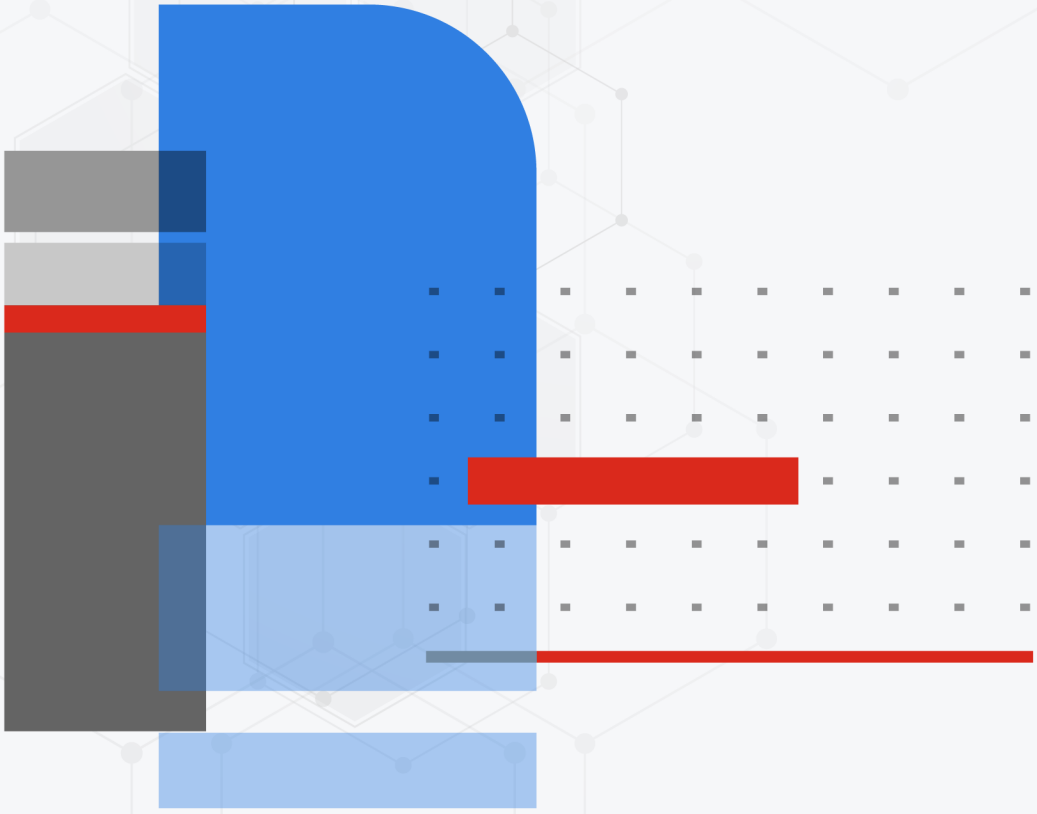
Deployment Guide

FortiAnalyzer Fabric 7.4.4



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 29, 2025
FortiAnalyzer Fabric 7.4.4 Deployment Guide
05-744-898419-20250429

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-09-17	Initial release.
2025-04-29	Updated High availability for FortiAnalyzer Fabric members on page 25. No support for FortiAnalyzer Fabric supervisor HA.

Introduction

The FortiAnalyzer Fabric enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzers acting as members. In this mode, FortiAnalyzer Fabric members form a Fabric with one device operating in supervisor mode as the root device. Incident and event information is synced from members to the supervisor using the API.

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

The FortiAnalyzer Fabric device operating as the supervisor includes the following modules:

Device Manager	Displays FortiAnalyzer Fabric members with their ADOMs and authorized logging devices.
FortiView	Summarizes SOC information in *FortiView* and *Monitors* dashboards, which include widgets displaying log data in graphical formats, network security, WiFi security, and system performance in real-time. The information is generated from all FortiAnalyzer Fabric members.
Log View	Displays logs collected across the FortiAnalyzer Fabric. Each log includes the *FortiAnalyzer Host Name* and *ADOM* it was collected on.
Incidents & Events	Displays incidents and events created on the FortiAnalyzer Fabric members and supervisor local events.
Reports	Generate reports using information from all devices in the FortiAnalyzer Fabric. You can also configure report templates, schedules, and output profiles, and manage charts and datasets.
System Settings	Configure the settings for the FortiAnalyzer Fabric supervisor. For information about deploying the FortiAnalyzer Fabric, see Deployment on page 8. For information about creating Fabric Groups within the FortiAnalyzer Fabric, see Fabric Groups on page 23. For information about other settings, see the FortiAnalyzer Administration Guide.
Management Extensions	Enables supported management extension applications. See the FortiAnalyzer Administration Guide.

For information on the modules available as a FortiAnalyzer Fabric member, see the FortiAnalyzer Administration Guide.

FortiAnalyzer Fabric roles

FortiAnalyzer Fabric includes two operation modes, including supervisor and member.

- Supervisors acts as the root device in the FortiAnalyzer Fabric. SOC administrators can use the supervisor to view member devices and their ADOMs and authorized logging devices, as well as incidents and events created on members.
- Members are devices in the FortiAnalyzer Fabric that send information to the supervisor for centralized viewing. When configured as a member, FortiAnalyzer devices continue to have access to the FortiAnalyzer features identified in the FortiAnalyzer Administration Guide. Incidents and events are created or raised from each member.

Logging devices cannot be registered to the Fabric supervisor and they will not be visible in *Device Manager*, *Log View*, or *Reports*. The Fabric supervisor is for centralized viewing of information from the Fabric members only.

Preparing for deployment

This section includes the following topics:

Requirements

- Fabric members and supervisors can have different timezones. For Reports and Fortiview, the supervisor's local timezone is used for data gathering.
- Logging devices cannot be registered to the Fabric supervisor but to Fabric members only.
- You can combine physical and virtual FortiAnalyzer appliances in the same FortiAnalyzer Fabric up to a maximum of 64 FortiAnalyzers.
- Incidents on the FortiAnalyzer Fabric supervisor are available in read-only mode.
- Traffic must be allowed for port TCP 514 on the supervisor and the members.

FortiAnalyzer v7.4 cannot form a fabric with FortiAnalyzers using v7.2.

Sizing

FortiAnalyzer Fabric members can be designed according to your company’s log rate and storage requirements as described in the FortiAnalyzer Architecture Guide. The FortiAnalyzer Fabric supervisor has lower resource needs because it does not handle log receiving, analysis, and reporting tasks but instead consolidates and aggregates data from multiple FortiAnalyzer Fabric members.

Deployment

This section includes the following topics:

Configuring the FortiAnalyzer Fabric

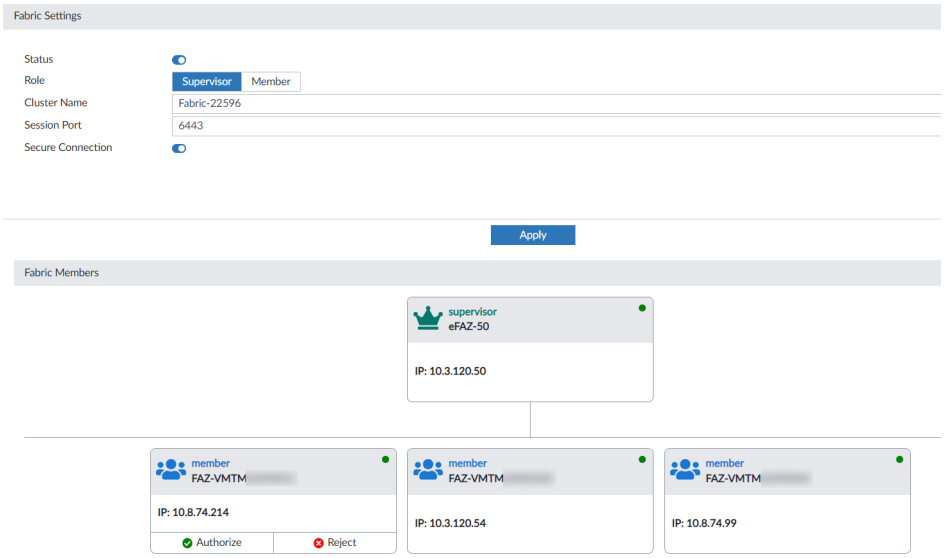
To configure a FortiAnalyzer Fabric, you must configure a supervisor, one or more members, and enable soc-fabric communication on the interfaces being used.

Members must be authorized from the FortiAnalyzer Fabric supervisor to complete the configuration. This can be done from the supervisor GUI or by using a `trusted-list` configured in the CLI.

Port TCP 514 is used when establishing the connection between the supervisor and the member. Traffic must be allowed for this port on the supervisor and all members.

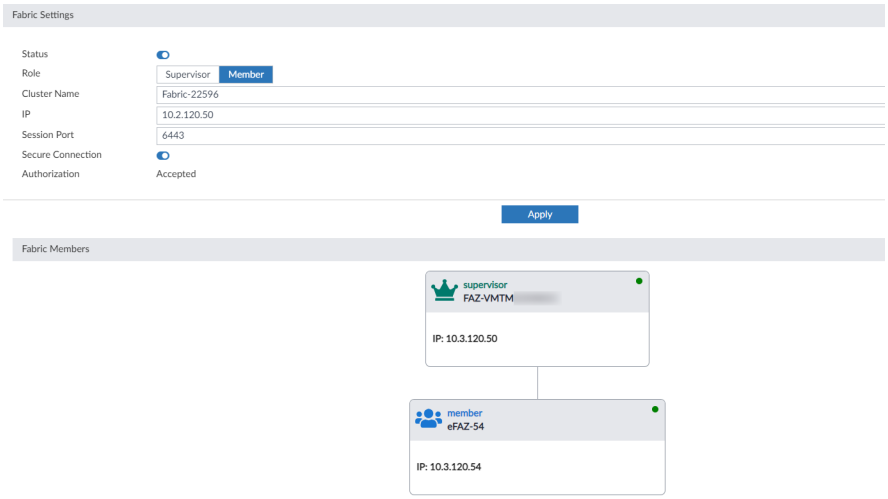
This topic includes the following processes:

Once the supervisor and the members are connected and synchronized, they display in *System Settings* > *Fabric Management* > *Fabric Settings* for the supervisor. You can hover over the role of a FortiAnalyzer Fabric member in the topology to display more information, including its serial number, version, and disk usage.



For more information about the devices, go to *Device Manager* in the FortiAnalyzer Fabric supervisor. See Device Manager on page 14.

The topology is also visible in *System Settings* > *Fabric Management* > *Fabric Settings* for the FortiAnalyzer Fabric members; however, it only displays that members connection to the supervisor.



Configuring a supervisor

To configure a supervisor from the CLI:

1. In the FortiAnalyzer Fabric supervisor CLI, enter the following commands to enable soc-fabric communication:
```
config system interface
   edit <interface used for soc-fabric communication>
      set allowaccess soc-fabric (enable other types of interface access as
           needed, for example https)
```
2. Enter the following commands to configure the supervisor:
```
config system soc-fabric
   set status enable
   set role supervisor
   set name <create the FortiAnalyzer Fabric name>
   set port 6443 <set the communication port if not using the default one>
   set secure-connection {enable | disable}
   next
end
```

To configure a supervisor from the GUI:

1. In the FortiAnalyzer Fabric supervisor, go to *System Settings* > *Network*, and edit the port that will be used for FortiAnalyzer Fabric communication.
2. For *Administrative Access*, enable *FortiAnalyzer Fabric*. Enable other types of interface access as needed as well.
3. Click *OK*.
4. In the FortiAnalyzer Fabric supervisor, go to *System Settings* > *Fabric Management* > *Fabric Settings*.

5. Set *Status* to *enabled*.
6. Configure the following settings for the supervisor, and then click *Apply* to save.

Role	Select *Supervisor*.
Cluster Name	Type a name for the FortiAnalyzer Fabric.
Session Port	Default = *6443*. Type the communication port if not using the default.
Secure Connection	Enable or disable secure connection.

Configuring a member

FortiAnalyzer Fabric allows multiple FortiAnalyzers to act as fabric members. Each FortiAnalyzer in Analyzer mode must be individually configured as a member to participate in the FortiAnalyzer Fabric.

To configure a member from the CLI:

1. In the FortiAnalyzer Fabric member CLI, enter the following commands to enable soc-fabric communication:
```
config system interface
   edit <interface used for soc-fabric communication>
      set allowaccess soc-fabric (enable other types of interface access as
           needed, for example https)
```
2. Enter the following commands to configure the member:
```
config system soc-fabric
   set status enable
   set role member
   set name <enter the FortiAnalyzer Fabric Name>
   set supervisor <enter the IP/FNDN of the supervisor>
   set port 6443 <set the communication port if not using the default one>
   set secure-connection {enable | disable}
   next
end
```

The member can now be authorized by the FortiAnalyzer Fabric supervisor.

To configure a member from the GUI:

1. In the FortiAnalyzer Fabric member, go to *System Settings* > *Network*, and edit the port that will be used for FortiAnalyzer Fabric communication.
2. For *Administrative Access*, enable *FortiAnalyzer Fabric*. Enable other types of interface access as needed as well.
3. Click *OK*.
4. Go to *System Settings* > *Fabric Management* > *Fabric Settings*.
5. Configure the following settings for the member, and then click *Apply* to save.

Role	Select *Member*.
Cluster Name	Type the name of the FortiAnalyzer Fabric.
IP	Type the IP of the supervisor for the FortiAnalyzer Fabric.

Session Port	Default = *6443*. Type the communication port if not using the default.
Secure Connection	Enable or disable secure connection.

The member can now be authorized by the FortiAnalyzer Fabric supervisor.

Authorizing members

After the members are configured, they must be authorized by the supervisor. You can authorize the members manually from the GUI, or you can authorize them automatically by creating a `trusted-list` on the FortiAnalyzer Fabric supervisor before configuring the members. A `trusted-list` can also be configured on the member to verify the legitimacy of the supervisor.

To authorize a member from the GUI:

1. In the FortiAnalyzer Fabric supervisor, go to *System Settings* > *Fabric Management* > *Fabric Settings*.
2. In the topology, find the card for the member.
3. In the card for the member, click *Authorize*.
   If you click *Reject*, the member will be removed from the topology. The member will be blocked-out for 10 minutes before it can attempt to rejoin the FortiAnalyzer Fabric.
   A message asks you to confirm the action.
4. To confirm, click *OK*.
   After the member is authorized, it is connected to the FortiAnalyzer Fabric and visible in the topology on the supervisor.

To create a trusted-list on the supervisor:

1. In the FortiAnalyzer Fabric supervisor's CLI, enter the following command:
```
config system soc-fabric
   config trusted-list
      edit 1
      set serial <member's serial number>
   end
end
```
2. Add other members to the trusted-list, as needed.

The `trusted-list` on the supervisor supports wildcards (*). For example, you can enter `set serial FAZ-VMTM120033*`.

Once a member is added to the trusted-list, it will automatically be authorized when it is configured to join the FortiAnalyzer Fabric.

To create a trusted-list on a member:

1. In the FortiAnalyzer Fabric member's CLI, enter the following command:
```
config system soc-fabric
   config trusted-list
      edit 1
      set serial <Supervisor's serial number>
```

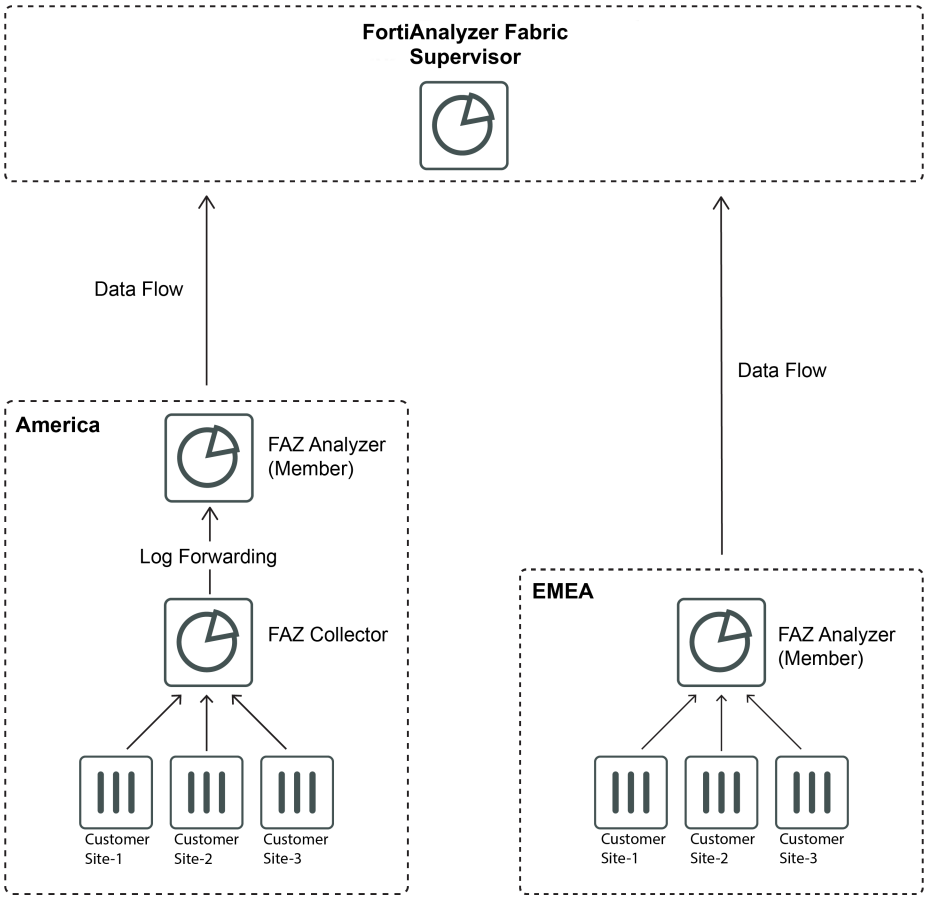
```
    end
  end
```

The member will now only join a FortiAnalyzer Fabric when the supervisor's serial number matches the `trusted-list`.

For members without a `trusted-list` configured, they will treat all supervisors as legitimate.

Deployment architecture

The following is an example of the topology that can make up the FortiAnalyzer Fabric, with the supervisor acting as the root device, and multiple FortiAnalyzer Fabric members sending information to the supervisor through the API. Information can be sent from a FortiAnalyzer operating as a Collector to an Analyzer before being synced to the supervisor. The FortiAnalyzer Fabric is ideal for use in high volume environments with many FortiAnalyzers.



Using the FortiAnalyzer Fabric supervisor

After deploying the FortiAnalyzer Fabric, you can use the supervisor as a centralized view of all devices in the Fabric.

The FortiAnalyzer Fabric supervisor includes the following features:

To filter *FortiView*, *Log View*, and *Reports* by specific FortiAnalyzer Fabric members or ADOMs, you can create Fabric Groups. See Fabric Groups on page 23.

Device Manager

In the FortiAnalyzer Fabric supervisor, the *Device Manager* is used to collect and display information from members. The supervisor will not display any information about its own devices.

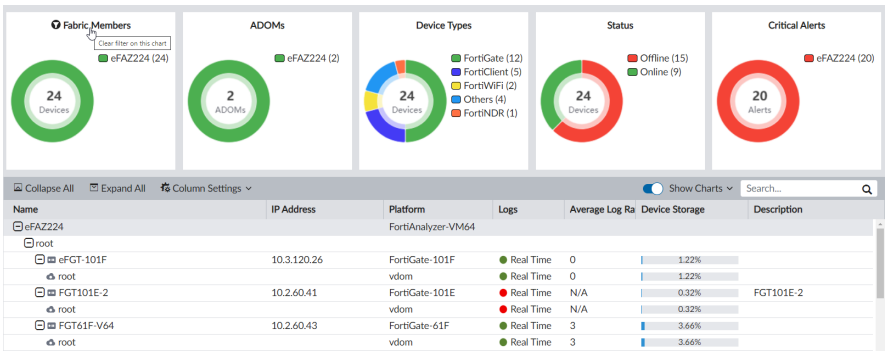
The *Device Manager* displays information about device storage, logging rates, and the current real time log status of devices registered to the FortiAnalyzer Fabric members.

Five summary charts are available in the *Device Manager*:

- *Fabric Members*
- *ADOMs*
- *Device Types*
- *Status*
- *Critical Alerts*

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

These charts provide an overview of the managed member devices in the FortiAnalyzer Fabric. You can hover your cursor over the charts to see more information about the data in a tooltip. You can also click areas in the chart or items in the legends to filter the *Device Manager* by that information. Click multiple charts and legends to apply multiple filters. A filter icon appears next to the chart title when it is used to filter the *Device Manager*. To remove the filters, click the title of the charts that were used.



The table in the *Device Manager* provides information about each FortiAnalyzer Fabric member. You can expand each member to view its ADOMs and authorized logging devices.

Device filtering can be performed in the table by searching for device information using the search field. For example, you can search "FortiGate" to view all FortiGate devices, or "100D" to view only FortiGate 100D models.

Device Manager includes the following information for each FortiAnalyzer Fabric member in the table:

Name	The name of the FortiAnalyzer Fabric member.
Serial Number	The device's serial number.
Platform	The device's platform.

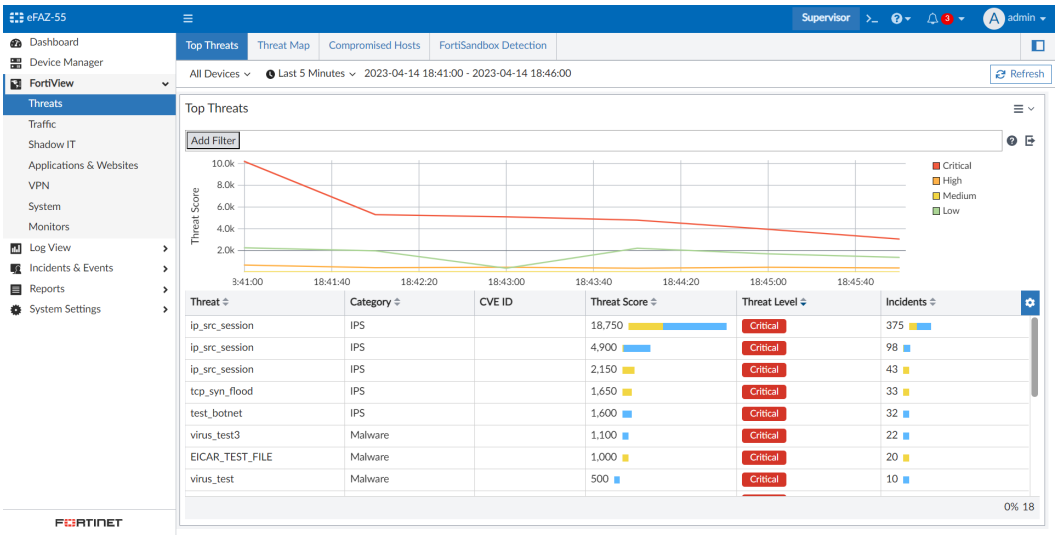
FortiAnalyzer Fabric member ADOMs are displayed below each member. Each ADOM includes their authorized logging devices. The following information is displayed for each device and VDOM in the table:

Name	The name of the device.
IP Address	The IP address of the device.
Platform	The platform of the device.
Logs	The real time log status. A green circle indicates that logs are being sent. A red circle indicates that logs are not being sent. The status indicator will turn from green to red when logs have not been sent for 15 minutes or longer.
Average Log Rate (Logs/Sec)	The average log rate per second. This information is only available when the device is sending logs in real time.
Device Storage	The amount of storage used by the device or VDOM.

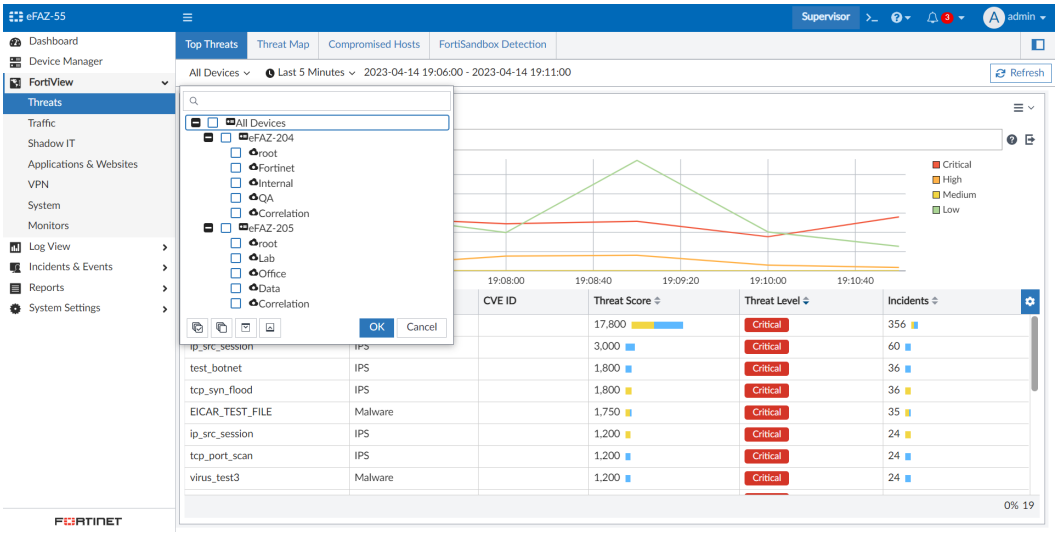
FortiView

The FortiAnalyzer Fabric supervisor allows you to see FortiView analytics across the FortiAnalyzer Fabric members. For more granular analysis, you can filter by the FortiAnalyzer Fabric members or ADOMs.

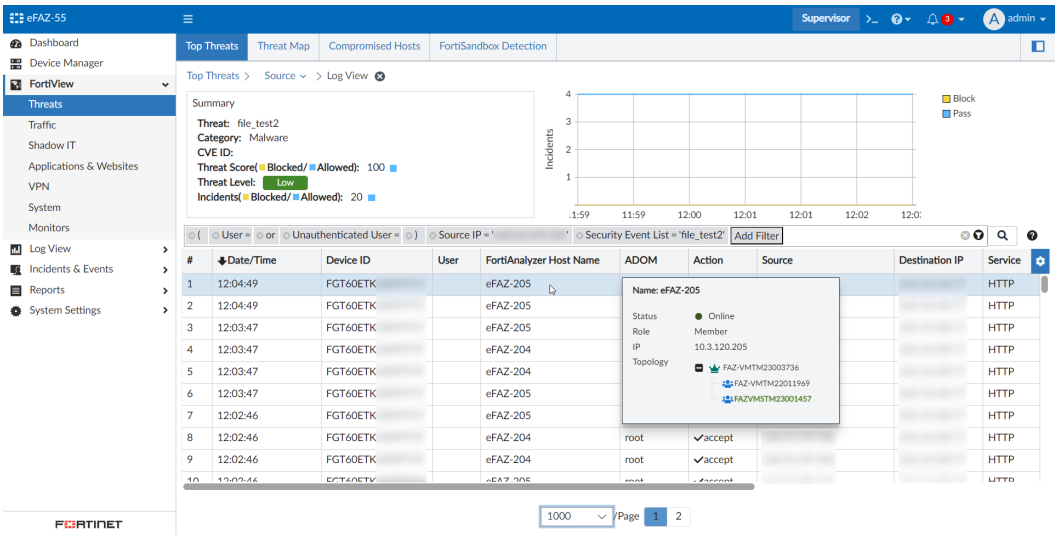
The information in supervisor's *FortiView* panes are generated from all members in the Fabric cluster. See the below example of *FortiView* > *Threats* > *Top Threats*.



The *Device Filter* dropdown in the toolbar lists FortiAnalyzer Fabric members and their available ADOMs. Select the members and ADOMs to filter the table.



Double-click an entry in the table to drill down to the *Log View* of the information. In this view, you can determine the member using the *FortiAnalyzer Fabric Host Name* column.

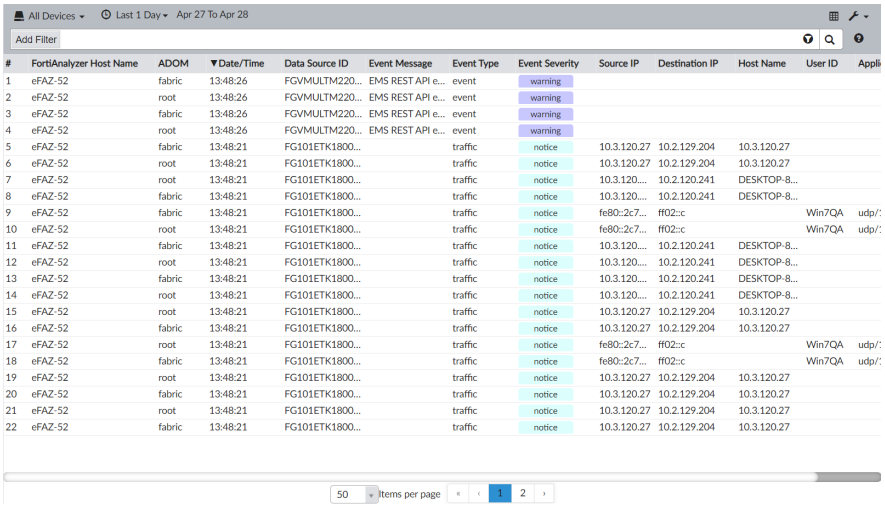


Log View

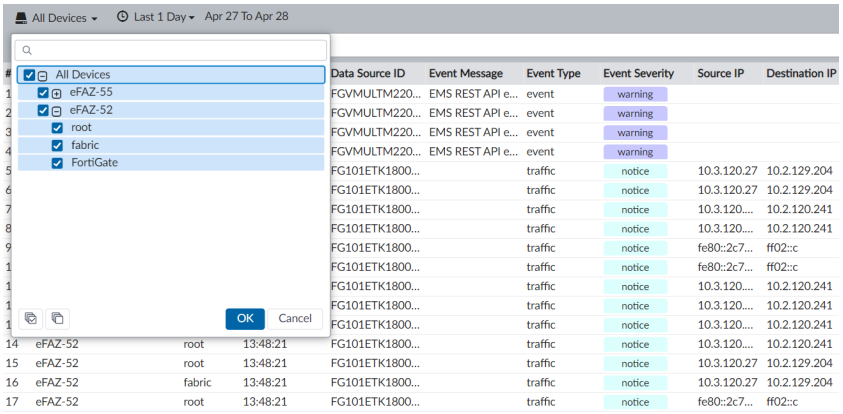
In the FortiAnalyzer Fabric supervisor, *Log View* displays logs collected on all FortiAnalyzer Fabric members. The logs contain the same information as displayed in the host FortiAnalyzer device they were collected on. The supervisor will not show any logs from its own devices; it is for centralized viewing of the members only.

Two columns are included in the FortiAnalyzer Fabric supervisor's *Log View* table to identify where the logs were collected:

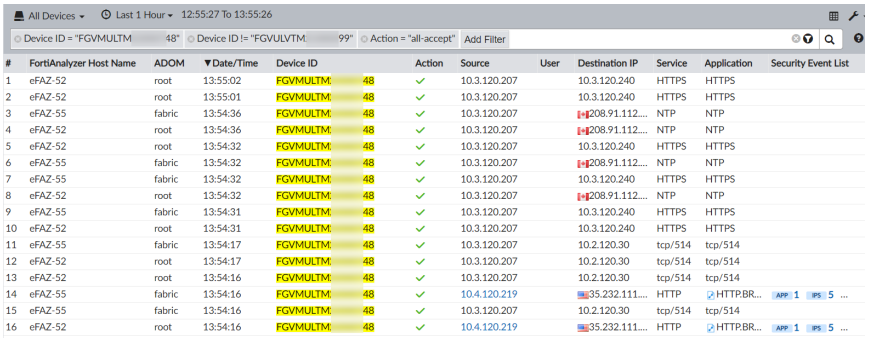
FortiAnalyzer Host Name	The host name for the FortiAnalyzer device that collected the log. To find or edit the *Host Name* for a FortiAnalyzer Fabric member, go to *Dashboard* > *System Information* in the GUI for the member device. For more information, see the FortiAnalyzer Administration Guide.
ADOM	The ADOM that the log was generated in.



The *Device Filter* dropdown in the toolbar lists FortiAnalyzer Fabric members and their available ADOMs. Select the members and ADOMs to filter list of logs in the table.

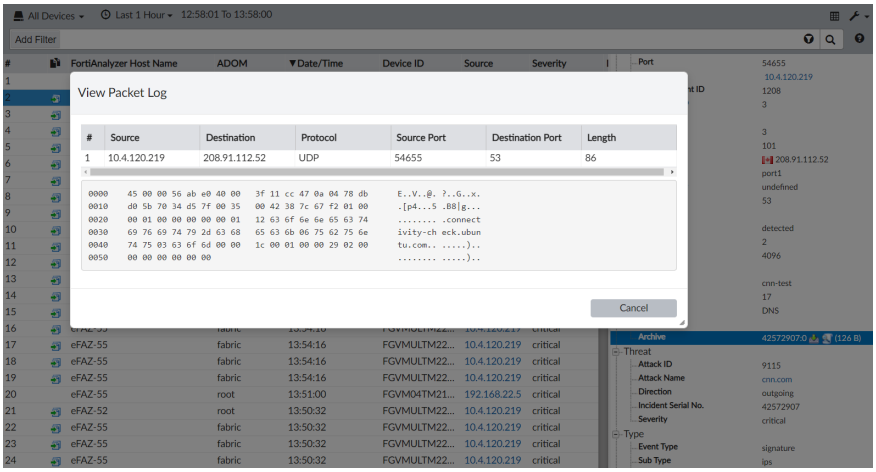


The search filter in the toolbar supports a global search across all members in the FortiAnalyzer Fabric.

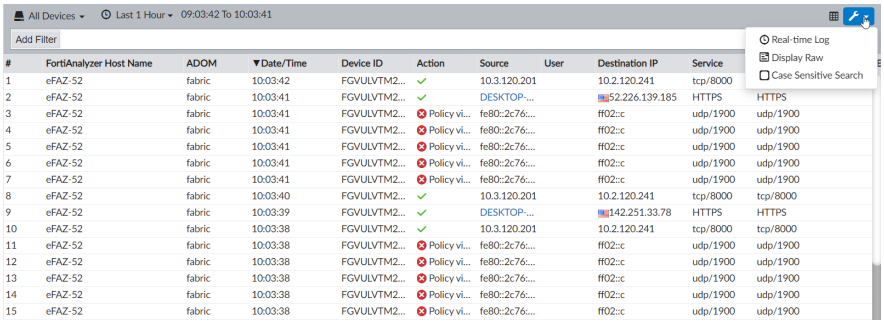


The sidebar in the supervisor's *Log View* includes most of the same menus as a typical FortiAnalyzer device. Select a menu in the sidebar to display logs from that device. For example, all FortiClient logs collected in the FortiAnalyzer Fabric are included in the *FortiClient* menu.

Administrators can view and download FortiGate archive files for security logs from the FortiAnalyzer Fabric supervisor.



The *Log View* in a FortiAnalyzer Fabric supervisor does not support *Log Group*, *Log Browse*, *Log Downloads*, *Custom View*, and *Chart Builder*. These features are available in FortiAnalyzer Fabric members and regular FortiAnalyzer devices.



All other features in *Log View* for the FortiAnalyzer Fabric supervisor are the same as the FortiAnalyzer Fabric members and regular FortiAnalyzer devices. For more information, see the FortiAnalyzer Administration Guide.

Events

On the FortiAnalyzer Fabric supervisor, *Incidents & Events* includes the following panes for monitoring events:

- Fabric Events on page 19
- Local Events on page 20

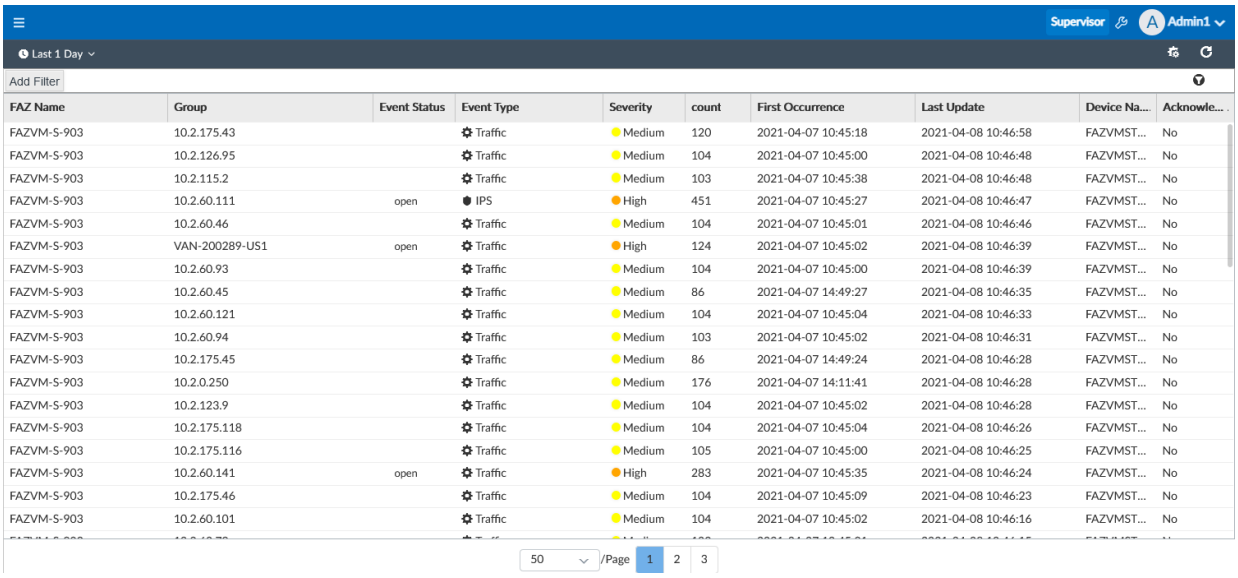
Fabric Events

The *Incidents & Events* > *Fabric Events* pane displays events created on each FortiAnalyzer Fabric member.

Event handlers must be configured on members for events to be viewable on the supervisor.

On the supervisor, events are organized into pages. You can configure the number of events that are displayed per page and navigate between the pages by using the page navigation buttons at the bottom of the pane.

Apply filters by clicking *Add Filter* or by right-clicking within a column in the events table and selecting your search parameters. You can also set time parameters from the time dropdown in the toolbar. By default, the view displays the *Last 1 Day*.



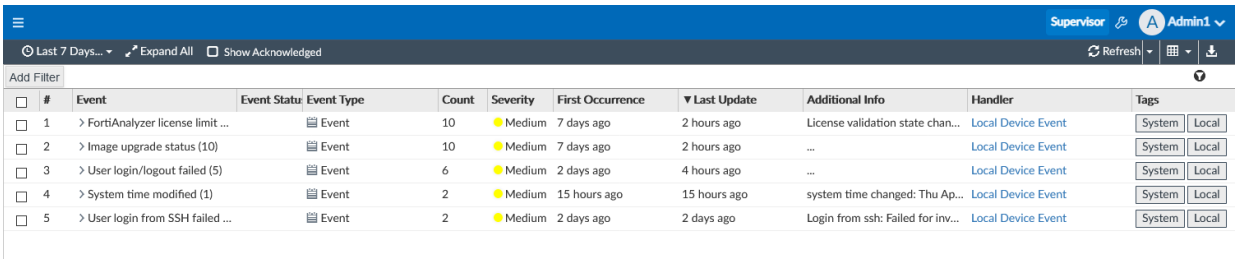
Double-click an event line to view the event group details. Event group details displays events from members in the FortiAnalyzer Fabric. The member name and ADOM is displayed in the table.

To view log details, select an event in the event group and click *View Log* from the right-click menu. You can drilldown further on each result to view event details.

Click *Search in Log View* in the right-click menu to perform a log view search using the selected event.

Local Events

The *Incidents & Events* > *Local Events* pane displays local events from the FortiAnalyzer acting as supervisor in the FortiAnalyzer Fabric. Local events include events such as license validation, system time changes, reboots, and other events that have occurred on the supervisor in the FortiAnalyzer Fabric.

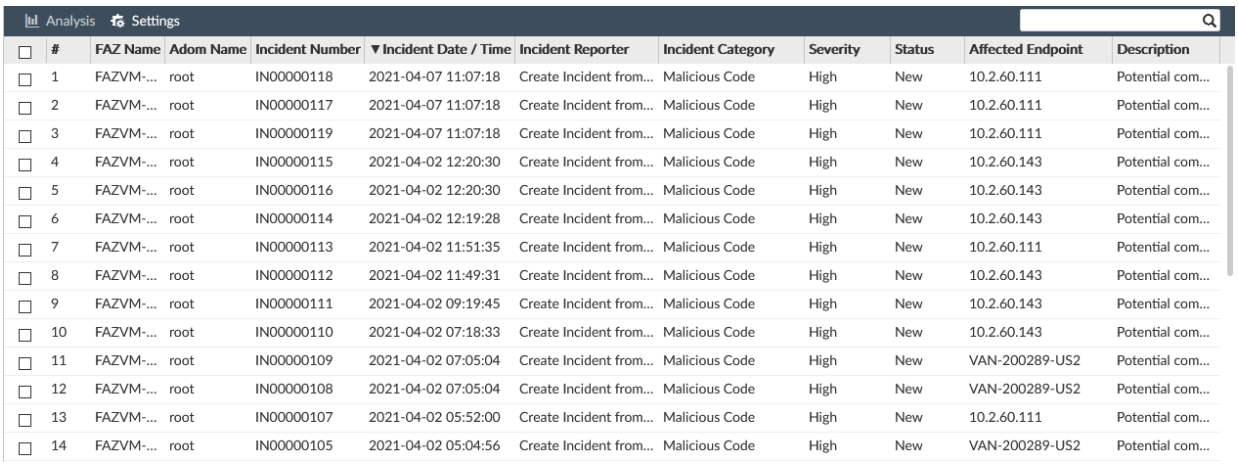


Incidents

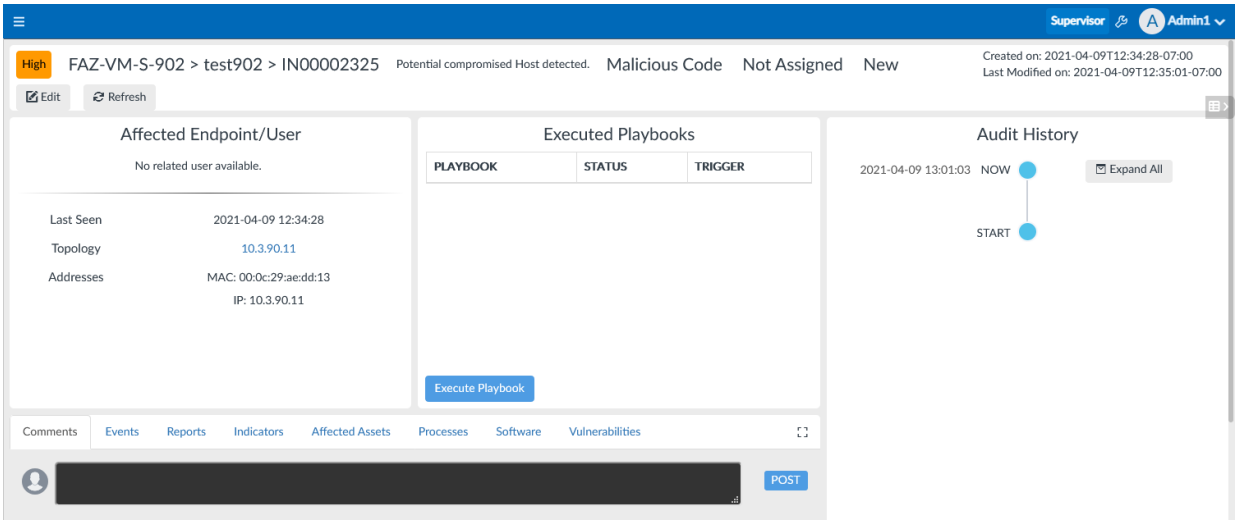
On the supervisor, *Incidents & Events* > *Incidents* displays all incidents created on FortiAnalyzer Fabric members.

Incidents contain event details, as well as information helpful for administrator analysis. From the incident's analysis page, you can view incidents, audit history, and attached reports, events, and comments.

Incident information syncs from members to the supervisor. New incidents can only be raised on FortiAnalyzer Fabric members.



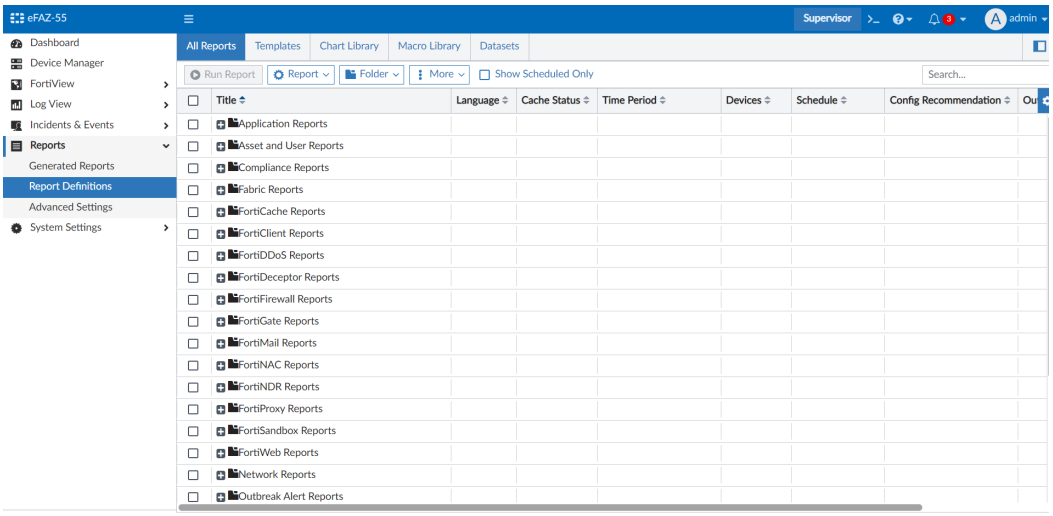
Double-click on an incident to view the incident analysis page. The incident analysis page indicates the FortiAnalyzer and ADOM that the incident was created on. For more information on the options available to SOC analysists, see the FortiAnalyzer Administration Guide.



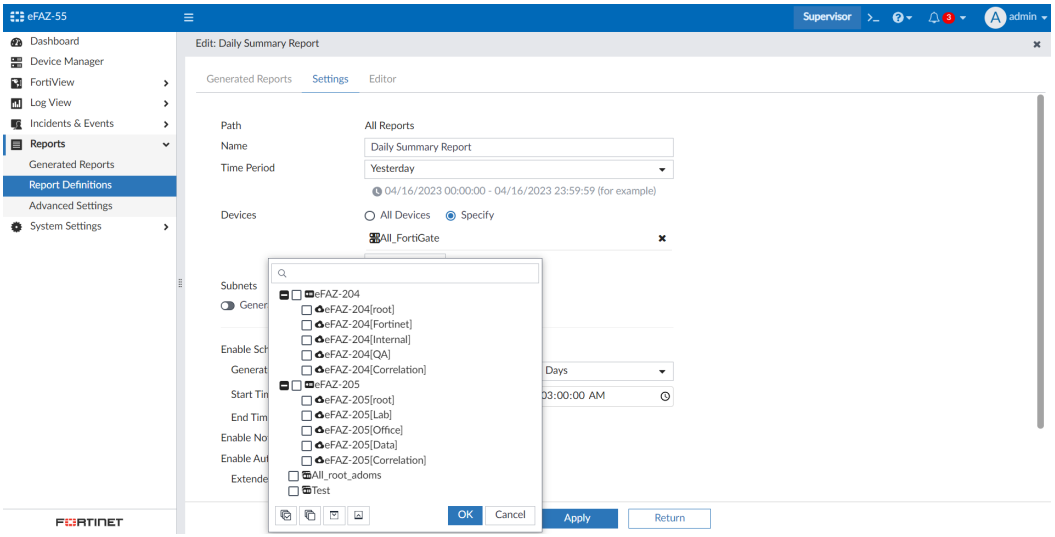
Reports

For *Reports*, the FortiAnalyzer Fabric supervisor is able to fetch and aggregate data from multiple members in the FortiAnalyzer Fabric.

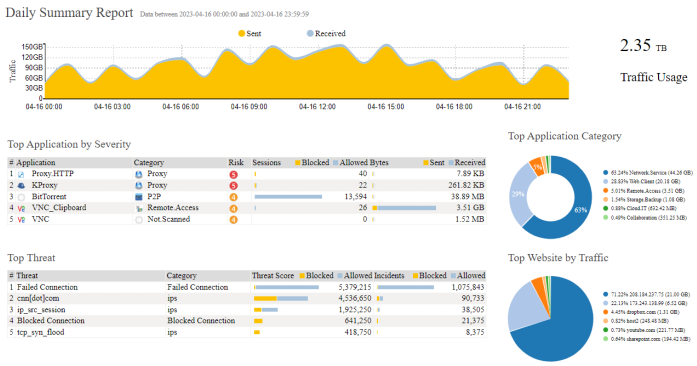
FortiAnalyzer Fabric members and supervisors can have different timezones. When running reports, the supervisor's local timezone is used. When the supervisor collects data from members, the requested time period is first converted to epoch and then passed down to each member to get the data within that time period.



To specify which Fabric members, ADOMs, and/or Fabric Groups to include when running a report, go to *Reports* > *Report Definitions* > *All Reports* in the supervisor. Select the check box for the report and, from the right-click menu, click *Edit*. In the *Settings* tab, specify the devices to include when running the report and click *Apply*.



The reports' formats, charts, and tables are the same as a regular FortiAnalyzer Fabric's, but they include aggregated results from all the selected members.

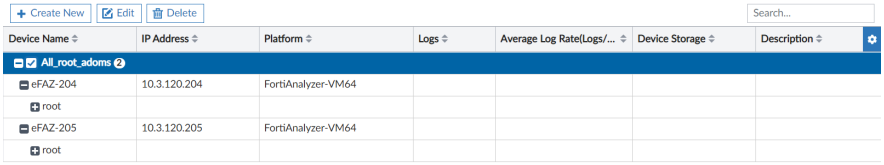


Fabric Groups

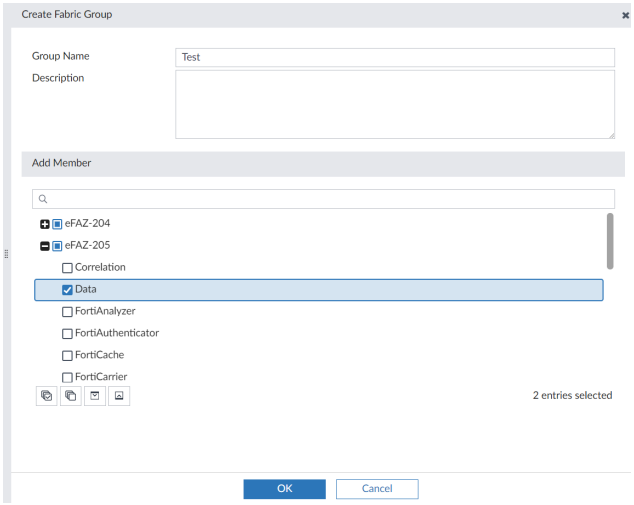
You can create Fabric Groups in the FortiAnalyzer Fabric supervisor. These Fabric Groups contain FortiAnalyzer Fabric members or ADOMs. They are visible in *Device Manager* and can be used to filter *FortiView*, *Log View*, and *Reports*.

To create a Fabric Group:

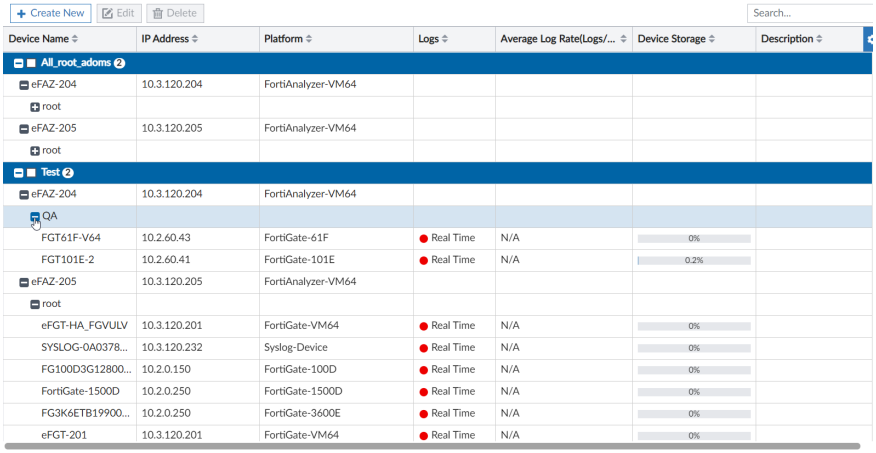
1. In the FortiAnalyzer Fabric supervisor, go to *System Settings* > *Fabric Management* > *Fabric Groups*.



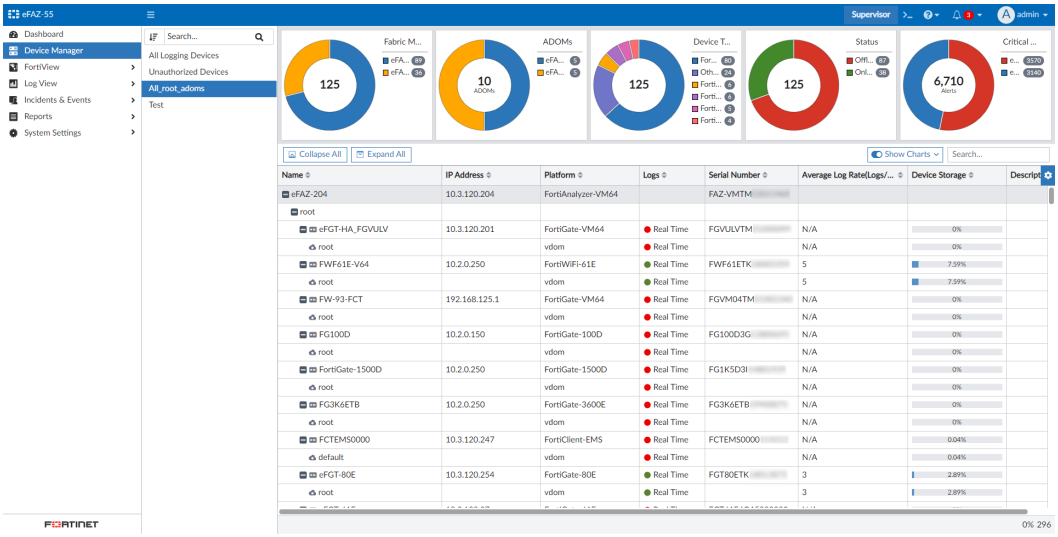
2. Click *Create New*.
3. In the *Group Name* field, enter a name for the Fabric Group.
4. In the *Add Member* section, select the FortiAnalyzer Fabric members to include.
   To add only specific ADOMs from the member, expand the member in the list and select the ADOMs to include.



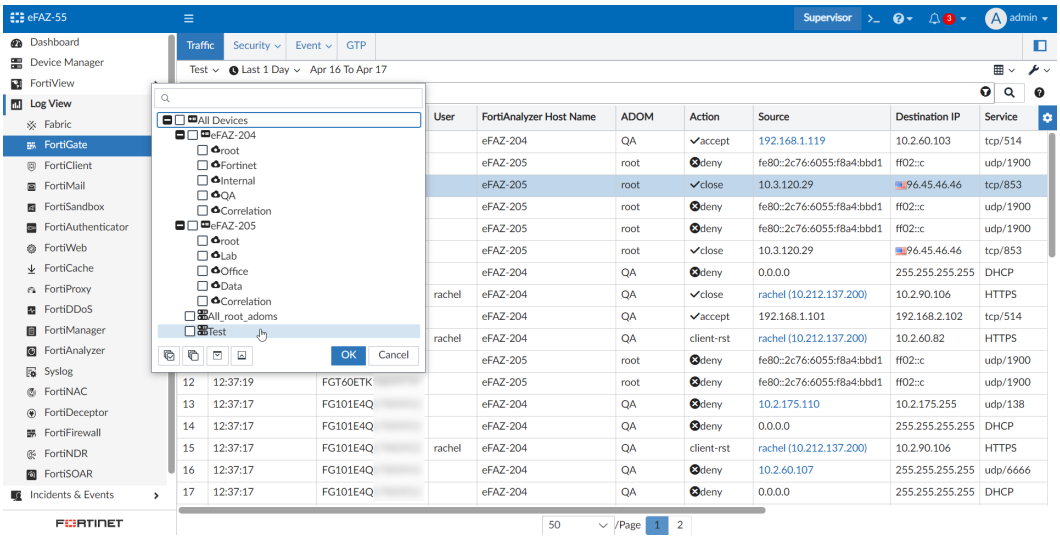
5. Click *OK*.
   The Fabric Group can now be edited or deleted from the table.



The Fabric Group is also visible in *Device Manager*.



It can be selected in the device filter for *FortiView*, *Log View*, and *Reports*. See an example in *Log View* below.



High availability for FortiAnalyzer Fabric members

When using high availability (HA) for a FortiAnalyzer Fabric member, you can configure an *Active-Active* or *Active-Passive* cluster. The HA primary node will display the same as a standalone member in the FortiAnalyzer Fabric. The member is synced to the secondary node, but the secondary node will not establish a connection to the FortiAnalyzer Fabric until there is a failover scenario.

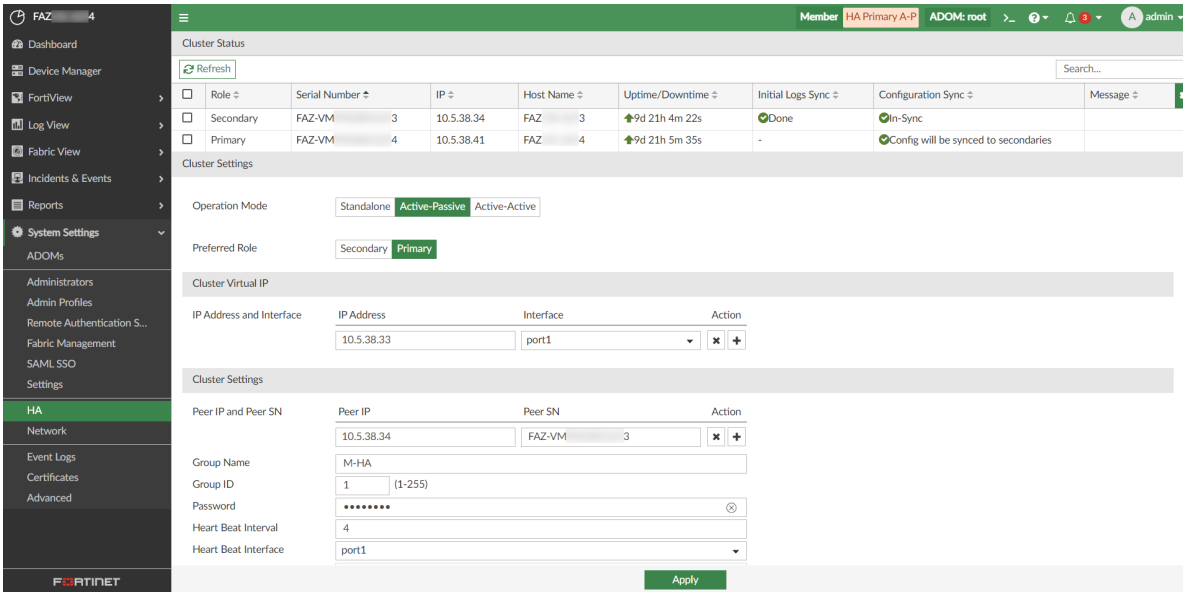
For complete instructions to to set up FortiAnalyzer HA, see the FortiAnalyzer Administration Guide.

HA is not supported on the FortiAnalyzer Fabric supervisor.

FortiAnalyzer Fabric member in HA mode:

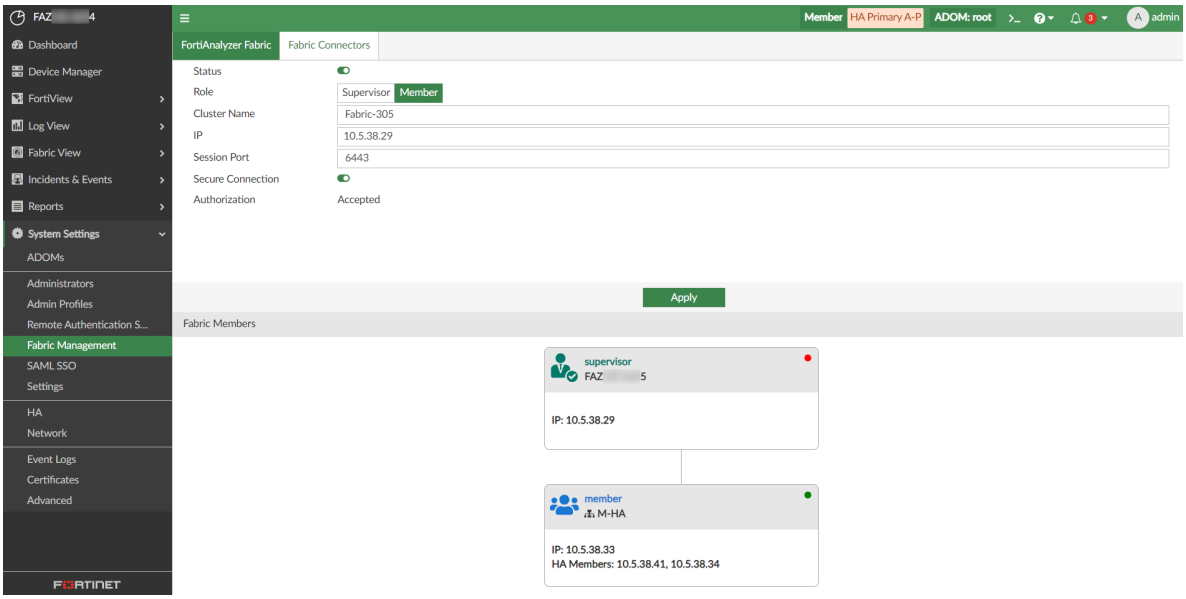
1. In the FortiAnalyzer Fabric member, you can configure the unit as part of an *Active-Passive* or *Active-Active* HA cluster.

   In the example below, the member is configured as the primary for an *Active-Passive* HA cluster.



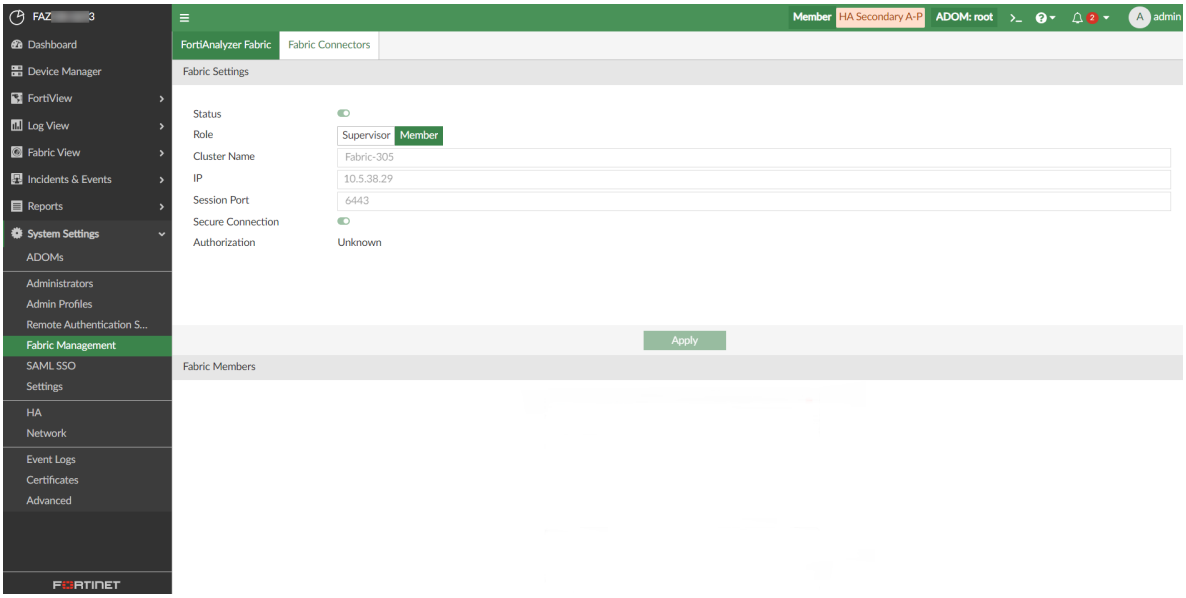
2. In the FortiAnalyzer Fabric member, go to *System Settings* > *Fabric Management* > *FortiAnalyzer Fabric*.

   In the topology chart, only the primary node establishes a connection and syncs data to the FortiAnalyzer Fabric supervisor.



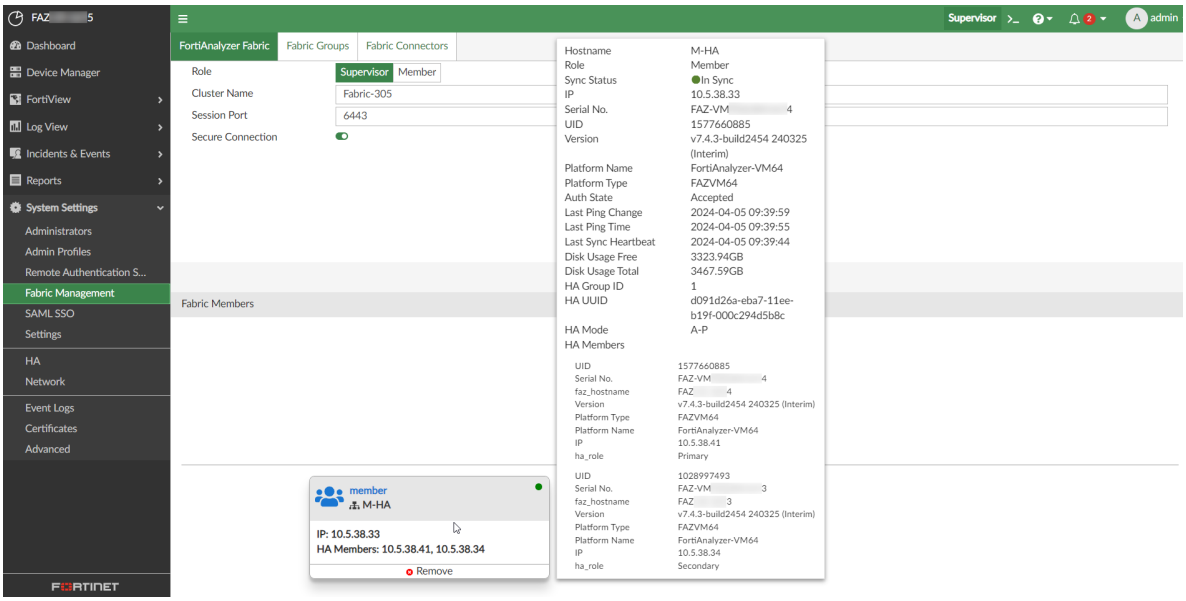
3. The FortiAnalyzer Fabric member that is the primary node syncs all *Fabric Management* configuration to the secondary node, but the secondary node will not establish the connection to FortiAnalyzer Fabric supervisor.

   In the example below, the secondary node displays the *Authorization* = *Unknown*.



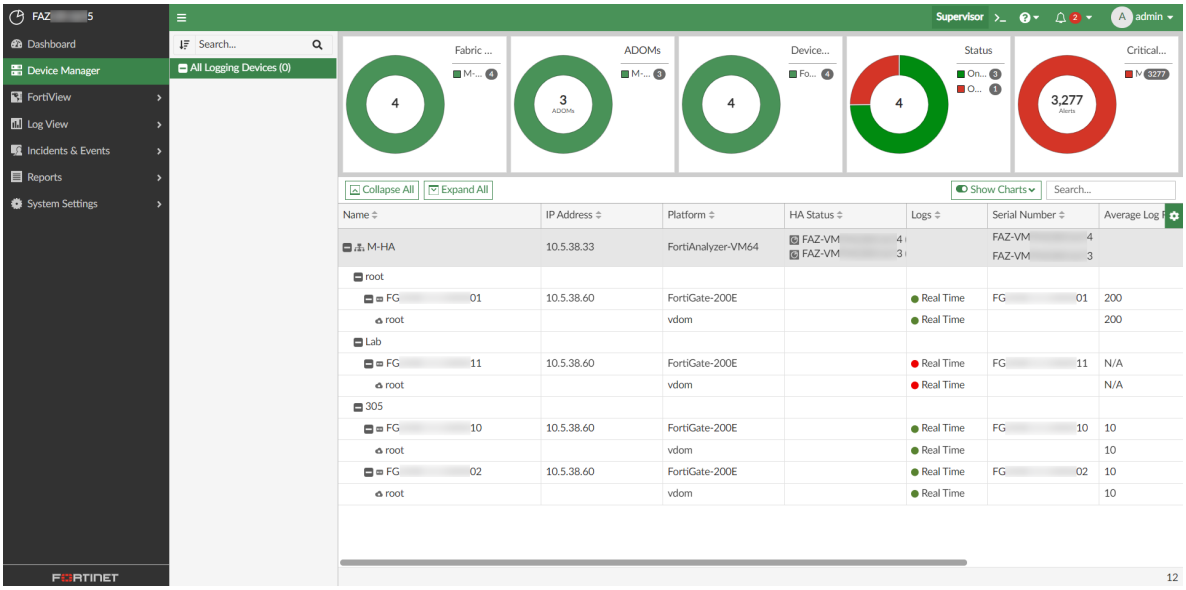
4. Once there is an HA failover for the FortiAnalyzer Fabric member, the secondary node will become the primary and it will automatically connect to FortiAnalyzer Fabric supervisor.
5. In the FortiAnalyzer Fabric supervisor, go to *System Settings* > *Fabric Management* > *FortiAnalyzer Fabric*.

   The tooltip for the member displays the HA details. The *Hostname* is the HA Group Name and the *IP* is the HA Cluster Virtual IP.



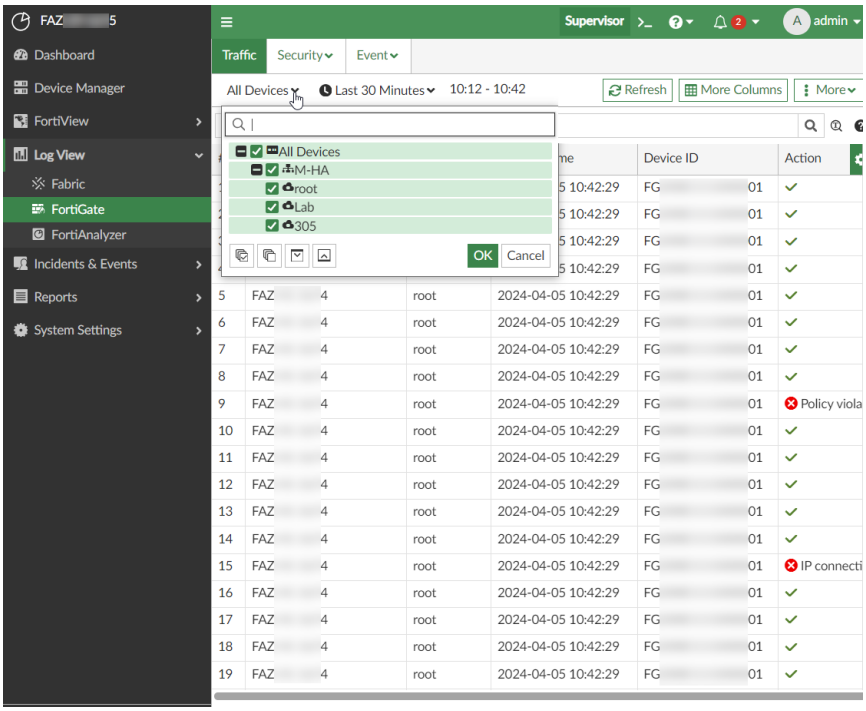
6. In the FortiAnalyzer Fabric supervisor, go to *Device Manager*.

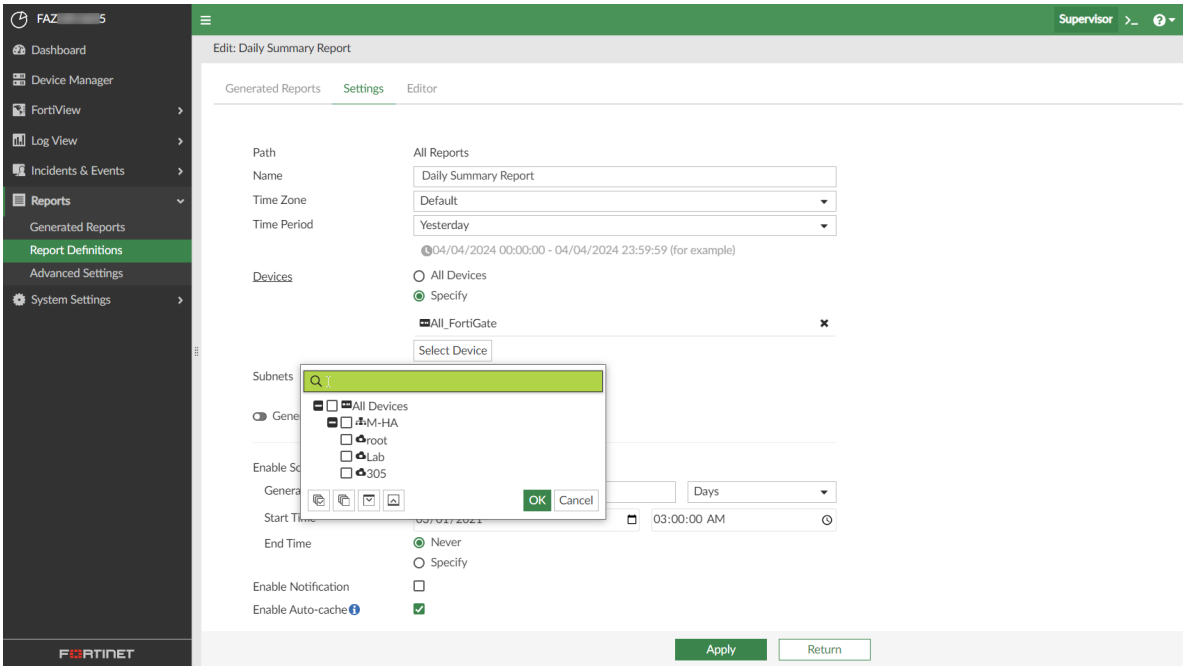
   The member's HA information is displayed in the table view.



7. In the supervisor's *Log View*, *FortiView*, and *Reports*, the HA member displays the same as a standalone member.

   See examples of *Log View* and *Reports* below.


FAZ 5
Supervisor
admin
Dashboard
Device Manager
FortiView
Log View
Fabric
FortiGate
FortiAnalyzer
Incidents & Events
Reports
System Settings
Traffic
Security
Event
All Devices
Last 30 Minutes
10:12 - 10:42
Refresh
More Columns
More
All Devices
M-HA
root
Lab
305
OK
Cancel
Device ID
Action
2024-04-05 10:42:29
Policy viola
IP connecti


FAZ 5
Supervisor
Dashboard
Device Manager
FortiView
Log View
Incidents & Events
Reports
Generated Reports
Report Definitions
Advanced Settings
System Settings
Edit: Daily Summary Report
Generated Reports
Settings
Editor
Path
All Reports
Name
Daily Summary Report
Time Zone
Default
Time Period
Yesterday
04/04/2024 00:00:00 - 04/04/2024 23:59:59 (for example)
Devices
All Devices
Specify
All_FortiGate
Select Device
Subnets
All Devices
M-HA
root
Lab
305
OK
Cancel
Days
03:00:00 AM
End Time
Never
Specify
Enable Notification
Enable Auto-cache
Apply
Return
FORTINET

Troubleshooting

Confirming a member has joined the Fabric

When adding a new member, check that the member has joined the Fabric.

To confirm that a member has joined the Fabric:

1. In the FortiAnalyzer Fabric supervisor CLI, enter the following command:
   ```
   diagnose test application fazsvcd 76 nodes
   ```
   This diagnostic shows all of the current members on the supervisor or on the member. Ensure that the *Status* for each member is *up*.

Member unable to join the Fabric

If the member does not join the Fabric, possible issues include:

- Incorrect supervisor IP
- Encryption setting mismatch between supervisor/member
- Incorrect Fabric name
- The supervisor allowaccess setting described above does not include the soc-fabric setting
- The supervisor is not reachable by the member, use ping to confirm
- The supervisor/member is not running

The supervisor uses a mixture of synchronized data and data retrieved directly from the member. This data is retrieved through the Fabric from the API service running on the member, so it is possible to view cached alert information while the member is not actually running.

Server error: Fabric member not available

Problem: When selecting an alert, the supervisor displays *Server Error: Fabric member xxx is not available*.

Description: The supervisor is not able to contact the member through the Fabric.

To troubleshoot a server error:

1. Ensure that the member has booted and is running.
2. Ensure that the member has connected to the Fabric using the following CLI command:
   ```
   diagnose test application fazsvcd 76 nodes
   ```

JSONAPI service reports error

Problem: When selecting an alert, the supervisor displays *JSONAPI Service reports: <error message>*.

Description: The member has joined the Fabric, but the API service of the member cannot service the request.

To troubleshoot a JSONAPI service reports error:

1. Ensure that the member has completely booted up.
2. Determine if the member is performing some type of database rebuild which may prevent service availability.
3. Access the members' GUI to determine if it can use its own JSONAPI service.

www.fortinet.com