

# New Features Guide

**FortiAnalyzer 8.0.0**



**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](mailto:techdoc@fortinet.com)



May 5, 2026

FortiAnalyzer 8.0.0 New Features Guide

05-800-1211640-20260505

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Overview</b> .....	<b>5</b>
<b>Security Operations (SOC)</b> .....	<b>6</b>
SOC automation .....	6
Playbook editor improvements .....	6
Incident and Alert Management .....	9
Alert explorer improvements .....	9
Dashboards .....	10
AI Access Visibility dashboard .....	10
Asset and Identity .....	12
Improvements to the user experience in the Asset and Identity Center .....	12
Others .....	15
FortiMQ connector for automated blocking .....	16
Machine learning for anomaly detection .....	21
<b>Log and Report</b> .....	<b>33</b>
Logging .....	33
FortiData incident support .....	33
Log Forwarding .....	35
FortiAnalyzer Fluentd supports the Azure Monitor Log Ingestion API .....	36
Reports .....	37
Anomaly login report .....	38
FortiDeceptor incident report .....	42
Shadow-AI report .....	48
<b>FortiAI</b> .....	<b>53</b>
FortiAI alert triage agent .....	53
FortiAI threat posture timeline .....	55
<b>System</b> .....	<b>59</b>
Others .....	59
Legal third party disclosure panel .....	59
Custom session labels in FortiAnalyzer event logs .....	61
SAML SSO supports SHA-256 and SHA-512 for both IdP and SP .....	65
FortiAnalyzer supports NTPv4 with SHA-256 encryption .....	66
Time-base retention is configurable for the task monitor and event log .....	68
FortiAnalyzer Fabric .....	68
Assign access to multiple fabric groups for a single admin .....	69
FortiAnalyzer Fabric Supervisor HA .....	71
<b>Index</b> .....	<b>76</b>
8.0.0 .....	76

# Change Log

Date	Change Description
2026-04-21	Initial release.
2026-05-05	Added: <ul style="list-style-type: none"><li>• Playbook editor improvements on page 6</li><li>• Alert explorer improvements on page 9</li><li>• AI Access Visibility dashboard on page 10</li><li>• Machine learning for anomaly detection on page 21</li><li>• Shadow-AI report on page 48</li><li>• FortiAI alert triage agent on page 53</li><li>• FortiAI threat posture timeline on page 55</li><li>• FortiAnalyzer Fabric Supervisor HA on page 71</li></ul>
2026-05-13	Added: <ul style="list-style-type: none"><li>• SAML SSO supports SHA-256 and SHA-512 for both IdP and SP on page 65</li><li>• FortiAnalyzer supports NTPv4 with SHA-256 encryption on page 66</li></ul>
2026-05-14	Added: <ul style="list-style-type: none"><li>• Time-base retention is configurable for the task monitor and event log on page 68</li></ul>

# Overview

This guide provides details of new features introduced in FortiAnalyzer 8.0. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiAnalyzer new features are organized into the following categories:

- [Security Operations \(SOC\) on page 6](#)
- [Log and Report on page 33](#)
- [FortiAI on page 53](#)
- [System on page 59](#)

For a list of all features organized by the version number that they were introduced, see [Index on page 76](#).

# Security Operations (SOC)

This section lists the new features added to FortiAnalyzer for security operations (SOC):

- [SOC automation on page 6](#)
- [Incident and Alert Management on page 9](#)
- [Dashboards on page 10](#)
- [Asset and Identity on page 12](#)
- [Others on page 15](#)

## SOC automation

This section lists the new features added to FortiAnalyzer for SOC automation:

- [Playbook editor improvements on page 6](#)

## Playbook editor improvements



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

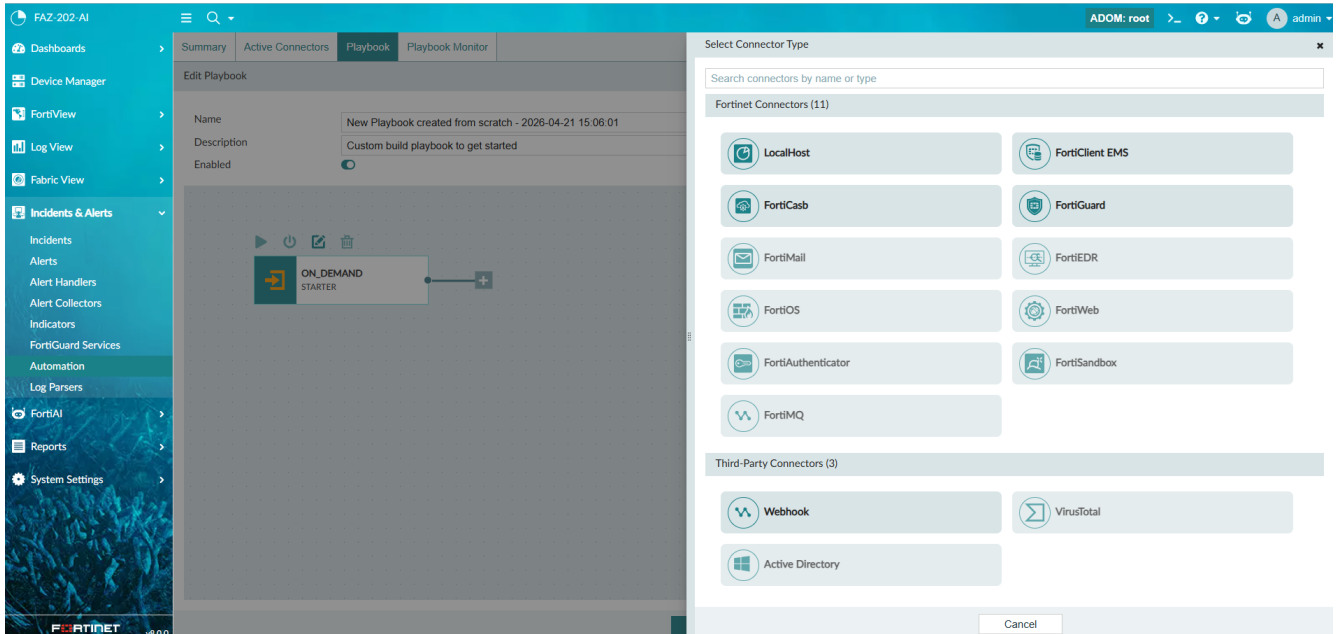
- [Playbooks](#)

The playbook editor in FortiAnalyzer 8.0.0 has been improved with a variety of features, including:

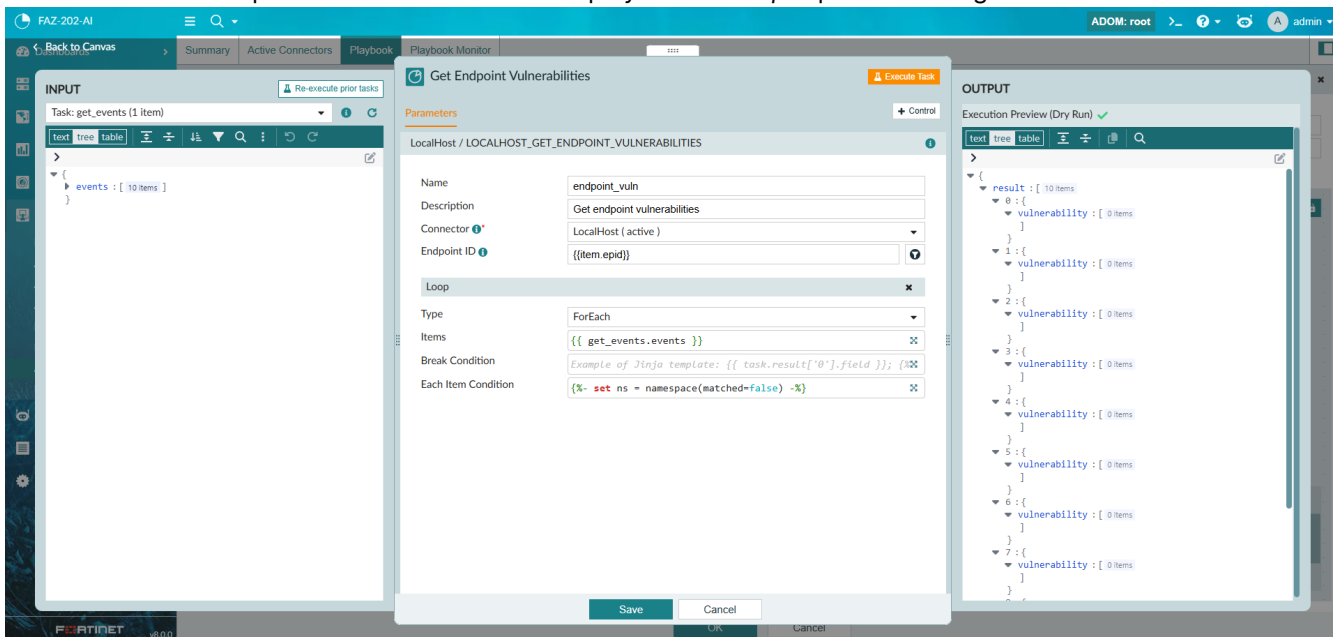
- Step-by-step debugging mode, including the capability to run, pause, and inspect data at each node (task).
- Play and re-play workflows, allowing you to use various input data for testing.
- Partial run capabilities, allowing you to restart from a specific node (task) instead of running the whole playbook.
- Extended workflow control support, including Branch(if), Wait Operator, Compare, and Switch.
- Jinja template support for control conditions and loops.

Below are some examples of the improvements with images included for reference. For complete instruction to create a playbook, see the FortiAnalyzer Administration Guide.

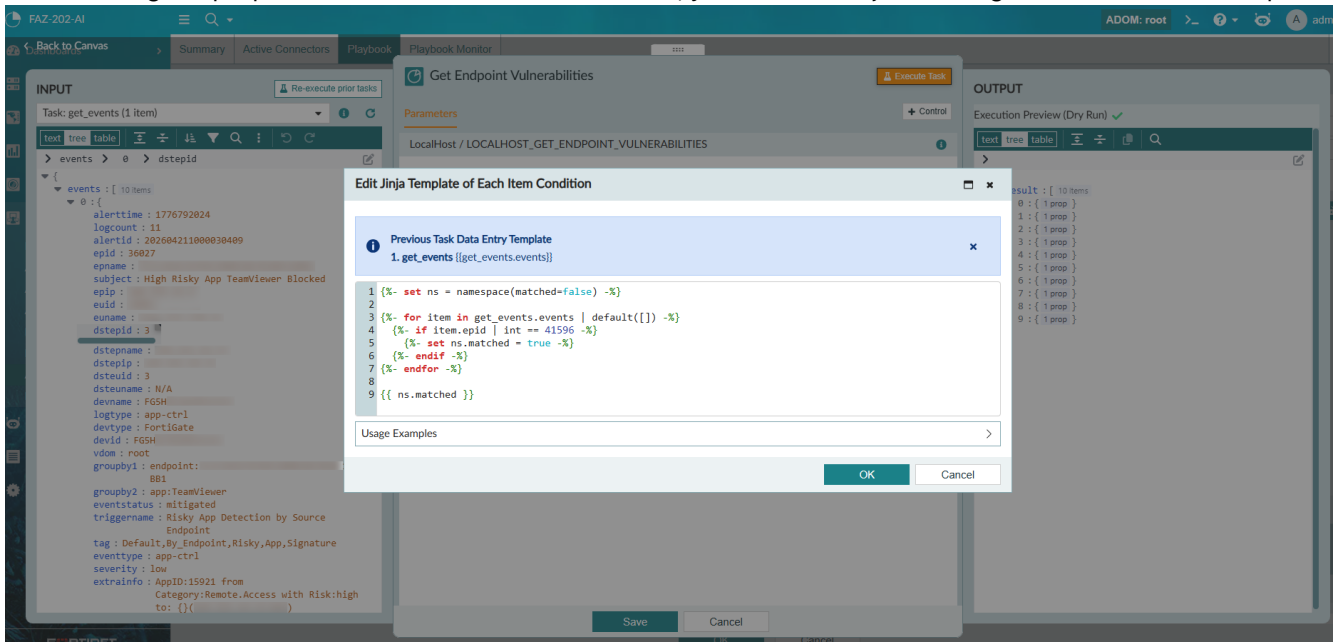
When selecting a connector for a playbook task, the unconfigured or inactive connectors are grayed out.



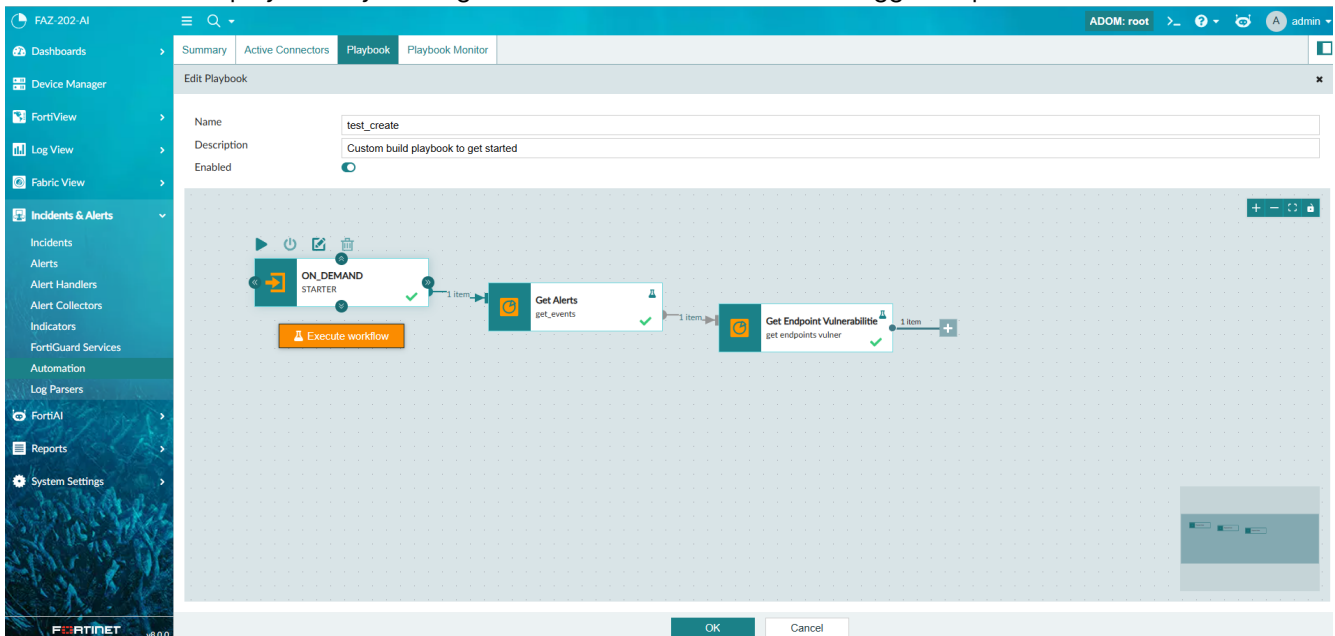
When configuring a task, the *Input* pane allows you to run the prior task and get results to use for debugging the current task. The output from the current task displays in the *Output* pane at the right.



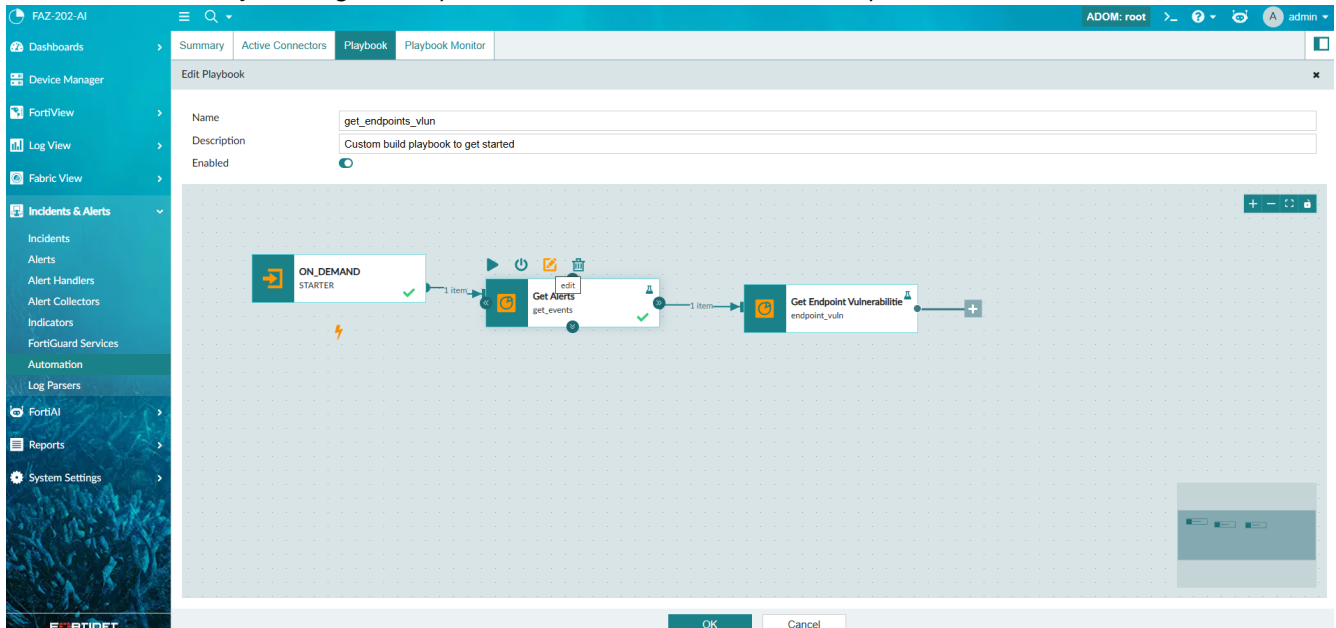
When editing the properties for a connector action (task), you can use Jinja to configure conditions and loops.



Execute the whole playbook by clicking *Execute Workflow* beneath the trigger step.



Execute step-by-step tasks by clicking the *Execute* button for the respective task. You can also delete or skip the current action by clicking the *Stop* button or *Delete* button for the respective task.



## Incident and Alert Management

This section lists the new features added to FortiAnalyzer for incident and alert management:

- [Alert explorer improvements on page 9](#)

### Alert explorer improvements



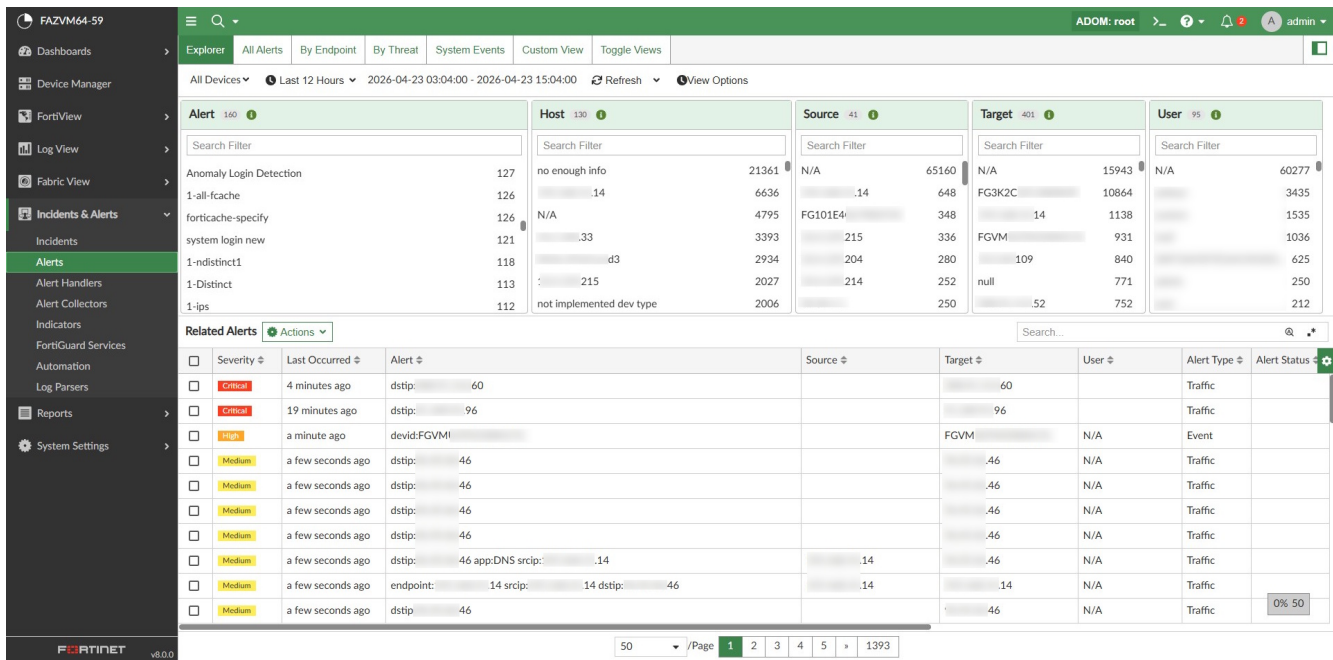
This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- [Explorer](#)

FortiAnalyzer 8.0.0 introduces improvements to *Incidents & Alerts > Alerts > Explorer*:

- The quick filters are sized to fit the width of the screen, so you do not have to scroll to find information.
- The Timeline chart is disabled by default to make more space for the Quick Filters and Related Alerts.
- A new option has been added to the *Actions*. Click *Details* to display information about the alert, handler, logs, and rules.

For more information about using this pane, see the FortiAnalyzer Administration Guide.



## Dashboards

This section lists the new features added to FortiAnalyzer for dashboards:

- [AI Access Visibility dashboard on page 10](#)

## AI Access Visibility dashboard



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

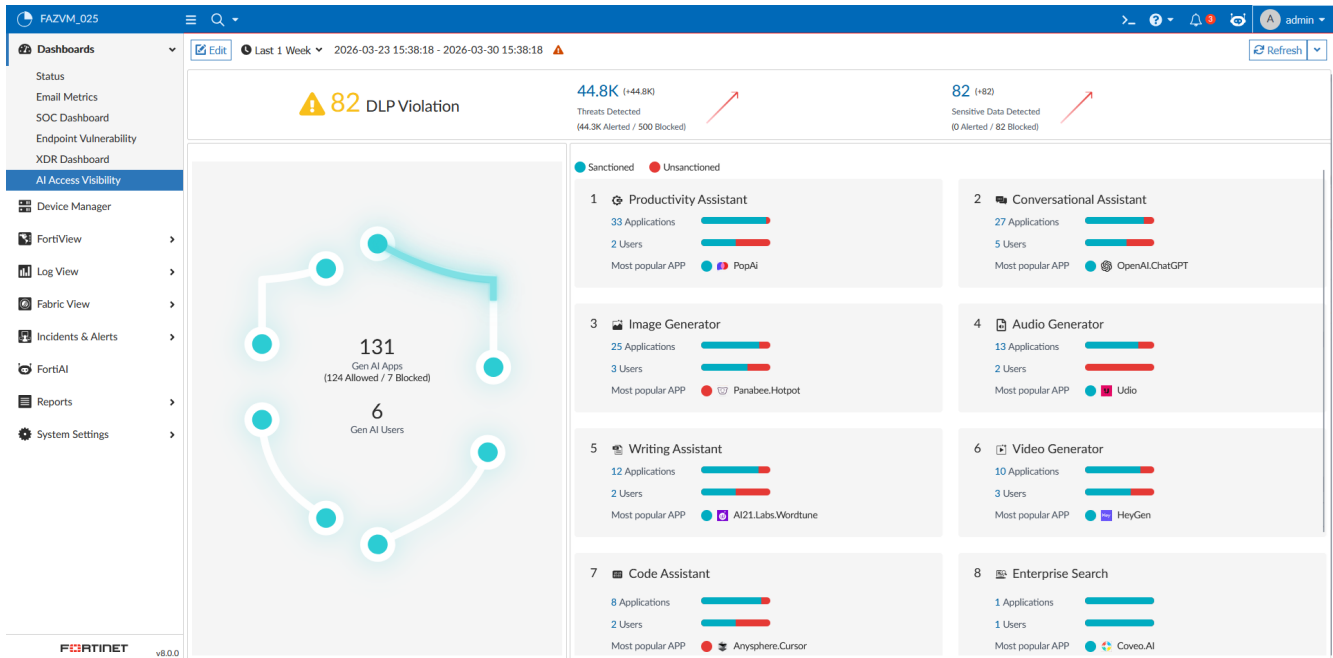
- [AI Access Visibility](#)

The *AI Access Visibility* dashboard has been added in FortiAnalyzer 8.0.0.

This dashboard displays AI access security information collected by authorized FortiGate devices, including:

- DLP logs
- DNS logs (category = Artificial Intelligence Technology)
- Web filter logs (category = Artificial Intelligence Technology)
- Application control logs (category = Generative AI)

You can filter the *AI Access Visibility* dashboard by timeframe and manually refresh the data or set a refresh interval.



This dashboard includes the following three widgets:

Widget	Description
<b>GEN AI Access Threats</b>	<p>This widget displays:</p> <ul style="list-style-type: none"> <li>Number of DLP violations detected.</li> <li>Number of threats detected, alerted, and blocked. Indicates if these numbers are trending up or down.</li> <li>Number of sensitive data detections, alerted, and blocked. Indicates if these numbers are trending up or down.</li> </ul>
<b>Gen AI Access Overview</b>	<p>Displays the total number of Generative AI applications accessed and total number of users that used these applications.</p> <p>This widget also displays the number of blocked and allowed applications available to the user.</p>
<b>Gen AI Access Categories</b>	<p>Displays the generative AI that has been accessed by category. Applications are grouped in the following categories, which are set in FortiGuard:</p> <ul style="list-style-type: none"> <li>Conversational Assistant</li> <li>Audio Generator</li> <li>Code Assistant</li> <li>Enterprise Search</li> <li>Image Generator</li> <li>Meeting Assistant</li> <li>Productivity Assistant</li> <li>Video Generator</li> <li>Writing Assistant</li> </ul>

Widget	Description
	Each category displays the total number of users and applications, including the most accessed application. The users and applications are divided into two groups: <i>Sanctioned</i> and <i>Unsanctioned</i> . These attributes are set in the authorized FortiGate devices.

## Asset and Identity

This section lists the new features added to FortiAnalyzer for asset and identity:

- Improvements to the user experience in the Asset and Identity Center on page 12

## Improvements to the user experience in the Asset and Identity Center



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

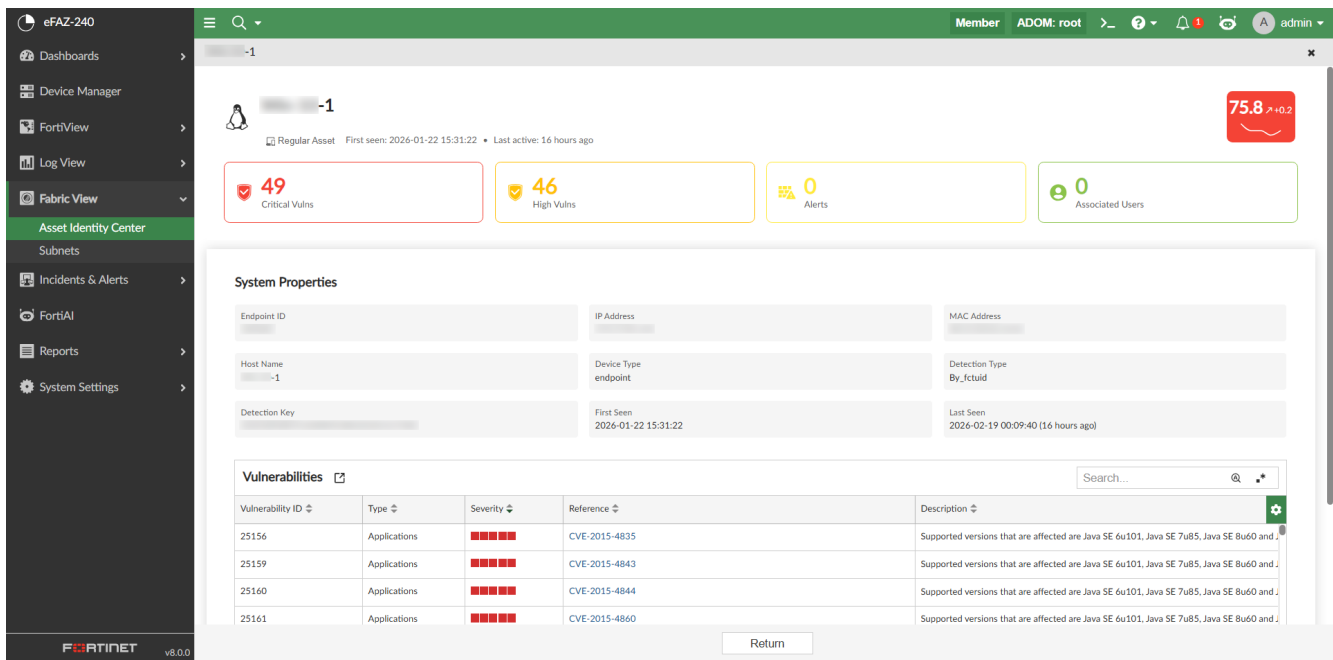
- Asset List
- Identity List

The GUI in *Fabric View > Asset Identity Center* has been changed in FortiAnalyzer 8.0.0 to improve the admin user experience.

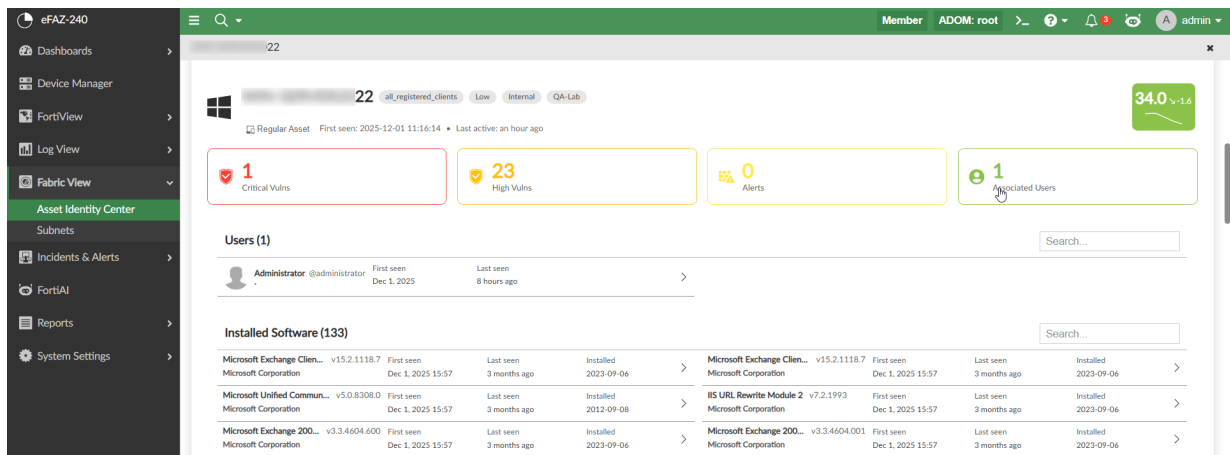
This includes the following changes in the *Asset and Identity List*:

- Colors are used with certain number fields to help identify severity. For example, see the *Top 10 Risky Assets* in the image above.
- Pagination is fixed on the footer of the *Asset Identity List*.
- The pill shape used in the *Asset Identity List*, such as in the *Vulnerabilities* column, is updated to unify with other elements in the UI.
- The *Top 10 Vulnerable Assets* widget does not display low severity vulnerabilities, since this widget is supposed to focus only on top threats.

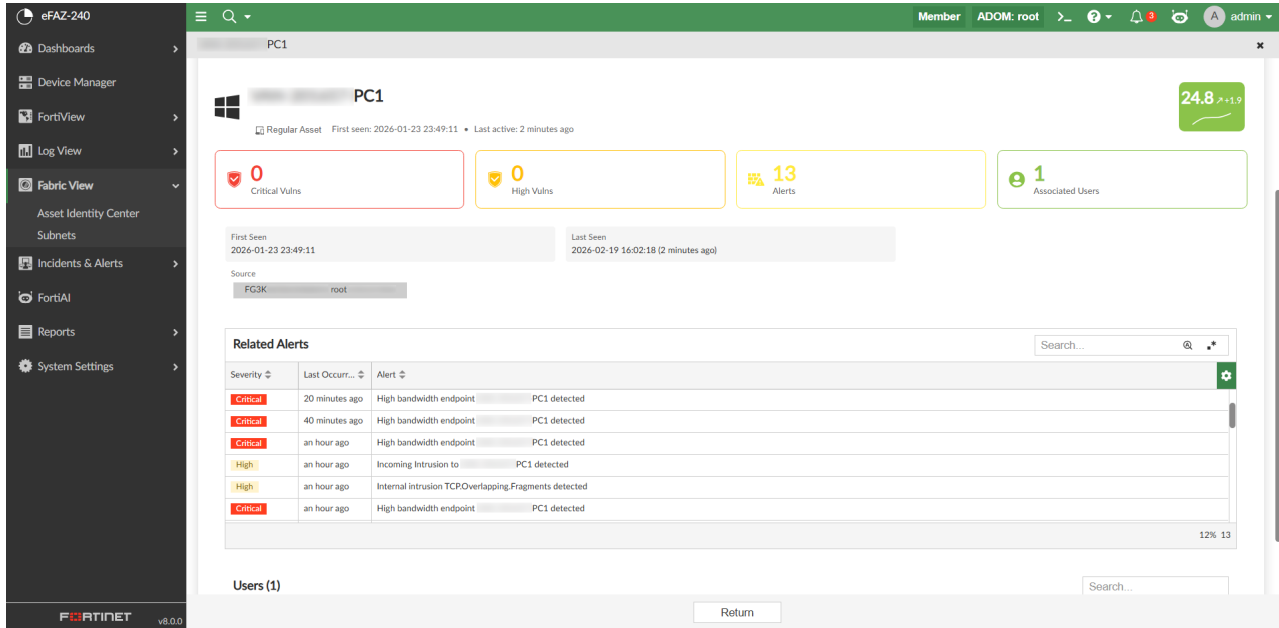
It also includes the following changes in the endpoint details:



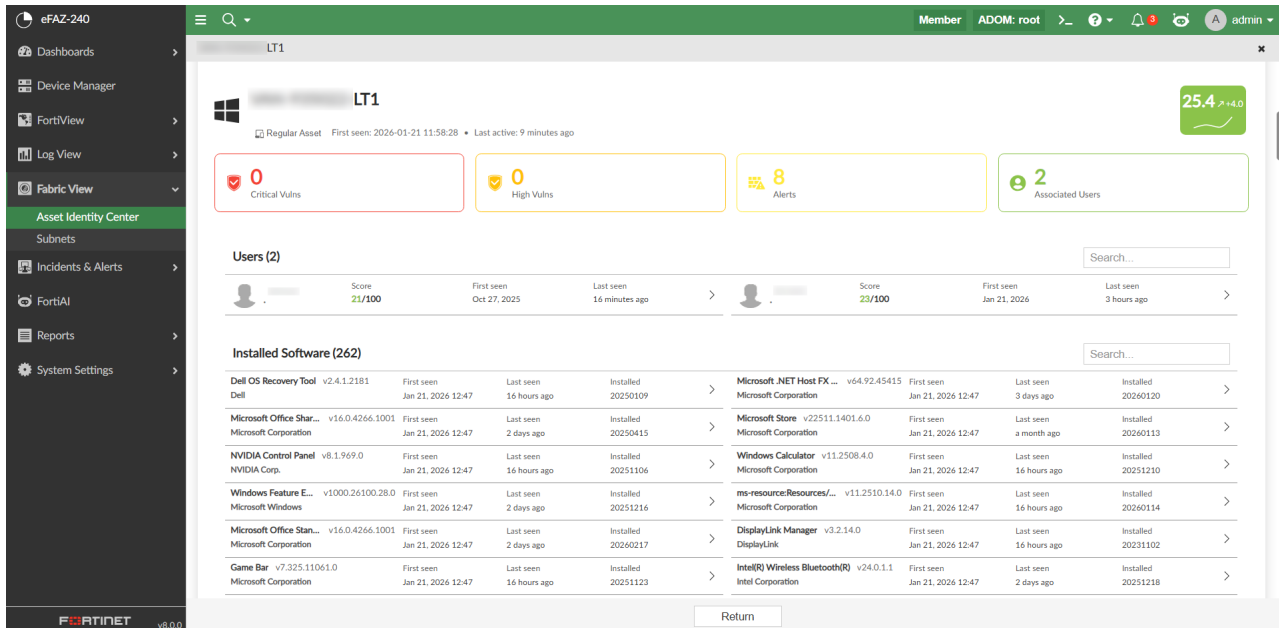
- After drilling down to an endpoint, the detail views now display in full screen.
- The four widgets at the top of the asset details are now colored to better visualize the information: *Critical Vulns*, *High Vulns*, *Alerts*, and *Associated Users*.
  - The four widgets at the top are also interactive; click the widget to jump to the related information within the detail view. For example, click the *Associated Users* to jump to the *Users* section in the details view.



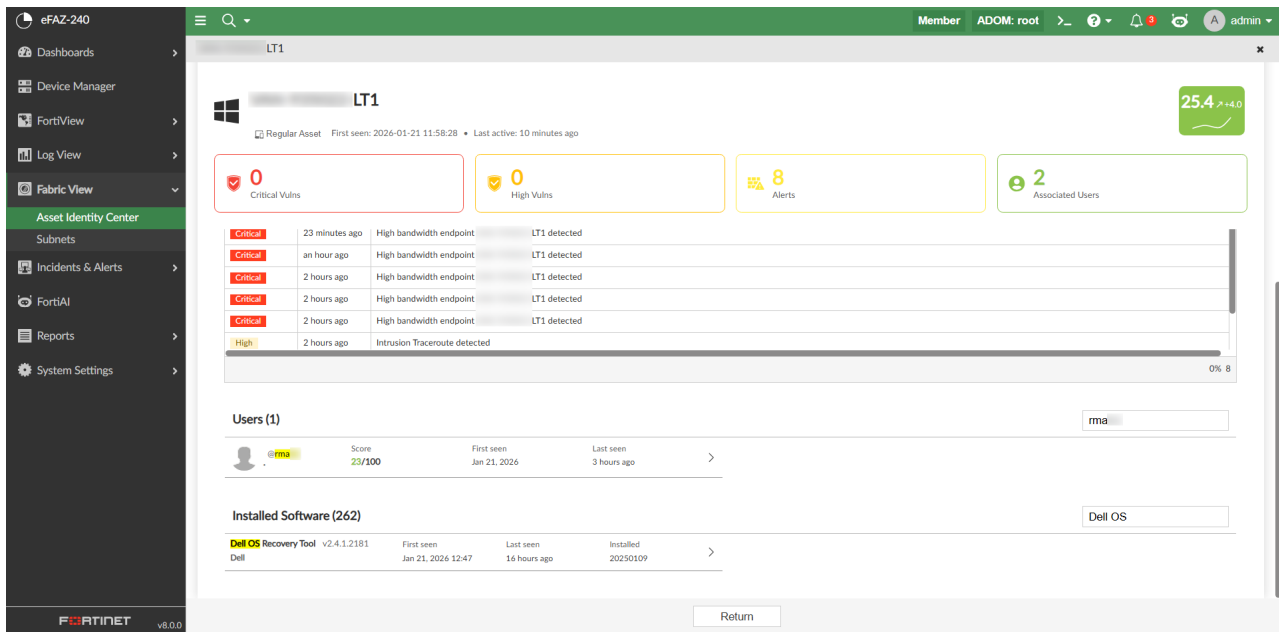
- The header information in the endpoint details, including the four widgets (*Critical Vulns*, *High Vulns*, *Alerts*, and *Associated Users*), is now fixed to the top so the user always sees key information as they scroll further down.
- The container heights have been increased to ensure more visibility, allowing the tables within containers to display at least six rows. For example, see the *Related Alerts* table below.



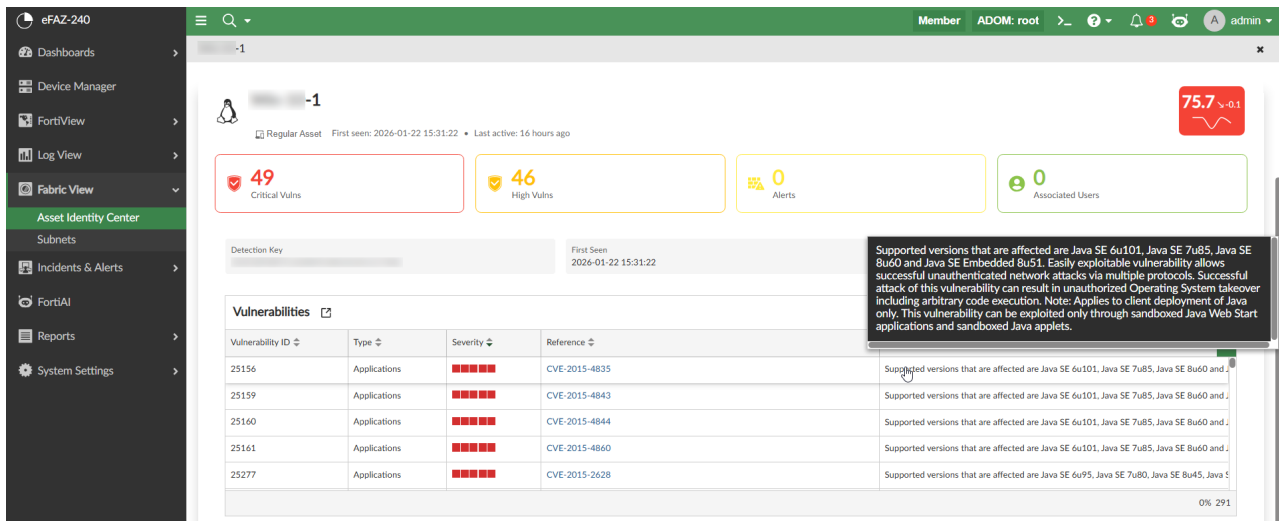
- The *Users* and *Installed Software* sections of the detail views now display in a split view, saving space while maintaining visibility and organization.



- The search tools in the details view, such as in the *Users* and *Installed Software* sections, will find and highlight the information for fast navigation.



- Tooltips now display in the color opposite of the color mode used by the interface, ensuring they are easily visible. Note that tooltip appearance delay is 300ms.



## Others

This section lists the new features added to FortiAnalyzer for other topics related to security operations:

- FortiMQ connector for automated blocking on page 16
- Machine learning for anomaly detection on page 21

# FortiMQ connector for automated blocking



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- [Connector actions > FortiMQ Connector](#)
- [Blocking indicators](#)

The FortiMQ Connector is introduced in FortiAnalyzer 8.0.0. This connector enables direct transmission of blocked indicators to FortiGate devices.

Previously, block lists could only be distributed to FortiGate devices using the FortiManager connector. This new feature provides an alternative and allows you to block indicators even without a FortiManager deployed in your environment.

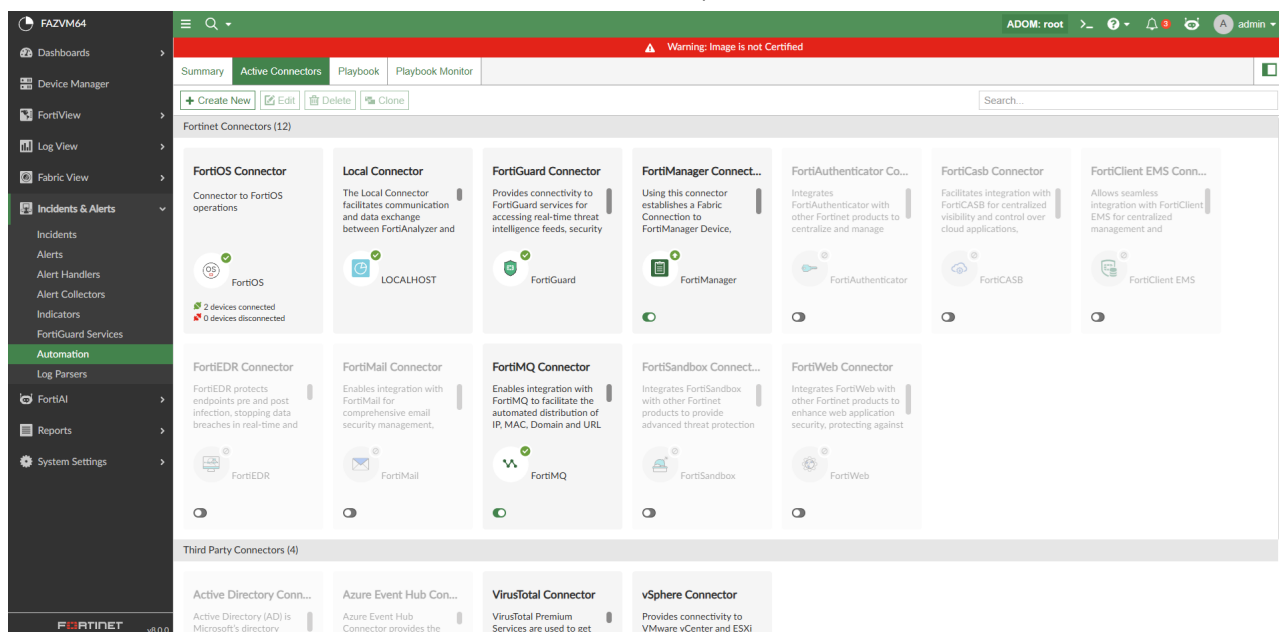
To enable the transmission of block lists from FortiAnalyzer to FortiGate, you must complete the following:

- Enable logging from the FortiGate devices to FortiAnalyzer. For more information, see the [FortiAnalyzer Administration Guide](#) and the [FortiGate/FortiOS Administration Guide](#).
- Verify that both FortiAnalyzer and FortiGate are registered under the same FortiCare account to allow proper communication and integration.
- Enable and configure Cloud-based Fabric Feed synchronization on FortiGate to consume and enforce the block indicators received. For more information, see the [FortiGate / FortiOS 8.0 New Features Guide](#).
- Enable the *FortiMQ Connector* in FortiAnalyzer.

The steps below assume the admin has already completed the first three requirements listed above. In these steps, they will enable and use the FortiMQ connector.


## To use the FortiMQ connector:

1. Go to *Incidents & Alerts > Automation > Active Connectors*, and enable the *FortiMQ Connector*.



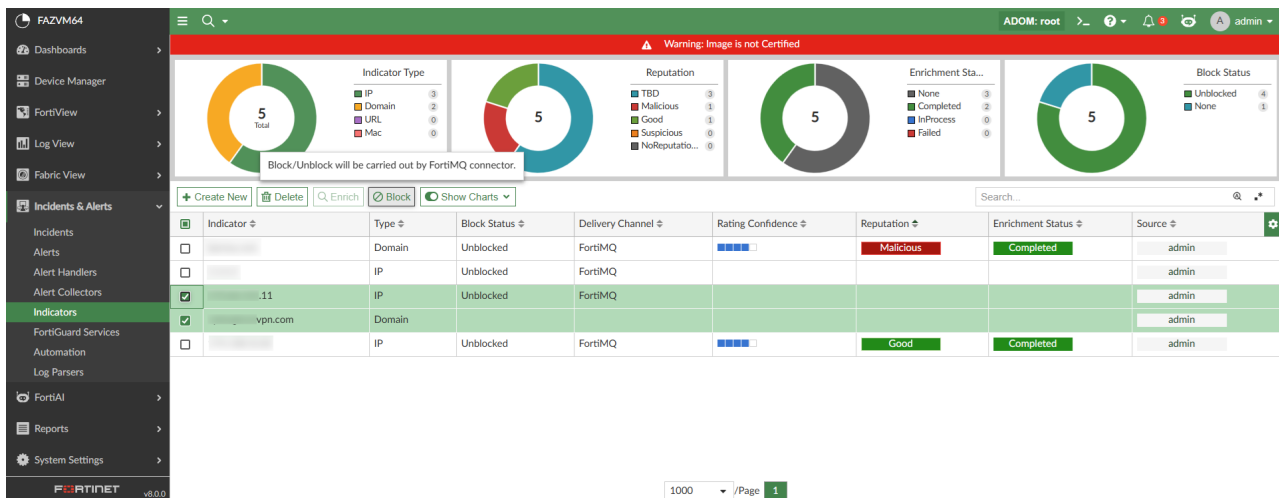
The FortiMQ connector is available and disabled by default in all Fabric and FortiGate-type ADOMs.

When enabled, this connector automatically establishes a connection to the FortiMQ cloud service; no additional configuration is required. The connector status reflects its health, indicating whether the API connection is successful.

 You cannot create new FortiMQ connectors or delete the existing one in the ADOM.


2. After confirming the connector is active, go to *Incidents & Alerts > Indicators* to block/unblock indicators. Indicators can also be blocked from *Incidents* and, as of 8.0.0, from *Log View* as well.
3. Select an indicator and click *Block*.

Mousing over the *Block* button displays the tooltip: “Block/Unblock will be carried out by FortiMQ connector.”

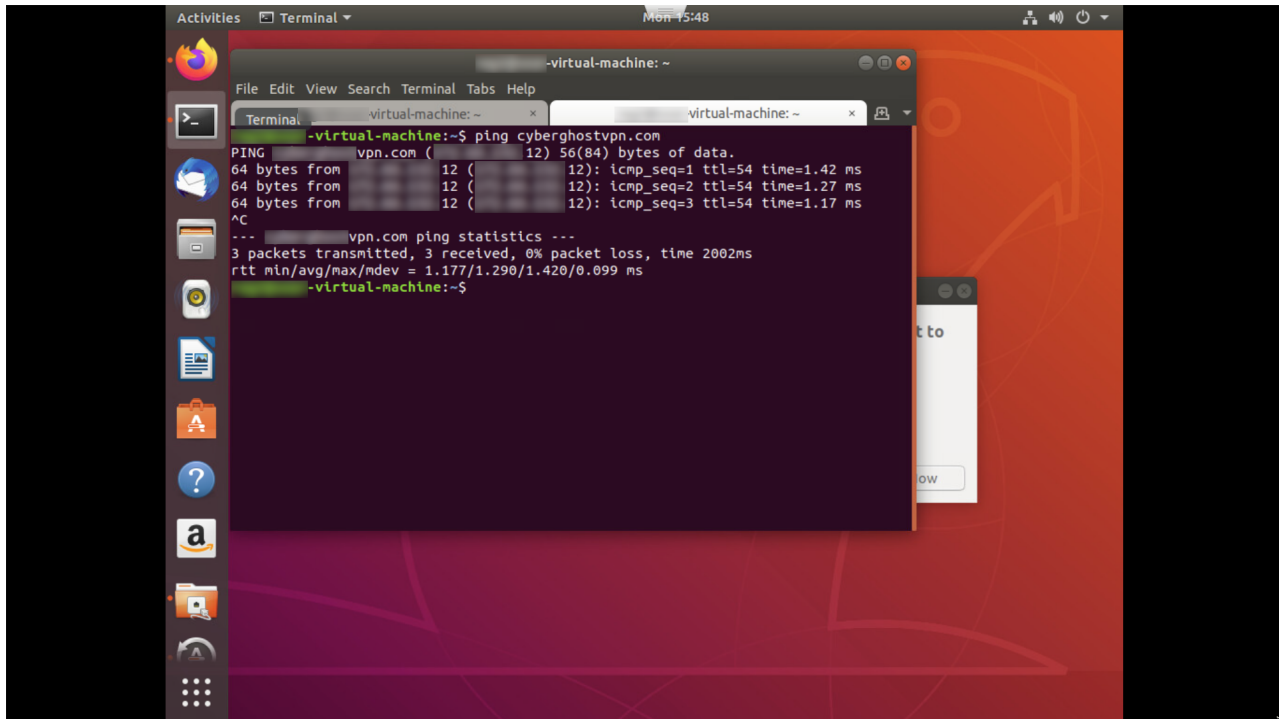


The screenshot shows the FortiAnalyzer interface for the 'Indicators' section. At the top, there are four donut charts: 'Indicator Type' (5 Total), 'Reputation' (5), 'Enrichment Sta...' (5), and 'Block Status' (5). Below these is a table of indicators. A tooltip is visible over the 'Block' button, stating 'Block/Unblock will be carried out by FortiMQ connector.'

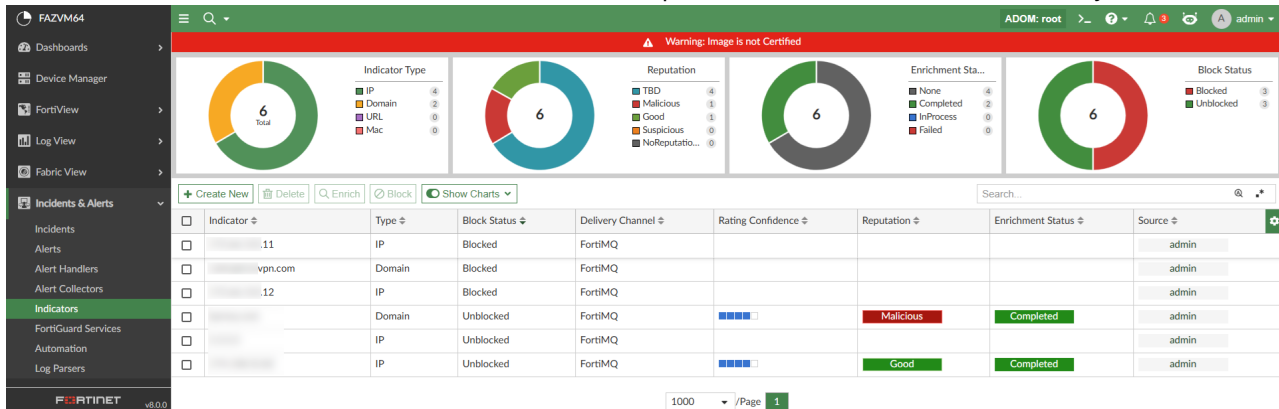
Indicator	Type	Block Status	Delivery Channel	Rating Confidence	Reputation	Enrichment Status	Source
[Redacted]	Domain	Unblocked	FortiMQ	[Progress Bar]	Malicious	Completed	admin
[Redacted]	IP	Unblocked	FortiMQ	[Progress Bar]	[Redacted]	[Redacted]	admin
[Redacted].11	IP	Unblocked	FortiMQ	[Progress Bar]	[Redacted]	[Redacted]	admin
[Redacted].vpn.com	Domain	Unblocked	FortiMQ	[Progress Bar]	Good	Completed	admin
[Redacted]	IP	Unblocked	FortiMQ	[Progress Bar]	[Redacted]	[Redacted]	admin

 When both FortiManager and FortiMQ connectors are available, blocking via FortiManager remains supported. However, priority is given to the FortiMQ connector. Indicators are sent via FortiManager only if the FortiMQ connector is disabled.

Below is an example where the above selected IP/domain are accessible from an endpoint before they were blocked:

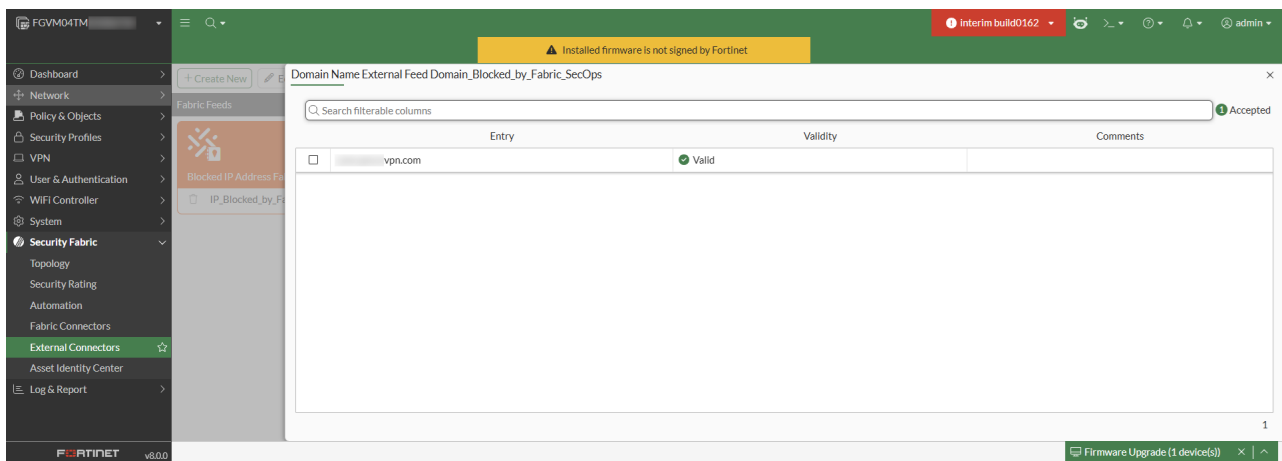
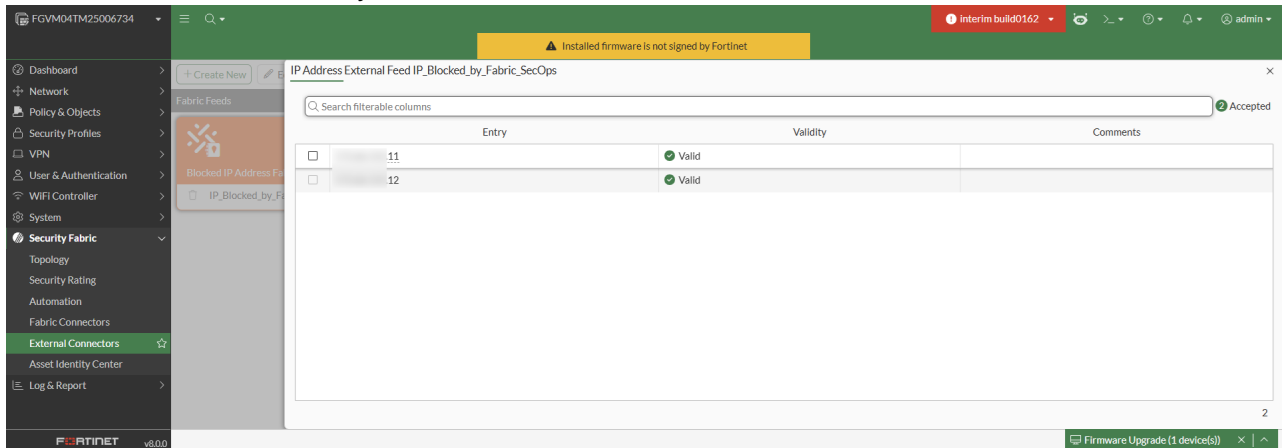


Upon confirming a *Block* or *Unblock* action, the “block\_indicator” playbook runs in the background and sends the indicators to FortiMQ. See below for an example of blocked indicators in FortiAnalyzer:

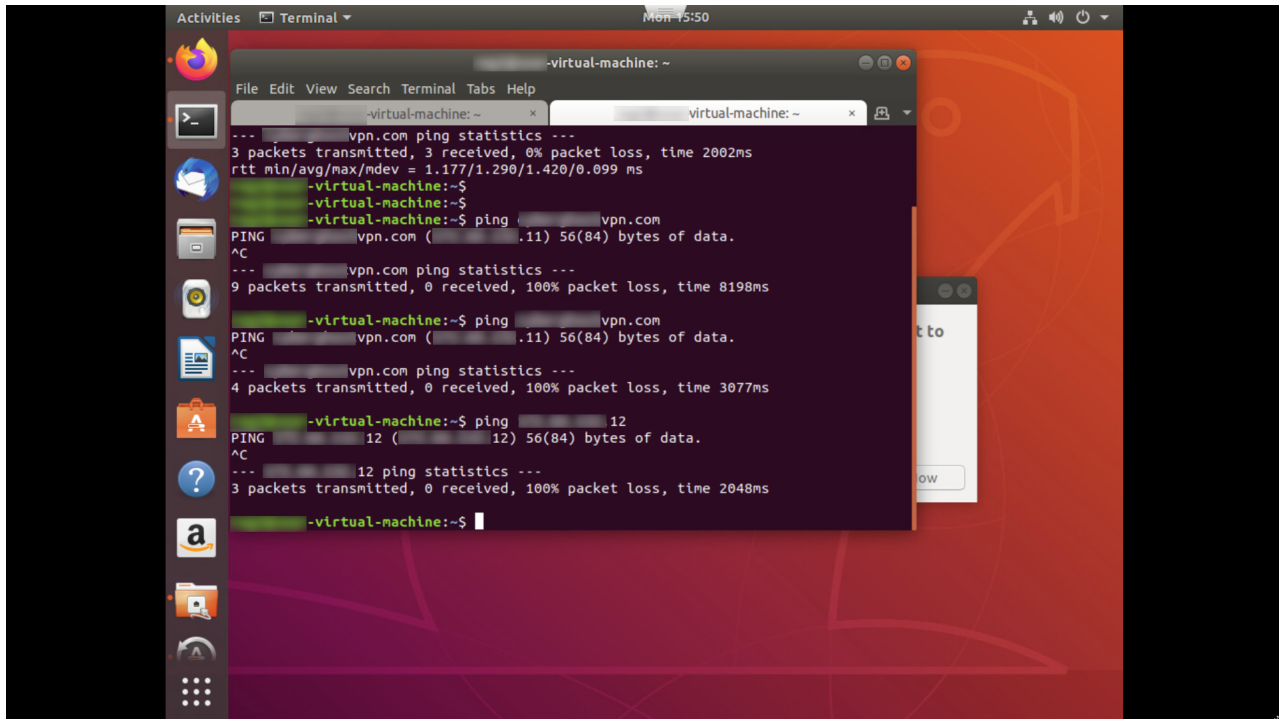


FortiGate retrieves these indicators from FortiMQ and updates them in the external feeds. These feeds can then be used in policies or profiles to deny access. External feeds are updated on FortiGate with the

indicators sent from FortiAnalyzer:

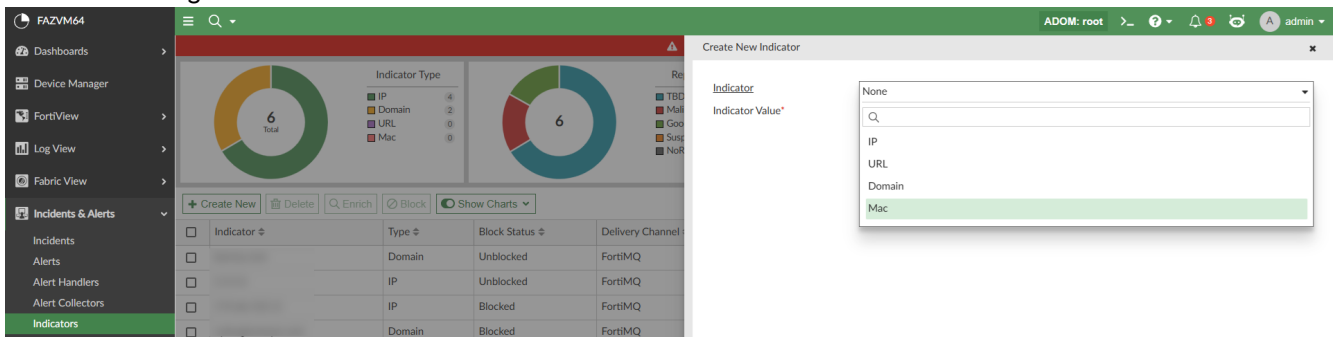


The policy in this example was setup to deny access to the above threat feeds. See below for the ping results:



💡 Unlike FortiManager, which operates at a global level, FortiMQ is ADOM-specific. Blocked indicators are applied only to FortiGate devices within the same FortiAnalyzer ADOM.

In FortiAnalyzer 8.0.0, a new type of indicator known as "Mac" can be created and blocked and unblocked to both FortiManager and FortiGate.



## To block indicators from Log View:

1. Go to *Log View*.
2. Right-click the value in the table, such as a malicious IP or domain, and select *Create indicator and block*.

The screenshot shows the FortiGate Log View interface. The table displays log entries with columns for #, Date/Time, Device ID, Action, Source, User, Destination IP, Service, Application, Sent/Received, and Security E. A context menu is open over the 'Destination IP' field of the 3rd log entry, showing options: 'Add AND Filter "Destination IP = ...16"', 'Add AND Filter "Destination IP != ...16"', 'Add OR Filter "Destination IP = ...16"', 'Add OR Filter "Destination IP != ...16"', 'Replace with Filter "Destination IP = ...16"', 'Replace with Filter "Destination IP != ...16"', and 'Create Indicator and Block'.

#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security E
1	2026-04-13 16:15:45	FGVM04TM	✓				HTTPS	SSL_TLSv1.3	1.9 KB/1.5 KB	
2	2026-04-13 16:15:32	FGVM5LTM	✓				RSH	RSH	60.0 B/0.0 KB	
3	2026-04-13 16:15:20	FGVM04TM	✓			.16	HTTPS	HTTPS	7.7 KB/10.2 KB	
4	2026-04-13 16:15:20	FGVM04TM	✓						7.7 KB/10.2 KB	
5	2026-04-13 16:15:17	FGVM5LTM	✓						5.5 KB/9.2 KB	
6	2026-04-13 16:15:17	FGVM5LTM	✓						300.0 B/0.0 KB	
7	2026-04-13 16:15:17	FGVM5LTM	✓						4.7 KB/12.0 KB	
8	2026-04-13 16:15:10	FGVM5LTM	✓						7.3 KB/10.6 KB	
9	2026-04-13 16:15:07	FGVM5LTM	✓						118.9 KB/84.4 KB	
10	2026-04-13 16:15:07	FGVM5LTM	✓				DNS	DNS	418.0 B/216.0 B	
11	2026-04-13 16:15:07	FGVM5LTM	✗ IP connecti				DNS	DNS	0 B/0 B	
12	2026-04-13 16:14:22	FGVM5LTM	✓				RSH	RSH	7.3 KB/10.6 KB	
13	2026-04-13 16:14:10	FGVM04TM	✓				DNS	DNS	345.0 B/839.0 B	
14	2026-04-13 16:13:45	FGVM04TM	✓				HTTPS	SSL_TLSv1.2	7.4 KB/7.3 KB	

You can also right-click the value in the log details view to access this action in the shortcut menu.

Supported field types for blocking indicators include:

- ip
- url
- domain
- mac-address

This action adds a new indicator and blocks it automatically.

## Machine learning for anomaly detection



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- [Machine learning for anomaly detection](#)

FortiAnalyzer 8.0.0 introduces a feature utilizing machine learning models to analyze historical log data and establish a unique behavioral profile for every user. This feature automates the detection of zero-day threats and insider threats that do not follow known attack signatures. It solves the issue of alert fatigue by reducing noise from static rules. It also addresses the detection gap by identifying account takeovers (unusual login times/locations) and data exfiltration (abnormal upload volumes) that would otherwise go unnoticed under traditional security policies.

As of 8.0.0, this feature supports the generation of anomaly alerts for the following scenarios:

- *FortiAuthenticator Login Anomalies*: Detects unusual login activities based on geographical location and time deviations.

- *FortiGate Traffic Anomalies*: Detects excessive or abnormal inbound and outbound traffic patterns, helping to identify potential data exfiltration or compromised hosts.

Before configuring this feature on your FortiAnalyzer, it is recommended to get familiar with the following machine learning components:

- **Model**: The core machine learning algorithm designed for a specific task (for example, login anomaly or traffic download anomaly).
- **Asset**: A specific entity being monitored, such as an enduser or an endpoint device.
- **Artifact**: The finalized, trained model data generated after processing historical logs. This artifact is what the system actively uses to perform real-time inference and detect anomalies.

To utilize the Machine Learning Anomaly Detection feature, you must enable the machine learning engine globally and configure the specific models to establish a training schedule.

The feature is managed in the FortiAnalyzer CLI. Enabling the machine learning flow (`mlflow`) initiates the creation of required materialized views (MVs) in the backend database.

## Enabling the machine learning engine and configuring models

In the FortiAnalyzer CLI, enable and configure the machine learning flow (`config system mlflow`).

This includes setting the training schedule, defining the historical data period (`train-data-days`), and enabling automatic deployment of the trained artifact. See the example below.

```
config system mlflow
  set status enable

  config models
    edit 1
      set status enable

      set model-type login-anomaly

      set artifact-max-count 10

      set artifact-retention 30

      set asset-max-count 10000

      set train-data-days 90

      set train-repeat-at '7d'

      set train-test-days 7

      set auto-deploy enable

      set inference-interval 20
```


```

    next
end
end

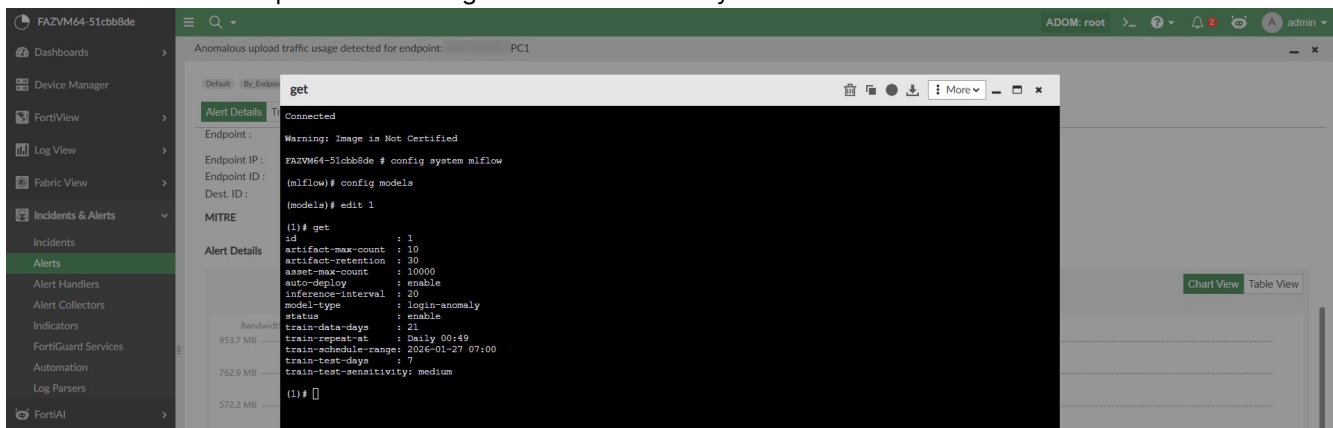
```

Variable descriptions:

Variable	Description
status {enable   disable}	Default disable, enable to allow training and inference of mlflow related logic for a specific model.
model-type {login-anomaly   traffic-download-anomaly   traffic-upload-anomaly}	Only one of each model-type allowed in config.
train-schedule-range <string>	Use system timezone. Start scheduled training after the start time. End scheduled training after end time. Training schedule range formats: <ul style="list-style-type: none"> <li>• Continuous training: 'YYYY-MM-DD HH:MM' For example: '2025-01-01 00:00'</li> <li>• Bounded range: 'YYYY-MM-DD HH:MM -- YYYY-MM-DD HH:MM' For example: '2025-01-01 00:00 -- 2026-01-01 00:00'</li> </ul> Default: Start from current time (continuous).
train-repeat-at <string>	Training repeat schedule formats: <ul style="list-style-type: none"> <li>• Daily: 'Daily HH:MM' For example: 'Daily 02:00'</li> <li>• Weekly: 'Weekly &lt;Day&gt; HH:MM' For example: 'Weekly Monday 02:00' or 'Weekly Mon 02:00'</li> <li>• Monthly (day of month): 'Monthly &lt;DD&gt; HH:MM' For example: 'Monthly 15 02:00' (15th of each month)</li> <li>• Monthly (nth weekday): 'Monthly &lt;N&gt; &lt;Day&gt; HH:MM' For example: 'Monthly 3 Monday 02:00' (3rd Monday of each month)</li> <li>• Interval: '&lt;N&gt;d' For example: '7d' (every 7 days)</li> </ul> Default: 7d (train every 7 days since the start time of train-schedule-range).
train-data-days <integer>	Number of days of historical data to use for model training. More training data generally improves model accuracy but increases training time and resource usage (1 - 365, default = 90).
train-test-days <integer>	Number of days used for testing the trained model. Must be less than or equal to train-data-days (1 - 90, default = 7). During testing, assets that fail to meet the sensitivity criteria are added to the exclusion list.
train-test-sensitivity {high   low   medium}	Training test sensitivity. <ul style="list-style-type: none"> <li>• high: High sensitivity. Uses strict criteria during testing, more assets in</li> </ul>

Variable	Description
	<p>exclusion list.</p> <ul style="list-style-type: none"> <li>• low: Low sensitivity. Uses lenient criteria during testing, fewer assets in exclusion list.</li> <li>• medium: Medium sensitivity. Balanced testing criteria, moderate asset in exclusion list.</li> </ul>
asset-max-count <integer>	Maximum number of assets to track. Assets include endusers and endpoints depending on the model type. Higher values require more memory and processing resources (100 - 100000, default = 1000).
auto-deploy {enable   disable}	Deploy artifact automatically when model is trained on schedule. If this is disabled, see <a href="#">Manually training the machine learning models and validating artifacts on page 26</a> to manually deploy the artifact.
inference-interval <integer>	<p>Inference interval in minutes (1 - 1440, default = 20). Defines how frequently the model analyzes new data for anomalies. Shorter intervals provide faster detection but use more resources.</p> <p>Recommended values by model type:</p> <ul style="list-style-type: none"> <li>• login-anomaly: 20 minutes</li> <li>• traffic-download-anomaly: 60 minutes (must be multiple of 60)</li> <li>• traffic-upload-anomaly: 60 minutes (must be multiple of 60)</li> </ul>
 Traffic models require inference-interval to be a multiple of 60.	
artifact-retention <integer>	<p>Artifact retention period in days (1 - 365, default = 30). Artifacts older than this period are automatically deleted. The most recent artifact-max-count artifacts are always retained regardless of age.</p>
artifact-max-count <integer>	<p>Maximum number of artifacts to retain per model (1 - 100, default = 10). Older artifacts beyond this count are deleted automatically. This limit is enforced regardless of artifact-retention setting.</p>

See below for an example mlflow configured in the FortiAnalyzer CLI:



## Monitoring the lifecycle of the machine learning models

You can use the `diagnose mlflow` commands to monitor the lifecycle of the machine learning models from training progress to artifact deployment.

Command	Description
<code>diagnose mlflow config</code>	Show per-model config and artifact stats (count, deployed, last trained).
<code>diagnose mlflow infer-result &lt;artifact_name&gt;</code>	Display latest inference results for an artifact. Enter the name of the artifact (for example, 2025123110000050100).
<code>diagnose mlflow list-artifacts &lt;arg0&gt;</code>	List all trained artifacts. Optional filters: <code>status=&lt;val&gt;</code> , <code>model_type=&lt;val&gt;</code> , <code>artifact_name=&lt;val&gt;</code> . For example: <code>status=deployed model_type=login-anomaly artifact_name=&lt;name&gt;</code>
<code>diagnose mlflow show-assets &lt;artifact_name&gt;</code>	List assets trained and excluded for the artifact. Enter the name of the artifact (for example, 2025123110000050100).
<code>diagnose mlflow show-details &lt;artifact_name&gt;</code>	Show detailed information about a specific artifact. Enter the name of the artifact (for example, 2025123110000050100).
<code>diagnose mlflow test-result &lt;artifact_name&gt;</code>	Display latest test results for an artifact. Enter the name of the artifact (for example, 2025123110000050100).
<code>diagnose mlflow training-status</code>	Show current training progress for models in training.

See below for examples of the `diagnose mlflow` outputs:

```
diagnose mlflow list...
Connected
Warning: Image is NOT Certified
FA2VM64-5lcb88de # diagnose mlflow list-artifacts
=== ML Artifacts ===
-----
id | artifact_name | model_type | status | ds_start_time | ds_end_time | created_at | deployed_at | retired_at | comment
-----
2026042310000000300 | 2026042310000000300 | traffic-upload-anomaly | deployed | 2026-04-02 00:49:00 | 2026-04-16 00:49:00 | 2026-04-23 00:57:18 | 2026-04-23 01:00:02 | | |
2026042310000000200 | 2026042310000000200 | traffic-download-anomaly | deployed | 2026-04-02 00:49:00 | 2026-04-16 00:49:00 | 2026-04-23 00:54:44 | 2026-04-23 00:57:50 | | |
2026042310000000100 | 2026042310000000100 | login-anomaly | deployed | 2026-04-02 00:49:00 | 2026-04-16 00:49:00 | 2026-04-23 00:49:01 | 2026-04-23 00:55:49 | | |
2026042110000000300 | 2026042110000000300 | traffic-upload-anomaly | retired | 2026-03-31 00:49:00 | 2026-04-14 00:49:00 | 2026-04-21 00:58:43 | 2026-04-21 01:01:43 | 2026-04-22 01:01:31 | |
2026042110000000200 | 2026042110000000200 | traffic-download-anomaly | retired | 2026-03-31 00:49:00 | 2026-04-14 00:49:00 | 2026-04-21 00:55:49 | 2026-04-21 00:58:55 | 2026-04-22 00:59:07 | |
2026042110000000100 | 2026042110000000100 | login-anomaly | retired | 2026-03-31 00:49:00 | 2026-04-14 00:49:00 | 2026-04-21 00:49:02 | 2026-04-21 00:56:55 | 2026-04-22 00:56:43 | |
2026042010000000300 | 2026042010000000300 | traffic-upload-anomaly | retired | 2026-03-30 00:49:00 | 2026-04-13 00:49:00 | 2026-04-20 00:59:04 | 2026-04-20 01:02:06 | 2026-04-21 01:01:43 | |
2026042010000000200 | 2026042010000000200 | traffic-download-anomaly | retired | 2026-03-30 00:49:00 | 2026-04-13 00:49:00 | 2026-04-20 00:56:11 | 2026-04-20 00:59:36 | 2026-04-21 00:58:55 | |
2026042010000000100 | 2026042010000000100 | login-anomaly | retired | 2026-03-30 00:49:00 | 2026-04-13 00:49:00 | 2026-04-20 00:49:05 | 2026-04-20 00:57:17 | 2026-04-21 00:56:55 | |
FA2VM64-5lcb88de #
```

```
diagnose mlflow conf...
FAZWM64-51cbb8de # diagnose mlflow config
=== Mlflow System Status ===
Mlflow: enabled

--- login-anomaly ---
Enabled: yes
Auto-Deploy: yes
Train Data Days: 21
Train Test Days: 7
Test Sensitivity: medium
Asset Max Count: 10000
Inference Interval: 30 min
Artifact Retention: 30 days
Artifact Max Count: 10
Train Schedule: 2026-01-27 07:00
Train Repeat At: Daily 00:49
Artifact Count: 3
Deployed Artifact: 2026042310000000100
Last Trained: 2026-04-23 00:49:01

--- traffic-download-anomaly ---
Enabled: yes
Auto-Deploy: yes
Train Data Days: 21
Train Test Days: 7
Test Sensitivity: medium
Asset Max Count: 10000
Inference Interval: 30 min
Artifact Retention: 30 days
Artifact Max Count: 10
Train Schedule: 2026-01-27 07:00
Train Repeat At: Daily 00:49
Artifact Count: 3
Deployed Artifact: 2026042310000000200
Last Trained: 2026-04-23 00:54:44

--- traffic-upload-anomaly ---
Enabled: yes
Auto-Deploy: yes
Train Data Days: 21
Train Test Days: 7
Test Sensitivity: medium
Asset Max Count: 10000
Inference Interval: 30 min
Artifact Retention: 30 days
Artifact Max Count: 10
Train Schedule: 2026-01-27 07:00
Train Repeat At: Daily 00:49
Artifact Count: 3
Deployed Artifact: 2026042310000000300
Last Trained: 2026-04-23 00:57:18
```

```
diagnose mlflow info...
FAZWM64-51cbb8de # diagnose mlflow infer-result
artifact_name Name of the artifact (e.g., 20251231100000050100).
FAZWM64-51cbb8de # diagnose mlflow infer-result 2026042310000000300
=== ML Inference Results for 2026042310000000300 (Latest 10) ===
id type event time adom name created at euid epid ext data
2026042330000040900 traffic-upload-anomaly 2026-04-23 08:00:00 root 2026-04-23 09:38:43 3 3441 ["end": 1776956400, "epid": 3441, "euid": 3, "recv": 50432319, "sent": 50432319, "type": "outgoing", "itime": 1776956400, "ratio": 32.430, "start": 1776956400, "predict": 4057211, "explanation": "During 8:00 to 9:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 46.10 MB is higher than predicted peak 3.87 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"09:00\", \"anomaly_hour_start\": \"08:00\", \"traffic_observed_bytes\": 50432319, \"traffic_observed_human\": 46.10 MB, \"traffic_predicted_bytes\": 4057211, \"traffic_predicted_human\": \"3.87 MB\"]
2026042330000040800 traffic-upload-anomaly 2026-04-23 08:00:00 root 2026-04-23 09:38:43 3 4686 ["end": 1776956000, "epid": 4686, "euid": 3, "recv": 9730614, "sent": 9730614, "type": "outgoing", "itime": 1776956400, "ratio": 3.116, "start": 1776956400, "predict": 3124988, "explanation": "During 8:00 to 9:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 9.28 MB is higher than predicted peak 2.98 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"09:00\", \"anomaly_hour_start\": \"08:00\", \"traffic_observed_bytes\": 9730614, \"traffic_observed_human\": \"9.28 MB\", \"traffic_predicted_bytes\": 3124988, \"traffic_predicted_human\": \"2.98 MB\"]
2026042330000041000 traffic-upload-anomaly 2026-04-23 08:00:00 root 2026-04-23 09:38:43 9435 11013 ["end": 1776960000, "epid": 11013, "euid": 9435, "recv": 28124179, "sent": 28124179, "type": "outgoing", "itime": 1776956400, "ratio": 1.334, "start": 1776956400, "predict": 21076462, "explanation": "During 8:00 to 9:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 26.82 MB is higher than predicted peak 20.10 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"09:00\", \"anomaly_hour_start\": \"08:00\", \"traffic_observed_bytes\": 28124179, \"traffic_observed_human\": \"26.82 MB\", \"traffic_predicted_bytes\": 21076462, \"traffic_predicted_human\": \"20.10 MB\"]
2026042330000038700 traffic-upload-anomaly 2026-04-23 07:00:00 root 2026-04-23 08:38:42 3 4397 ["end": 1776956400, "epid": 4397, "euid": 3, "recv": 6466967, "type": "outgoing", "itime": 1776952800, "ratio": 10.985, "start": 1776952800, "predict": 588700, "explanation": "During 7:00 to 8:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 6.17 MB is higher than predicted peak 0.56 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"08:00\", \"anomaly_hour_start\": \"07:00\", \"traffic_observed_bytes\": 6466967, \"traffic_observed_human\": \"6.17 MB\", \"traffic_predicted_bytes\": 588700, \"traffic_predicted_human\": \"0.56 MB\"]
2026042330000038900 traffic-upload-anomaly 2026-04-23 07:00:00 root 2026-04-23 08:38:42 1602 3314 ["end": 1776956400, "epid": 3314, "euid": 1602, "recv": 14449407, "sent": 14449407, "type": "outgoing", "itime": 1776952800, "ratio": 1.677, "start": 1776952800, "predict": 8616327, "explanation": "During 7:00 to 8:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 13.78 MB is higher than predicted peak 8.22 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"08:00\", \"anomaly_hour_start\": \"07:00\", \"traffic_observed_bytes\": 14449407, \"traffic_observed_human\": \"13.78 MB\", \"traffic_predicted_bytes\": 8616327, \"traffic_predicted_human\": \"8.22 MB\"]
2026042330000038300 traffic-upload-anomaly 2026-04-23 07:00:00 root 2026-04-23 08:38:42 3 2969 ["end": 1776956400, "epid": 2969, "euid": 3, "recv": 59131409, "sent": 59131409, "type": "outgoing", "itime": 1776952800, "ratio": 11.421, "start": 1776952800, "predict": 517286, "explanation": "During 7:00 to 8:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 56.39 MB is higher than predicted peak 4.94 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"08:00\", \"anomaly_hour_start\": \"07:00\", \"traffic_observed_bytes\": 59131409, \"traffic_observed_human\": \"56.39 MB\", \"traffic_predicted_bytes\": 517286, \"traffic_predicted_human\": \"4.94 MB\"]
2026042330000038800 traffic-upload-anomaly 2026-04-23 07:00:00 root 2026-04-23 08:38:42 2991 3206 ["end": 1776956400, "epid": 3206, "euid": 2991, "recv": 31897573, "sent": 31897573, "type": "outgoing", "itime": 1776952800, "ratio": 1.331, "start": 1776952800, "predict": 23957796, "explanation": "During 7:00 to 8:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 30.42 MB is higher than predicted peak 22.85 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"08:00\", \"anomaly_hour_start\": \"07:00\", \"traffic_observed_bytes\": 31897573, \"traffic_observed_human\": \"30.42 MB\", \"traffic_predicted_bytes\": 23957796, \"traffic_predicted_human\": \"22.85 MB\"]
2026042330000038600 traffic-upload-anomaly 2026-04-23 07:00:00 root 2026-04-23 08:38:42 1571 3441 ["end": 1776956400, "epid": 3441, "euid": 1571, "recv": 10717176, "sent": 10717176, "type": "outgoing", "itime": 1776952800, "ratio": 23.605, "start": 1776952800, "predict": 4540213, "explanation": "During 7:00 to 8:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 102.21 MB is higher than predicted peak 4.33 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"08:00\", \"anomaly_hour_start\": \"07:00\", \"traffic_observed_bytes\": 10717176, \"traffic_observed_human\": \"102.21 MB\", \"traffic_predicted_bytes\": 4540213, \"traffic_predicted_human\": \"4.33 MB\"]
2026042330000038400 traffic-upload-anomaly 2026-04-23 07:00:00 root 2026-04-23 08:38:42 2958 3629 ["end": 1776956400, "epid": 3629, "euid": 2958, "recv": 53682431, "sent": 53682431, "type": "outgoing", "itime": 1776952800, "ratio": 2.080, "start": 1776952800, "predict": 25813624, "explanation": "During 7:00 to 8:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 51.20 MB is higher than predicted peak 24.62 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"08:00\", \"anomaly_hour_start\": \"07:00\", \"traffic_observed_bytes\": 53682431, \"traffic_observed_human\": \"51.20 MB\", \"traffic_predicted_bytes\": 25813624, \"traffic_predicted_human\": \"24.62 MB\"]
2026042330000038900 traffic-upload-anomaly 2026-04-23 07:00:00 root 2026-04-23 08:38:42 1326 3340 ["end": 1776956400, "epid": 3340, "euid": 1326, "recv": 13983533, "sent": 13983533, "type": "outgoing", "itime": 1776952800, "ratio": 1.626, "start": 1776952800, "predict": 8547737, "explanation": "During 7:00 to 8:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 13.34 MB is higher than predicted peak 8.15 MB based on historical data from 2026-04-02 to 2026-04-16, \"anomaly_date\": \"Thu 2026-04-23\", \"anomaly_hour_end\": \"08:00\", \"anomaly_hour_start\": \"07:00\", \"traffic_observed_bytes\": 13983533, \"traffic_observed_human\": \"13.34 MB\", \"traffic_predicted_bytes\": 8547737, \"traffic_predicted_human\": \"8.15 MB\"]
FAZWM64-51cbb8de #
```

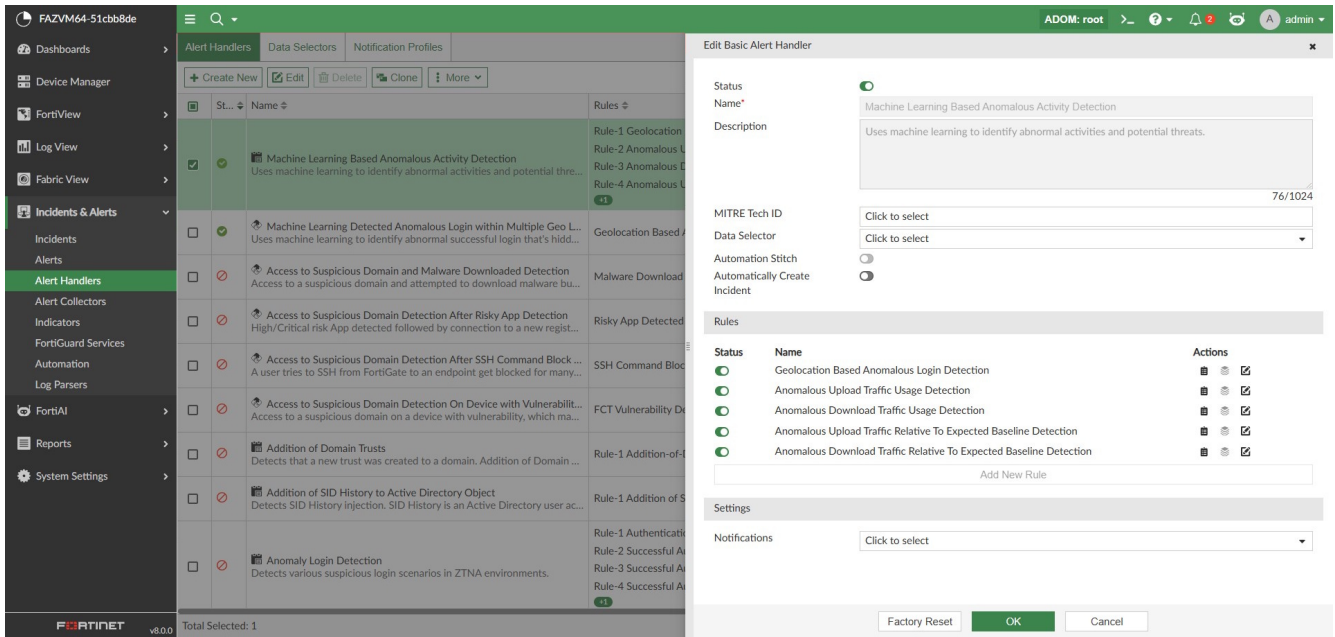
## Manually training the machine learning models and validating artifacts

You can use the execute mlflow commands to manually train the machine learning models, exclude assets, and validate artifacts.

Command	Description
<code>execute mlflow cancel &lt;artifact_name&gt;</code>	Cancel artifact training.
<code>execute mlflow delete &lt;artifact_name&gt;</code>	Permanently delete artifact.
<code>execute mlflow deploy &lt;artifact_name&gt;</code>	Deploy artifact for active inference.
<code>execute mlflow exclusion-list {artifact   model} {add   list   remove} &lt;asset&gt;</code>	<p>Manage ML exclusion-lists.</p> <ul style="list-style-type: none"> <li><b>artifact:</b> Artifact-level exclusion-list operations. <ul style="list-style-type: none"> <li><code>add</code>: Add asset to artifact exclusion-list.</li> <li><code>list</code>: List exclusion-listed assets for artifact.</li> <li><code>remove</code>: Remove asset from artifact exclusion-list.</li> </ul> </li> <li><b>model:</b> Model-level exclusion-list operations. <ul style="list-style-type: none"> <li><code>add</code>: Add asset to model exclusion-list.</li> <li><code>list</code>: List exclusion-listed assets for model type.</li> <li><code>remove</code>: Remove asset from model exclusion-list.</li> </ul> </li> </ul>
<code>execute mlflow test &lt;artifact_name&gt; &lt;start_time&gt; &lt;end_time&gt;</code>	<p>Test/validate artifact on specified time range.</p> <ul style="list-style-type: none"> <li><code>&lt;start_time&gt; &lt;end_time&gt;</code>: Start time and end time can be entered in the following format: YYYY-MM-DD HH:MM.</li> </ul>
<code>execute mlflow train &lt;model_type&gt; &lt;start_time&gt; &lt;end_time&gt; [train-assets-limit]</code>	<p>Train the machine learning model on specified time range.</p> <ul style="list-style-type: none"> <li><code>&lt;model_type&gt;</code>: Model type includes login-anomaly, traffic-download-anomaly, traffic-upload-anomaly.</li> <li><code>&lt;start_time&gt; &lt;end_time&gt;</code>: Start time and end time can be entered in the following format: YYYY-MM-DD HH:MM.</li> <li><code>[train-assets-limit]</code>: Optionally, set the maximum number of assets to train (1 - 100000).</li> </ul> <p>Example:</p> <pre>execute mlflow train login-anomaly '2026-02-05' '2026-05-05'</pre>
<code>execute mlflow undeploy &lt;artifact_name&gt;</code>	Undeploy artifact from active inference.

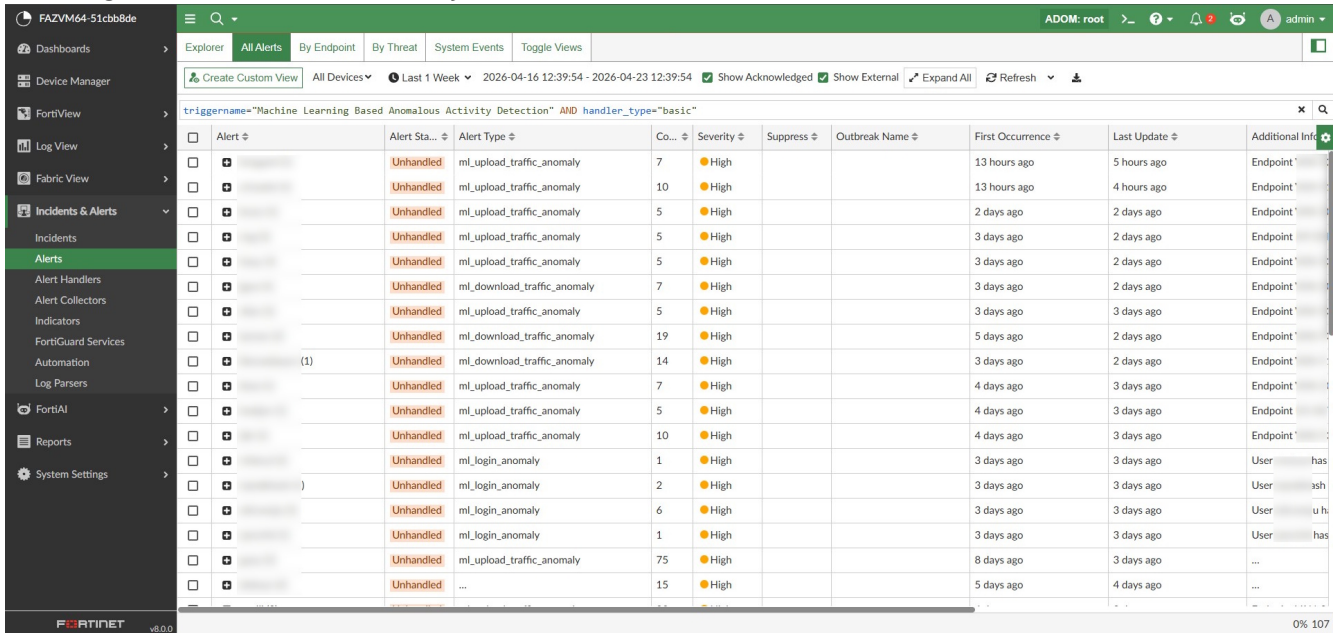
## Alert Handler: Machine Learning Based Anomalous Activity Detection

The internal inference events are automatically processed by the predefined alert handler named *Machine Learning Based Anomalous Activity Detection*.



Once triggered, an alert is generated, providing the analyst with context regarding the deviation. For example, an alert highlighting that an upload volume exceeded the user's specific 90-day behavioral pattern.

The alerts can be found in *Incidents & Alerts > Alerts > All Alerts*; filter by the triggered alert handler (Machine Learning Based Anomalous Activity Detection).



Click the alerts to view their details. See examples below.

### Example: Anomalous upload traffic usage

ADOM: root > admin

Anomalous upload traffic usage detected for endpoint: LTO

Alert Details Triggering Logs Actions

Formatted View Raw JSON

Alert Time: 4/23/2026, 7:07:49 AM  
 Update Time: 4/23/2026, 8:07:59 AM  
 Last Log Time: 4/23/2026, 6:00:00 AM  
 First Log Time: 4/23/2026, 12:00:00 AM

Alert ID: 202604231000000002  
 Alert Type: ml\_upload\_traffic\_anomaly  
 Severity: High

Rule Information

Rule Name: Anomalous Upload Traffic Usage Detection  
 Handler Type: basic  
 Log Type: siem  
 Acknowledged Time: N/A  
 Automation Stitch: no

Alert Handler Name: Machine Learning Based Anomalous Activity Detection  
 Device Type: SIEM  
 Acknowledged: no  
 Log Count: 7  
 Suppressed: no

Endpoint

Endpoint Name: LTO  
 Endpoint IP: [redacted]  
 Endpoint User ID: 1566  
 Dest. ID: 0  
 Dest. User ID: 0

MITRE

Alert Details

Weekly Bandwidth Per Hour

Bandwidth

333.8 MB  
 286.1 MB

ADOM: root > admin

Anomalous upload traffic usage detected for endpoint: LTO

Alert Details Triggering Logs Actions

Endpoint Name: LTO

Endpoint IP: 158  
 Endpoint User ID: 1566  
 Endpoint ID: 3214  
 Dest. User ID: 0  
 Dest. ID: 0

MITRE

Alert Details

Weekly Bandwidth Per Hour

Bandwidth

333.8 MB  
 286.1 MB  
 238.4 MB  
 190.7 MB  
 143.1 MB  
 95.4 MB  
 47.7 MB  
 0.0 KB

Upload

Fri. 00:00:00 Sat. 00:00:00 Sun. 00:00:00 Mon. 00:00:00 Tue. 00:00:00 Wed. 00:00:00 Thu. 00:00:00

Rule Summary

When (Threshold Duration): 1440 minutes  
 Group By: enduser, endpoint  
 Description: data\_sourcetype='FortiGate' and event\_type='traffic'  
 Pattern: IF ML\_ANOMALY\_OUTBOUND\_TRAFFIC(\*)>=5  
 FILTER data\_sourcetype='FortiGate' and event\_type='traffic'

Click the table view to display the information in text format:

**Anomalous upload traffic usage detected for endpoint:** LTO

Endpoint IP: [redacted] 158  
 Endpoint User ID: 1566  
 Endpoint ID: 3214  
 Dest. User ID: 0  
 Dest. ID: 0

**Alert Details**

12:00 am to 1:00 am, Thu 2026-04-23  
 During 0:00 to 1:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 9.72 MB is higher than predicted peak 2.56 MB based on historical data from 2026-04-02 to 2026-04-16

1:00 am to 2:00 am, Thu 2026-04-23  
 During 1:00 to 2:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 10.07 MB is higher than predicted peak 2.55 MB based on historical data from 2026-04-02 to 2026-04-16

2:00 am to 3:00 am, Thu 2026-04-23  
 During 2:00 to 3:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 9.71 MB is higher than predicted peak 2.57 MB based on historical data from 2026-04-02 to 2026-04-16

4:00 am to 5:00 am, Thu 2026-04-23  
 During 4:00 to 5:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 9.63 MB is higher than predicted peak 2.45 MB based on historical data from 2026-04-02 to 2026-04-16

5:00 am to 6:00 am, Thu 2026-04-23  
 During 5:00 to 6:00 on Thu 2026-04-23, the outgoing traffic observed at endpoint 10.07 MB is higher than predicted peak 2.45 MB based on historical data from 2026-04-02 to 2026-04-16

**Rule Summary**

When (Threshold Duration): 1440 minutes  
 Description: data\_sourcetype='FortiGate' and event\_type='traffic'

Group By: enduser, endpoint  
 Pattern: IF ML\_ANOMALY\_OUTBOUND\_TRAFFIC[\*]>=5  
 FILTER data\_sourcetype='FortiGate' and event\_type='traffic'

### Example: Anomalous download traffic usage

**Anomalous download traffic usage detected for endpoint:** PC1

Alert Time: 4/21/2026, 6:35:24 AM  
 Update Time: 4/21/2026, 11:35:34 AM  
 Last Log Time: 4/21/2026, 10:00:00 AM  
 First Log Time: 4/20/2026, 2:00:00 PM

Alert ID: 202604211000000002  
 Alert Type: ml\_download\_traffic\_anomaly  
 Severity: High

**Rule Information**

Rule Name: Anomalous Download Traffic Usage Detection  
 Handler Type: basic  
 Log Type: siem  
 Acknowledged Time: N/A  
 Automation Stitch: no

Alert Handler Name: Machine Learning Based Anomalous Activity Detection  
 Device Type: SIEM  
 Acknowledged: no  
 Log Count: 7  
 Suppressed: no

**Endpoint**

Endpoint: [redacted] PC1  
 Endpoint Name: [redacted] PC1  
 Endpoint IP: [redacted]  
 Endpoint User ID: 2958  
 Endpoint ID: 3629  
 Dest. User ID: 0  
 Dest. ID: 0

**Alert Details**

Weekly Bandwidth Per Hour

Bandwidth: 4.7 GB

FAZVM64-51cbb8de ADOM: root admin

Anomalous download traffic usage detected for endpoint: PC1

Alert Details Triggering Logs Actions

Endpoint Name: PC1  
 Endpoint IP: 168  
 Endpoint User ID: 2958  
 Endpoint ID: 3629  
 Dest. User ID: 0  
 Dest. ID: 0

MITRE

Alert Details

Weekly Bandwidth Per Hour

Bandwidth: 4.7 GB, 3.7 GB, 2.8 GB, 1.9 GB, 953.7 MB, 0.0 KB

Download

Rule Summary

When (Threshold Duration): 1440 minutes

Description: data\_sourcetype='FortiGate' and event\_type='traffic'

Group By: enduser, endpoint

Pattern: IF ML\_ANOMALY\_INBOUND\_TRAFFIC(\*)>=5  
 FILTER data\_sourcetype='FortiGate' and event\_type='traffic'

FAZVM64-51cbb8de ADOM: root admin

Anomalous download traffic usage detected for endpoint: PC1

Alert Details Triggering Logs Actions

Endpoint Name: PC1  
 Endpoint IP: 168  
 Endpoint User ID: 2958  
 Endpoint ID: 3629  
 Dest. User ID: 0  
 Dest. ID: 0

MITRE

Alert Details

Collapse All

- 2:00 pm to 3:00 pm, Mon 2026-04-20  
 During 16:00 to 17:00 on Wed 2026-04-20, the incoming traffic observed at endpoint 154.64 MB is higher than predicted peak 106.93 MB based on historical data from 1969-12-31 to 1969-12-31
- 3:00 pm to 4:00 pm, Mon 2026-04-20  
 During 16:00 to 17:00 on Wed 2026-04-20, the incoming traffic observed at endpoint 206.22 MB is higher than predicted peak 79.15 MB based on historical data from 1969-12-31 to 1969-12-31
- 11:00 pm 2026-04-20 to 12:00 am 2026-04-21  
 During 16:00 to 17:00 on Wed 2026-04-20, the incoming traffic observed at endpoint 235.94 MB is higher than predicted peak 198.49 MB based on historical data from 1969-12-31 to 1969-12-31
- 4:00 am to 5:00 am, Tue 2026-04-21  
 During 16:00 to 17:00 on Wed 2026-04-21, the incoming traffic observed at endpoint 700.97 MB is higher than predicted peak 89.62 MB based on historical data from 1969-12-31 to 1969-12-31
- 5:00 am to 6:00 am, Tue 2026-04-21  
 During 16:00 to 17:00 on Wed 2026-04-21, the incoming traffic observed at endpoint 280.17 MB is higher than predicted peak 113.19 MB based on historical data from 1969-12-31 to 1969-12-31

Rule Summary

When (Threshold Duration): 1440 minutes

Description: data\_sourcetype='FortiGate' and event\_type='traffic'

Group By: enduser, endpoint

Pattern: IF ML\_ANOMALY\_INBOUND\_TRAFFIC(\*)>=5  
 FILTER data\_sourcetype='FortiGate' and event\_type='traffic'

### Example: Anomalous login

**Alert Details** Triggering Logs Timeline Actions

**Formatted View** Raw JSON

Alert Time : 4/7/2026, 5:28:27 PM  
 Update Time : 4/8/2026, 8:58:37 AM  
 Last Log Time : 4/8/2026, 8:11:14 AM  
 First Log Time : 4/7/2026, 4:46:44 PM

**Rule Information**

Rule Name : Geolocation Based Anomalous Login Detection  
 Handler Type : basic  
 Log Type : siem  
 Acknowledged Time : N/A  
 Automation Stitch : no

**Endpoint**

Endpoint User ID : 4582  
 Dest. User ID : 0

**MITRE**

**Alert Details**

Alert ID : 202604071000000447  
 Alert Type : ml\_login\_anomaly  
 Severity : High

Alert Handler Name : Machine Learning Based Anomalous Activity Detection  
 Device Type : SIEM  
 Acknowledged : no  
 Log Count : 28  
 Suppressed : no

Endpoint ID : 0  
 Dest. ID : 0

**Alert Details** Triggering Logs Timeline Actions

Collapse All

**Baseline login location: Burnaby, Canada**  
 A deviation was detected on 2026-04-07 16:46:44-07:00

- New location: Paris, France
- New IP Address: 20

This event may indicate unusual or potentially unauthorized access.

**Rule Summary**

When (Threshold Duration) : 1440 minutes  
 Group By : enduser

Pattern : IF ML\_ANOMALY\_LOGIN(\*)=1  
 FILTER

**Note**

0/1023

# Log and Report

This section lists the new features added to FortiAnalyzer for logs and reports:

- [Logging on page 33](#)
- [Log Forwarding on page 35](#)
- [Reports on page 37](#)

## Logging

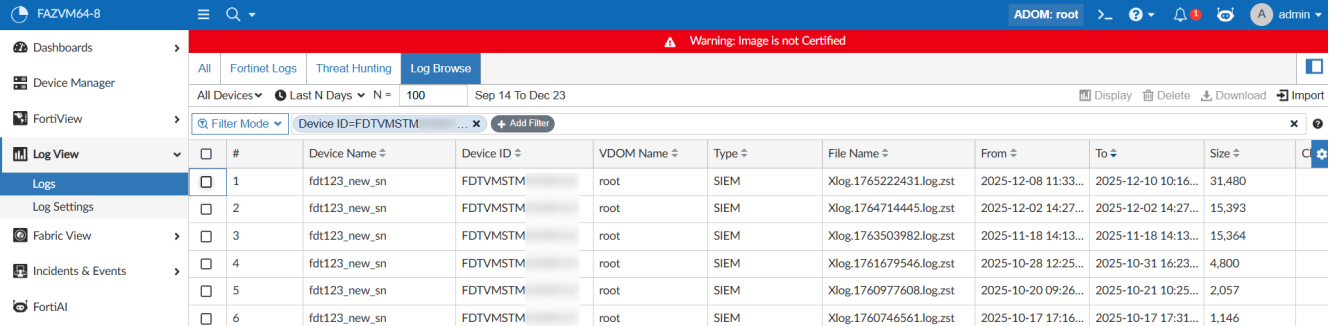
This section lists the new features added to FortiAnalyzer for logging:

- [FortiData incident support on page 33](#)

## FortiData incident support

FortiData is now a supported device for FortiAnalyzer.

The FortiData device (FDTxxxxxx) can be added in FortiAnalyzer *Device Manager*. The FortiData device will send SIEM Xlog log files to FortiAnalyzer. These files can be seen in FortiAnalyzer *Log View > Logs > Log Browse*.



#	Device Name	Device ID	VDOM Name	Type	File Name	From	To	Size
1	fdt123_new_sn	FDTVMSTM	root	SIEM	Xlog.1765222431.log.zst	2025-12-08 11:33...	2025-12-10 10:16...	31,480
2	fdt123_new_sn	FDTVMSTM	root	SIEM	Xlog.1764714445.log.zst	2025-12-02 14:27...	2025-12-02 14:27...	15,393
3	fdt123_new_sn	FDTVMSTM	root	SIEM	Xlog.1763503982.log.zst	2025-11-18 14:13...	2025-11-18 14:13...	15,364
4	fdt123_new_sn	FDTVMSTM	root	SIEM	Xlog.1761679546.log.zst	2025-10-28 12:25...	2025-10-31 16:23...	4,800
5	fdt123_new_sn	FDTVMSTM	root	SIEM	Xlog.1760977608.log.zst	2025-10-20 09:26...	2025-10-21 10:25...	2,057
6	fdt123_new_sn	FDTVMSTM	root	SIEM	Xlog.1760746561.log.zst	2025-10-17 17:16...	2025-10-17 17:31...	1,146

These logs will insert into the FortiAnalyzer SIEM database (siemdb), so the logs can be found in *Log View > Logs > All*. The following three types of incident logs are currently supported in FortiAnalyzer 8.0.0:

• Issue

Warning: Image is not Certified

ADOM: root

FAZVM64-8

Filter Mode: Data Source ID=FDTVMSTM AND Event Type=Issue

#	Date/Time	Data Source ID	Event Message	Event Type	Data Parser Name	Data Source Tags
1	2025-12-09 13:48:39	FDTVMSTM	Publicly shared sensitive SharePoint (Microsoft 365) files	Issue	FortiData Log Parser	oftp-NA,ext-alert
2	2025-12-09 13:48:35	FDTVMSTM	Sensitive financial documents are shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
3	2025-12-09 13:48:35	FDTVMSTM	Publicly shared sensitive SharePoint (Microsoft 365) files	Issue	FortiData Log Parser	oftp-NA,ext-alert
4	2025-12-09 13:48:35	FDTVMSTM	Legal documents are shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
5	2025-12-09 13:48:35	FDTVMSTM	Publicly shared legal documents	Issue	FortiData Log Parser	oftp-NA,ext-alert
6	2025-12-09 13:48:35	FDTVMSTM	Personally Identifiable Information (PII) is shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
7	2025-12-09 13:48:35	FDTVMSTM	Publicly shared Personally Identifiable Information (PII)	Issue	FortiData Log Parser	oftp-NA,ext-alert
8	2025-12-09 13:48:34	FDTVMSTM	Protected Health Information (PHI) is shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
9	2025-12-09 13:48:34	FDTVMSTM	Publicly shared Protected Health Information (PHI)	Issue	FortiData Log Parser	oftp-NA,ext-alert
10	2025-12-09 13:48:34	FDTVMSTM	Credit card numbers are shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
11	2025-12-09 13:48:34	FDTVMSTM	Cardholder Data (CHD) is shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
12	2025-12-09 13:48:34	FDTVMSTM	Publicly shared credit card numbers	Issue	FortiData Log Parser	oftp-NA,ext-alert
13	2025-12-09 13:48:34	FDTVMSTM	Publicly shared Cardholder Data (CHD)	Issue	FortiData Log Parser	oftp-NA,ext-alert
14	2025-12-09 13:48:34	FDTVMSTM	Sensitive authentication data (SAD) is shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
15	2025-12-09 13:48:34	FDTVMSTM	Source code is shared with external users	Issue	FortiData Log Parser	oftp-NA,ext-alert
16	2025-12-09 13:48:34	FDTVMSTM	Publicly shared source code references	Issue	FortiData Log Parser	oftp-NA,ext-alert

Total logs for analysis: 59 days 23 hours

1000 /Page 1 ^ 0.62 seconds

Event Details:

- Action: FortiData Log Parser
- Data Parser Name: FDTVMSTM
- Data Source ID: fdt123\_new\_sn
- Data Source Name: oft-NA,ext-alert
- Data Source Tags: FortiData
- Data Source Type: FortiData
- Data Timestamp: 2025-12-09 13:36:15
- Date/Time: 2025-12-09 13:48:39
- Time Stamp: 2025-12-09 13:48:39

Event Category: Public Exposure

Event Message: Publicly shared sensitive SharePoint (Microsoft 365) files refers to documents or data stored in SharePoint that contain confidential or sensitive information and have been made accessible to the public or external parties, intentionally or unintentionally, through sharing settings.

Raw log: itime=2025-12-09 13:48:39 epid=1 eid=1 data\_parsername=FortiData Log Parser data\_sourceid=FDTVMSTM data\_source=fdt123\_new\_sn data\_sourcetype=FortiData data\_timestamp=1765316175 event\_message=Publicly shared sensitive SharePoint (Microsoft 365) files refers to documents or data stored in SharePoint that contain confidential or sensitive information and have been made accessible to the public or external parties, intentionally or unintentionally, through sharing settings.

• Risk Record

Warning: Image is not Certified

ADOM: root

FAZVM64-8

Filter Mode: Data Source ID=FDTVMSTM AND Event Type=Risk Record

#	Date/Time	Data Source ID	Event Message
1	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: SharePoint (Microsoft 365) files containing sensitive data are shared with external users
2	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared sensitive SharePoint (Microsoft 365) files
3	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: SharePoint (Microsoft 365) files containing sensitive data are shared with external users
4	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Sensitive financial documents are shared with external users
5	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared sensitive financial documents
6	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared sensitive SharePoint (Microsoft 365) files
7	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared sensitive SharePoint (Microsoft 365) files
8	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared legal documents
9	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared Personally Identifiable Information (PII)
10	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: SharePoint (Microsoft 365) files containing sensitive data are shared with external users
11	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared sensitive SharePoint (Microsoft 365) files
12	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: SharePoint (Microsoft 365) files containing sensitive data are shared with external users
13	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Sensitive financial documents are shared with external users
14	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared sensitive financial documents
15	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: Publicly shared sensitive SharePoint (Microsoft 365) files
16	2025-12-09 13:48:35	FDTVMSTM	Risk Record scanned by policy: SharePoint (Microsoft 365) files containing sensitive data are shared with external users

Total logs for analysis: 59 days 23 hours

1000 /Page 1 ^ 1.12 seconds

Event Details:

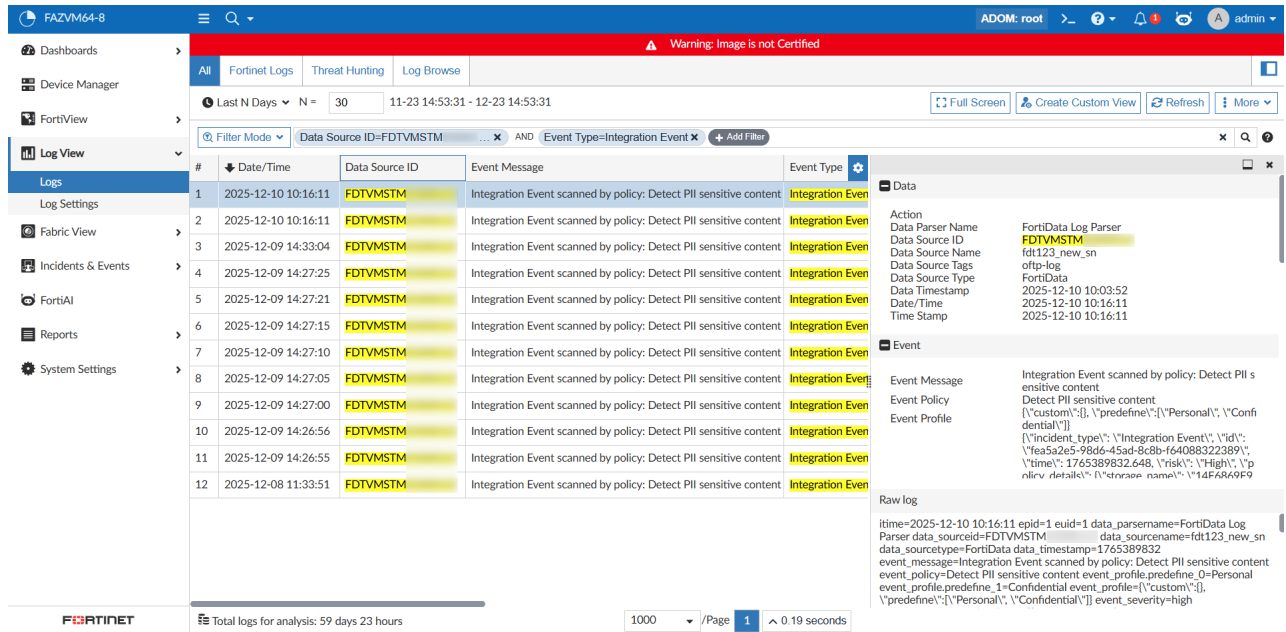
- Action: FortiData Log Parser
- Data Parser Name: FDTVMSTM
- Data Source ID: fdt123\_new\_sn
- Data Source Name: oft-NA
- Data Source Tags: FortiData
- Data Source Type: FortiData
- Data Timestamp: 2025-12-09 13:36:17
- Date/Time: 2025-12-09 13:48:35
- Time Stamp: 2025-12-09 13:48:35

Event Message: Risk Record scanned by policy: SharePoint (Microsoft 365) files containing sensitive data are shared with external users

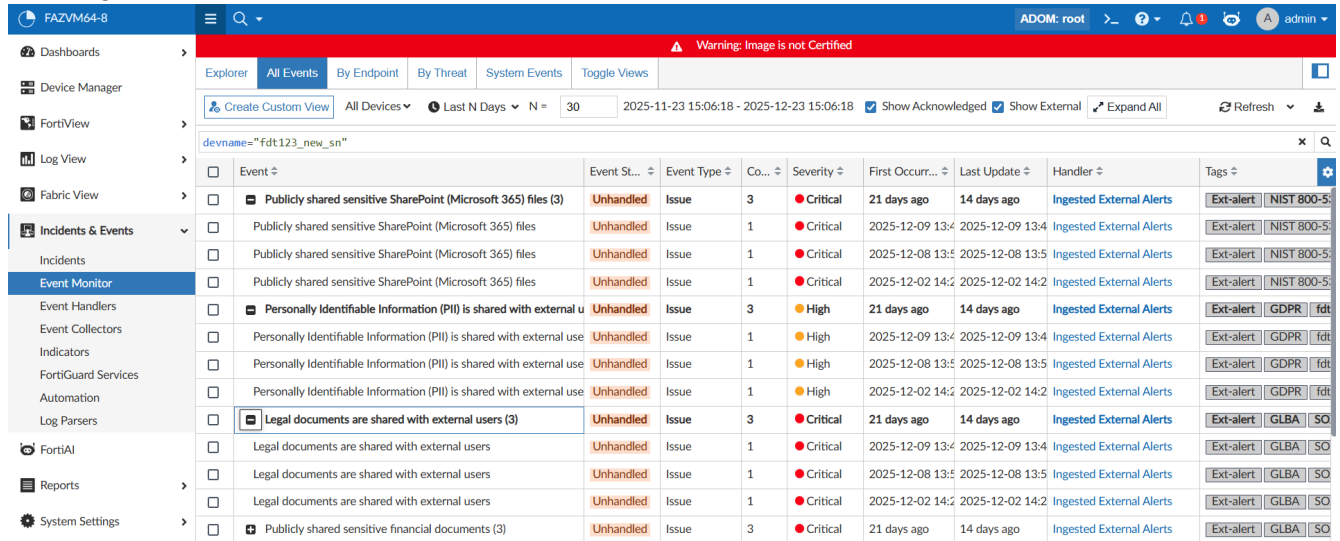
Event Policy: \[incident\_type\]: \[Risk Record\] \[id\]: \[108f2f8bb-5680-48d3-afe5-8256e5c0e2f8\] \[issue\_id\]: \[7387660e-29

Raw log: itime=2025-12-09 13:48:35 epid=1 eid=1 data\_parsername=FortiData Log Parser data\_sourceid=FDTVMSTM data\_source=fdt123\_new\_sn data\_sourcetype=FortiData data\_timestamp=1765316177 event\_message=Risk Record scanned by policy: SharePoint (Microsoft 365) files containing sensitive data are shared with external users event\_policy=SharePoint (Microsoft 365) files containing sensitive data are shared with external users

• Integration Event



The predefined *Ingested External Alerts* event handler, enabled by default, will trigger alerts from FortiData Issue logs. These alerts can be found in *Incidents & Events > Event Monitor*.



You can create custom event handlers in FortiAnalyzer to trigger alerts using the other log types from FortiData as well.

## Log Forwarding

This section lists the new features added to FortiAnalyzer for log forwarding:

- FortiAnalyzer Fluentd supports the Azure Monitor Log Ingestion API on page 36

# FortiAnalyzer Fluentd supports the Azure Monitor Log Ingestion API



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- Output profiles
- Output profile example

FortiAnalyzer Fluentd now supports the Azure Logs Ingestion API in *Output Profiles*.

## To configure the log ingestion in the Azure portal:

1. Login to your Azure portal: <https://portal.azure.com>.
2. Create an application through App registration.
3. Create a Log Analytics Workspace.
4. Create a Data Collection Endpoint (DCE).
5. Create a new custom table (Direct Ingest).
  - When creating the table, if no data collection rule exists, select *Create a new data collection rule* to create one.
  - For the required sample.json, prepare the content as `{"logtime": "2026-01-16T20:30:00Z", "message": "hello logs ingestion"}`.
  - For the transformation, use `source\n| extend TimeGenerated = todatetime(logtime)\n| project-away logtime\n`, which indicates:
    - `extend TimeGenerated = todatetime(logtime)`: add a new column named `TimeGenerated` into the table with the value as `todatetime(logtime)`. This is mandatory since the Azure Logs Ingestion API requires the column `TimeGenerated`.
    - `project-away logtime`: discard the column `logtime`.
  - When creating a custom table, you must use the `_CL` suffix. For example, instead of naming the table "apptest", you must name it "apptest\_CL".
  - Complete the App Registration in which *Tenant ID* and *Client ID* are available. You must *Create Secret* to get `Client Secret(value)` for this application.
    - Add role assignment(*Monitoring Metrics Publisher*) to link the application with the DCR.

## To configure the FortiAnalyzer Fluentd in 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:

Option	Description
<b>Name</b>	Enter a name for the output profile.
<b>Type</b>	Select <i>Azure Logs Ingestion</i> .

Option	Description														
<b>Configuration</b>	<p>Click <i>Use Default</i> to use the default Fluentd configuration. The default configuration indicates that:</p> <pre># The following six parameters are required. tenant_id #&lt;TENANT_ID&gt; client_id #&lt;CLIENT_ID&gt; client_secret #&lt;CLIENT_SECRET&gt; dce_url #&lt;DCE_URL&gt; dcr_id #&lt;DCR_ID&gt; table_name #&lt;TABLE_NAME&gt;</pre>														
<b>Field   Value   Action</b>	<p>Configure the required parameters according to your Azure portal. For example:</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td><b>TENANT_ID</b></td> <td>Enter the tenant ID for the Azure portal.</td> </tr> <tr> <td><b>CLIENT_ID</b></td> <td>Enter the client ID for the Azure portal.</td> </tr> <tr> <td><b>CLIENT_SECRET</b></td> <td>Enter the client secret for the Azure portal.</td> </tr> <tr> <td><b>DCE_URL</b></td> <td>Enter the Data Collection Endpoint URL.</td> </tr> <tr> <td><b>DCR_ID</b></td> <td>Enter the Data Collection Rule ID.</td> </tr> <tr> <td><b>TABLE_NAME</b></td> <td>Enter the custom table name from the Azure portal.</td> </tr> </tbody> </table>	Field	Value	<b>TENANT_ID</b>	Enter the tenant ID for the Azure portal.	<b>CLIENT_ID</b>	Enter the client ID for the Azure portal.	<b>CLIENT_SECRET</b>	Enter the client secret for the Azure portal.	<b>DCE_URL</b>	Enter the Data Collection Endpoint URL.	<b>DCR_ID</b>	Enter the Data Collection Rule ID.	<b>TABLE_NAME</b>	Enter the custom table name from the Azure portal.
Field	Value														
<b>TENANT_ID</b>	Enter the tenant ID for the Azure portal.														
<b>CLIENT_ID</b>	Enter the client ID for the Azure portal.														
<b>CLIENT_SECRET</b>	Enter the client secret for the Azure portal.														
<b>DCE_URL</b>	Enter the Data Collection Endpoint URL.														
<b>DCR_ID</b>	Enter the Data Collection Rule ID.														
<b>TABLE_NAME</b>	Enter the custom table name from the Azure portal.														

4. Click *Validate and Save*.
5. You can now use this Output Profile in Log Forwarding from the FortiAnalyzer. For more information about configuring Log Forwarding using an output profile, see the [FortiAnalyzer Administration Guide](#).

## Reports

This section lists the new features added to FortiAnalyzer for reports:

- [Anomaly login report on page 38](#)
- [FortiDeceptor incident report on page 42](#)
- [Shadow-AI report on page 48](#)

## Anomaly login report



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- ZTNA login alert handlers

The new *Anomaly Login Report* provides a comprehensive overview of security events involving remote users and devices accessing office resources through Zero Trust Network Access (ZTNA). The report examines user behavior, including concurrent access with multiple devices, unusual login locations or times, access to atypical resources, abnormal data transfers, and other relevant factors. Categorizing these events as security breaches or suspicious activities, the report offers valuable insights into potential threats.

This report requires FortiAuthenticator event logs in FortiAnalyzer to trigger the predefined *ZTNA Login Anomaly Detection* alert handler. For more information about this alert handler, see the [FortiAnalyzer Administration Guide](#).

The *Anomaly Login Report* is a global report, and it can be found in the Fabric Reports folder in *Reports > Report Definitions > All Reports*.

<input type="checkbox"/>	Title	Language	Cache Status	Time Period	Devices	Schedule	Origin	Config Recommendation	Output Profile	Report Owner
<input type="checkbox"/>	Application Reports									
<input type="checkbox"/>	Asset and User Reports									
<input type="checkbox"/>	Compliance Reports									
<input type="checkbox"/>	Fabric Reports									
<input checked="" type="checkbox"/>	Anomaly Login Report	English		This Week	All Devices		Built-in			
<input type="checkbox"/>	Endpoint Security Vulnerability Report	English					Built-in			
<input type="checkbox"/>	360 Protection Report	English		Previous 7 Days	All Devices		Built-in			
<input type="checkbox"/>	Bandwidth and Applications Report (SIEM)	English		Previous 7 Days	All_FortiGate		Built-in			
<input type="checkbox"/>	Fortinet Email Risk Assessment	English		Previous 7 Days	All Devices		Built-in			
<input type="checkbox"/>	FortiPortal User Summary Report	English		Previous 7 Days	All Devices		Built-in			
<input type="checkbox"/>	Security Events and Incidents Summary	English		Previous 7 Days	All_FortiGate		Built-in			
<input type="checkbox"/>	Situation Awareness Report	English		Previous 7 Days	All Devices		Built-in			
<input type="checkbox"/>	What is New Report	English		Previous 7 Days	All Devices		Built-in			
<input type="checkbox"/>	FortiADC Reports									
<input type="checkbox"/>	FortiCache Reports									
<input type="checkbox"/>	FortiClient Reports									

The report template can be found in *Reports > Report Definitions > Templates*.

Title	La...	Description	Category	Preview	Origin
Template - 360 Protection Report	en	Present a brief summary of hardware/software inventory of the FortiGate devices over a 30 day period.	System	HTML PDF	Built
Template - 360 Security Report	en	Present a brief summary report about traffic, threat, app, user, incident, compromised host and so on.	Security	HTML PDF	Built
Template - 360-Degree Security Review	en	Security review of Application Visibility and Control, Threat Detection, Data Exfiltration Detection, Endpoint Detection, P	Security	HTML PDF	Built
Template - Admin and System Events Report	en	Admin login and failed login attempts and system severity event counts.	System	HTML PDF	Built
Template - Anomaly Login Report	en	Present a brief summary of Anomaly Login activity, specifically highlighting events captured by related event handlers with	Security	HTML PDF	Built
Template - Application Risk and Control	en	Application risk, categories, bandwidth by app, web categories, vulnerability exploits, virus, botnet, adware malicious attack	Application	HTML PDF	Built
Template - Asset and Identity Report	en	Present a brief summary report on assets and their users, vulnerabilities, software installed as well as running processes.	Assets	HTML PDF	Built
Template - Bandwidth and Applications Report	en	Traffic, Bandwidth, Sessions, Destinations summaries - by users and applications	Application	HTML PDF	Built
Template - Bandwidth and Applications Report (SIEM)	en	Traffic, Bandwidth, Sessions, Destinations summaries - by users and applications	Application	HTML PDF	Built
Template - C-Suite SD-WAN Insights Report	en	Present an SD-WAN insights report which focuses on high-level key performance indicators.	System	HTML PDF	Built
Template - CIS Controls Security Rating Report	en	Present a brief summary report about CIS Controls security rating report.	Security	HTML PDF	Built
Template - Client Reputation	en	Client and user network behaviour, incidents by user, devices, threat summary.	User	HTML PDF	Built
Template - Cyber Threat Assessment	en	Cyber Threat review of Application Visibility and Control, Threat Detection, Prevention and Recommended Actions.	Security	HTML PDF	Built
Template - Cyber-Bullying Indicators Report	en	Cyber-Bullying Indicators Report.	Application	HTML PDF	Built
Template - Daily Summary Report	en	Present a brief summary report about traffic, threat, app, user, incident, compromised host and so on.	Security	HTML PDF	Built
Template - Data Loss Prevention Detailed Report	en	Violation Summary and Activity Details of Email, Web, and FTP.	Security	HTML PDF	Built

The Anomaly Login charts used for the report can be found in *Reports > Report Definitions > Chart Library*.

Name	Description	Device Type	Category	Origin
Active Traffic Users	List of active traffic users	FortiGate	Traffic	Built-in
Admin Login Summary by Date	Administrator login summary by date	FortiGate	Event	Built-in
Admin Login Summary with failed	Administrator login summary by date	FortiGate	Event	Custom
Adware Timeline	Adware timeline	FortiGate	Antivirus	Built-in
All Applications Discovered on the Network	All Applications Discovered on the N	FortiGate	Traffic	Built-in
Anomaly Login Incident Count by Severity	Anomaly Login Incident Count by Se	FortiAuthenticator	Event	Built-in
Anomaly Login Incident Count by Status	Anomaly Login Incident Count by Sta	FortiAuthenticator	Event	Built-in
Anomaly Login Incident End User	Anomaly Login Incident End User	FortiAuthenticator	Event	Built-in
Anomaly Login Incident End User List	Anomaly Login Incident End User Lis	FortiAuthenticator	Event	Built-in
Anomaly Login Incident User Attachment	Anomaly Login Incident User Attach	FortiAuthenticator	Event	Built-in
Antivirus Inspections	Antivirus Inspections	FortiGate	Antivirus	Built-in
App Categories	Application categories by bandwidth	FortiGate	Traffic	Built-in
App Categories (Pie)	Application categories by bandwidth	FortiGate	Traffic	Built-in
App Risk Control Files Analyzed by FortiCloud Sandbox	App Risk Control Files analyzed by Fi	FortiGate	Antivirus	Built-in
Application Bandwidth Usage	Application bandwidth usage details	FortiGate	Traffic	Built-in
Application Behavioral Characteristics	Application Behavioral Characteristic	FortiGate	Traffic	Built-in

The Anomaly Login macros used for the report can be found in *Reports > Report Definitions > Macro Library*.

Name	Description	Device Type	Category	Origin
00-macro	test	FortiGate	Traffic	Custom
360-Security Total Malware Detected	360-Security Total Malware Detected	FortiGate	Virus	Built-in
Affected Endpoint Count	Affected Endpoint Count	FortiGate		Built-in
Analyzed Security Event Count	Analyzed Security Event Count	FortiGate		Built-in
Anomaly Login Enduser Count	Anomaly Login Enduser Count	FortiAuthenticator	Event	Built-in
Anomaly Login Incident Count with High Risk	Anomaly Login Incident Count with High Risk	FortiAuthenticator	Event	Built-in
Anomaly Login Incident Count with Medium Risk	Anomaly Login Incident Count with Medium Risk	FortiAuthenticator	Event	Built-in
Anomaly Login Incident Endpoint Icon	Anomaly Login Incident Endpoint Icon	FortiAuthenticator	Event	Built-in
Anomaly Login Incident Enduser Icon	Anomaly Login Incident Enduser Icon	FortiAuthenticator	Event	Built-in
Anomaly Login Incident Severity Icon	Anomaly Login Incident Severity Icon	FortiAuthenticator	Event	Built-in
App Count of Self-Harm Risky Terms	App Count of Self-Harm Risky Terms	FortiGate	Application Control	Built-in
Application Category with Highest Bandwidth	Application Category with Highest Bandwidth	FortiGate	Traffic	Built-in
Application Category with Highest Session Count	Application category with the highest session count	FortiGate	Traffic	Built-in
Application Risk Malware Total Count	Application Risk Malware Total Count	FortiGate	Traffic	Built-in
Application Risk Threats Total Count	Application Risk Threats Total Count	FortiGate	Application Control	Built-in
Application Risk Total Bandwidth	Application Risk Total Bandwidth	FortiGate	Traffic	Built-in

The Anomaly Login datasets (incidentnt-Anomaly-Login) used for the report can be found in *Reports > Report Definitions > Datasets*.

Name	Device Type	Log Type	Origin
High-Risk-Application-By-Sessions	FortiGate	Traffic	Built-in
incident-Anomaly-Login-Count-by-Severity	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-Count-by-Status	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-End-User	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-End-User-Attachment	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-End-User-Count	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-End-User-List	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-Endpoint-and-Enduser-Count	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-High-Risk-Count	FortiAuthenticator	Event	Built-in
incident-Anomaly-Login-Medium-Risk-Count	FortiAuthenticator	Event	Built-in
incident-Incident-Count-by-Status	FortiGate	Application Control	Built-in
incident-Incident-Count-Timeline	FortiGate	Application Control	Built-in
Interested-Applications-by-Risk-Level	FortiGate	Traffic	Built-in
intf-Device-Rcvd-Sent-Summary	FortiGate	Event	Built-in
intf-Device-Sent-Summary	FortiGate	Event	Built-in
intf-Device-Summary	FortiGate	Event	Built-in

Below is a sample of some pages from the report in PDF format.



EXECUTIVE SUMMARY

The report provides a comprehensive overview of security events involving remote users and devices accessing office resources through Zero Trust Network Access (ZTNA). It examines user behavior, including concurrent access with multiple devices, unusual login locations or times, access to atypical resources, abnormal data transfers, and other relevant factors. Categorizing these events as security breaches or suspicious activities, the report offers valuable insights into potential threats.

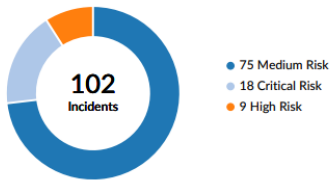
**27** Critical/High Risk Incidents

**75** Medium Risk Incidents

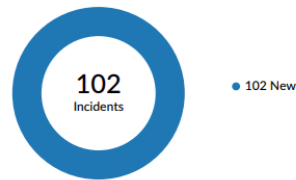
**86** Users

**38** Devices

INCIDENT SEVERITY



INCIDENT STATUS





**High Risk**  
ZTNA Brute Force Login

- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇨🇦 Canada, 🇩🇪 Germany, 🇳🇿 New Zealand  
2026-02-19 19:13:57
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇨🇦 Canada, 🇩🇪 Germany, 🇳🇿 New Zealand  
2026-02-19 19:17:15
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇩🇪 Germany, 🇨🇦 Canada, 🇳🇿 New Zealand  
2026-02-19 19:22:41
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇨🇦 Canada, 🇳🇿 New Zealand  
2026-02-19 19:25:39
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇳🇿 New Zealand, 🇩🇪 Germany, 🇨🇦 Canada  
2026-02-19 21:12:01

- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇳🇿 New Zealand, 🇨🇦 Canada, 🇩🇪 Germany  
2026-02-19 21:16:47
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇳🇿 New Zealand, 🇩🇪 Germany, 🇨🇦 Canada  
2026-02-19 21:22:11
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇩🇪 Germany, 🇨🇦 Canada  
2026-02-19 21:26:05
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇳🇿 New Zealand, 🇩🇪 Germany, 🇺🇸 United States  
2026-02-19 22:08:49
- **Authentication Failed from Multiple Geo Locations**  
Authentication failed from multiple geo locations for user: [redacted]  
🇳🇿 New Zealand, 🇩🇪 Germany, 🇺🇸 United States  
2026-02-19 22:11:49

**High Risk**  
Anomaly Login Detection

- **Successful Authentication from Multiple Geo Locations**  
Suspicious successful authentication from multiple geo locations for user: [redacted]  
🇳🇿 New Zealand: Auckland, 🇮🇳 India: Bangalore  
2026-02-19 18:26:41
- **Successful Authentication from Multiple Geo Locations**  
Suspicious successful authentication from multiple geo locations for user: [redacted]  
🇺🇸 United States: Miami, 🇨🇦 Canada: Vancouver, 🇳🇿 New Zealand: Auckland  
2026-02-19 19:31:17

page 2 of 31

## FortiDeceptor incident report



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- Using the template - FortiDeceptor incident report

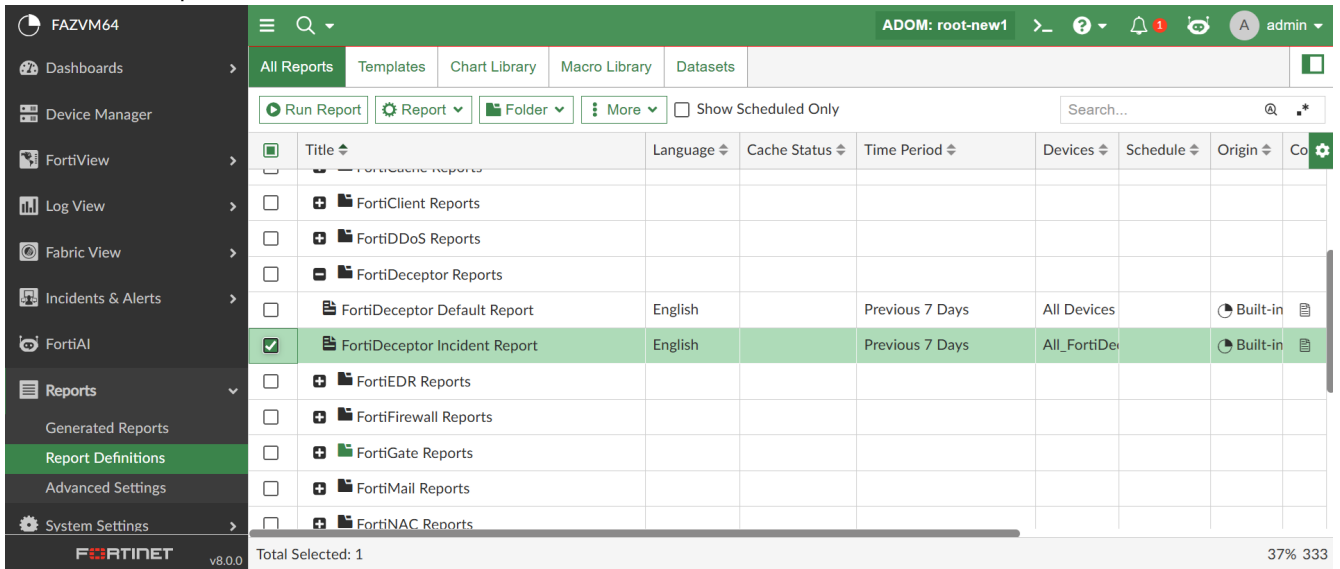
The new *FortiDeceptor Incident Report* lists *Critical* and *High* risk incidents triggered by an alert handler. The report includes the attacker IP and the victim IP, user, port, incident ID, and more so for SOC analysts to use the report effectively for incident triage and response.

This report requires FortiDeceptor logs in FortiAnalyzer to trigger the predefined *Default-FDC-Honey-Pot-Detection* alert handler. This alert handler is disabled by default, and it must be enabled in *Incidents & Alerts >*

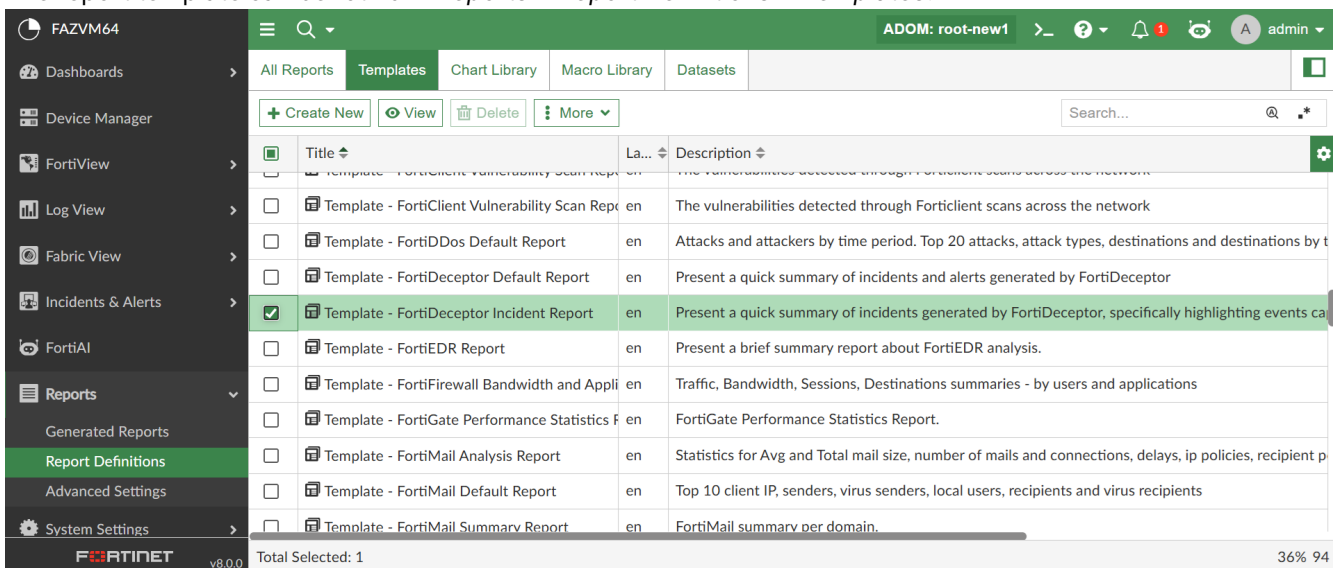
Alert Handlers.

Incidents triggered by the alert handler can be found in *Incidents & Alerts > Incidents*. The *Name* of the related incidents begin with *FDC-Honey-Pot-Detection*.

The report can be found in the FortiDeceptor Reports folder in *Reports > Report Definitions > All Reports*. It is an ADOM-level report.



The report template can be found in *Reports > Report Definitions > Templates*.



The FortiDeceptor charts used for the report can be found in *Reports > Report Definitions > Chart Library*.

Name	Description	Device Type	Category	Origin
FortiDeceptor-FDC Incident Attachment	FDC Incident Attachment	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor Incident Count by Status	FortiDeceptor Incident Count by Status	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor Incident Count by User Status	FortiDeceptor Incident Count by User Status	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor Incident High Risk Attacker and Victims List	FortiDeceptor Incident High Risk Attacker and Victims List	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor Incident Top Attacker IP	FortiDeceptor Incident Top Attacker IP	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor Incident Top Victim IP	FortiDeceptor Incident Top Victim IP	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor Medium Risk Incident List	FortiDeceptor Medium Risk Incident List	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor-Top Attack Tools Based On IPS Alerts	Top 10 Attack Tools Based On IPS Alerts	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor-Top Attacker IPs Based On IPS Alerts	Top 10 Attacker IPs Based On IPS Alerts	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor-Top Attacker IPs By Incidents	Top 10 Attacker IPs by Incidents	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor-Top Failed Login By Username	Top 10 Failed Login by Username	FortiDeceptor	Event	Built-in
FortiDeceptor-FortiDeceptor-Top Malicious Files By Incidents	Top 10 Malicious Files by Incidents	FortiDeceptor	Event	Built-in

Total Selected: 6

The FortiDeceptor macros used for the report can be found in *Reports > Report Definitions > Macro Library*.

Name	Description	Device Type	Category
FortiDeceptor-FortiDeceptor Incident Count with High Risk	FortiDeceptor Incident Count with High Risk	FortiDeceptor	Event
FortiDeceptor-FortiDeceptor Incident Count with Medium Risk	FortiDeceptor Incident Count with Medium Risk	FortiDeceptor	Event
FortiDeceptor-FortiDeceptor Incident Total Count	FortiDeceptor Incident Total Count	FortiDeceptor	Event
FortiDeceptor-FortiDeceptor Incident Total Count with Closed Status	FortiDeceptor Incident Total Count with Closed Status	FortiDeceptor	Event

4/369

The FortiDeceptor datasets (fdc-Incident) used for the report can be found in *Reports > Report Definitions > Datasets*.

Name	Device Type	Log Type	Origin
fdc-Incident-Attachment	FortiDeceptor	Event	Built-in
fdc-Incident-Attachment-List	FortiDeceptor	Event	Built-in
fdc-Incident-Attacker-And-Victim-Info	FortiDeceptor	Event	Built-in
fdc-Incident-Count-by-Status	FortiDeceptor	Event	Built-in
fdc-Incident-High-Risk-Attacker-And-Victims-List	FortiDeceptor	Event	Built-in
fdc-Incident-High-Risk-Count	FortiDeceptor	Event	Built-in
fdc-Incident-List-Per-Attacker	FortiDeceptor	Event	Built-in
fdc-Incident-Medium-Risk-Count	FortiDeceptor	Event	Built-in
fdc-Incident-Top-Attacker-IP	FortiDeceptor	Event	Built-in
fdc-Incident-Top-Victim-IP	FortiDeceptor	Event	Built-in
fdc-Incident-Total-Count	FortiDeceptor	Event	Built-in
fdc-Incident-Total-Count-with-Closed-Status	FortiDeceptor	Event	Built-in

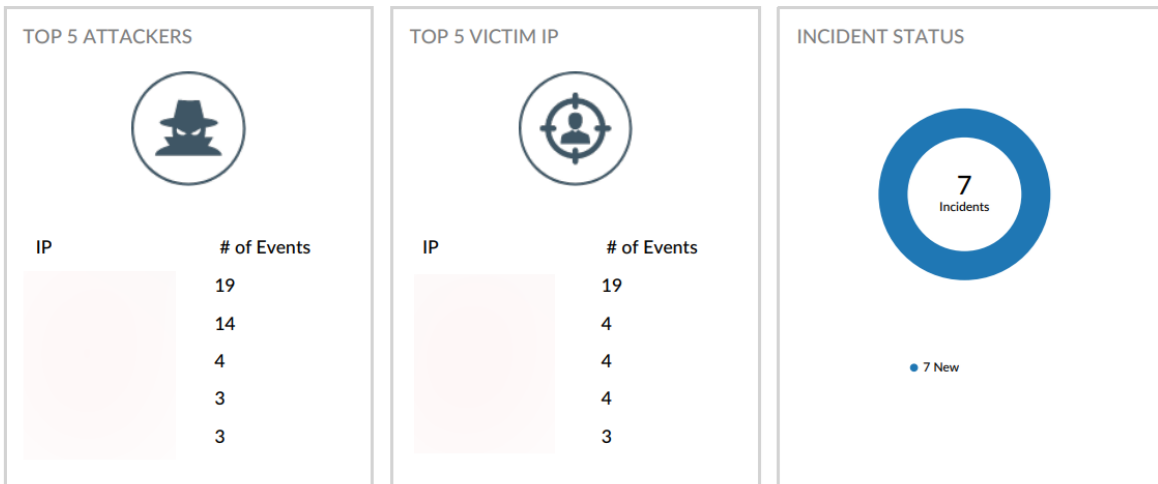
Below is a sample of some pages from the report in PDF format.



**EXECUTIVE SUMMARY**

FortiDeceptor uses deception technology to strengthen breach protection by detecting and stopping attacks from internal and external sources before they cause harm. This report details incidents, including attacker and victim information, incident specifics, and investigation results.

**0** Critical/High Risk Incidents      **7** Medium Risk Incidents      **7** Total # of Incidents      **0** Closed





INCIDENTS

**Attacker**

User: [Redacted]  
IP: [Redacted]  
Port: **NA**

**1** Incidents 1 New


**Incident ID: IN00000124** Medium Risk 2026-02-20 16:02:19 New

Victim IP: [Redacted] Assign To: [Redacted]  
Victim Port: **NA** Description: [Redacted]  
Detected By: [Redacted]-FDC

- **Attack detected by FDC**  
attackerip: [Redacted]  
2026-02-20 16:02:17
- **Port\_Scan**  
137  
2026-02-20 16:02:33
- **Port\_Scan**  
137  
2026-02-20 16:04:57
- **Port\_Scan**  
137  
2026-02-20 16:07:16

### FortiDeceptor Incident Report

Data Range: 2026-02-15 00:00:00 2026-02-20 16:08:39PST



#### Attacker

User: [Redacted]  
IP: [Redacted]  
Port: NA

1 Incidents

1 New

**Incident ID: IN00000120** **Medium Risk** **2026-02-20 16:01:35** **New**

Victim IP: [Redacted] Assign To: [Redacted]  
Victim Port: NA Description: [Redacted]  
Detected By: [Redacted] FDC

- **Attack detected by FDC**  
attackerip: [Redacted]  
2026-02-20 16:01:35
- **Port\_Scan 3702**  
2026-02-20 16:01:49
- **Port\_Scan 3702**  
2026-02-20 16:02:29
- **Port\_Scan 3702**  
2026-02-20 16:02:48
- **Port\_Scan 3702**  
2026-02-20 16:02:50
- **Port\_Scan 3702**  
2026-02-20 16:03:49

- **Port\_Scan 3702**  
2026-02-20 16:04:51
- **Port\_Scan 3702**  
2026-02-20 16:05:53
- **Port\_Scan 3702**  
2026-02-20 16:06:29
- **Port\_Scan 3702**  
2026-02-20 16:06:54
- **Port\_Scan 3702**  
2026-02-20 16:06:56
- **Port\_Scan 3702**  
2026-02-20 16:07:53

page 3 of 8

## Shadow-AI report

The *Shadow-AI Report* is a new report template for FortiOS GenAI detections coming from Application Control (app-ctrl), DLP (dlp), Web Filter (webfilter), and DNS (dns) logs. This report highlights organizational AI adoption, with a focus on sanctioned versus unsanctioned usage, top applications, and user activity.

The *Shadow-AI Report* can be found in *Reports > Report Definitions > All Reports*.

Title	Language	Cache Status	Time Period	Devices	Schedule	Origin	Co
Fabric Reports							
Anomaly Login Report	English					Built-in	
Endpoint Security Vulnerability Report	English					Built-in	
360 Protection Report	English		Previous 7 Days	All Devices		Built-in	
Bandwidth and Applications Report (SIEM)	English		Previous 7 Days	All_FortiGat		Built-in	
Fortinet Email Risk Assessment	English		Previous 7 Days	All Devices		Built-in	
FortiPortal User Summary Report	English		Previous 7 Days	All Devices		Built-in	
Security Events and Incidents Summary	English		Previous 7 Days	All_FortiGat		Built-in	
<b>Shadow-AI Report</b>	English		This Month	All Devices		Built-in	
Situation Awareness Report	English		Previous 7 Days	All Devices		Built-in	

The report template can be found in *Reports > Report Definitions > Templates*.

Title	La...	Description
Template - Security Events and Incidents Summ...	en	Present a brief summary of the events/incidents collected.
Template - Self-Harm and Risk Indicators Rep...	en	Self-Harm and Risk Indicators Report.
Template - Shadow IT Report	en	Present a brief summary report about cloud-based services.
<b>Template - Shadow-AI Report</b>	en	This report highlights organizational AI adoption, with a focus on sanctioned versus unsanctioned us...
Template - Situation Awareness Rep...	en	...e awareness of your current security posture, and allow for a better understanding of the 'big p...
Template - SOC 2 Compliance Repo...	en	...t a brief summary report about SOC 2 Compliance Report.
Template - SOC Incident Report	en	...t a brief summary of SOC Incidents.
Template - Social Media Usage Report	en	Social Media Usage Report.
Template - Threat Report	en	Malware, Botnets - detected, victims and sources. Intrusions detected, sources, blocked severity and...
Template - Throughput Utilization Billing by C...	en	Interface Throughput Utilization Billing by Device and Interface Report.
Template - Throughput Utilization Billing Rep...	en	Interface Throughput Utilization Billing Report.

The datasets (*shadowai*) used for the report can be found in *Reports > Report Definitions > Datasets*.

Name	Device Type	Log Type	Origin
<b>shadowai</b> -Adoption-Growth-Trend	Fabric	Normalized	Built-in
<b>shadowai</b> -AI-App-Count	Fabric	Normalized	Built-in
<b>shadowai</b> -AI-Use-Case	Fabric	Normalized	Built-in
<b>shadowai</b> -AI-Use-Case-By-App-Sanction-Status	Fabric	Normalized	Built-in
<b>shadowai</b> -Top-AI-App-User-By-Dlp	Fabric	Normalized	Built-in
<b>shadowai</b> -Top-Sanctioned-AI-App-By-User	Fabric	Normalized	Built-in
<b>shadowai</b> -Top-Unsanctioned-AI-App-By-User	Fabric	Normalized	Built-in
<b>shadowai</b> -Top-Unsanctioned-AI-App-User-By-Usage	Fabric	Normalized	Built-in

The charts used for the report can be found in *Reports > Report Definitions > Chart Library*.

Name	Description	Device Type	Category
Security Rating SOC 2 Sub Compliance Failed Statistics Recommendation	Security Rating SOC 2 Sub Compliance Failed St	FortiGate	Normalized
SIEM-AI Applications Adoption Growth Trend	AI Applications Adoption Growth Trend	Fabric	Normalized
SIEM-Top 5 AI Application Use Cases	Top 5 AI Application Use Cases	Fabric	Normalized
SIEM-Top 5 AI Application Use Cases By App Sanction Status	Top 5 AI Application Use Cases By App Sanction	Fabric	Normalized
SIEM-Top 5 AI Application Users By DLP Incident	Top 5 AI Application Users By DLP Incident	Fabric	Normalized
SIEM-Top 5 Sanctioned AI Applications By User	Top 5 Sanctioned AI Applications By User	Fabric	Normalized
SIEM-Top 5 Unsanctioned AI Application Users By Usage	Top 5 Unsanctioned AI Application Users By Usa	Fabric	Normalized
SIEM-Top 5 Unsanctioned AI Applications By User	Top 5 Unsanctioned AI Applications By User	Fabric	Normalized
SIEM-Total Number of AI Applications Detected	Total Number of AI Applications Detected	Fabric	Normalized
Top 10 Botnet by Domain	Top 10 Botnet by Domain	FortiGate	DNS

Below is a brief sample of the report in PDF format.

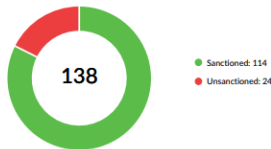


**EXECUTIVE SUMMARY**

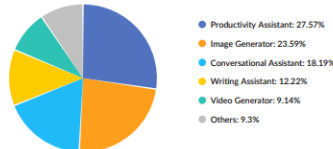
This report highlights organizational AI adoption, with a focus on sanctioned versus unsanctioned usage, top applications, and user activity. The analysis identifies the most widely used apps, key users driving adoption, and potential risks where sensitive data may be involved. Trends show overall growth in AI usage, compliance gaps between sanctioned and non-compliant apps, and risk exposure by application type. These insights support stronger governance, policy alignment, and risk mitigation.

**GEN AI APPLICATION INVENTORY**

TOTAL NUMBER OF AI APPLICATIONS DETECTED



TOP AI USE CASES



**TOP AI APPLICATIONS**

**TOP 5 AI APPLICATIONS (UNSANCTIONED)**

Application	Use Case	Top Risk Level	# of Users
Slidesgo	Productivity Assistant	Medium	2
VanceAI	Image Generator	Medium	2
HARPA.AI	Conversational Assistant	Medium	2
ThinkAny	Conversational Assistant	Medium	2
Speechmatics	Audio Generator	Medium	2



TOP 5 AI APPLICATIONS (SANCTIONED)

Application	Use Case	Top Risk Level	# of Users
Google.Gemini	Conversational Assistant	Info	5
OpenAI.ChatGPT	Conversational Assistant	Info	4
Canva	Image Generator	Medium	3
CapCut	Video Generator	Medium	3
DeepL	Productivity Assistant	Info	3

TOP 5 USERS BY AI USAGE (UNSANCTIONED)

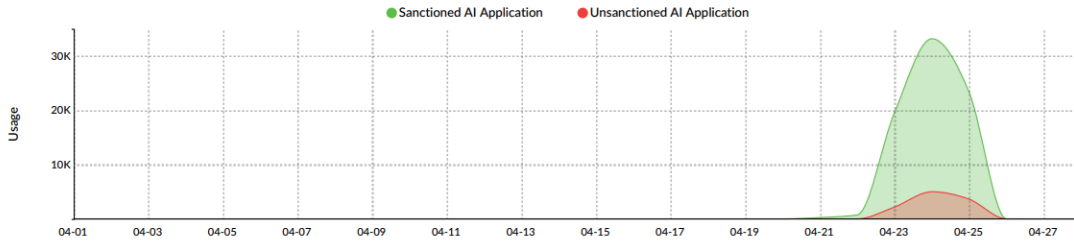
User	Most Used Application	Application Access	Detection Source(s)	Top Risk Level
user6	Grammarly	7,854	Application Control	Medium
user5	Grammarly	2,766	Application Control	Medium
not_me	DeepL	219	Application Control	Medium

TOP 5 USERS BY DATA LOSS PREVENTION INCIDENTS

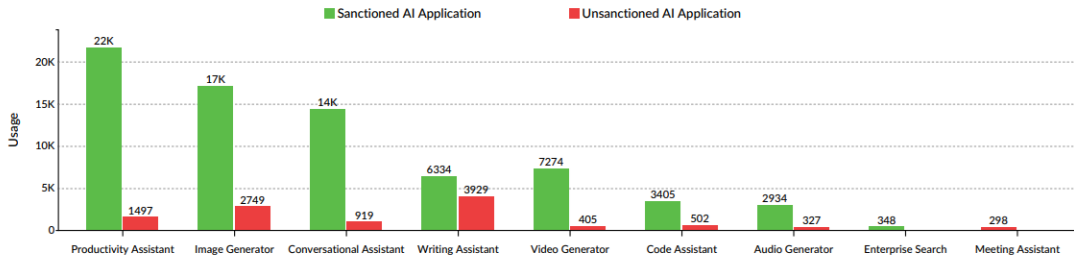
No matching log data for this report



ADOPTION GROWTH TREND



AI APPLICATION USAGE BY TYPE



# FortiAI

This section lists the new features added to FortiAnalyzer for FortiAI:

- FortiAI alert triage agent on page 53
- FortiAI threat posture timeline on page 55

## FortiAI alert triage agent



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- Alert triage agent

The new *Triage Agent* leverages agentic AI to support SOC analysts in triaging alerts and performing next steps from within the FortiAnalyzer GUI. The goal is to reduce investigation time, enhance correlation accuracy, and give customers immediate awareness without manual log searching or cross-device analysis.

### To use the alert triage agent:

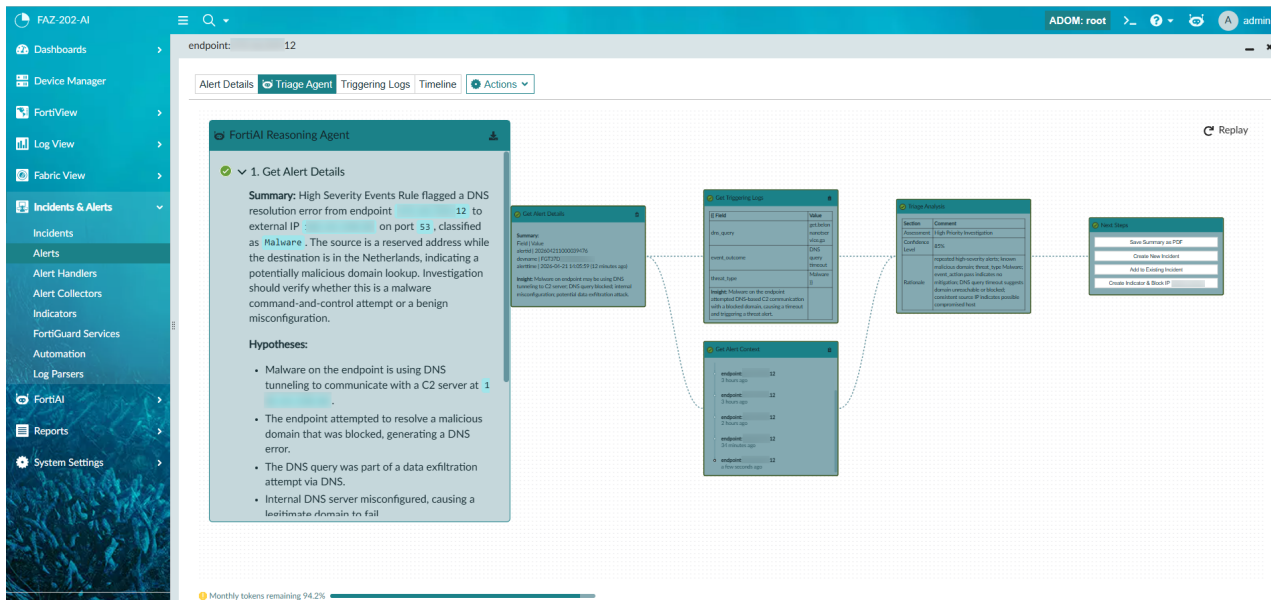
1. Go to *Incidents & Alerts > Alerts*.
2. Right-click an alert and, from the shortcut menu, click *Details*.

Severity	Last Occurred	Alert	Source	Target	User	Details	Device
High	9 minutes ago	endpoint: 12				endpoint:	FGT37
High	9 minutes ago	endpoint:172.16.76.204				endpoint:	FG101E
High	9 minutes ago	endpoint:				endpoint:	FG101E
High	9 minutes ago	endpoint:				endpoint:	FG101E
High	9 minutes ago	endpoint:				endpoint:	FG101E
High	9 minutes ago	endpoint:				endpoint:	FG101E
High	9 minutes ago	endpoint:				endpoint:	FG101E
High	9 minutes ago	endpoint:				endpoint:	FG101E
High	9 minutes ago	endpoint:				endpoint:	0% 50 101E

Alternatively, you can double-click the alert to open the Alert details.

3. In the Alert details, go to the *Triage Agent* tab.
4. Wait for the *FortiAI Reasoning Agent* to finish the analysis, including:

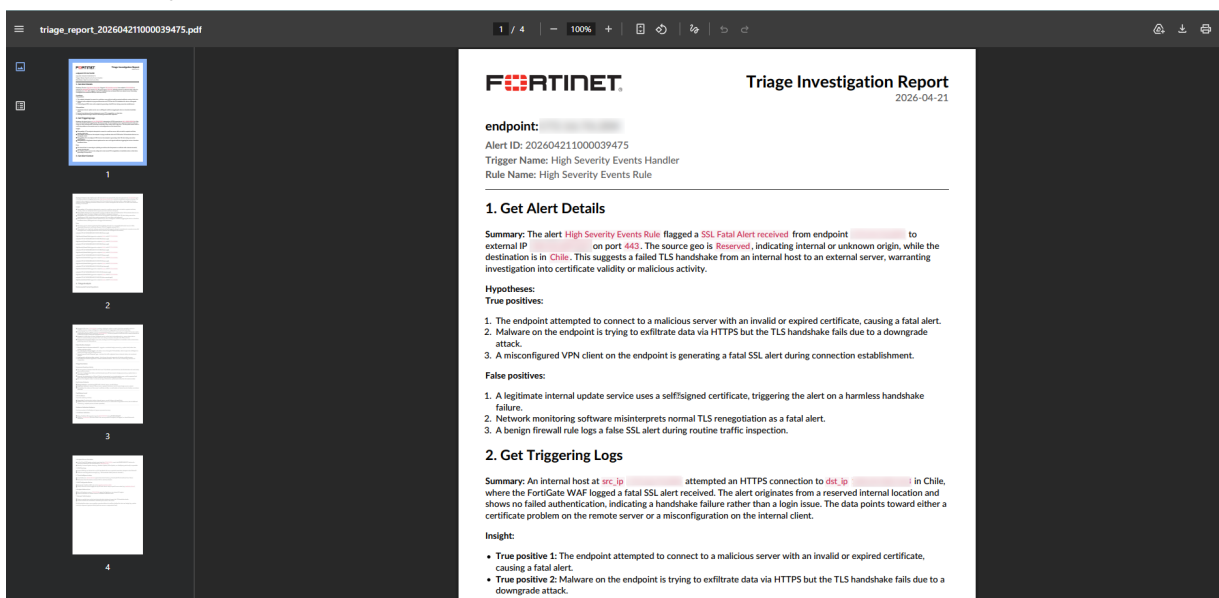
- *Get Alert Details*
- *Get Triggering Logs*
- *Get Entity Details*
- *Get Alert Context*
- *Triage Analysis*
- *Next Steps*



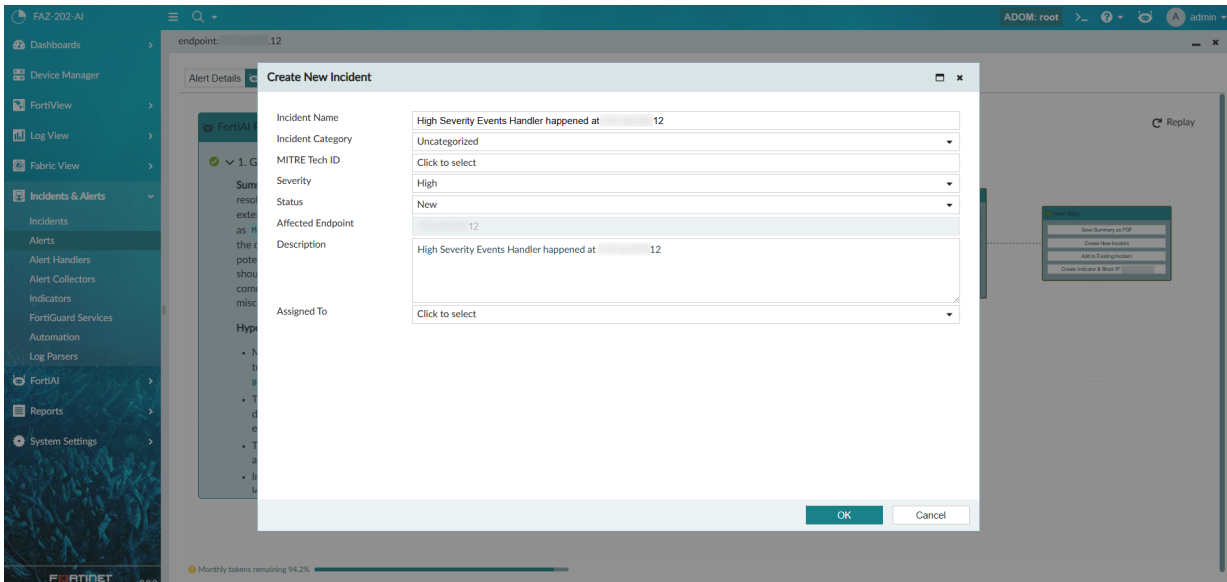
5. Review the AI reasoning by clicking on the steps within the *FortiAI Reasoning Agent* window.
6. From the *Next Steps* window, select the next step to perform on the alert.

For example:

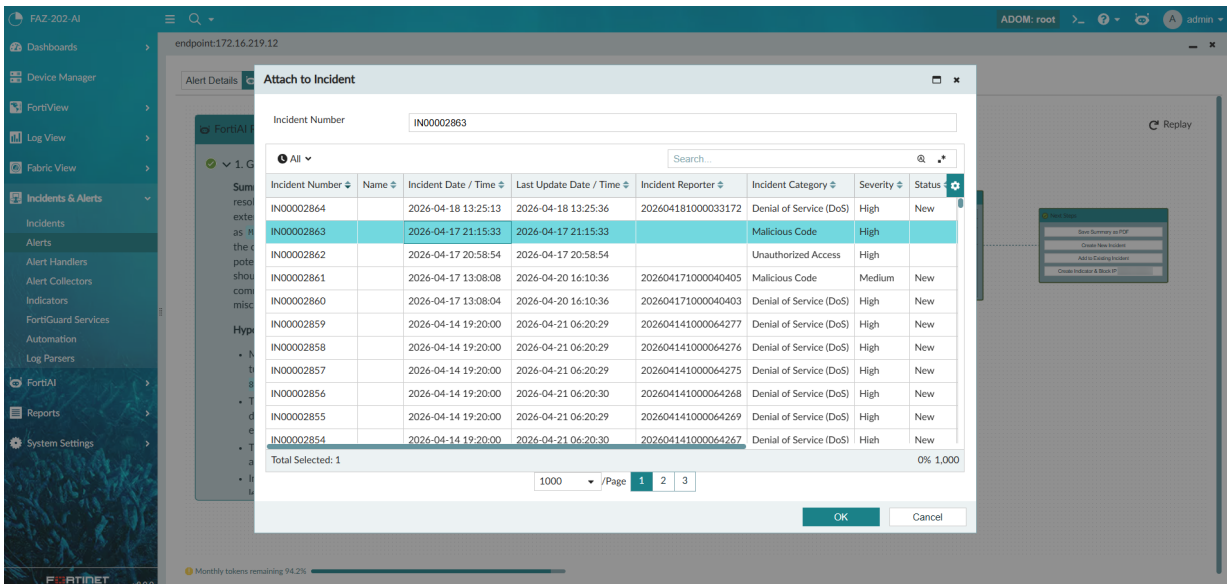
- *Save Summary as PDF*



- *Create New Incident*



- Add to Existing Incident



Other next step actions can include *Suppress Alert* and *Create Indicator & Block IP*, depending on recommendations from the agent and available connectors.

## FortiAI threat posture timeline



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- FortiAI threat posture timeline

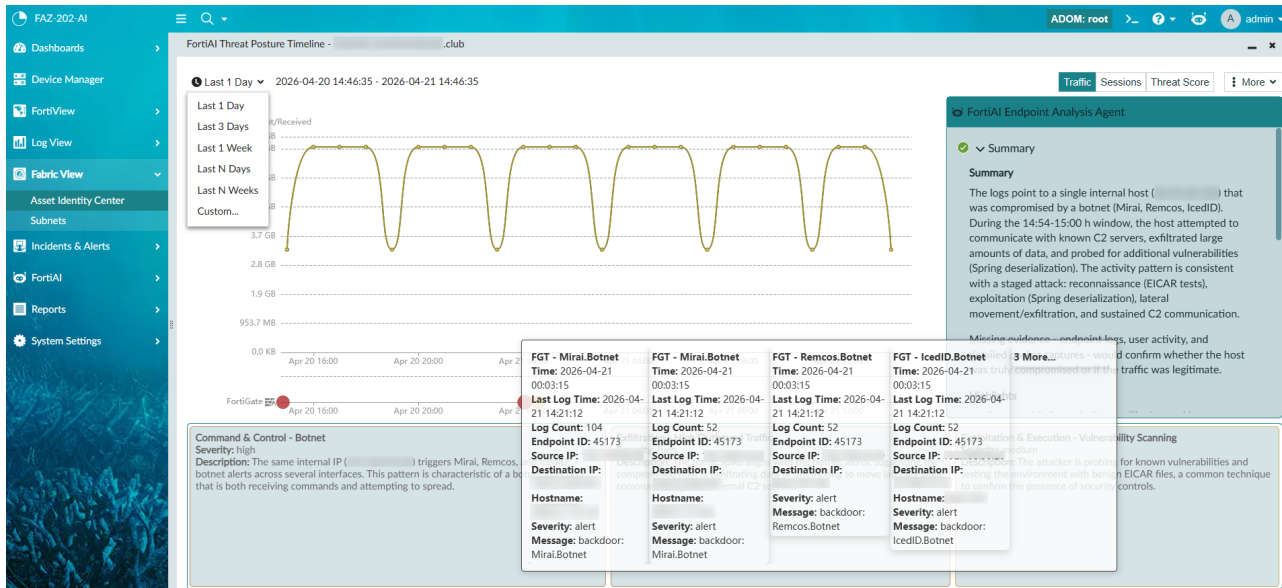
The new FortiAI Threat Posture Timeline provides an automated, consolidated security assessment for any asset or user identity. By aggregating UTM logs, alerts, incidents, and behavioral indicators from multiple sources (FortiGate, FortiClient, FortiMail, FortiAuthenticator), the system uses AI to determine the current threat posture, detect developing risks, and surface contextual insights.

### To use the FortiAI threat posture timeline:

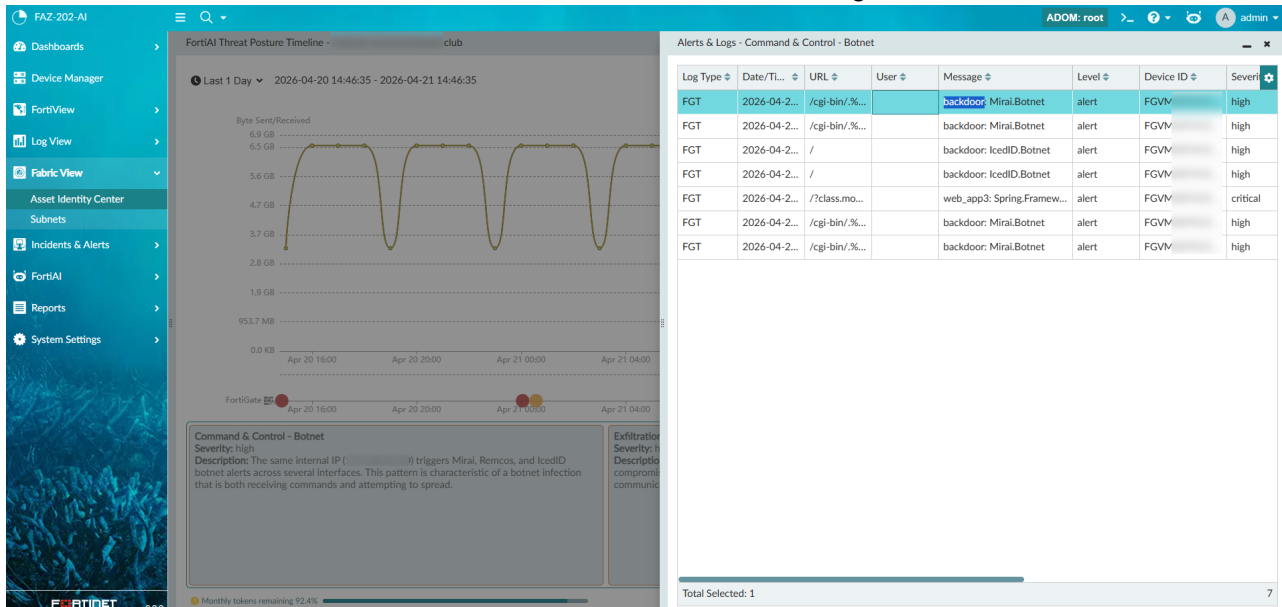
1. In the FortiAnalyzer GUI, go to *Fabric View > Asset Identity Center > Asset Identity List*.
2. Right-click an endpoint and, from the shortcut menu, select *Open FortiAI Threat Posture Timeline*.

Alternatively, open the endpoint details and click *Threat Posture Timeline*.

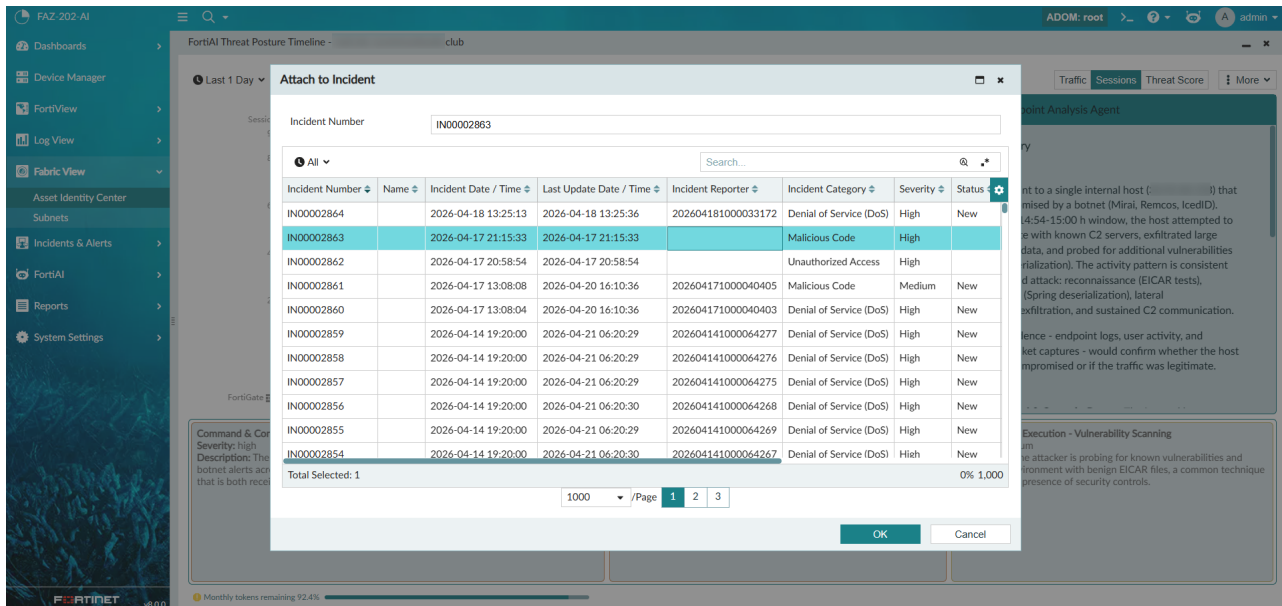
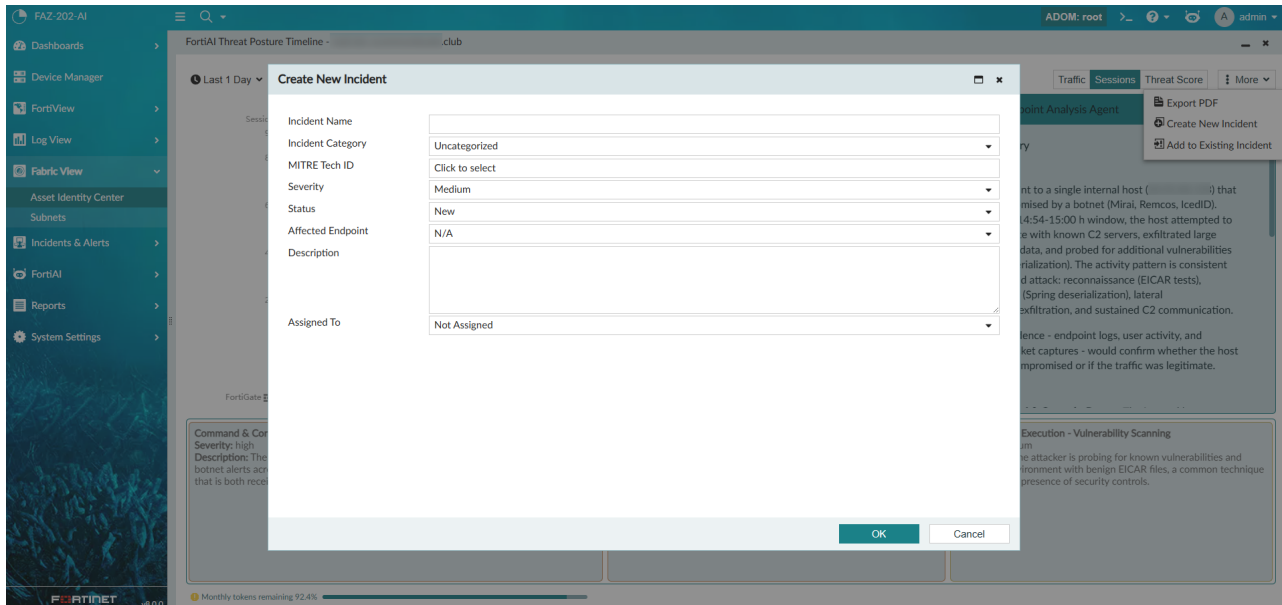
3. Wait for AI Agent analysis to finish. Review the analysis result in the *FortiAI Endpoint Analysis Agent* pane. The endpoint threats are highlighted at the bottom, below the timeline.



4. Mouse over the timeline and click areas to view the related alerts and logs.



5. From the More dropdown, you can proceed with next steps, such as exporting the PDF to share with other SOC analysts, creating a new incident, or adding to an existing incident.



# System

This section lists the new features added to FortiAnalyzer for system settings:

- [Others on page 59](#)
- [FortiAnalyzer Fabric on page 68](#)

## Others

This section lists the new features added to FortiAnalyzer for other features relating to system settings:

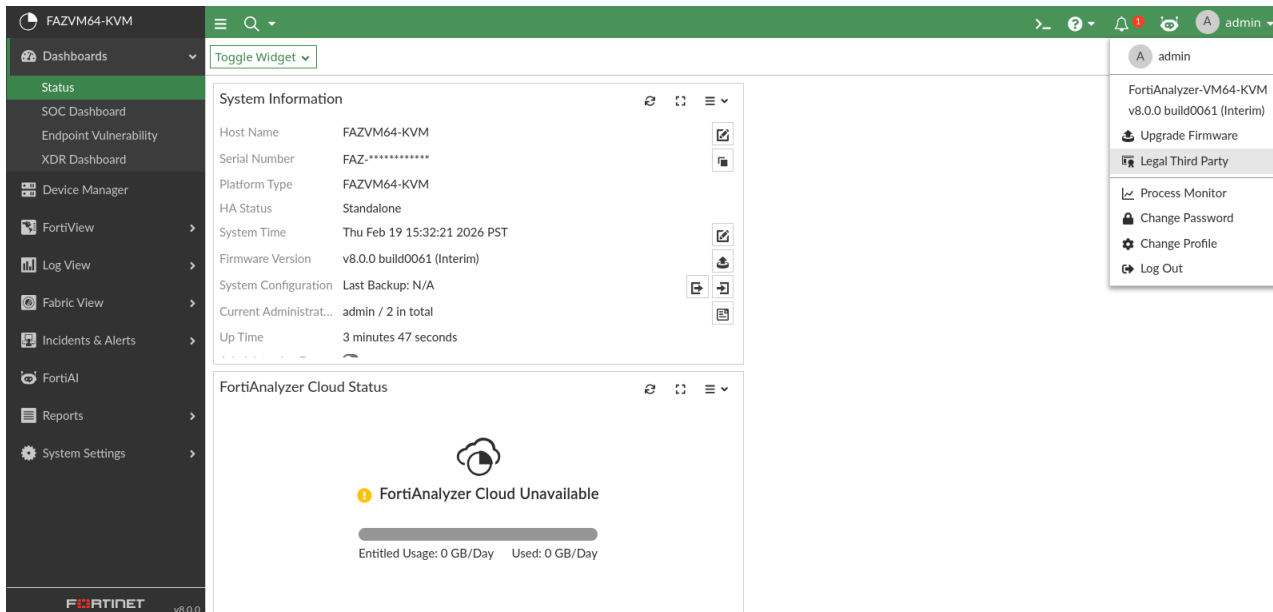
- [Legal third party disclosure panel on page 59](#)
- [Custom session labels in FortiAnalyzer event logs on page 61](#)
- [SAML SSO supports SHA-256 and SHA-512 for both IdP and SP on page 65](#)
- [Time-base retention is configurable for the task monitor and event log on page 68](#)

## Legal third party disclosure panel

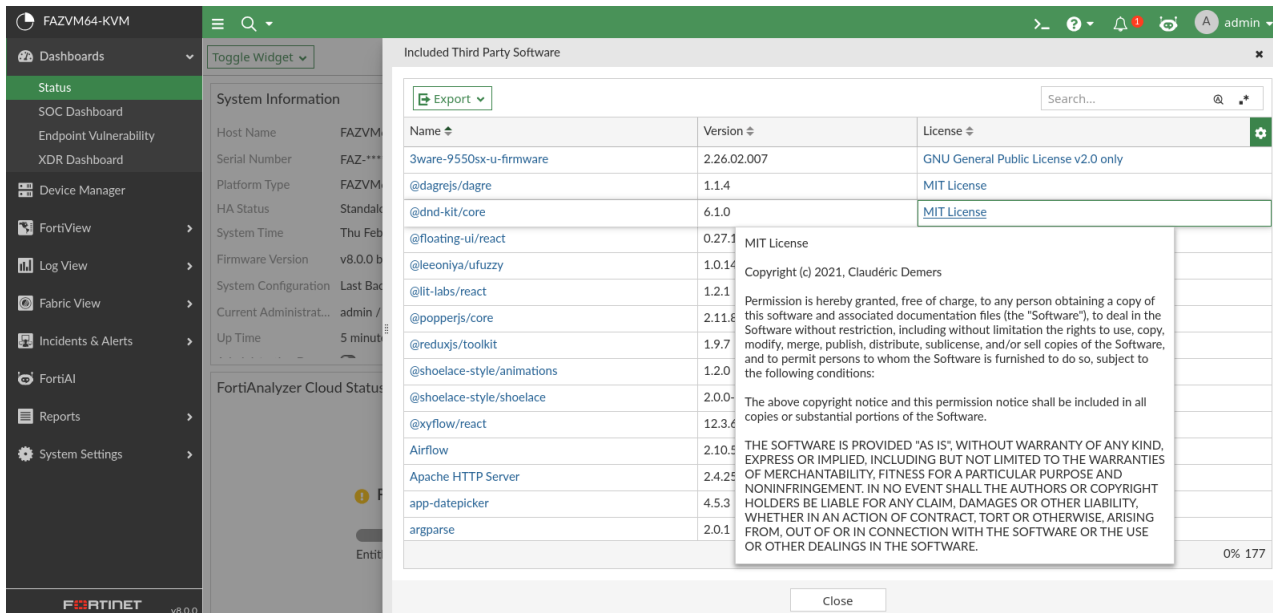
A Legal Third Party panel is added to the GUI, providing a searchable and exportable list of all third-party software used in FortiAnalyzer, along with their required licenses, license terms, and version information. This centralizes all third-party licensing details in one single, easily accessible location.

**To access and use the third-party software list:**

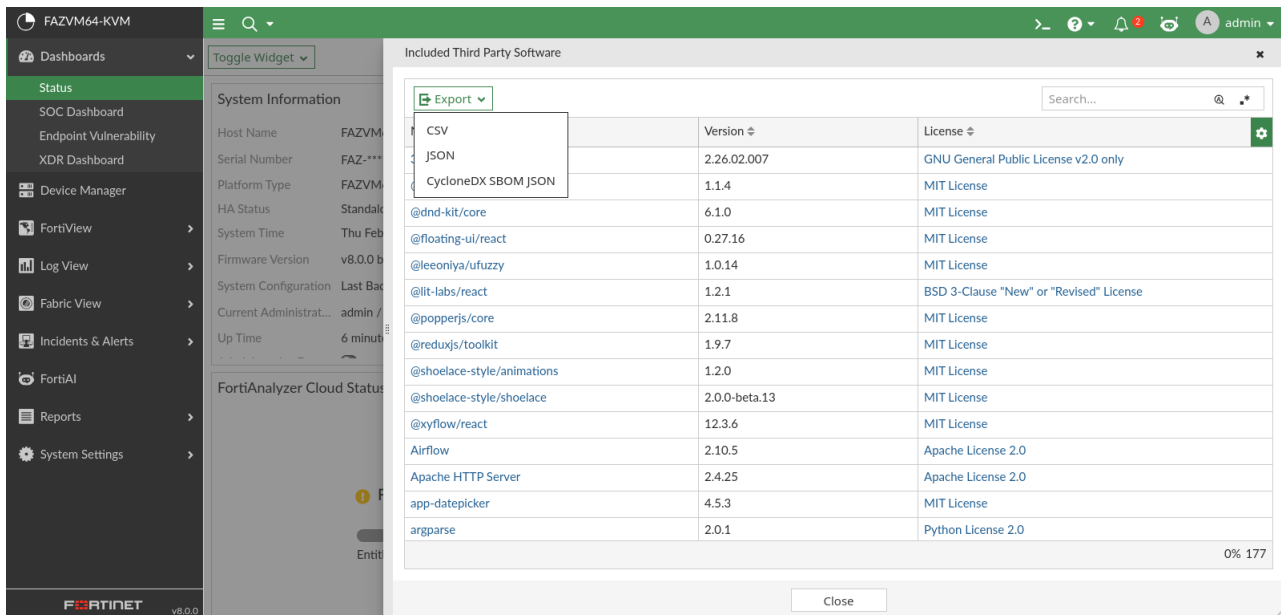
1. Select the *user name* > *System* > *Legal Third Party* to open the *Included Third Party Software* list.



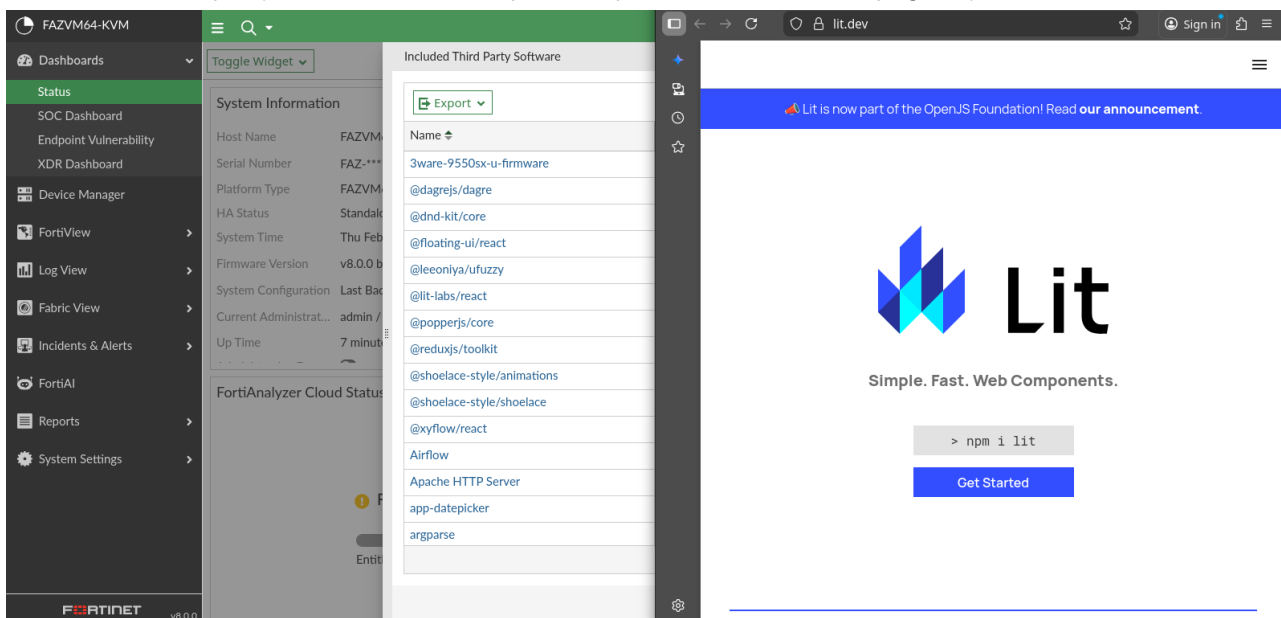
2. Hover over the *License* terms field to display additional information about the license terms.



3. Click *Export* to export the list in the CSV, JSON, or CycloneDX SBOM JSON format.



- Click on the third party software name to open that product's information page in your browser.



## Custom session labels in FortiAnalyzer event logs

FortiAnalyzer supports the ability to set custom session labels.

When a custom session label is set, all actions performed by the administrator during that session will be tagged with the session label in the *Event Log*.

The custom session label feature can be enabled using the FortiAnalyzer CLI. By default, this feature is disabled.

When enabled, you can set the session label mode as one of the following options:

- **Changeable:** The custom session label can be changed during an active session (default).
- **Unique per-session:** After a custom session label has been set, it cannot be changed until the session is terminated.



When custom session labels are enabled, it is mandatory for an administrator to set a custom session label.

Unique session labels are not enforced, which means it is possible to have multiple sessions with the same session label.

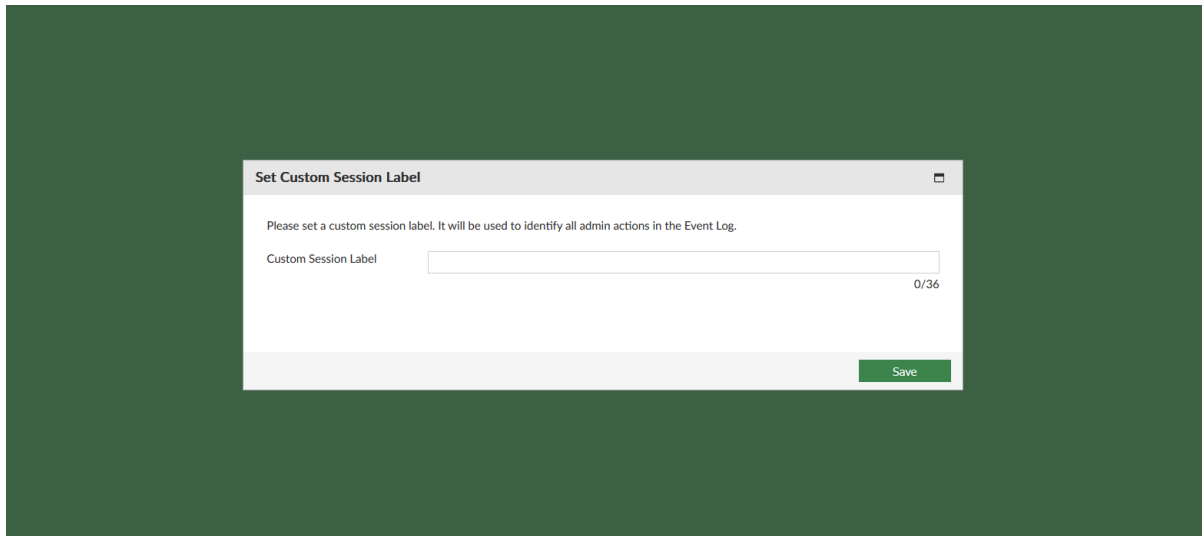
### To use custom session labels:

1. Enable custom session labels in the FortiAnalyzer CLI:

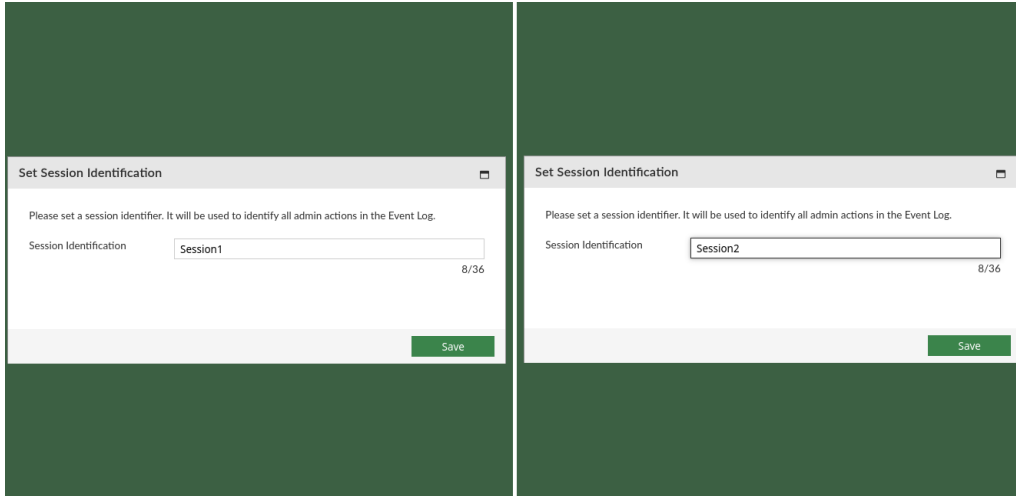
```
config system admin setting
    set custom-session-label enable
    set custom-session-label-mode {changeable | unique-per-session}
end
```

2. Log in to the FortiAnalyzer GUI.

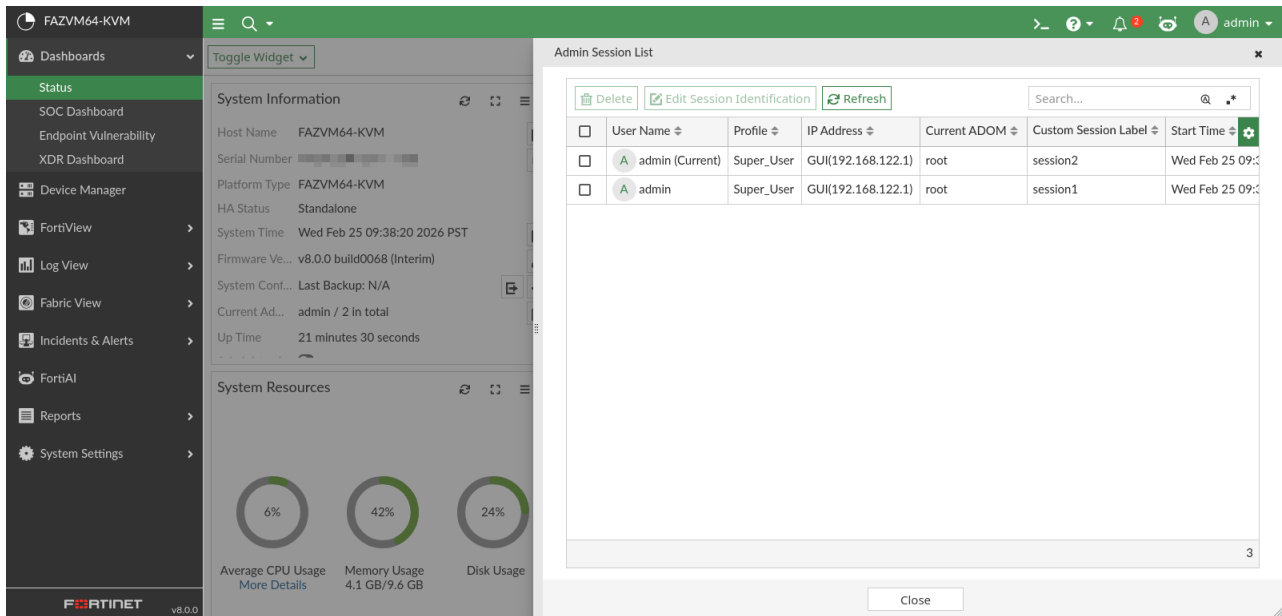
Administrators will see a *Set Custom Session Label* dialog after successfully logging in to FortiAnalyzer.



3. Enter your login credentials and enter a custom session label, then click *Login*. Custom session labels can be up to 36 characters in length. When there are multiple logins from the same administrator, different custom session labels can be used to distinguish the sessions.



- View a list of active sessions by going to *Dashboard* and clicking on the *Current Session List* icon in the *System Information* widget. The custom session labels for active users are displayed.



- Go to *System Settings* > *Event Logs* and review the Custom Session ID column to see the session label associated with each event.

#	Date/Time	Device ID	ADOM	Sub Type	User	Message	Operation	Performed ...	Changes	Custom Session Label
1	2026-02-25 0		n/a	fortism	n/a	[FORTISM Violation: domain=	open_r	/data/.uid.bi	open_r on /da	
2	2026-02-25 0		n/a	fortism	n/a	[FORTISM Violation: domain=	open_r	/data/.uid.bi	open_r on /da	
3	2026-02-25 0		root	dvm	admin		Successfully lc	root	'admin' succes	session1
4	2026-02-25 0		root	system	admin	User 'admin' with profile 'Sup	login	GUI(192.168.	'admin' login a	session1
5	2026-02-25 0			system	system	System performance status: li	Perf stats	Local system	Show system i	
6	2026-02-25 0		n/a	fortism	n/a	[FORTISM Violation: domain=	open_r	/data/.uid.bi	open_r on /da	
7	2026-02-25 0		n/a	fortism	n/a	[FORTISM Violation: domain=	open_r	/data/.uid.bi	open_r on /da	
8	2026-02-25 0		root	dvm	admin		Successfully lc	root	'admin' succes	session2
9	2026-02-25 0		root	system	admin	User 'admin' with profile 'Sup	login	GUI(192.168.	'admin' login a	session2
10	2026-02-25 0			system	system	System performance status: li	Perf stats	Local system	Show system i	
11	2026-02-25 0		root	system	admin	User 'admin' with profile 'Sup	logout	GUI(192.168.	'admin' logout	
12	2026-02-25 0			system	admin		edit	console	path=system.a	
13	2026-02-25 0			system	admin	User 'admin' with profile 'Sup	login	console	'admin' login a	
14	2026-02-25 0		n/a	fortism	n/a	[FORTISM Violation: domain=	open_r	/data/.uid.bi	open_r on /da	
15	2026-02-25 0		root	dvm	admin		Successfully lc	root	'admin' succes	

## Change an active custom session label

When changeable mode is enabled, administrators can change their custom session label during an active session using one of the following methods.

### To change an active session's label:

1. In the *System Information* widget's *Current Session List* menu, select the administrator and click *Edit Custom Session Label*.

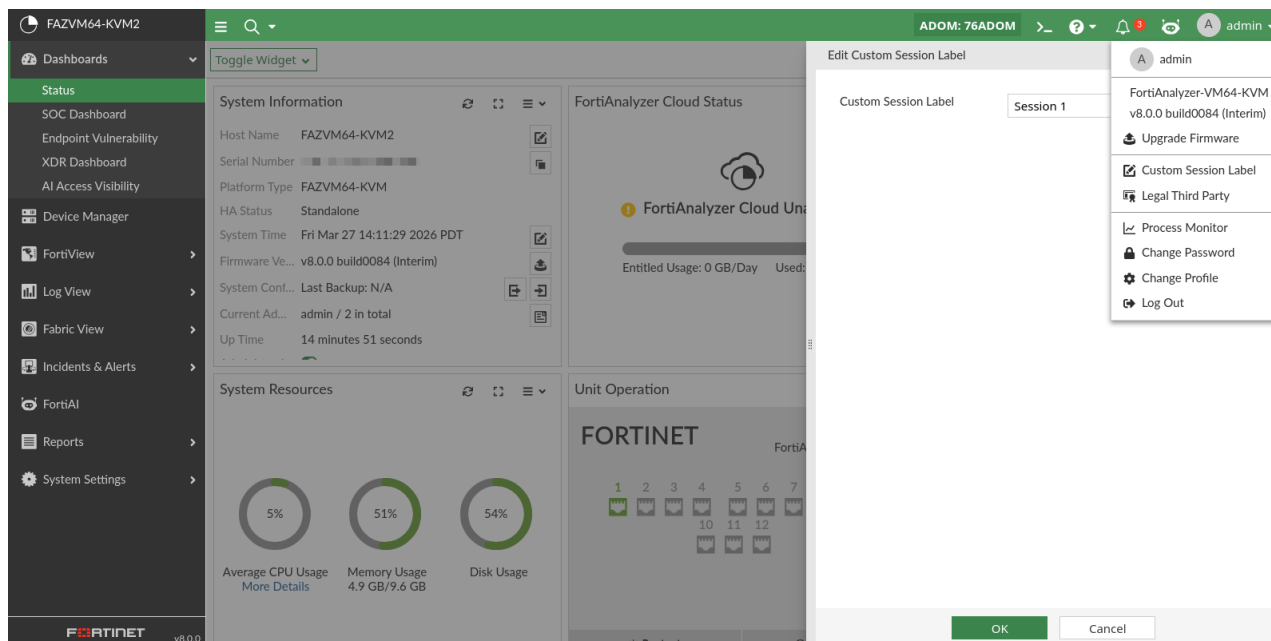
The screenshot shows the FortiAnalyzer interface with the System Information widget. The Admin Session List is open, showing a table of active sessions. The 'admin (Current)' session is selected. The 'Edit Custom Session Label' dialog box is open, allowing the user to change the session label to 'Session 1'.

User Name	Profile
<input checked="" type="checkbox"/> admin (Current)	Super_User
<input type="checkbox"/> admin	Super_User

Custom Session Label:  (0-36 Characters)

Buttons: OK, Cancel

2. In the toolbar's administrator dropdown menu, click *Custom Session Label*.



After changing the session label, you can see the updated session label in the *Current Session List*.

## SAML SSO supports SHA-256 and SHA-512 for both IdP and SP



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- [SAML admin authentication](#)

SAML SSO configurations on FortiAnalyzer support SHA-256 and SHA-512.

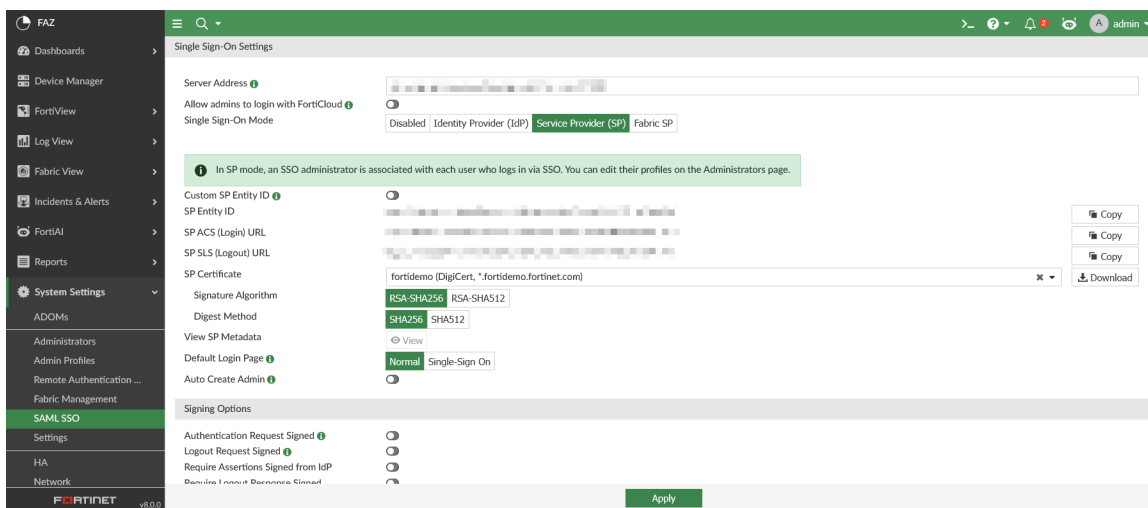
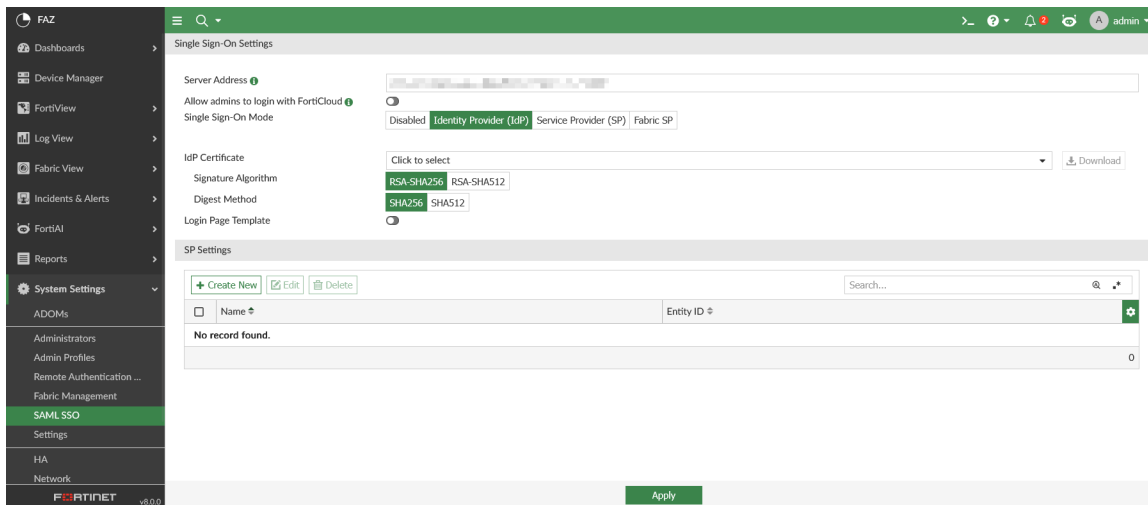
SHA-1 is considered cryptographically weak and has been deprecated for secure digital signatures and digests. Support for SHA-1 on FortiAnalyzer has been removed.

When configuring IdP and SP settings on FortiAnalyzer, administrators can select SHA-256 or SHA-512 for the Signature Algorithm and Digest Method. Because the SAML SSO trust model is based on asymmetric cryptography, the IdP and SP can use different cryptographic algorithms.

For example, when the IdP uses SHA-256 as the Signature Algorithm and Digest Method, the SP can use SHA-256 or SHA-512.

### To configure the Signature Algorithm and Digest Method for SAML SSO:

1. Go to *System Settings > SAML SSO*.
2. Select *Identity Provider (IdP)* or *Service Provider (SP)* as the *Single Sign-On Mode*.
3. Choose an *IdP Certificate* or *SP Certificate*.
4. Select the *Signature Algorithm* as *RSA-SHA256* or *RSA-SHA512*.
5. Select the *Digest Method* as *SHA256* or *SHA512*.



6. Configure the remaining settings as required and click *Apply*.

## FortiAnalyzer supports NTPv4 with SHA-256 encryption

FortiAnalyzer supports NTPv4 with SHA-256 encryption.

### Example: Configuring an NTPv4 server with SHA-256 encryption on FortiAnalyzer:

1. Create a Chrony server in Linux and change the following files:

`/etc/chrony.conf`

```
Allow <FortiAnalyzer gateway>

Bindaddress <internal IP of the linux>

Make sure keyfile is not commented
```

`/etc/chrony.keys`

```
123 SHA256 HEX:f3c79b2288a249f8a218646af0492706014fc9f4beb58fd3b6aa6d45782dd6ca
222 SHA256 somepassword
<key id> <ENC algorithm> <key>
```



The value 123 in the example above must match the key-id defined in the FortiAnalyzer configuration, and the hex key must also match exactly.

## 2. Configure the NTP server settings on FortiAnalyzer in the CLI:

```
config system ntp
  config ntpserver
    edit <server name>
      set server <hostname/IP>
      set authentication enable
      set key-type sha256
      set key-fmt <hex/ascii>
      set key <hex/ascii string>
      set key-id <key ID for authentication>
    next
  end
end
```

- Example Using HEX

```
config system ntp
  config ntpserver
    edit server1
      set server 10.2.2.2
      set authentication enable
      set key-type sha256
      set key-fmt hex
      set key f3c79b2288a249f8a218646af0492706014fc9f4beb58fd3b6aa6d45782dd6ca
      set key-id 123
    next
  end
end
```

- Example using ASCII:

```
config system ntp
  config ntpserver
    edit server1
      set server 10.2.2.2
      set authentication enable
      set key-type sha256
      set key-fmt ascii
      set key somepassword
      set key-id 222
    next
  end
end
```

```
end
end
```

3. Use `diagnose system ntp status` to confirm the connection was successful.

## Time-base retention is configurable for the task monitor and event log



This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- Task Monitor
- Event Log

Time-base retention is configurable for the task monitor and event log in FortiAnalyzer.

You can configure this setting in the FortiAnalyzer CLI:

```
config system local log disk setting
    set log-max-days <integer between 0 and 365>
end
```



If the user set the log-max days to 0, it will return to default setting which is to use the disk quota as the log retention rule.

### Example: Configure the maximum logging days for the task monitor and event log

1. In this example, the current date is April 20, 2026, and there are logs in the Task Monitor and Event Log that exists for 30 days.
2. In the FortiAnalyzer CLI, configure the log max days to 5.

```
config system local log disk setting
    set log-max-days 5
end
```

3. Based on the configured settings above, by midnight all off the logs that are older than April 16, 2026 will be truncated.

## FortiAnalyzer Fabric

This section lists the new features added to FortiAnalyzer for FortiAnalyzer Fabric:

- [Assign access to multiple fabric groups for a single admin on page 69](#)
- [FortiAnalyzer Fabric Supervisor HA on page 71](#)

# Assign access to multiple fabric groups for a single admin



This information is also available in the FortiAnalyzer Fabric 8.0.0 Deployment Guide:

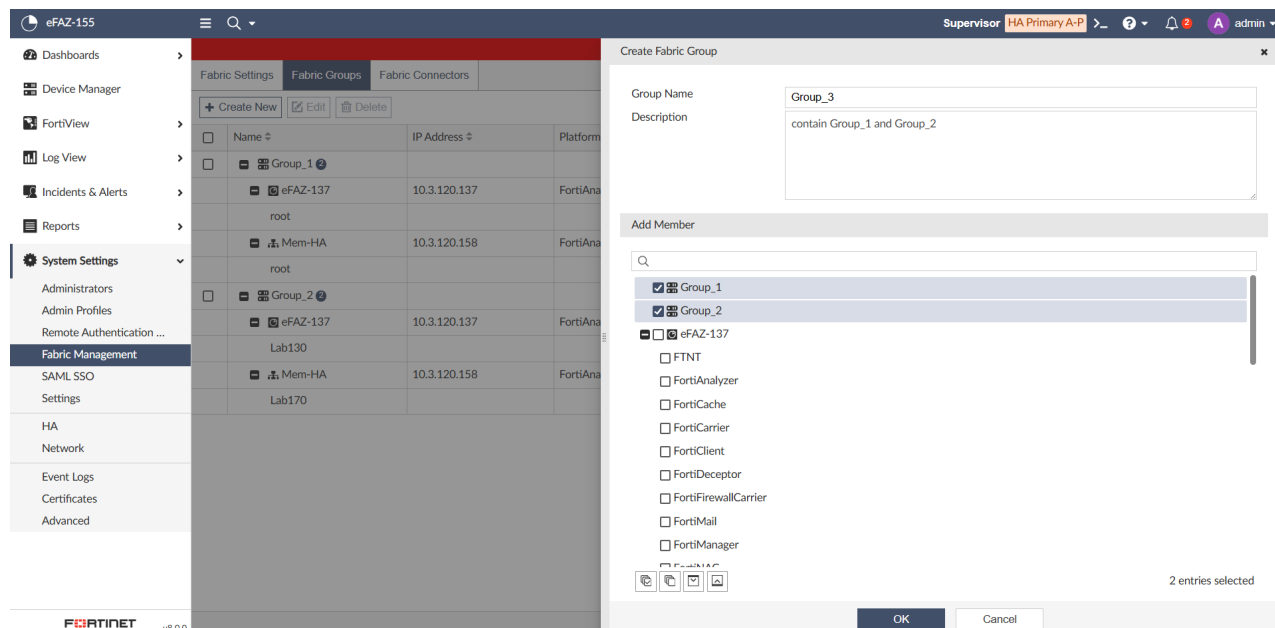
- Fabric Groups

In a FortiAnalyzer Fabric, the configured fabric groups can now contain other fabric groups. This allows you to assign multiple fabric groups to a single admin for role-based access control (RBAC) in a FortiAnalyzer Fabric.

## To create a fabric group containing other groups and assign it to a user:

1. In *System Settings > Fabric Management > Fabric Groups*, create a new fabric group that contains other fabric groups.

In the example below, there are existing fabric groups: *Group\_1* and *Group\_2*. The admin creates a new fabric group (*Group\_3*) and adds *Group\_1* and *Group\_2* as members.



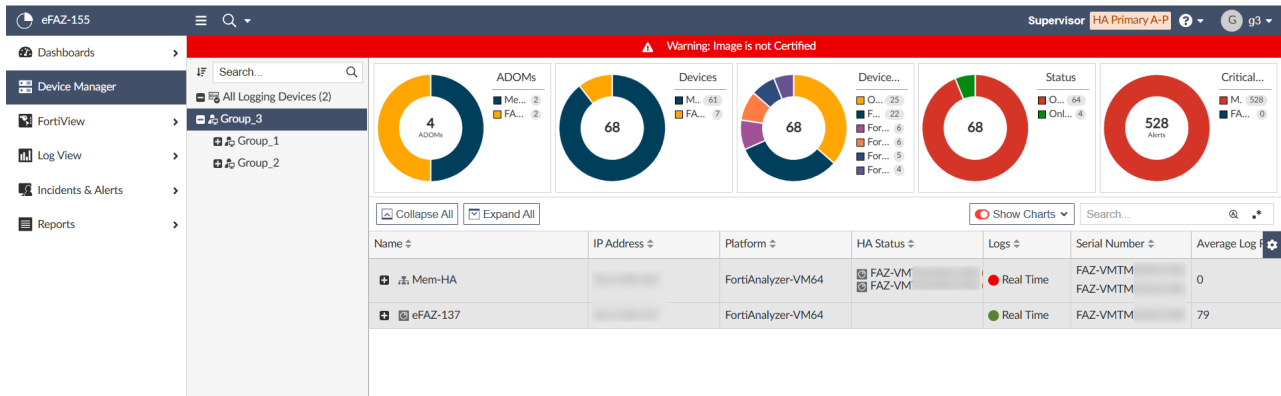
After *Group\_3* is created, it displays in the *Fabric Groups* table view with its assigned members (*Group\_1* and *Group\_2*) listed below.

Name	IP Address	Platform	Logs	Average Log Rate(Logs/...	Disk Quota Usage	Description
Group_1						
eFAZ-137		FortiAnalyzer-VM64	Real Time	73		
root			Real Time	36	(1.47%)	
Mem-HA		FortiAnalyzer-VM64	Real Time	N/A		
root			Real Time	N/A	(9.49%)	
Group_2						
eFAZ-137		FortiAnalyzer-VM64	Real Time	73		
Lab130			Real Time	34	(6.83%)	
Mem-HA		FortiAnalyzer-VM64	Real Time	N/A		
Lab170			Real Time	N/A	(0%)	
Group_3						contain Group_1 and Group_2
Group_1						
Group_2						
Group_4						
eFAZ-137		FortiAnalyzer-VM64	Real Time	73		
FTNT			Real Time	2	(0.15%)	
Mem-HA		FortiAnalyzer-VM64	Real Time	N/A		

2. In *System Settings > Administrators*, create a new admin user and assign the newly created fabric group (*Group\_3*).

The screenshot shows the 'Edit Administrator' form for user 'g3'. The 'Fabric Group' dropdown menu is open, showing a list of groups: Group\_1, Group\_2, Group\_3, and Group\_4. Group\_3 is selected. The user's name is 'g3', the type is 'LOCAL', and the profile is 'Standard\_User'. The description field is empty. The 'Admin Type' is set to 'LOCAL', and 'FortiToken Cloud' is disabled. The 'Fabric Group' is set to 'Group\_3'. The 'Admin Profile' is 'Standard\_User'. The 'JSON API Access' is checked. The 'Theme Mode' is 'Standard'. The 'Trusted Hosts' field is empty. The 'Meta Fields' and 'Advanced Options' sections are collapsed.

The new user will have access to *Group\_3*, which contains both *Group\_1* and *Group\_2*. For example, see the user's view of *Device Manager* displayed below.



## FortiAnalyzer Fabric Supervisor HA



This information is also available in the FortiAnalyzer Fabric 8.0.0 Deployment Guide:

- Supervisor HA

Beginning in FortiAnalyzer 8.0.0, high availability (HA) is supported on the FortiAnalyzer Fabric Supervisor.

When using HA for the FortiAnalyzer supervisor, only the *Active-Passive* operation mode is available. The supervisor's *Fabric Settings* configuration is synced to secondary node, but the secondary node will not establish connection to the FortiAnalyzer members until it becomes the primary node. In a failover scenario, all FortiAnalyzer members will automatically connect to the new primary, and all data will sync to this new primary as well.

Configuration is similar to normal FortiAnalyzer HA. For more information about HA configuration options, see the [FortiAnalyzer Administration Guide](#).

### To configure FortiAnalyzer supervisor HA:

1. In the FortiAnalyzer supervisor, configure the unit as the primary node of an *Active-Passive* HA cluster. The *Active-Active* HA operation mode is not available for FortiAnalyzer supervisors.

**Cluster Status**

Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Supervisor Data Sync	Message
Secondary	FAZ-VMTM 0	10.3.15.206	eFAZ-206	1d 5h 22m 10s	Done	In-Sync	Done	
Primary	FAZ-VMTM 1	10.3.15.205	eFAZ-205	1d 5h 26m 16s	-	Config will be synced to secondaries	-	

**Cluster Settings**

Operation Mode: Standalone **Active-Passive**

Preferred Role: Secondary **Primary**

Initial Sync:

**Cluster Virtual IP**

IP Address and Interface	IP Address	Interface	Action
	10.3.15.174	port1	<input type="checkbox"/> <input type="checkbox"/>

**Cluster Settings**

Peer Address and Peer SN	Peer Address	Peer SN	Action
	10.3.15.206	FAZ-VMTM 0	<input type="checkbox"/> <input type="checkbox"/>

Group Name: Super-HA  
 Group ID: 174 (1-255)  
 Password: \*\*\*\*\*  
 Heart Beat Interval: 4  
 Heart Beat Interface: port1  
 Failover Threshold: 12  
 Priority: 100 (1-120)  
 Log Data Sync:

2. In the FortiAnalyzer to act as the secondary node, configure the HA options.

You can review the HA status in the top *Cluster Status* section. The *Supervisor Data Sync* column displays the supervisor data sync status.

**Cluster Status**

Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Supervisor Data Sync	Message
Secondary	FAZ-VMTM 0	10.3.15.206	eFAZ-206	1d 5h 28m 13s	Done	In-Sync	Done	
Primary	FAZ-VMTM 1	10.3.15.205	eFAZ-205	1d 5h 28m 05s	-	-	-	

**Cluster Settings**

Operation Mode: Standalone **Active-Passive**

Preferred Role: **Secondary** Primary

Initial Sync:

**Cluster Virtual IP**

IP Address and Interface	IP Address	Interface	Action
	10.3.15.174	port1	<input type="checkbox"/> <input type="checkbox"/>

**Cluster Settings**

Peer Address and Peer SN	Peer Address	Peer SN	Action
	10.3.15.205	FAZ-VMTM 1	<input type="checkbox"/> <input type="checkbox"/>

Group Name: Super-HA  
 Group ID: 174 (1-255)  
 Password: \*\*\*\*\*  
 Heart Beat Interval: 4  
 Heart Beat Interface: port1  
 Failover Threshold: 12  
 Priority: 100 (1-120)  
 Log Data Sync:

Once HA is established, the same FortiAnalyzer topology is displayed in both primary and secondary. To view the topology in a node, go to *System Settings > Fabric Management > Fabric Settings*.

The screenshot displays the FortiAnalyzer System Settings interface for Fabric Management on the primary node (eFAZ-205). The main dashboard shows the HA cluster topology with two nodes: Mem-HA (IP 10.3.15.175) and eFAZ-240 (IP 10.3.15.240). Both nodes are in 'In Sync' status. The primary node (eFAZ-205) is the Supervisor, and the member (eFAZ-240) is a Member. The member's resource usage is detailed as follows:

Resource	Usage	Limit
CPU Usage	14.3 %	11.9 GB / 32.9 GB
Memory Usage	36 %	380.18 GB / 491.08 GB
Disk Usage	77.4 %	

Same as in a normal FortiAnalyzer HA cluster, the secondary node cannot perform some actions. For example, actions such as authorizing, rejecting or deleting members, and creating Fabric Groups are grayed out in the secondary.

The screenshot displays the FortiAnalyzer System Settings interface for Fabric Management on the secondary node (eFAZ-206). The main dashboard shows the HA cluster topology with two nodes: Mem-HA (IP 10.3.15.175) and eFAZ-240 (IP 10.3.15.240). Both nodes are in 'In Sync' status. The secondary node (eFAZ-206) is a Member, and the primary node (eFAZ-205) is the Supervisor. The member's resource usage is detailed as follows:

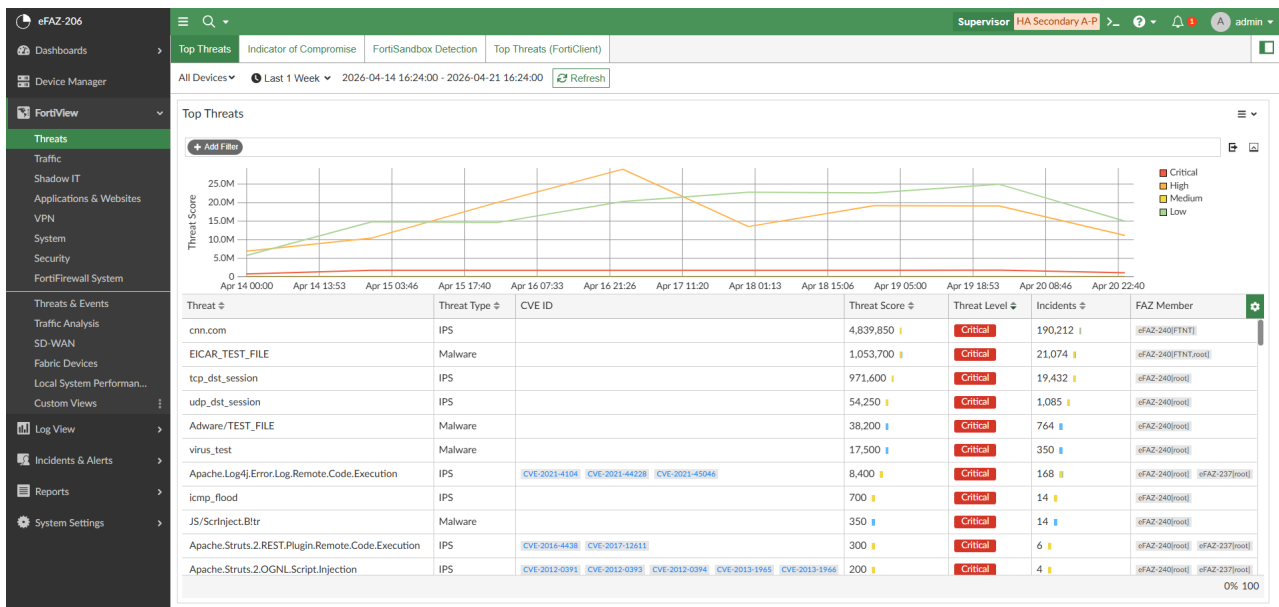
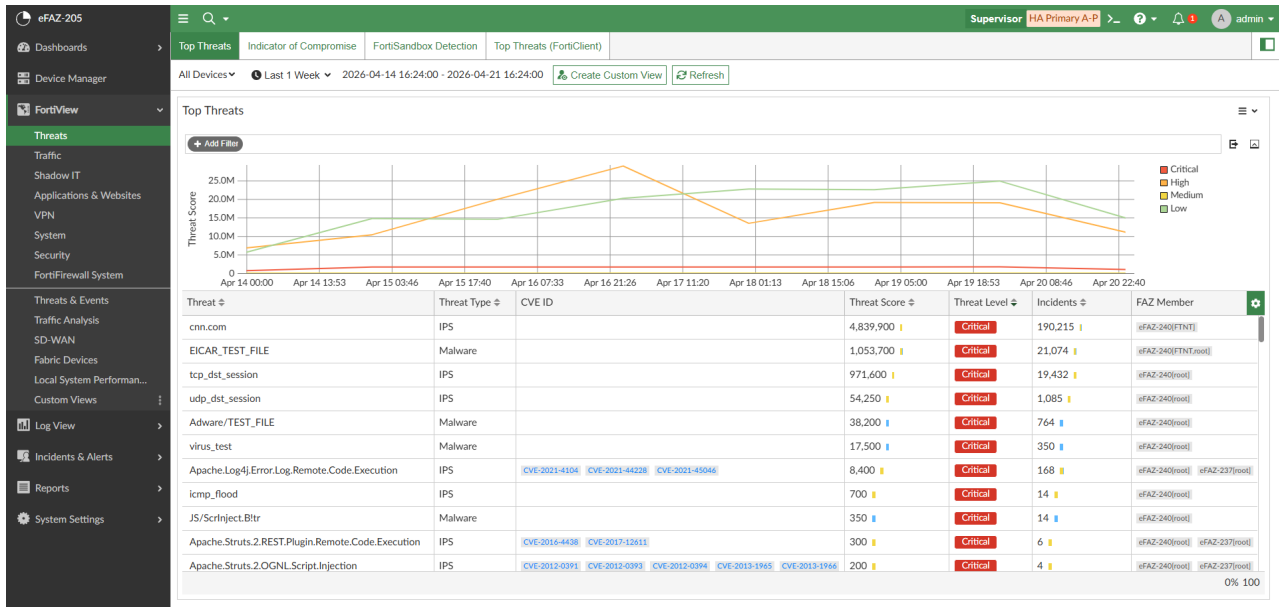
Resource	Usage	Limit
CPU Usage	17.4 %	9.8 GB / 32.9 GB
Memory Usage	36 %	131.61 GB / 491.08 GB
Disk Usage	77.4 %	

The 'Fabric Settings' panel is open, showing the cluster configuration:

- Status:  On
- Role:  Supervisor  Member
- Cluster Name: Fabric
- Session Port: 6443
- Secure Connection:  On

The secondary node can view members' devices, logs, FortiView, and Reports data, but the connection is established through supervisor primary node. See examples below.

- FortiView in both the secondary and primary:



- Log View in both the secondary and primary:

Supervisor HA Primary A-P

Fortinet Logs Threat Hunting

285

FortiGate

Traffic Security Event GTP FortiSwitch

All Devices Last 1 Hour 15:25:16 - 16:25:16 Full Screen Refresh More

Filter Mode Add Filter

#	FortiAnaly...	ADOM	Date/Tim	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	eFAZ-240	Lab	2026-04-21 1	FG101FTK	✓				tcp/541	tcp/541	300.0 B/0.0 KB	
2	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				GitHub-GitHu	SSL_TLsv1.3	2.8 KB/11.2 KB	APP 2
3	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				HTTPS	Microsoft.Outlook	56.2 KB/29.3 KB	
4	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				HTTPS	HTTPS	2.2 KB/552.0 B	
5	eFAZ-237	root	2026-04-21 1	FG3K6ETB	⊗ Pending				HTTPS	HTTPS	0 B/0 B	
6	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				DNS	DNS	286.0 B/623.0 B	
7	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				HTTPS	Microsoft.Teams	14.3 KB/26.0 KB	APP 2
8	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				IKE	ISAKMP	29.0 MB/0.0 KB	
9	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				Google-DNS	DNS	57.0 B/85.0 B	
10	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				HTTPS	Microsoft.365.Portal	29.8 KB/13.8 KB	
11	eFAZ-237	root	2026-04-21 1	FG3K6ETB	✓				MS_FILE_SHA	SMBv3	1.4 KB/1.0 KB	APP 2

Supervisor HA Secondary A-P

Fortinet Logs Threat Hunting

285

FortiGate

Traffic Security Event GTP FortiSwitch

All Devices Last 1 Hour 15:25:17 - 16:25:17 Full Screen Refresh More

Filter Mode Add Filter

#	FortiAnaly...	ADOM	Date/Tim	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				HTTPS	Microsoft.Authentication	5.7 KB/20.2 KB	APP 1
2	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				TCP_30000-6	TCP_30000-65535	52.0 B/40.0 B	
3	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				HTTPS	HTTPS	1.6 KB/3.5 KB	
4	eFAZ-240	root	2026-04-21 1	FG3K6ET	⊗ Pending				HTTPS	HTTPS	0 B/0 B	
5	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				HTTPS	Microsoft.Exchange.Serve	10.4 KB/16.6 KB	
6	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				DNS	DNS	88.0 B/104.0 B	
7	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				DNS	DNS	292.0 B/268.0 B	
8	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				DNS	DNS	138.0 B/223.0 B	
9	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				MMS	IPSec	112.0 B/112.0 B	
10	eFAZ-240	root	2026-04-21 1	FG3K6ET	✓				MMS	IPSec	112.0 B/112.0 B	

# Index

The following index provides a list of all new features added to FortiAnalyzer 8.0. The index allows you to quickly identify the version where the feature first became available in FortiAnalyzer.

Select a version number to navigate in the index to the new features available for that release:

- [8.0.0 on page 76](#)

## 8.0.0

### Security Operations

SOAR SIEM	<ul style="list-style-type: none"><li>• <a href="#">Playbook editor improvements on page 6</a></li></ul>
Incident and event management	<ul style="list-style-type: none"><li>• <a href="#">Alert explorer improvements on page 9</a></li></ul>
Dashboards	<ul style="list-style-type: none"><li>• <a href="#">AI Access Visibility dashboard on page 10</a></li></ul>
Asset and identity	<ul style="list-style-type: none"><li>• <a href="#">Improvements to the user experience in the Asset and Identity Center on page 12</a></li></ul>
Other enhancements	<ul style="list-style-type: none"><li>• <a href="#">FortiMQ connector for automated blocking on page 16</a></li><li>• <a href="#">Machine learning for anomaly detection on page 21</a></li></ul>

### Log and Report

Logging	<ul style="list-style-type: none"><li>• <a href="#">FortiData incident support on page 33</a></li></ul>
Log forwarding	<ul style="list-style-type: none"><li>• <a href="#">FortiAnalyzer Fluentd supports the Azure Monitor Log Ingestion API on page 36</a></li></ul>
Reports	<ul style="list-style-type: none"><li>• <a href="#">Anomaly login report on page 38</a></li><li>• <a href="#">FortiDeceptor incident report on page 42</a></li><li>• <a href="#">Shadow-AI report on page 48</a></li></ul>

### FortiAI

FortiAI	<ul style="list-style-type: none"><li>• <a href="#">FortiAI alert triage agent on page 53</a></li><li>• <a href="#">FortiAI threat posture timeline on page 55</a></li></ul>
---------	--

## System

- |                      |   |
|----------------------|---|
| Other enhancements   | <ul style="list-style-type: none"><li>• <a href="#">Legal third party disclosure panel on page 59</a></li><li>• <a href="#">Custom session labels in FortiAnalyzer event logs on page 61</a></li><li>• <a href="#">SAML SSO supports SHA-256 and SHA-512 for both IdP and SP on page 65</a></li><li>• <a href="#">FortiAnalyzer supports NTPv4 with SHA-256 encryption on page 66</a></li><li>• <a href="#">Time-base retention is configurable for the task monitor and event log on page 68</a></li></ul> |
| FortiAnalyzer Fabric | <ul style="list-style-type: none"><li>• <a href="#">Assign access to multiple fabric groups for a single admin on page 69</a></li><li>• <a href="#">FortiAnalyzer Fabric Supervisor HA on page 71</a></li></ul>   |



[www.fortinet.com](http://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.