable | disable}	Enable/disable FortiAnalyzer Collectors to be authenticated before forwarding data (default = disable). When enabled, the Collector must be authorized by an admin in the FortiAnalyzer that is operating in Analyzer mode before it can forward data. The device can be authorized in *Device Manager* in the Analyzer's GUI.

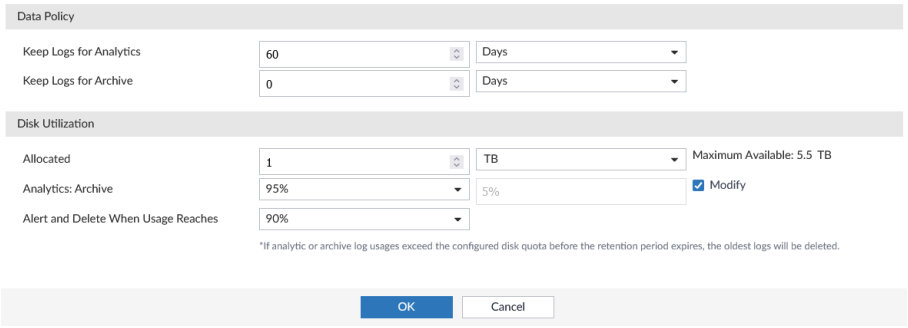
Configuring the Analyzer

To configure the Analyzer:

1. Ensure the FortiAnalyzer Operation Mode is *Analyzer*. See Configuring the operation mode on page 62
2. Check and configure the storage policy for the Analyzer. See Log storage information on page 173.

For the Analyzer you should allocate most of the disk space for Analytics logs. You may want to keep the Analytics logs for 30–90 days. After this initial configuration, you can monitor the storage usage and adjust it as you go.

Following is a storage configuration example of the Analyzer.



3. Make sure that the aggregation service is enabled on the Analyzer. If not, use this CLI command to enable it:

```
config system log-forward-service
   set accept-aggregation enable
end
```

4. Add the FortiGate device of the remote office that the Collector will forward logs for. See Authorizing devices on page 89.

Once the FortiGate of the remote office is added, the Analyzer starts receiving its logs from the Collector.

Fetching logs from the Collector to the Analyzer

At times, you might want to fetch logs from the Collector to the Analyzer. The Collector will perform the role of the fetch server, and the Analyzer will perform the role of fetch client. For information about how to conduct log fetching, see Log Fetching on page 529.

Appendix A - Supported RFC Notes

This section identifies the request for comment (RFC) notes supported by FortiAnalyzer.

RFC 2548

Description:

Microsoft Vendor-specific RADIUS Attributes

Category:

Informational

Webpage:

http://tools.ietf.org/html/rfc2548

RFC 2665

Description:

Ethernet-like MIB parts that apply to FortiAnalyzer units.

Category:

Standards Track

Webpage:

http://tools.ietf.org/html/rfc2665

RFC 1918

Description:

Address Allocation for Private Internets.

Category:

Best Current Practice

Webpage:

http://tools.ietf.org/html/rfc1918

RFC 1213

Description:

MIB II parts that apply to FortiAnalyzer units.

Category:

FortiAnalyzer (SNMP)

Webpage:

http://tools.ietf.org/html/rfc1213

Appendix B - Log Integrity and Secure Log Transfer

This section identifies the options for enabling log integrity and secure log transfer settings between FortiAnalyzer and FortiGate devices.

Log Integrity

FortiAnalyzer can create an MD5 checksum for each log file in order to secure logs from being modified after they have been sent to an analytics platform.

The log integrity setting selected determines the values recorded at the time of transmission or when rolling the log:

- **MD5**: Record the log file's MD5 hash value only.
- **MD5-auth**: Record the log file's MD5 hash value and authentication code.
- **None**: Do not record the log file checksum (default).

Configuring log integrity settings

To configure FortiAnalyzer log integrity:

1. In the FortiAnalyzer CLI, enter the following commands:
```
configure system global
   set log-checksum {md5 | md5-auth | none}
end
```

Verifying log-integrity

When log integrity settings are applied, you can view the MD5 checksum for logs in FortiAnalyzer event logs and the FortiAnalyzer CLI.

To view the log file's MD5 checksum in event logs:

1. Go to *Incidents & Events* > *Event Monitor* > *All Events* and select an event log.
2. In the toolbar, select *Display Raw* to view the raw log details.
   The MD5 checksum is included in the details of the raw log.

```
id=6906469110439837696 itime=2020-12-18 06:47:59 euid=1 epid=1 dsteuid=1 dstepid=1 log_
      id=0031040026 subtype=logfile type=event level=information time=06:47:59 date=2020-12-18
      user=system action=roll msg=Rolled log file tlog.1608270213.log of device
      FGVM01TM20000000 [FGVM01TM20000000] vdom root, MD5 checksum:
      ad85f8e889a3436d75b22b4a33c492ec userfrom=system desc=Rolling disk log file
      devid=FAZVMSTM20000000 devname=FAZVMSTM20000000 dtime=2020-12-18 06:47:59 itime_
      t=1608270479
```

To query the log file's MD5 checksum in the CLI:

1. Enter the following command in the FortiAnalyzer CLI:
   ```
   execute log-integrity <device_name> <vdom name> <log_name>
   ```
   For example:
   ```
   execute log-integrity FGVM01TM20000000 root tlog.1608279204.log.gz
      Integrity checking passed:
      MD5 checksum is [82598ec0086319db73bd0f9de2396047]
   ```

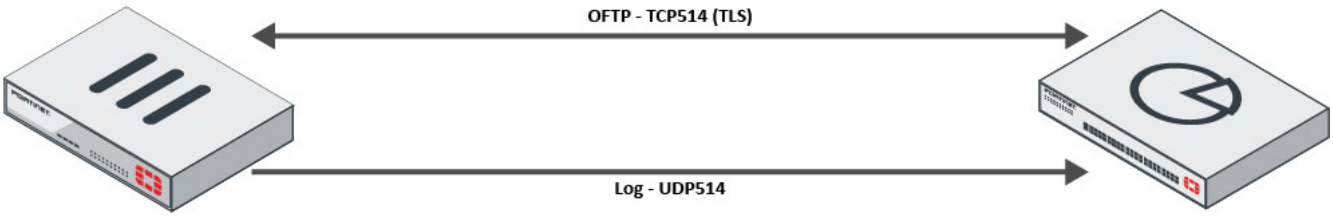
Secure Log Transfer

Optimized Fabric Transfer Protocol (OFTP) is a proprietary Fortinet protocol. It is used for connectivity, performing health checks, file transfers, and log display on FortiGate. OFTP listens on ports TCP514 and UDP514.

In the default configuration, there are two communication streams between FortiGate and FortiAnalyzer. OFTP communication is encrypted and log communication is not.

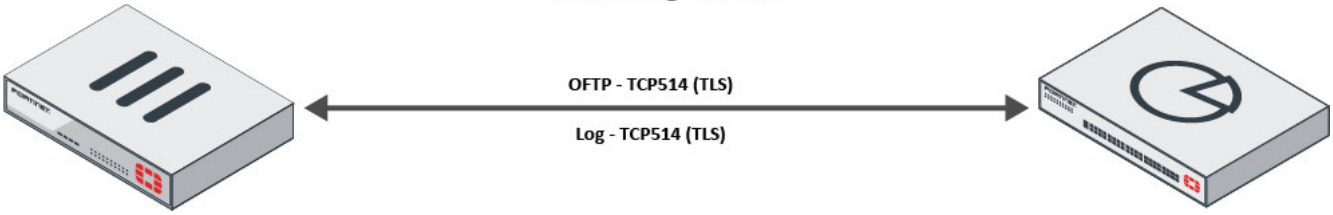
- OFTP communication occurs on TCP514 using TLS.
- Log communication occurs on UDP514 (default setting).

Default FortiGate Settings



To secure log transfer, you can enable TCP and encryption. When enabled, logs are transferred securely between the FortiGate and FortiAnalyzer using TCP514 (TLS).

Secure Log Transfer



Configuring secure log transfer settings

Reliable logging from FortiGate to FortiAnalyzer prevents lost logs when the connection between FortiGate and FortiAnalyzer is disrupted. If connection is lost between the FortiAnalyzer and FortiGate device, logs will be cached and sent to FortiAnalyzer once the connection resumes. For more information, see *FortiAnalyzer log caching* in the FortiGate / FortiOS Administration Guide.

To enable secure log transfer:

1. In the FortiGate CLI, enter the following commands:
```
configure log fortianalyzer setting
   set reliable enable
end
```



Enabling secure log transfer over TCP will impact overall logging performance.



OFTP SSL protocol supports SSLv3, TLSv1.0, TLSv1.2, and TLSv1.3 (default TLSv1.2).

Log caching with secure log transfer enabled

When secure log transfer is enabled, log sync logic guarantees that no logs are lost due to connection issues between the FortiGate and FortiAnalyzer. When connection is lost, logs will be cached and sent to FortiAnalyzer once the connection resumes.

To confirm cached logs are sent when connection is lost/resumed between FortiGate and FortiAnalyzer:

1. Confirm the value of `logsync_enabled` is `1` on the FortiGate device.
   In the FortiGate CLI, enter the following command:
```
diagnose test application fgtlogd 1

faz2: global , enabled
   server=10.2.169.54, realtime=1, ssl=1, state=connected
   server_log_status=Log is allowed.,
   src=, mgmt_name=FGh_Log_root_10.2.169.54, reliable=1, sni_prefix_type=none,
   required_entitlement=none, region=ca-west-1,
   logsync_enabled:1, logsync_conn_id:131071, seq_no:257
      status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
      SNs: last sn update:2097 seconds ago.
         Sn list:
         (FAZ-VM0000000001,age=2097s)    (FAZ-VMJY00000004,age=2097s)
      queue: qlen=0.
filter: severity=6, sz_exclude_list=0
```

2. While connection between the FortiGate and FortiAnalyzer is established, check the log sequence number on the OFTP connection.
   In the FortiAnalyzer CLI, enter the following command:
   ```
   diagnose test application oftpd 3
   #  DEVICE            CONN         HOSTNAME       IP          UPTIME  IDLETIME  #PKTS
   ---------------------------------------------------------------------------------------
   1  FGT40FTK20025663  131071: 257  FortiGate-40F  10.3.169.1  31m14s  4s        620
   ```
   The `CONN` column has been added to record the connection ID and log sequence number. In this example, the connection ID is `131071` and the sequence number is `257`.
3. When connection between the FortiGate and FortiAnalyzer is lost, check the log sequence number on the OFTP connection.
   In the FortiAnalyzer CLI, enter the following command:
   ```
   diagnose test application oftpd 3
   #  DEVICE            CONN         HOSTNAME       IP          UPTIME  IDLETIME  #PKTS
   ---------------------------------------------------------------------------------------
   1  FGT40FTK20025663  131071: 257  FortiGate-40F  10.3.169.1  35m14s  244s        620
   ```
   While the connection is lost, logs generated on the FortiGate device will be stored in its memory queue. The log squence number on the OFTP connection will not increase. In this example, the log sequence number has remained at `257`.
4. When the connection between the FortiGate and FortiAnalyzer devices resumes, check logs on the FortiGate device.
   In the FortiGate CLI, enter the following command:
   ```
   diagnose test application fgtlogd 41

   cache maximum: 100573388(95MB) objects: 37 used: 25788(0MB) allocated: 29440(0MB)

   VDOM:root
   Memory queue for: global-faz
      queue:
         num:0 size:0(0MB) total size:25788(0MB) max:100573388(95MB) logs:0
   Confirm queue for: global-faz
      queue:
         num:25 size:17382(0MB) total size:25788(0MB) max:100573388(95MB) logs:81
   Memory queue for: global-faz2
      queue:
         num:0 size:0(0MB) total size:25788(0MB) max:100573388(95MB) logs:0
   Confirm queue for: global-faz2
      queue:
         num:12 size:8406(0MB) total size:25788(0MB) max:100573388(95MB) logs:40
   ```
   The confirm queue on the FortiGate device shows all the logs that are waiting to be confirmed and cleared. Once the confirm queue displays 0, all of the cached logs have been sent to the FortiAnalyzer device.
5. Once the logs have been confirmed and cleared from the FortiGate device, check the log sequence number on the OFTP connection.
   In the FortiAnalyzer CLI, enter the following command:
   ```
   diagnose test application oftpd 3
   #  DEVICE            CONN         HOSTNAME       IP          UPTIME  IDLETIME  #PKTS
   ---------------------------------------------------------------------------------------
   1  FGT40FTK20025663  131071: 308  FortiGate-40F  10.3.169.1  36m23s  6s        635
   ```
   Once the cached logs have been sent to the FortiAnalyzer device, the log sequence number increases. In this example, the log sequence number has increased to `308`.

Supported ciphers

The list of supported ciphers is determined when configuring `enc_algorithm` using the `configure log fortianalyzer setting` command in the FortiGate CLI.

Cipher security levels

FortiAnalyzer allows administrators to specify the security levels for cipher suites as low, medium, or high. Using a higher security level means using more secure ciphers. SSL static key ciphers can be disabled to support forward secrecy.

Defining the `enc-algorithm` and `ssl-static-key-ciphers` usage settings in FortiAnalyzer allows administrators to choose which OpenSSL cipher suites are supported.

- Low `enc-algorithm` uses all OpenSSL ciphers.
- Medium `enc-algorithm` uses high and medium OpenSSL ciphers.
- High `enc-algorithm` uses only high OpenSSL ciphers.
- Disabling `ssl-static-key-ciphers` enables forward secrecy.

To configure the cipher suite security level in the FortiAnalyzer CLI:

1. Enter the following command in the FortiAnalyzer CLI:

```
config system global
   set enc-algorithm {high | medium | low}
   set ssl-static-key-ciphers {enable | disable}
end
```

If `enc-algorithm` is set to `custom`, configure the ssl-cipher-suites table to enforce the user specified preferred cipher order in the incoming SSL connections. Enter the following command:

```
config system global
   config ssl-cipher-suites
      edit <priority>
         set cipher <string>
         set version {tls1.2-or-below | tls1.3}
      end
```

If using `enc-algorithm` is set to `high`, `medium`, or `low`, see the list of supported ciphers based on security level settings below.

ssl-static-key-ciphers enabled	
enc-algorithm	
Low	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-

AES256-CCM:DHE-RSA-AES256-CCM:ECDHE-ECDSA-ARIA256-GCM-SHA384:ECDHE-ARIA256-GCM-SHA384:DHE-DSS-ARIA256-GCM-SHA384:DHE-RSA-ARIA256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:DHE-RSA-CAMELLIA256-SHA256:DHE-DSS-CAMELLIA256-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA20-POLY1305:DHE-PSK-CHACHA20-POLY1305:ECDHE-PSK-CHACHA20-POLY1305:DHE-PSK-AES256-CCM:RSA-PSK-ARIA256-GCM-SHA384:DHE-PSK-ARIA256-GCM-SHA384:AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:PSK-AES256-GCM-SHA384:PSK-CHACHA20-POLY1305:PSK-AES256-CCM:PSK-ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:ECDHE-PSK-AES256-CBC-SHA384:ECDHE-PSK-AES256-CBC-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC-SHA:RSA-PSK-AES256-CBC-SHA384:DHE-PSK-AES256-CBC-SHA384:RSA-PSK-AES256-CBC-SHA:DHE-PSK-AES256-CBC-SHA:ECDHE-PSK-CAMELLIA256-SHA384:RSA-PSK-CAMELLIA256-SHA384:DHE-PSK-CAMELLIA256-SHA384:AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA384:PSK-AES256-CBC-SHA:PSK-CAMELLIA256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-CCM:DHE-RSA-AES128-CCM:ECDHE-ECDSA-ARIA128-GCM-SHA256:ECDHE-ARIA128-GCM-SHA256:DHE-DSS-ARIA128-GCM-SHA256:DHE-RSA-ARIA128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:DHE-RSA-CAMELLIA128-SHA256:DHE-DSS-CAMELLIA128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:RSA-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-CCM:RSA-PSK-ARIA128-GCM-SHA256:DHE-PSK-ARIA128-GCM-SHA256:AES128-GCM-SHA256:AES128-CCM:ARIA128-GCM-SHA256:PSK-AES128-GCM-SHA256:PSK-AES128-CCM:PSK-ARIA128-GCM-SHA256:AES128-SHA256:CAMELLIA128-SHA256:ECDHE-PSK-AES128-CBC-SHA256:ECDHE-PSK-AES128-CBC-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-128-CBC-SHA:RSA-PSK-AES128-CBC-SHA256:DHE-PSK-AES128-CBC-SHA256:RSA-PSK-AES128-CBC-SHA:DHE-PSK-AES128-CBC-SHA:ECDHE-PSK-CAMELLIA128-SHA256:RSA-PSK-CAMELLIA128-SHA256:DHE-PSK-CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:PSK-AES128-CBC-SHA256:PSK-AES128-CBC-SHA:PSK-CAMELLIA128-SHA256:ECDHE-ECDSA-AES256-CCM8:ECDHE-ECDSA-AES128-CCM8:DHE-RSA-AES256-CCM8:DHE-RSA-AES128-CCM8:DHE-PSK-AES256-CCM8:DHE-PSK-AES128-CCM8:AES256-CCM8:AES128-CCM8:PSK-AES256-CCM8:PSK-AES128-CCM8

Medium	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES256-CCM:DHE-RSA-AES256-CCM:ECDHE-ECDSA-ARIA256-GCM-SHA384:ECDHE-ARIA256-GCM-SHA384:DHE-DSS-ARIA256-GCM-SHA384:DHE-RSA-ARIA256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:DHE-RSA-CAMELLIA256-SHA256:DHE-DSS-CAMELLIA256-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA20-POLY1305:DHE-PSK-CHACHA20-POLY1305:ECDHE-PSK-CHACHA20-POLY1305:DHE-PSK-AES256-CCM:RSA-PSK-ARIA256-GCM-SHA384:DHE-PSK-ARIA256-GCM-SHA384:AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:PSK-AES256-GCM-SHA384:PSK-CHACHA20-POLY1305:PSK-AES256-CCM:PSK-ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:ECDHE-PSK-AES256-CBC-SHA384:ECDHE-PSK-AES256-CBC-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC-SHA:RSA-PSK-AES256-CBC-SHA384:DHE-PSK-AES256-CBC-SHA384:RSA-PSK-AES256-CBC-SHA:DHE-PSK-AES256-CBC-SHA:ECDHE-PSK-CAMELLIA256-SHA384:RSA-PSK-CAMELLIA256-SHA384:DHE-PSK-CAMELLIA256-SHA384:AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA384:PSK-AES256-CBC-SHA:PSK-CAMELLIA256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-CCM:DHE-RSA-AES128-CCM:ECDHE-ECDSA-ARIA128-GCM-SHA256:ECDHE-ARIA128-GCM-SHA256:DHE-DSS-ARIA128-GCM-SHA256:DHE-RSA-ARIA128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:DHE-RSA-CAMELLIA128-SHA256:DHE-DSS-CAMELLIA128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:RSA-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-CCM:RSA-PSK-ARIA128-GCM-SHA256:DHE-PSK-ARIA128-GCM-SHA256:AES128-GCM-SHA256:AES128-CCM:ARIA128-GCM-SHA256:PSK-AES128-GCM-SHA256:PSK-AES128-CCM:PSK-ARIA128-GCM-SHA256:AES128-SHA256:CAMELLIA128-SHA256:ECDHE-PSK-AES128-CBC-SHA256:ECDHE-PSK-AES128-CBC-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-128-CBC-SHA:RSA-PSK-AES128-CBC-SHA256:DHE-PSK-AES128-CBC-SHA256:RSA-PSK-AES128-CBC-SHA:DHE-PSK-AES128-CBC-SHA:ECDHE-PSK-CAMELLIA128-SHA256:RSA-PSK-CAMELLIA128-SHA256:DHE-PSK-CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-

	SHA:PSK-AES128-CBC-SHA256:PSK-AES128-CBC-SHA:PSK-CAMELLIA128-SHA256:ECDHE-ECDSA-AES256-CCM8:ECDHE-ECDSA-AES128-CCM8:DHE-RSA-AES256-CCM8:DHE-RSA-AES128-CCM8:DHE-PSK-AES256-CCM8:DHE-PSK-AES128-CCM8:AES256-CCM8:AES128-CCM8:PSK-AES256-CCM8:PSK-AES128-CCM8
High	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES256-CCM:DHE-RSA-AES256-CCM:ECDHE-ECDSA-ARIA256-GCM-SHA384:ECDHE-ARIA256-GCM-SHA384:DHE-DSS-ARIA256-GCM-SHA384:DHE-RSA-ARIA256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:DHE-RSA-CAMELLIA256-SHA256:DHE-DSS-CAMELLIA256-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA20-POLY1305:DHE-PSK-CHACHA20-POLY1305:ECDHE-PSK-CHACHA20-POLY1305:DHE-PSK-AES256-CCM:RSA-PSK-ARIA256-GCM-SHA384:DHE-PSK-ARIA256-GCM-SHA384:AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:PSK-AES256-GCM-SHA384:PSK-CHACHA20-POLY1305:PSK-AES256-CCM:PSK-ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:ECDHE-PSK-AES256-CBC-SHA384:ECDHE-PSK-AES256-CBC-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC-SHA:RSA-PSK-AES256-CBC-SHA384:DHE-PSK-AES256-CBC-SHA384:RSA-PSK-AES256-CBC-SHA:DHE-PSK-AES256-CBC-SHA:ECDHE-PSK-CAMELLIA256-SHA384:RSA-PSK-CAMELLIA256-SHA384:DHE-PSK-CAMELLIA256-SHA384:AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA384:PSK-AES256-CBC-SHA:PSK-CAMELLIA256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-CCM:DHE-RSA-AES128-CCM:ECDHE-ECDSA-ARIA128-GCM-SHA256:ECDHE-ARIA128-GCM-SHA256:DHE-DSS-ARIA128-GCM-SHA256:DHE-RSA-ARIA128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:DHE-RSA-CAMELLIA128-SHA256:DHE-DSS-CAMELLIA128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:RSA-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-CCM:RSA-PSK-ARIA128-GCM-SHA256:DHE-PSK-ARIA128-GCM-SHA256:AES128-GCM-SHA256:AES128-CCM:ARIA128-GCM-SHA256:PSK-AES128-GCM-SHA256:PSK-AES128-CCM:PSK-ARIA128-GCM-SHA256:AES128-

	SHA256:CAMELLIA128-SHA256:ECDHE-PSK-AES128-CBC-SHA256:ECDHE-PSK-AES128-CBC-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-128-CBC-SHA:RSA-PSK-AES128-CBC-SHA256:DHE-PSK-AES128-CBC-SHA256:RSA-PSK-AES128-CBC-SHA:DHE-PSK-AES128-CBC-SHA:ECDHE-PSK-CAMELLIA128-SHA256:RSA-PSK-CAMELLIA128-SHA256:DHE-PSK-CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:PSK-AES128-CBC-SHA256:PSK-AES128-CBC-SHA:PSK-CAMELLIA128-SHA256
fips enabled	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:AES256-SHA:AES256-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES256-GCM-SHA384:AES128-SHA:AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES128-GCM-SHA256

The following ciphers are *not available* when using forward secrecy (`ssl-static-key-ciphers` is disabled).

ssl-static-key-ciphers disabled	
enc-algorithm	
Low	AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:AES256-SHA:CAMELLIA256-SHA:AES128-GCM-SHA256:AES128-CCM:AES128-SHA256:CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:AES256-CCM8:AES128-CCM8
Medium	AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:AES256-SHA:CAMELLIA256-SHA:AES128-GCM-SHA256:AES128-CCM:AES128-SHA256:CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:AES256-CCM8:AES128-CCM8
High	AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:AES256-SHA:CAMELLIA256-SHA:AES128-GCM-SHA256:AES128-CCM:AES128-SHA256:CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA
fips enabled	AES256-SHA:AES256-SHA256:AES128-SHA:AES128-SHA256

Maximum TLS/SSL version compatibility

The tables below indicate the maximum supported TLS version that you can configure for communication between a FortiGate and FortiAnalyzer, as well as FortiAnalyzer's configured with log forwarding when the type is *FortiAnalyzer*.

For more information on secure log transfer and log integrity settings between FortiGate and FortiAnalyzer, see Appendix B - Log Integrity and Secure Log Transfer on page 618.

Maximum configurable TLS version for FortiGate to FortiAnalyzer communication:

	FAZ 6.4.0+	**FAZ 6.2.0+**	**FAZ 6.0.0+**
FGT 6.4.0+	tlsv1.3	tlsv1.2	tlsv1.2
FGT 6.2.3 – 6.2.8	tlsv1.3	tlsv1.2	tlsv1.2
FGT 6.2.0 – 6.2.2	tlsv1.2	tlsv1.2	tlsv1.2
FGT 6.0.2 – 6.0.12	tlsv1.2	tlsv1.2	tlsv1.2
FGT 6.0.0 – 6.0.1	The setting is not configurable in FGT 6.0.0 - 6.0.1.	This setting is not configurable in FGT 6.0.0 - 6.0.1.	This setting is not configurable in FGT 6.0.0 - 6.0.1.

Maximum configurable TLS version for FortiAnalyzer to FortiAnalyzer log forwarding:

	FAZ 6.4.0+	**FAZ 6.2.0+**	**FAZ 6.0.0+**
FAZ 6.4.0+	tlsv1.3	tlsv1.2	tlsv1.2
FAZ 6.2.0+	tlsv1.2	tlsv1.2	tlsv1.2
FAZ 6.0.0+	tlsv1.2	tlsv1.2	tlsv1.2

To configure the global TLS/SSL version on FortiAnalyzer:

1. In the FortiAnalyzer CLI, enter the following:
```
config system global
   set global-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2 | tlsv1.3}
```

To configure the global TLS/SSL version on FortiGate:

1. In the FortiGate CLI, enter the following:
```
config system global
   set ssl-min-proto-version {tlsv1.3 | tlsv1.2 | tlsv1.1 | tlsv1.0 | sslv3}
```

Appendix C - FortiAnalyzer Ansible Collection documentation

Documentation for the Fortinet FortiAnalyzer Ansible Collection is available through the link below.

- FortiAnalyzer Ansible Collection documentation

Appendix D - FortiAI token entitlements for FortiAnalyzer

The monthly token allocation for the FortiAI license varies by FortiAnalyzer platform. In addition to the monthly token entitlements, you can also purchase the FortiAI Token Top-up license for additional tokens.

For information about FortiAI tokens, see FortiAI tokens on page 409.

Tokens per FortiAnalyzer appliance

FortiAnalyzer appliance	Total monthly entitled tokens
FortiAnalyzer-150G	1000000
FortiAnalyzer-300G	2249862
FortiAnalyzer-810G	5440628
FortiAnalyzer-1000G	7498984
FortiAnalyzer-3510G	26532226
FortiAnalyzer-3700G	35041552
FortiAnalyzer-BigData 4500G	72489382

Tokens per FortiAnalyzer-VMS

SKU	GB/Day of logs	Total monthly entitled tokens
FC1-10-AZVMS-1118-01-DD	5	105128
FC2-10-AZVMS-1118-01-DD	50	759280
FC3-10-AZVMS-1118-01-DD	500	1460068

Tokens per FortiAnalyzer-VM

SKU	GB/Day of logs	Total monthly entitled tokens
FC1-10-LV0VM-1118-02-DD	1 - 6	140166
FC2-10-LV0VM-1118-02-DD	1 - 11	420498
FC3-10-LV0VM-1118-02-DD	1 - 26	1518560
FC4-10-LV0VM-1118-02-DD	1 - unlimited	26117636

SKU	GB/Day of logs	Total monthly entitled tokens
FC5-10-LV0VM-1118-02-DD	1 - 101	4088274
FC6-10-LV0VM-1118-02-DD	1 - 501	5840258
FC7-10-LV0VM-1118-02-DD	1 - 2001	23361034

Tokens per FortiAnalyzer Cloud

SKU	GB/Day of logs	Total monthly entitled tokens
FC1-10-AZCLD-1118-01-DD	5	105128
FC2-10-AZCLD-1118-01-DD	50	759280
FC3-10-AZCLD-1118-01-DD	500	1460068

FortiAI Token Top-up

SKU	Total tokens
FC1-10-AITAZ-1089-02-DD	500000 per seat

When you purchase multiple contracts, the activation date of each subsequent contract will be set from the end date of the previous. This is automatically set if the contracts are bought at the same time or if the subsequent contracts are bought before the previous contract expires. For example:

Contract	Activation Date	Expiration Date
First contract	2025-01-16	2026-01-16
Second contract	2026-01-16	2027-01-16
Third contract	2027-01-16	2028-01-16

To merge multiple contracts and increase the number of top-up tokens within a single activation period, contact the FortiCare team for assistance with a co-term purchase.



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.