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

May 5, 2026
FortiAnalyzer 8.0.0 New Features Guide
05-800-1211640-20260505

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-04-21	Initial release.
2026-05-05	Added: • Playbook editor improvements on page 6 • Alert explorer improvements on page 9 • AI Access Visibility dashboard on page 10 • Machine learning for anomaly detection on page 21 • Shadow-AI report on page 48 • FortiAI alert triage agent on page 53 • FortiAI threat posture timeline on page 55 • FortiAnalyzer Fabric Supervisor HA on page 71
2026-05-13	Added: • SAML SSO supports SHA-256 and SHA-512 for both IdP and SP on page 65 • FortiAnalyzer supports NTPv4 with SHA-256 encryption on page 66
2026-05-14	Added: • Time-base retention is configurable for the task monitor and event log on page 68

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:

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

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

Playbook editor improvements

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

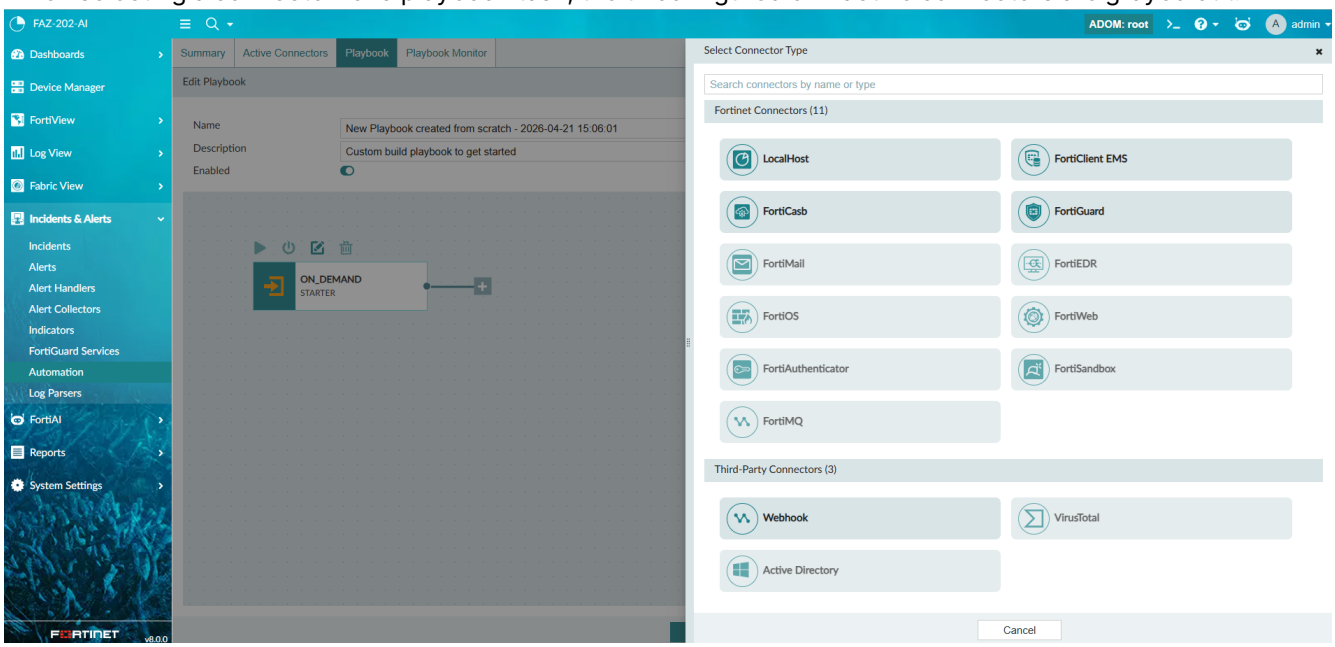
- Playbooks

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

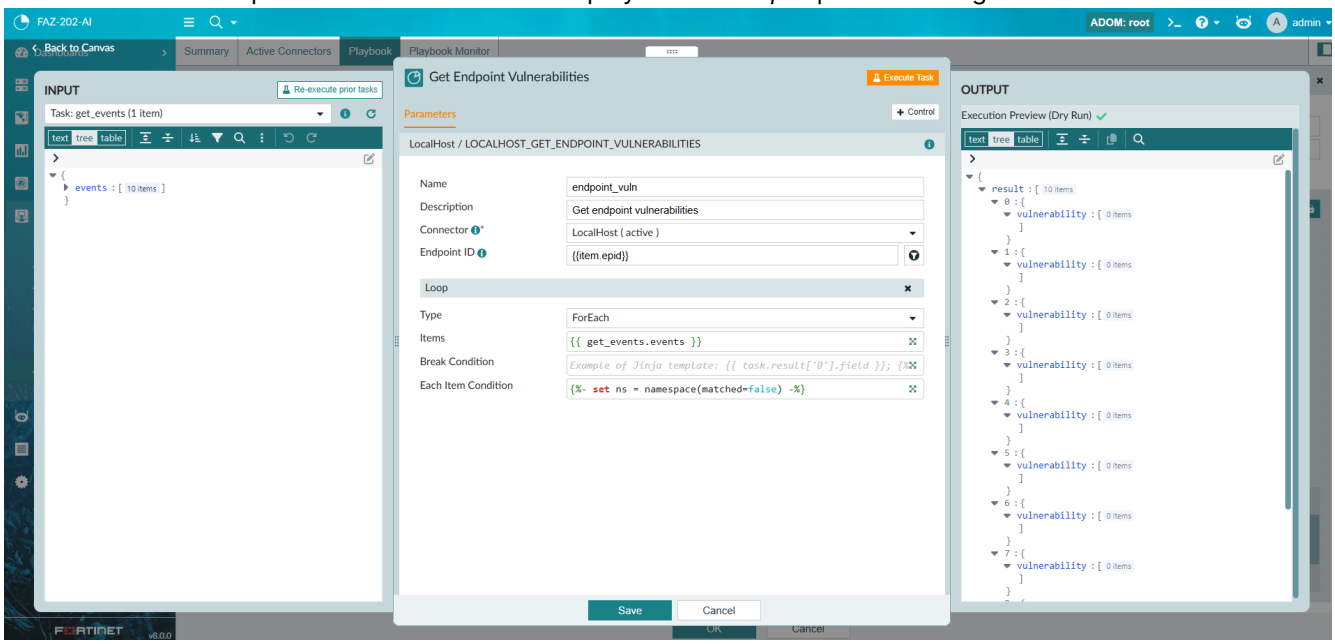
- Step-by-step debugging mode, including the capability to run, pause, and inspect data at each node (task).
- Play and re-play workflows, allowing you to use various input data for testing.
- Partial run capabilities, allowing you to restart from a specific node (task) instead of running the whole playbook.
- 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.

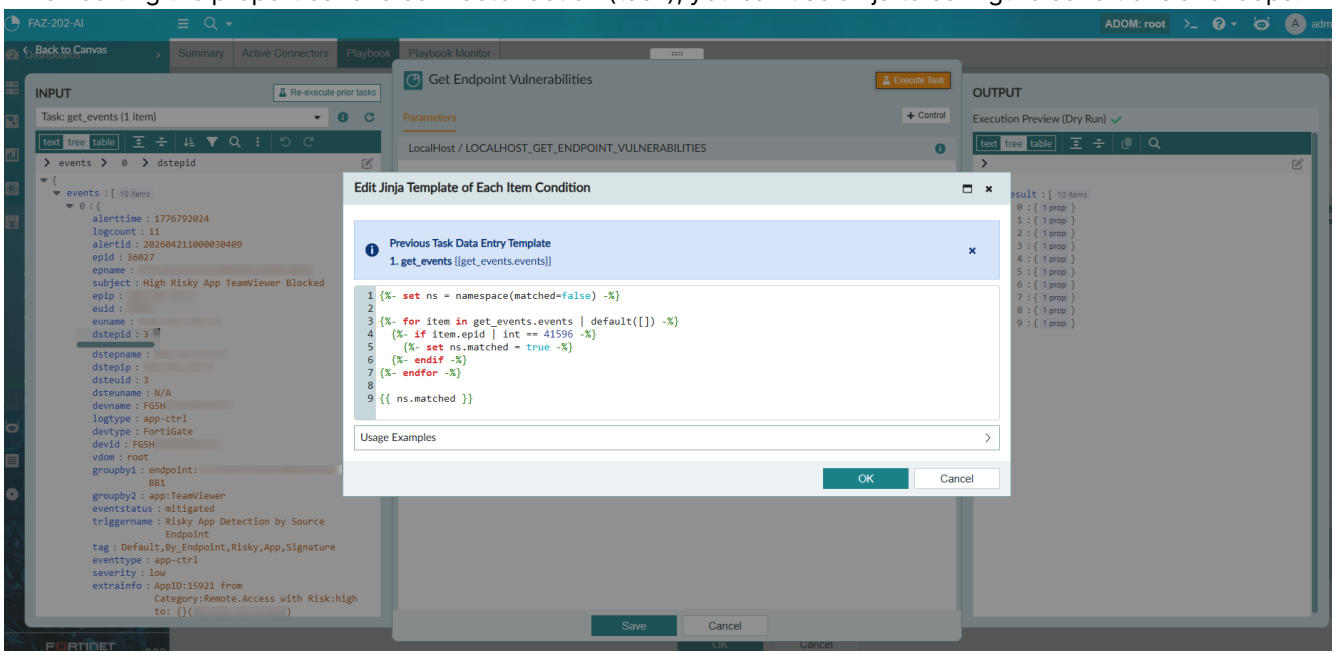
When selecting a connector for a playbook task, the unconfigured or inactive connectors are grayed out.



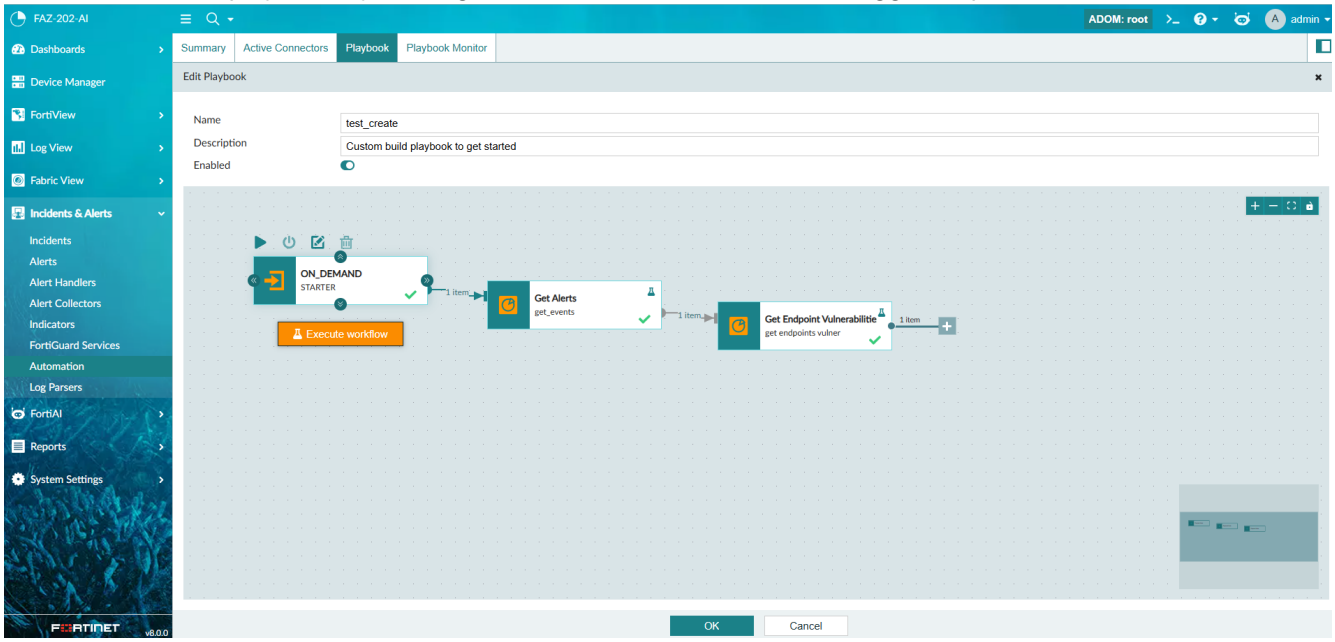
When configuring a task, the *Input* pane allows you to run the prior task and get results to use for debugging the current task. The output from the current task displays in the *Output* pane at the right.



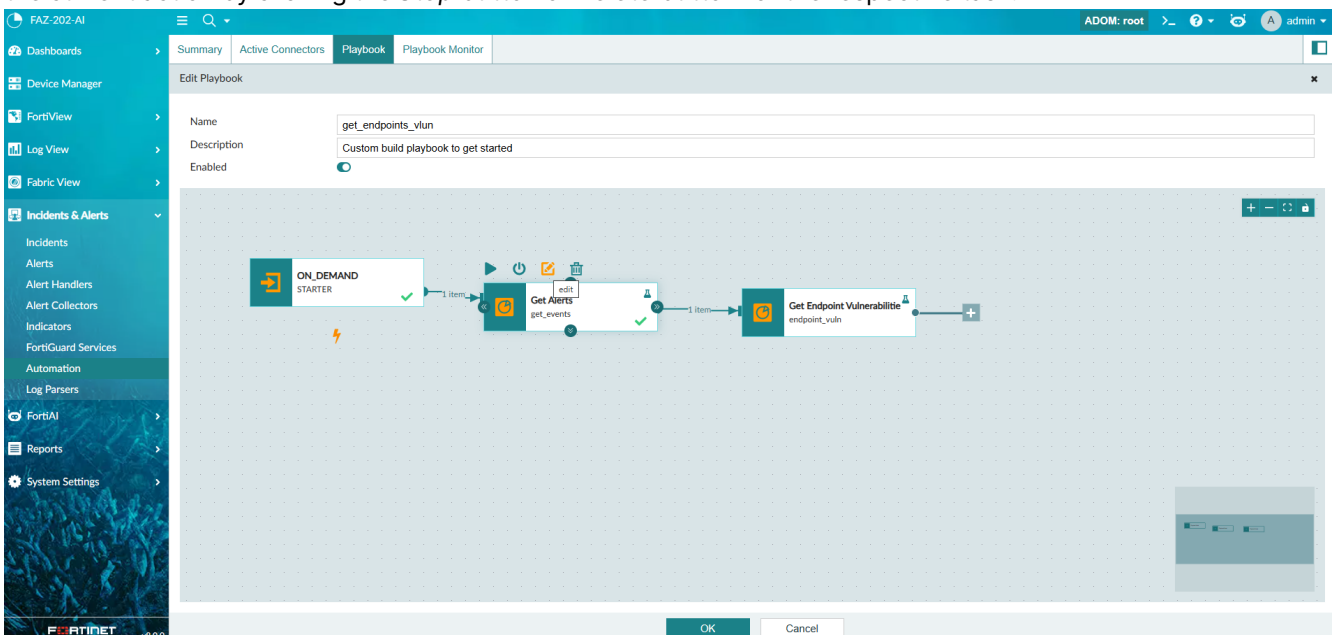
When editing the properties for a connector action (task), you can use Jinja to configure conditions and loops.



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

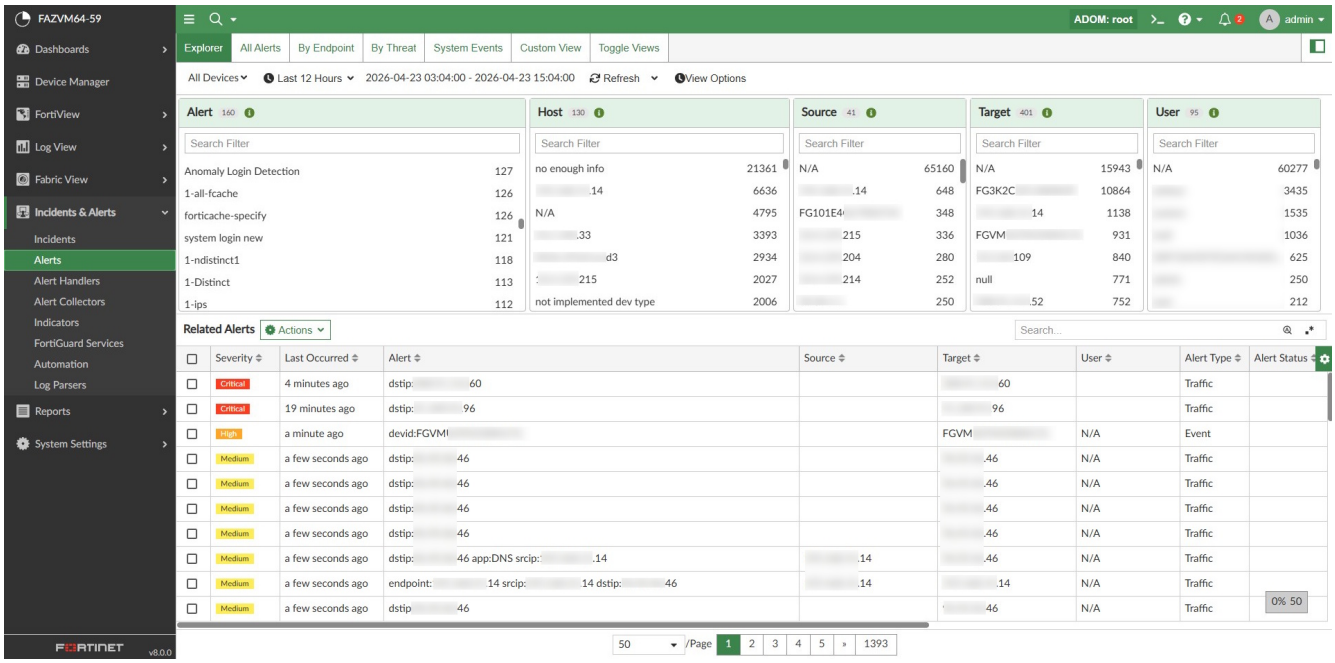
Alert explorer improvements

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

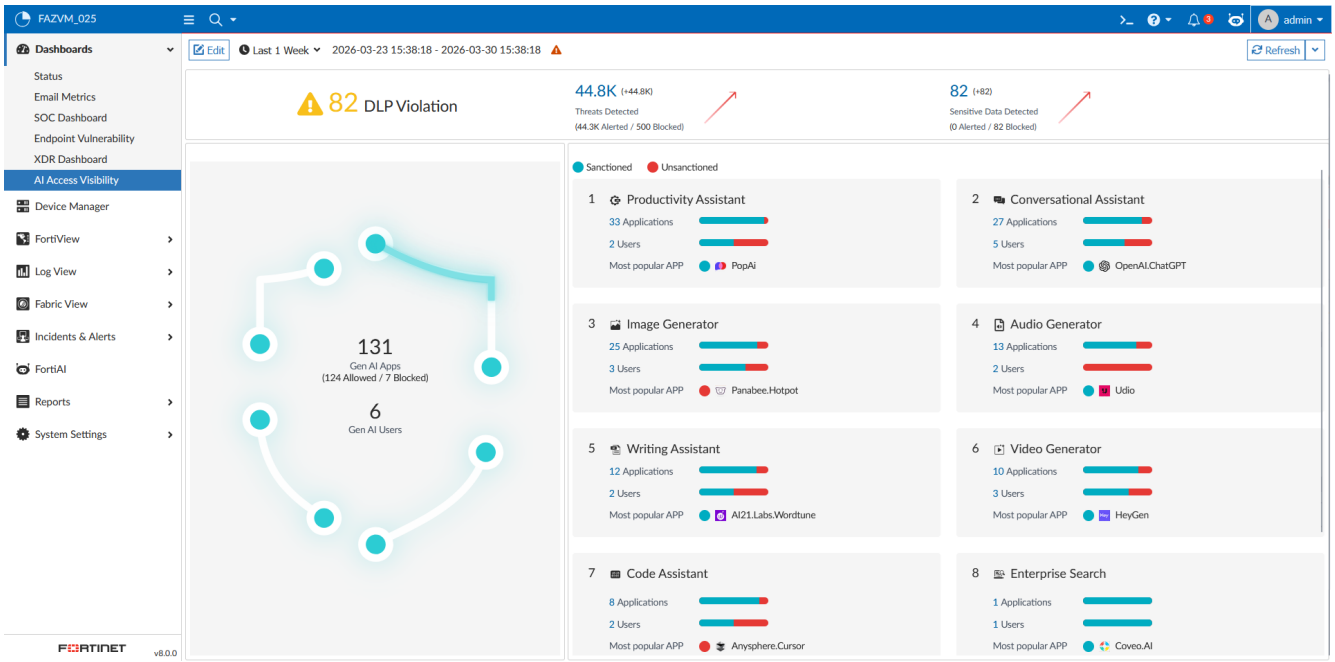
> This information is also available in the FortiAnalyzer 8.0 Administration Guide:
> - AI Access Visibility

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
GEN AI Access Threats	This widget displays: • Number of DLP violations detected. • Number of threats detected, alerted, and blocked. Indicates if these numbers are trending up or down. • Number of sensitive data detections, alerted, and blocked. Indicates if these numbers are trending up or down.
Gen AI Access Overview	Displays the total number of Generative AI applications accessed and total number of users that used these applications. This widget also displays the number of blocked and allowed applications available to the user.
Gen AI Access Categories	Displays the generative AI that has been accessed by category. Applications are grouped in the following categories, which are set in FortiGuard: • Conversational Assistant • Audio Generator • Code Assistant • Enterprise Search • Image Generator • Meeting Assistant • Productivity Assistant • Video Generator • Writing Assistant

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: *Sanctioned* and *Unsanctioned*. 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

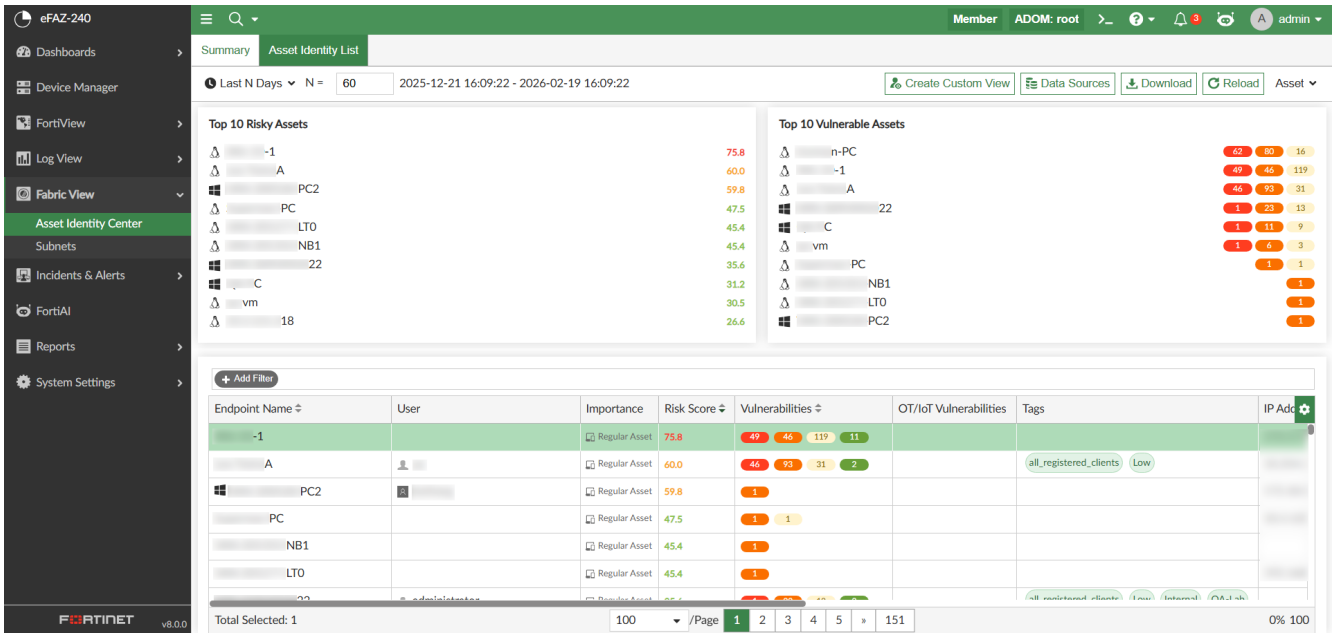
Improvements to the user experience in the Asset and Identity Center

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

- Asset List
- Identity List

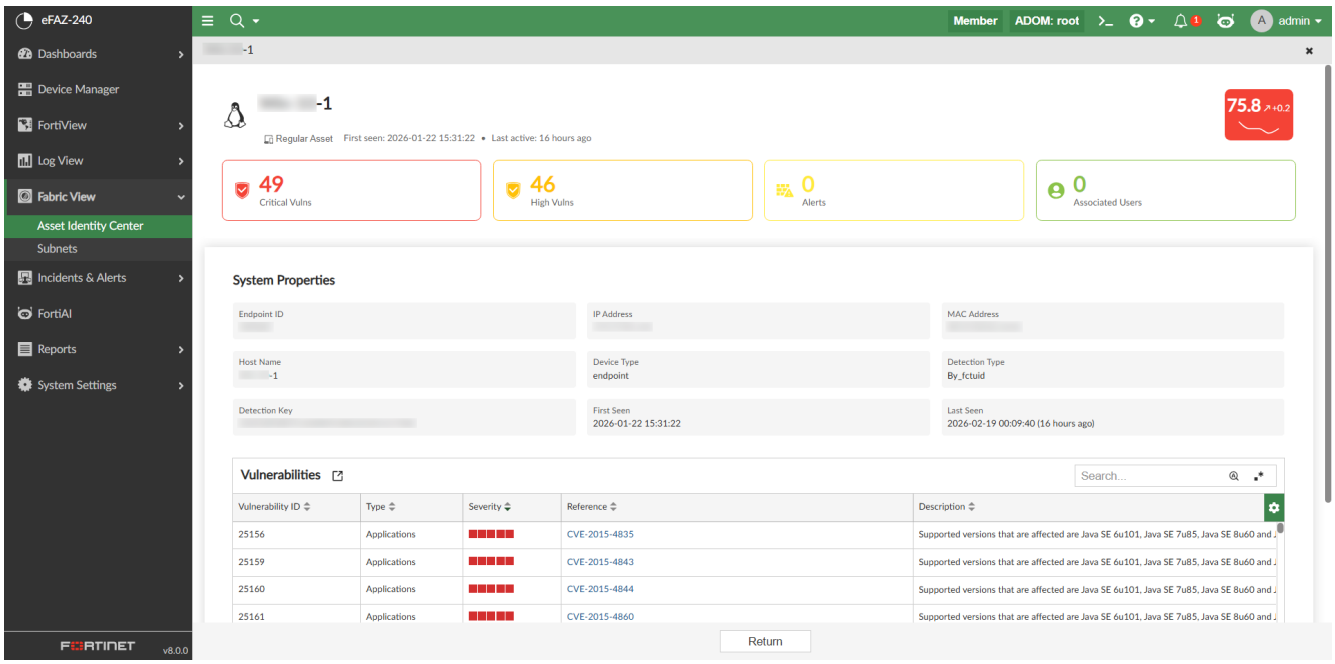
The GUI in *Fabric View* > *Asset Identity Center* has been changed in FortiAnalyzer 8.0.0 to improve the admin user experience.

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

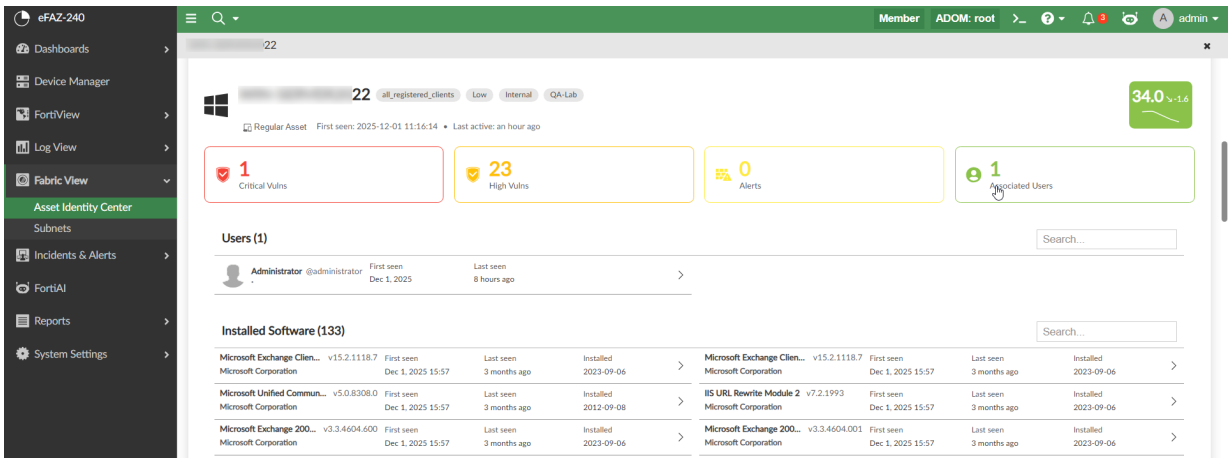


- Colors are used with certain number fields to help identify severity. For example, see the *Top 10 Risky Assets* in the image above.
- Pagination is fixed on the footer of the *Asset Identity List*.
- The pill shape used in the *Asset Identity List*, such as in the *Vulnerabilities* column, is updated 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.

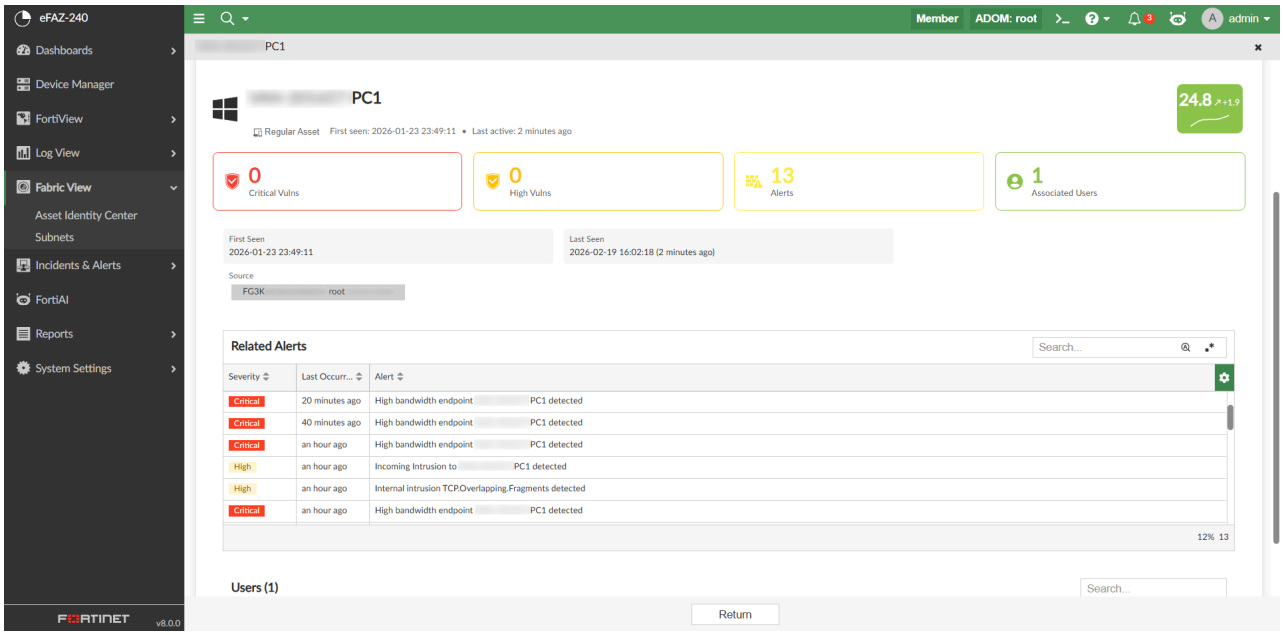
It also includes the following changes in the endpoint details:



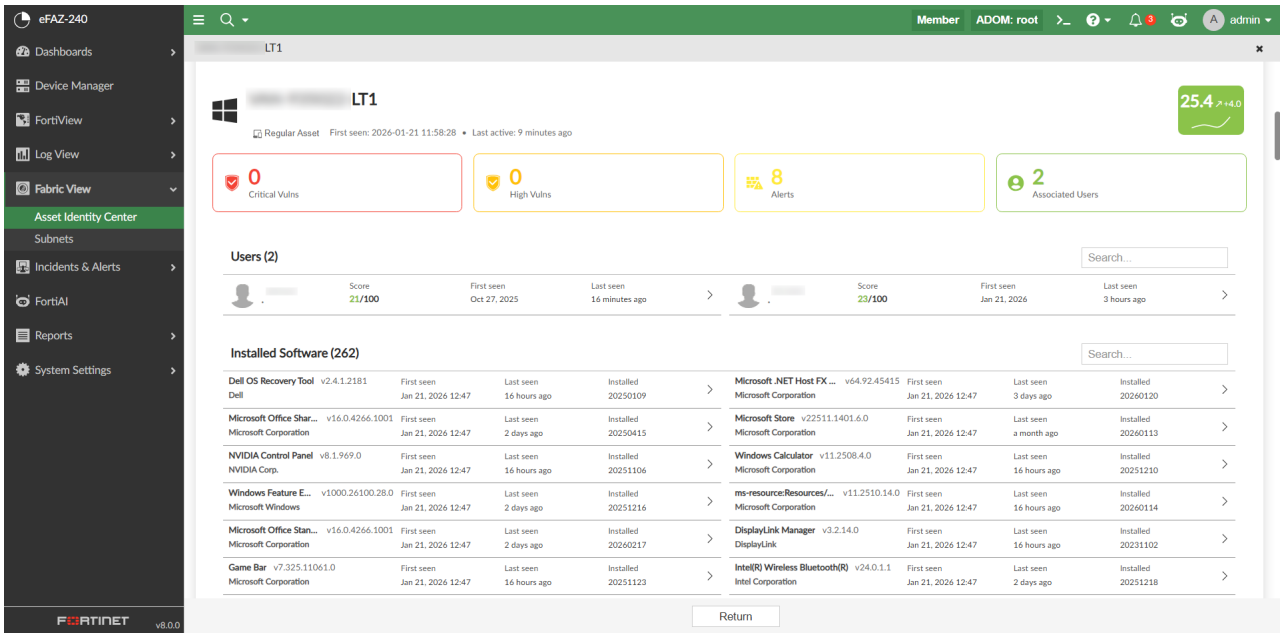
- After drilling down to an endpoint, the detail views now display in full screen.
- The four widgets at the top of the asset details are now colored to better visualize the information: *Critical Vulns*, *High Vulns*, *Alerts*, and *Associated Users*.
  - The four widgets at the top are also interactive;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



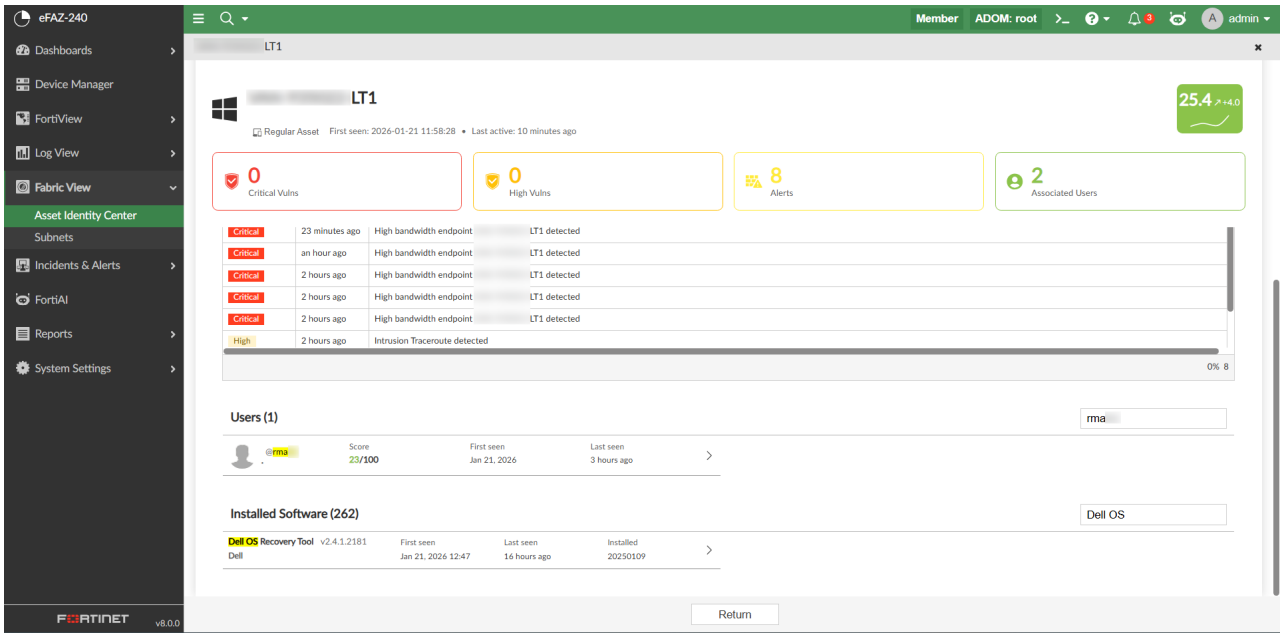
- The header information in the endpoint details, including the four widgets (*Critical Vulns*, *High Vulns*, *Alerts*, and *Associated Users*), is now fixed to the top so the user always sees key information as they scroll further down.
- The container heights have been increased to ensure more visibility,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



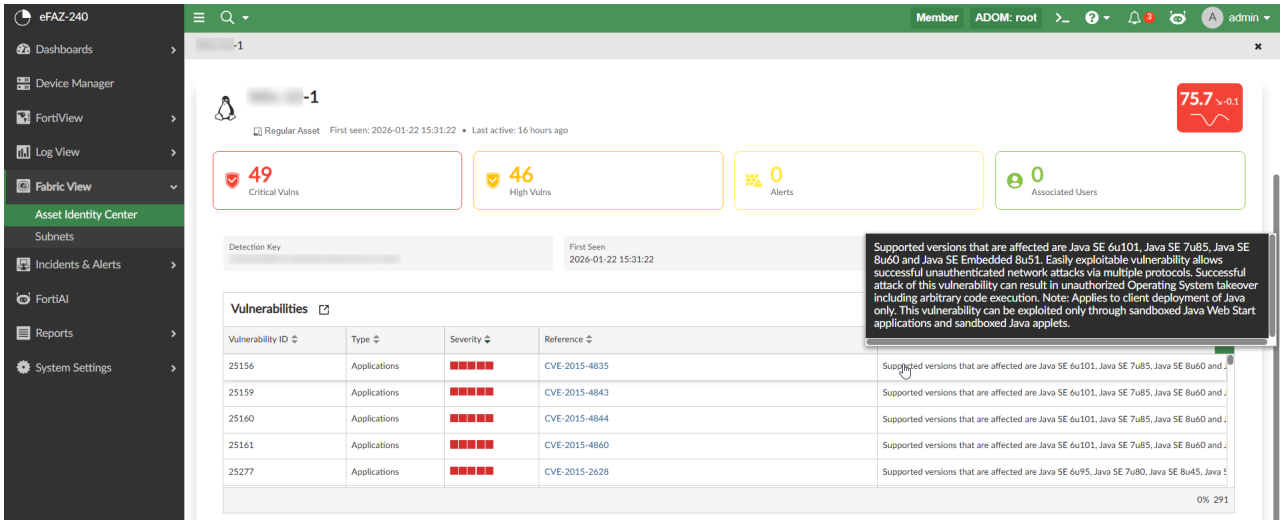
- The *Users* and *Installed Software* sections of the detail views now display in a split view, saving space while maintaining visibility and organization.



- 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.

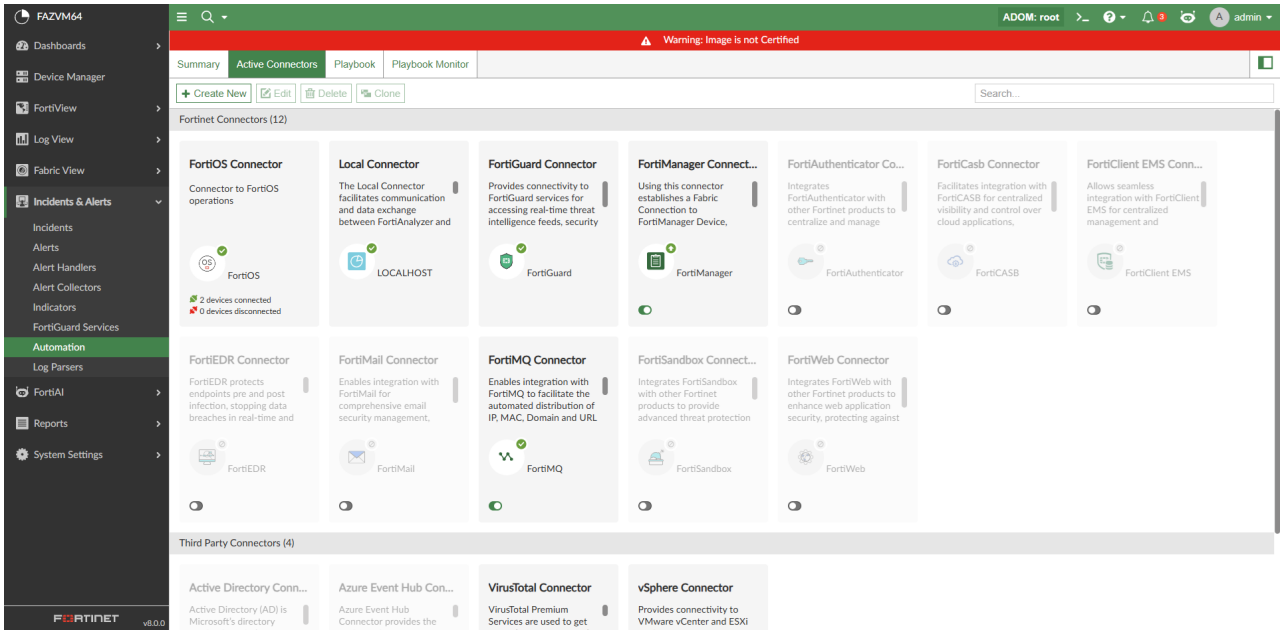
To enable the transmission of block lists from FortiAnalyzer to FortiGate, you must complete the following:

- 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*.

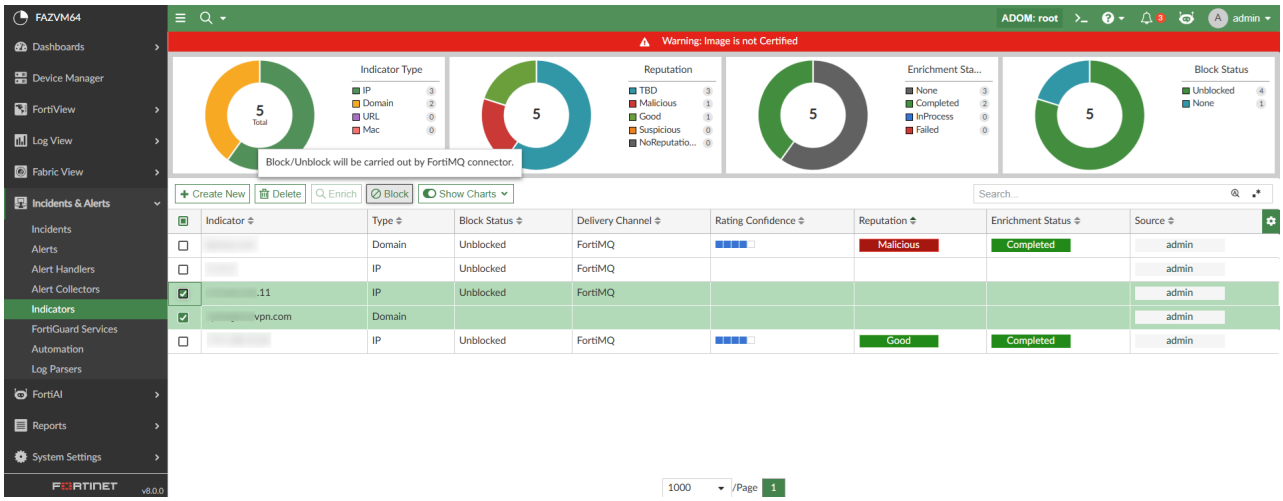


The FortiMQ connector is available and disabled by default in all Fabric and FortiGate-type ADOMs.

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.

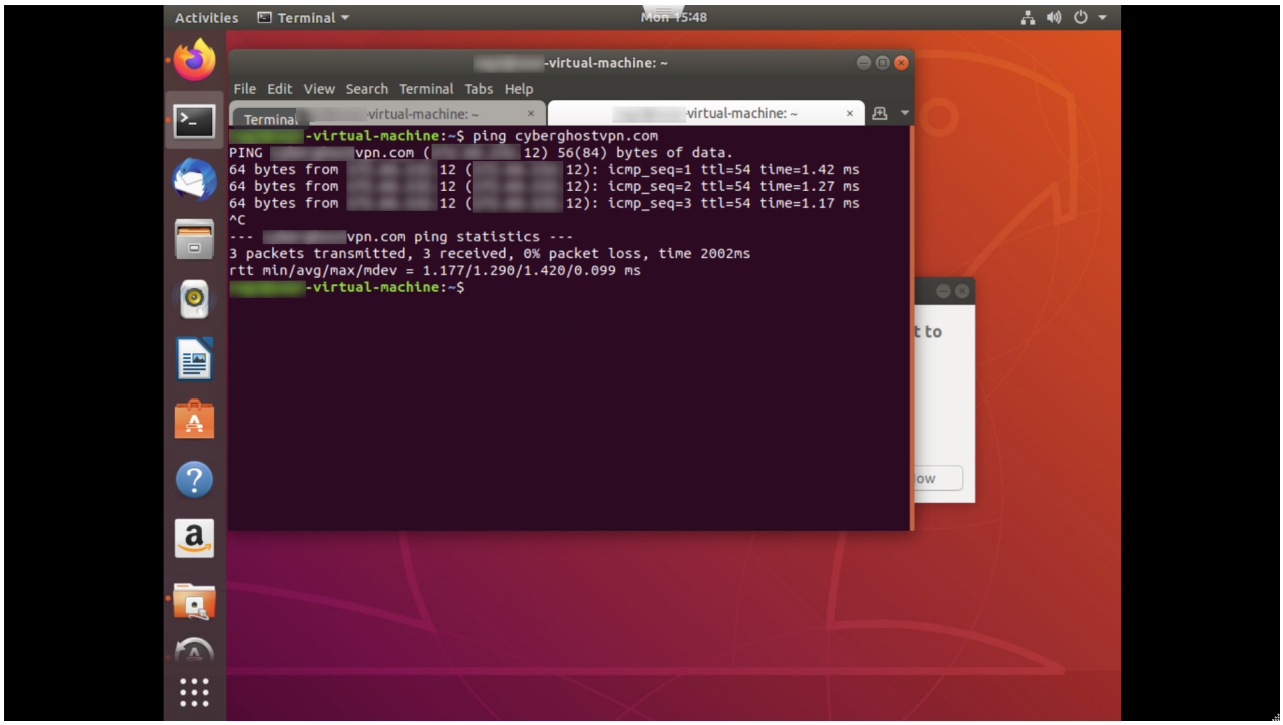
> You cannot create new FortiMQ connectors or delete the existing one in the ADOM.

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.”

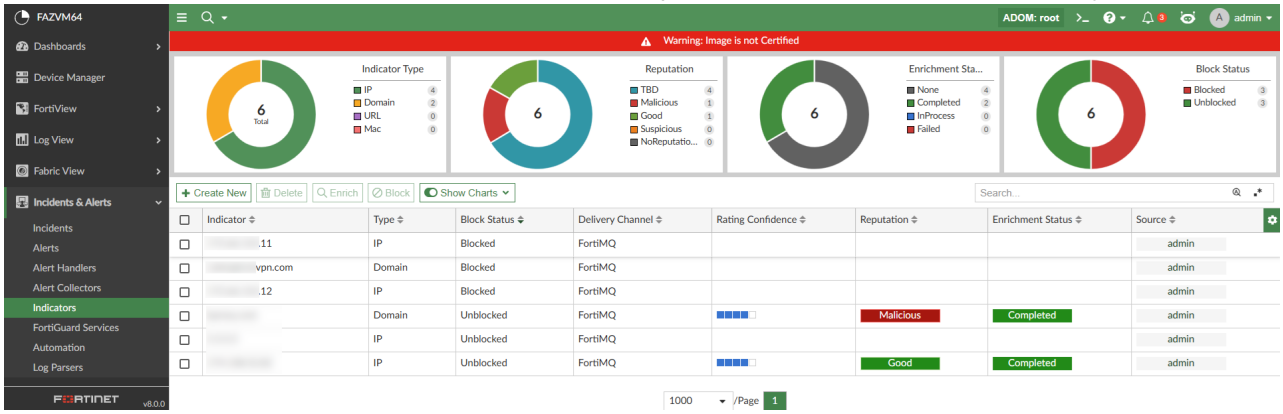


> When both FortiManager and FortiMQ connectors are available, blocking via FortiManager remains supported. However, priority is given to the FortiMQ connector. Indicators are sent via FortiManager only if the FortiMQ connector is disabled.

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

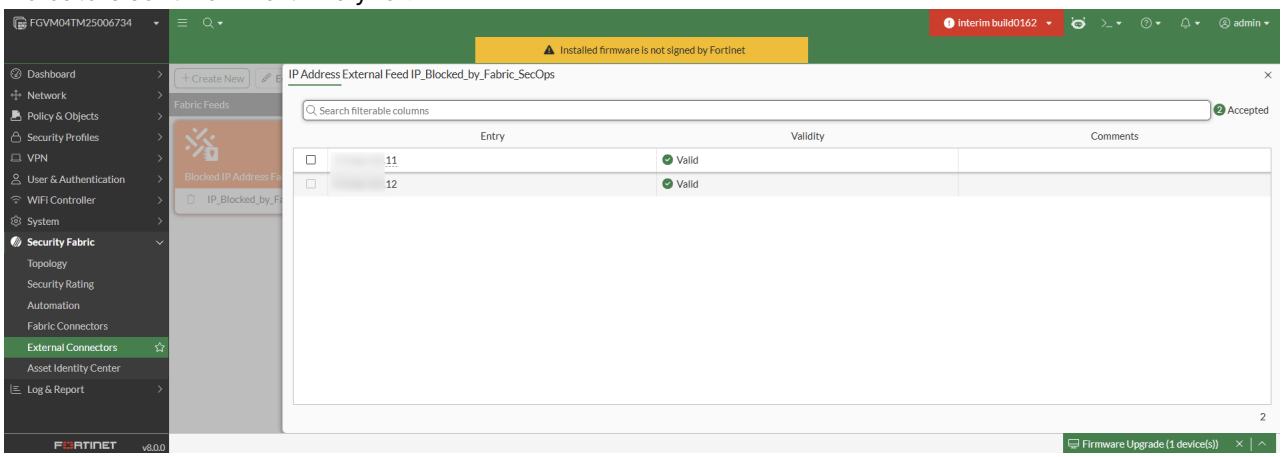


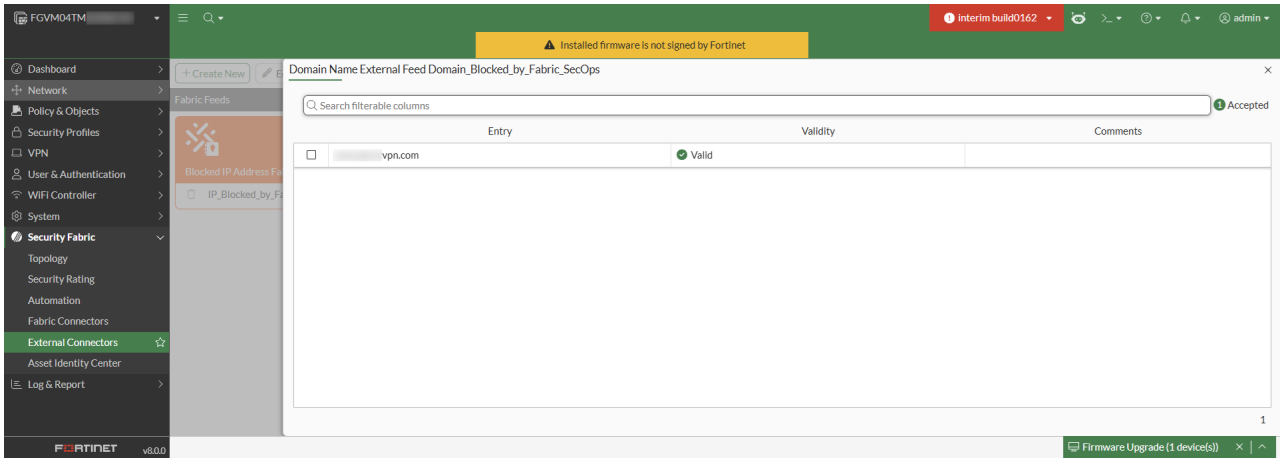
Upon confirming a *Block* or *Unblock* action, the "`block_indicator`" playbook runs in the background and sends the indicators to FortiMQ. See below for an example of blocked indicators in FortiAnalyzer:



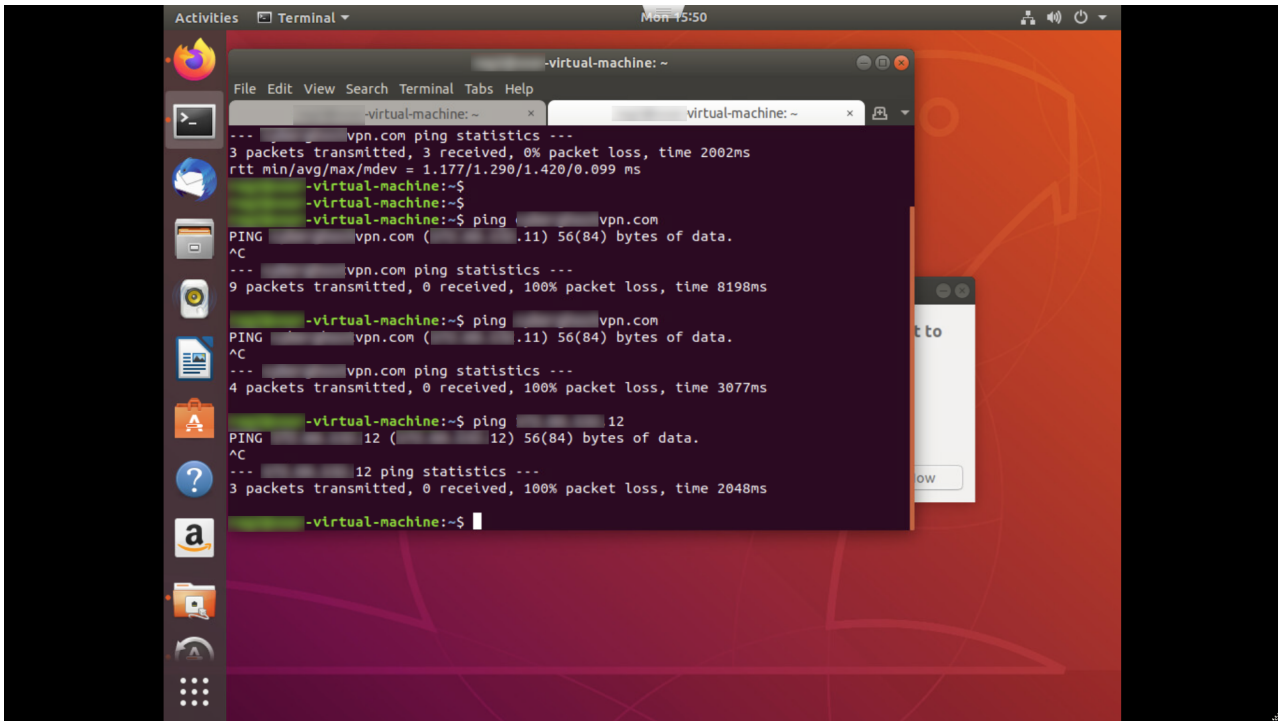
FortiGate retrieves these indicators from FortiMQ and updates them in the external feeds. These feeds can then be used in policies or profiles to deny access. External feeds are updated on FortiGate with the

indicators sent from FortiAnalyzer:



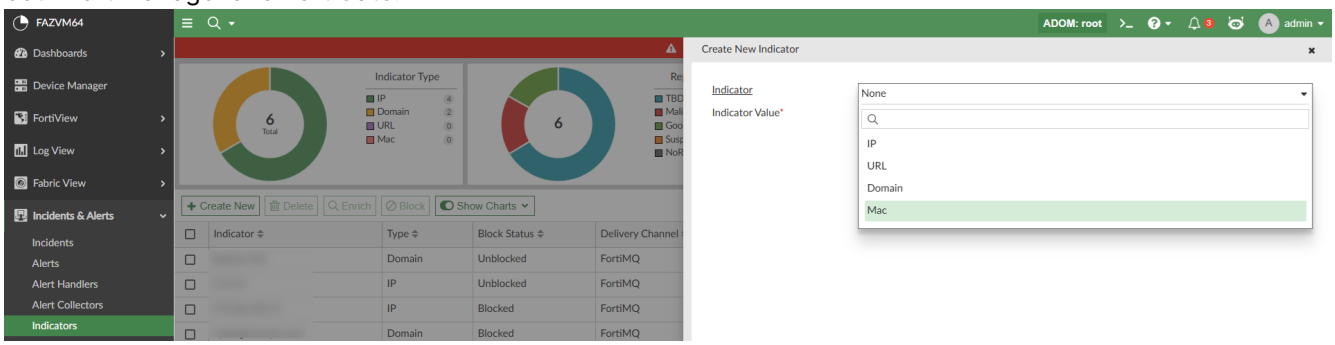


The policy in this example was setup to deny access to the above threat feeds. See below for the ping results:



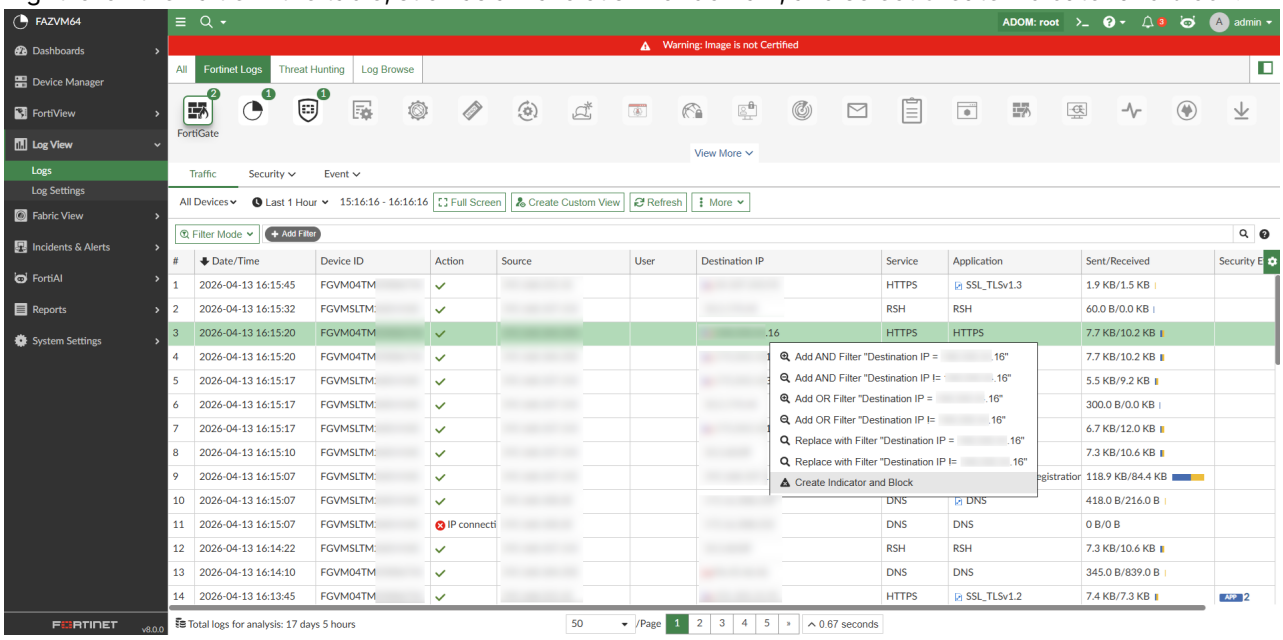
Unlike FortiManager, which operates at a global level, FortiMQ is ADOM-specific. Blocked indicators are applied only to FortiGate devices within the same FortiAnalyzer ADOM.

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*.



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
```

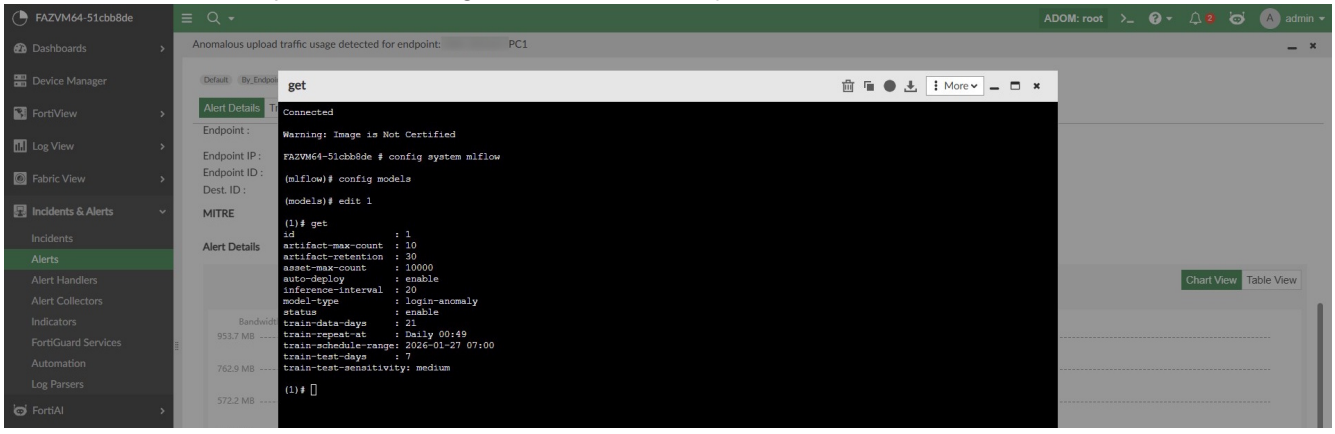
```
        next

    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: • Continuous training: `'YYYY-MM-DD HH:MM'` For example: `'2025-01-01 00:00'` • Bounded range: `'YYYY-MM-DD HH:MM -- YYYY-MM-DD HH:MM'` For example: `'2025-01-01 00:00 -- 2026-01-01 00:00'` Default: Start from current time (continuous).
train-repeat-at <string>	Training repeat schedule formats: • Daily: `'Daily HH:MM'` For example: `'Daily 02:00'` • Weekly: `'Weekly <Day> HH:MM'` For example: `'Weekly Monday 02:00'` or `'Weekly Mon 02:00'` • Monthly (day of month): `'Monthly <DD> HH:MM'` For example: `'Monthly 15 02:00'` (15th of each month) • Monthly (nth weekday): `'Monthly <N> <Day> HH:MM'` For example: `'Monthly 3 Monday 02:00'` (3rd Monday of each month) • Interval: `'<N>d'` For example: `'7d'` (every 7 days) 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. • `high`: High sensitivity. Uses strict criteria during testing, more assets in

Variable	Description
	exclusion list. • `low`: Low sensitivity. Uses lenient criteria during testing, fewer assets in exclusion list. • `medium`: Medium sensitivity. Balanced testing criteria, moderate asset in exclusion list.
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 Manually training the machine learning models and validating artifacts on page 26 to manually deploy the artifact.
inference-interval <integer>	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. Recommended values by model type: • login-anomaly: 20 minutes • traffic-download-anomaly: 60 minutes (must be multiple of 60) • traffic-upload-anomaly: 60 minutes (must be multiple of 60) Traffic models require inference-interval to be a multiple of 60.
artifact-retention <integer>	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.
artifact-max-count <integer>	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.

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

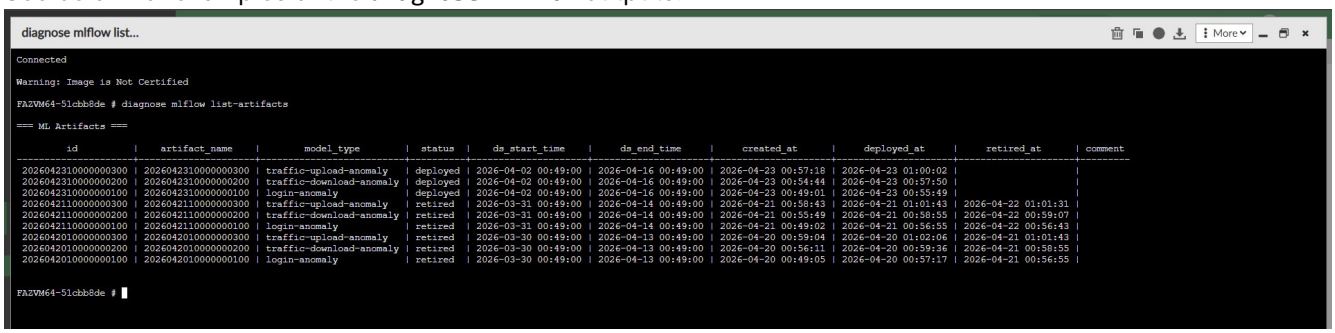


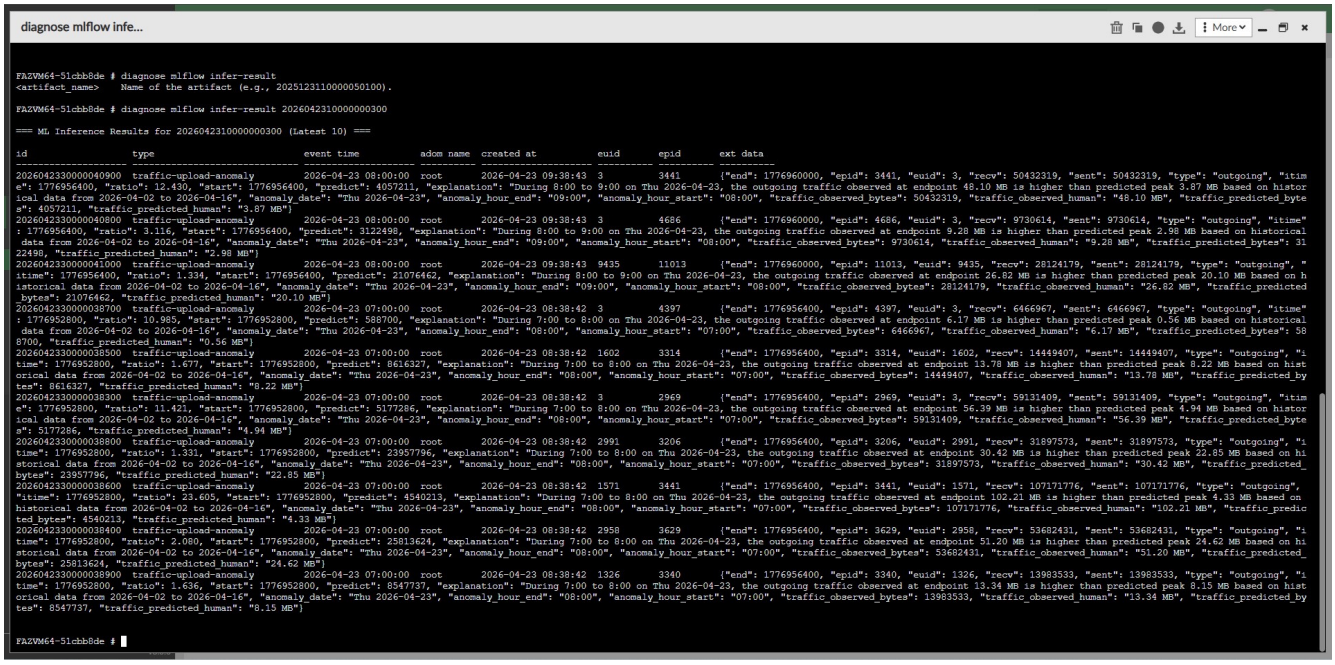
Monitoring the lifecycle of the machine learning models

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

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

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





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.

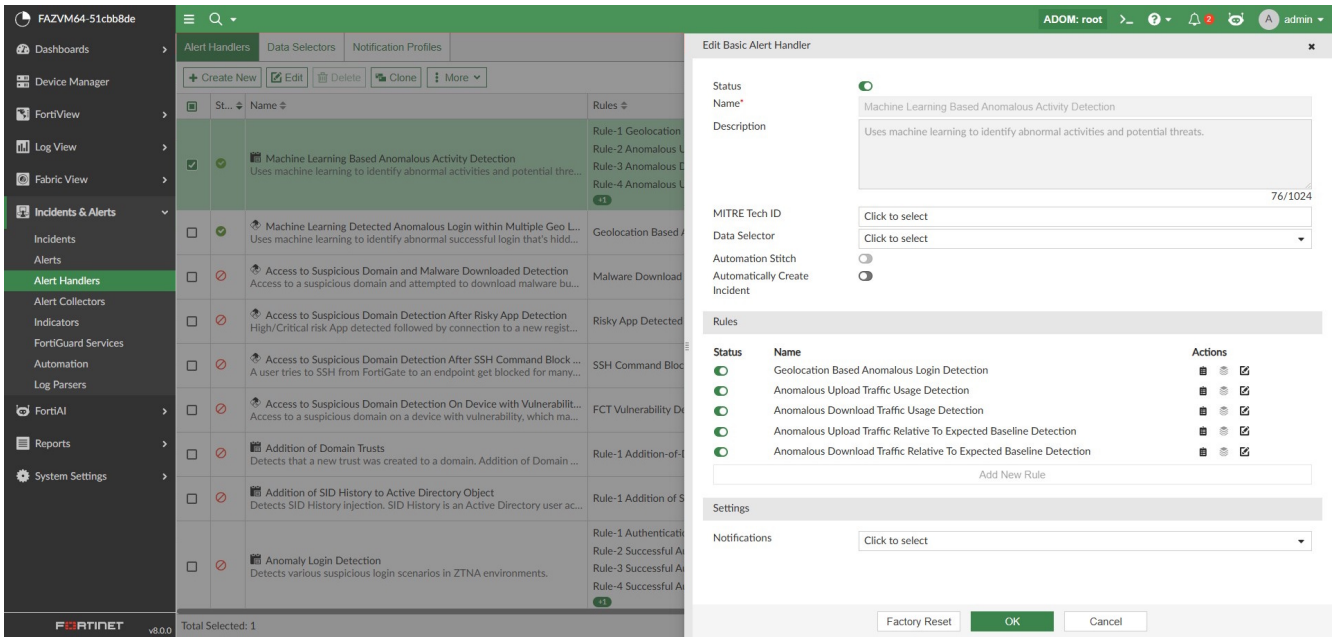
Command	Description
execute mlflow cancel <artifact_name>	Cancel artifact training.
execute mlflow delete <artifact_name>	Permanently delete artifact.
execute mlflow deploy <artifact_name>	Deploy artifact for active inference.

execute mlflow exclusion-list {artifact | model} {add | list | remove} <asset>	Manage ML exclusion-lists.
	• `artifact`: Artifact-level exclusion-list operations.
	  • `add`: Add asset to artifact exclusion-list.
	  • `list`: List exclusion-listed assets for artifact.
	  • `remove`: Remove asset from artifact exclusion-list.
	• `model`: Model-level exclusion-list operations.
	  • `add`: Add asset to model exclusion-list.
	  • `list`: List exclusion-listed assets for model type.
	  • `remove`: Remove asset from model exclusion-list.

execute mlflow test <artifact_name> <start_time> <end_time>	Test/validate artifact on specified time range. • `<start_time> <end_time>`: Start time and end time can be entered in the following format: `YYYY-MM-DD HH:MM`.
execute mlflow train <model_type> <start_time> <end_time> [train-assets-limit]	Train the machine learning model on specified time range. • `<model_type>`: Model type includes `login-anomaly`, `traffic-download-anomaly`, `traffic-upload-anomaly`. • `<start_time> <end_time>`: Start time and end time can be entered in the following format: `YYYY-MM-DD HH:MM`. • `[train-assets-limit]`: Optionally, set the maximum number of assets to train (1 - 100000). Example: `execute mlflow train login-anomaly '2026-02-05' '2026-05-05'`
execute mlflow undeploy <artifact_name>	Undeploy artifact from active inference.

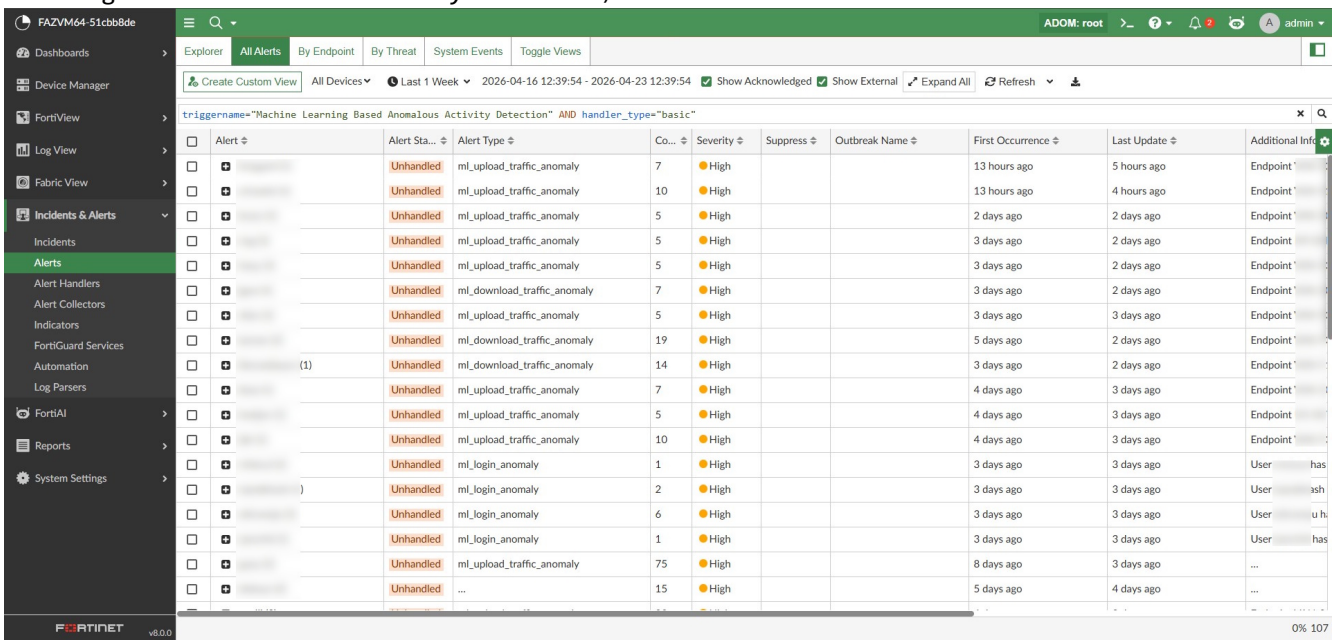
Alert Handler: Machine Learning Based Anomalous Activity Detection

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



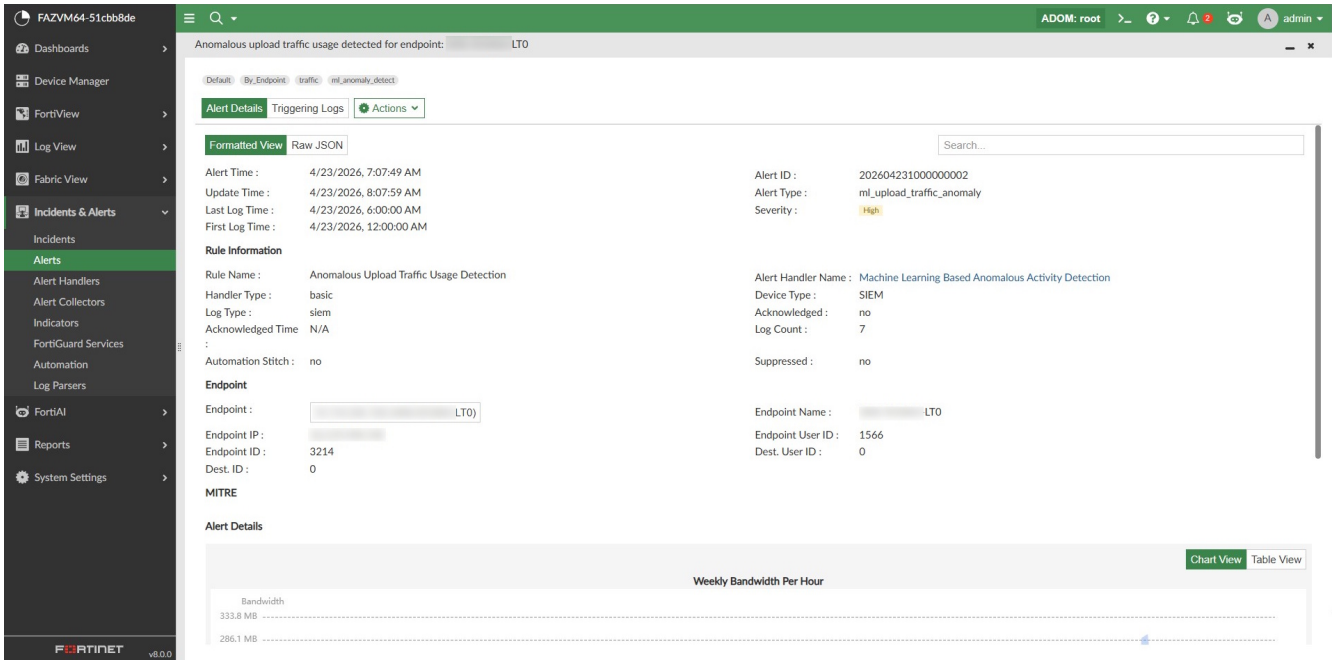
Once triggered, an alert is generated, providing the analyst with context regarding the deviation. For example, an alert highlighting that an upload volume exceeded the user's specific 90-day behavioral pattern.

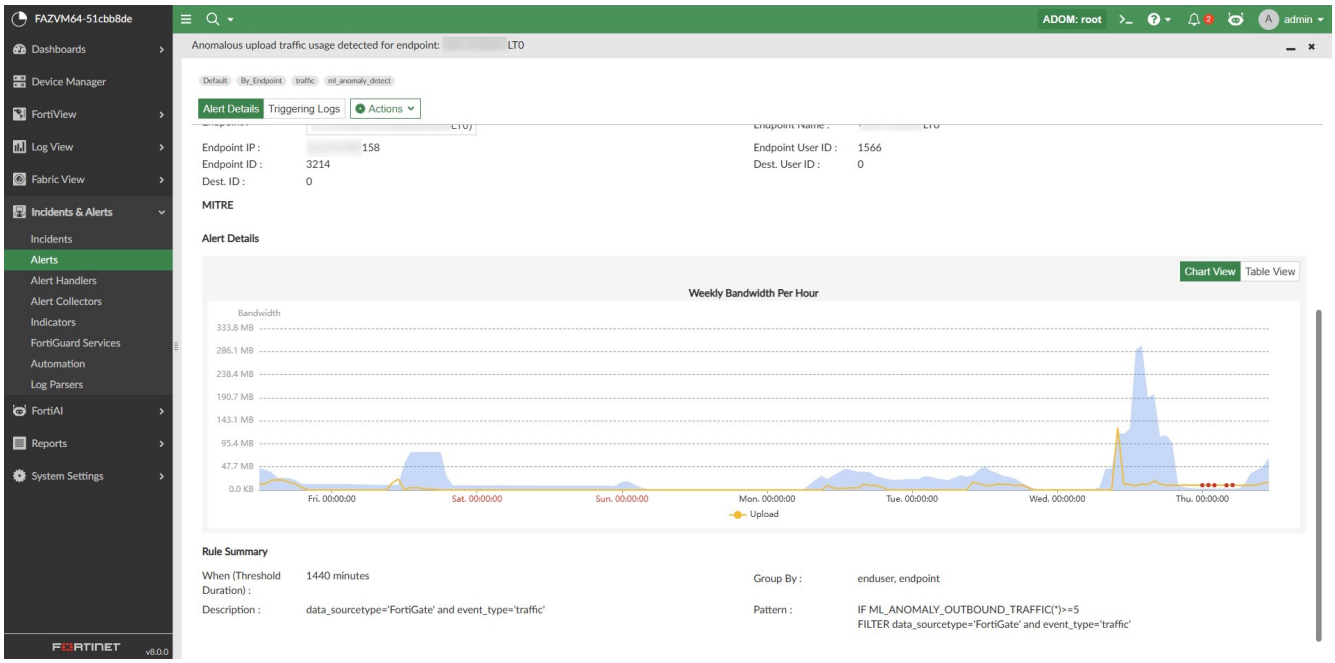
The alerts can be found in *Incidents & Alerts* > *Alerts* > *All Alerts*; filter by the triggered alert handler (`Machine Learning Based Anomalous Activity Detection`).



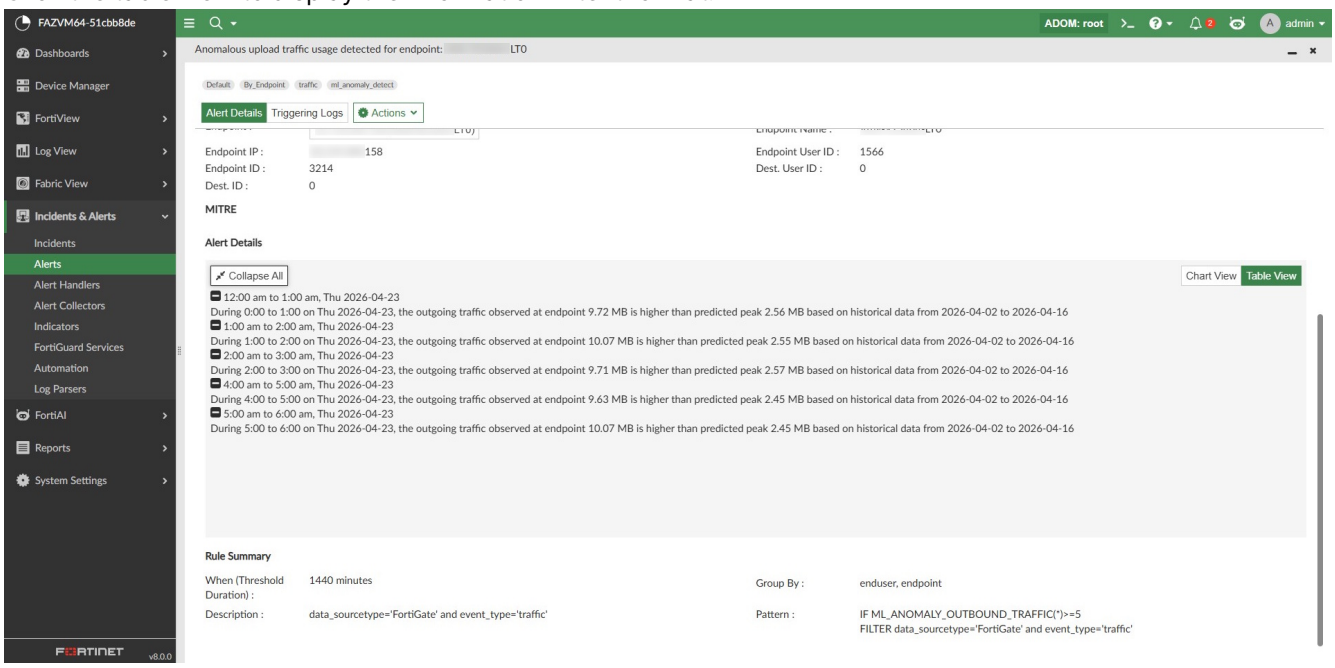
Click the alerts to view their details. See examples below.

Example: Anomalous upload traffic usage

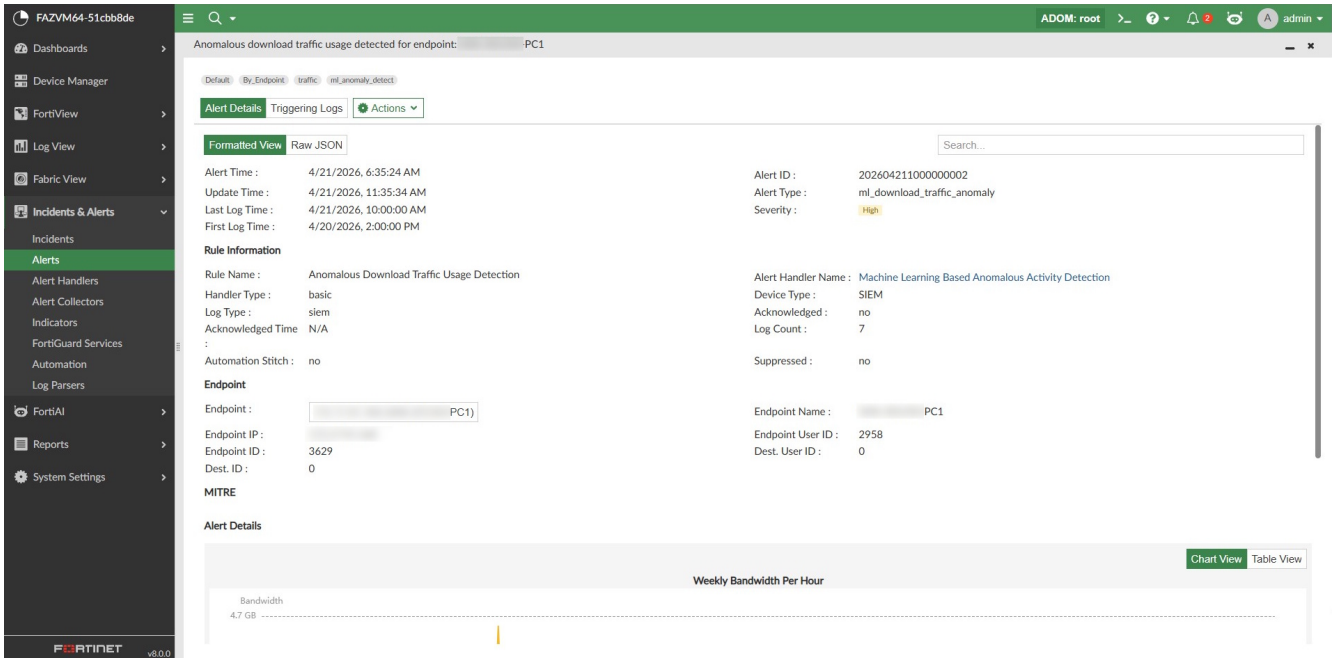


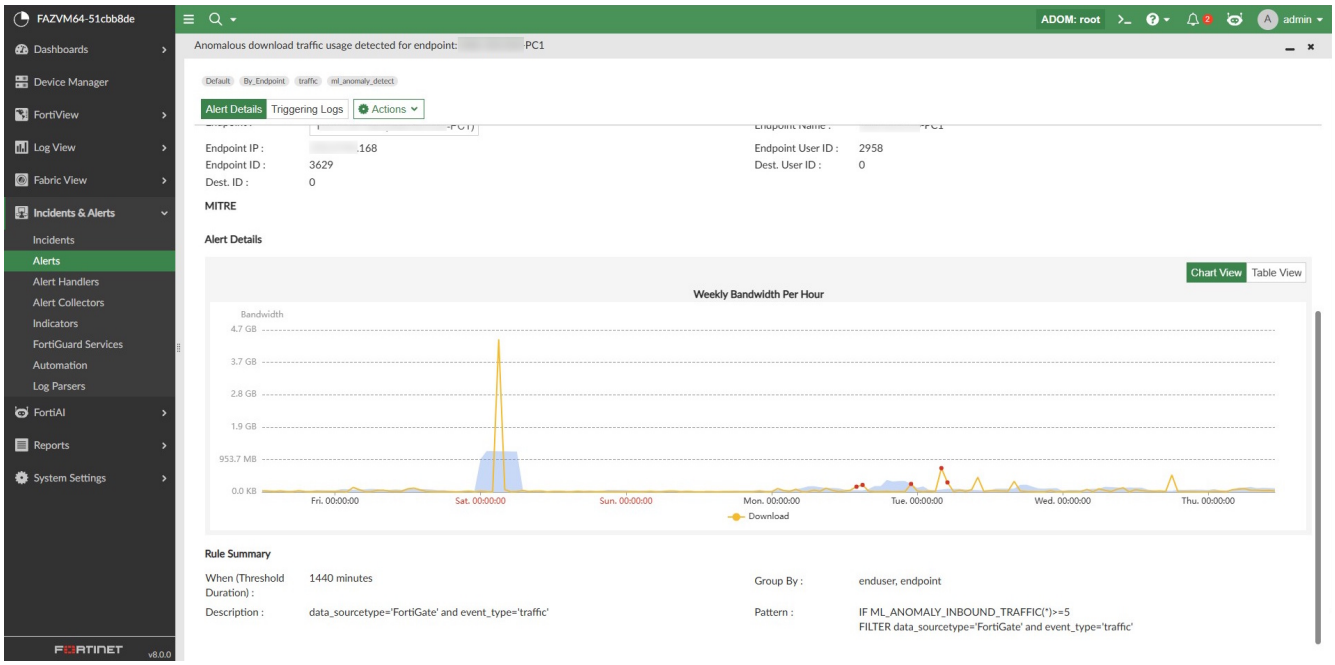


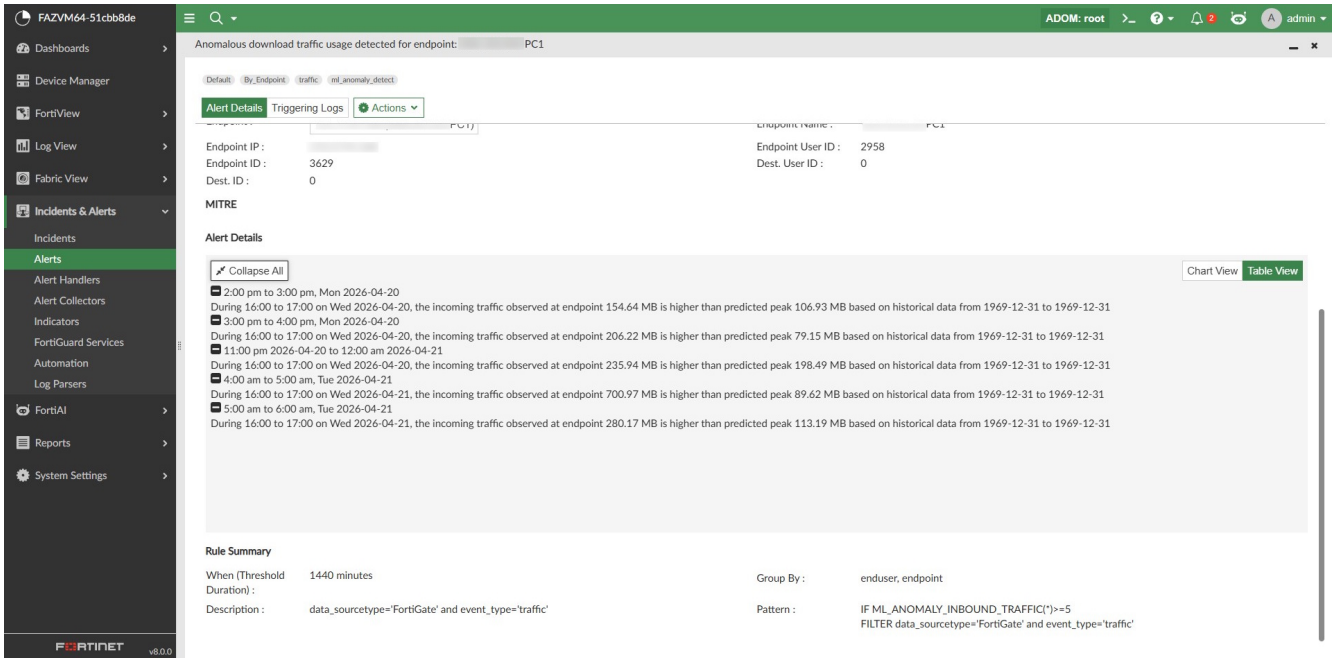
Click the table view to display the information in text format:



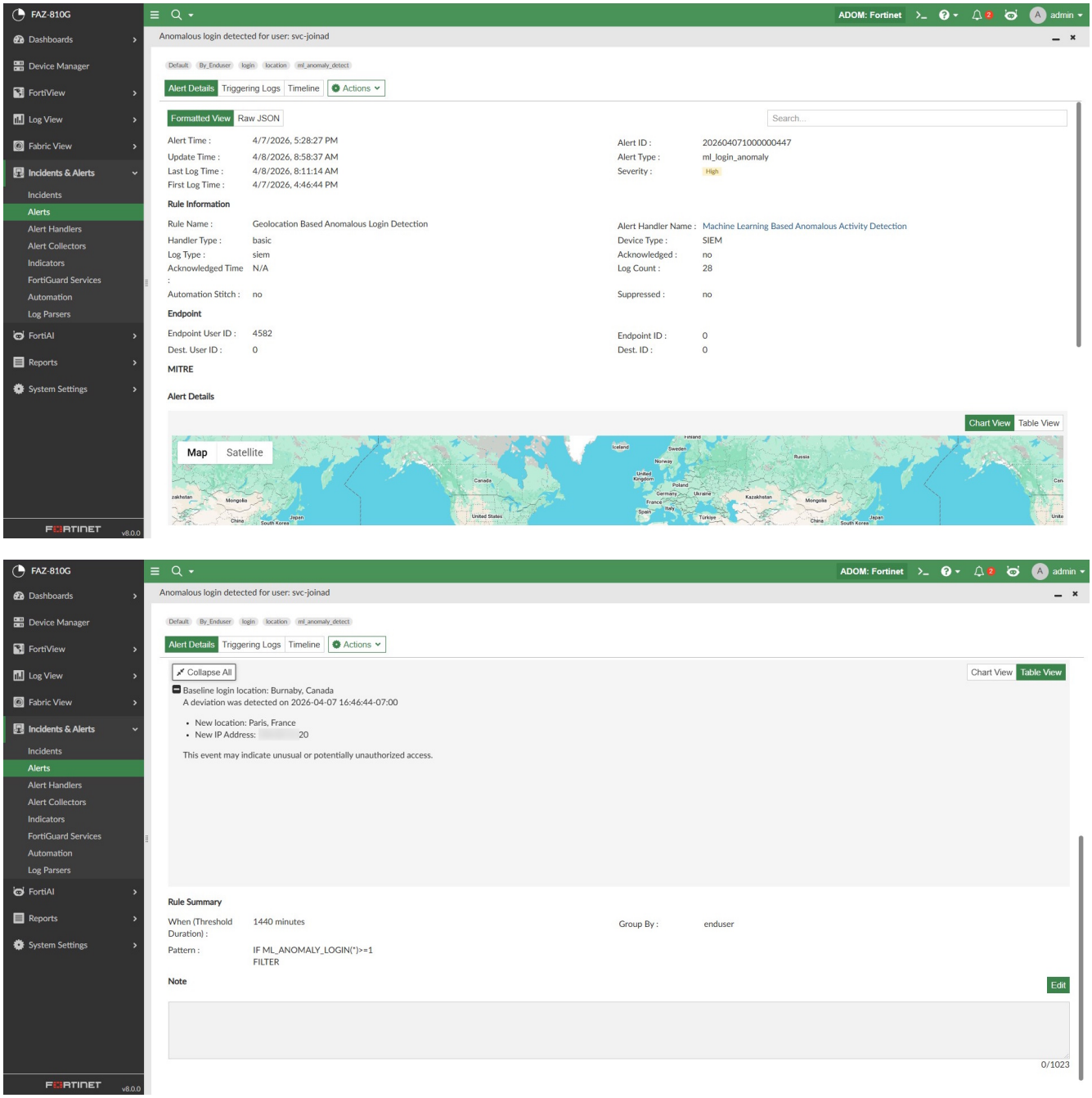
Example: Anomalous download traffic usage




FAZVM64-51cbb8de
ADOM: root
admin
Dashboards
Device Manager
FortiView
Log View
Fabric View
Incidents & Alerts
Incidents
Alerts
Alert Handlers
Alert Collectors
Indicators
FortiGuard Services
Automation
Log Parsers
FortiAI
Reports
System Settings
Anomalous download traffic usage detected for endpoint: PC1
Default By_Endpoint traffic ml_anomaly_detect
Alert Details
Triggering Logs
Actions
Endpoint IP : .168
Endpoint ID : 3629
Dest. ID : 0
Endpoint User ID : 2958
Dest. User ID : 0
MITRE
Alert Details
Chart View
Table View
Weekly Bandwidth Per Hour
Bandwidth
4.7 GB
3.7 GB
2.8 GB
1.9 GB
953.7 MB
0.0 KB
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
Download
Rule Summary
When (Threshold Duration) : 1440 minutes
Group By : enduser, endpoint
Description : data_sourcetype='FortiGate' and event_type='traffic'
Pattern : IF ML_ANOMALY_INBOUND_TRAFFIC(*)>=5
FILTER data_sourcetype='FortiGate' and event_type='traffic'
v8.0.0


FAZVM64-51cbb8de
ADOM: root
admin
Dashboards
Device Manager
FortiView
Log View
Fabric View
Incidents & Alerts
Incidents
Alerts
Alert Handlers
Alert Collectors
Indicators
FortiGuard Services
Automation
Log Parsers
FortiAI
Reports
System Settings
Anomalous download traffic usage detected for endpoint: PC1
Default By_Endpoint traffic ml_anomaly_detect
Alert Details
Triggering Logs
Actions
Endpoint IP :
Endpoint ID : 3629
Dest. ID : 0
Endpoint User ID : 2958
Dest. User ID : 0
MITRE
Alert Details
Collapse All
Chart View
Table View
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
Group By : enduser, endpoint
Description : data_sourcetype='FortiGate' and event_type='traffic'
Pattern : IF ML_ANOMALY_INBOUND_TRAFFIC(*)>=5
FILTER data_sourcetype='FortiGate' and event_type='traffic'
v8.0.0

Example: Anomalous login



Log and Report

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

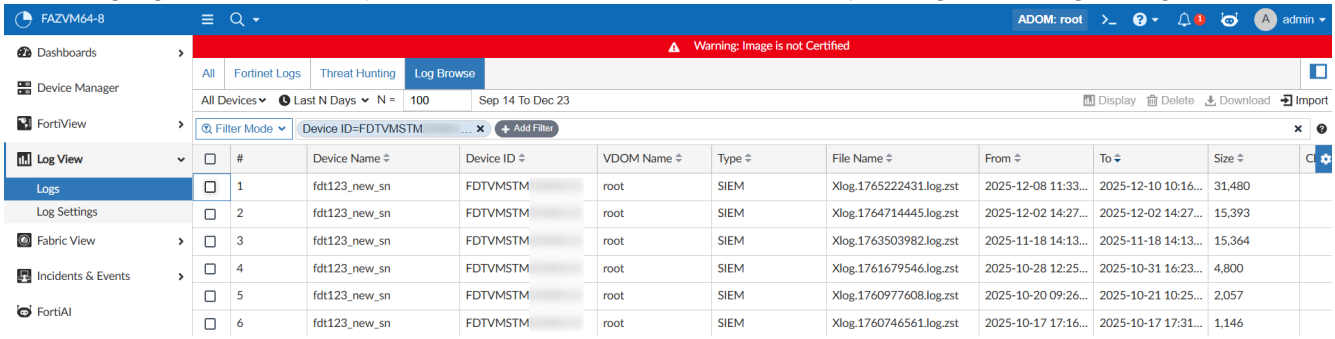
Logging

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

FortiData incident support

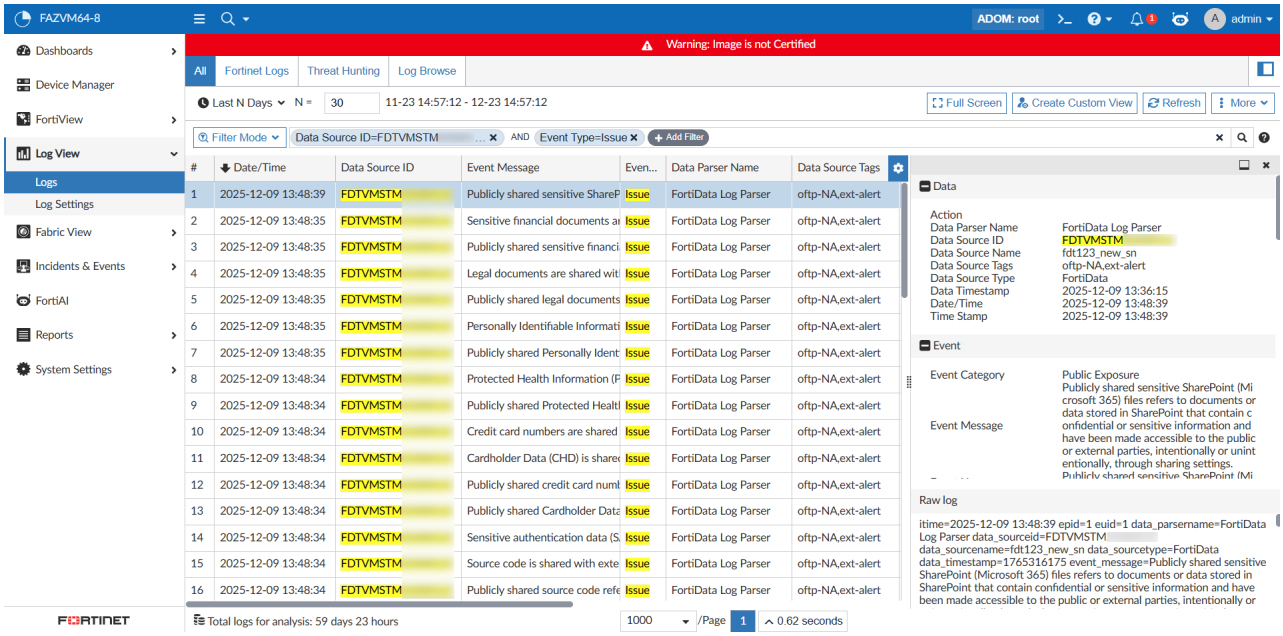
FortiData is now a supported device for FortiAnalyzer.

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*.

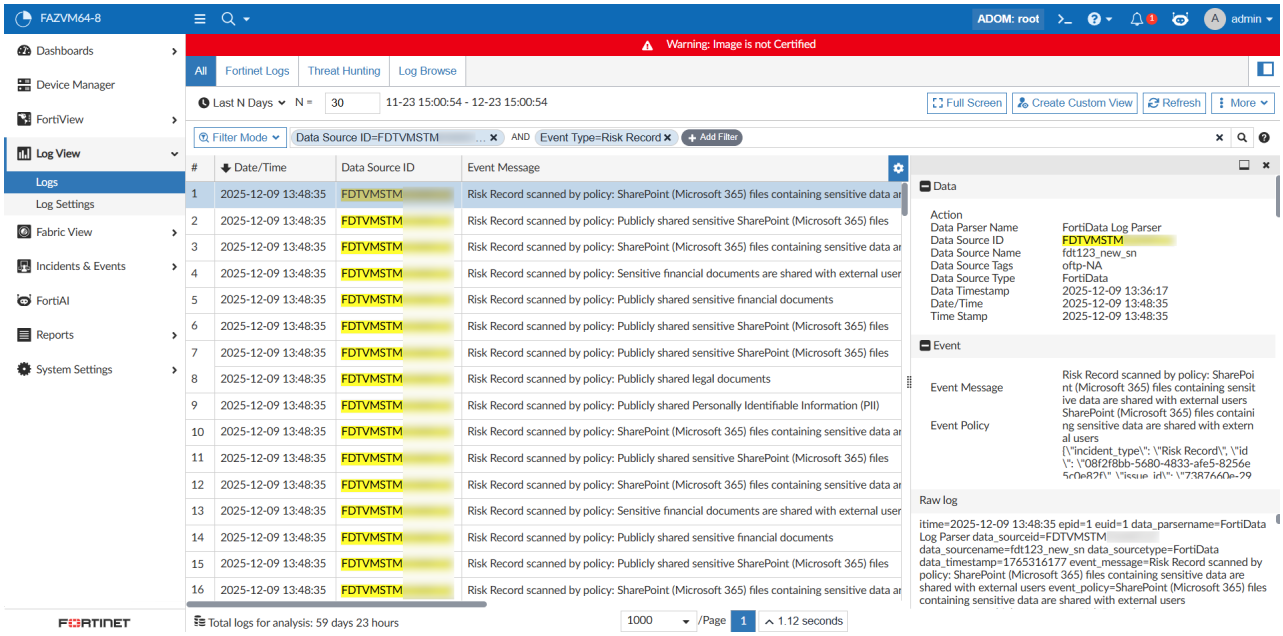


These logs will insert into the FortiAnalyzer SIEM database (siemdb), so the logs can be found in *Log View* > *Logs* > *All*. The following three types of incident logs are currently supported in FortiAnalyzer 8.0.0:

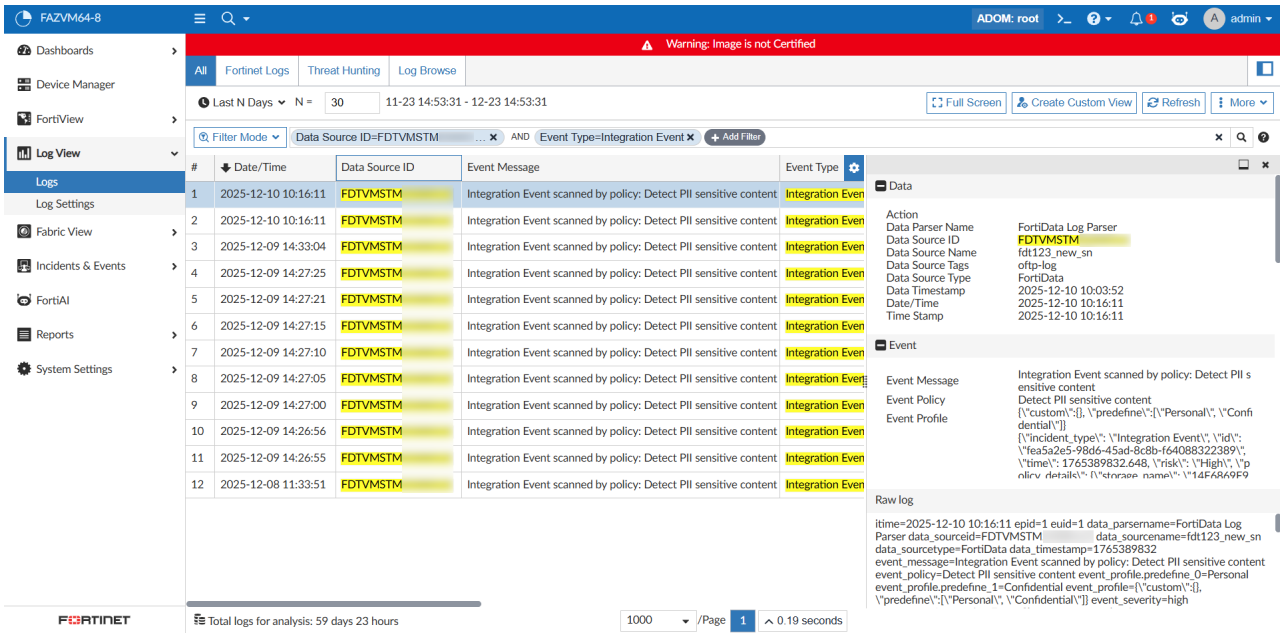
- Issue



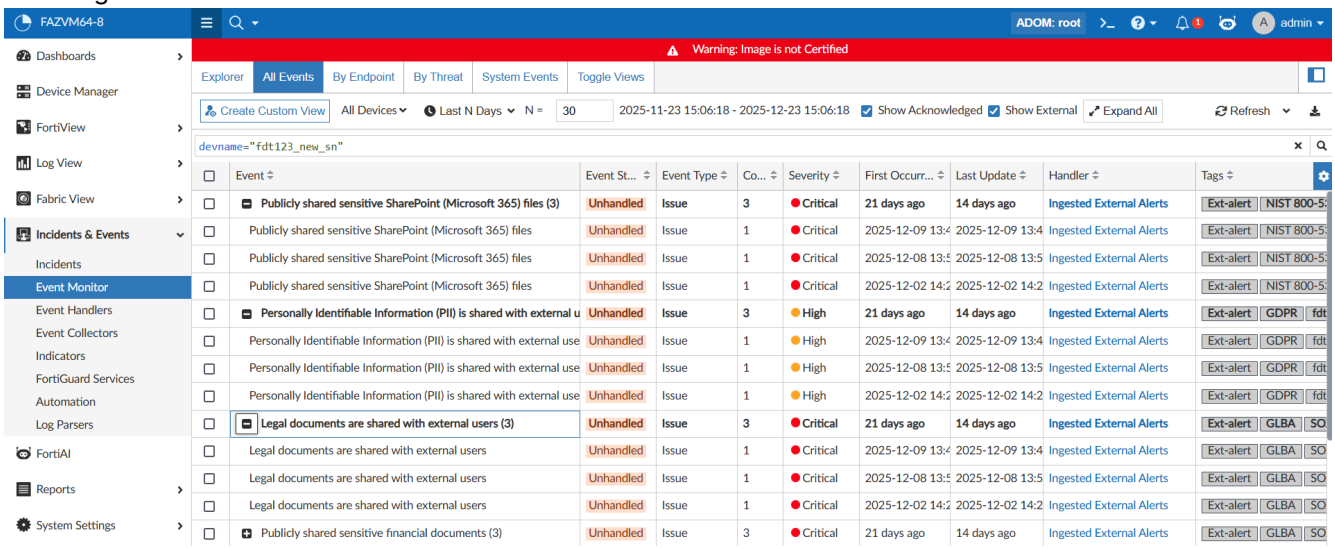
- Risk Record



- 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
Name	Enter a name for the output profile.
Type	Select *Azure Logs Ingestion*.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Configuration</td><td>Click Use Default to use the default Fluentd configuration. The default configuration indicates that:

<pre># The following six parameters are required.
tenant_id #<TENANT_ID>
client_id #<CLIENT_ID>
client_secret #<CLIENT_SECRET>
dce_url #<DCE_URL>
dcr_id #<DCR_ID>
table_name #<TABLE_NAME></pre></td></tr>
<tr><td>Field | Value | Action</td><td>Configure the required parameters according to your Azure portal.
For example:

<table><tr><th>Field</th><th>Value</th></tr><tr><td>TENANT_ID</td><td>Enter the tenant ID for the Azure portal.</td></tr><tr><td>CLIENT_ID</td><td>Enter the client ID for the Azure portal.</td></tr><tr><td>CLIENT_SECRET</td><td>Enter the client secret for the Azure portal.</td></tr><tr><td>DCE_URL</td><td>Enter the Data Collection Endpoint URL.</td></tr><tr><td>DCR_ID</td><td>Enter the Data Collection Rule ID.</td></tr><tr><td>TABLE_NAME</td><td>Enter the custom table name from the Azure portal.</td></tr></table></td></tr>
</table>

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

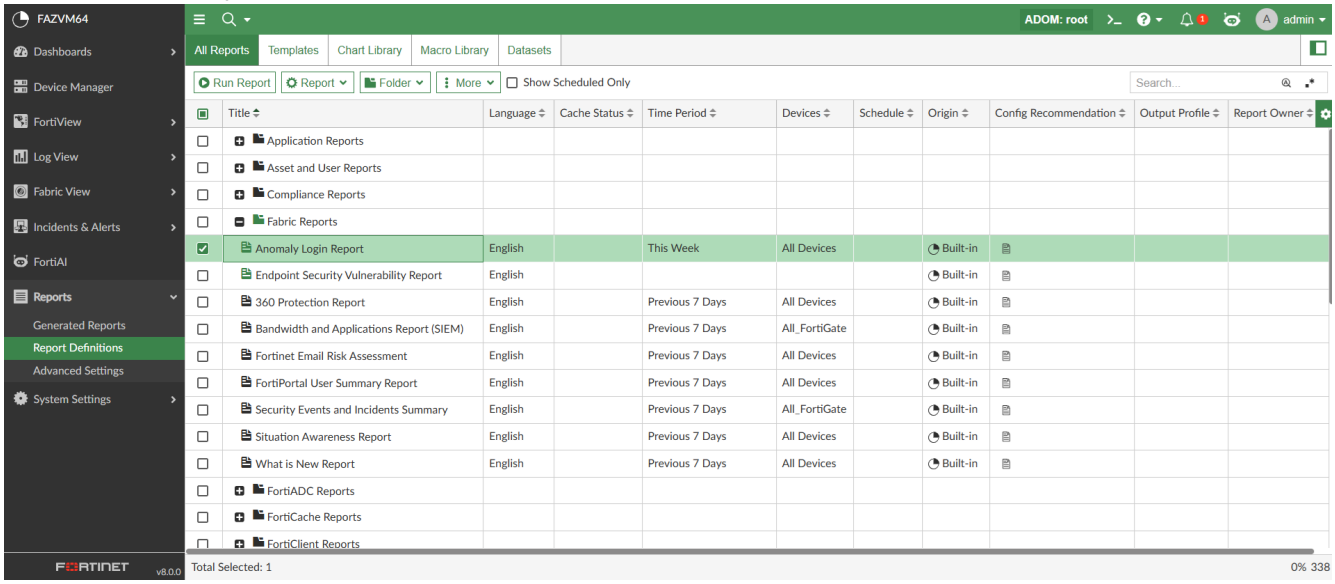
This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- ZTNA login alert handlers

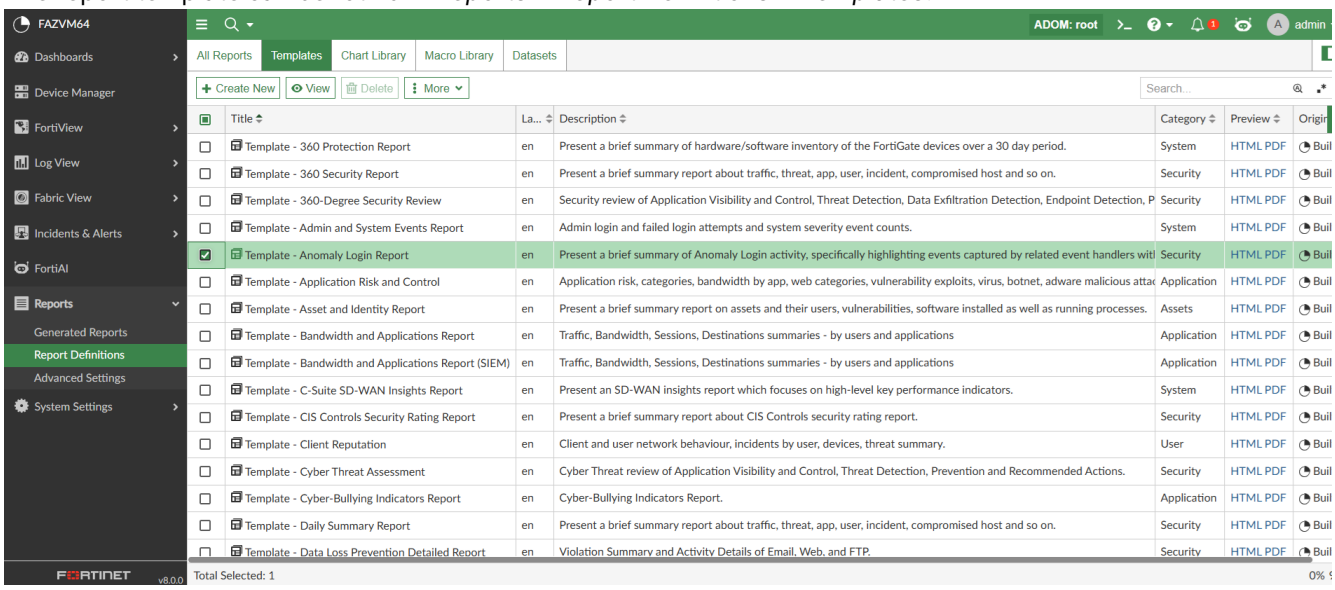
The new *Anomaly Login Report* provides a comprehensive overview of security events involving remote users and devices accessing office resources through Zero Trust Network Access (ZTNA). The report examines user behavior, including concurrent access with multiple devices, unusual login locations or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

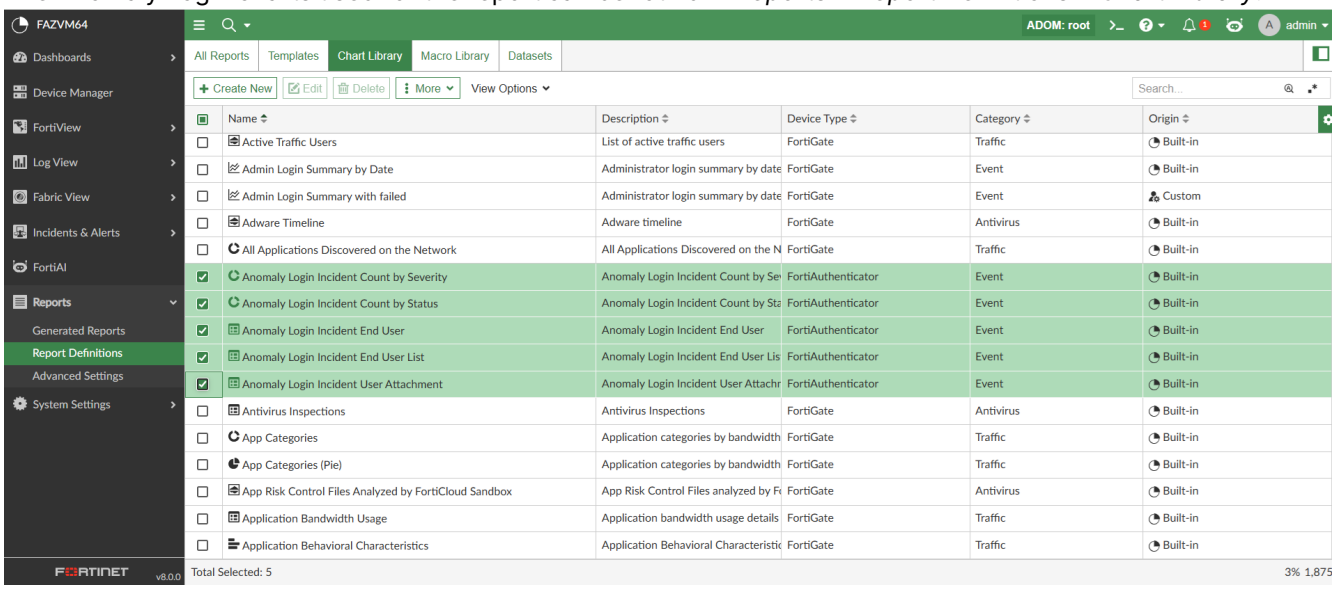
The *Anomaly Login Report* is a global report, and it can be found in the Fabric Reports folder in *Reports > Report Definitions > All Reports*.



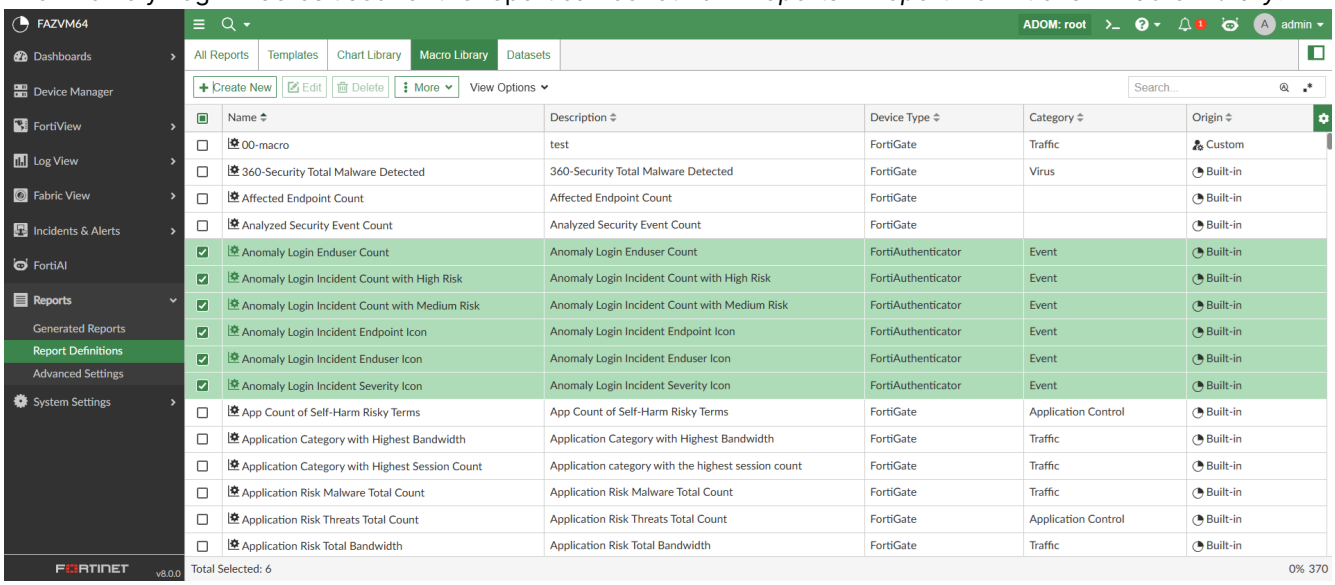
The report template can be found in *Reports > Report Definitions > Templates*.



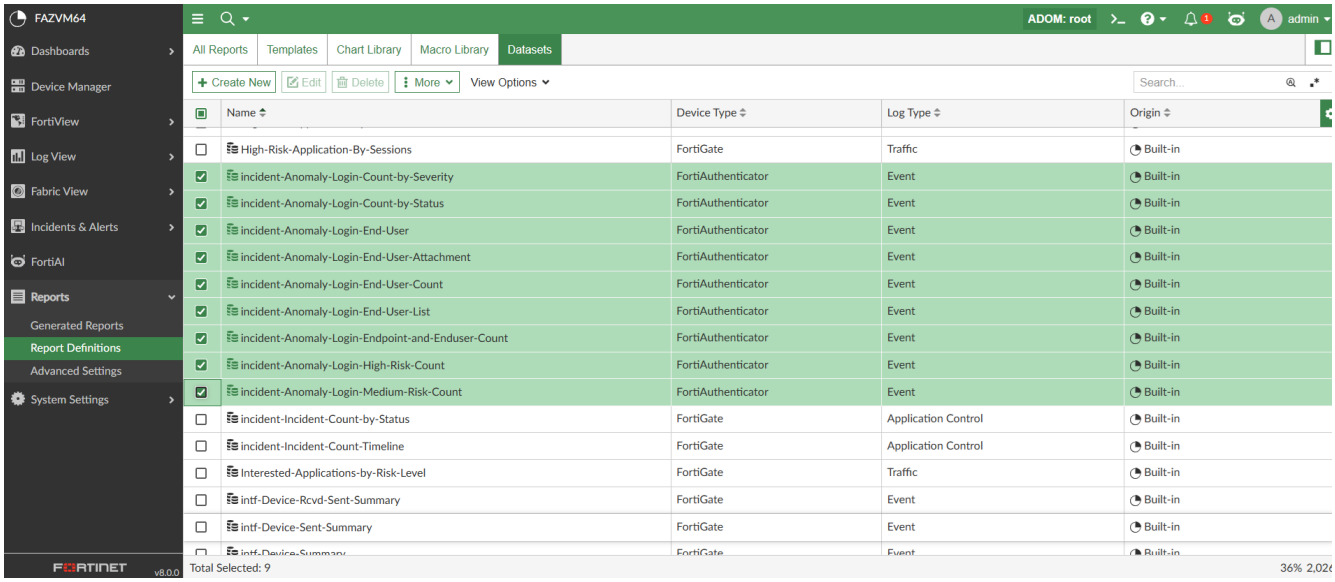
The Anomaly Login charts used for the report can be found in *Reports > Report Definitions > Chart Library*.



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



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



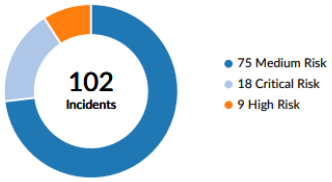
Below is a sample of some pages from the report in PDF format.

EXECUTIVE SUMMARY

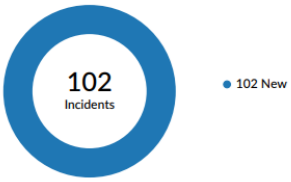
The report provides a comprehensive overview of security events involving remote users and devices accessing office resources through Zero Trust Network Access (ZTNA). It examines user behavior, including concurrent access with multiple devices, unusual login locations or times, access to atypical resources, 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

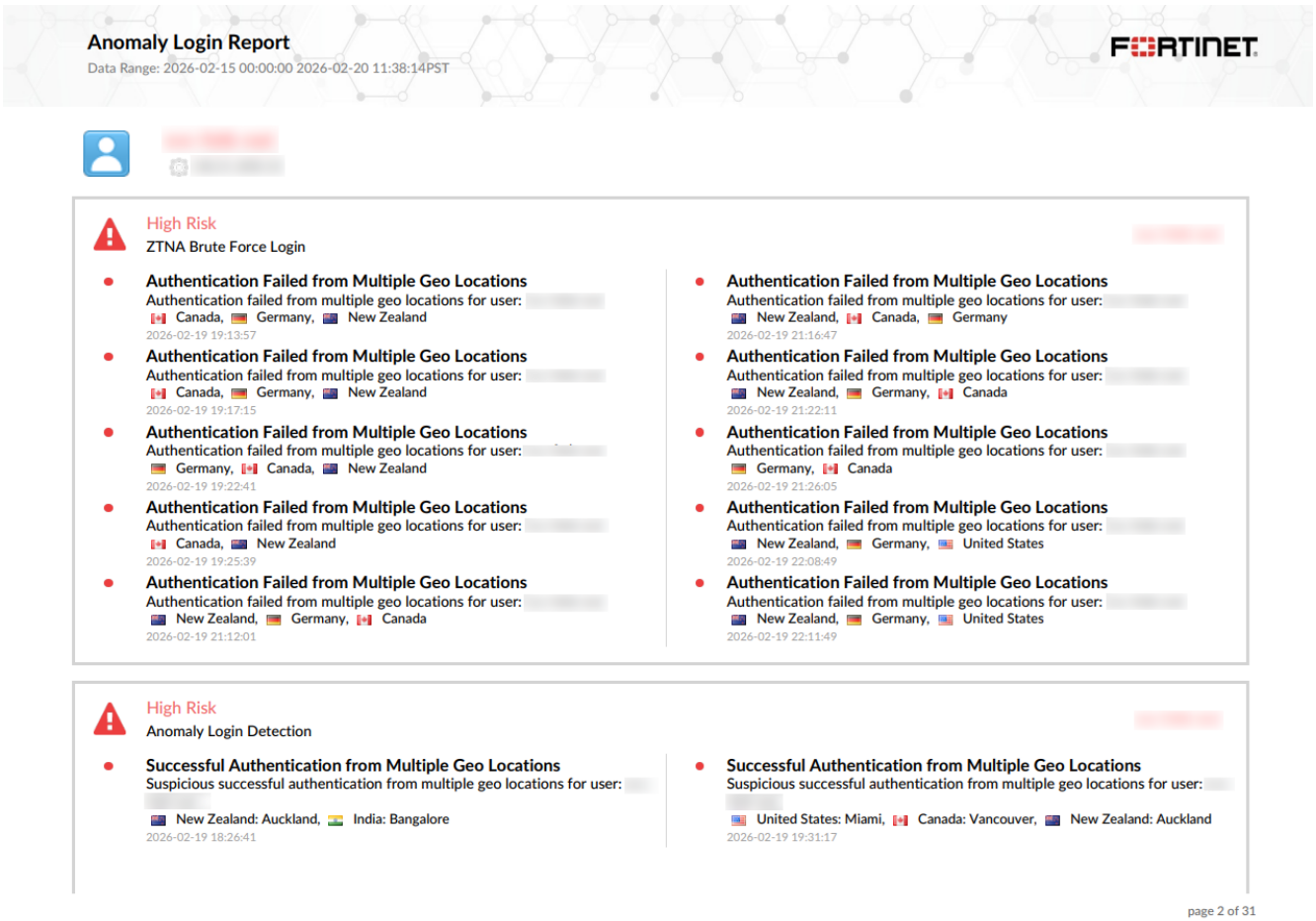
INCIDENT SEVERITY



INCIDENT STATUS



page 1 of 31



FortiDeceptor incident report

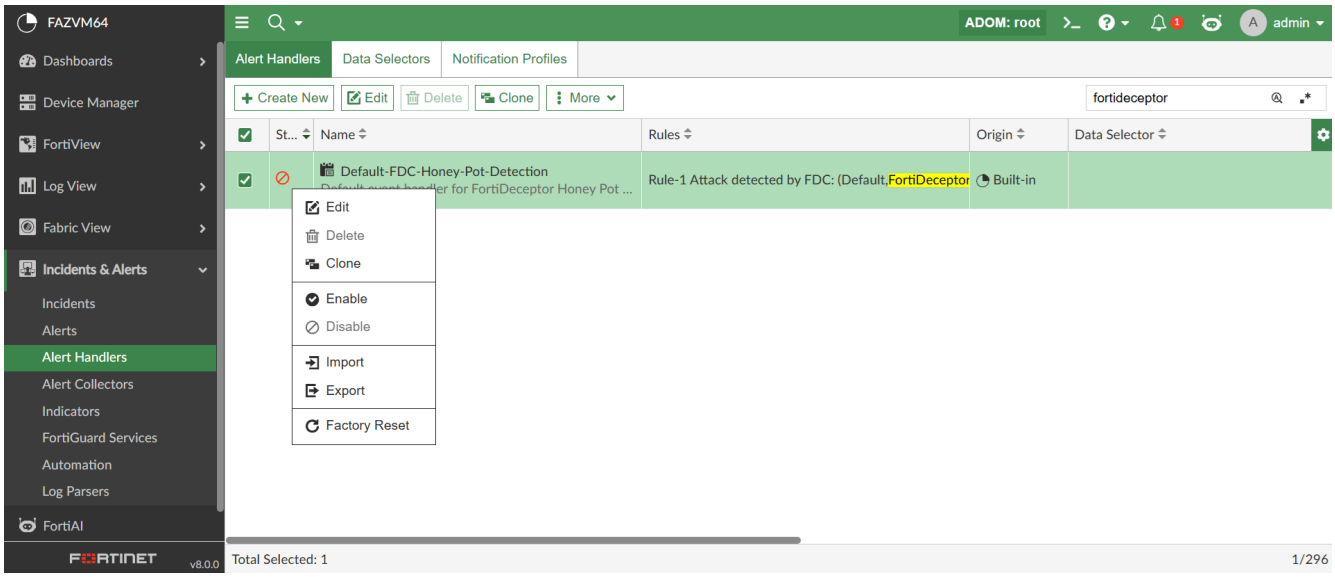
This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- Using the template - FortiDeceptor incident report

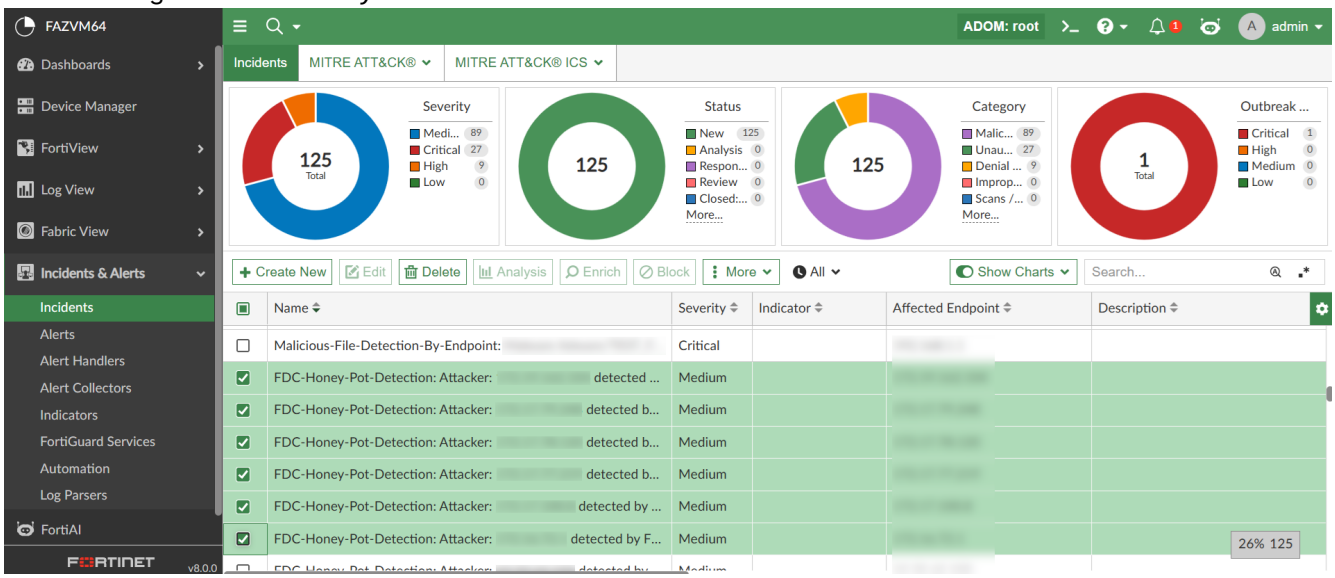
The new *FortiDeceptor Incident Report* lists *Critical* and *High* risk incidents triggered by an alert handler. The report includes the attacker IP and the victim IP, user, port, incident ID, and more so for SOC analysts to use the report effectively for incident triage and response.

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* >

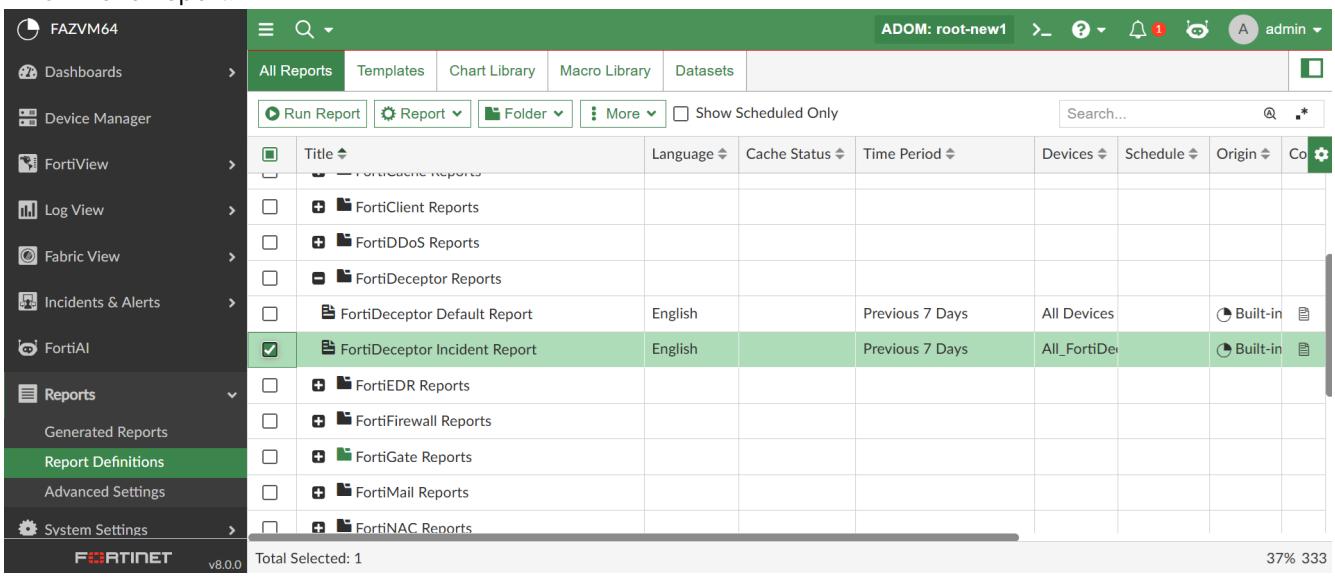
Alert Handlers.



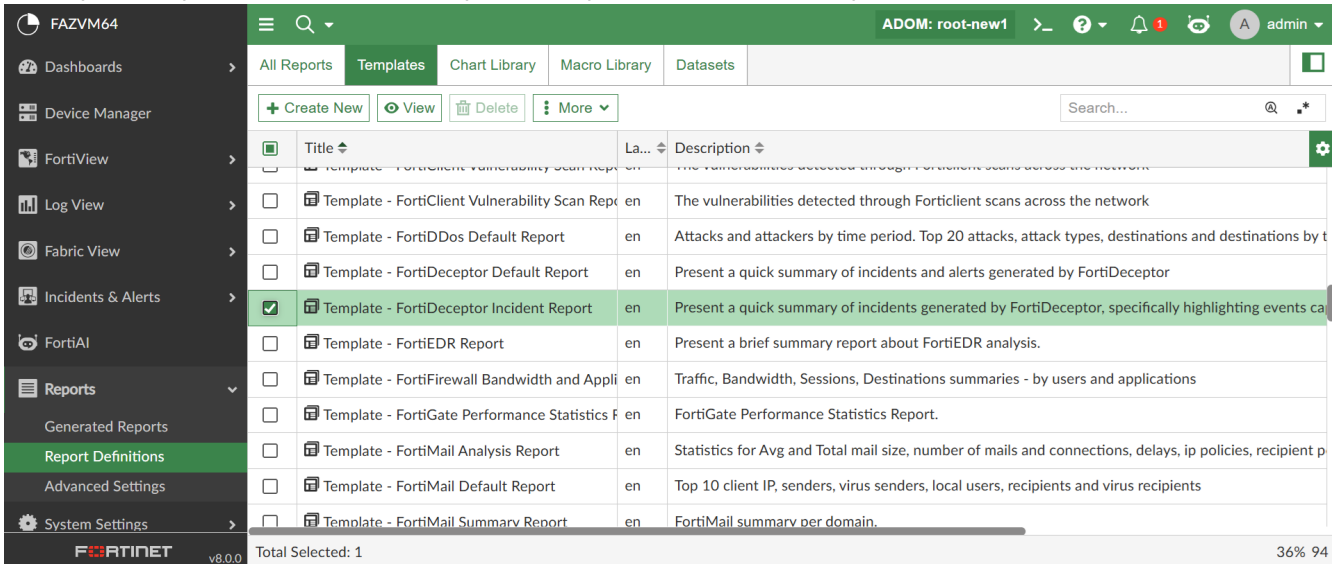
Incidents triggered by the alert handler can be found in *Incidents & Alerts* > *Incidents*. The *Name* of the related incidents begin with `FDC-Honey-Pot-Detection`.



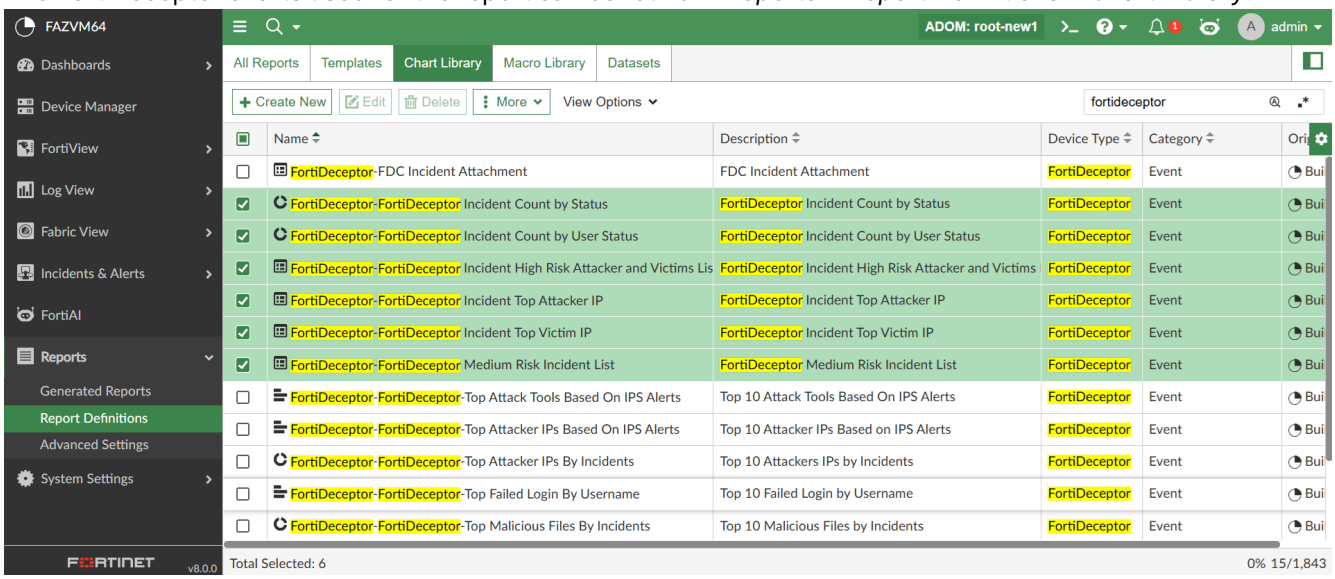
The report can be found in the FortiDeceptor Reports folder in *Reports* > *Report Definitions* > *All Reports*. It is an ADOM-level report.



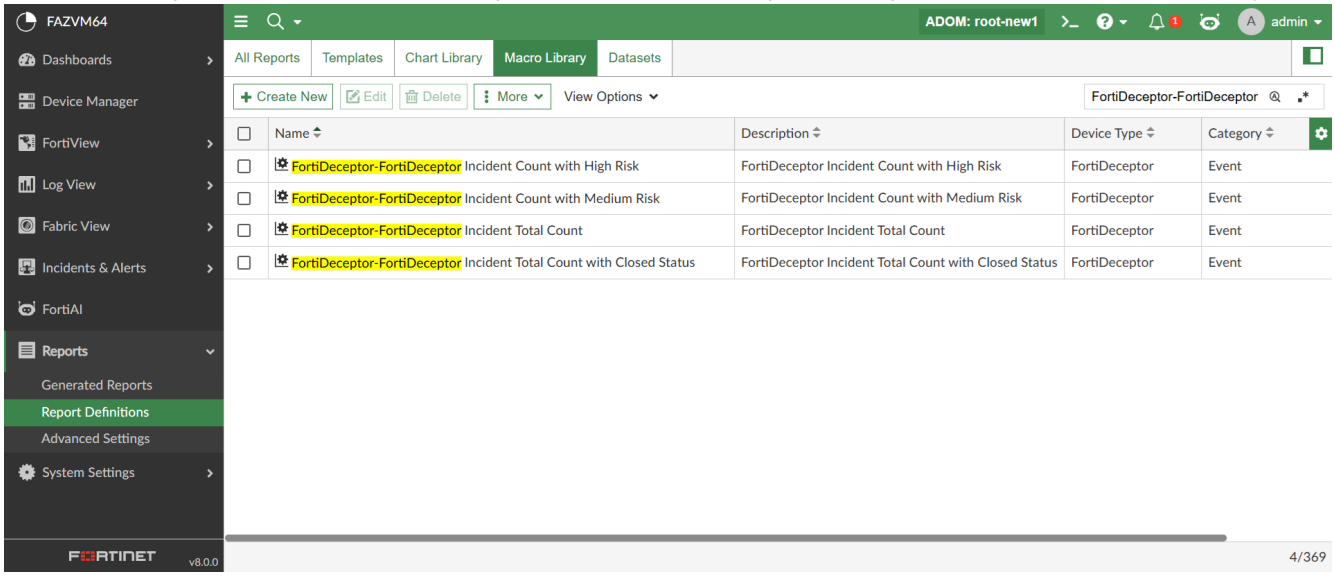
The report template can be found in *Reports* > *Report Definitions* > *Templates*.



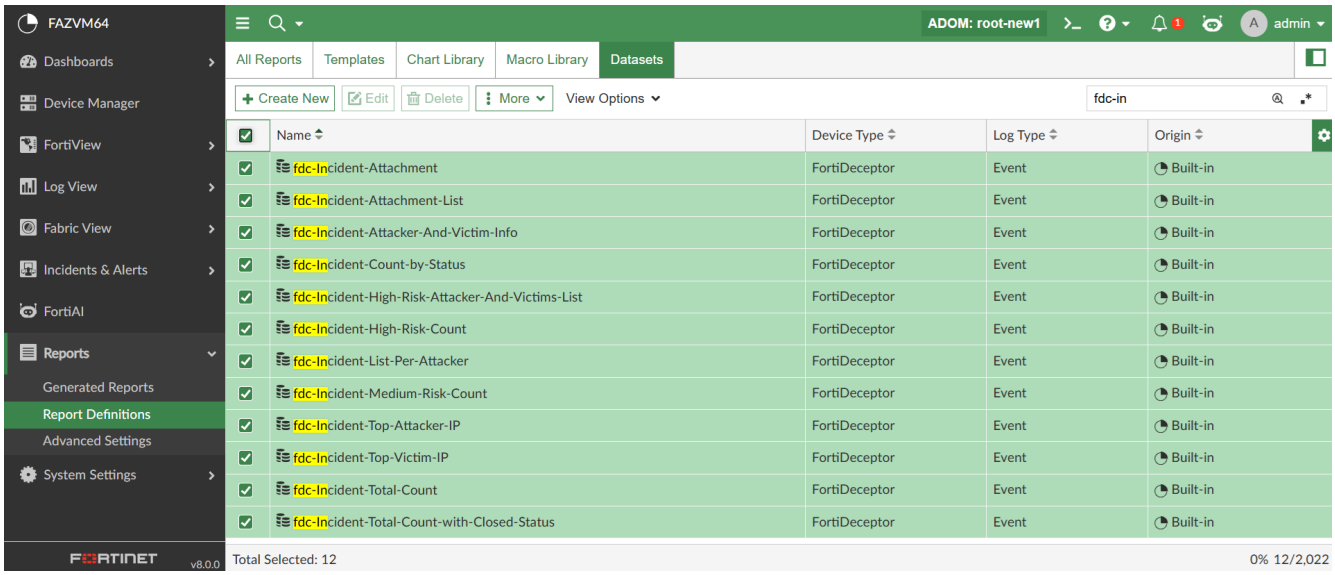
The FortiDeceptor charts used for the report can be found in *Reports > Report Definitions > Chart Library*.



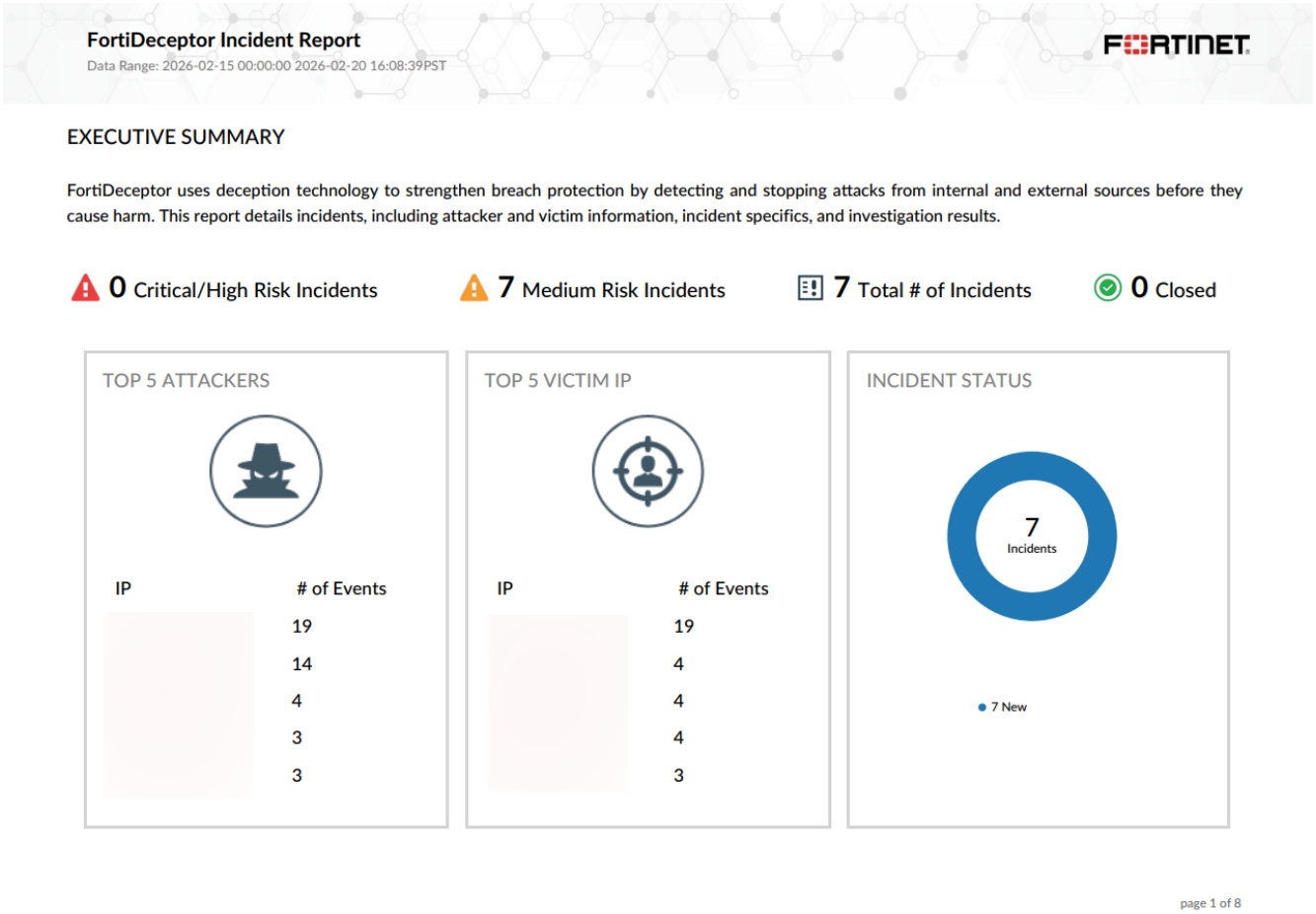
The FortiDeceptor macros used for the report can be found in *Reports > Report Definitions > Macro Library*.

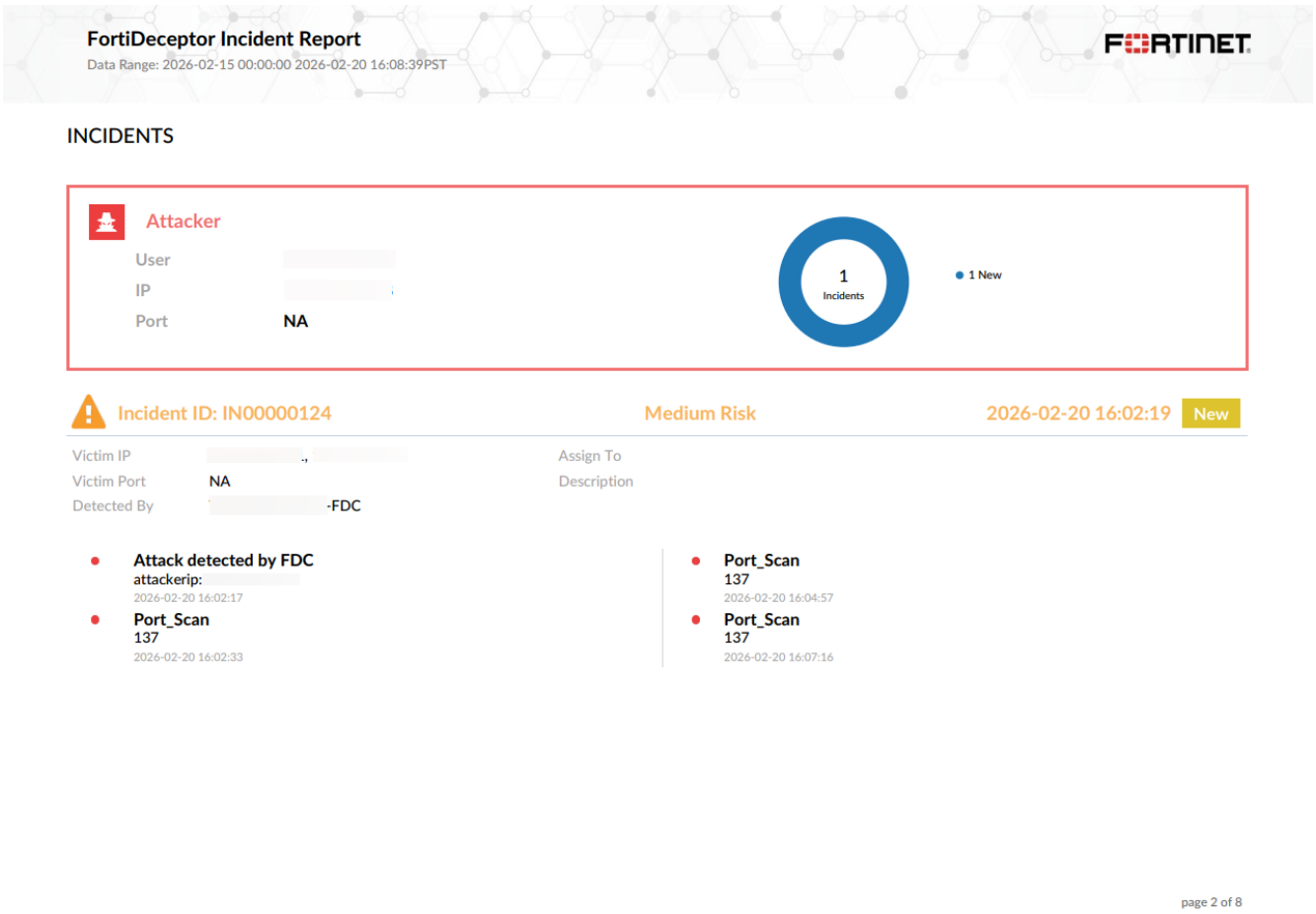


The FortiDeceptor datasets (`fdc-Incident`) used for the report can be found in *Reports* > *Report Definitions* > *Datasets*.



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





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

FORTINET

INCIDENTS

Attacker

User
IP
Port NA

1 Incidents

1 New

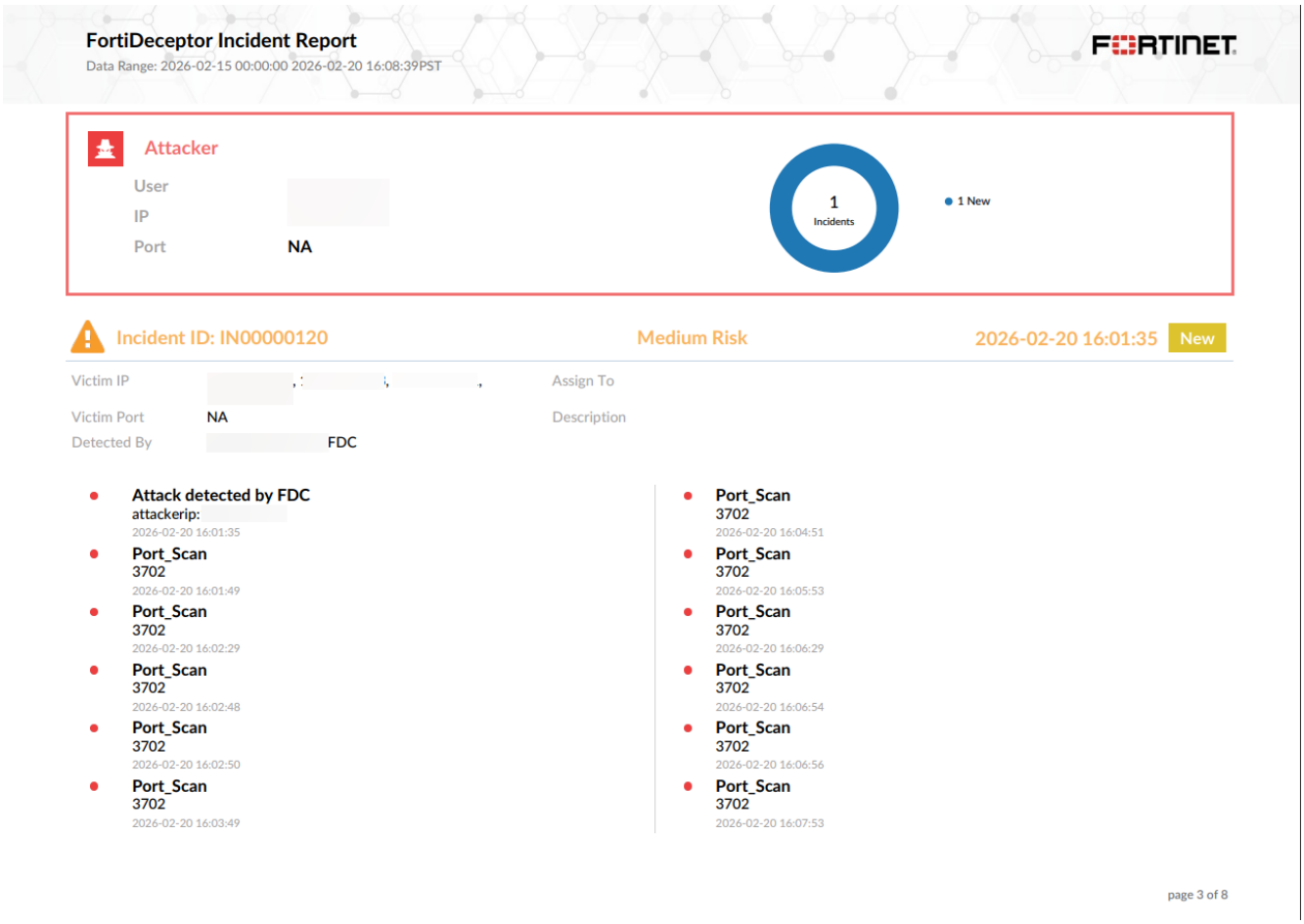
Incident ID: IN00000124 Medium Risk 2026-02-20 16:02:19 New

Victim IP
Victim Port NA
Detected By -FDC

Assign To
Description

- Attack detected by FDC
  attackerip:
  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

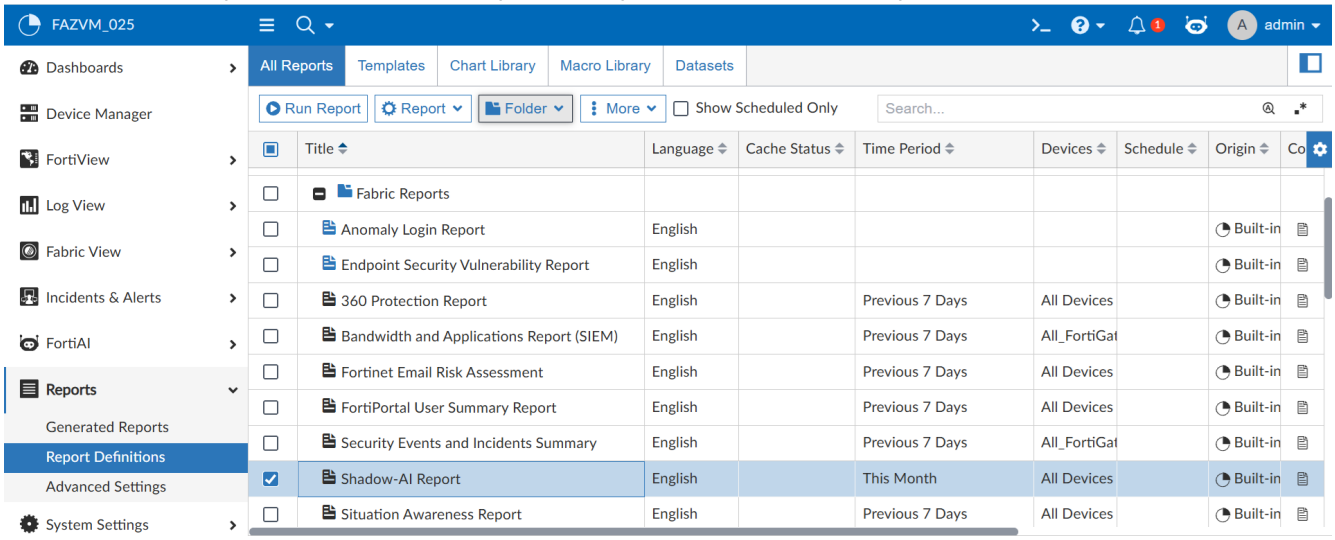
page 2 of 8



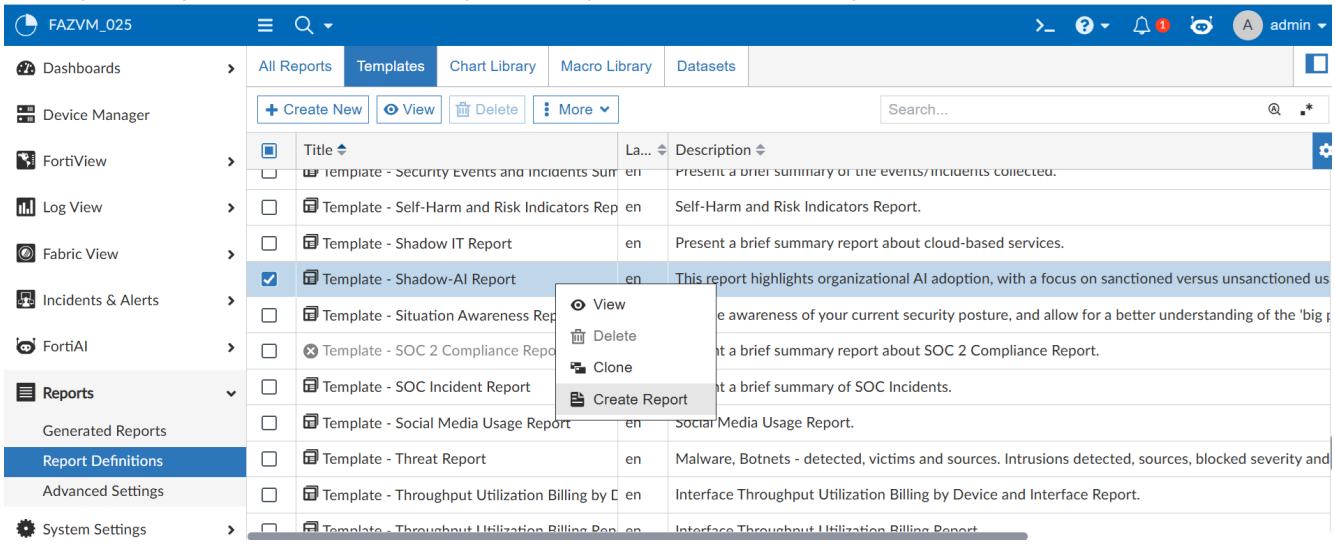
Shadow-AI report

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.

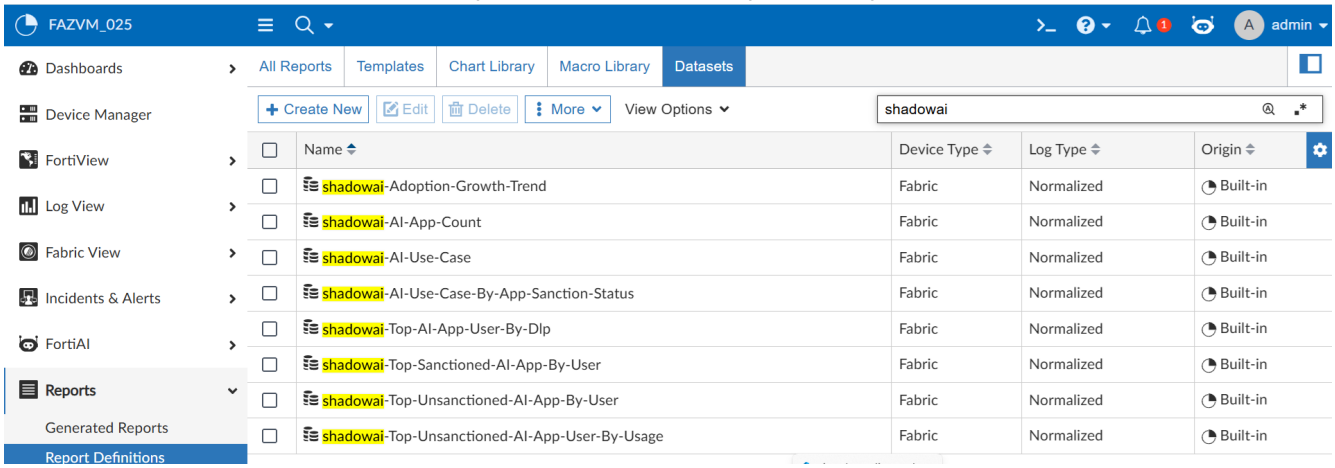
The *Shadow-AI Report* can be found in *Reports* > *Report Definitions* > *All Reports*.



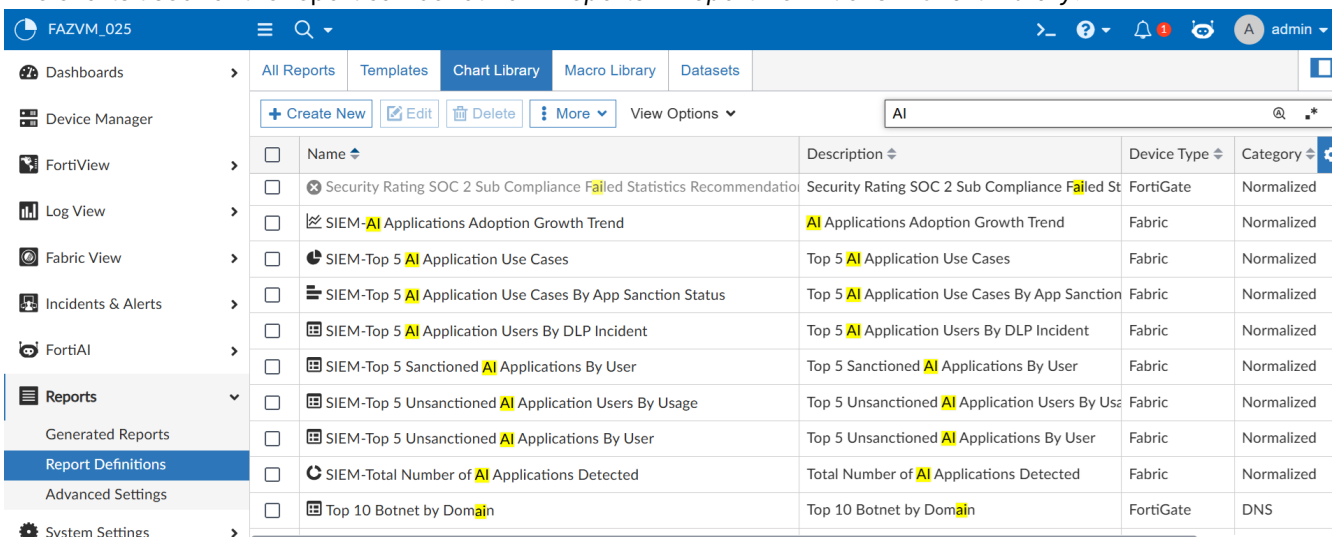
The report template can be found in *Reports* > *Report Definitions* > *Templates*.



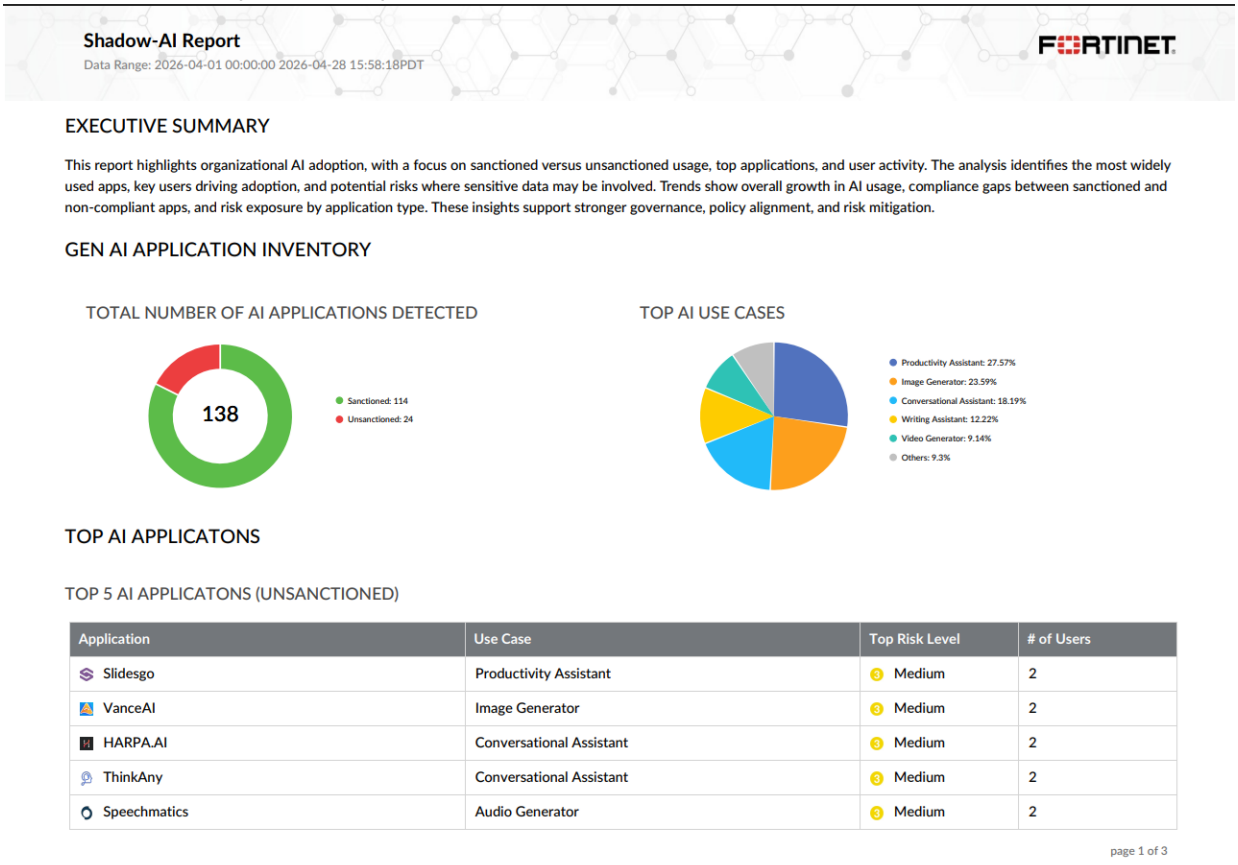
The datasets (`shadowai`) used for the report can be found in *Reports* > *Report Definitions* > *Datasets*.



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



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



Shadow-AI Report

Data Range: 2026-04-01 00:00:00 2026-04-28 15:58:18PDT

FORTINET

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 APPLICATONS

TOP 5 AI APPLICATONS (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

page 1 of 3

Shadow-AI Report

Data Range: 2026-04-01 00:00:00 2026-04-28 15:58:18PDT

FORTINET

TOP 5 AI APPLICATONS (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

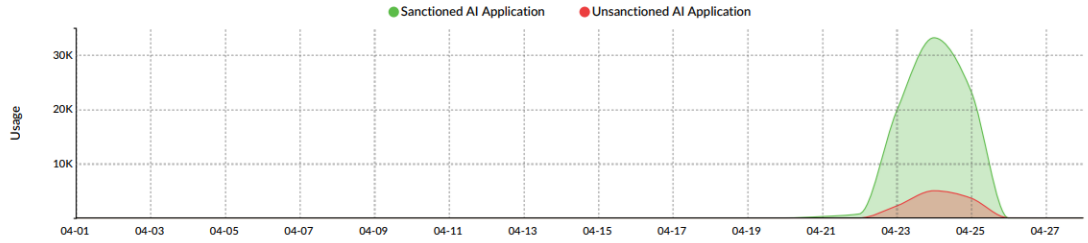
No matching log data for this report

page 2 of 3

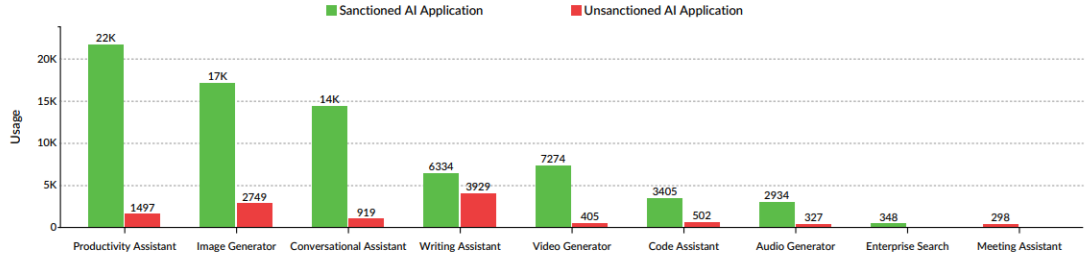
Shadow-AI Report

Data Range: 2026-04-01 00:00:00 2026-04-28 15:58:18PDT

ADOPTION GROWTH TREND



AI APPLICATION USAGE BY TYPE



FortiAI

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

FortiAI alert triage agent

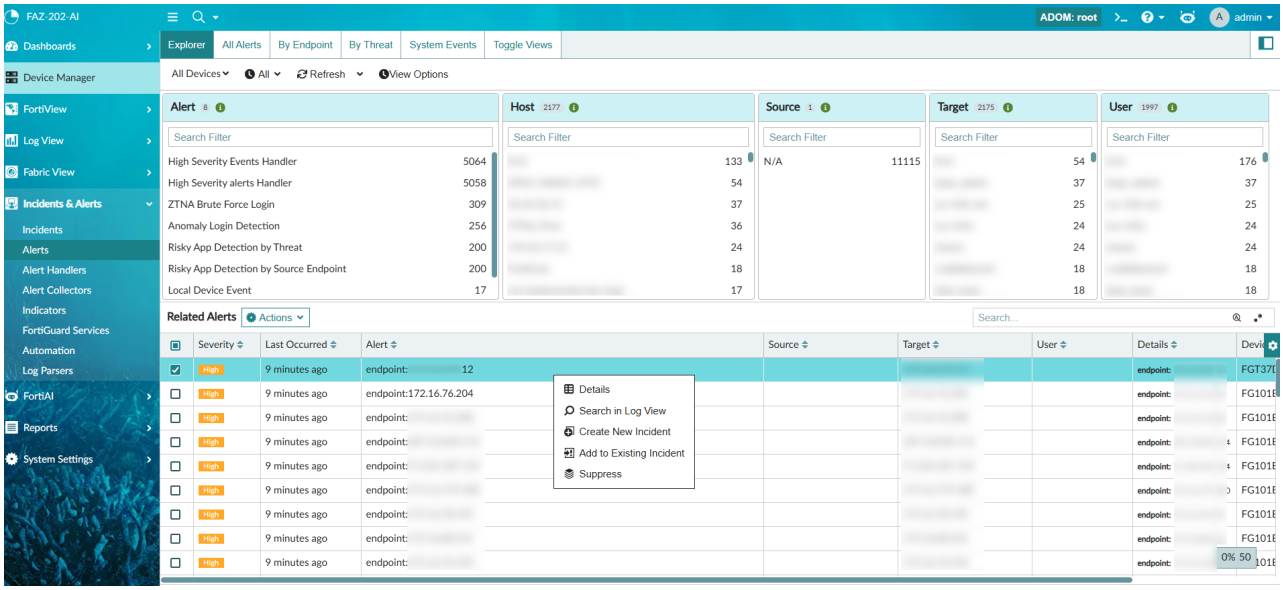
This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- 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.

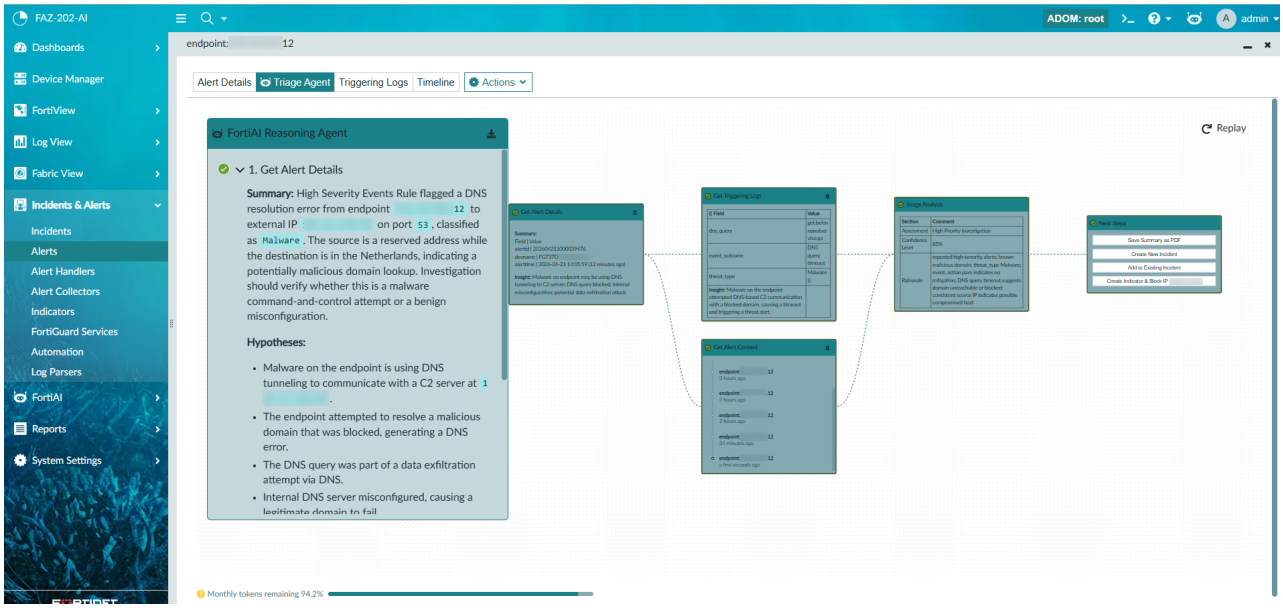
To use the alert triage agent:

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

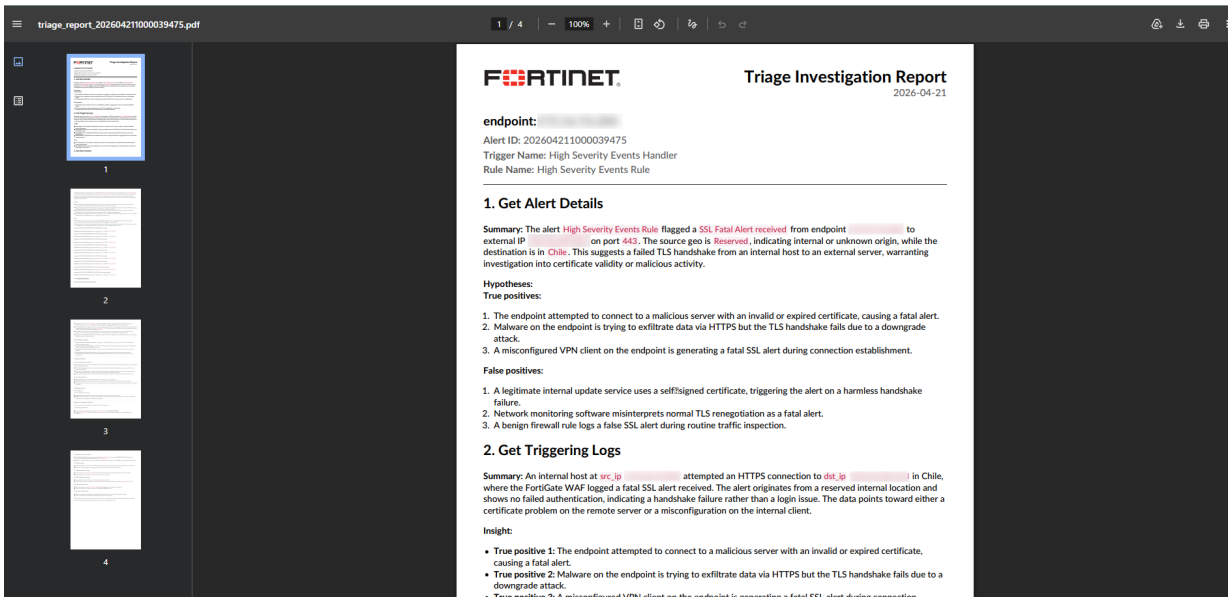


   Alternatively, you can double-click the alert to open the Alert details.
3. In the Alert details, go to the *Triage Agent* tab.
4. Wait for the *FortiAI Reasoning Agent* to finish the analysis, including:

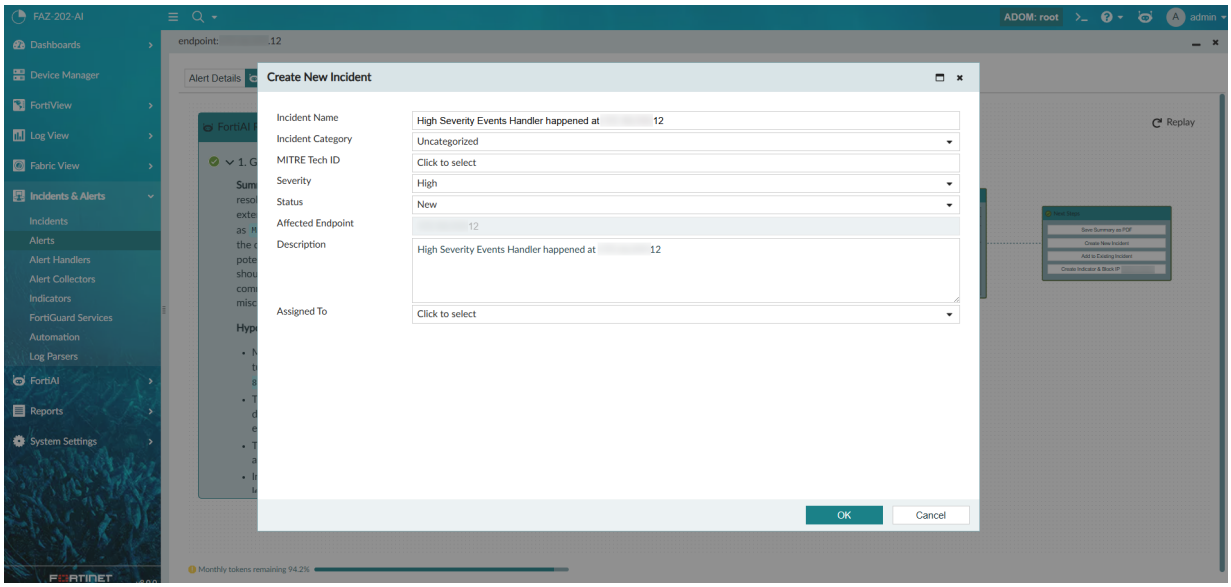
- *Get Alert Details*
- *Get Triggering Logs*
- *Get Entity Details*
- *Get Alert Context*
- *Triage Analysis*
- *Next Steps*



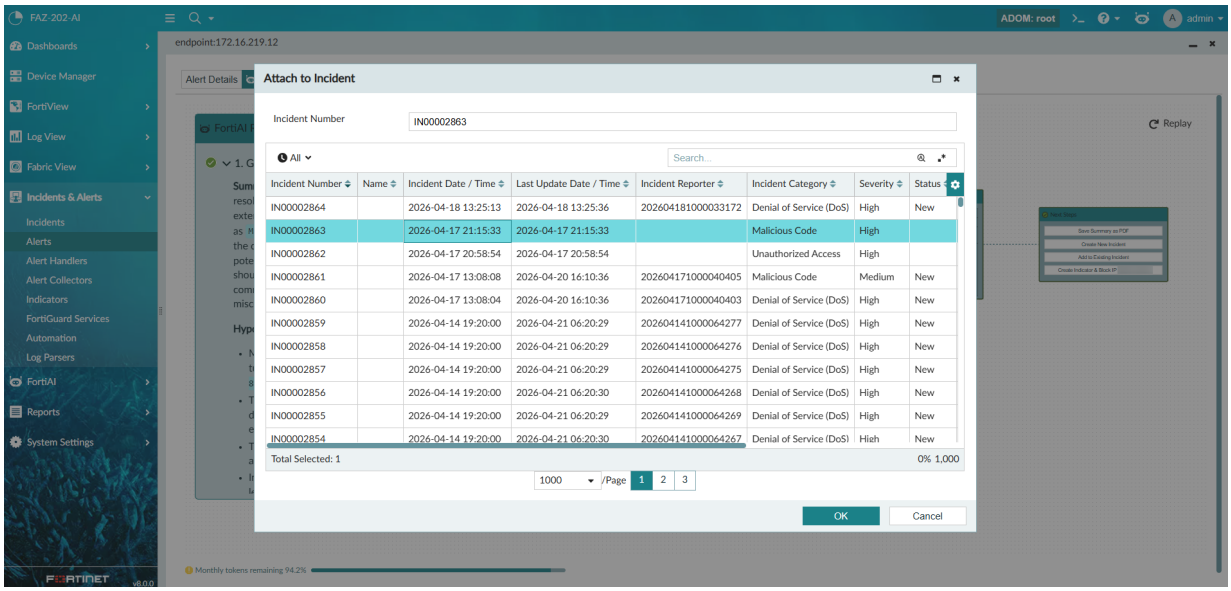
5. Review the AI reasoning by clicking on the steps within the *FortiAI Reasoning Agent* window.
6. From the *Next Steps* window, select the next step to perform on the alert.
   For example:
   - *Save Summary as PDF*



   - *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

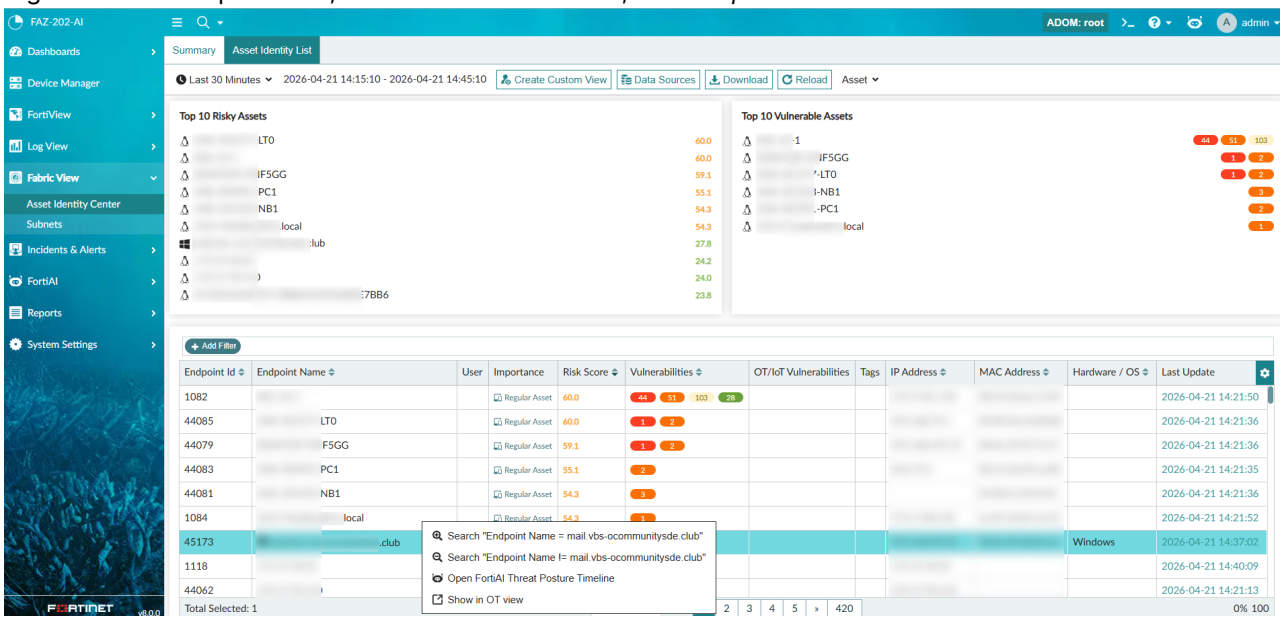
This information is also available in the FortiAnalyzer 8.0 Administration Guide:

- FortiAI threat posture timeline

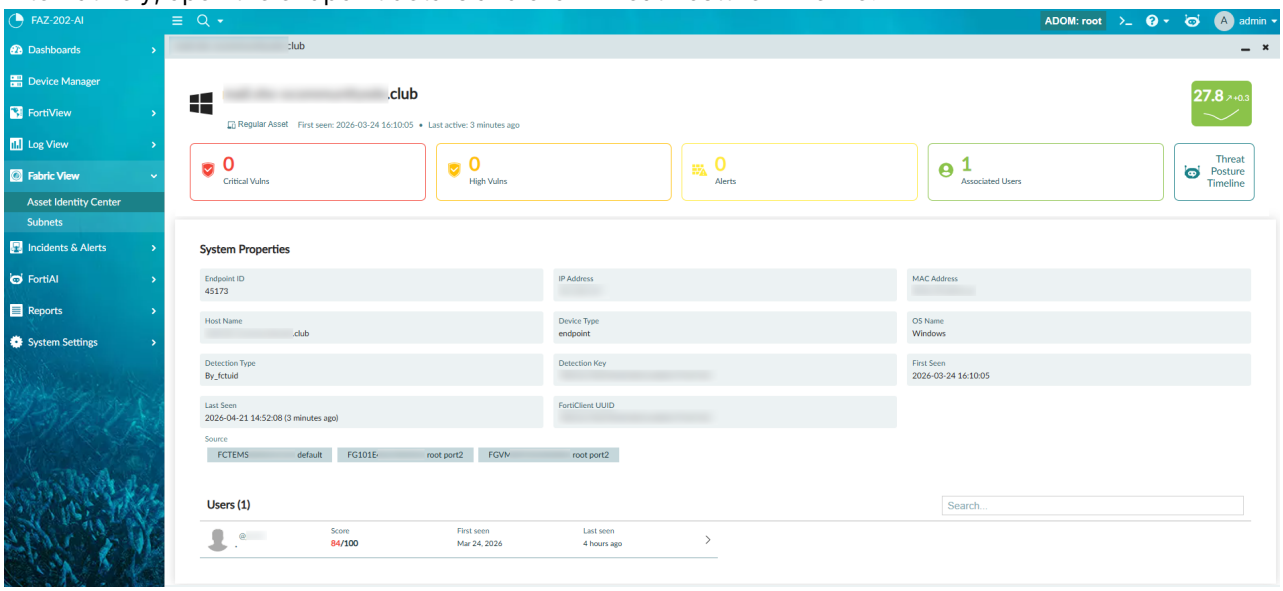
The new FortiAI Threat Posture Timeline provides an automated, consolidated security assessment for any asset or user identity. By aggregating UTM logs, alerts, incidents, and behavioral indicators from multiple sources (FortiGate, FortiClient, FortiMail, FortiAuthenticator), the system uses AI to determine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

To use the FortiAI threat posture timeline:

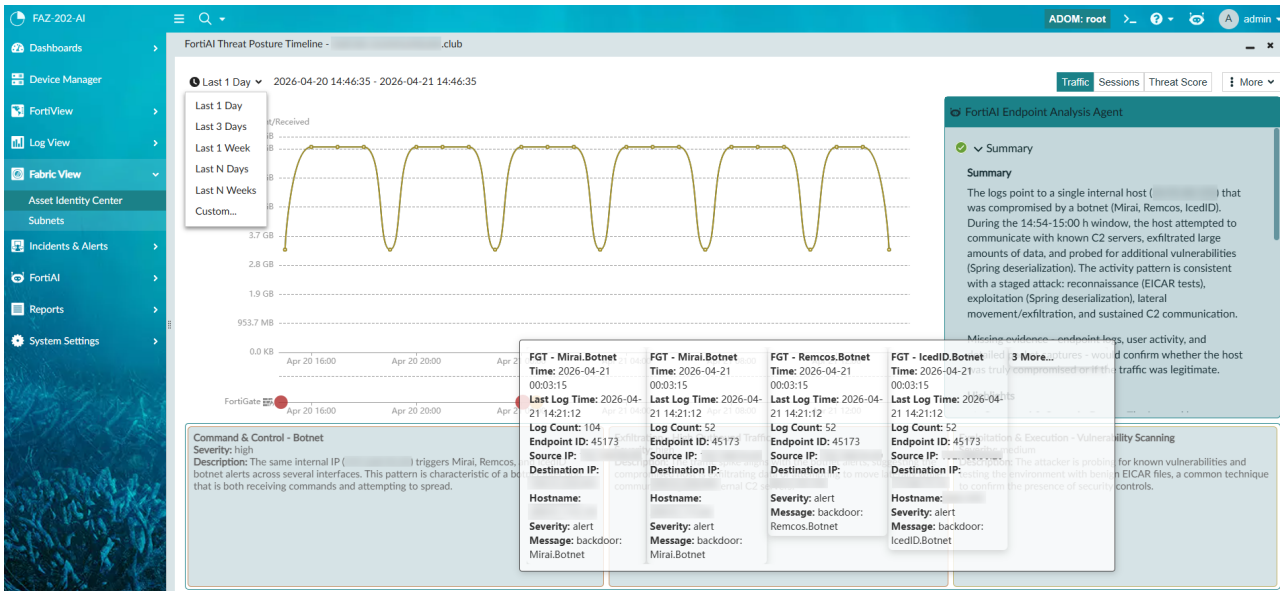
1. In the FortiAnalyzer GUI, go to *Fabric View* > *Asset Identity Center* > *Asset Identity List*.
2. Right-click an endpoint and, from the shortcut menu, select *Open FortiAI Threat Posture Timeline*.



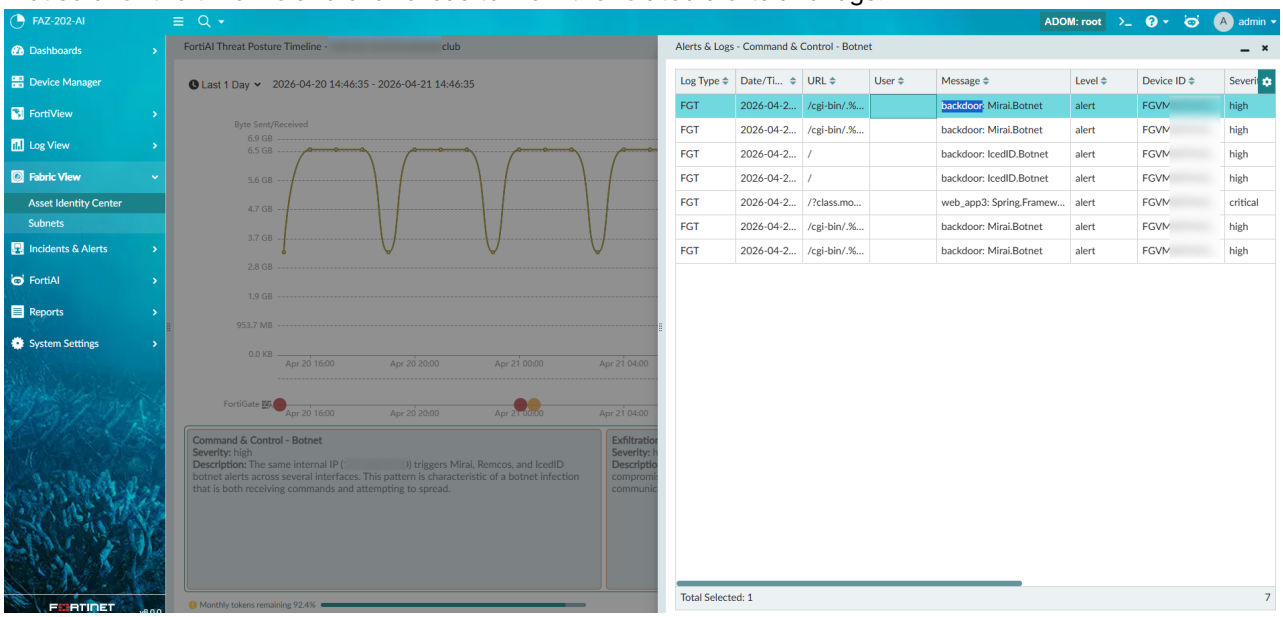
Alternatively, open the endpoint details and click *Threat Posture Timeline*.



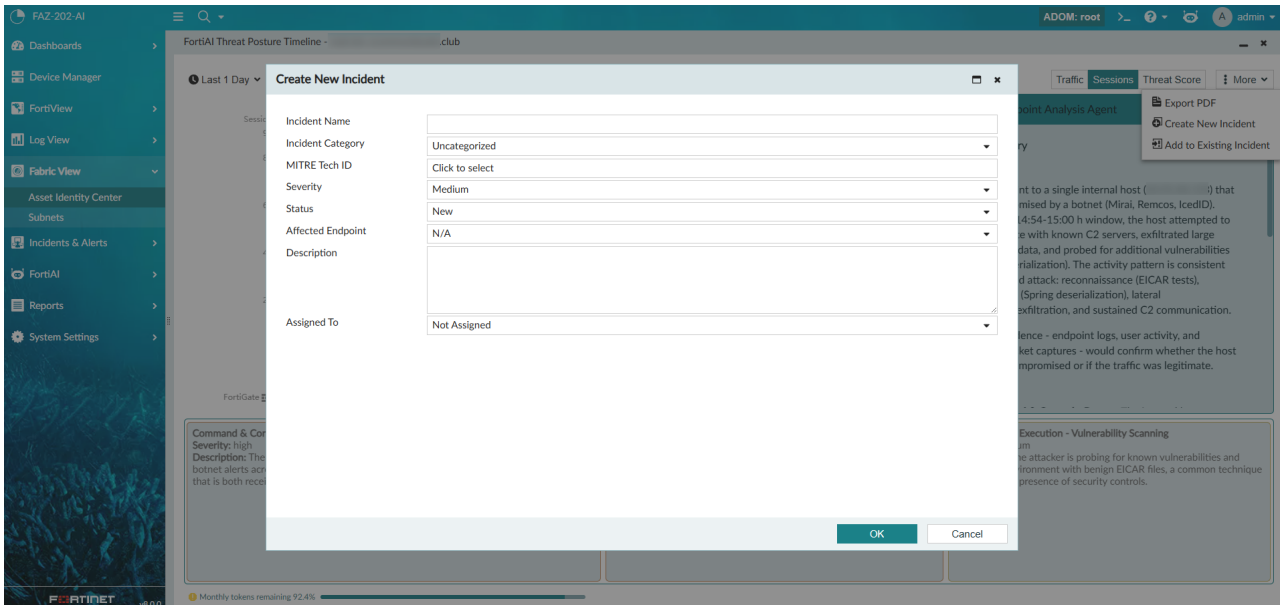
3. Wait for AI Agent analysis to finish. Review the analysis result in the *FortiAI Endpoint Analysis Agent* pane. The endpoint threats are highlighted at the bottom, below the timeline.

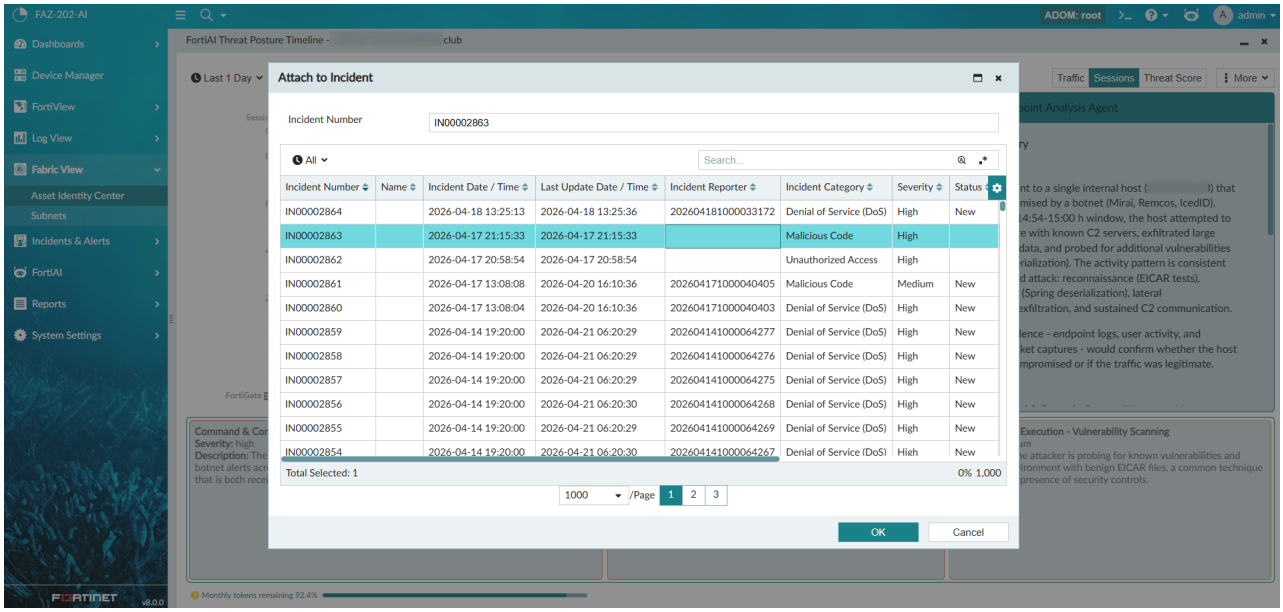


4. Mouse over the timeline and click areas to view the related alerts and logs.



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.


Create New Incident
Incident Name
Incident Category
Uncategorized
MITRE Tech ID
Click to select
Severity
Medium
Status
New
Affected Endpoint
N/A
Description
Assigned To
Not Assigned
OK
Cancel


Attach to Incident
Incident Number
IN00002863
Incident Number
Name
Incident Date / Time
Last Update Date / Time
Incident Reporter
Incident Category
Severity
Status
IN00002864 2026-04-18 13:25:13 2026-04-18 13:25:36 202604181000033172 Denial of Service (DoS) High New
IN00002863 2026-04-17 21:15:33 2026-04-17 21:15:33 Malicious Code High
IN00002862 2026-04-17 20:58:54 2026-04-17 20:58:54 Unauthorized Access High
IN00002861 2026-04-17 13:08:08 2026-04-20 16:10:36 202604171000040405 Malicious Code Medium New
IN00002860 2026-04-17 13:08:04 2026-04-20 16:10:36 202604171000040403 Denial of Service (DoS) High New
IN00002859 2026-04-14 19:20:00 2026-04-21 06:20:29 202604141000064277 Denial of Service (DoS) High New
IN00002858 2026-04-14 19:20:00 2026-04-21 06:20:29 202604141000064276 Denial of Service (DoS) High New
IN00002857 2026-04-14 19:20:00 2026-04-21 06:20:29 202604141000064275 Denial of Service (DoS) High New
IN00002856 2026-04-14 19:20:00 2026-04-21 06:20:30 202604141000064268 Denial of Service (DoS) High New
IN00002855 2026-04-14 19:20:00 2026-04-21 06:20:29 202604141000064269 Denial of Service (DoS) High New
IN00002854 2026-04-14 19:20:00 2026-04-21 06:20:30 202604141000064267 Denial of Service (DoS) High New
Total Selected: 1
0% 1,000
1000 /Page 1 2 3
OK
Cancel

System

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

Others

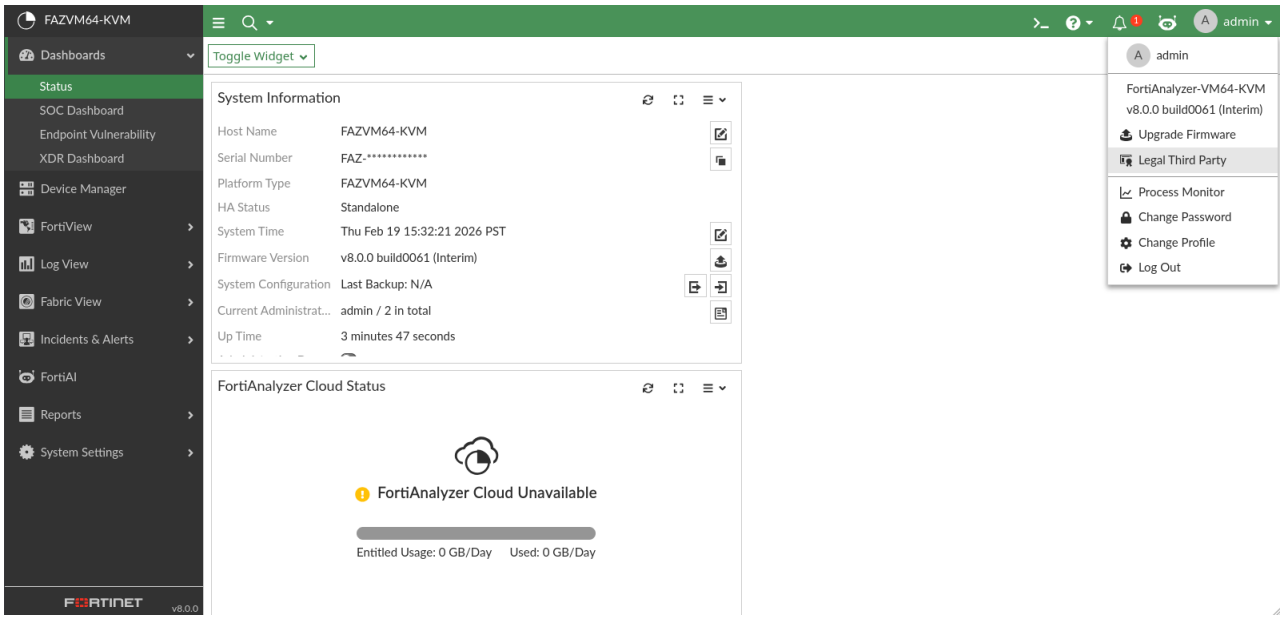
This section lists the new features added to FortiAnalyzer for other features relating to system settings:

Legal third party disclosure panel

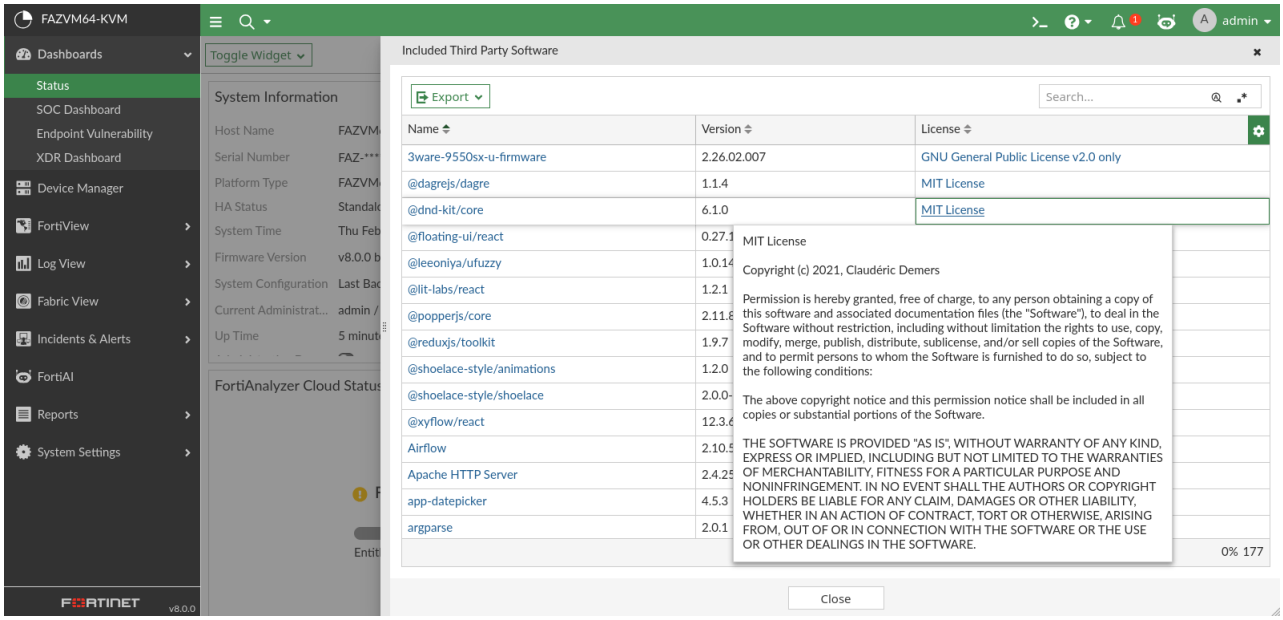
A Legal Third Party panel is added to the GUI, providing a searchable and exportable list of all third-party software used in FortiAnalyzer, along with their required licenses, license terms, and version information. This centralizes all third-party licensing details in one single, easily accessible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

To access and use the third-party software list:

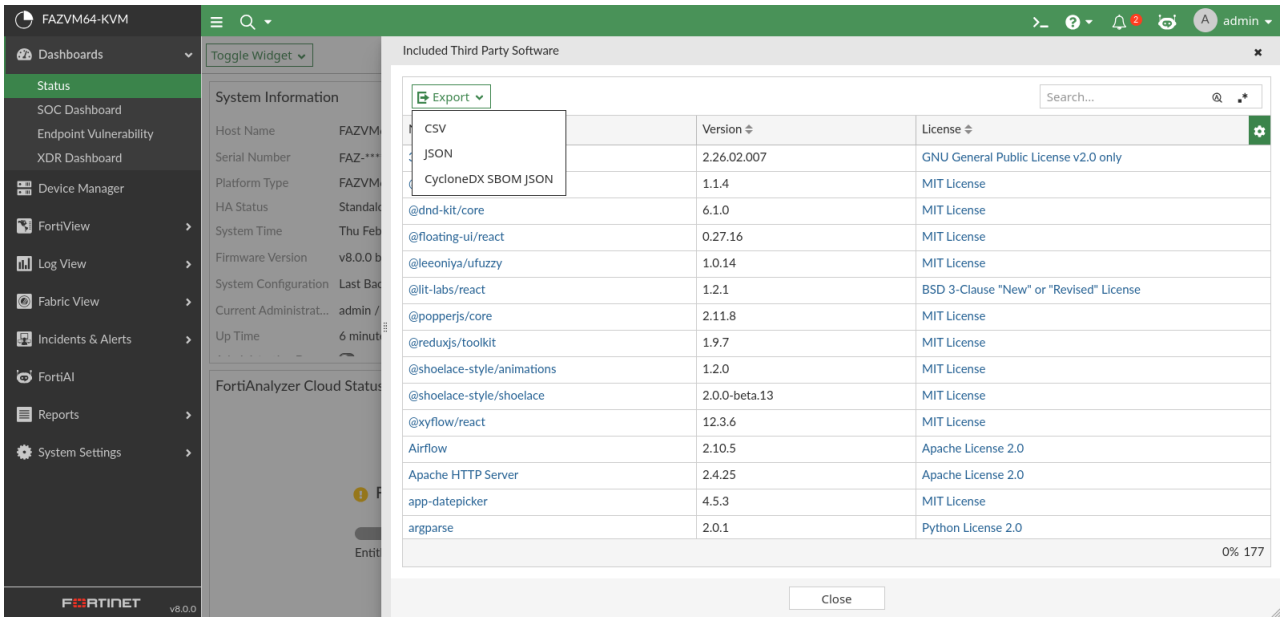
1. Select the *user name* > *System* > *Legal Third Party* to open the *Included Third Party Software* list.



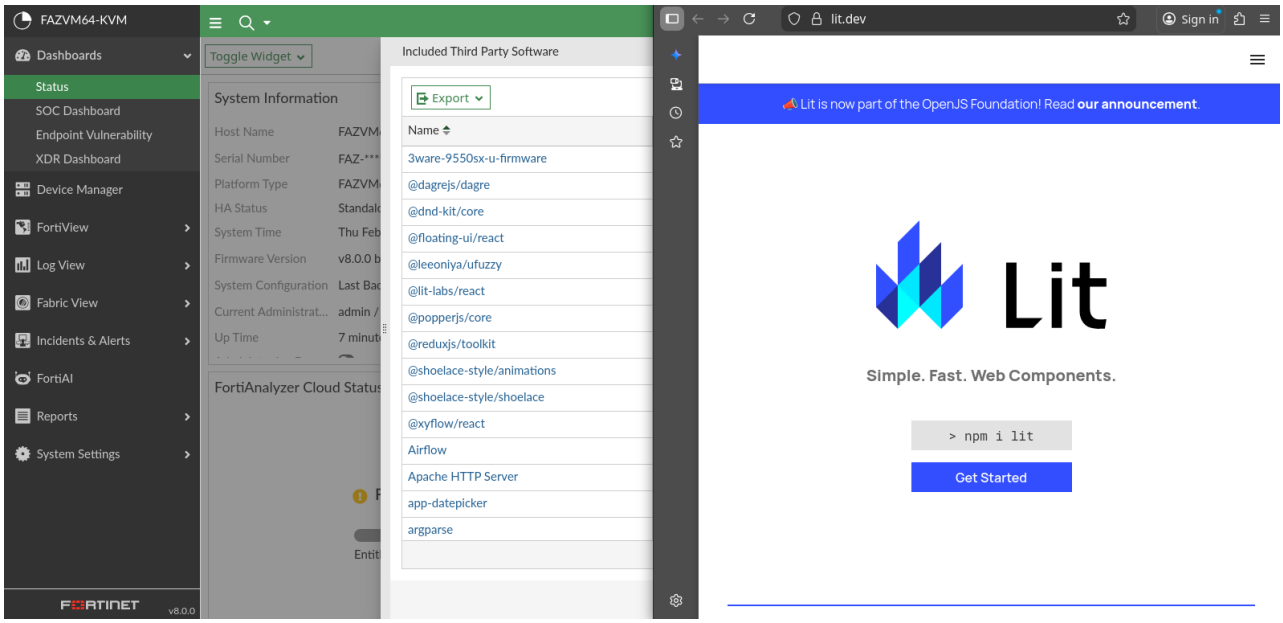
2. Hover over the *License* terms field to display additional information about the license terms.



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



4. 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.

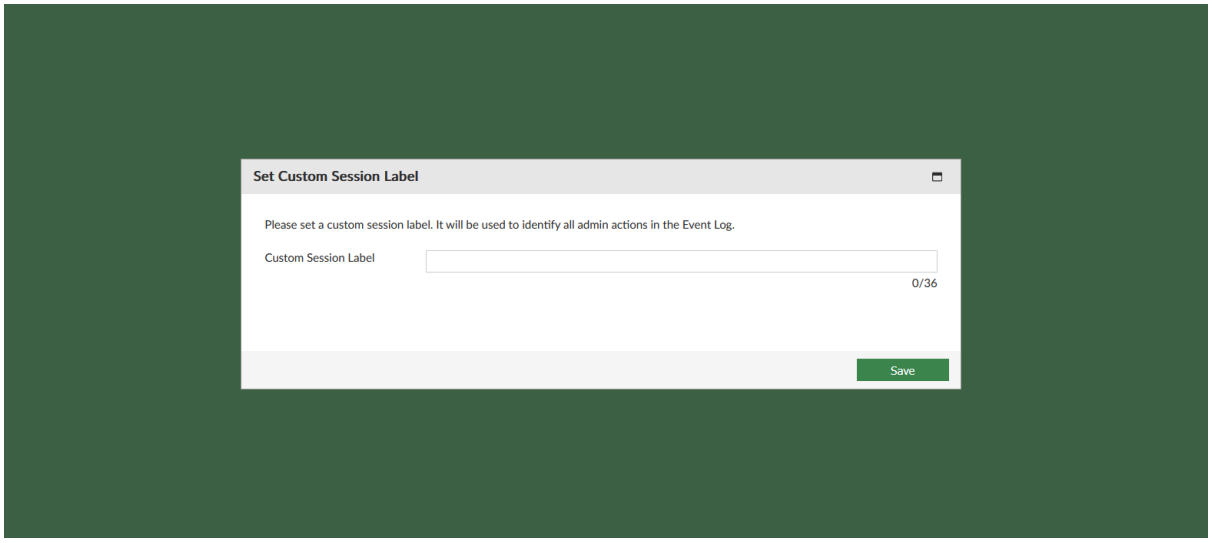
> ⚠ When custom session labels are enabled, it is mandatory for an administrator to set a custom session label.
>
> Unique session labels are not enforced, which means it is possible to have multiple sessions with the same session label.

To use custom session labels:

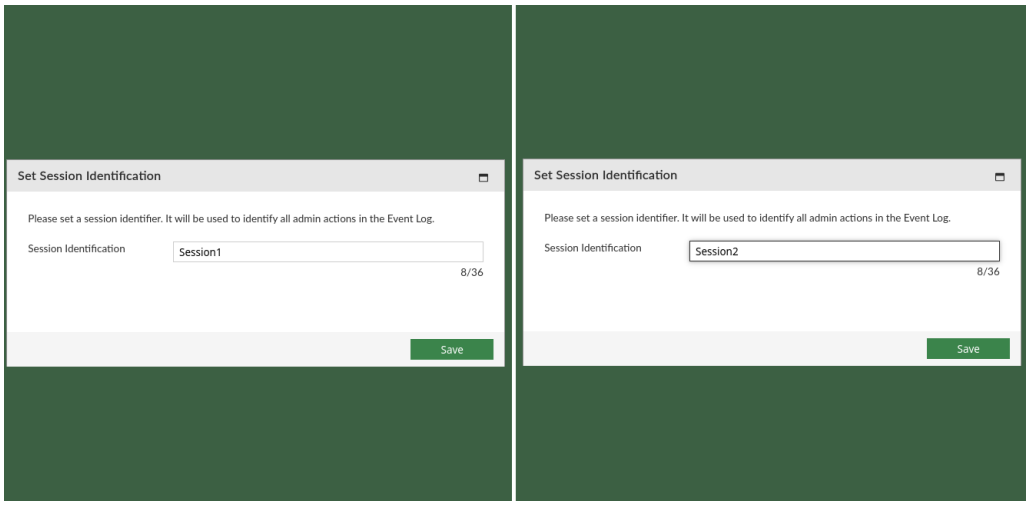
1. Enable custom session labels in the FortiAnalyzer CLI:

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

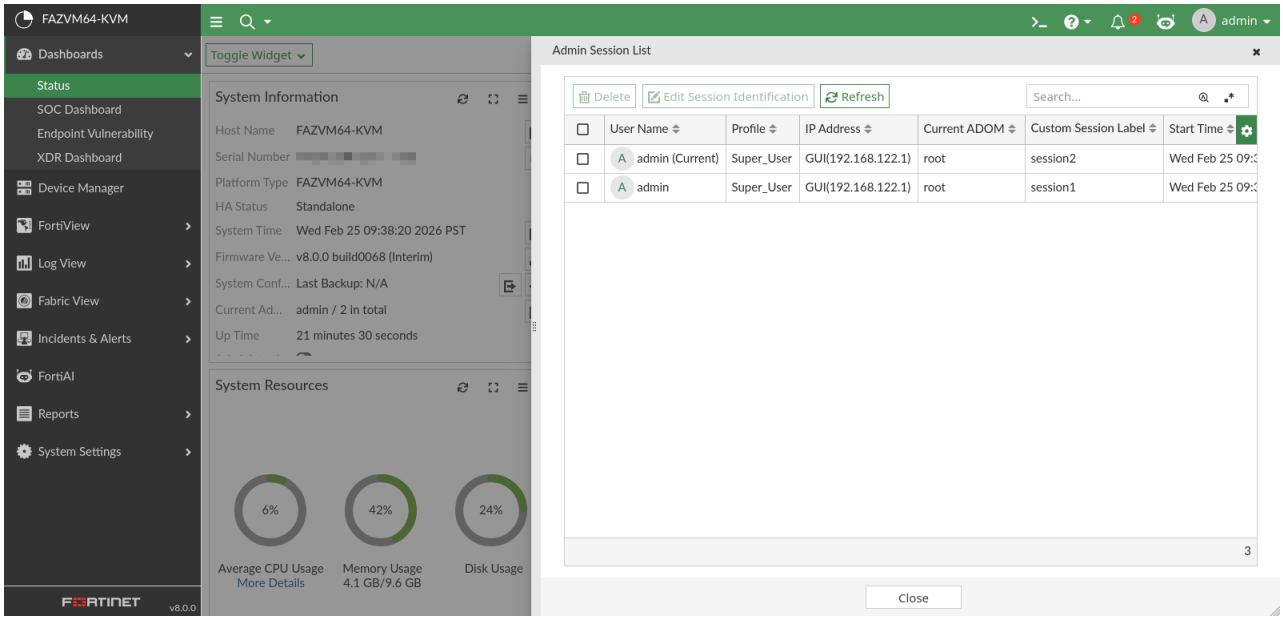
2. Log in to the FortiAnalyzer GUI.
   Administrators will see a *Set Custom Session Label* dialog after successfully logging in to FortiAnalyzer.



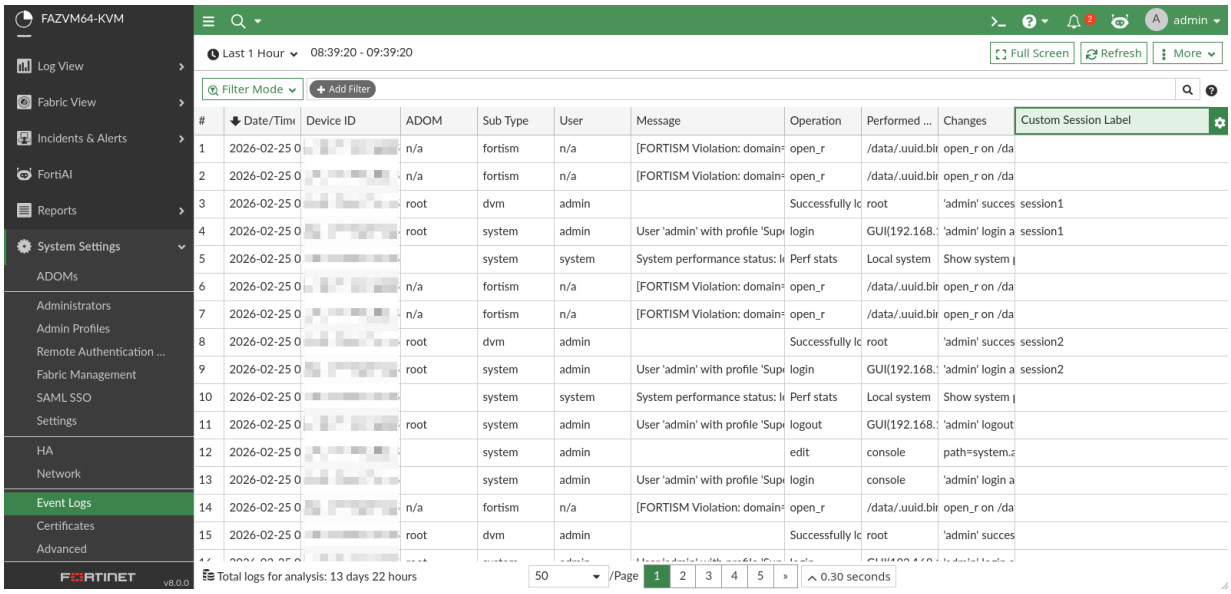
3. Enter your login credentials and enter a custom session label, then click *Login*. Custom session labels can be up to 36 characters in length.
   When there are multiple logins from the same administrator, different custom session labels can be used to distinguish the sessions.



4. 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.



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

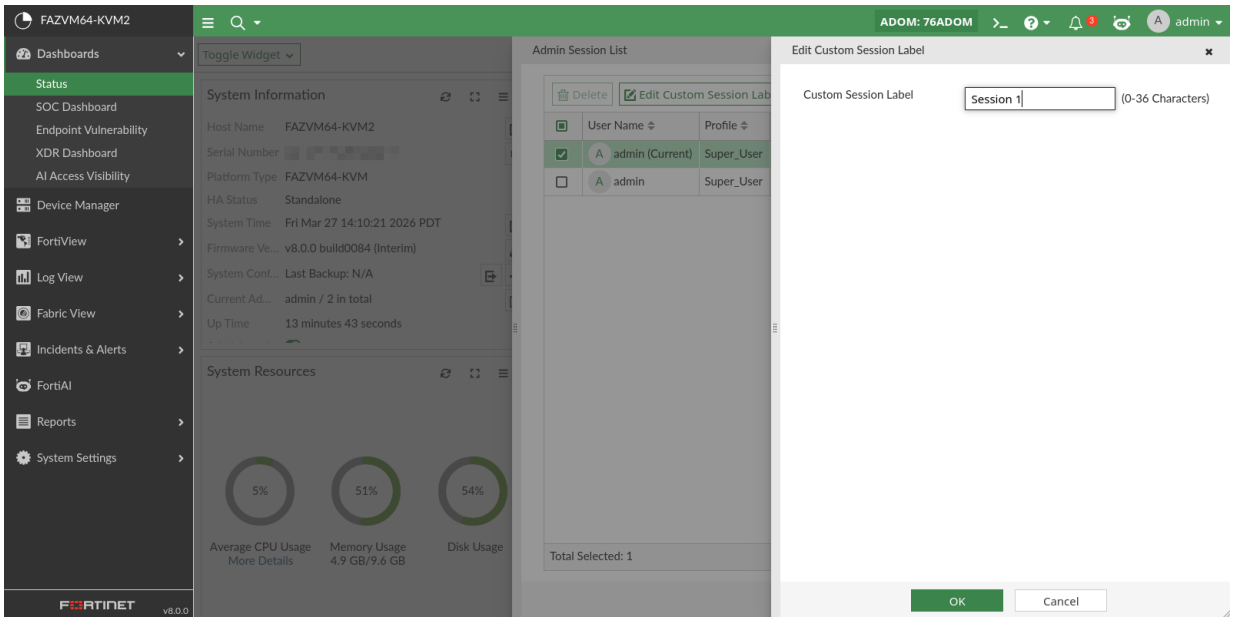


Change an active custom session label

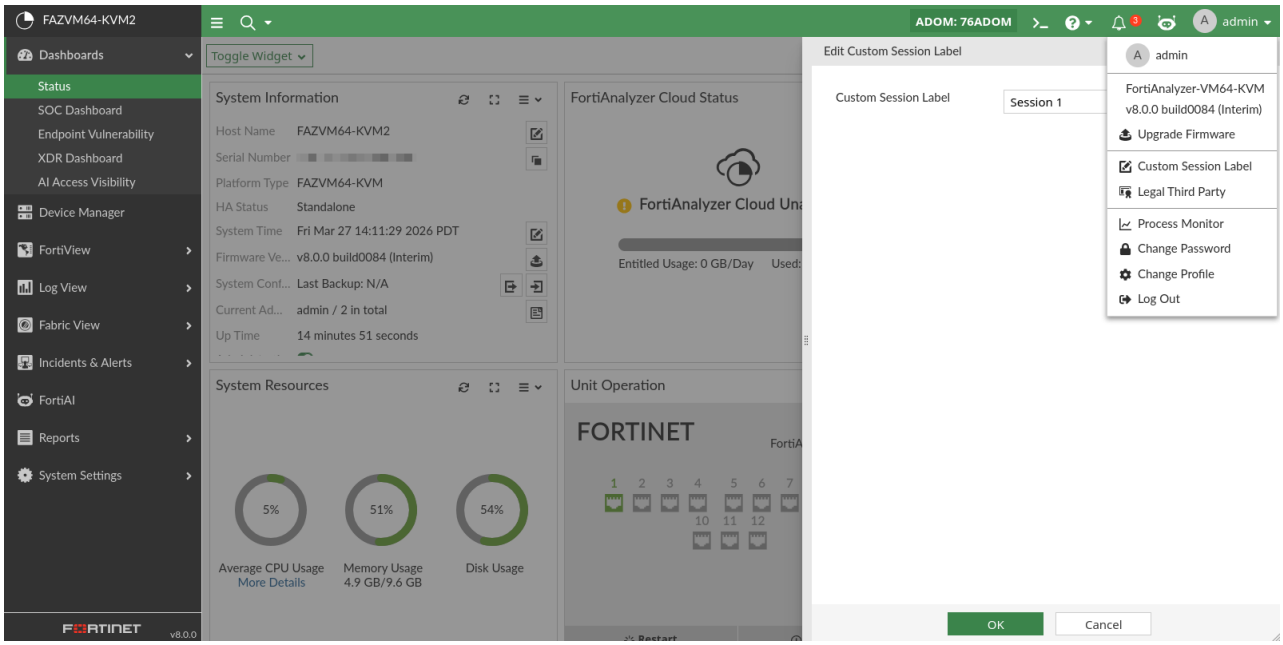
When `changeable` mode is enabled, administrators can change their custom session label during an active session using one of the following methods.

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*.



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.

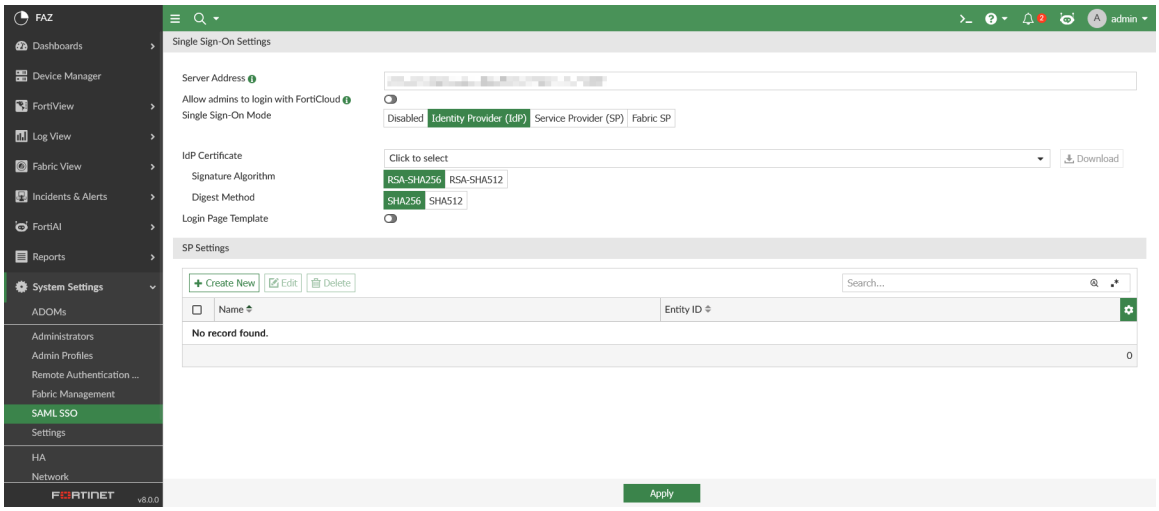
SHA-1 is considered cryptographically weak and has been deprecated for secure digital signatures and digests. Support for SHA-1 on FortiAnalyzer has been removed.

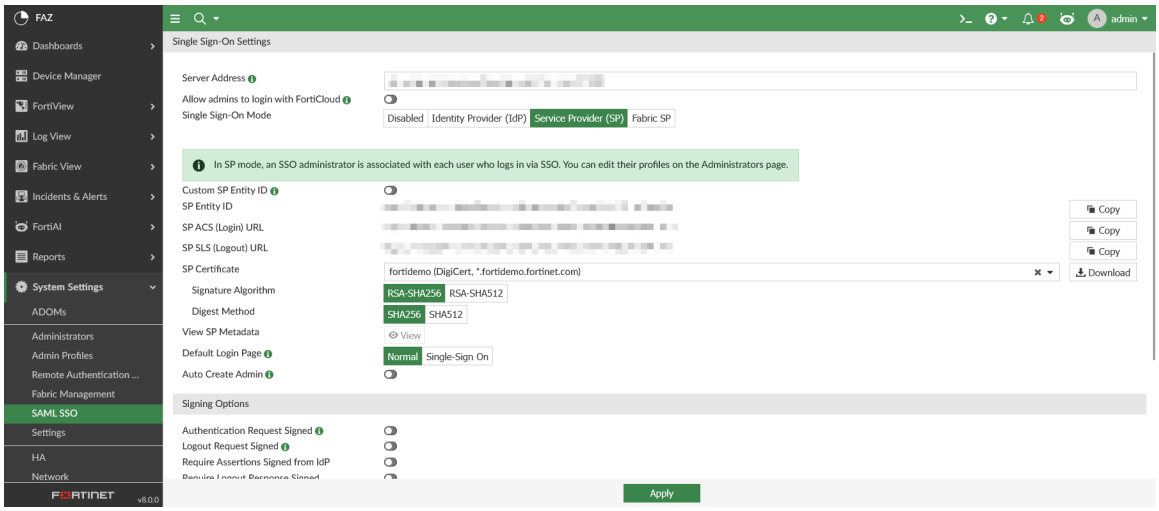
When configuring IdP and SP settings on FortiAnalyzer, administrators can select SHA-256 or SHA-512 for the Signature Algorithm and Digest Method. Because the SAML SSO trust model is based on asymmetric cryptography, the IdP and SP can use different cryptographic algorithms.

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
```

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:

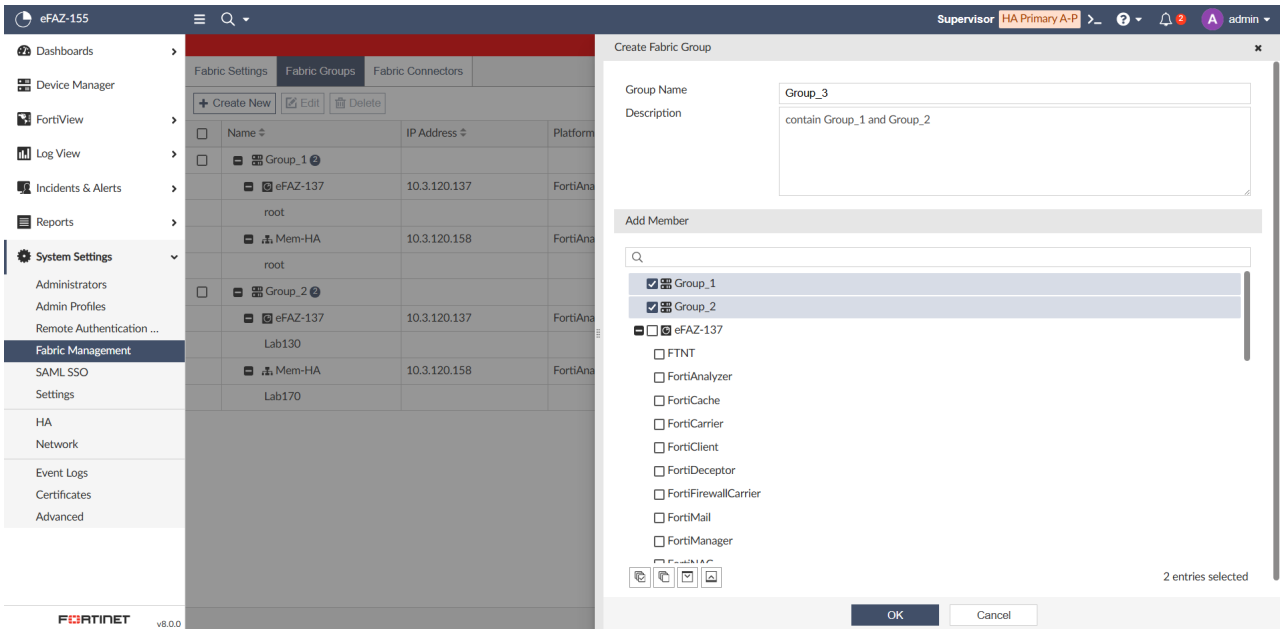
- Fabric Groups

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.

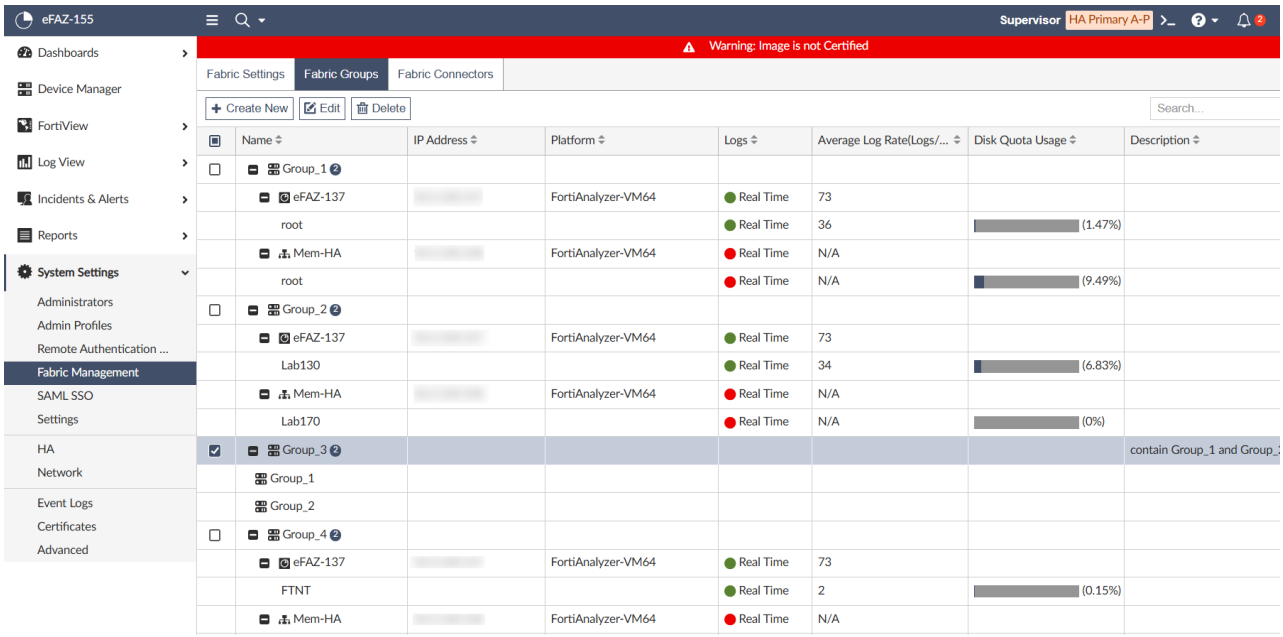
To create a fabric group containing other groups and assign it to a user:

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

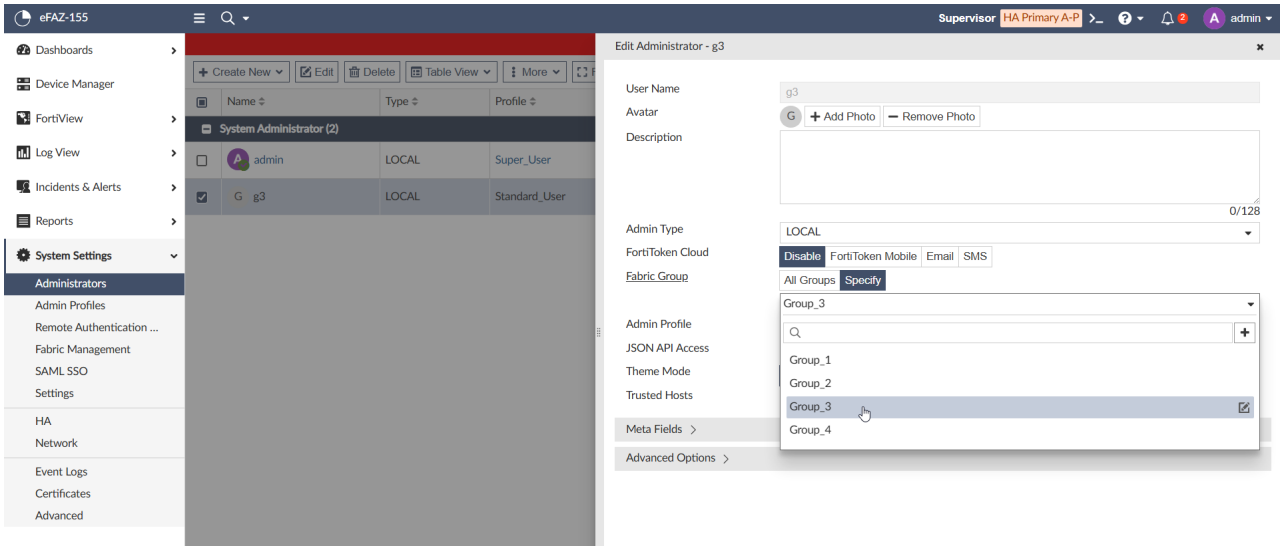
   In the example below, there are existing fabric groups: *Group_1* and *Group_2*. The admin creates a new fabric group (*Group_3*) and adds *Group_1* and *Group_2* as members.



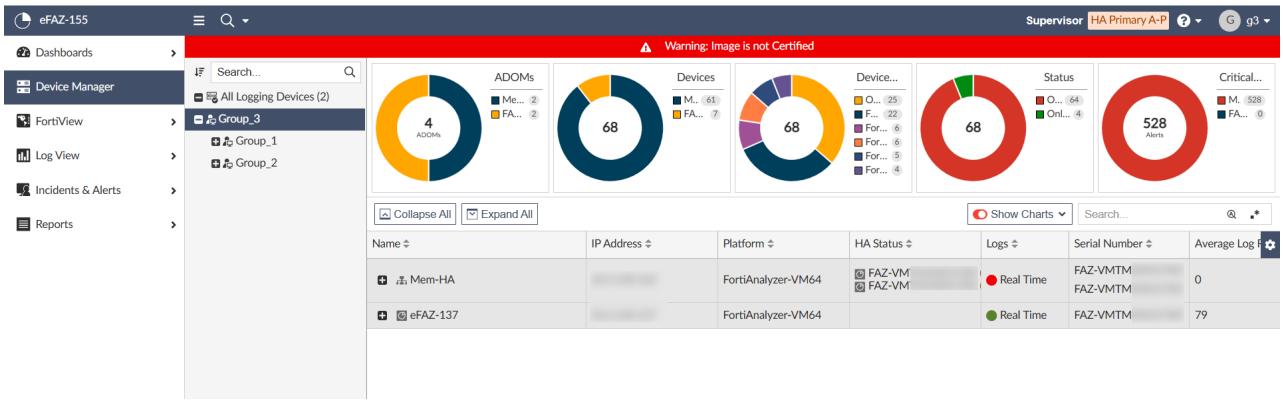
   After *Group_3* is created, it displays in the *Fabric Groups* table view with its assigned members (*Group_1* and *Group_2*) listed below.



2. In *System Settings* > *Administrators*, create a new admin user and assign the newly created fabric group (*Group_3*).



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

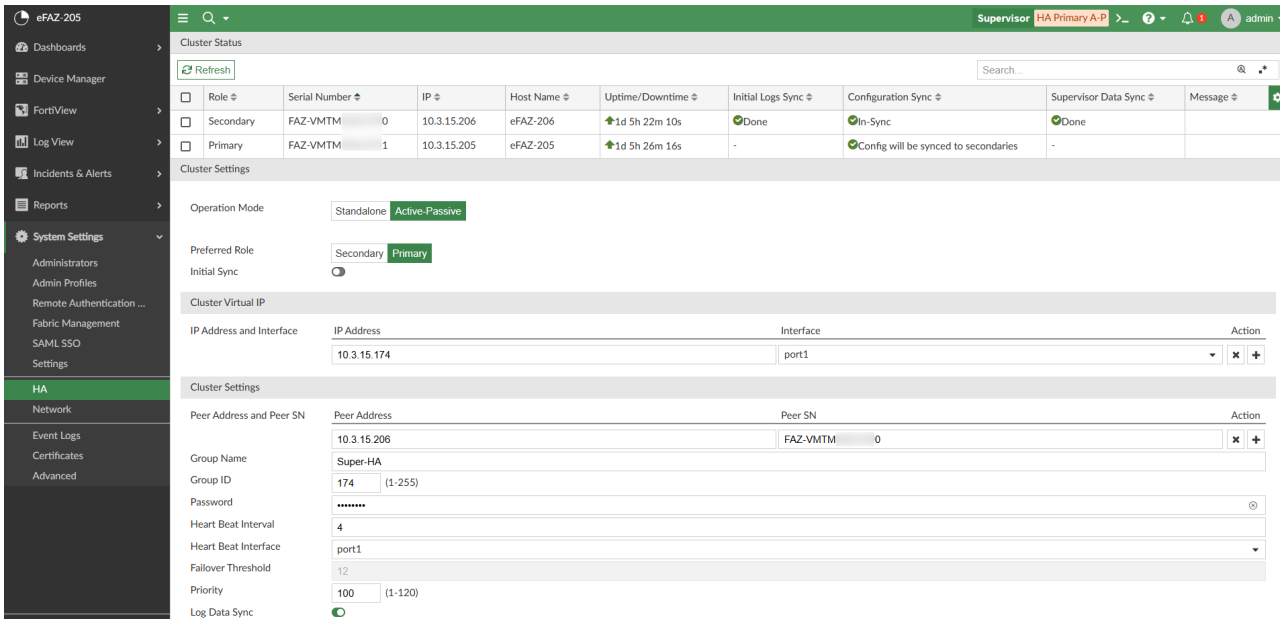
Beginning in FortiAnalyzer 8.0.0, high availability (HA) is supported on the FortiAnalyzer Fabric Supervisor.

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.

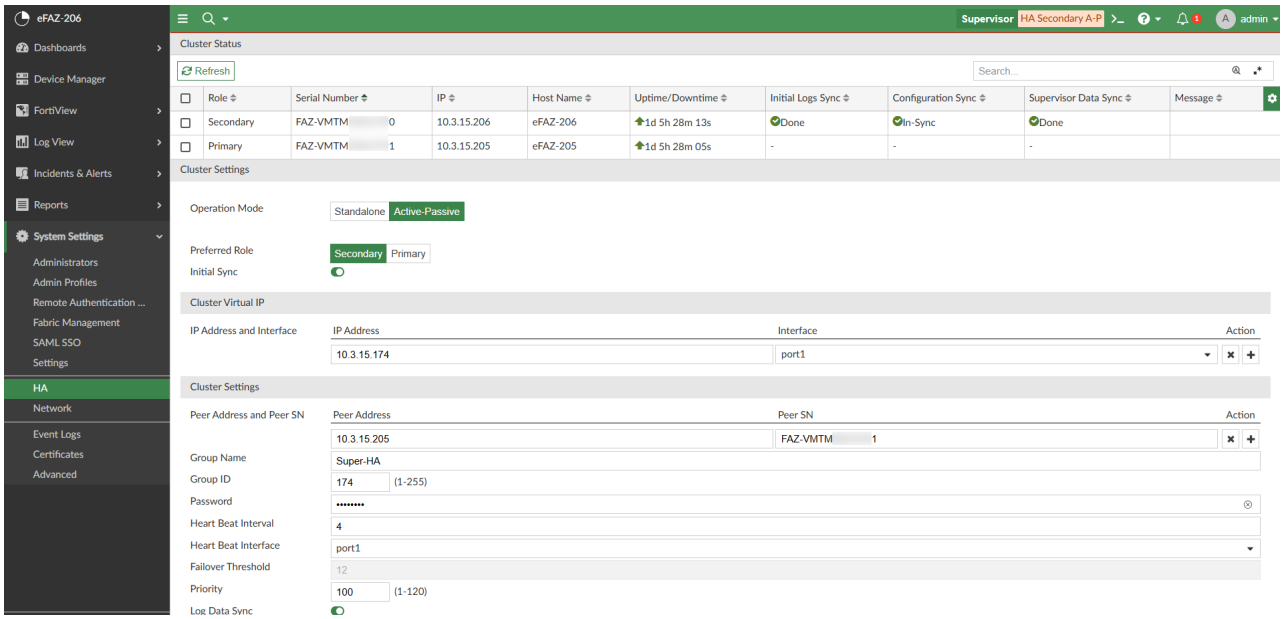
To configure FortiAnalyzer supervisor HA:

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.

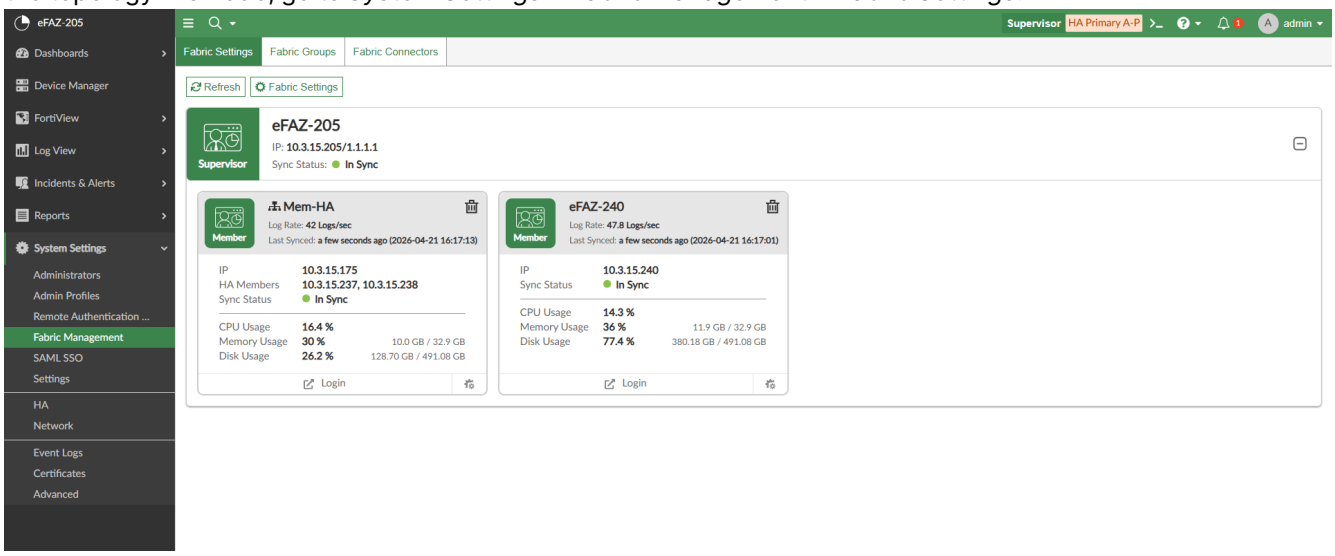


2. In the FortiAnalyzer to act as the secondary node, configure the HA options.

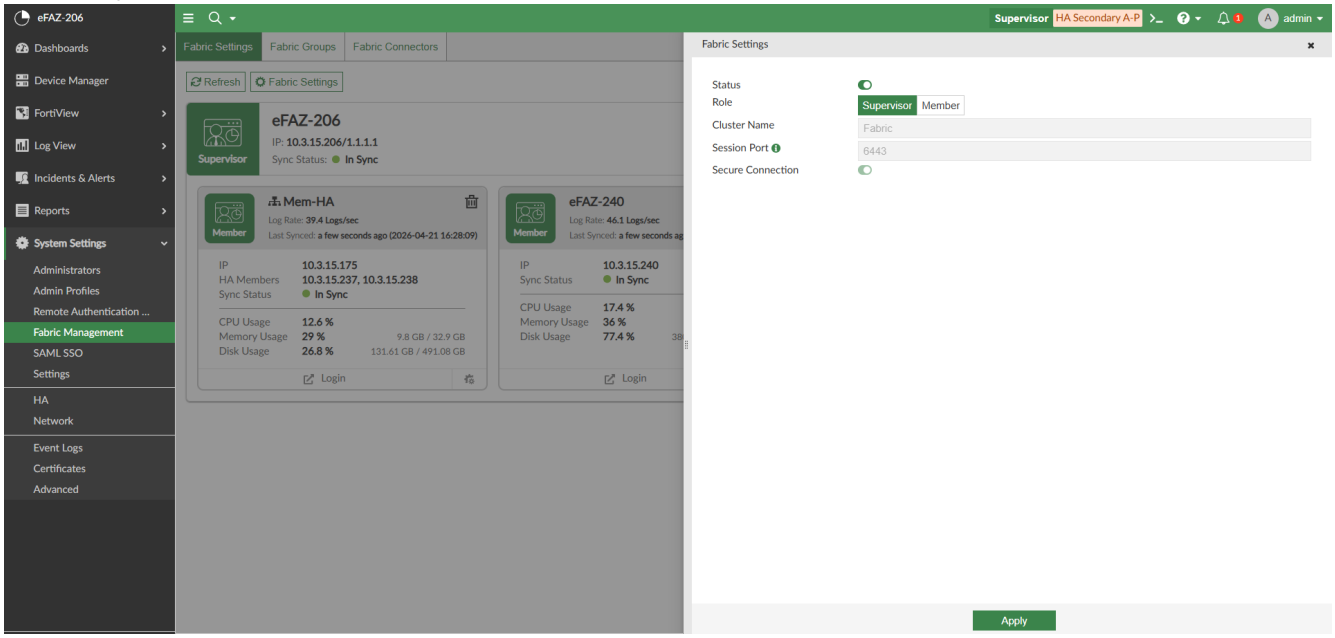
   You can review the HA status in the top *Cluster Status* section. The *Supervisor Data Sync* column displays the supervisor data sync status.



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*.

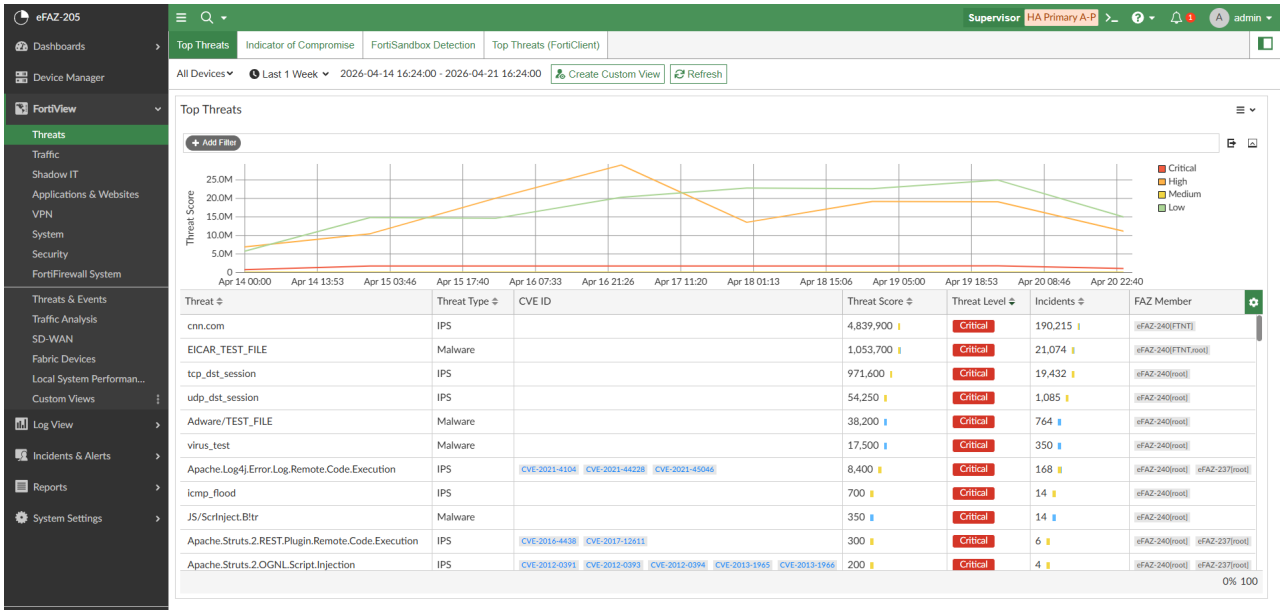


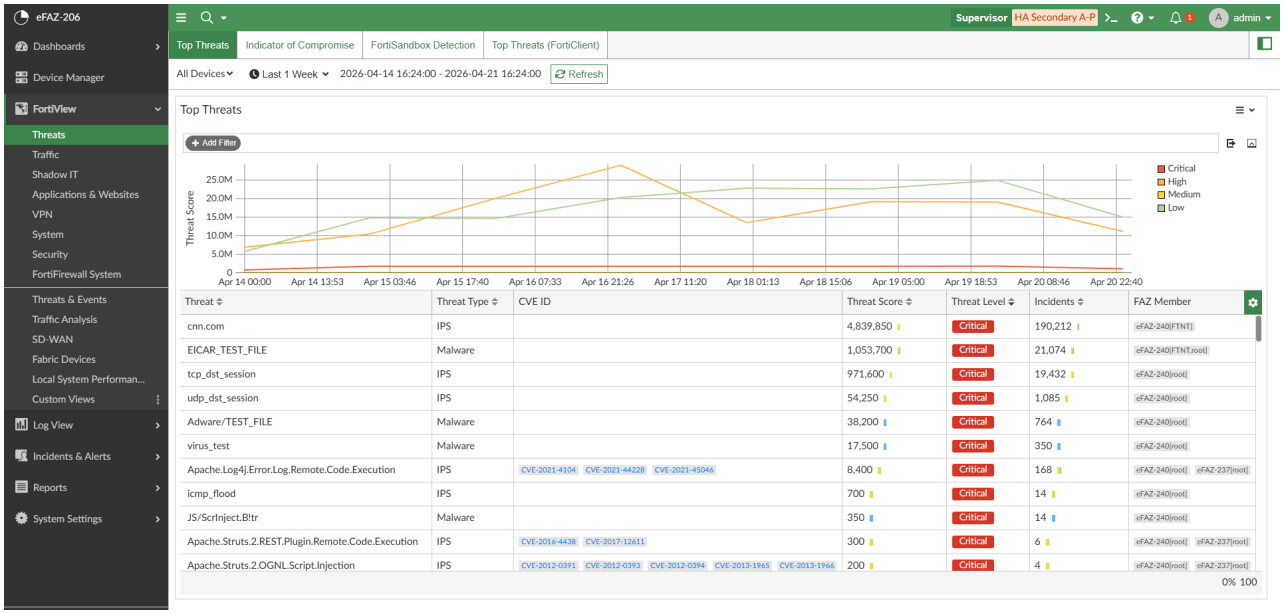
Same as in a normal FortiAnalyzer HA cluster, the secondary node cannot perform some actions. For example, actions such as authorizing, rejecting or deleting members, and creating Fabric Groups are grayed out in the secondary.



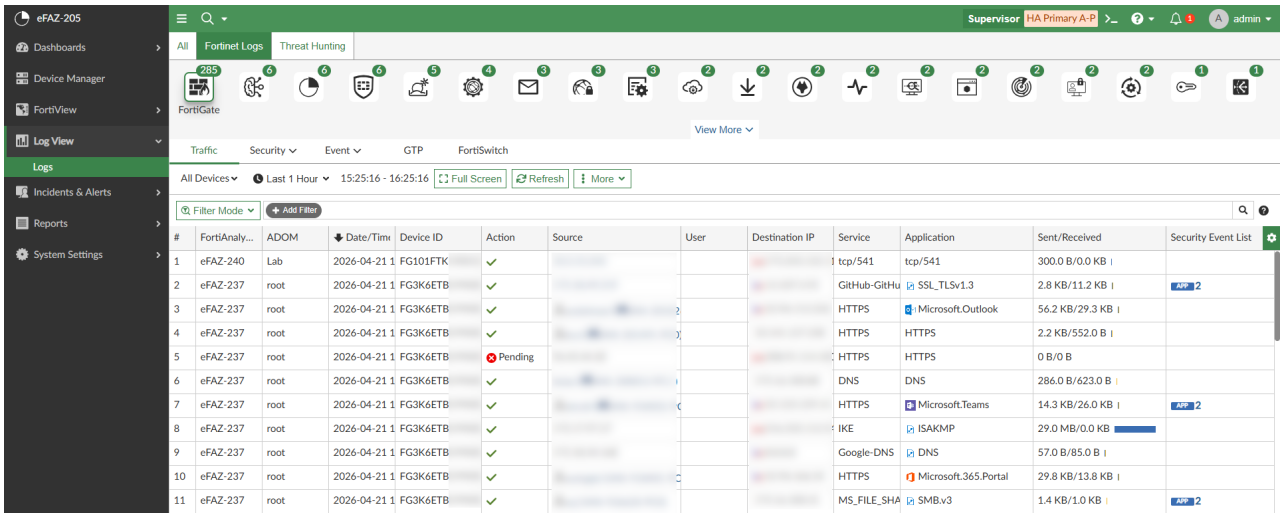
The secondary node can view members' devices, logs, FortiView, and Reports data, but the connection is established through supervisor primary node. See examples below.

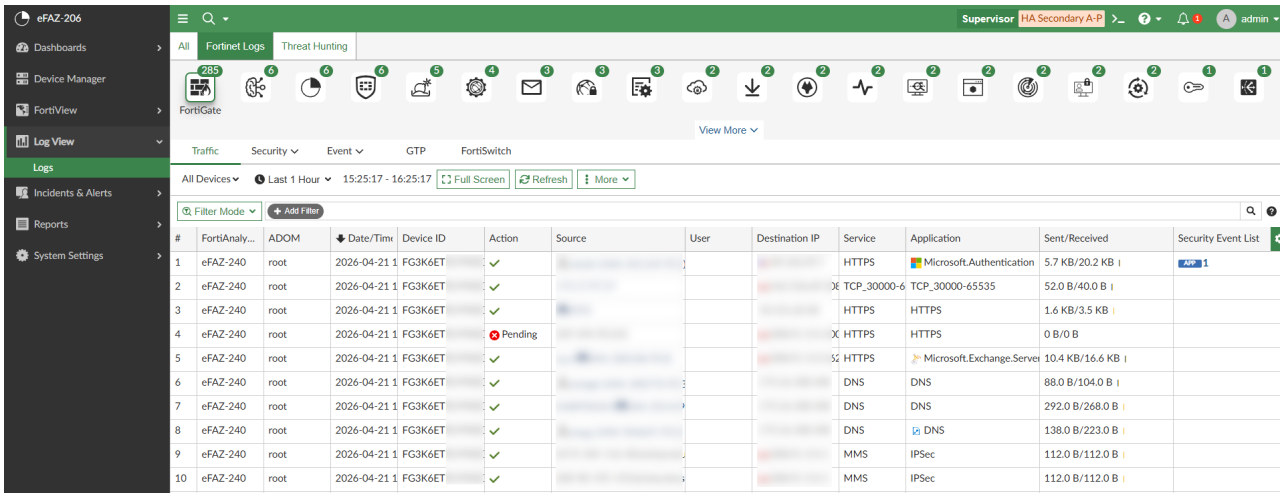
- *FortiView* in both the secondary and primary:





- *Log View* in both the secondary and primary:


eFAZ-205
Supervisor
HA Primary A-P
admin
Dashboards
Device Manager
FortiView
Log View
Logs
Incidents & Alerts
Reports
System Settings
All
Fortinet Logs
Threat Hunting
FortiGate
View More
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 SMB.v3 1.4 KB/1.0 KB APP 2


eFAZ-206
Supervisor
HA Secondary A-P
admin
Dashboards
Device Manager
FortiView
Log View
Logs
Incidents & Alerts
Reports
System Settings
All
Fortinet Logs
Threat Hunting
FortiGate
View More
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.Server 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

Security Operations

SOAR SIEM	• Playbook editor improvements on page 6
Incident and event management	• Alert explorer improvements on page 9
Dashboards	• AI Access Visibility dashboard on page 10
Asset and identity	• Improvements to the user experience in the Asset and Identity Center on page 12
Other enhancements	• FortiMQ connector for automated blocking on page 16 • Machine learning for anomaly detection on page 21

Log and Report

Logging	• FortiData incident support on page 33
Log forwarding	• FortiAnalyzer Fluentd supports the Azure Monitor Log Ingestion API on page 36
Reports	• Anomaly login report on page 38 • FortiDeceptor incident report on page 42 • Shadow-AI report on page 48

FortiAI

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

System

Other enhancements	• 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 • FortiAnalyzer supports NTPv4 with SHA-256 encryption on page 66 • Time-base retention is configurable for the task monitor and event log on page 68
FortiAnalyzer Fabric	• Assign access to multiple fabric groups for a single admin on page 69 • FortiAnalyzer Fabric Supervisor HA on page 71

www.fortinet.com