FORTINET

Deployment Guide

FortiAnalyzer Fabric 7.2.0

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

FORTINET VIDEO GUIDE
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 CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 21, 2023
FortiAnalyzer Fabric 7.2.0 Deployment Guide
05-720-0793164-20230821

TABLE OF CONTENTS

Change Log

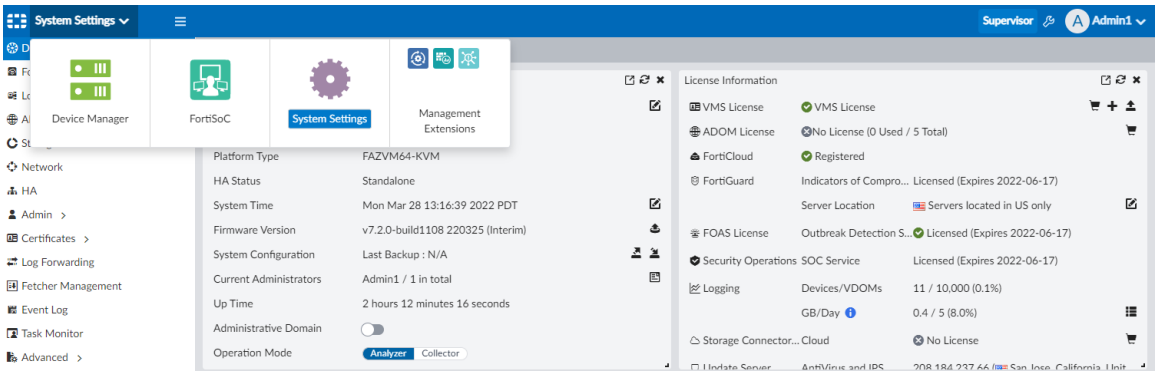
Date	Change Description
2022-04-11	Initial release.
2022-04-21	Updated Appendix B - Troubleshooting on page 16.
2023-08-08	Updated FortiAnalyzer Fabric roles on page 5.
2023-08-21	Updated Introduction on page 5.

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.
FortiSoC	Displays the *Event Monitor* and *Incidents* panes. Administrators can view incidents and events created on member FortiAnalyzer Fabric.
System Settings	Configure the settings for the FortiAnalyzer supervisor. 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.

Deployment

This section includes the following topics:

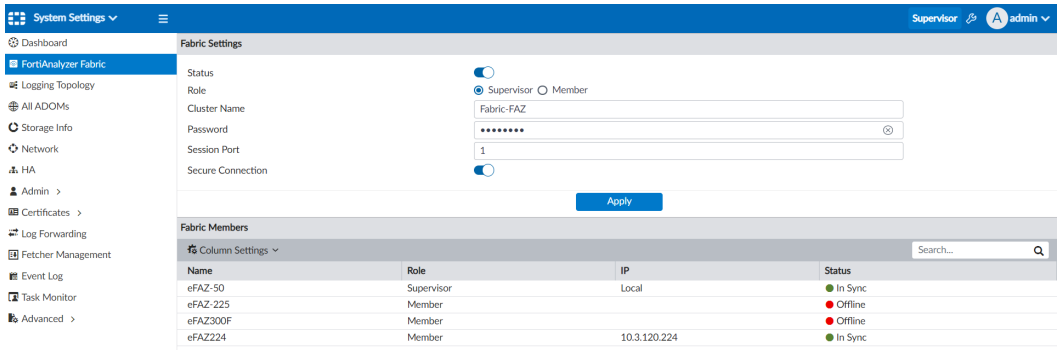
Configuring the FortiAnalyzer Fabric

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

All FortiAnalyzer Fabric members must be configured with the same timezone settings as the supervisor.

Once the supervisor and members are connected and synchronized, they display in *System Settings* > *FortiAnalyzer Fabric* for the FortiAnalyzer Fabric supervisor. The *Fabric Members* table includes the following information for each FortiAnalyzer in the FortiAnalyzer Fabric:

Name	The name of the FortiAnalyzer.
Role	The role of the FortiAnalyzer in the FortiAnalyzer Fabric (supervisor or member).
IP	The IP address of the FortiAnalyzer.
Status	The status of the FortiAnalyzer.



For more information about the devices, go to *Device Manager* in the FortiAnalyzer Fabric supervisor. See Device Manager on page 11.

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 psk <create the FortiAnalyzer Fabric password>
  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* > *FortiAnalyzer Fabric*.
2. Set *Status* to *enabled*.
3. 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.
Password	Type a password 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 psk <enter the FortiAnalyzer Fabric auth password>
    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
```

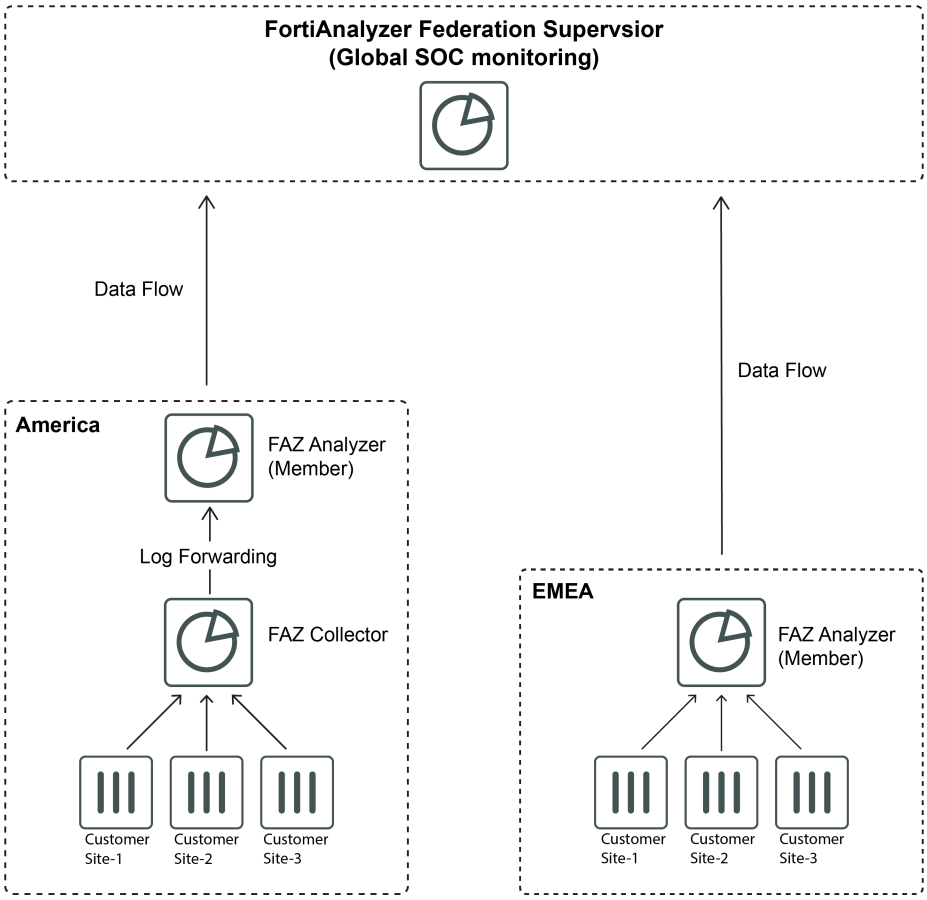
To configure a member from the GUI:

1. Go to *System Settings* > *FortiAnalyzer Fabric*.
2. 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.
Password	Type the password configured for the FortiAnalyzer Fabric.
Session Port	Default = *6443*. Type the communication port if not using the default.
Secure Connection	Enable or disable secure connection.

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

The FortiAnalyzer Fabric supervisor includes the following features:

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.

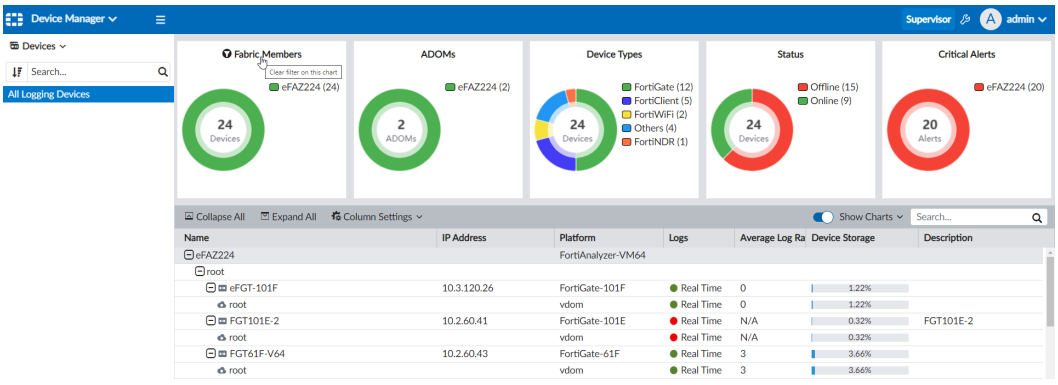
The *Device Manager* displays information about device storage, logging rates, and the current real time log status of devices registered to the FortiAnalyzer Fabric members.

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

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

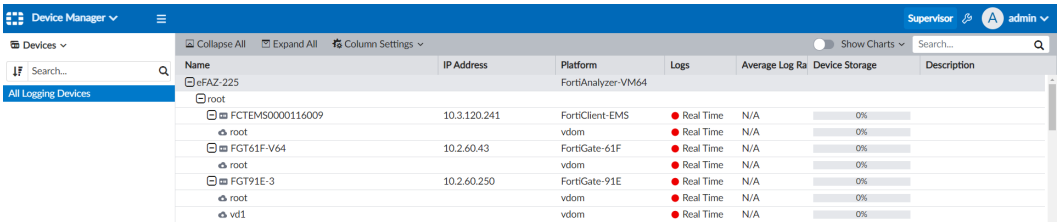
By default, the *Show Charts* toggle is enabled. You can select which charts appear by selecting them in the *Show Charts* dropdown, or you can hide all the charts by disabling the *Show Charts* toggle.

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.
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.

Event Monitor

On the FortiAnalyzer Fabric supervisor, the event monitor includes *All Events* and *Supervisor Local Events panes*.

- All Events on page 12
- Supervisor Local Events on page 13

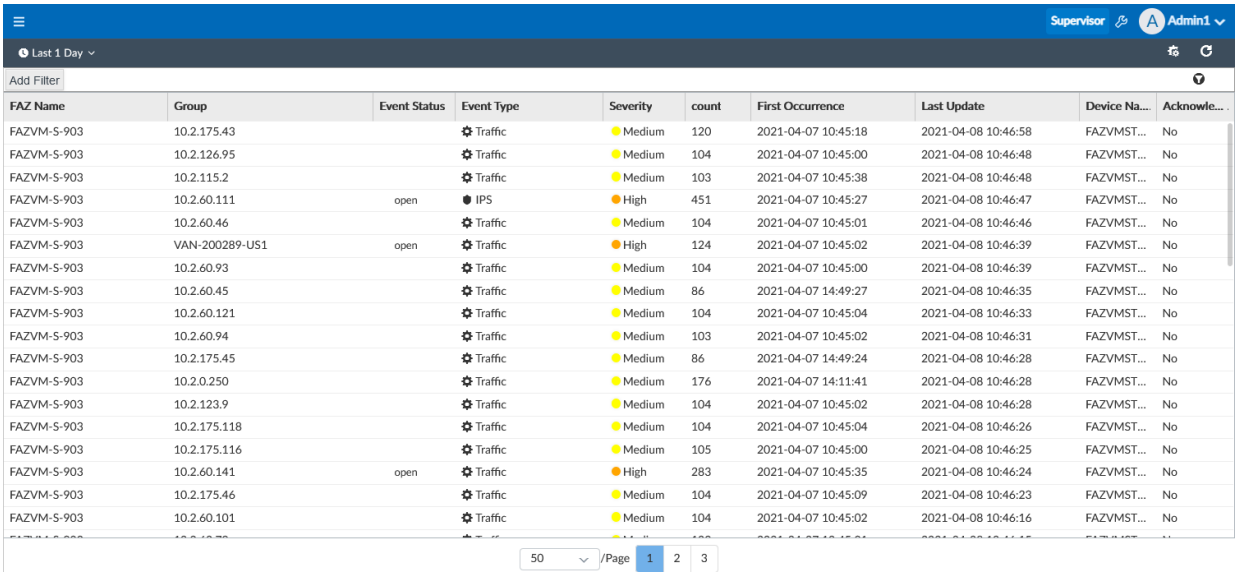
All Events

The *All 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*.



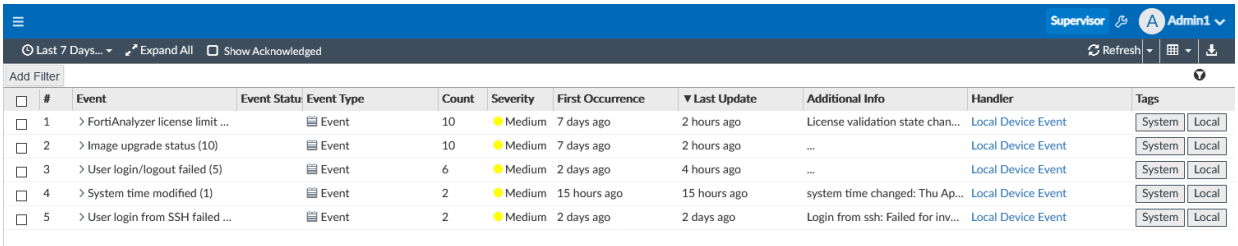
Double-click an event line to view the event group details. Event group details displays events from members in the FortiAnalyzer Fabric. The member name and ADOM is displayed in the table.

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

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

Supervisor Local Events

Supervisor Local Events shows 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.

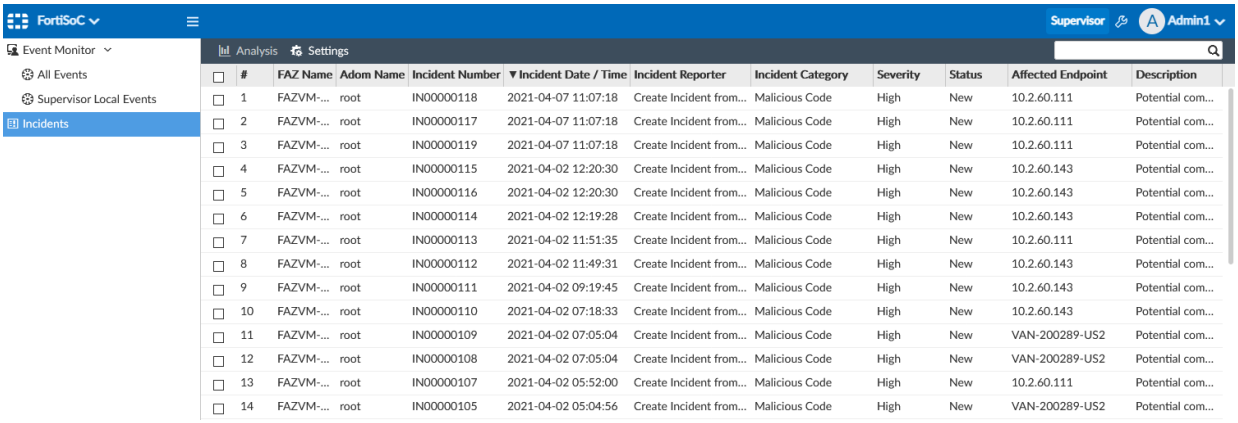


Incidents

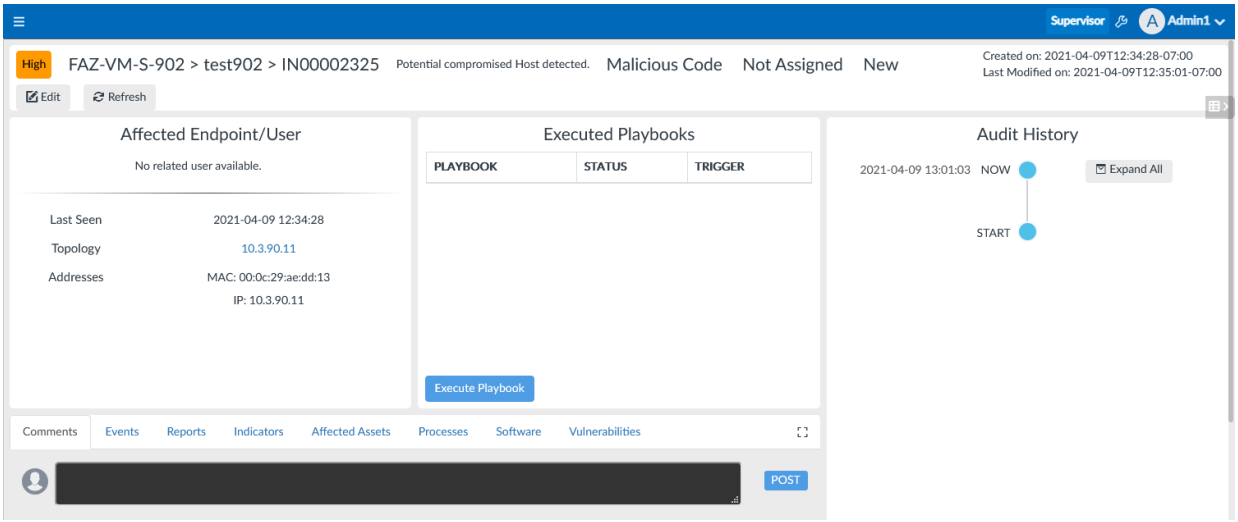
On the supervisor, *Incidents* displays all incidents created on FortiAnalyzer Fabric members.

Incidents contain event details, as well as information helpful for administrator analysis. From the incident's analysis page, administrators 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.



Appendix A - FortiAnalyzer Fabric limitations

FortiAnalyzer Fabric includes the following limitations in 7.2.0:

- FortiAnalyzer Fabric supports the creation of incidents, event handlers, and events on members with centralizing viewing from the supervisor.
- FortiAnalyzer Fabric supports log analysis, including *LogView* and *Reports*, on FortiAnalyzer Fabric members.
- Incidents on the FortiAnalyzer Fabric supervisor are available in read-only mode.
- FortiAnalyzers configured in high availability (HA) mode can join the FortiAnalyzer Fabric as members. HA is not supported for FortiAnalyzer Fabric supervisors.

Appendix B - 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
- Incorrect PSK
- 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 JSONAPI 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 JSONAPI service of the member cannot service the request.

To troubleshoot a JSON API 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