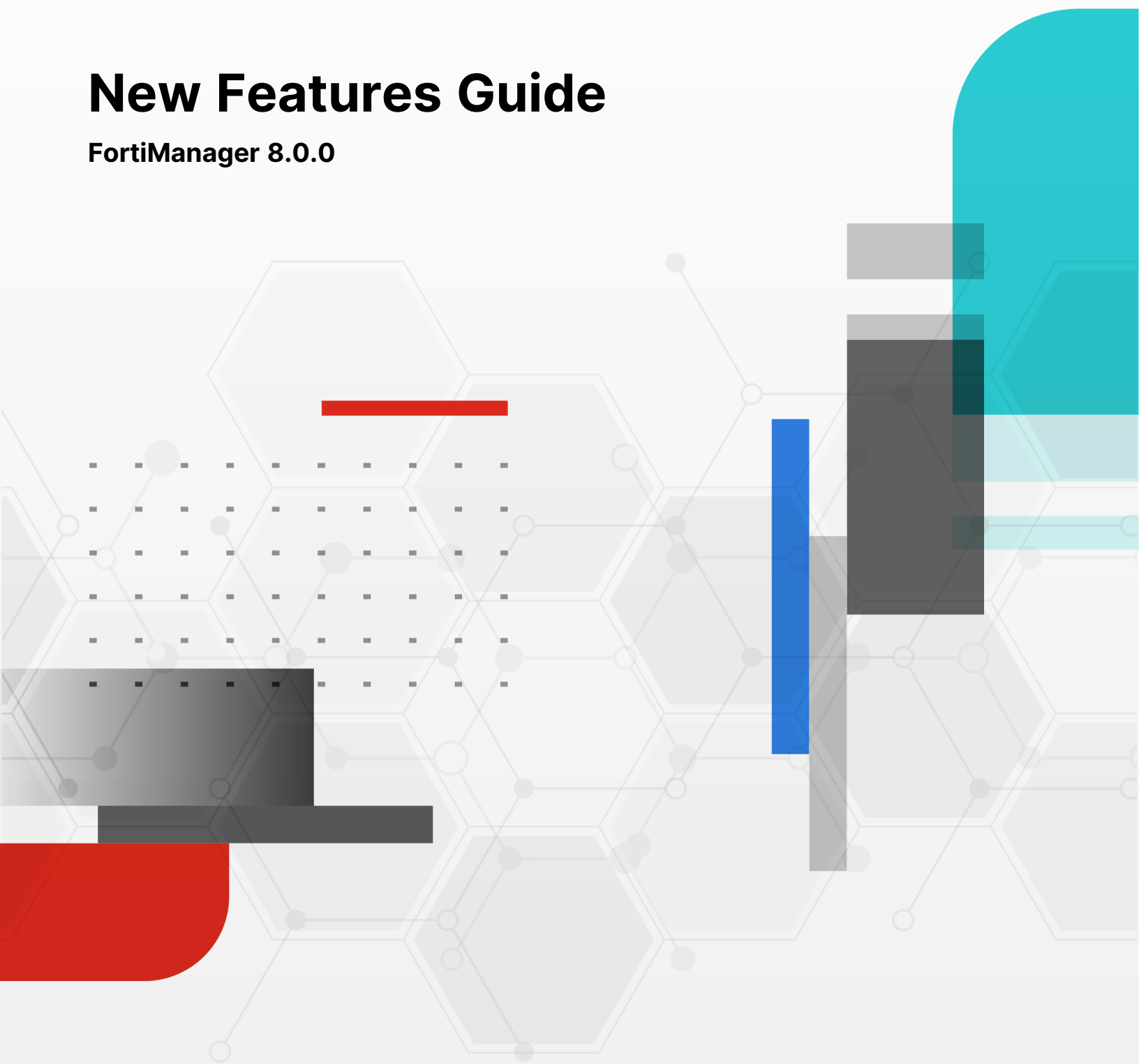


New Features Guide

FortiManager 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



April 21st, 2026

FortiManager 8.0.0 New Features Guide

02-800-1211639-20260421

TABLE OF CONTENTS

Change Log	5
Overview	6
Device Manager	7
Templates	7
Local certificates lifecycle management (set validity and renew) and expiry notification alerts	7
Central Management	15
FortiSwitch Manager	15
FortiSwitch Template adds override option to modify specific port settings on selected devices	15
Others	18
Workspace Mode supports onboarding new devices and creating new policy packages without ADOM lock	19
Interface-based bandwidth graph uses average bandwidth logic	22
FortiSwitch, FortiAP and FortiExtender templates can be assigned from Fabric Authorization Template	23
Certificate templates can be selected in model device, model HA device, and device blueprint configurations	25
New workflow mode design to control individual admin sessions with selective approvals	30
Factory default IPsec template to configure FortiClient VPN	33
Central monitoring dashboard for Firewall Users with filters for authentication method and user group	35
Maximum length of meta variables value increased to 32768 characters	39
Admin profile adds granular control on device manager (Interface, Log & Report, Security Fabric) and Routing	41
pxGrid connector is enhanced to display Device Type and Session State	44
Managing FortiGate registration to FortiCare	47
Enhanced asset details and identity monitoring	49
Administrators can create protected objects	61
FortiManager supports downgrade and roll-back for FortiGuard packages to allow setting a preferred package version for devices	66
FortiManager supports importing password-type objects from FortiGate devices with private data encryption	69
Policy and Objects	71
Policy	71
Local In policies are supported in the Global ADOM and in policy blocks	71
Fabric View	82
Connectors	82
New external connectors: GuardiCore, Microsoft Azure (Proxy Mode), and Application Centric Infrastructure (ACI Proxy Mode)	82
FortiAI Ops connector	87
Central management for ACI features	98

FortiAI	101
FortiAI can diagnose, troubleshoot, and remediate slow access to cloud or on-premise servers and applications	101
Example 1: Network is slow from IP 10.1.1.10 to Salesforce application	102
Example 2: Network slow between IP 10.1.1.10 to YouTube	104
Example 3: Network slow between IP 10.1.1.10 to 10.1.2.10	106
Example 4: Network slow between IP 10.1.1.10 and cloud server 172.20.1.10	108
System	110
Others	110
Legal third party disclosure panel	110
Custom session labels in FortiManager event logs	112
Index	116
8.0.0	116

Change Log

Date	Change Description
2026-04-21	Initial release.

Overview

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

The FortiManager new features are organized into the following categories:

- [Device Manager on page 7](#)
- [Central Management on page 15](#)
- [Policy and Objects on page 71](#)
- [Fabric View on page 82](#)
- [FortiAI on page 101](#)
- [System on page 110](#)

For a list of all features organized by the version number that they were introduced, see [Index on page 116](#).

Device Manager

This section lists the new features added to FortiManager for the device manager:

- [Templates on page 7](#)

Templates

This section lists the new features added to FortiManager for templates:

- [Local certificates lifecycle management \(set validity and renew\) and expiry notification alerts on page 7](#)

Local certificates lifecycle management (set validity and renew) and expiry notification alerts



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

- [Managing certificate templates](#)
- [Renewing local certificates](#)

FortiManager has added support for configuring a validity period for certificates generated through certificate templates. You can renew certificates through the FortiManager GUI, and are notified when a managed device has certificates expiring within 30 days.

This topic includes the following:

- [Configure a validity period for certificates on page 7](#)
- [Generate and renew certificates on page 8](#)
- [View expiring certificates from the notifications page on page 12](#)



Only *Local* type certificates support configuration of a validity period and certificate renewal. *External* type certificates do not support these features.

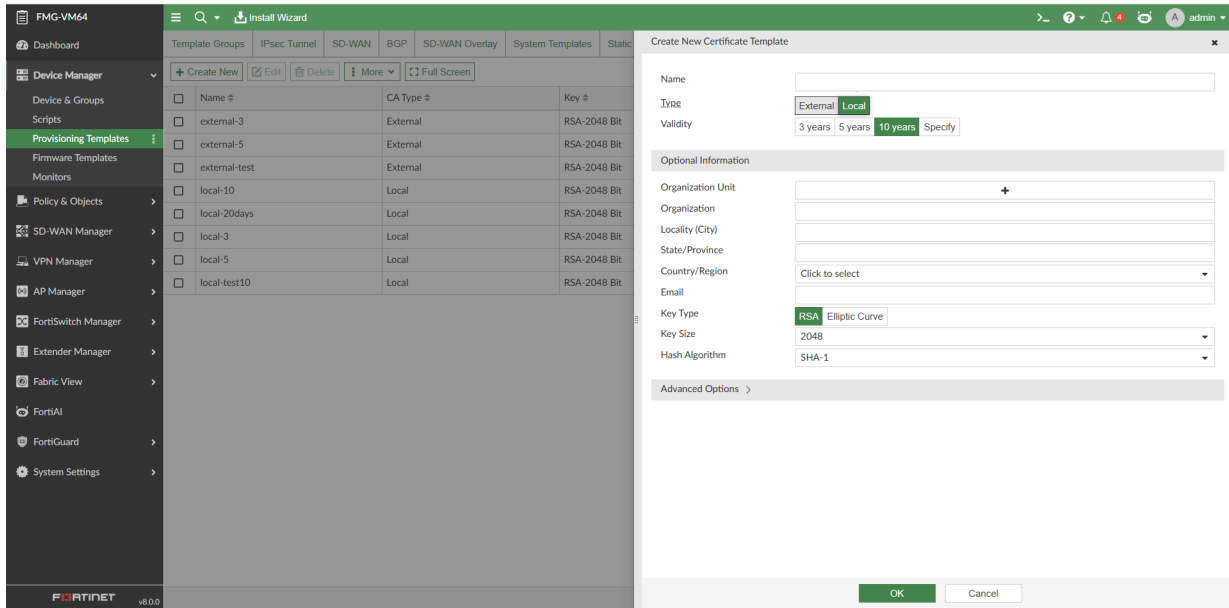
Configure a validity period for certificates

To set a validity period for certificates generated by a certificate template:

1. Go to *Device Manager > Provisioning Templates > Certificate*.
2. Click *Create New*.
3. Select the *Type* as *Local*.

4. Set the *Validity* period.

The local type certificate supports the option to generate a certificate with a validity period of 3 years, 5 years, 10 years, or to specify a custom period up to 3650 days.



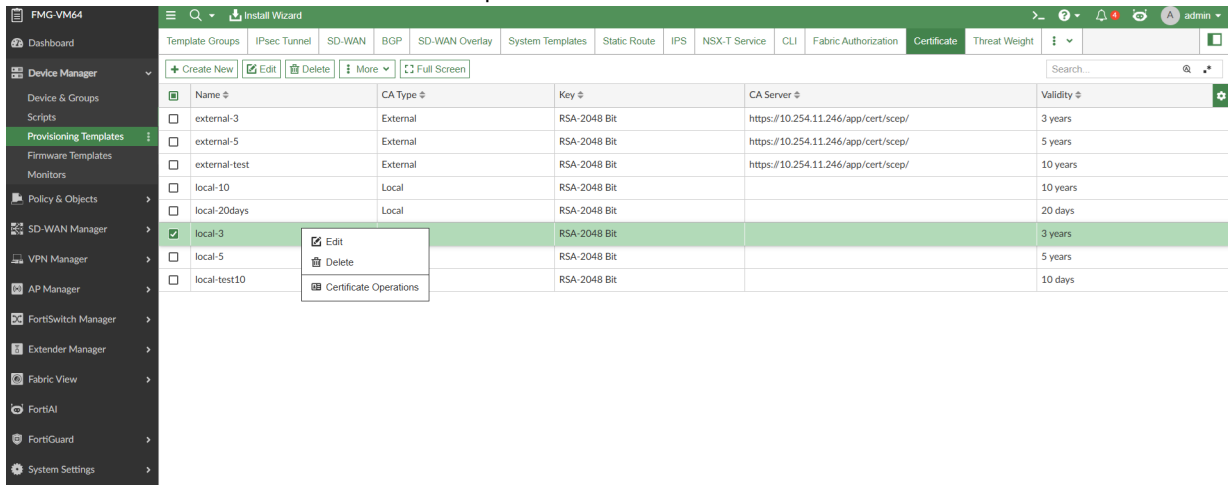
5. Configure the remaining information as needed, and click *OK* to create the certificate template.

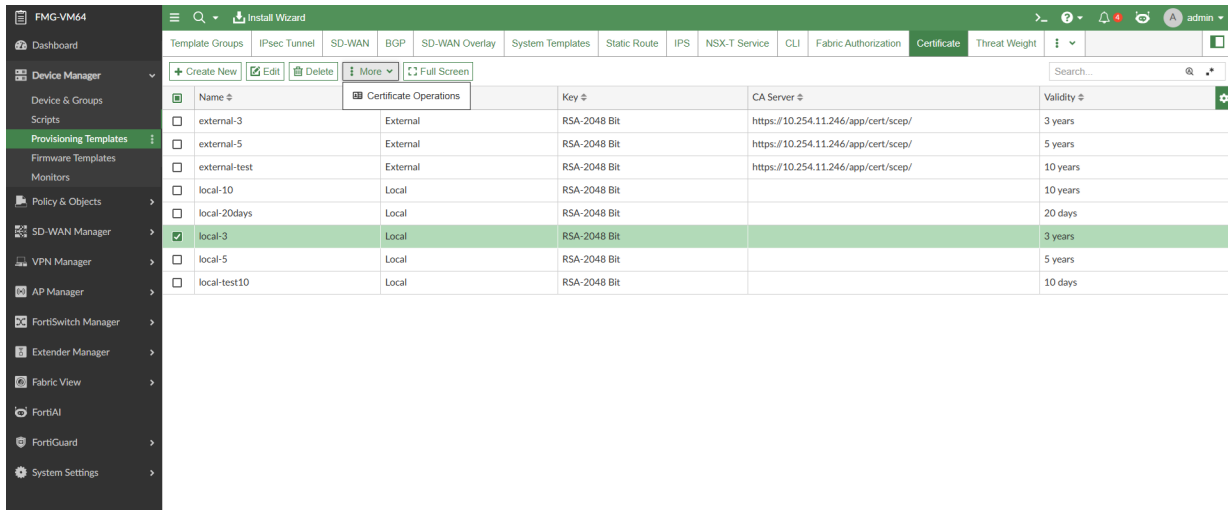
Generate and renew certificates

To generate and renew certificates:

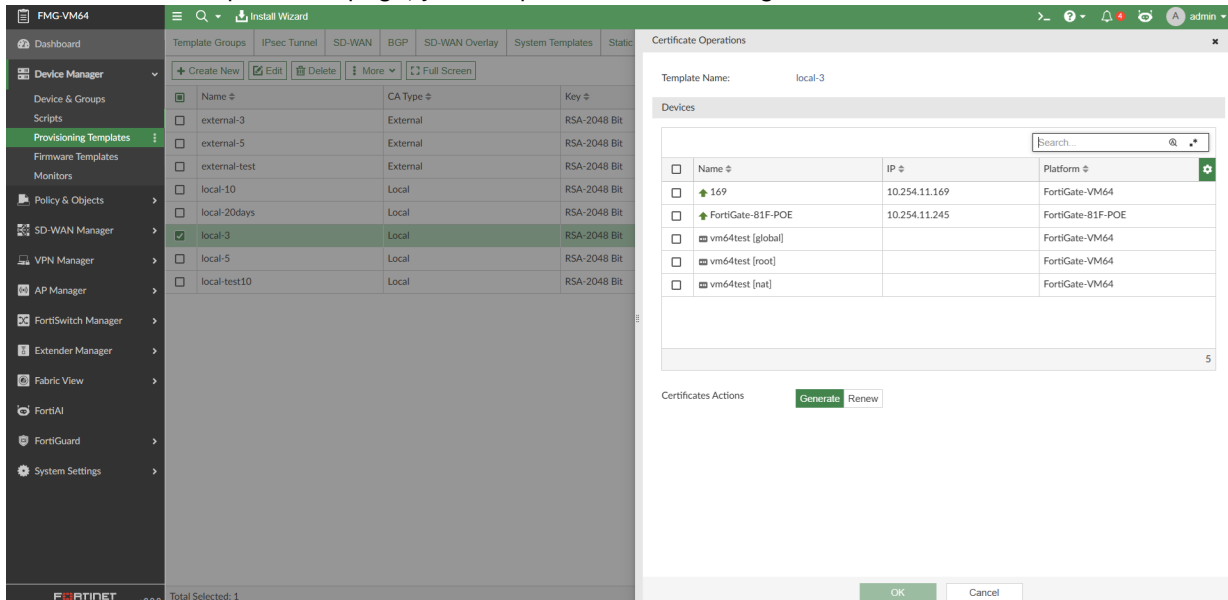
1. Generate the certificate from the right-click menu or the more button
2. Right-click on a configured certificate and click *Certificate Operations* or select *More > Certificate Operations* from the toolbar.

The *Certificate Operations* page opens. This dialog is where the administrator can generate and renew certificates based on this certificate template.

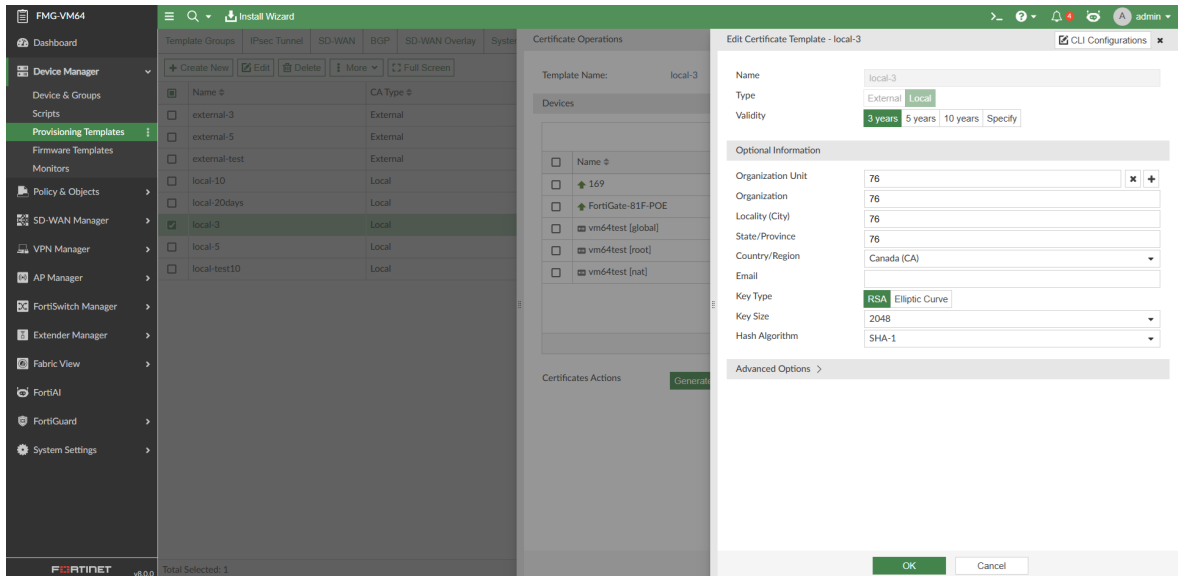




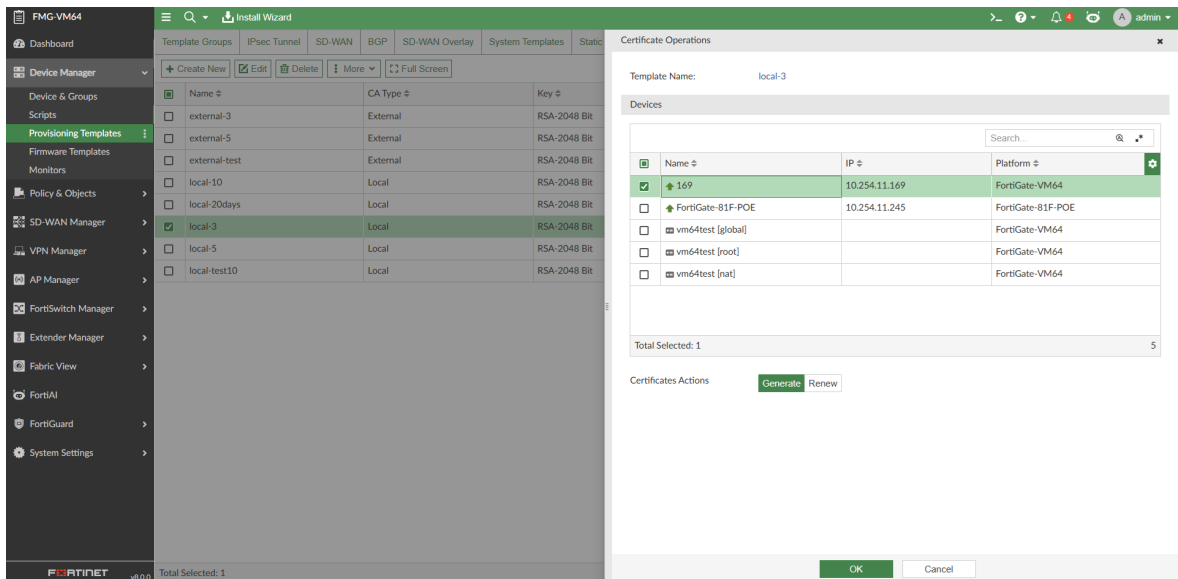
In the *Certificate Operations* page, you can perform the following actions:



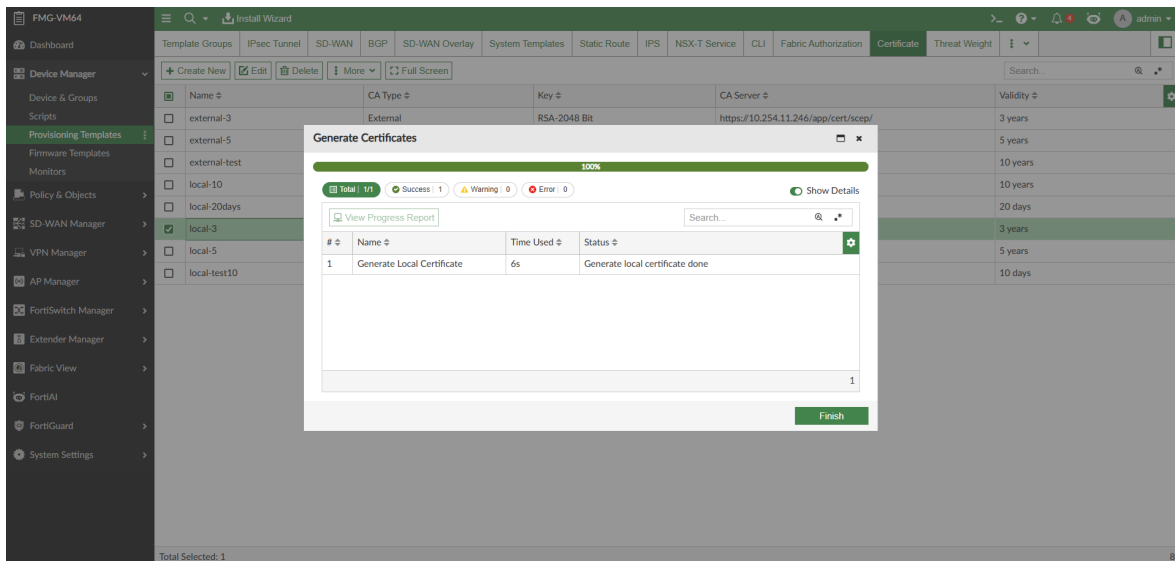
- a. Edit the certificate template:
 - i. Click on the template name to open the template edit page where you can modify the configuration.
 - ii. Click *OK* to save your modifications and return to the *Certificate Operations* dialog.



- b. Generate certificates:
 - i. Select *Generate* as the *Certificate Action*.
The device table shows managed devices.
 - ii. Select one or more devices, and click *OK*.



FortiManager generates the certificate for the selected devices.

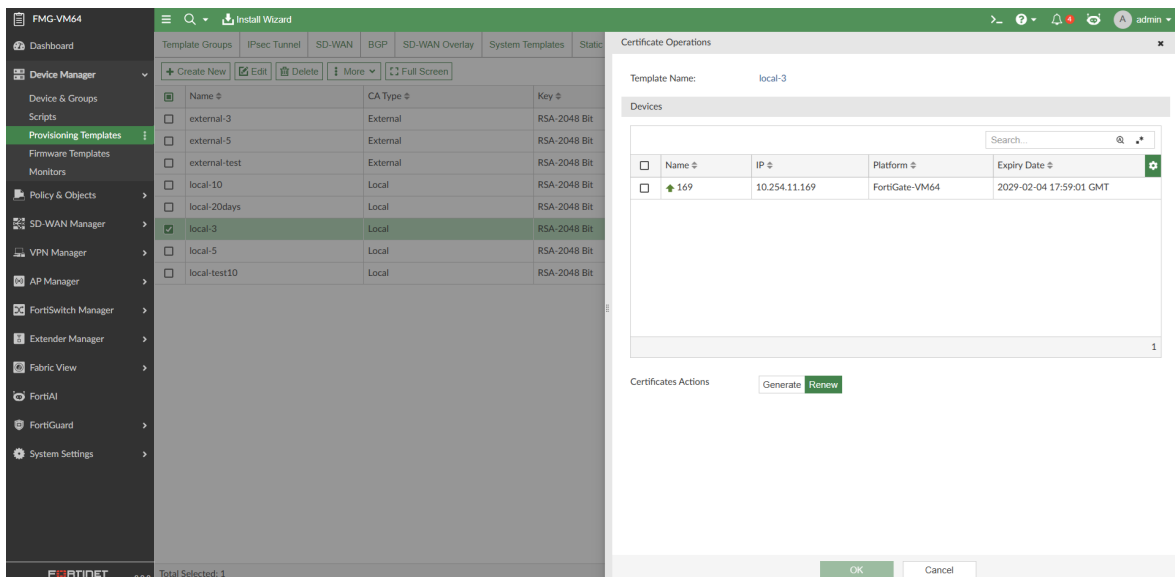


c. Renew certificates:

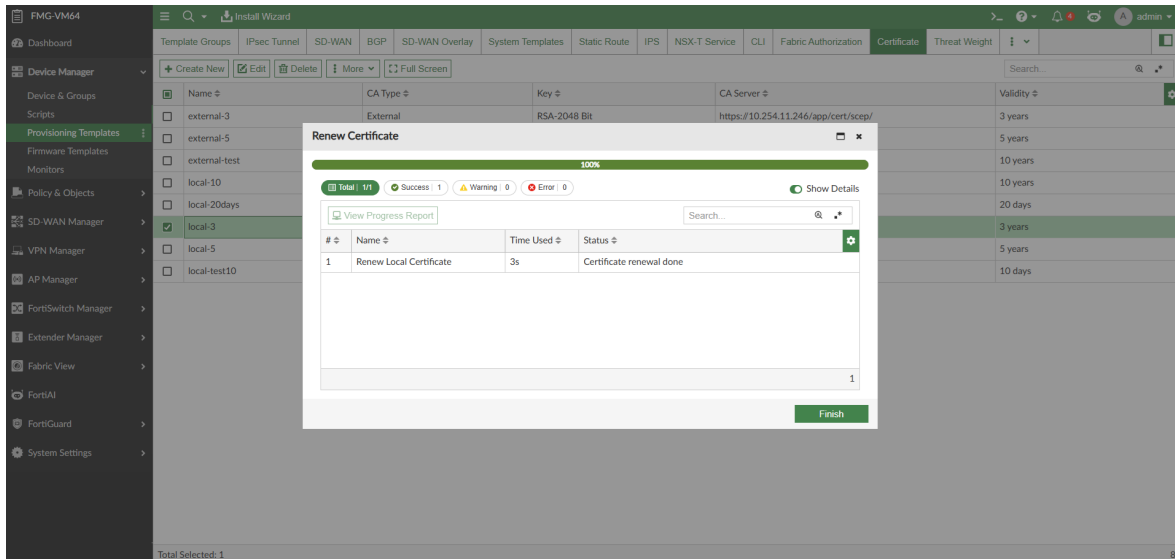
i. Select *Renew* as the *Certificate Action*.

The device table shows only the devices which have a certificate already generated from this template.

ii. Select FortiGate devices to renew the certificate for and click *OK*.



FortiManager renews the certificates for the selected devices.



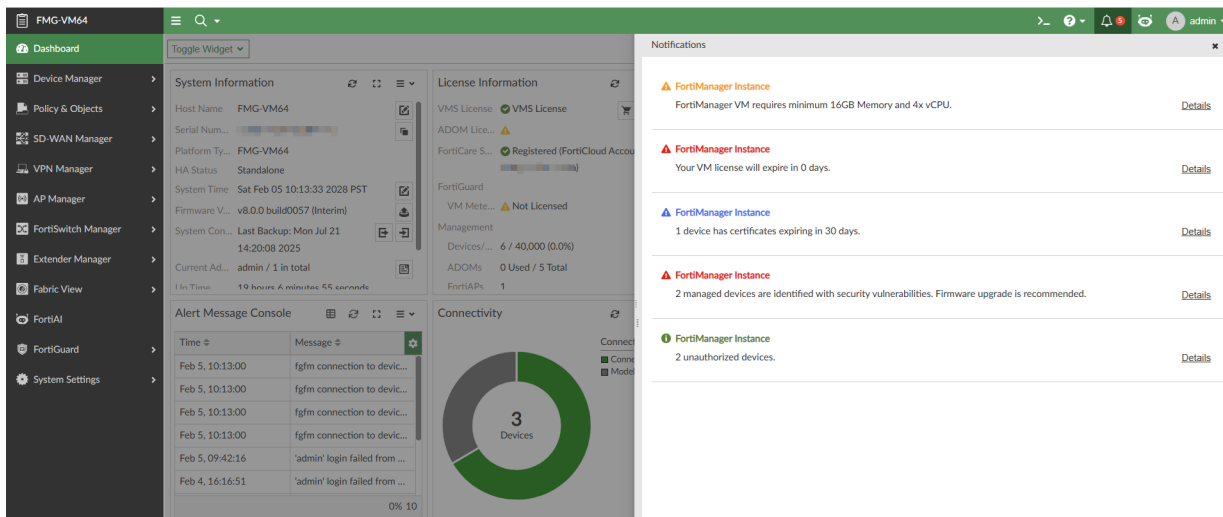
View expiring certificates from the notifications page

A notification will be displayed in the Notifications pane when a managed device's certificate is expiring within 30 days.

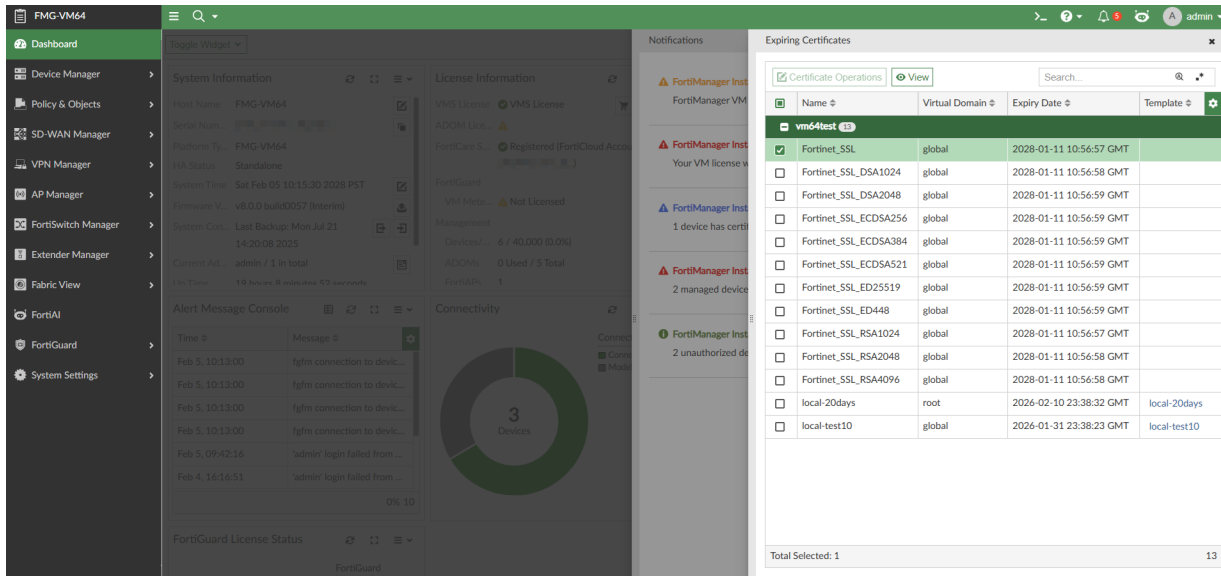
To view expiring certificates:

1. From the top navigation bar, click the bell icon to open the *Notifications* pane.

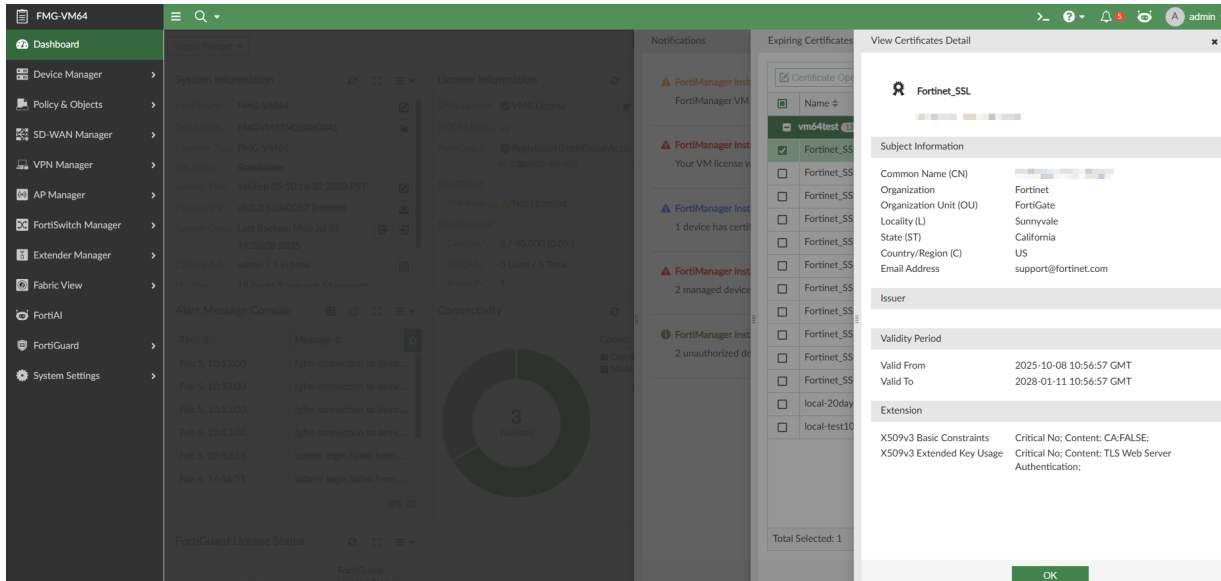
When there are certificates expiring within 30 days, a notification is displayed which indicates the number of affected devices.



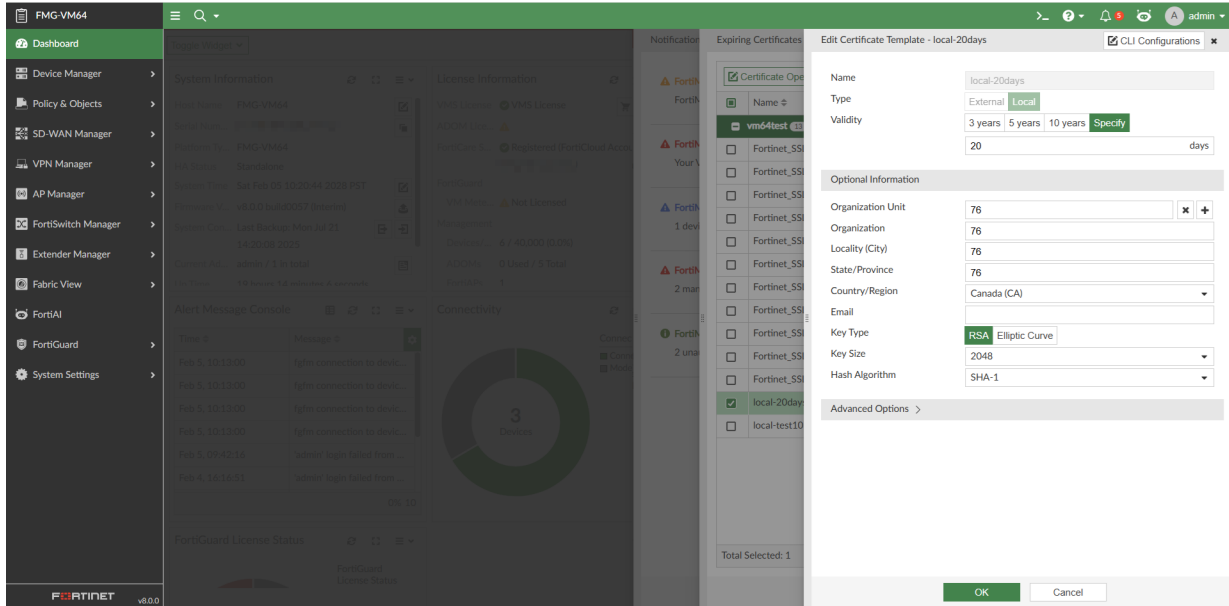
2. Click *Details* to view the certificates that will be expiring. Expiring certificates are displayed in a table, organized by device.



3. Select a certificate and click *View* to see the default certificate.



4. Select a certificate and click *Certificate Operations* to edit the certificate template.



Central Management

This section lists the new features added to FortiManager for central management:

- [FortiSwitch Manager on page 15](#)
- [Others on page 18](#)

FortiSwitch Manager

This section lists the new features added to FortiManager for FortiSwitch manager:

- [FortiSwitch Template adds override option to modify specific port settings on selected devices on page 15](#)

FortiSwitch Template adds override option to modify specific port settings on selected devices



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

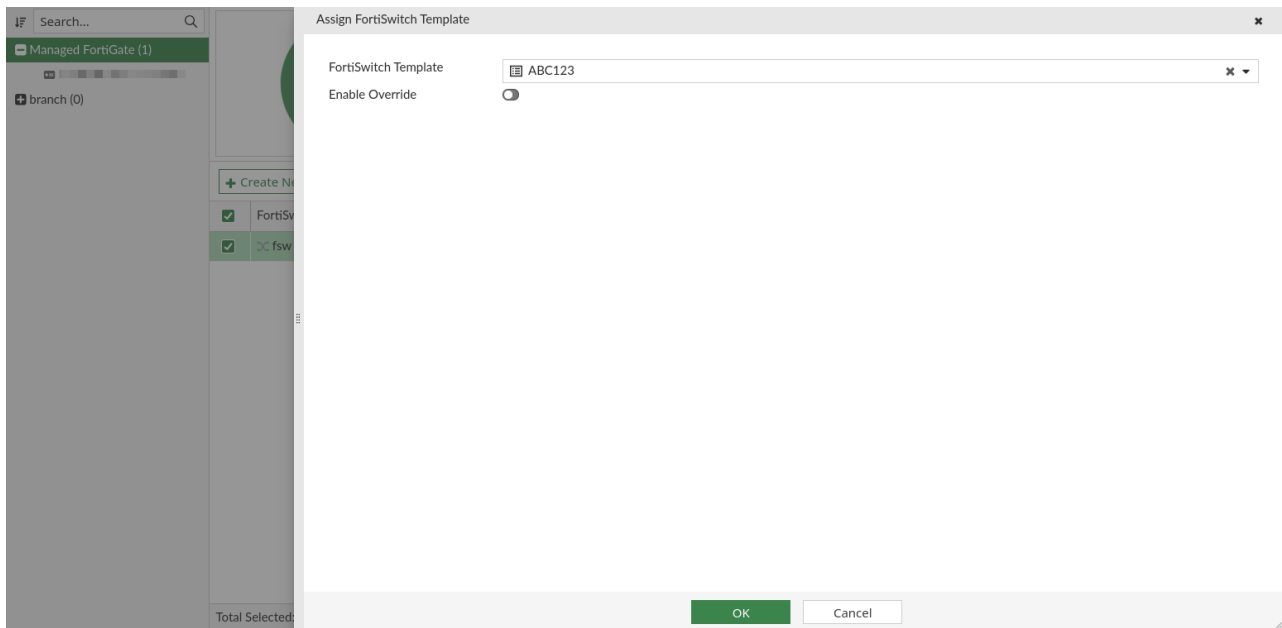
- [Override FortiSwitch template settings](#)

FortiSwitch templates on FortiManager include an override option which allows an administrator to override settings from the template with a custom setting for the device.

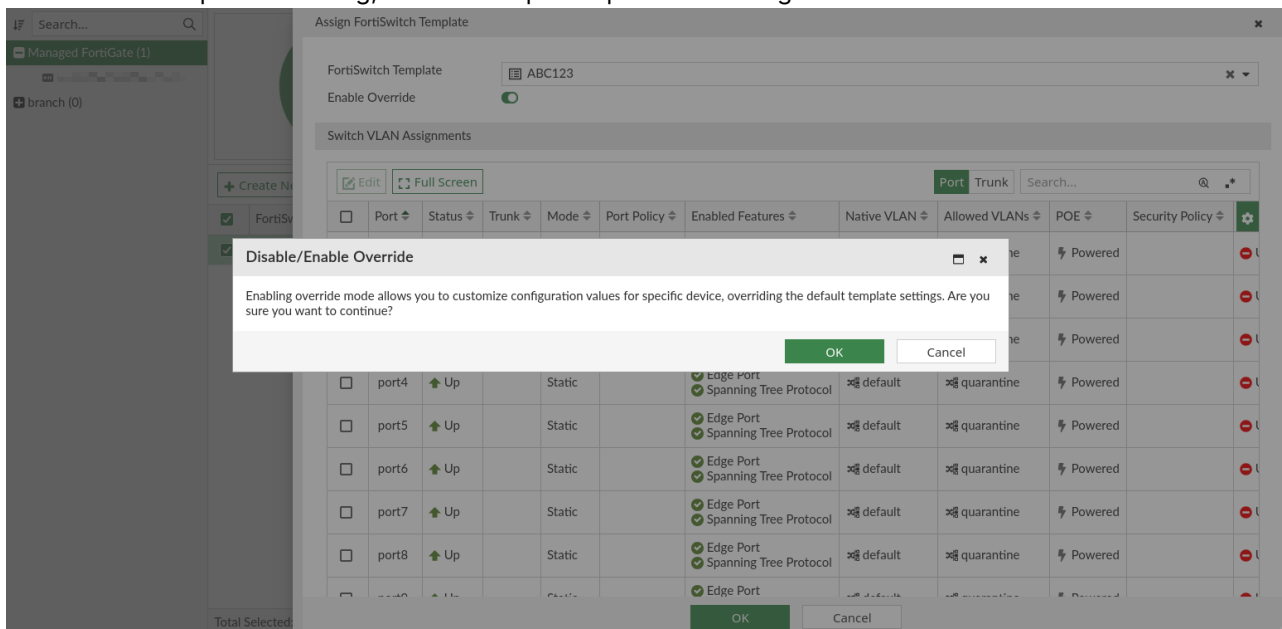
This feature can be used when a template is assigned to multiple FortiSwitch devices, but you need to make changes to the settings configured by the template for specific devices.

To create an override for a FortiSwitch template:


1. Create a FortiSwitch Template.
2. Assign the template to a device.
3. Select the FortiSwitch device in the *Manged FortiSwitches* table, and click *More > Assign Template > Configure Override* in the toolbar.
4. Ensure the correct FortiSwitch template is assigned to the device, and toggle the *Enable Override* toggle to the ON position.

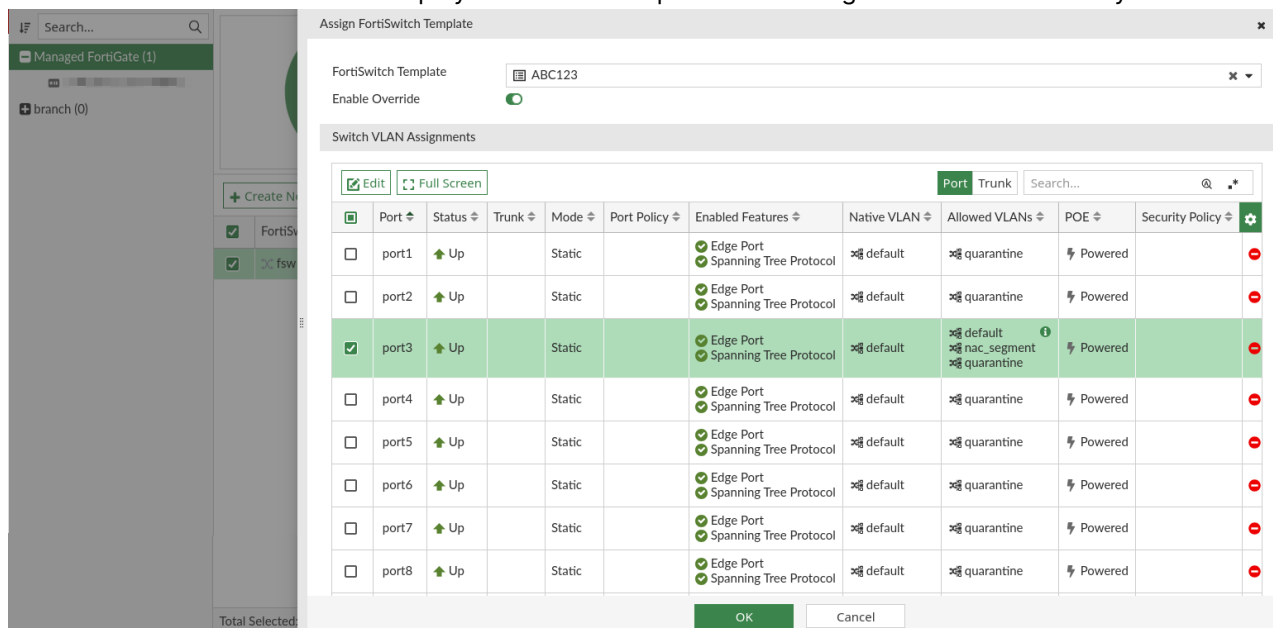


5. Click **OK** to accept the warning, and the template opens for editing.



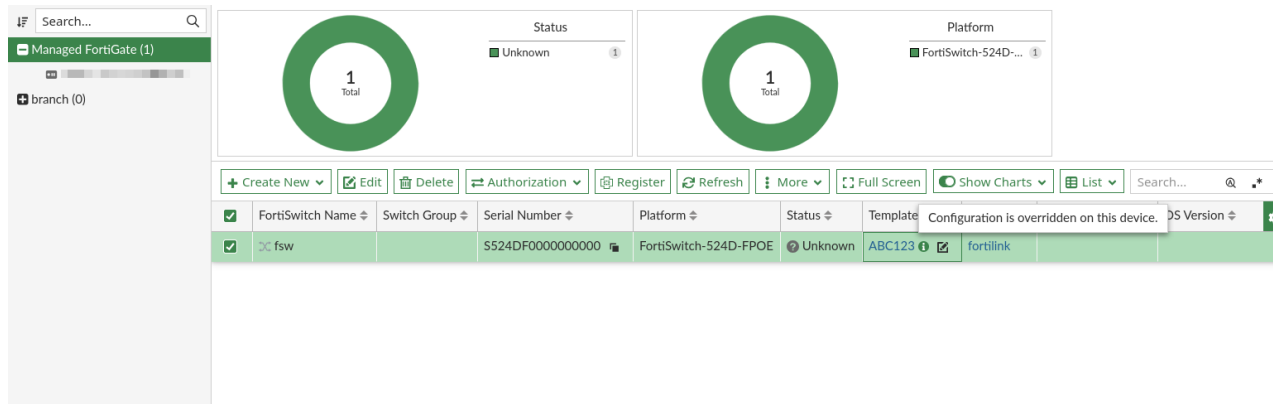
6. Override the template settings by hovering over the cell and clicking the edit icon, or by right-clicking on a port and selecting *Edit*.

Cells that have been edited are displayed with a tooltip icon  making them easier to identify.

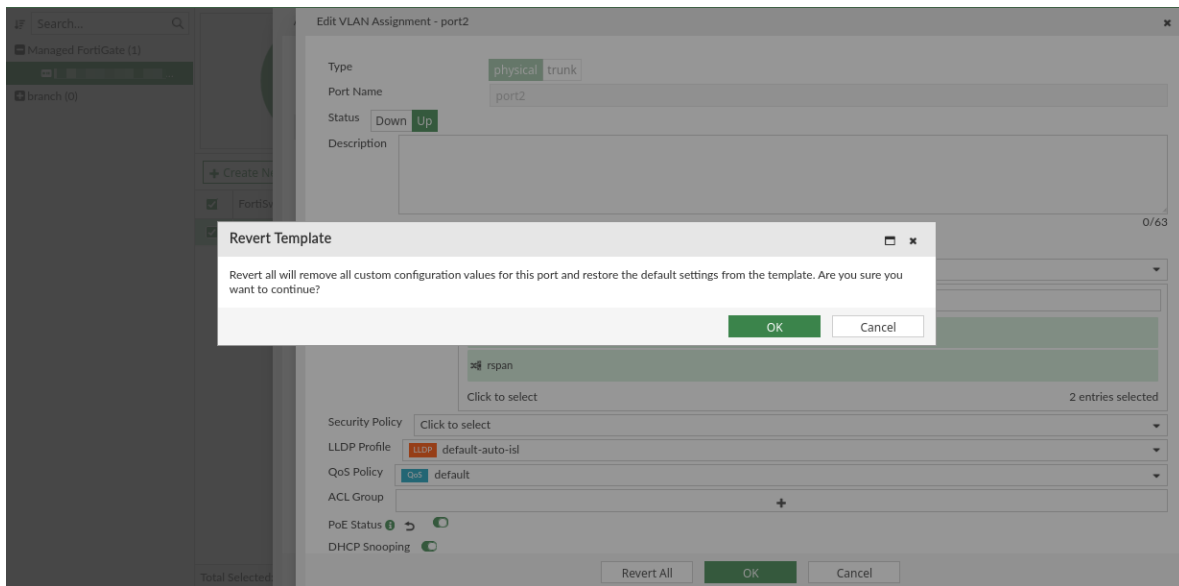


7. Click **OK** to save the device override options for the template.

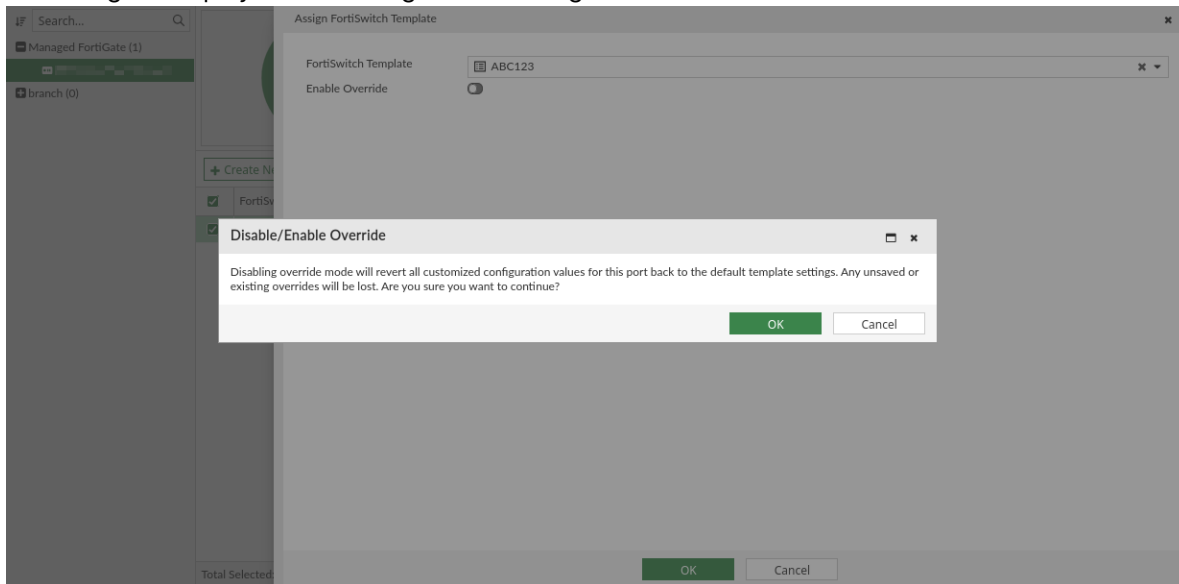
A tooltip icon is displayed in the *Template* column for the selected device in *FortiSwitch Manager* > *Managed FortiSwitches* when an override has been performed for that device.



8. (Optional) To discard all customizations made to a specific port included in the template, click **Revert All** when editing the port in the template.



9. (Optional) To discard all customized configurations made for a device, select the FortiSwitch device and click *More > Assign Template > Configure Override*, and then move the *Enable Override* toggle to the OFF position. A message is displayed confirming that disabling override mode will revert all customized values.



Others

This section lists the new features added to FortiManager for other topics relating to central management:

- [Workspace Mode supports onboarding new devices and creating new policy packages without ADOM lock on page 19](#)
- [Interface-based bandwidth graph uses average bandwidth logic on page 22](#)

- FortiSwitch, FortiAP and FortiExtender templates can be assigned from Fabric Authorization Template on page 23
- Certificate templates can be selected in model device, model HA device, and device blueprint configurations on page 25
- New workflow mode design to control individual admin sessions with selective approvals on page 30
- Factory default IPsec template to configure FortiClient VPN on page 33
- Central monitoring dashboard for Firewall Users with filters for authentication method and user group on page 35
- Maximum length of meta variables value increased to 32768 characters on page 39
- Admin profile adds granular control on device manager (Interface, Log & Report, Security Fabric) and Routing on page 41
- pxGrid connector is enhanced to display Device Type and Session State on page 44
- Managing FortiGate registration to FortiCare on page 47
- Enhanced asset details and identity monitoring on page 49
- Administrators can create protected objects on page 61
- FortiManager supports downgrade and roll-back for FortiGuard packages to allow setting a preferred package version for devices on page 66
- FortiManager supports importing password-type objects from FortiGate devices with private data encryption on page 69

Workspace Mode supports onboarding new devices and creating new policy packages without ADOM lock



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

- [Adding new devices and policy packages without locking the ADOM](#)

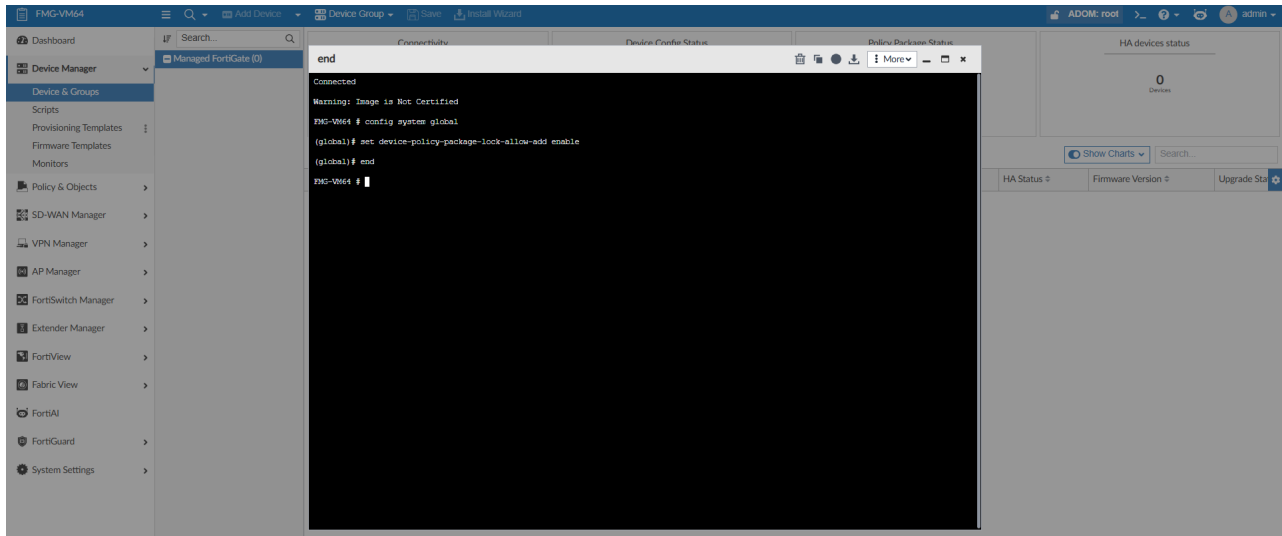
In FortiManager 8.0.0, the following global command has been added to the CLI to allow administrators to add devices and policy packages without needing to lock the ADOM while in Workspace mode. By default, this command is set to disabled.

```
set device-policy-package-lock-allow-add {enable | disable}
```

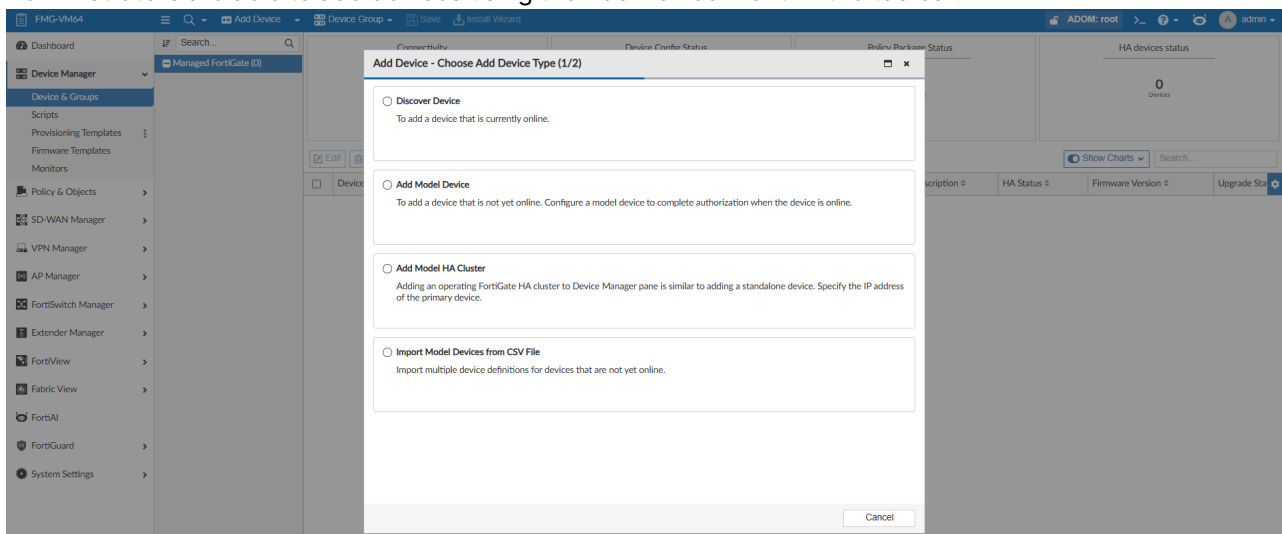
To allow administrators to add devices and policy packages without locking the ADOM:

1. In the FortiManager CLI, enter the following commands:

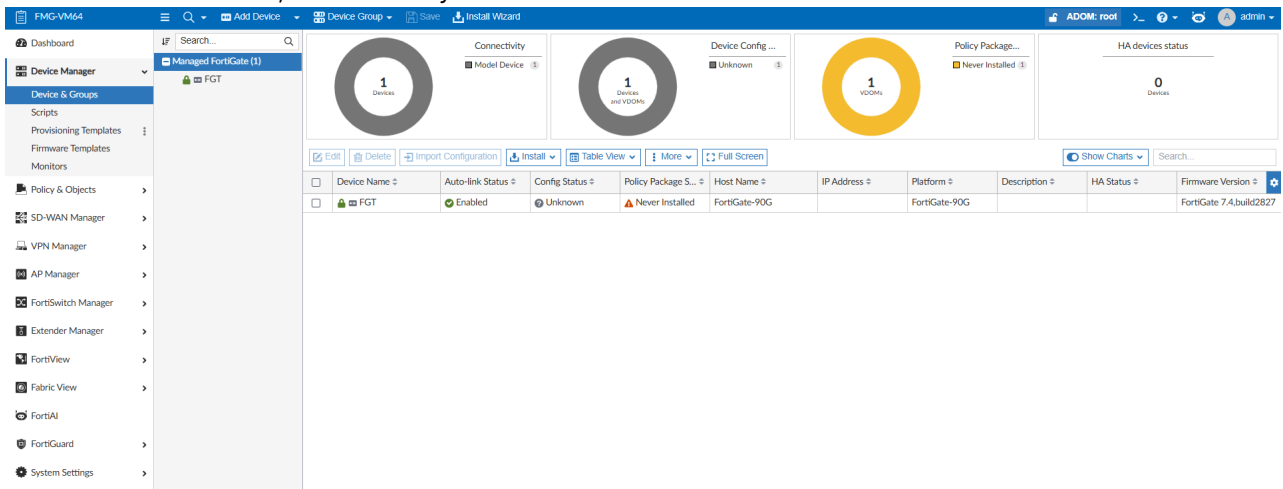
```
config system global
    set device-policy-package-lock-allow-add enable
end
```



2. Enter an unlocked ADOM with Workspace mode enabled.
3. Go to *Device Manager > Devices & Groups*. Administrators are able to add devices using the *Add Device* menu in the toolbar.

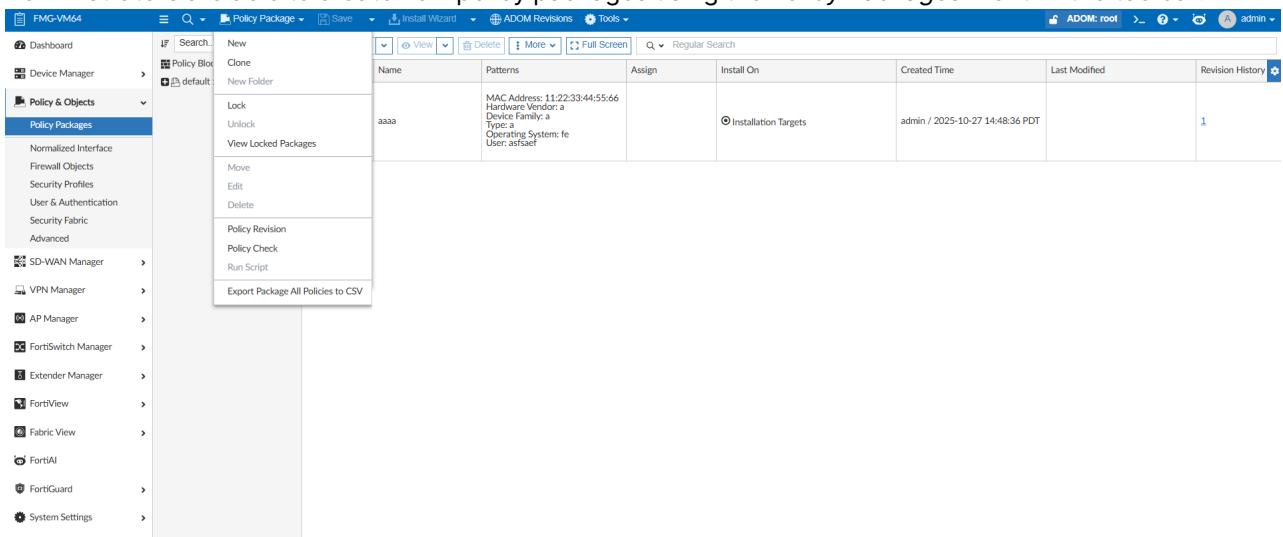


After a device is added, it is locked by default.

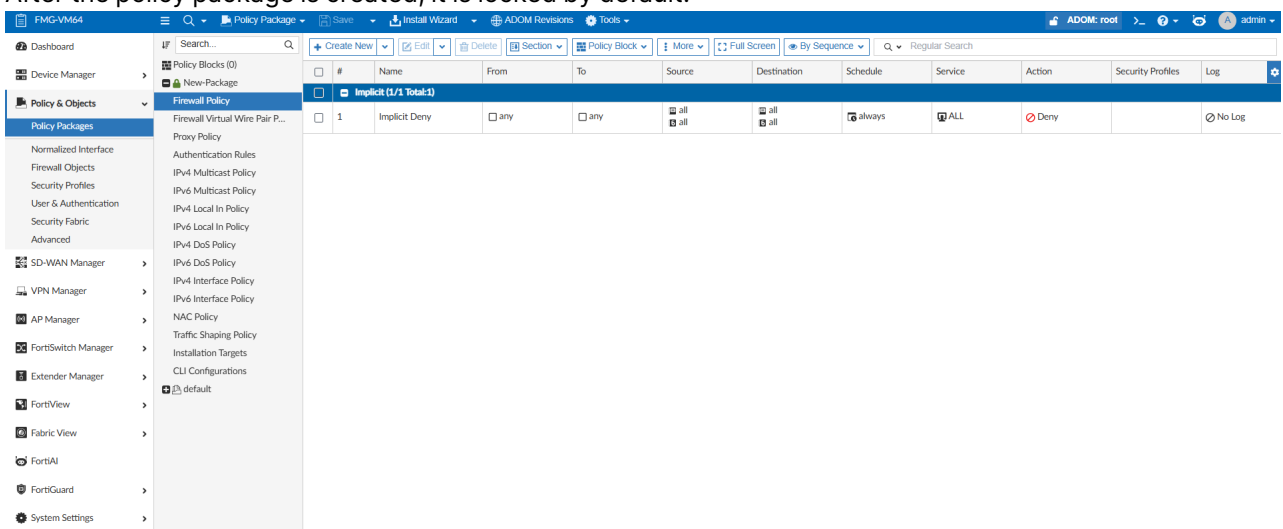


4. Go to *Policy & Objects > Policy Packages*.

Administrators are able to create new policy packages using the *Policy Packages* menu in the toolbar.



After the policy package is created, it is locked by default.



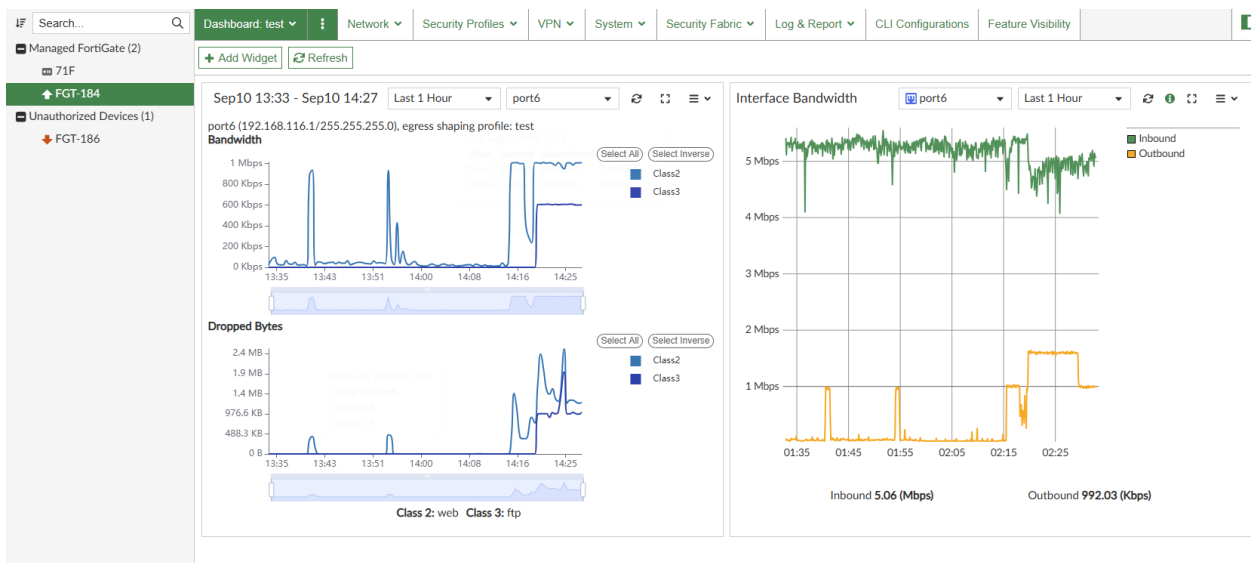
Interface-based bandwidth graph uses average bandwidth logic

The bandwidth graph of the *Traffic Shaping (interface-based)* widget has been enhanced to plot the average bandwidth values instead of the current bandwidth.

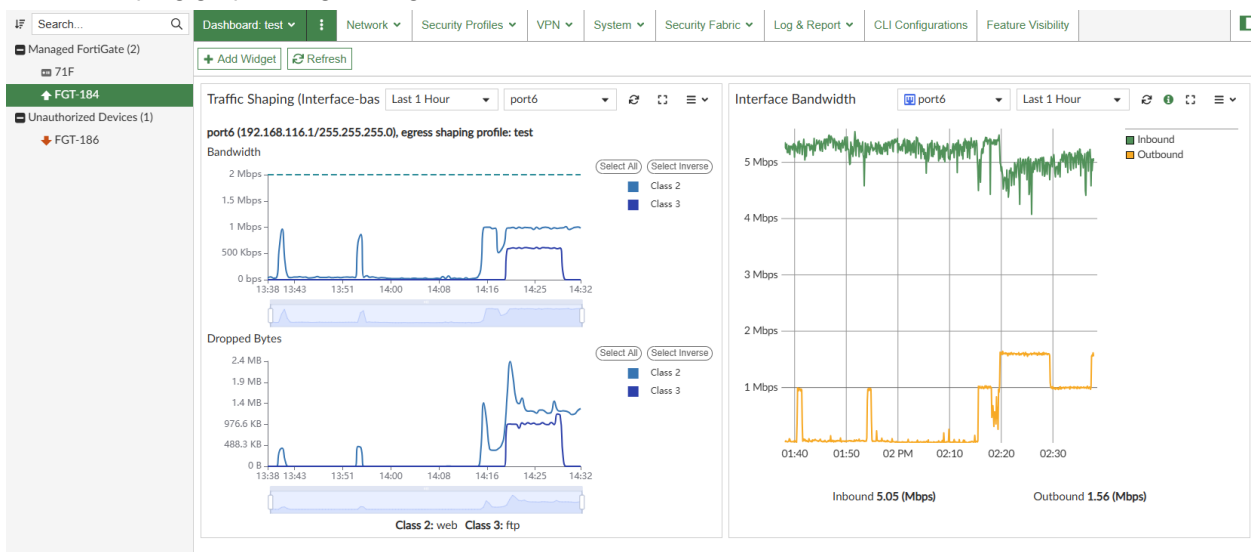
This method uses the same averaging method as the *Interface Bandwidth* widget, and aligns it with the visualization method used in the *Interface Bandwidth* widget.

Example

- Traffic Shaping graph using current bandwidth (legacy)



- Traffic Shaping graph using averaged bandwidth (new)



FortiSwitch, FortiAP and FortiExtender templates can be assigned from Fabric Authorization Template



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

- Fabric authorization templates

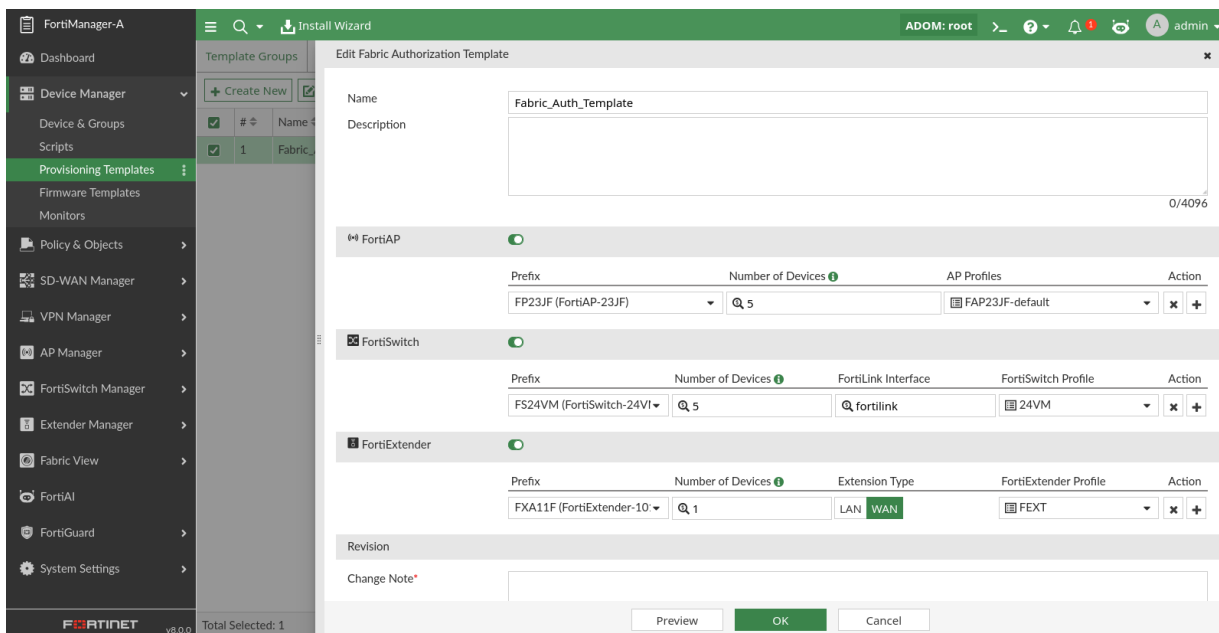
FortiSwitch, FortiAP, and FortiExtender templates can be assigned from within a Fabric Authorization Template. Device Blueprint adds configuration for a Firmware Template and Fabric Authorization Template.

To assign profiles to model devices using Fabric Authorization Templates:

1. Create a Fabric Authorization Template.
 - a. Go to *Device Manager > Provisioning Templates > Fabric Authorization*, and click *Create New* to create a new Fabric Authorization Template.
 - b. Expand the *FortiAP*, *FortiSwitch*, or *FortiExtender* drawers, and select the *Prefix* and number of devices that can be authorized.
 - c. Click the *AP Profiles*, *FortiSwitch Profile*, or *Extender Profile* dropdown menus to select a configured profile. Only profiles that match the selected prefix are displayed as option. Alternatively, you can click the add button to create a new profile.



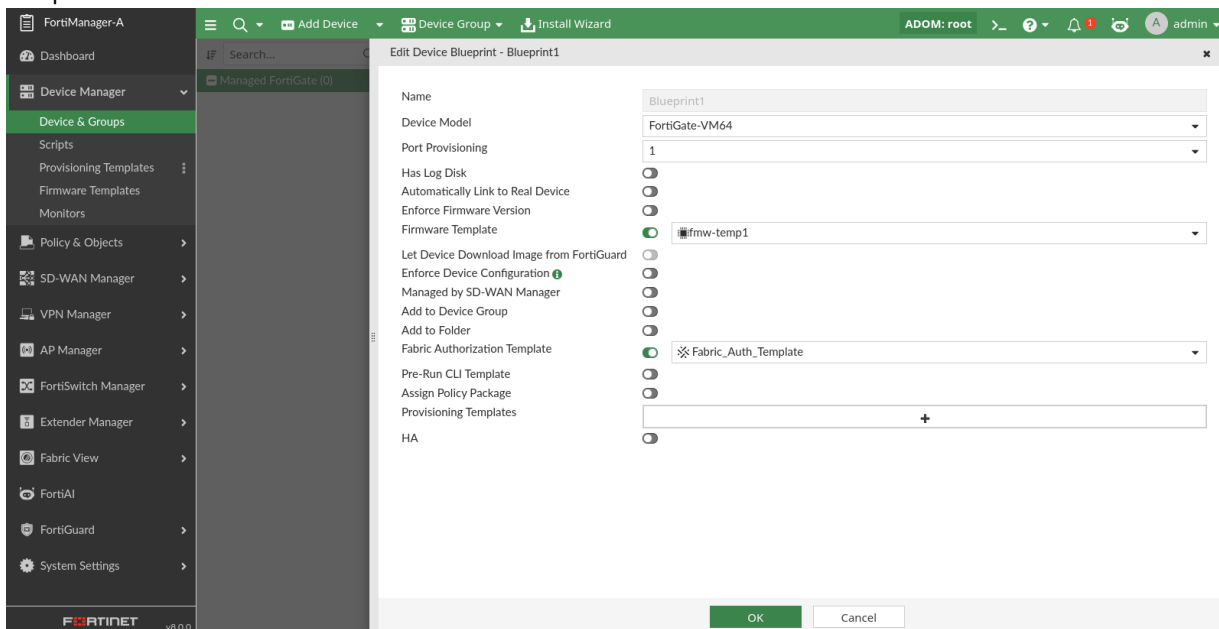
Adding FortiSwitch/FortiAP profiles in an Fabric Authorization Template is only supported when Central Management for FortiSwitch/FortiAP is enabled in the ADOM settings. When the ADOM is operating in Per Device Mode, the FortiSwitch Profile/FortiAP Profile options are not displayed in Fabric Authorization template.



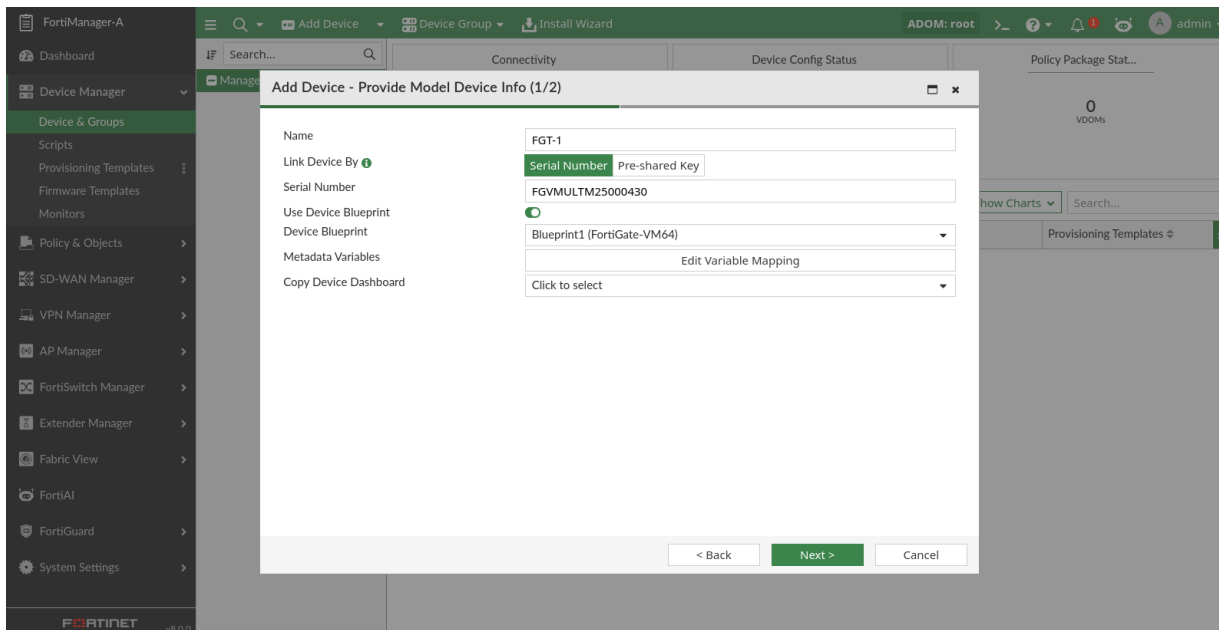
- d. Click *OK* to save the template.

2. Add the Fabric Authorization Template to a Device Blueprint.

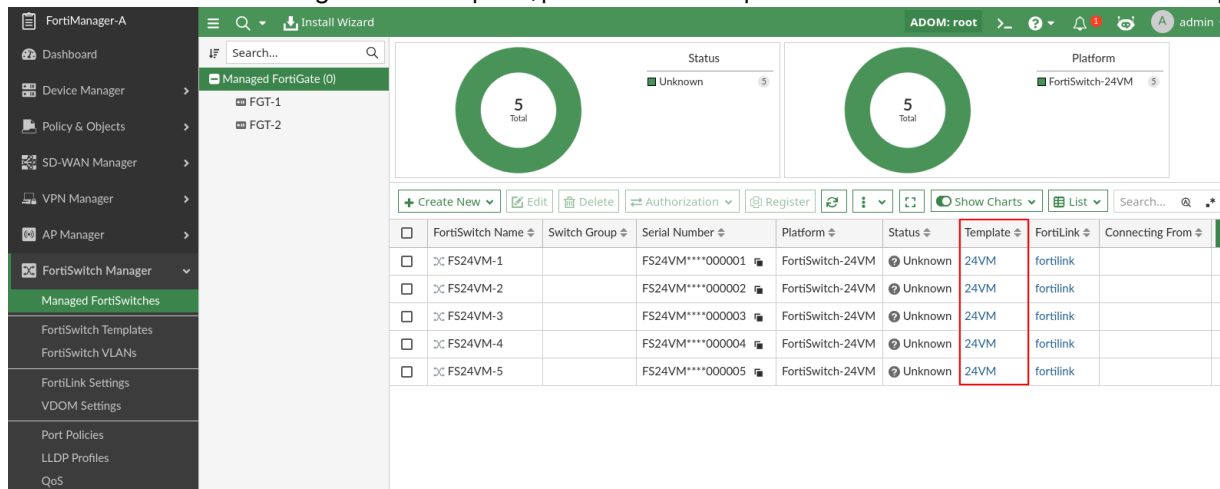
- a. Go to *Device Manager > Devices & Groups* and click the *Add Device* dropdown and select *Device Blueprint*.
- b. Create a new blueprint, enable *Fabric Authorization Template*, and select the previously configured template.



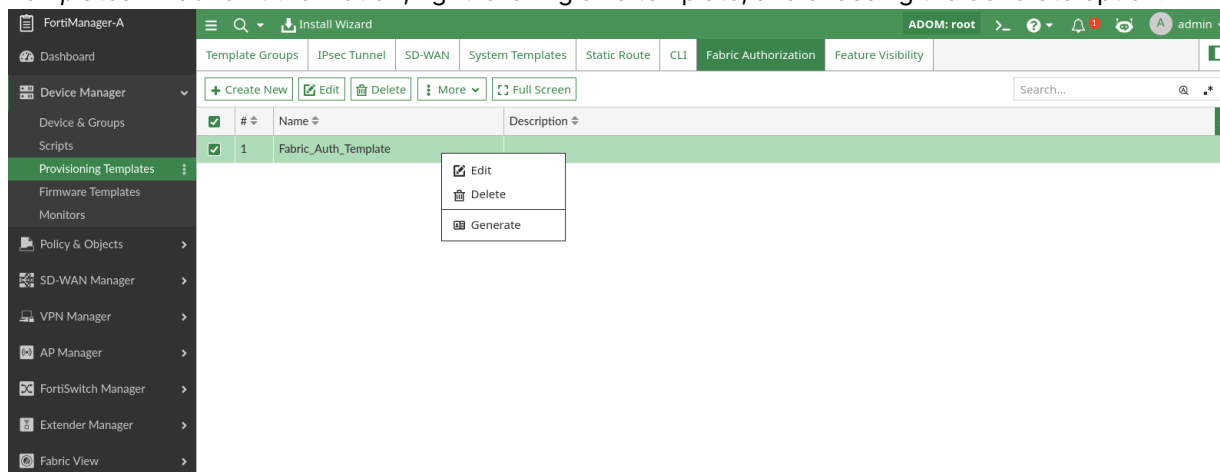
- c. Click *OK* to save the blueprint.
3. Create a FortiGate model device using the device blueprint.
 - a. Go to *Device Manager > Device & Groups*.
 - b. Click *Add Device*, and choose a method for adding model devices. For example *Add Model Device*.
 - c. Toggle *Use Device Blueprint* on and select the previously configured blueprint.
 - d. Configure the remaining settings as needed and complete *the Add Device wizard* to add the model device.



4. Go to the *FortiSwitch Manager, AP Manager, and/or Extender Manager* to see that the model devices have been created and are assigned the template/profile that was specified in the Fabric Authorization Template.



You can also apply the Fabric Authorization Template to existing model devices by going to *Provisioning Templates > Fabric Authorization*, right-clicking on a template, and choosing the *Generate* option.



Certificate templates can be selected in model device, model HA device, and device blueprint configurations



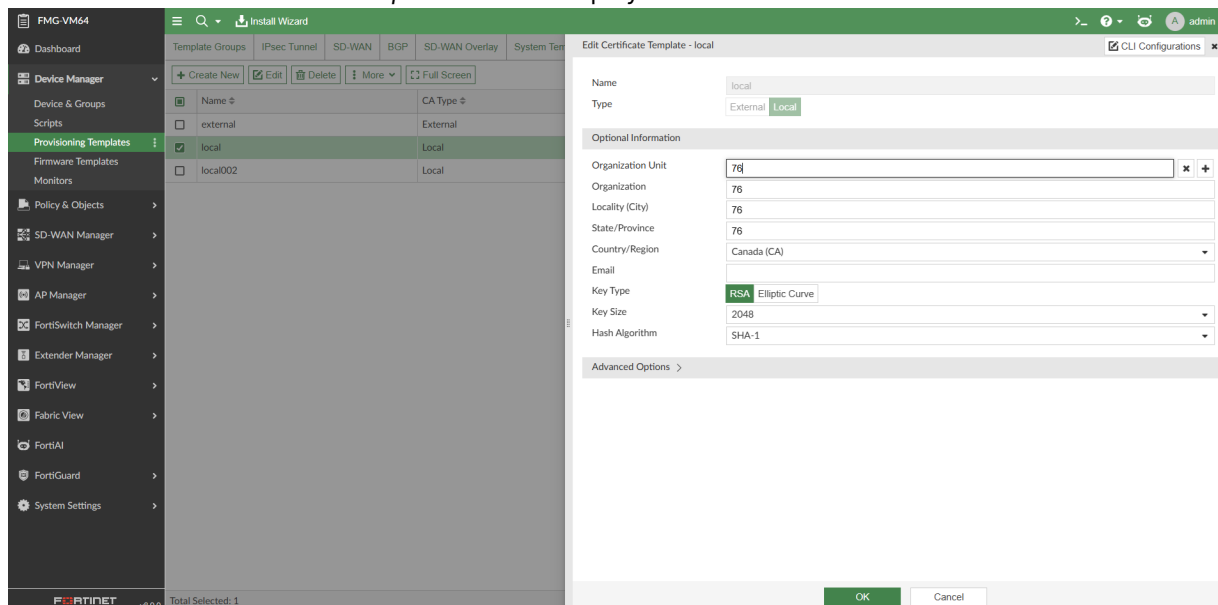
This information is also available in the FortiManager 8.0 Administration Guide:

- Adding offline model devices
- Using device blueprints for model devices
- Adding a FortiGate HA cluster

Certificate templates are available as provisioning templates and can now be selected when adding a model device/model HA cluster and when configuring device blueprint.

To create a certificate template:

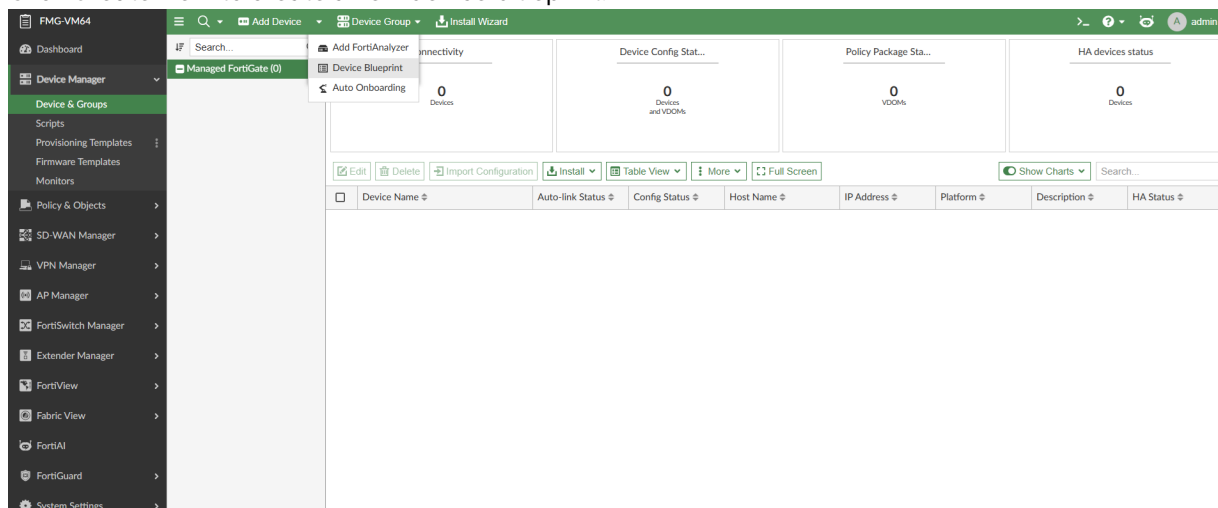
1. Go to *Device Manager > Provisioning Templates > Feature Visibility*, and enable *Certificate*.
2. Go to *Device Manager > Provisioning Templates > Certificate*, and click *Create New*.
The *Create New Certificate Template* menu is displayed.



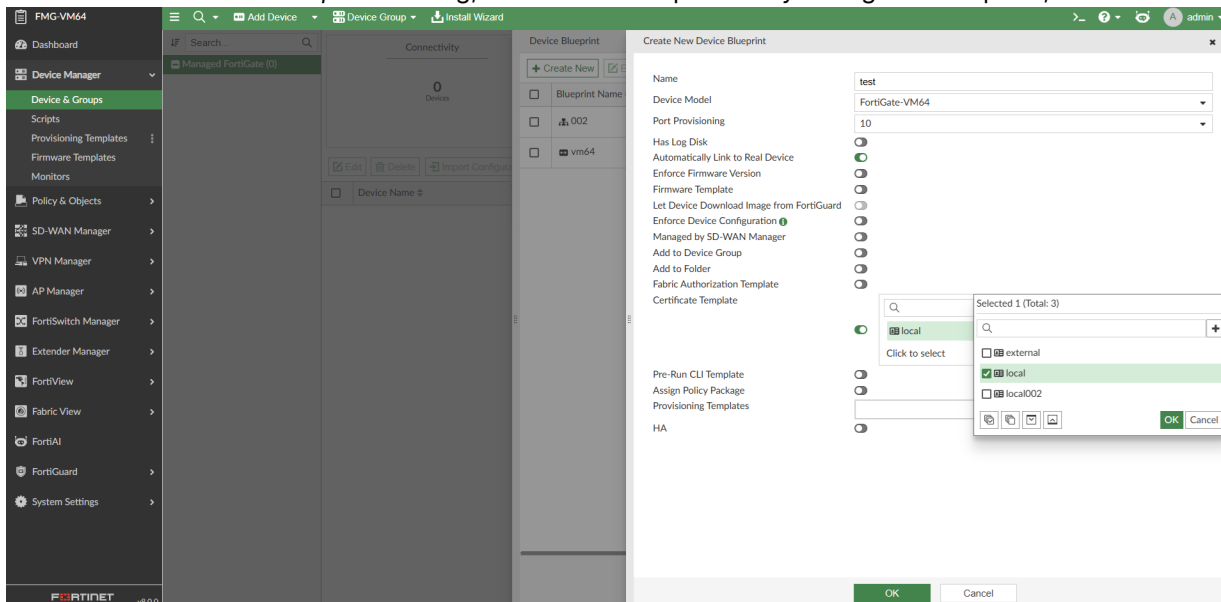
3. Configure the certificate details, and click *OK* to save the template.

To assign the certificate template to a Device Blueprint.

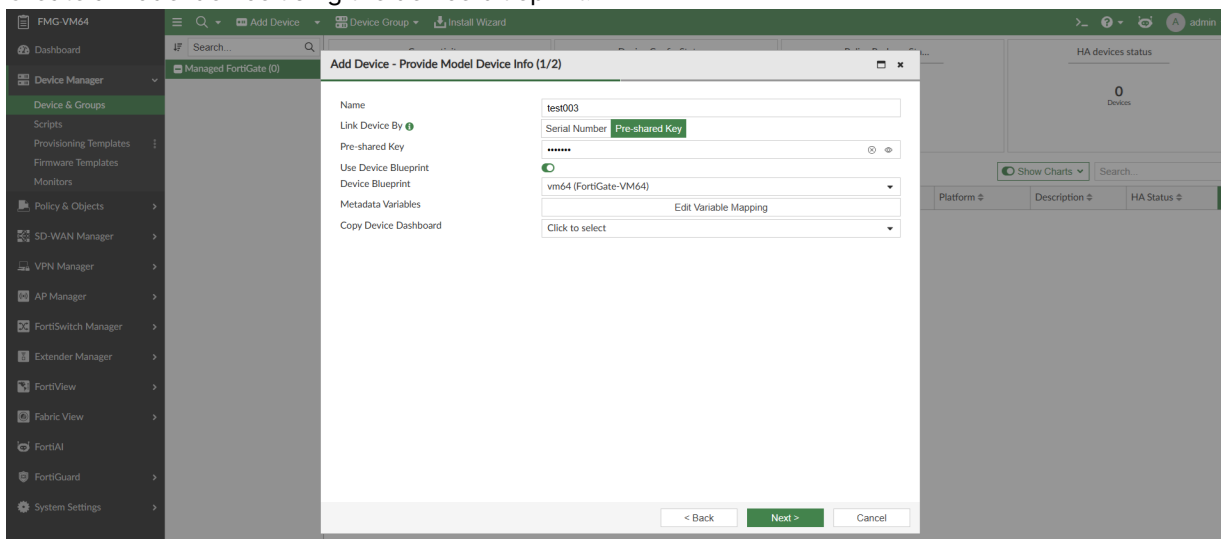
1. Go to *Device Manager > Device & Groups*, click the dropdown menu next to *Add Device* and select *Device Blueprint*.
2. Click *Create New* to create a new device blueprint.



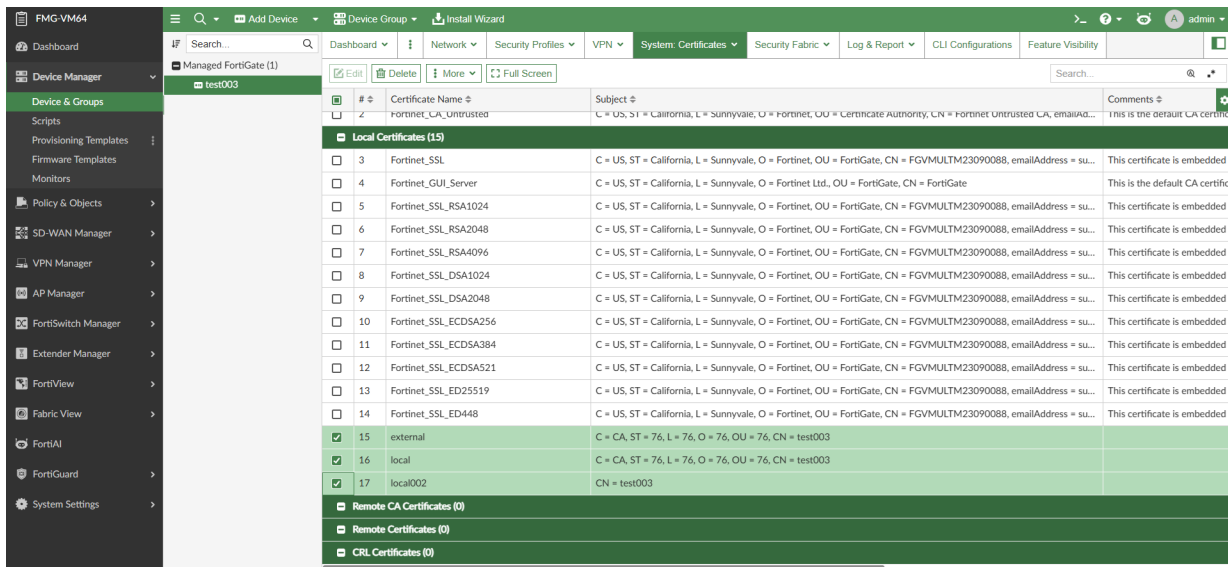
3. Enable the *Certificate Template* setting, and choose the previously configured template, and then click OK.



4. Create a model device using the device blueprint.

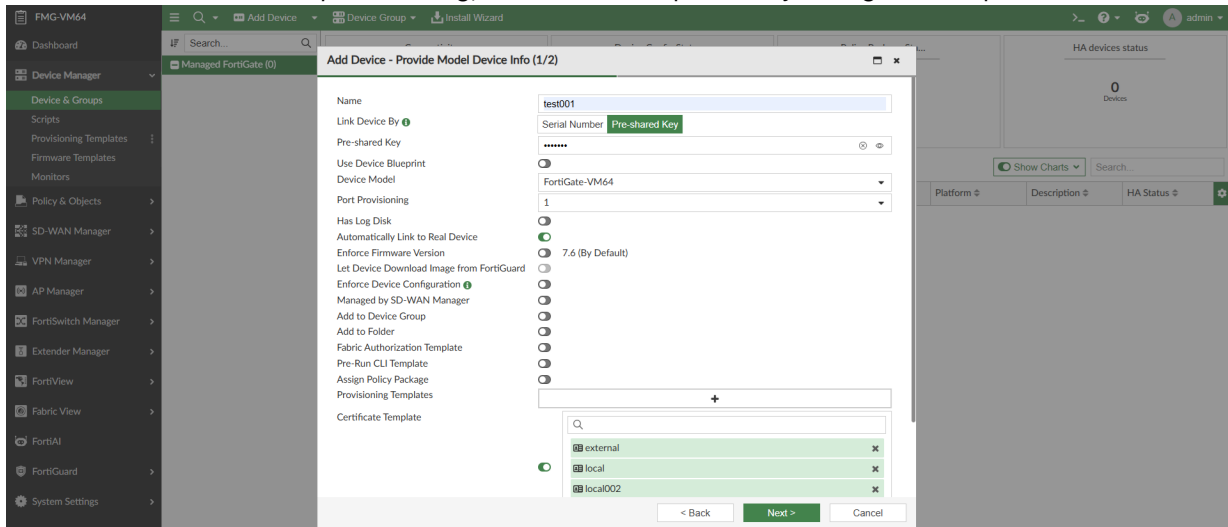


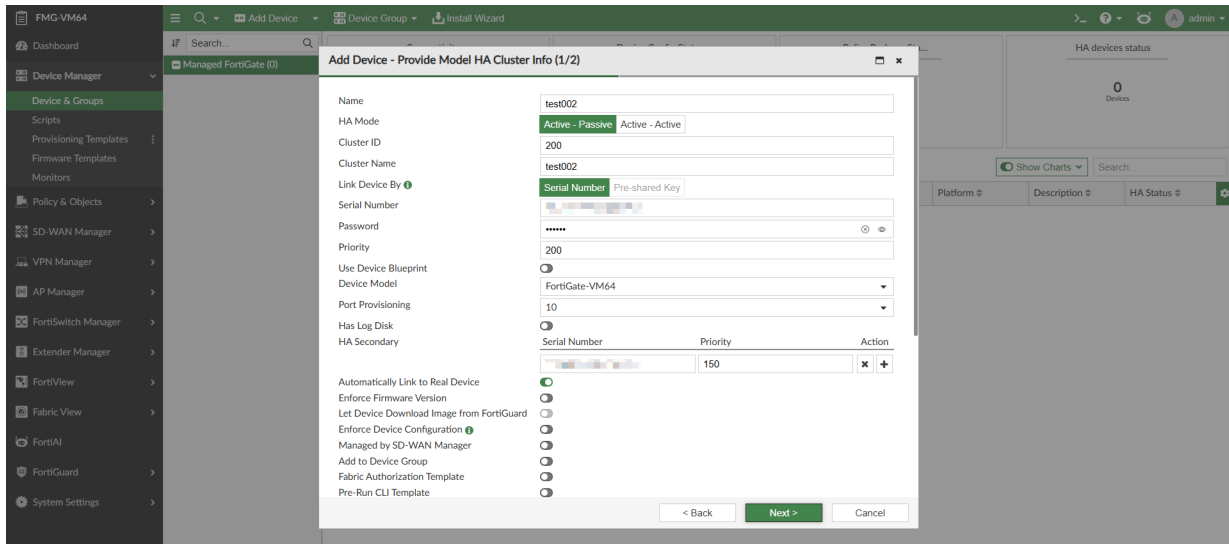
After the model device or model HA cluster is added, you can see the certificates automatically generated on the `system:certificates` page.



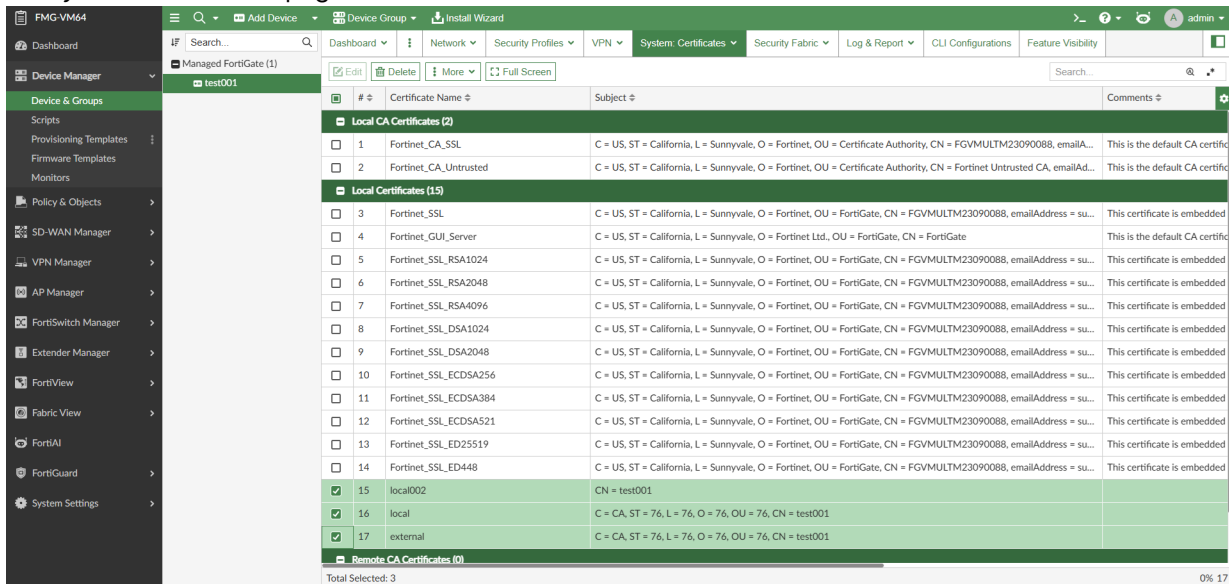
To assign the certificate template to a model device/model HA cluster device:

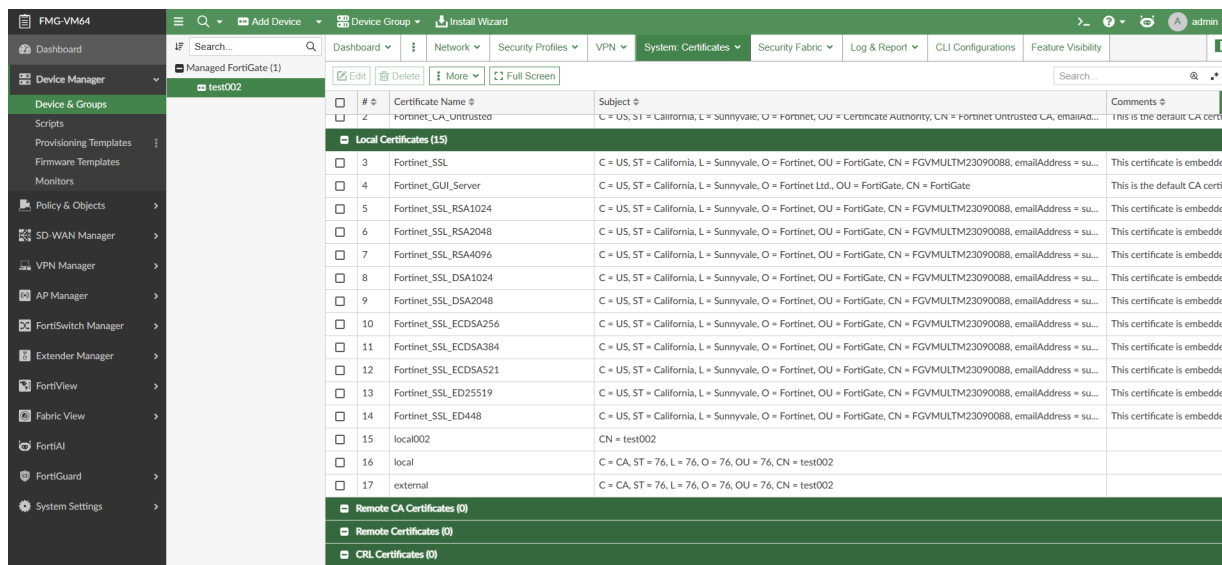
1. Go to *Device Manager > Device & Groups*, and add a model device or model HA cluster device.
2. Enable the *Certificate Template* setting, and choose the previously configured template





3. After the model device/model device is added, you can see the certificates automatically generated on the `system:certificates` page.





New workflow mode design to control individual admin sessions with selective approvals



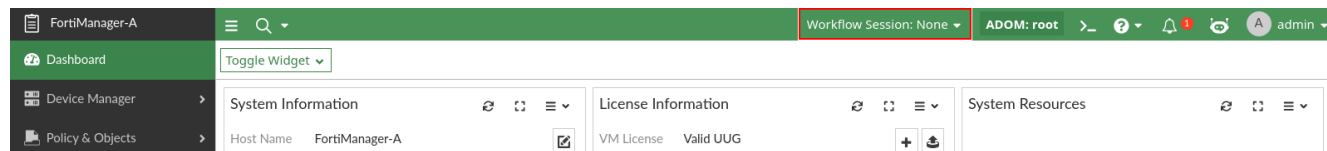
This information is also available in the FortiManager 8.0 Administration Guide:

- Workflow mode
- Workflow sessions

Beginning in FortiManager 8.0.0, workflow mode has been redesigned to support control over individual admin sessions with selective approvals. With this updated design, locking an ADOM is no longer required, allowing multiple users to create sessions simultaneously. Additionally, sessions can be approved in any order and are not restricted to being approved in the order they are submitted.

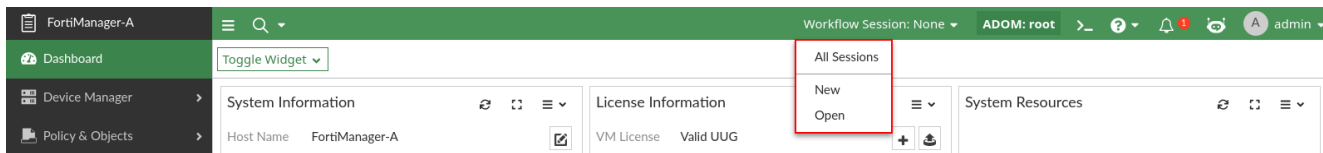
Creating and approving sessions

When an administrator first enters an ADOM in workflow mode, the *Workflow Session* displayed in the toolbar will be set to *None*.



In the toolbar, click the *Workflow Session* dropdown to see the following options:

All Sessions	View all sessions in the session list.
New	Create a new session.
Open	Open an in-progress session which has not yet been submitted.



Example

In this example, there are two administrators named *admin1* and *admin2*. Both administrators create policies in the same ADOM using two separate sessions, Session1 and Session2. When both sessions have been submitted, administrators that are part of the approval group can selectively approve sessions in any order.

To create and approve sessions:

1. *admin1* opens a new session called Session1 and creates a new policy called policy1, then submits the session for approval.
2. *admin2* opens a new session called Session2 and creates a new policy called policy2, then submits the session for approval.
3. Admins can view the *All Sessions* menu to see both sessions with the status *Waiting Approval*.

ID	Session Name	Current Status	Created By	Date Submitted	Approval Status	Comments
2	Session2	Waiting Approval	admin2 (Current)	2025-11-20 14:16:09 PST	0/0	
1	Session1	Waiting Approval	admin1	2025-11-20 14:14:49 PST	0/0	

4. Admins who are a part of the ADOMs *Approval Group* can selectively approve sessions in any order. For example, even though Session2 was submitted after Session1, it can be approved first.

ID	Session Name	Current Status	Created By	Date Submitted	Approval Status	Comments
2	Session2	Waiting Approval	admin2 (Current)	2025-11-20 14:16:09 PST	0/1	
1	Session1	Waiting Approval	admin1	2025-11-20 14:14:49 PST	0/1	

When Session2 is approved, policy2 is added to the ADOM.

#	Name	From	To	Source	Destination	Schedule	Se
1	policy2	any	any	all	all	always	ALL
Implicit (2/2 Total:1)							
2	Implicit Deny	any	any	all	all	always	ALL

When Session1 is approved, policy1 is added to the ADOM alongside policy2.

Search...									
+ Create New View Delete Section More Full Screen By Sequence Regular Search									
<input type="checkbox"/>	#	Name	From	To	Source	Destination	Schedule	Se	Settings
<input type="checkbox"/>	1	policy2	<input type="checkbox"/> any	<input type="checkbox"/> any	<input type="checkbox"/> all	<input type="checkbox"/> all	<input type="checkbox"/> always	<input type="checkbox"/> ALL	<input type="checkbox"/> ALL
<input type="checkbox"/>	2	policy1	<input type="checkbox"/> any	<input type="checkbox"/> any	<input type="checkbox"/> all	<input type="checkbox"/> all	<input type="checkbox"/> always	<input type="checkbox"/> ALL	<input type="checkbox"/> ALL
<input type="checkbox"/> Implicit (3/3 Total:1)									
<input type="checkbox"/>	3	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input type="checkbox"/> all	<input type="checkbox"/> all	<input type="checkbox"/> always	<input type="checkbox"/> ALL	<input type="checkbox"/> ALL

Session conflicts

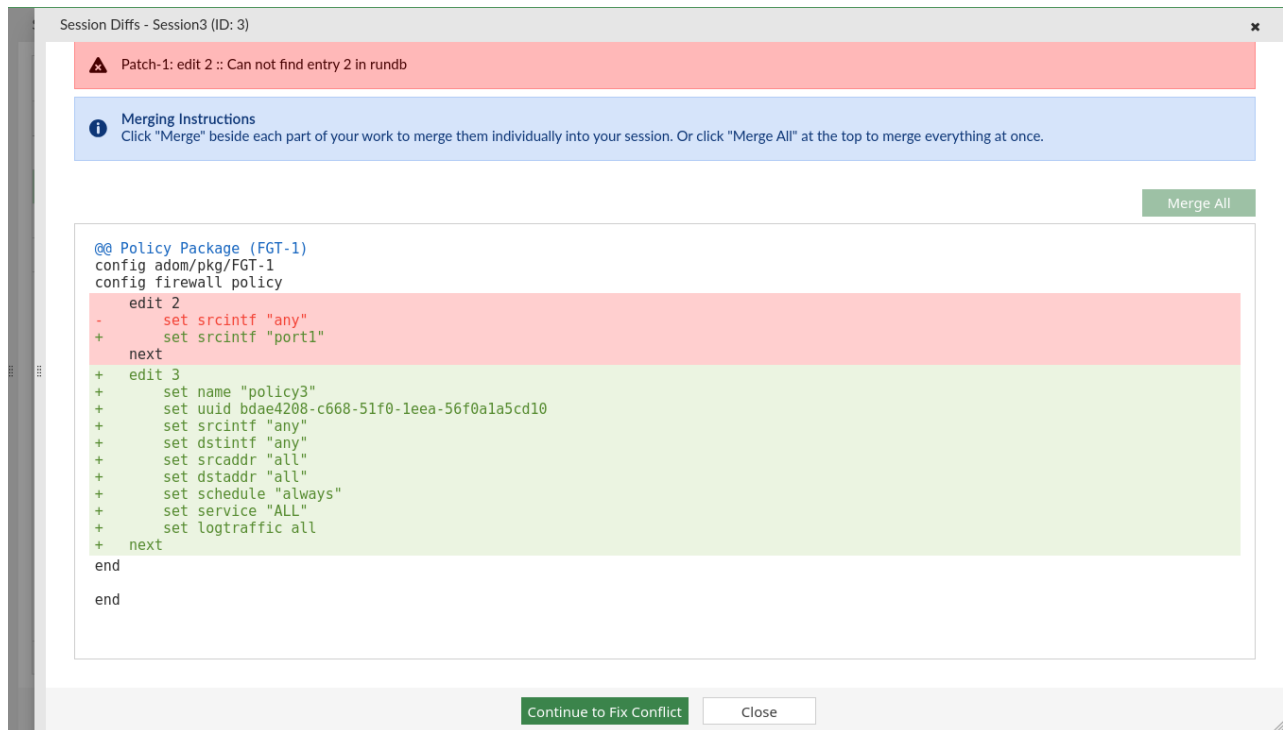
Because the new workflow design allows administrators to approve sessions in any order, there is a chance for changes to affect each other and cause a conflict. When this occurs, the administrator will see an error indicating a conflict when attempting to approve the session. The administrator can review the changes and has the option to merge changes and attempt to fix the conflict.

Example

1. *admin1* creates a new session named *Session3*, and makes the following changes:
 - a. Edits *policy1* and changes the *Incoming Interface* from *any* to *port1*.
 - b. Creates a new policy called *policy3*.
2. *admin2* creates *Session4* and deletes *policy1*.
3. Both users save and submit their sessions.

Session List						
+ Create New Open View Diff Approve Reject Repair Discard More Search...						
ID	Session Name	Current Status	Created By	Date Submitted	Approval Status	Comments
4	Session4	Waiting Approval	A admin2 (Current)	2025-11-20 15:30:59 PST	0/1	
3	Session3	Waiting Approval	A admin1	2025-11-20 15:29:39 PST	0/1	
2	Session2	Approved	A admin2 (Current)	2025-11-20 14:16:09 PST	1/1	
1	Session1	Approved	A admin1	2025-11-20 14:14:49 PST	1/1	

4. *admin2* approves *Session4* which causes the removal of *policy1* from the ADOM.
5. *admin1* attempts to approve *Session3*, but because *Session3* modifies *policy1* which was removed with the approval of *Session4*, a conflict is identified. The conflicting changes are identified in red, and non-conflicting changes are identified in green.
6. *admin1* clicks *Merge All* to merge all non-conflicting changes (green). Changes with conflicts (red) are ignored.



7. admin1 clicks *Continue to Fix Conflict* to copy the latest run database including the configuration after Session4 was approved and all of Session3's merged changes. All unmerged changes are permanently removed.
8. admin1 can now make additional changes, resubmit, and approve Session3.

Factory default IPsec template to configure FortiClient VPN



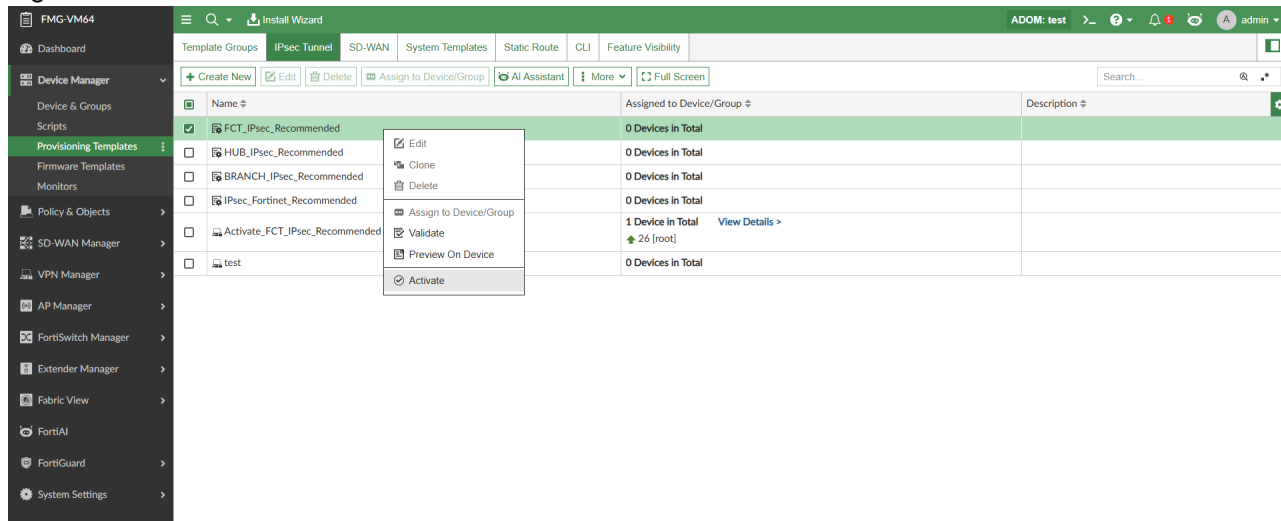
This information is also available in the FortiManager 8.0 Administration Guide:

- Recommended IPsec templates

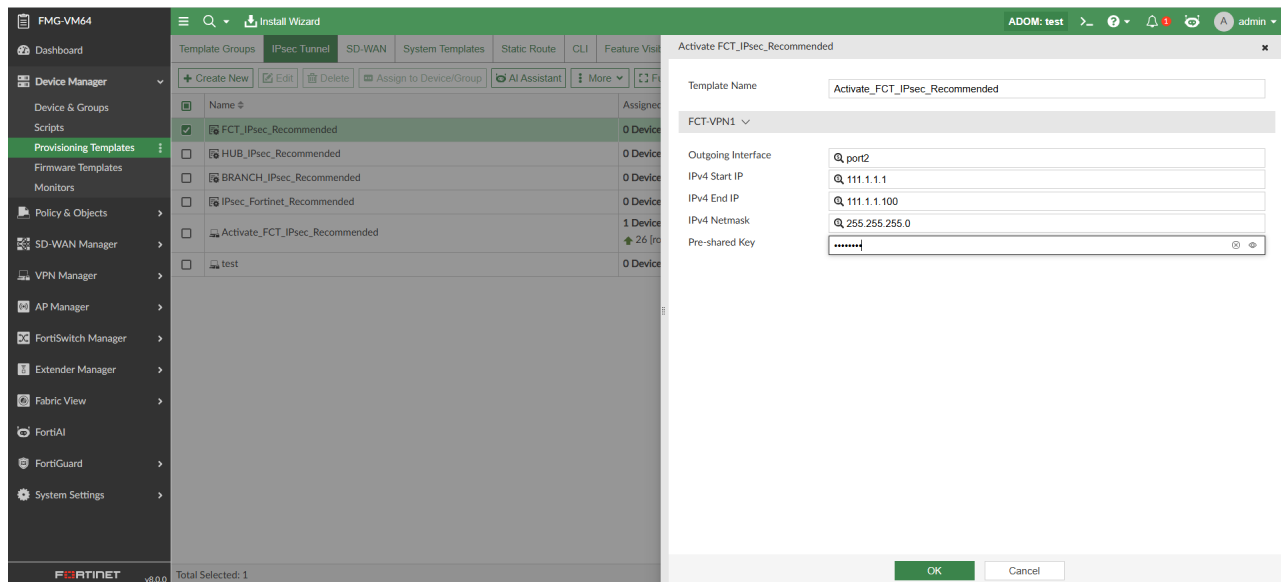
You can use the *FCT_IPsec_Recomended* factory default IPsec template for FortiClient VPN configuration.

To use the *FCT_IPsec_Recommended* factory default template:

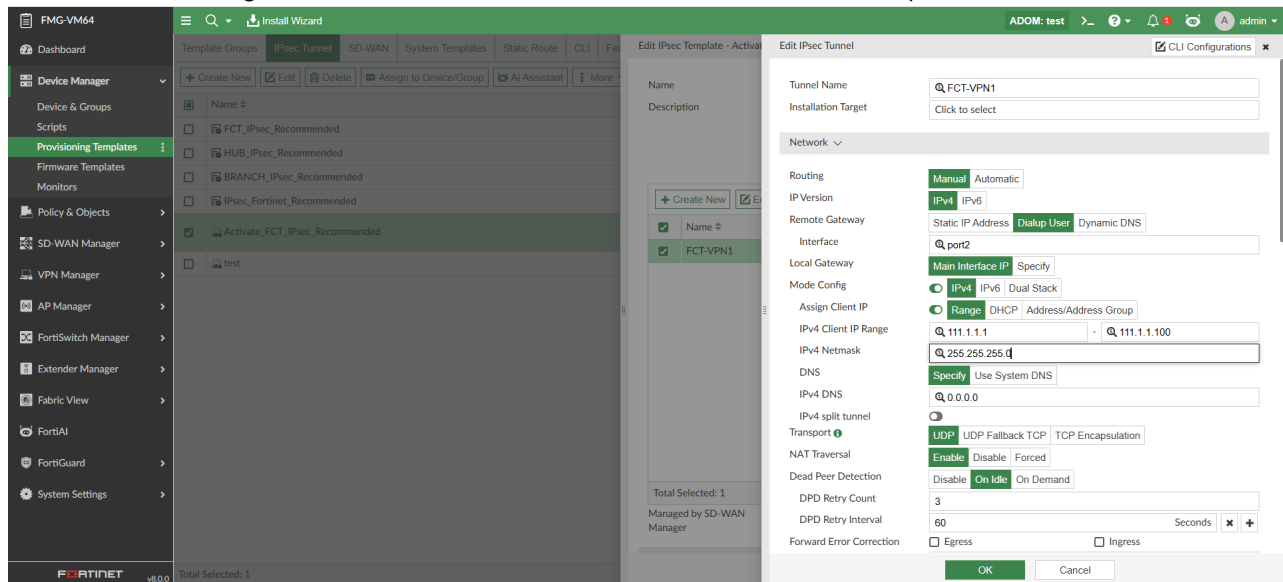
1. Go to *Device Manager > Provisioning Templates > IPsec Tunnel*.
2. Right-click *FCT_IPsec_Recommended*.



3. Click *Activate* and set parameters.



4. Click **OK**. FortiManager creates the *Activate_FCT_IPsec_Recommended* template.



5. Install the template to a managed device to push the configuration to FortiGate.

Central monitoring dashboard for Firewall Users with filters for authentication method and user group



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

- Firewall users

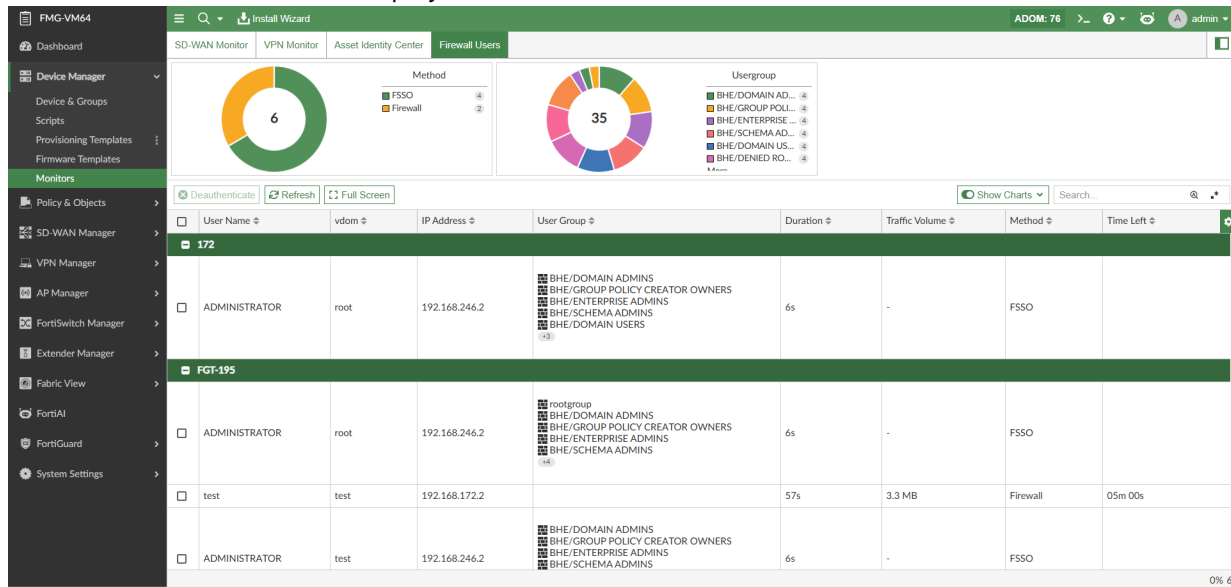
The *Firewall Users* monitor displays all currently logged in firewall users. You can use the monitor to diagnose user-related logons or to highlight and deauthenticate a user.

For more information on firewall user monitors, see the [FortiGate/FortiOS Administration Guide](#).

To view the firewall user monitor:

1. Go to *Device Manager > Monitor > Firewall Users*.

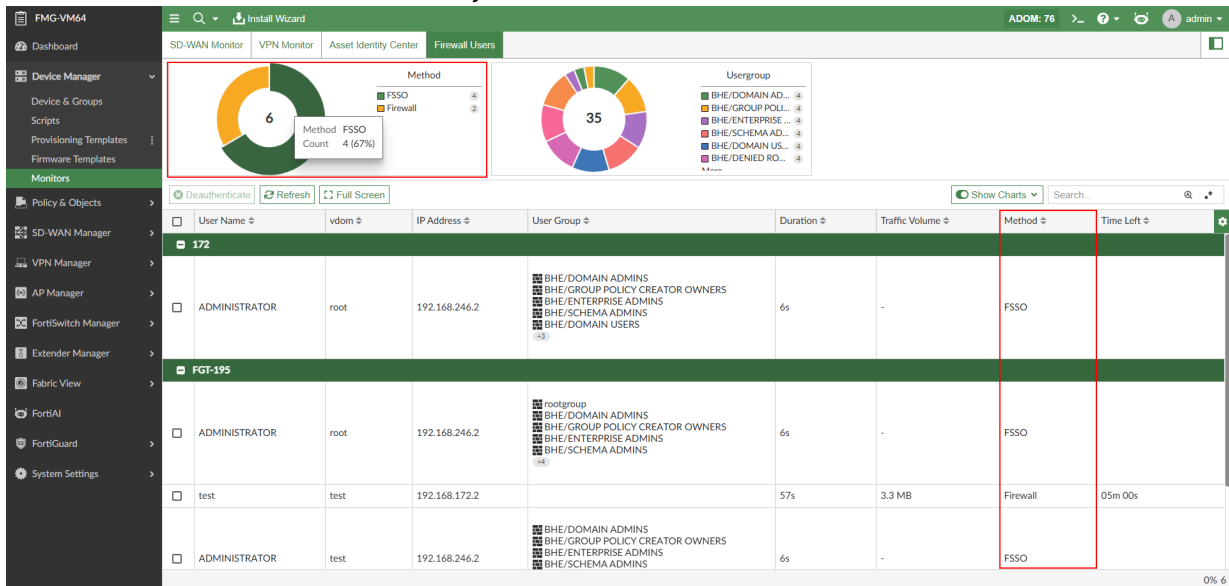
The *Firewall Users* monitor is displayed.



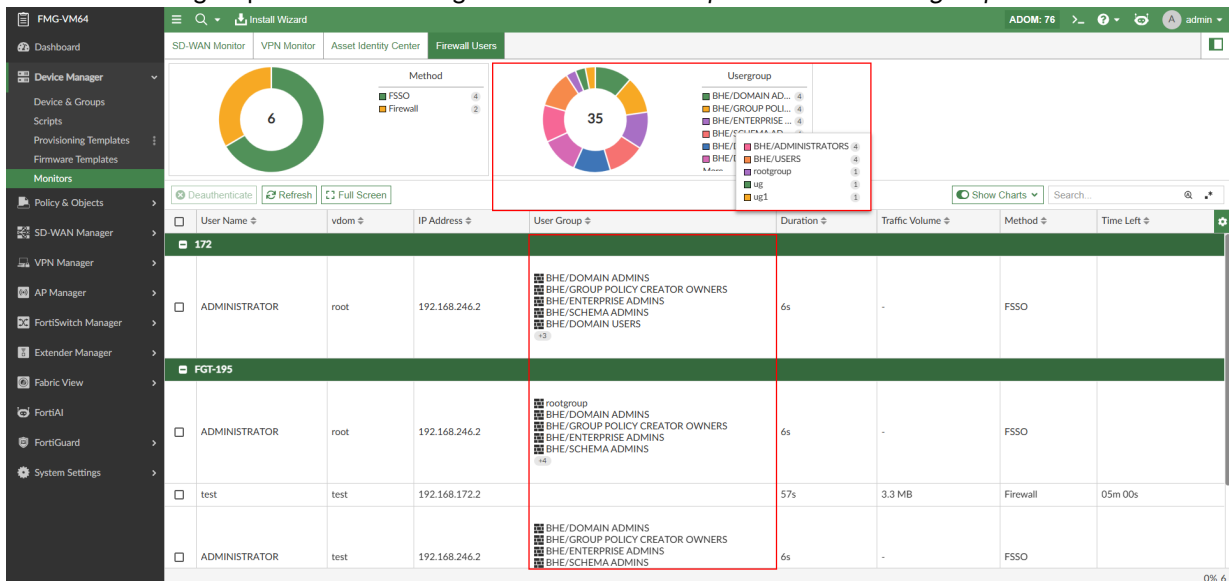
2. In the *Firewall Users* monitor, information about each firewall user is organized by FortiGate.

The following information and functionality is available:

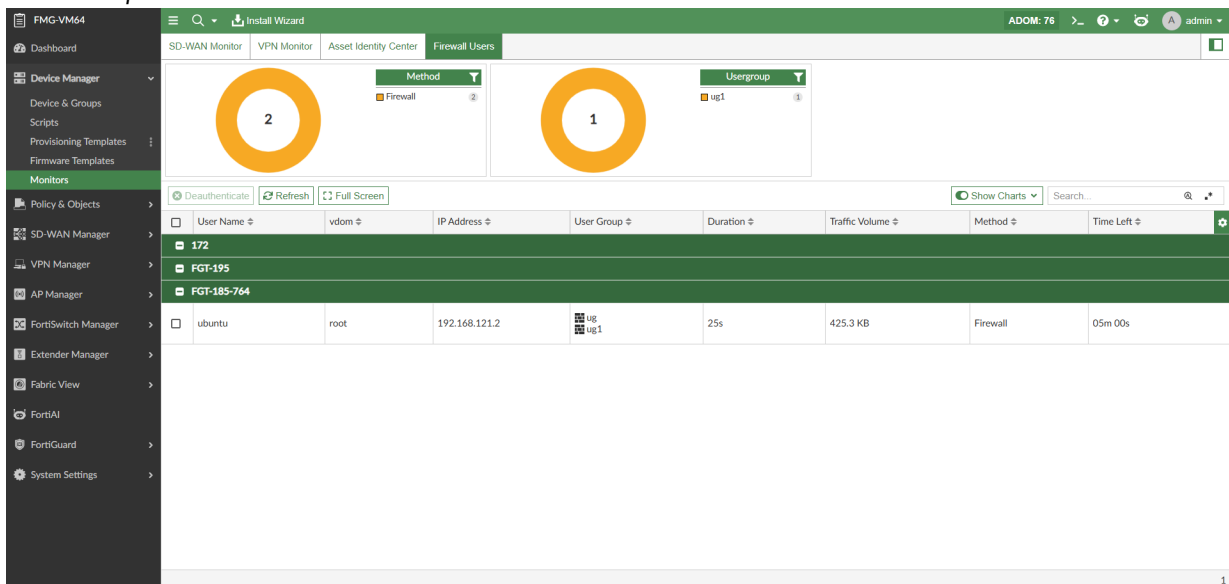
- View the authentication method used by each firewall user in the *Method* column and chart.



- See which user groups the user belongs to in the *User Group* column and *Usergroup* chart.



- Use the filters in the charts above the table to filter data based on the user's authentication *Method* and *User Group*.

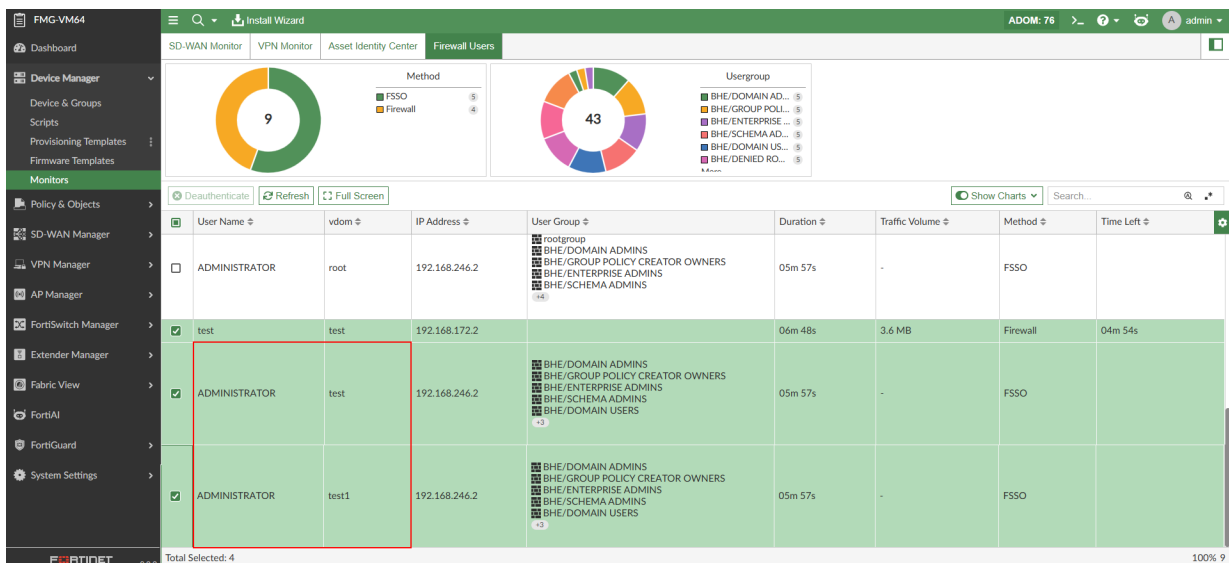


- Deauthenticate firewall users by selecting a user in the table and clicking *Deauthenticate* in the toolbar.

User Name	vdom	IP Address	User Group	Duration	Traffic Volume	Method	Time Left
ADMINISTRATOR	root	192.168.246.2	rootgroup BHE/DOMAIN ADMINS BHE/GROUP POLICY CREATOR OWNERS BHE/ENTERPRISE ADMINS BHE/SCHEMA ADMINS	05m 57s	-	FSSO	
test	test	192.168.172.2		06m 48s	3.6 MB	Firewall	04m 54s
ADMINISTRATOR	test	192.168.246.2	BHE/DOMAIN ADMINS BHE/GROUP POLICY CREATOR OWNERS BHE/ENTERPRISE ADMINS BHE/SCHEMA ADMINS BHE/DOMAIN USERS	05m 57s	-	FSSO	
ADMINISTRATOR	test1	192.168.246.2	BHE/DOMAIN ADMINS BHE/GROUP POLICY CREATOR OWNERS BHE/ENTERPRISE ADMINS BHE/SCHEMA ADMINS BHE/DOMAIN USERS	05m 57s	-	FSSO	

User Name	vdom	IP Address	User Group	Duration	Traffic Volume	Method	Time Left
win	root	192.168.171.2		04m 10s	7.6 MB	Firewall	04m 56s
ADMINISTRATOR	root	192.168.246.2	rootgroup BHE/DOMAIN ADMINS BHE/GROUP POLICY CREATOR OWNERS BHE/ENTERPRISE ADMINS BHE/SCHEMA ADMINS	09m 24s	-	FSSO	
ADMINISTRATOR	test	192.168.246.2	BHE/DOMAIN ADMINS BHE/GROUP POLICY CREATOR OWNERS BHE/ENTERPRISE ADMINS BHE/SCHEMA ADMINS BHE/DOMAIN USERS	09m 24s	-	FSSO	
ADMINISTRATOR	test1	192.168.246.2	BHE/DOMAIN ADMINS BHE/GROUP POLICY CREATOR OWNERS BHE/ENTERPRISE ADMINS BHE/SCHEMA ADMINS BHE/DOMAIN USERS	09m 24s	-	FSSO	

- Distinguish users that exist in two different VDOMs using the *VDOM* column.



Maximum length of meta variables value increased to 32768 characters



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

- ADOM-level metadata variables

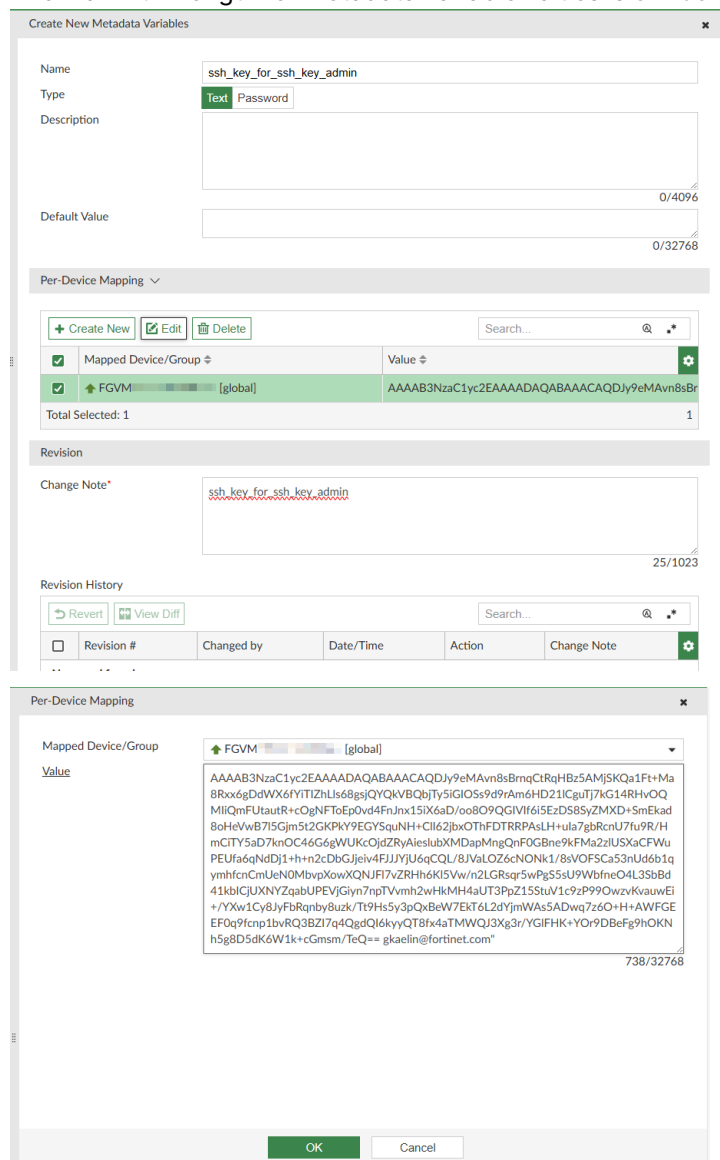
The maximum length for metadata variable values has been increased to 32768 characters. In previous versions, these values only supported up to 256 characters.

For example: Use a metadata variable for SSH key

1. Create a metadata variable called `ssh_key_for_ssh_key_admin`.
2. Set the value to be a long string:

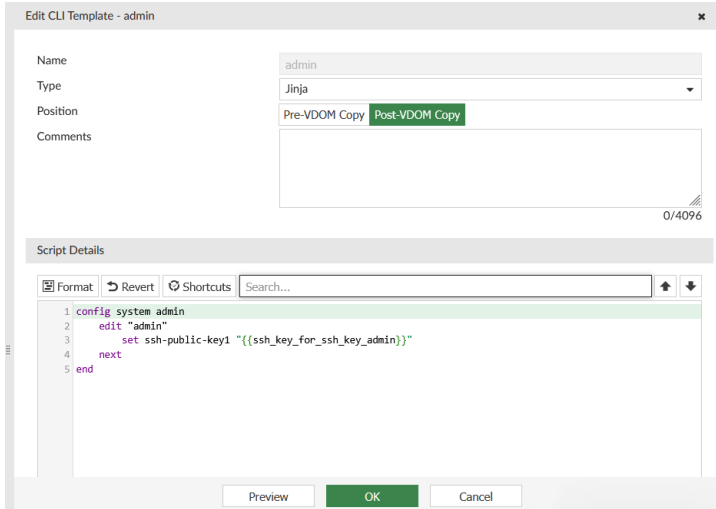
```
"ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDQJy9eMAvn8sBrnqCtRqHBz5AMjSKQa1Ft+Ma8Rxx6gDdWX6fYiTIzhLls68gsjQY
QkVBQbjTy5iGI0Ss9d9rAm6HD21lCguTj7kG14RHv0QMIiQmFUtautR+cOgNFToEp0vd4FnJnx15iX6aD/oo809QGIVIf6
i5EzDS8SyZMXD+SmeKad8oHeVwB715Gjm5t2GKPKY9EGYSquNH+C1I62jbx0ThFDTRRPAsLH+uIa7gbRcnU7fu9R/HmCiT
Y5aD7kn0C46G6gWUKc0jdZRYaies1ubXMDapMngQnF0GBne9kFma2z1USXaCFWuPEUfa6qNdDj1+h+n2cDbGJjeiv4FJJJ
YjU6qCQL/8JVaLOZ6cN0nk1/8sVOFSCa53nUd6b1qymhfCnCMuEN0MbvpXowXQNjF17vZRHh6K15Vw/n2LGRsqr5wPgS5s
U9Wbfn04L3SbD41kbICjUXNYZqabUPEVjGiyn7npTVvmh2wHkMH4uT3PpZ15StuV1c9zP990wzvKvauwEi+/YXw1Cy8
JyFbRqnby8uzk/Tt9Hs5y3pQxBew7EkT6L2dYjmwAs5ADwq7z60+H+AWFGEEF0q9fcnp1bvRQ3BZI7q4QgdQI6kyyQT8fx
4aTMWQJ3Xg3r/YG1FHK+Y0r9DBeFg9h0KNh5g8D5dK6W1k+cGmsm/TeQ== abbccd@fortinet.com"
```

The maximum length for metadata variable values is 32768 characters.

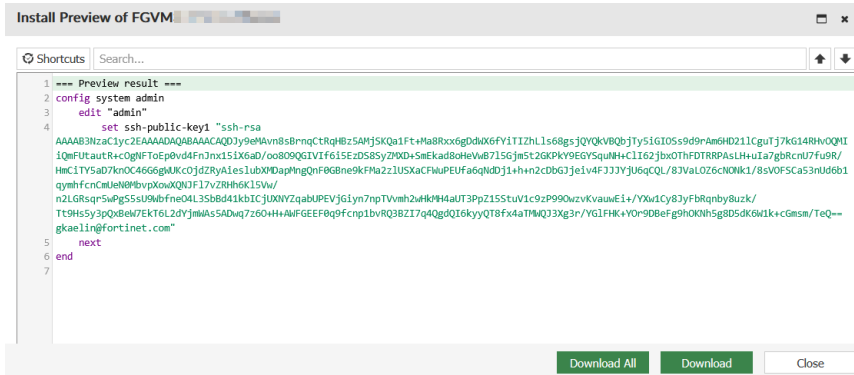


3. Create a Jinja CLI template and use the metadata in the Jinja script.

```
config system admin
    edit "admin"
        set ssh-public-key1 "{{ssh_key_for_ssh_key_admin}}"
    next
end
```



4. Assign the Jinja CLI template to a FortiGate and install the configuration.



Admin profile adds granular control on device manager (Interface, Log & Report, Security Fabric) and Routing




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

- Role-based access control for device configurations and routing

Administrator permissions have been updated to allow for granular control over access to provisioning templates and device configurations.

Permission	Description
Manage Device Configurations	The Manage Device Configurations permission is separated into the following permissions: <ul style="list-style-type: none"> • <i>Interface</i> • <i>Log & Report</i> • <i>Security Fabric</i> • <i>Others</i>

Permission	Description
	These permissions control a users ability to make changes to devices using the device configuration menu in Device Manager.
Interface device-interface	Controls permissions for the following sections in the device configuration menu: <ul style="list-style-type: none"> • <i>Network > Interfaces</i> • <i>Network > DHCP Servers</i>
Log & Report device-log	Controls permissions for the following sections in the device configuration menu: <ul style="list-style-type: none"> • <i>Log & Report > Log Settings</i>
Security Fabric device-fabric	Controls permissions for the following sections in the device configuration menu: <ul style="list-style-type: none"> • <i>Security Fabric > Automation Stitch</i> • <i>Security Fabric > Automation Trigger</i> • <i>Security Fabric > Automation Action</i>
Others device-config	Controls access to the device configuration menu in the Device Manager along with other settings not included under <i>Interface</i> , <i>Log & Report</i> , and <i>Security Fabric</i> permissions. <div style="border: 1px solid orange; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> If <i>Other</i> is set to <i>None</i>, the admin will be unable to access the device configurations menu in the <i>Device Manager</i> even when other settings (<i>Interface</i>, <i>Log & Report</i>, <i>Security Fabric</i>, <i>Route</i>, <i>SD-WAN</i>) are set to higher permission levels.</p> </div>
SD-WAN device-wan-link-load-balance	Controls permissions for SD-WAN templates and SD-WAN device configurations.
Routing device-route	Controls permissions for routing templates and configurations. The following provisioning templates are controlled by this permission: <ul style="list-style-type: none"> • BGP Templates • Static Route Templates The following managed device configurations are controlled by this permission: <ul style="list-style-type: none"> • <i>Network > Static Routes</i> • <i>Network > Policy Routes</i> • <i>Network > RIP</i> • <i>Network > BGP</i> • <i>Network > OSPF</i> • <i>Network > Routing Objects</i> • <i>Network > Multicast</i>



Permissions applied to custom profiles during upgrade

When upgrading to 8.0.0, the *Interface*, *Log & Report*, *Security Fabric*, and *Routing* permissions are set to *None* for existing custom permission profiles. The *Others* permission will follow the settings applied to the previously available *Manage Device Configurations* permission.

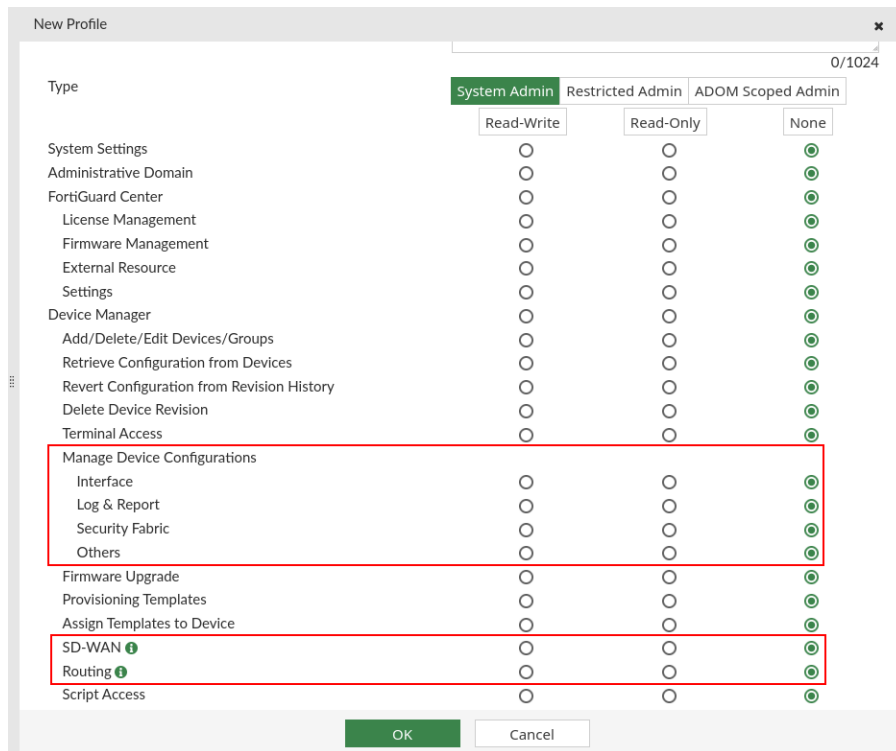
For example, when upgrading to 8.0.0 with *Read-Write* permissions for *Manage Device Configurations*:

- **Interface:** *None*
- **Log & Report:** *None*
- **Security Fabric:** *None*
- **Others:** *Read-Write*
- **Routing:** *None*

SD-WAN will retain its permission levels in custom permission profiles following upgrade.

To configure permissions for device configurations and routing in the GUI:

1. Go to *Systems Settings > Admin Profiles > Create New*.
2. Configure settings for the following permission levels.
 - Interface
 - Log & Report
 - Security Fabric
 - Others
 - SD-WAN
 - Routing
3. Click *OK* to save the permission.




To configure permissions for device configurations and routing in the CLI:

```

config system admin profile
  edit "profile "
    set device-config {read-write | read | none}
    set device-interface {read-write | read | none}
    set device-log {read-write | read | none}
    set device-fabric {read-write | read | none}
    set device-wan-link-load-balance {read-write | read | none}
    set device-route {read-write | read | none}
  next
end
    
```

pxGrid connector is enhanced to display Device Type and Session State

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

- [Creating Cisco pxGrid connectors](#)

The pxGrid connector displays the *Device Type* and *Session State* information for connected users in the FortiManager GUI and CLI.

To view pxGrid Device Type and Session State in the GUI:

1. Go to *Fabric View > External Connectors* or *Policy & Objects > Security Fabric > Endpoint/Identity*.
2. Edit an existing pxGrid connector. See [Creating Cisco pxGrid Connectors](#).
3. In the *Connected Users* table, the *Device Type* and *Session State* is displayed for connected users.

The first screenshot shows the 'Edit pxGrid Connector - bug-1231196-ISE' configuration page. The 'Connector Users' table is visible, showing a list of users with columns for Name, IP Address, Device Type, and Session State. One user is highlighted: '1.1.1.1' with 'VMWare-Device' and 'Started' session state.

Name	IP Address	Device Type	Session State
px_bug-1231196-ISE_ANY (0/0)			
px_bug-1231196-ISE_Auditors (0/0)			
px_bug-1231196-ISE_BYOD (0/0)			
px_bug-1231196-ISE_Contractors (0/0)			
px_bug-1231196-ISE_Developers (1/1)			
1.1.1.1		VMWare-Device	Started
px_bug-1231196-ISE_Development_Servers (0/0)			
px_bug-1231196-ISE_Employees (1/1)			
px_bug-1231196-ISE_Guests (0/0)			
px_bug-1231196-ISE_Network_Services (0/0)			

The second screenshot shows the 'Fabric Connectors' table in the 'Endpoint/Identity' view. The 'bug-1231196-ISE' connector is selected, showing its IP address as 192.168.15.218.

Name	Type	Details
Poll Active Directory Server		
Fortinet Single Sign-On Agent		
RADIUS Single Sign-On Agent		
pxGrid Connector		
bug-1231196-ISE	pxGrid Connector	192.168.15.218
ClearPass Connector		
NSX-T Connector		
FortiFlex Connector		
vCenter Connector		
Symantec Endpoint Protection		
Exchange Server Connector		
JSON API Connector		
Guardicore Connector		
Cisco ACI Connector		
Microsoft Azure Connector		

To view pxGrid Device Type and Session State in the CLI:

1. In the FortiManager CLI, enter the following command:

```
diagnose system print connector <dom> pxgrid <connector_name> <optional_filter/tag>
```

For example, the command is run to view connected user information from a pxGrid connector without any filters:

```
diagnose system print connector root pxgrid bug-1231196-ISE
```

User List:

```
idx: 0; key: 1.1.1.1-1.1.1.1; name: user123; state: 1; grpname: pxgrid-ISE_Developers; start_
ip: 1.1.1.1; end_ip: 1.1.1.1; grpidx: 4
-----Filter Attrs-----device_type: VMWare-Device; session_state: STARTED;
```

Group List:

```
idx: 0; id: 92bb1950-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_ANY; tag: 65535; desc: Any
Security Group; flags: 0
idx: 1; id: 934557f0-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Auditors; tag: 9; desc:
Auditor Security Group; flags: 0
idx: 2; id: 935d4cc0-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_BYOD; tag: 15; desc: BYOD
Security Group; flags: 0
idx: 3; id: 9370d4c0-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Contractors; tag: 5; desc:
Contractor Security Group; flags: 0
idx: 4; id: 93837260-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Developers; tag: 8; desc:
Developer Security Group; flags: 0
idx: 5; id: 9396d350-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Development_Servers; tag:
12; desc: Development Servers Security Group; flags: 0
idx: 6; id: 93ad6890-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Employees; tag: 4; desc:
Employee Security Group; flags: 0
idx: 7; id: 93c66ed0-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Guests; tag: 6; desc: Guest
Security Group; flags: 0
idx: 8; id: 93e1bf00-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Network_Services; tag: 3;
desc: Network Services Security Group; flags: 0
idx: 9; id: 93f91790-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_PCI_Servers; tag: 14; desc:
PCI Servers Security Group; flags: 0
idx: 10; id: 940facd0-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Point_of_Sale_Systems;
tag: 10; desc: Point of Sale Security Group; flags: 0
idx: 11; id: 9423aa00-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Production_Servers; tag:
11; desc: Production Servers Security Group; flags: 0
idx: 12; id: 9437a730-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Production_Users; tag: 7;
desc: Production User Security Group; flags: 0
idx: 13; id: 944b2f30-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Quarantined_Systems; tag:
255; desc: Quarantine Security Group; flags: 0
idx: 14; id: 94621290-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Test_Servers; tag: 13;
desc: Test Servers Security Group; flags: 0
idx: 15; id: 947832a0-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_TrustSec_Devices; tag: 2;
desc: TrustSec Devices Security Group; flags: 0
idx: 16; id: 92adf9f0-8c01-11e6-900c-525400b41111; name: pxgrid-ISE_Unknown; tag: 0; desc:
Unknown Security Group; flags: 0
```

Summary:

```
matched: user number = 1, changed user number = 0, adgrp number = 17
```

You can use the *Session State* and *Device Type* as keywords to filter the command output.

For example, the command is run to view connected user information from a pxGrid connector with the *STARTED* Session State filter.

```
diagnose system print connector root pxgrid bug-1231196-ISE STARTED
```

User List:

```
idx: 0; key: 1.1.1.1-1.1.1.1; name: user123; state: 1; grpname: px_bug-1231196-ISE_Developers;
start_ip: 1.1.1.1; end_ip: 1.1.1.1; grpidx: 4
-----Filter Attrs-----device_type: VMWare-Device; session_state: STARTED;
```

Summary:

matched: user number = 1, changed user number = 0, adgrp number = 0

Managing FortiGate registration to FortiCare

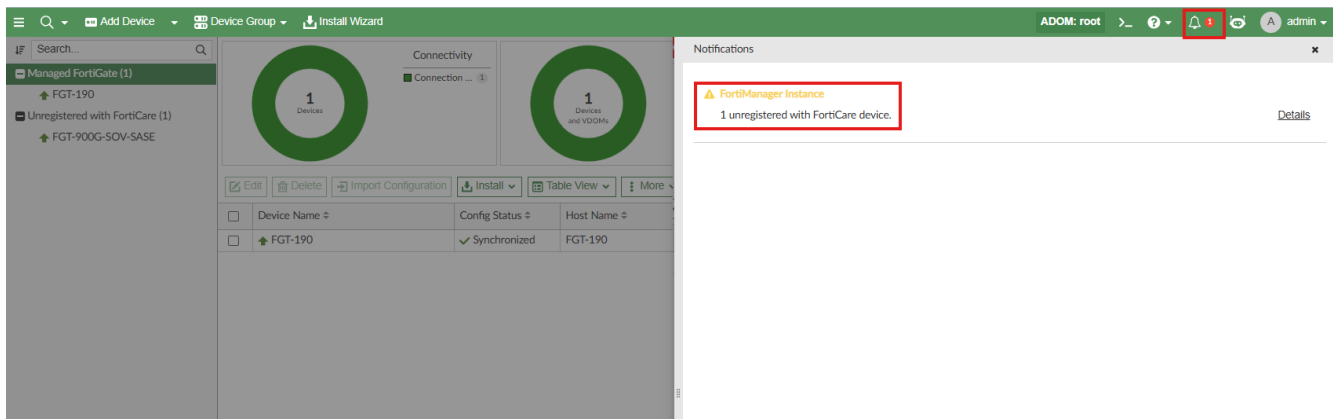


This information is also available in the FortiManager 8.0 Administration Guide:

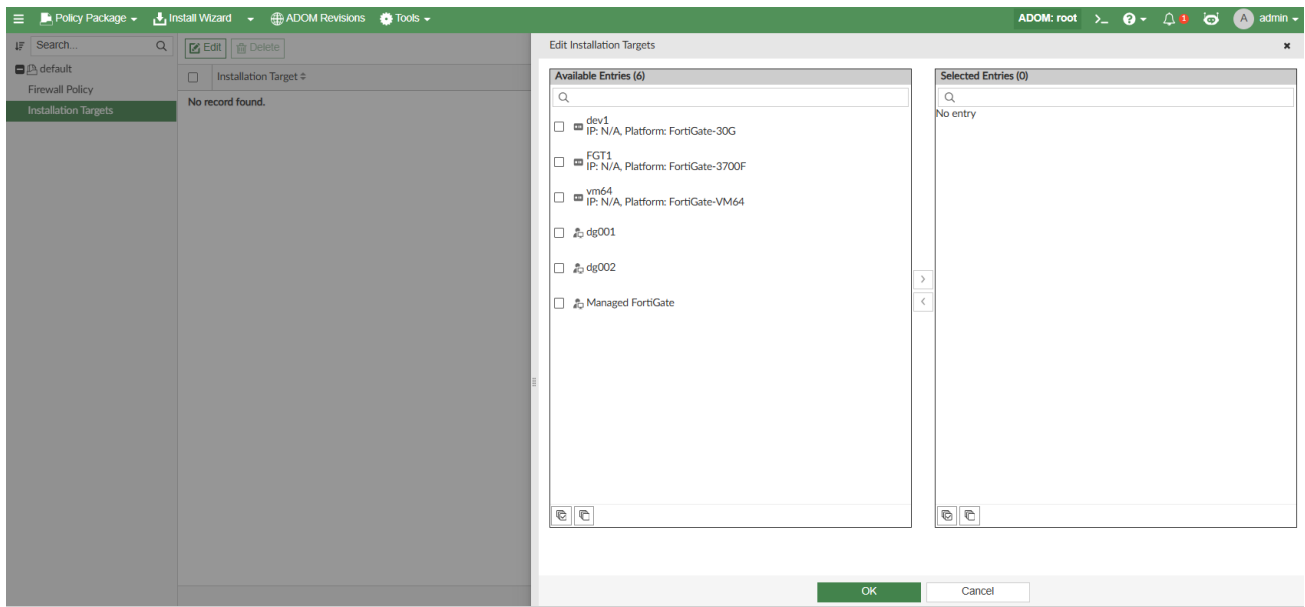
- [Managing FortiGate registration to FortiCare](#)

When FortiGate devices are first added to FortiManager, FortiManager will check the device's FortiCare contract status. FortiGate devices that are unregistered with FortiCare are automatically assigned to the *Unregistered with FortiCare* device group.

A FortiManager notification is displayed when there are managed devices that are currently unregistered with FortiCare.

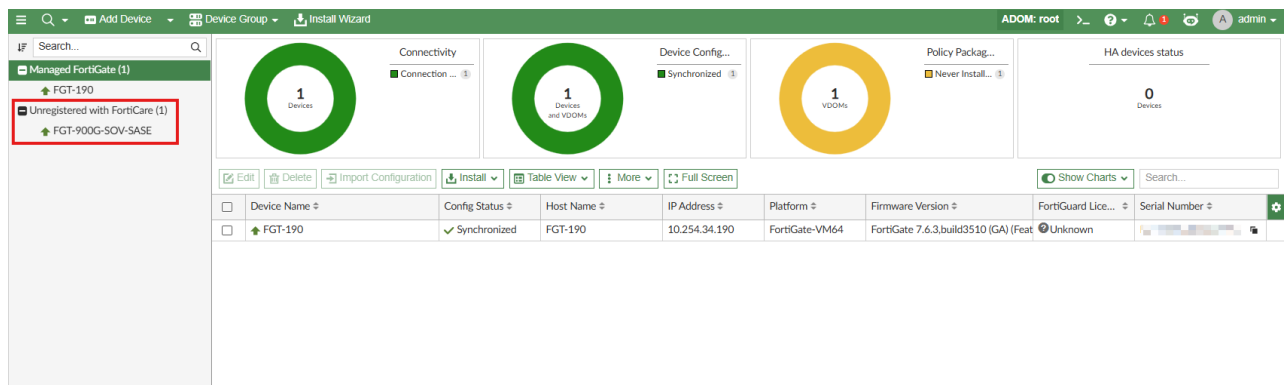


Unregistered devices cannot be selected as *Installation Targets* for policy packages.

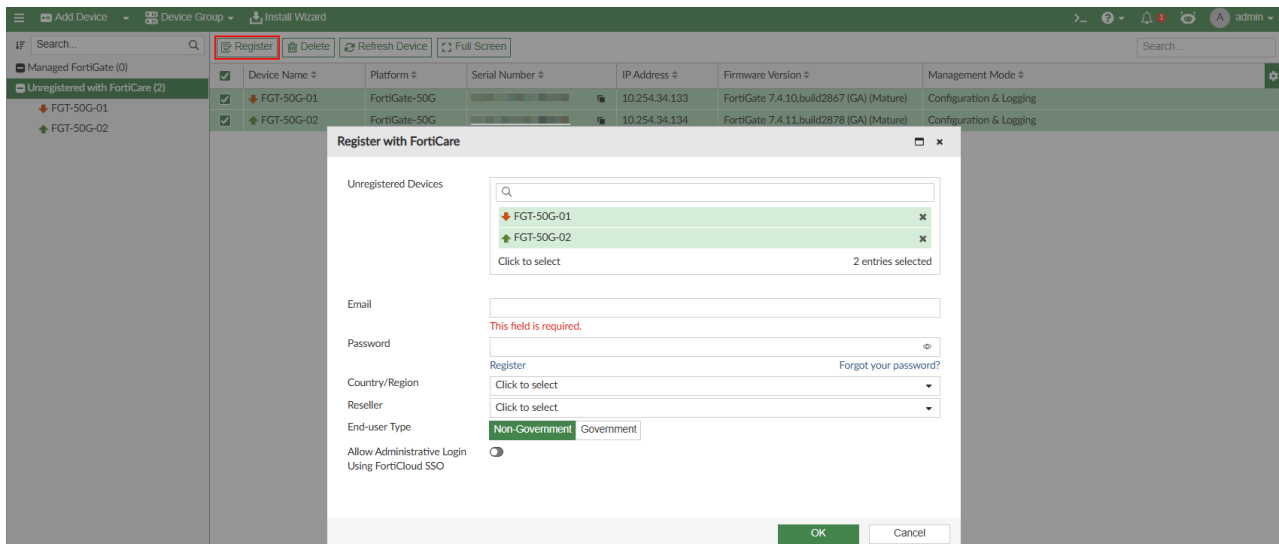


To register FortiGate devices to FortiCare through FortiManager:

1. Go to *Devices Manager > Devices & Groups*, and select the *Unregistered with FortiCare* device group.



2. Select one or more devices in the device table, and click *Register* in the toolbar. The Register with FortiCare dialog is displayed.

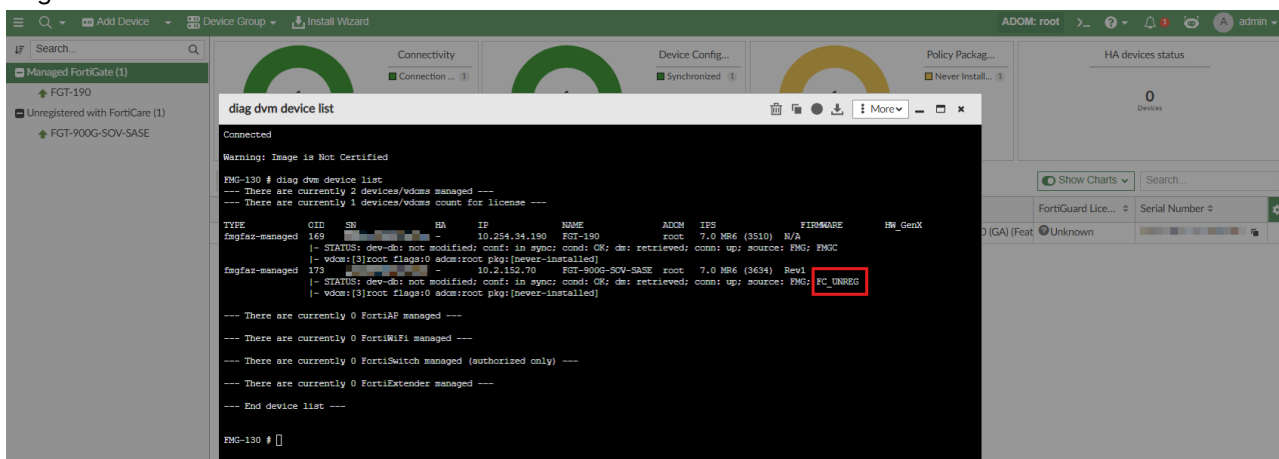


3. Enter the registration information, and click *OK*.
4. Once the registration has been completed successfully, click *Finish*.
The now registered devices will be moved into the default *Managed FortiGate* device group.

To view managed FortiGate's FortiCare registration status in the CLI:

You can use the `diagnose dvm device list` command in the FortiManager CLI to view the FortiCare registration status of managed FortiGate devices.

- Unregistered devices have the *FC_UNREG* status.
- Registered devices have the *FMG* status.



Enhanced asset details and identity monitoring




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

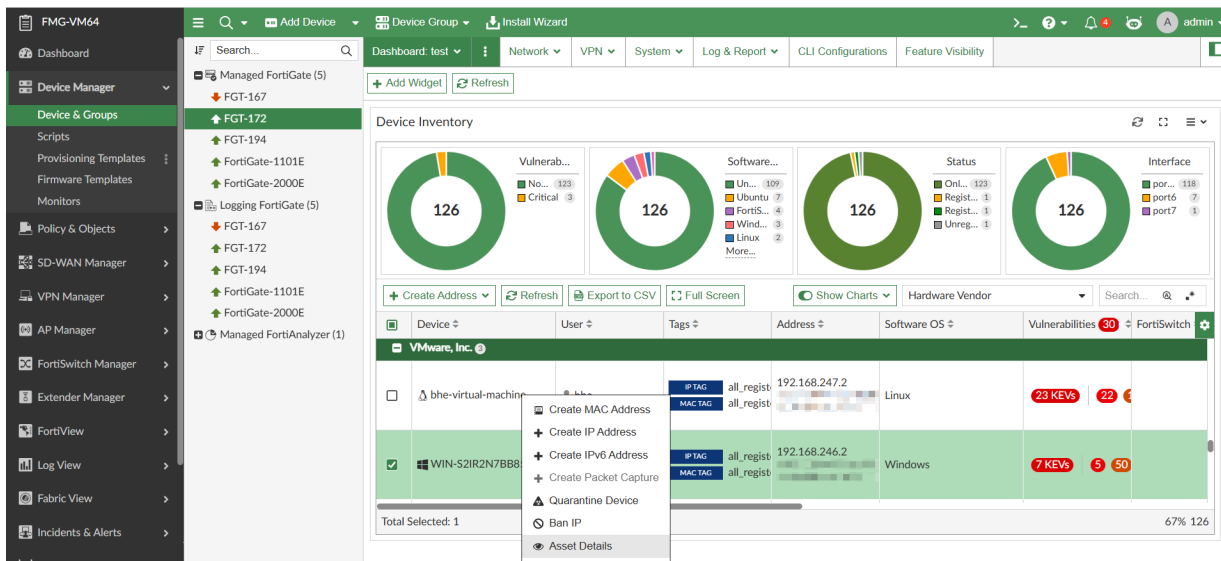
- Enhanced asset details and identity monitoring

Enhanced Assets Details and Identity Monitoring was added to the Device Dashboard to view assets information, create or ban IP/MAC addresses, disassociated wireless clients, and review vulnerability and risk scores.

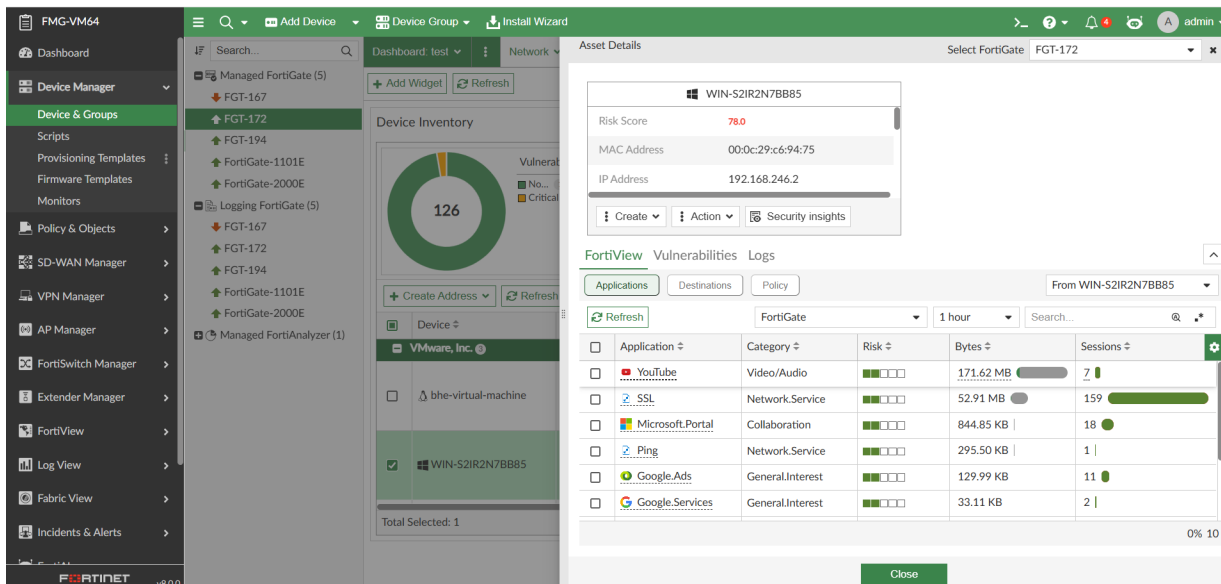
To access asset details in the Device Inventory widget:

1. Go to *Device Manager > Device & Groups* and select a device from the tree menu to view its configuration.
2. In the *Device Inventory* widget, right-click on an asset in the table and select *Asset Details* from the context menu.

 The *Device Inventory* widget can be added to a dashboard through the *Add Widget* feature.

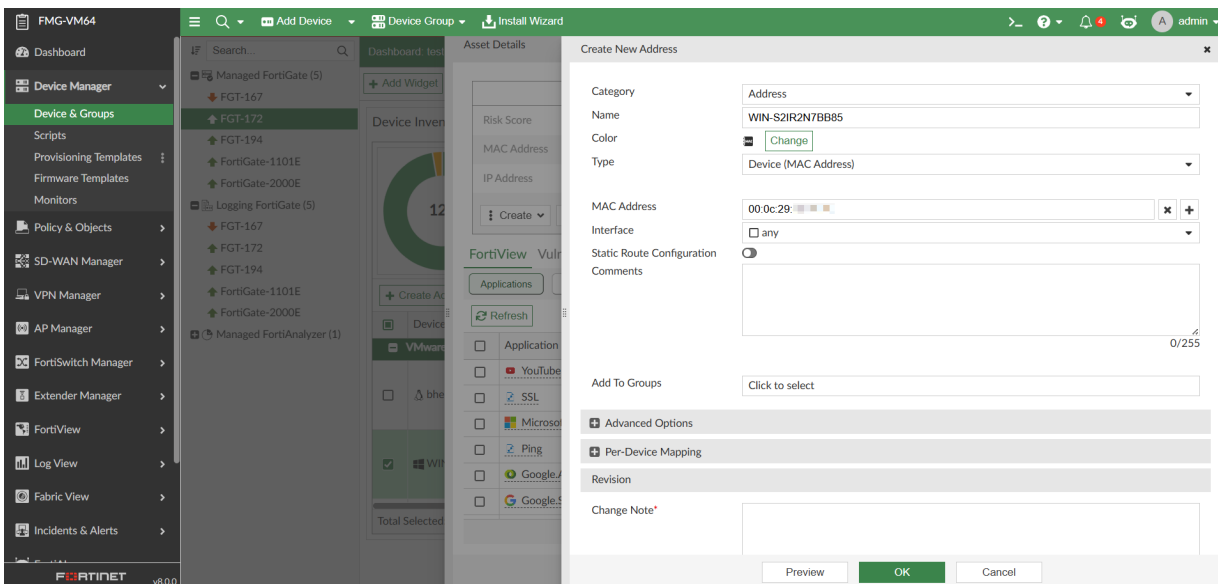
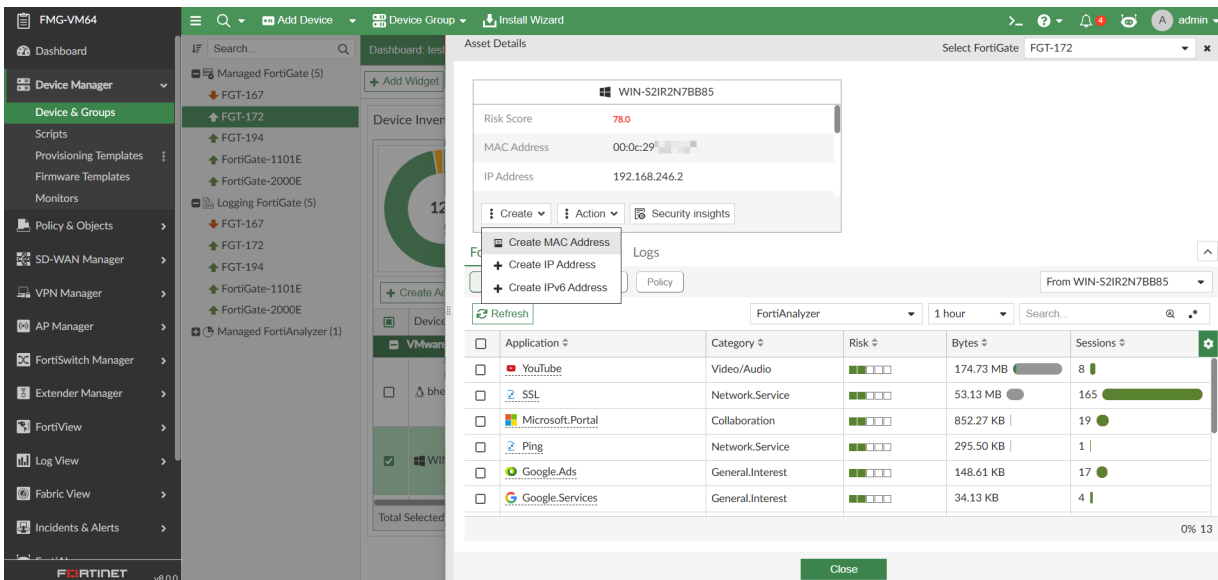


The *Asset Details* menu is displayed. This menu includes additional information for enhanced visibility, diagnosis, and analysis, similar to FortiGate.

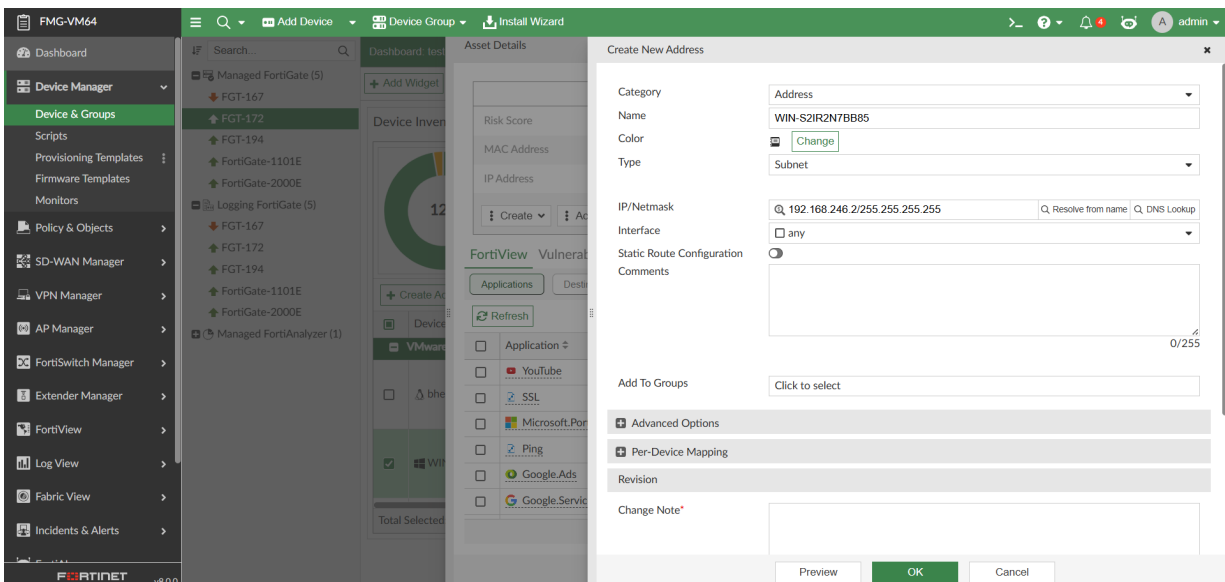
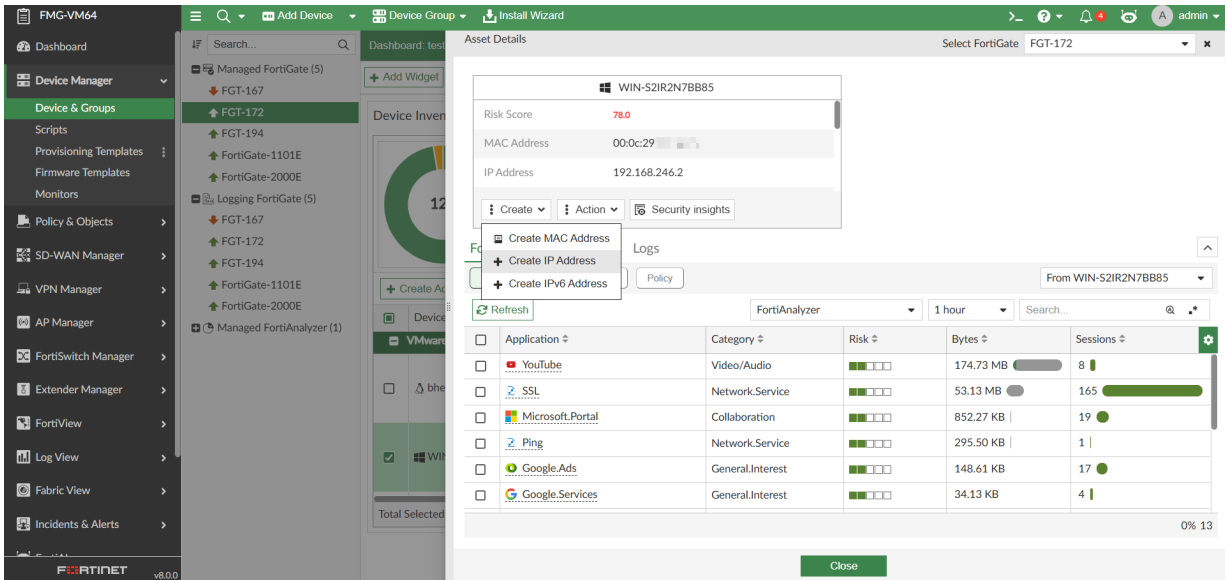


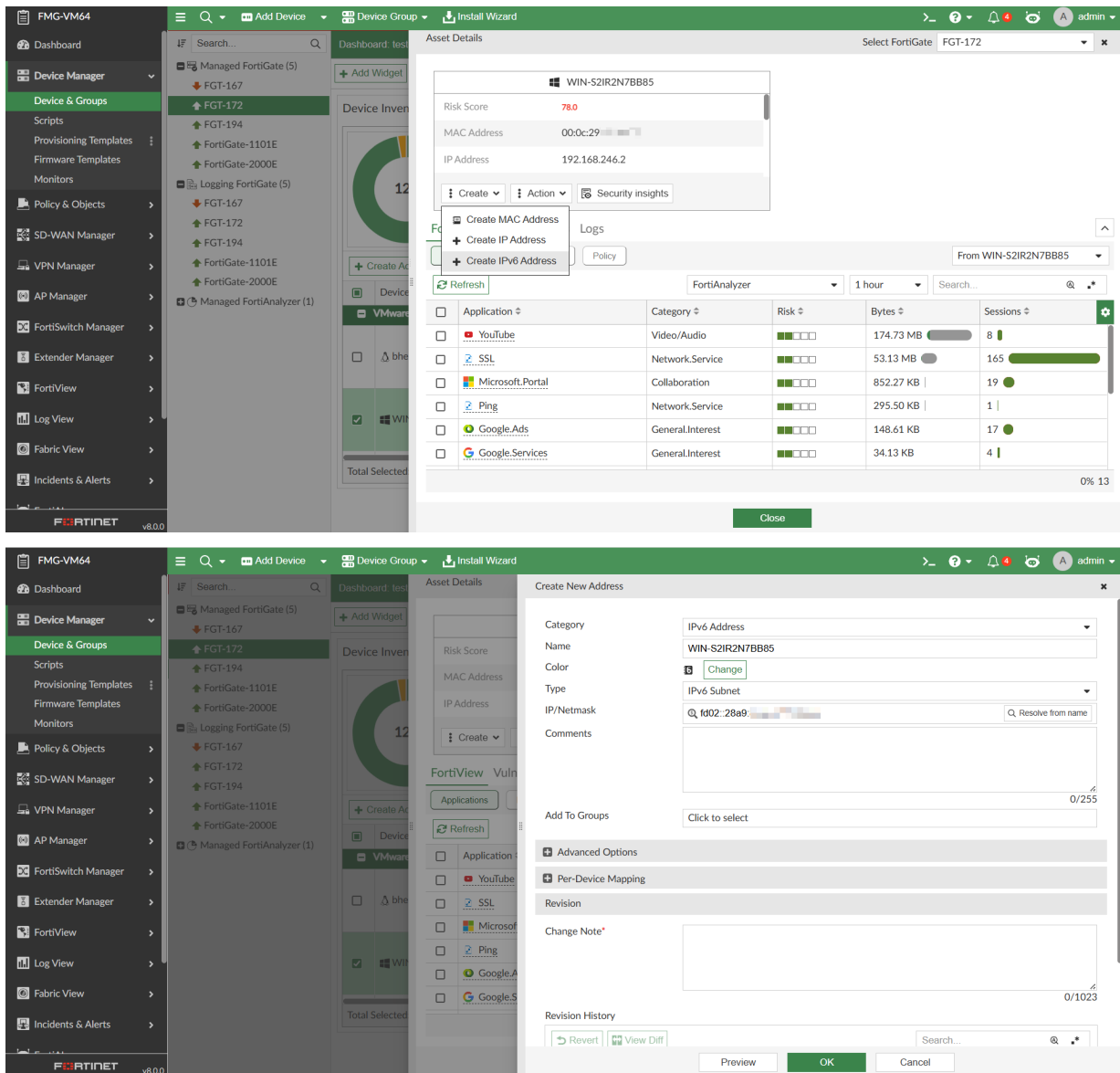
3. From the *Asset Details* menu, you can perform the following actions:

a. Create MAC addresses.

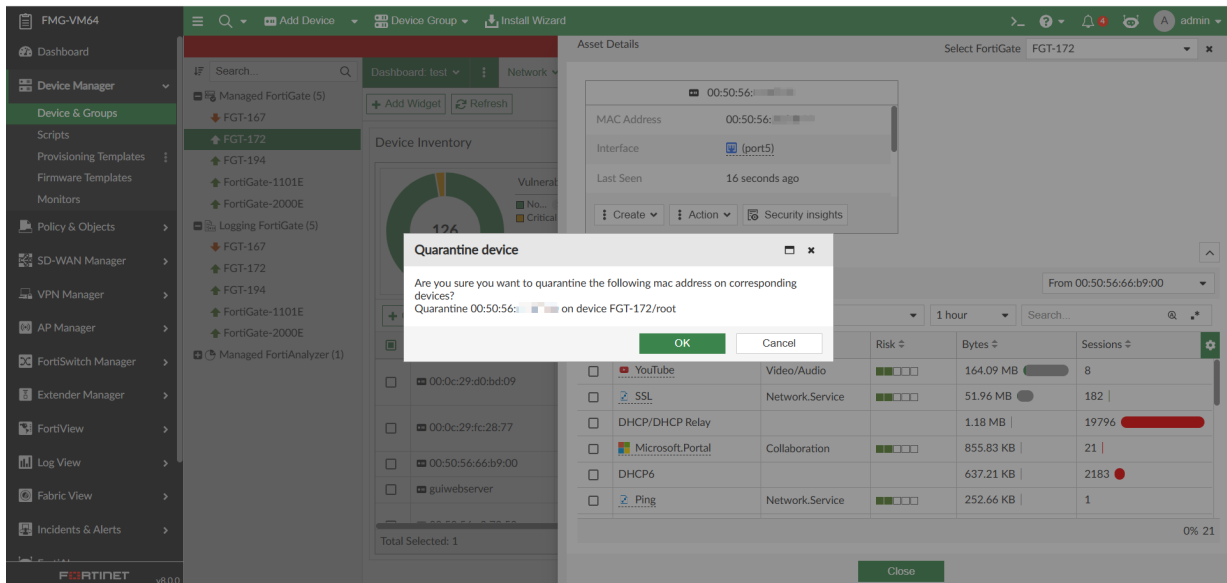
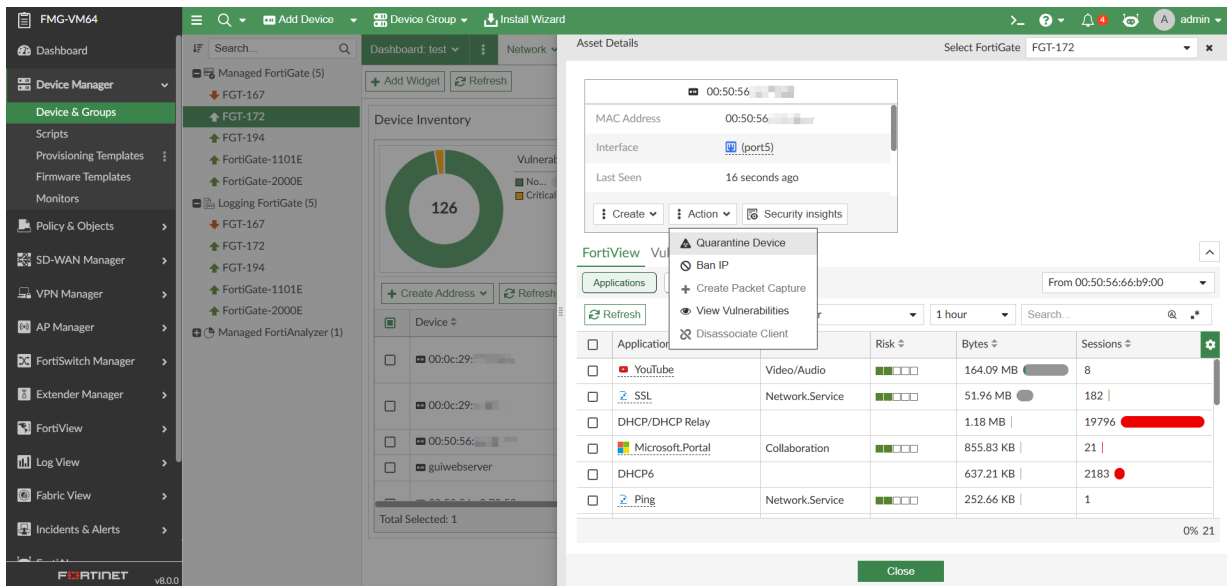


b. Create IP addresses (IPv4 and IPv6)

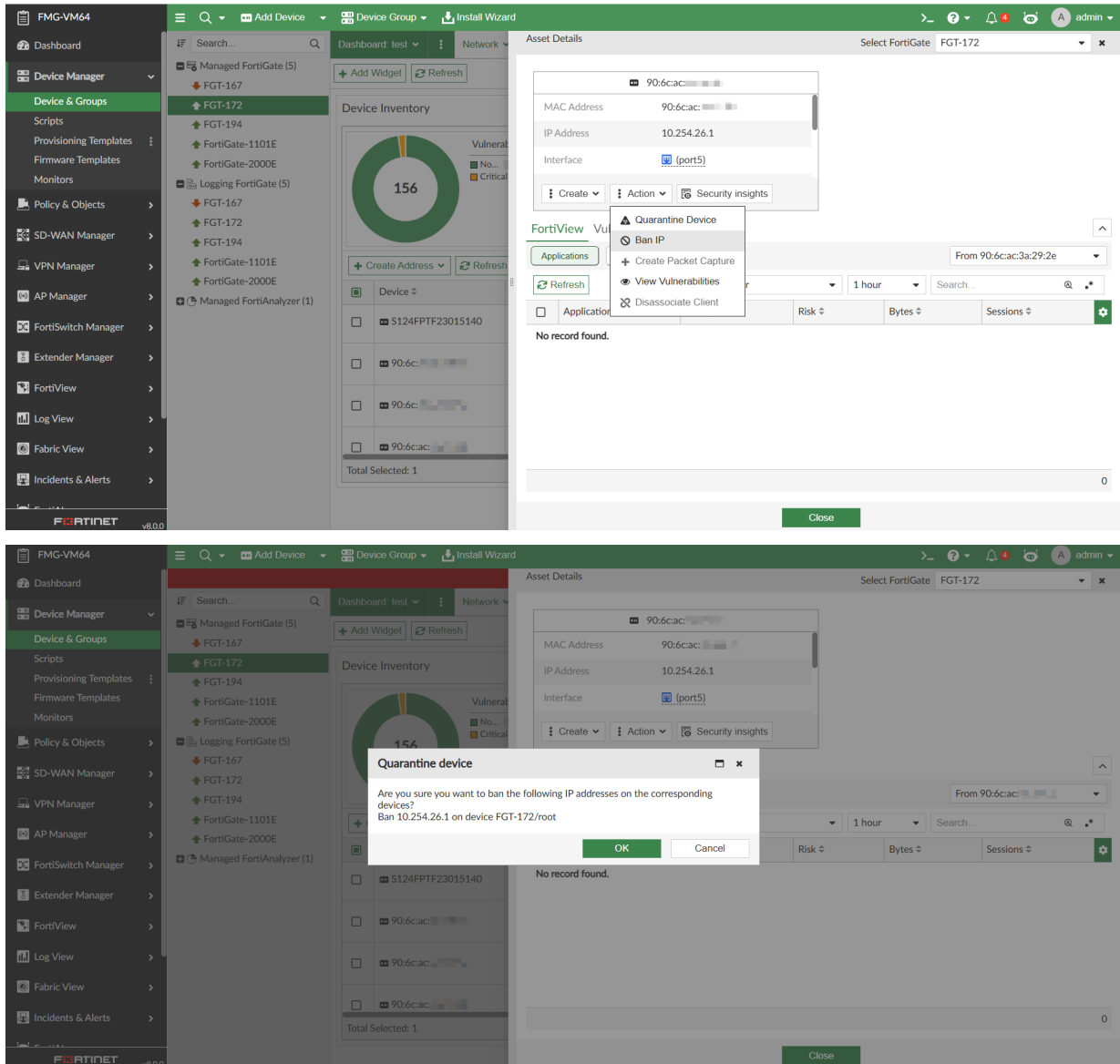




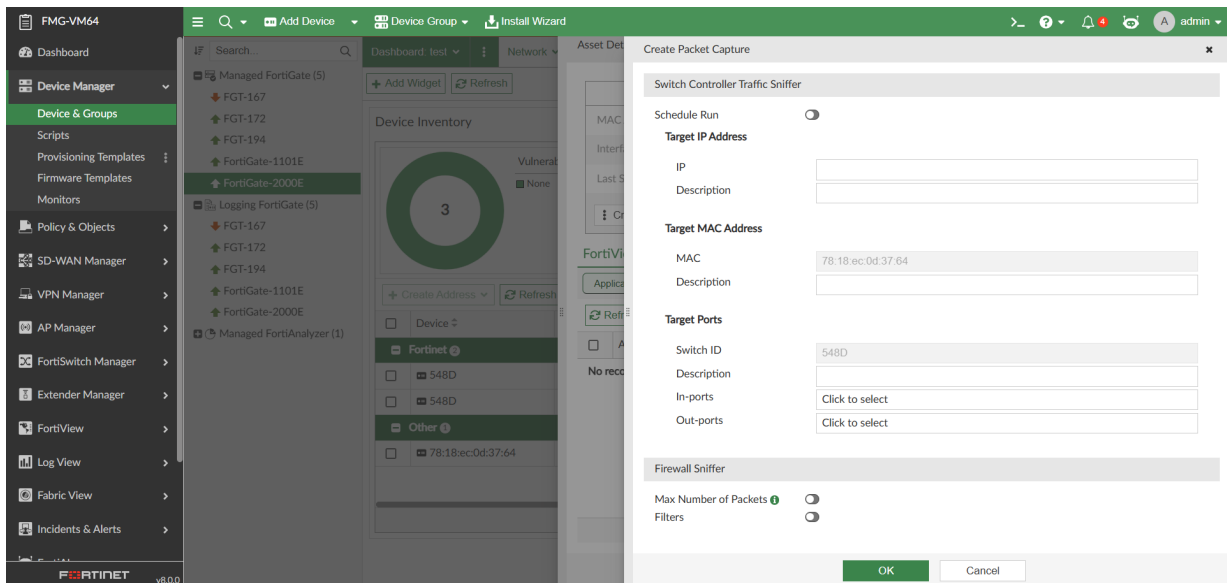
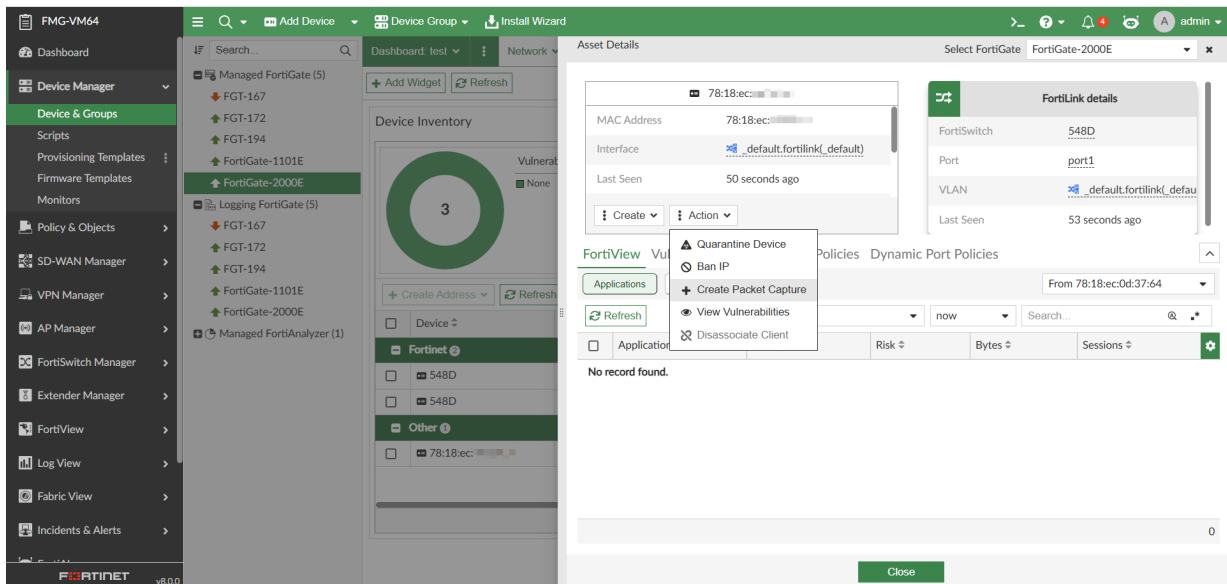
c. Quarantine devices.



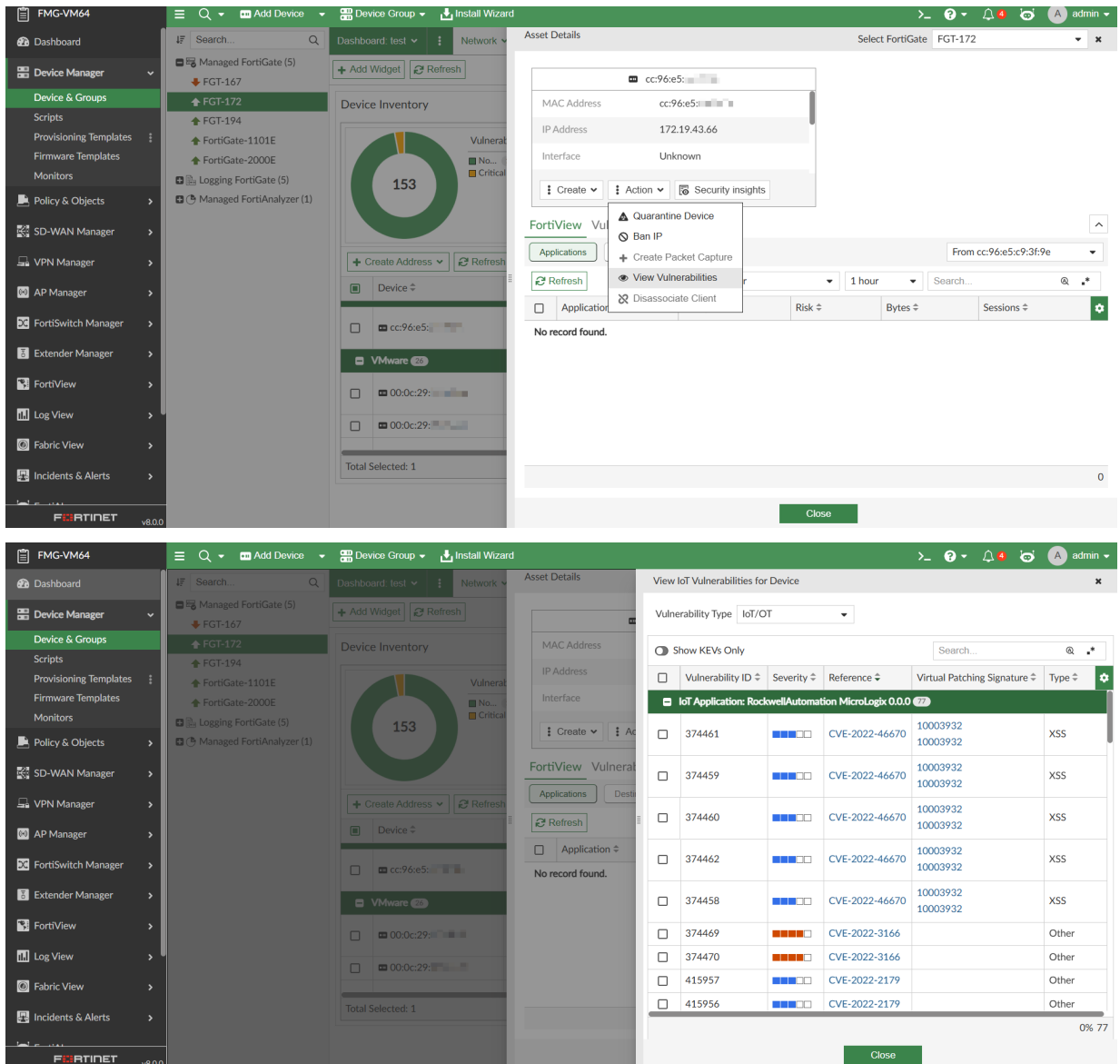
d. Ban IP addresses.



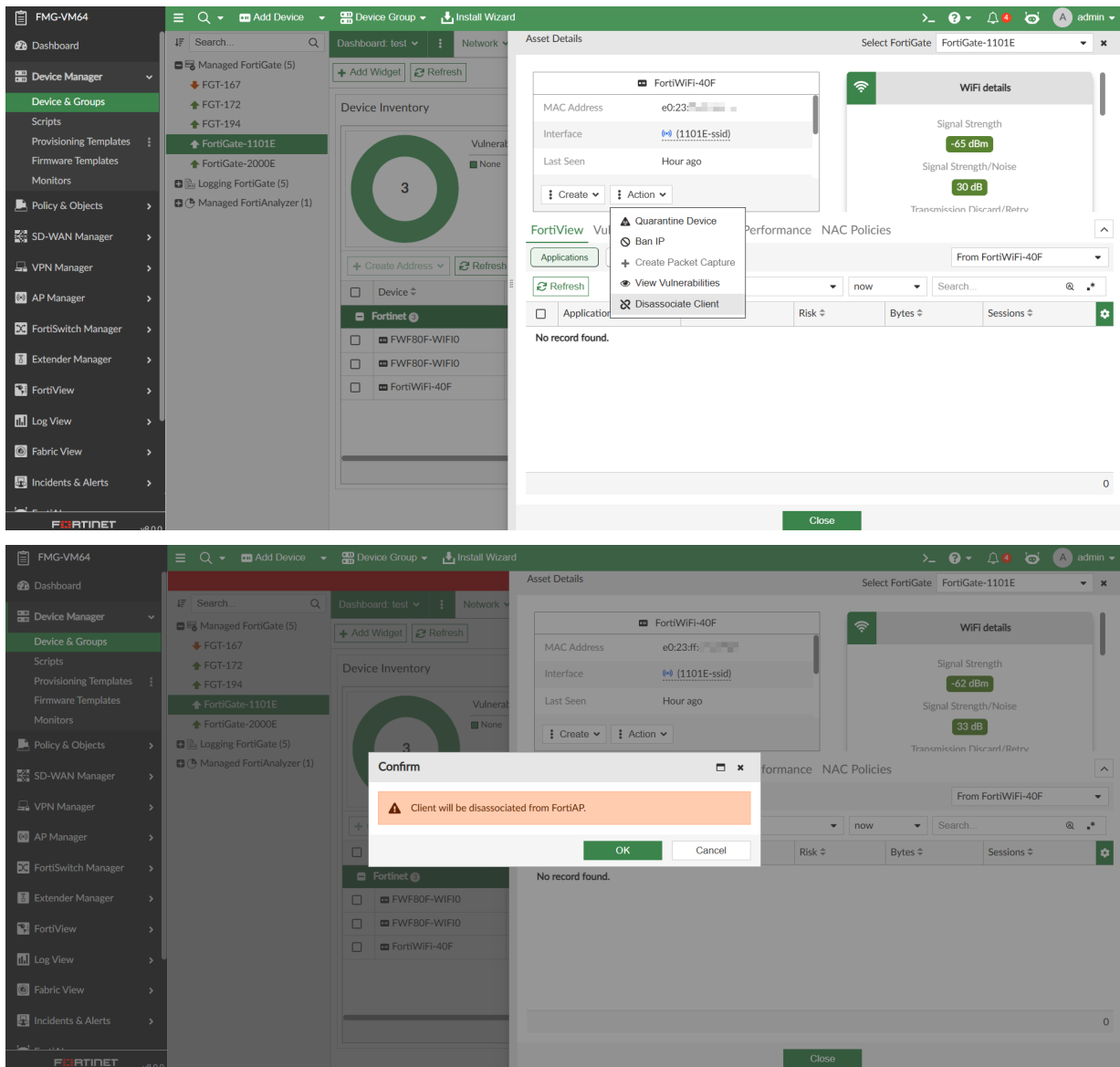
- e. Create packet capture. This feature requires that the device is connected to a FortiSwitch.



- f. View vulnerabilities detected by *FortiClient* or *IoT/OT*. This feature requires that the device is connected to FortiClient EMS.

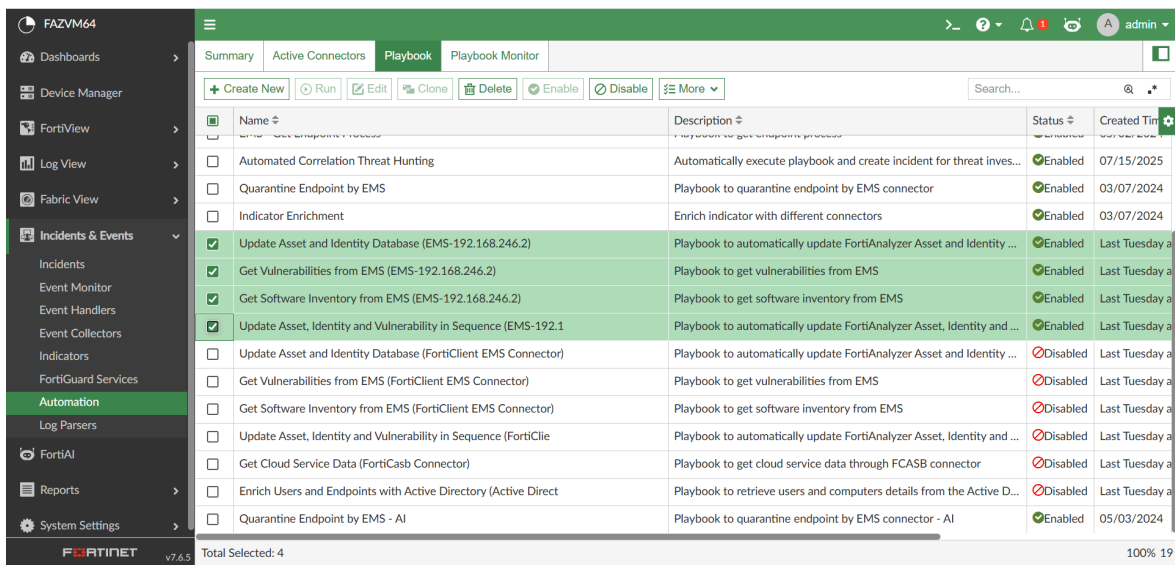
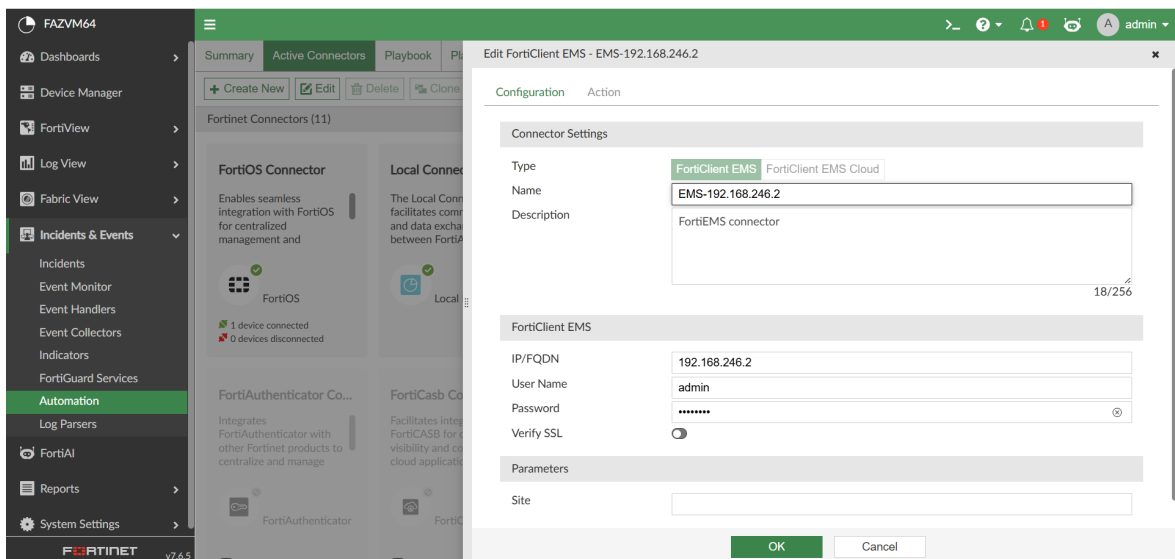


- g. Disassociate clients. This feature requires that the device is connected to a FortiAP.

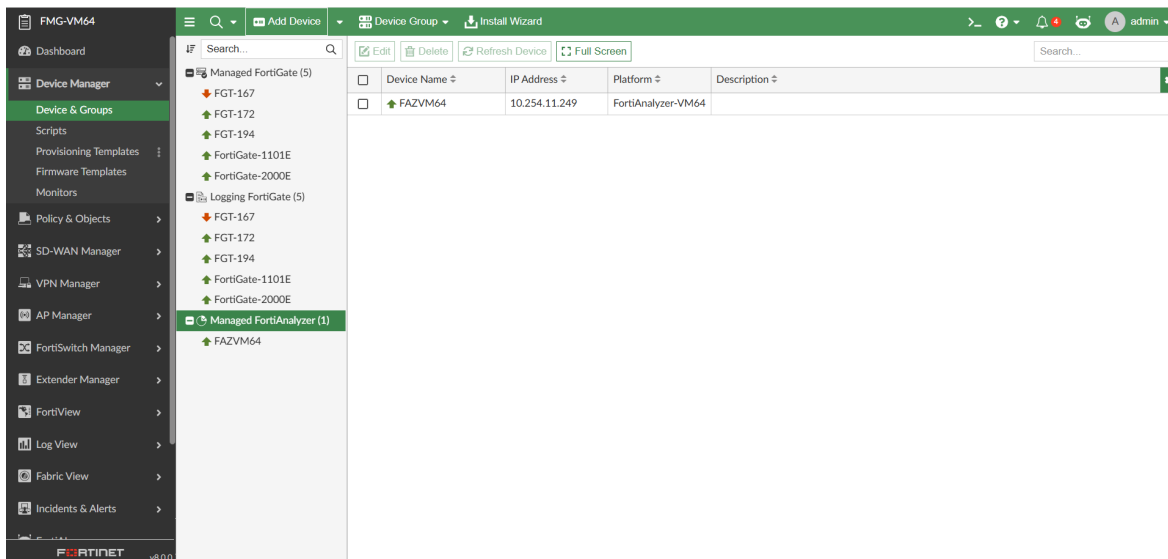


- h. View the risk score. This feature requires that the device is connected to FortiClient and FortiClient EMS. To enable security insights and risk scores:

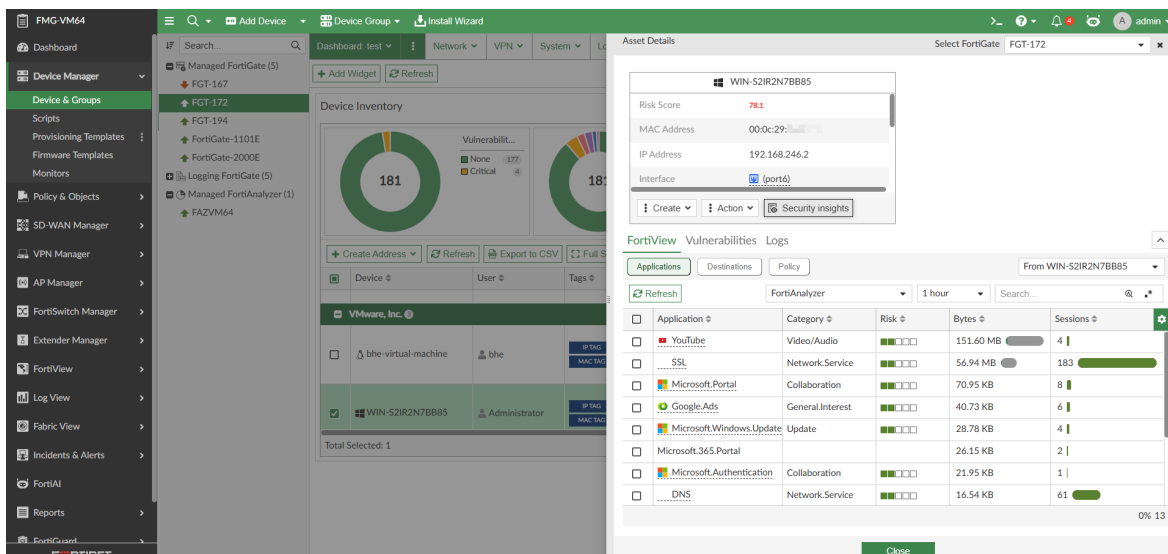
i. On FortiAnalyzer, add FortiClient EMS and enable the FortiClient EMS playbooks.

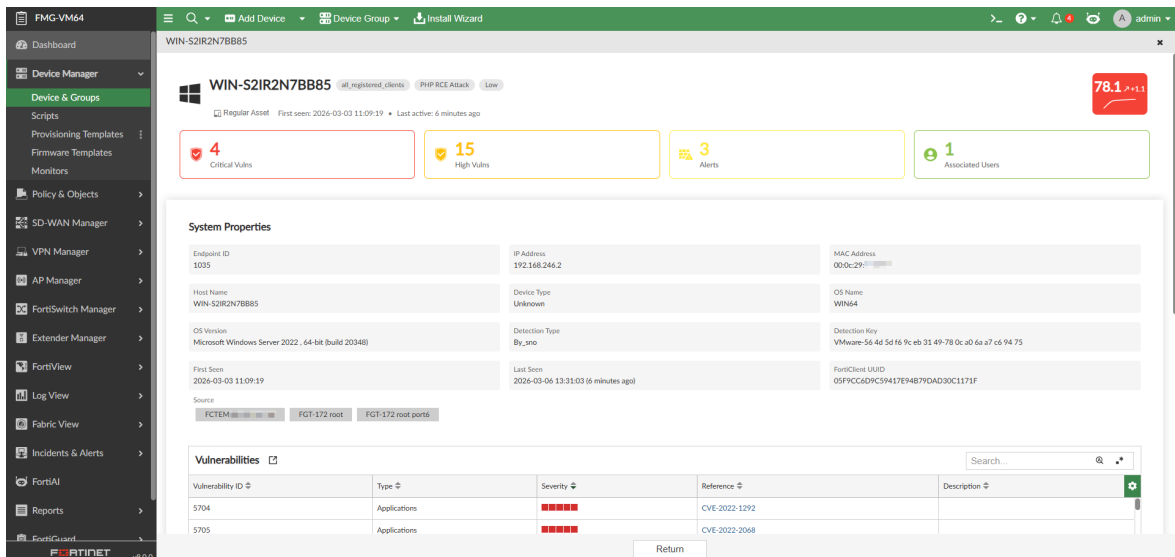


ii. On FortiManager, add the FortiGate and FortiAnalyzer.

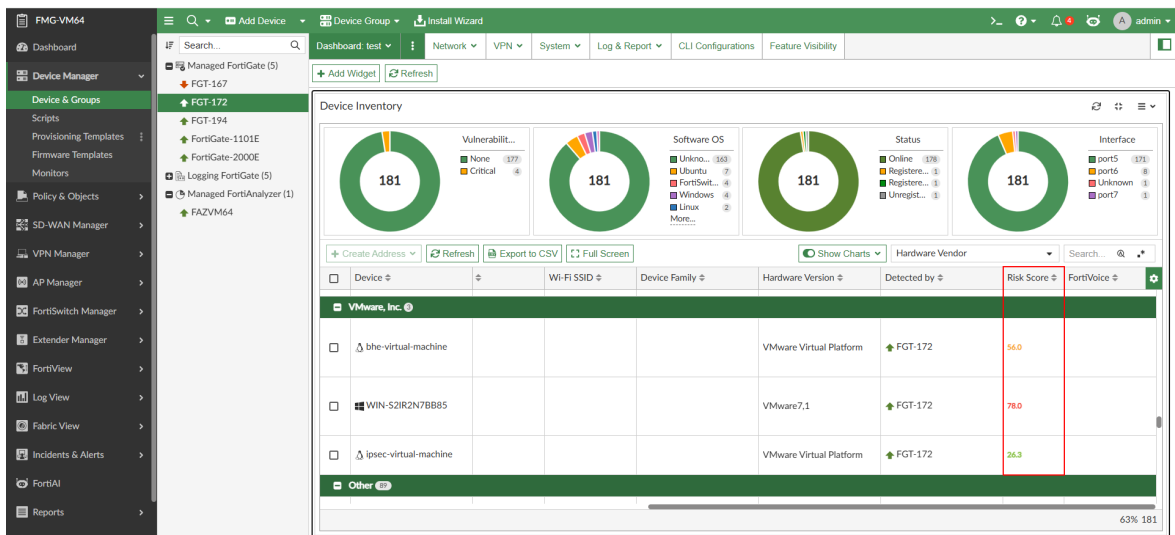


- iii. Go to the *Asset Details* menu for a device and select *Security Insights* to view security information including the risk score, detected vulnerabilities, and system properties.





iv. Go to the *Device Manager* and view a device's configuration. The *Risk Score* is displayed for devices in the *Device Inventory* widget.



Administrators can create protected objects



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

- Protected object permissions

FortiManager administrator can create protected objects (Policy Packages, firewall policies and objects) to prevent regular administrators to modify or delete them.

- Enabling protected object permissions on page 62
- Marking policies and objects as protected on page 62
- Users without protected object permissions on page 64

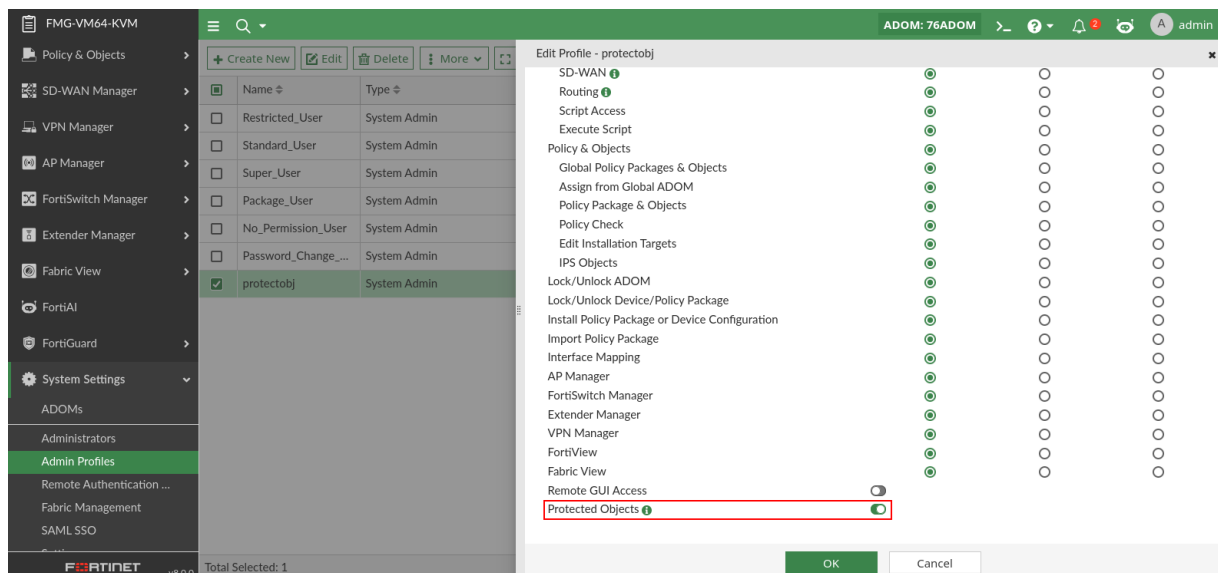
Enabling protected object permissions

To enable protected objects permissions:

1. In the FortiManager CLI, enable protected object permission visibility:

```
config system global
    set gui-object-protect enable
end
```

2. Go to *Systems settings > Admin Profile* and create or edit an admin profile.
3. Enable the *Protected Objects* option.



4. Assign the admin profile to an administrator

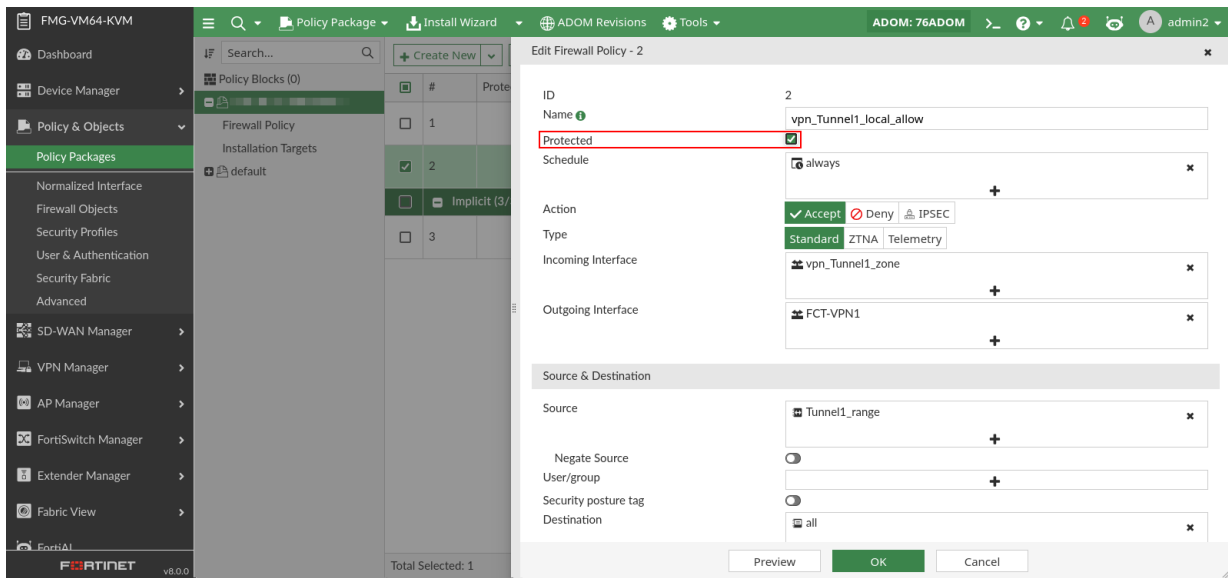
To configure an administrator profile with protected object permissions in the CLI:

```
config system admin profile
    edit <profile name>
        ....
        set protected-objects <enable/disable>
    end
```

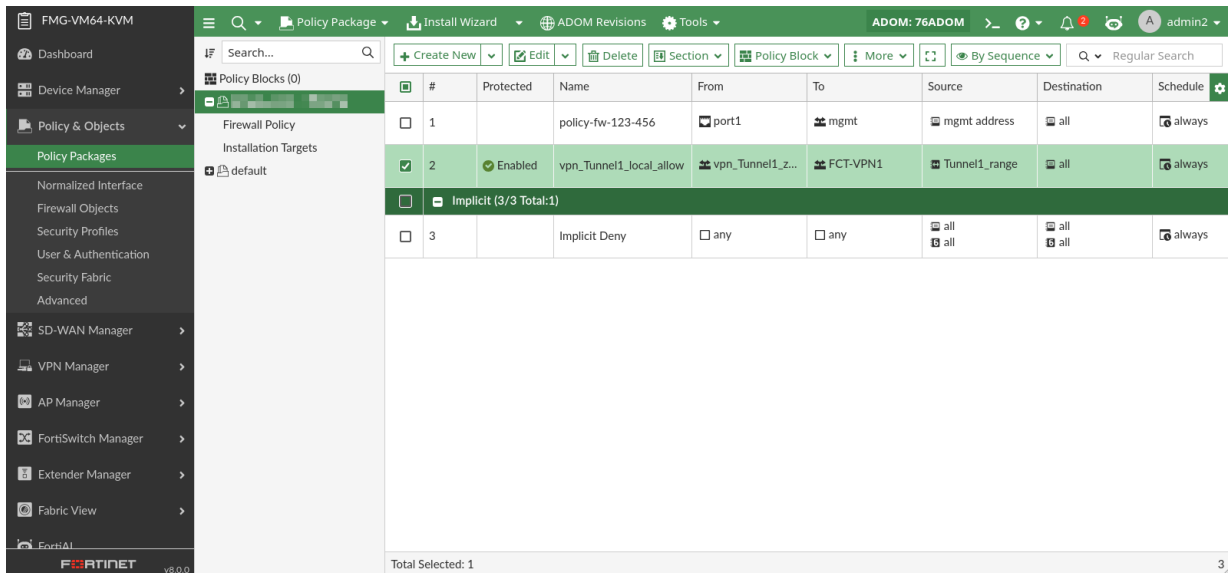
Marking policies and objects as protected

To mark policies and objects as protected:

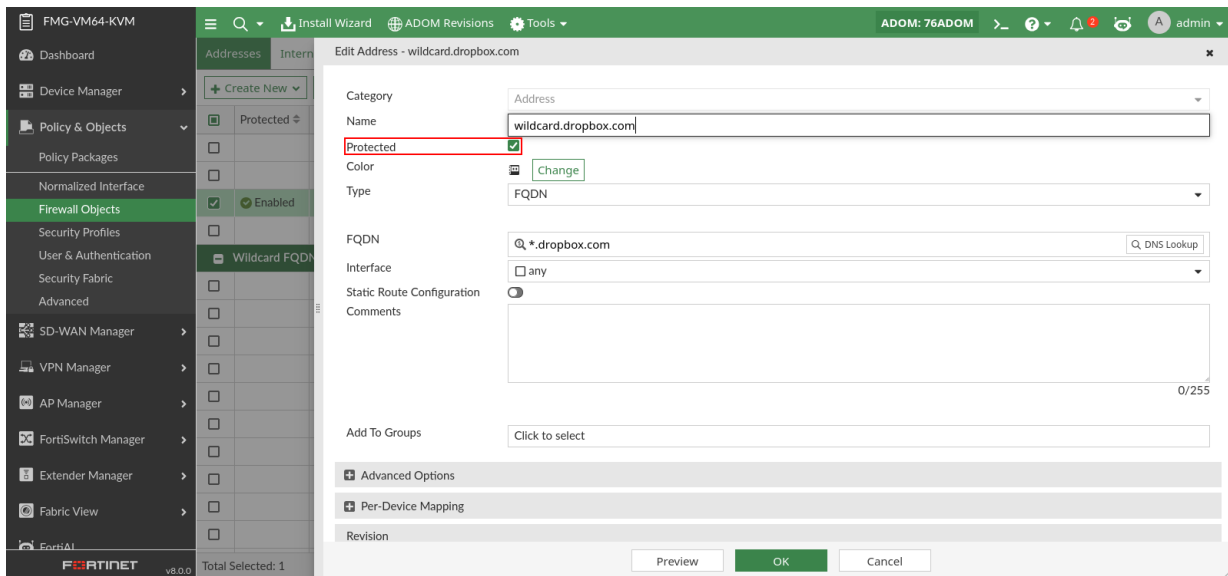
1. Log in as the administrator and go to *Policy & Objects > Policy Package*.
2. Edit an existing policy, and enable the *Protected* option, then save the policy.



You can see that the object has the *Enabled* status in the *Protected* column in the policy table.



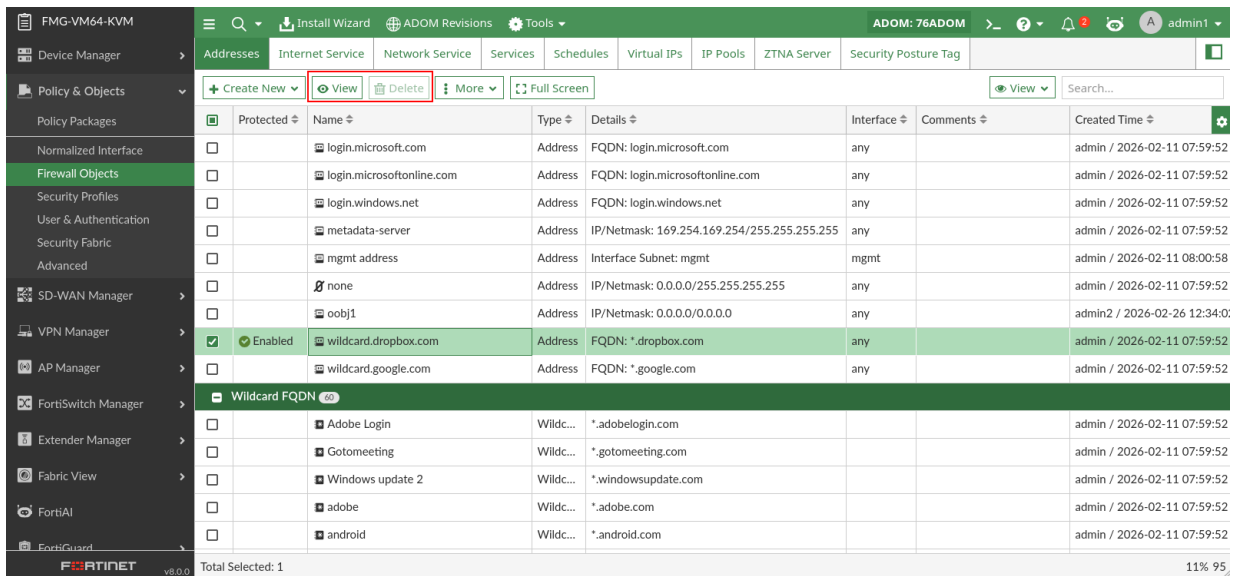
- Go to *Policy & Objects*, and add the protected object for the policy objects.



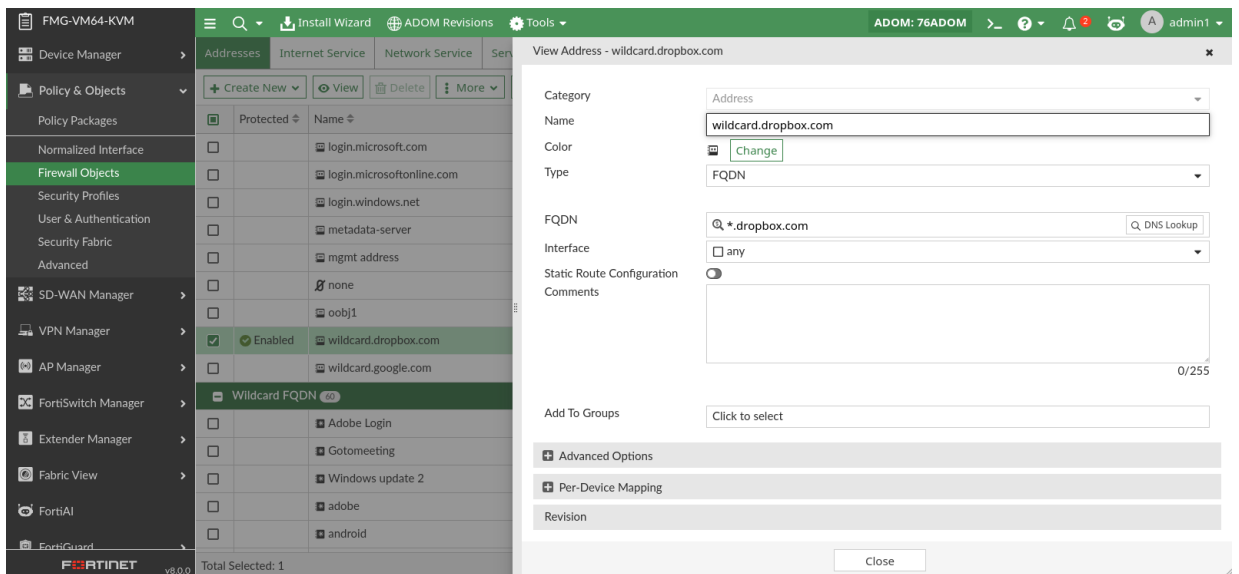
Protected	Name	Type	Details	Interface	Comments	Created Time	Last Modified
<input type="checkbox"/>	none	Address	IP/Netmask: 0.0.0.0/255.255.255.255	any		admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	oobj1	Address	IP/Netmask: 0.0.0.0/0.0.0.0	any		admin2 / 2026-02-26 12:34:02 PST	admin/202
<input checked="" type="checkbox"/>	wildcard.dropbox.com	Address	FQDN: *.dropbox.com	any		admin / 2026-02-11 07:59:52 PST	admin/202
<input type="checkbox"/>	wildcard.google.com	Address	FQDN: *.google.com	any		admin / 2026-02-11 07:59:52 PST	
Wildcard FQDN (40)							
<input type="checkbox"/>	Adobe Login	Wildcard FQDN	*.adobe.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	Gotomeeting	Wildcard FQDN	*.gotomeeting.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	Windows update 2	Wildcard FQDN	*.windowsupdate.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	adobe	Wildcard FQDN	*.adobe.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	android	Wildcard FQDN	*.android.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	apple	Wildcard FQDN	*.apple.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	appstore	Wildcard FQDN	*.appstore.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	auth.gfx.ms	Wildcard FQDN	*.auth.gfx.ms			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	autoupdate.opera.com	Wildcard FQDN	*autoupdate.opera.com			admin / 2026-02-11 07:59:52 PST	
<input type="checkbox"/>	cdn-apple	Wildcard FQDN	*.cdn-apple.com			admin / 2026-02-11 07:59:52 PST	

Users without protected object permissions

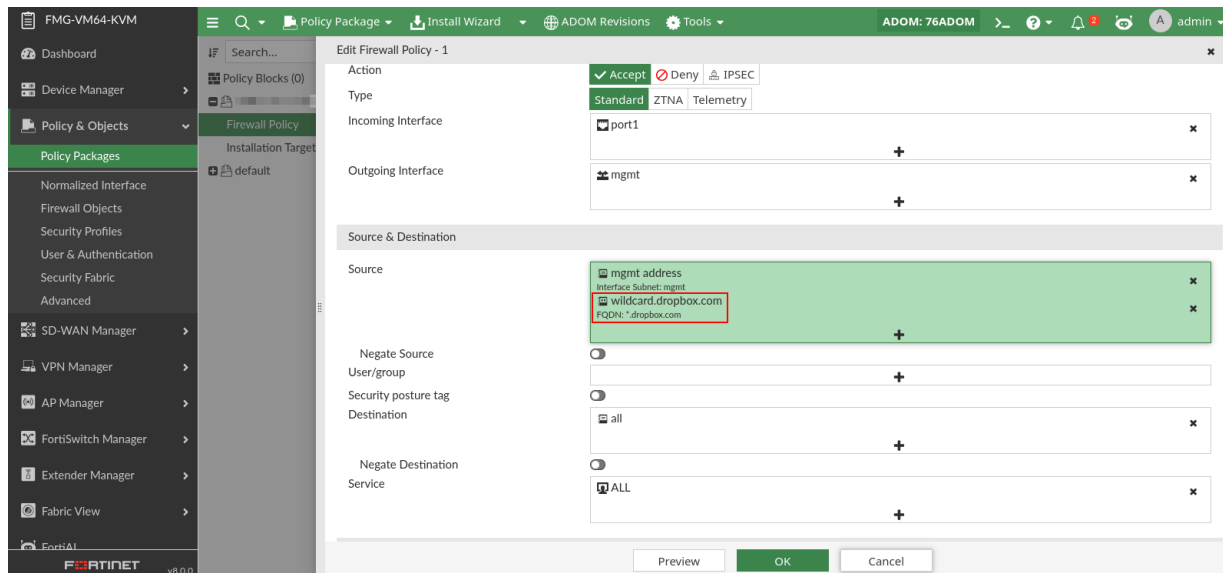
- When object protection mode is enabled, users without the *Protected Objects* permission will have read-only access to the protected objects.



- When viewing a protected object, the Protected Objects toggle is not available and you cannot edit or save the object.



- In policy packages, you can use protected objects inside the policy even without the *Protected Objects* permission.



FortiManager supports downgrade and roll-back for FortiGuard packages to allow setting a preferred package version for devices



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

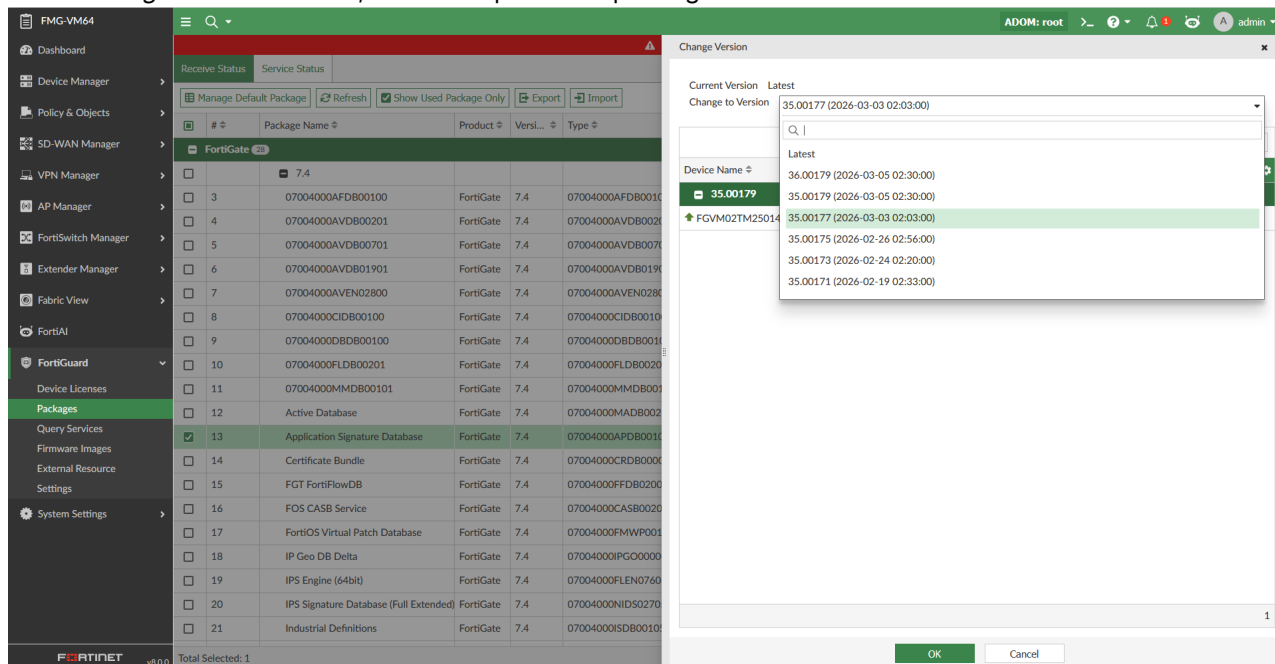
- [Choosing a preferred package version to deploy](#)

FortiManager supports downgrade and roll-back for FortiGuard packages to allow setting a preferred package version for devices.

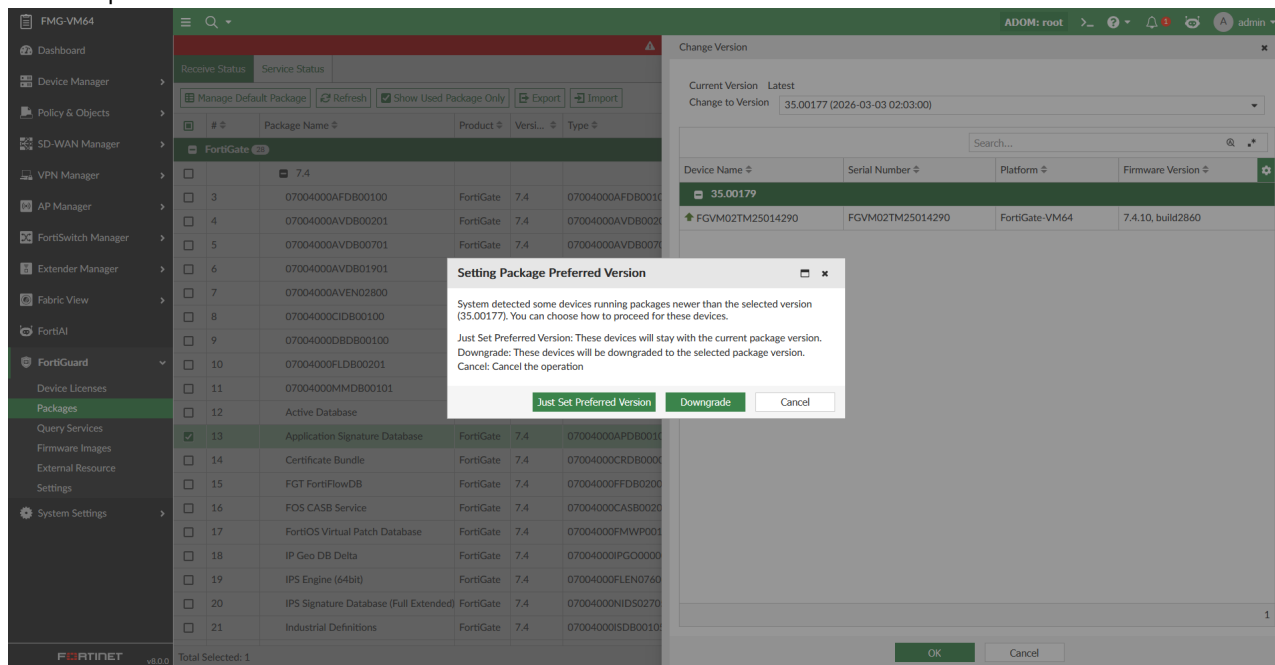
To set a preferred package version in FortiManager:

1. Go to *FortiGuard > Packages > Receive Status*.
In the *To Be Deployed Version* column, you can see the current package version selected for each package. The default is *Latest*.
2. Click *Change* to open the *Change Version* dialog.

3. In the *Change to Version* field, select the preferred package version and click OK.



4. A dialog will appear to confirm if you want to downgrade devices to the selected package version or just set it as the preferred version.



Select one of the following options:

- a. *Just Set Preferred Version*: Sets the selected version as the preferred version. Devices already on later versions of the package will not be downgraded to the preferred version, but they will not receive any packages released after the preferred package version.

#	Package Name	Product	Version	Type	Latest Version (Release Data/TL...)	To Be Deployed Version	Service Entitlement	Size	Update History
3	07004000AFDB00100	FortiGate	7.4	07004000AFDB00100	1.00019 (2025-12-09 19:06:00)	Latest		608B	
4	07004000AVDB00201	FortiGate	7.4	07004000AVDB00201	93.06759 (2026-03-06 22:32:00)	Latest		2.43 MB	
5	07004000AVDB00701	FortiGate	7.4	07004000AVDB00701	93.06759 (2026-03-06 22:31:00)	Latest		14.43 MB	
6	07004000AVDB01901	FortiGate	7.4	07004000AVDB01901	4.03868 (2026-03-06 22:45:00)	Latest		3.93 MB	
7	07004000AVEN02800	FortiGate	7.4	07004000AVEN02800	7.00030 (2024-07-02 17:11:00)	Latest		3.43 MB	
8	07004000CICDB00100	FortiGate	7.4	07004000CICDB00100	1.00199 (2026-02-20 17:33:00)	Latest		137.54 KB	
9	07004000DRDB00100	FortiGate	7.4	07004000DRDB00100	3.01541 (2026-03-06 19:34:00)	Latest		641.94 KB	
10	07004000FLDB00201	FortiGate	7.4	07004000FLDB00201	93.06759 (2026-03-06 22:46:00)	Latest		17.35 MB	
11	07004000MADB00101	FortiGate	7.4	07004000MADB00101	93.06759 (2026-03-06 22:35:00)	Latest		2.06 MB	
12	Active Database	FortiGate	7.4	07004000MADB00200	1.00313 (2026-03-03 22:00:00)	Latest	MAC Address DB	533.48 KB	
13	Application Signature Database	FortiGate	7.4	07004000APDB00105	36.00177 (2026-03-05 02:30:00)	35.00177	FortiCare	355.58 KB	
14	Certificate Bundle	FortiGate	7.4	07004000CRDB00000	1.00062 (2026-01-09 21:59:00)	Latest	Certificate Bundle Database	156.89 KB	
15	FGT FortiFlowDB	FortiGate	7.4	07004000FFDB02008	7.04413 (2026-03-06 19:58:00)	Latest	Internet Service DB	8.48 MB	
16	FOS CASB Service	FortiGate	7.4	07004000CASB00201	1.00009 (2025-07-30 17:58:00)	Latest	Firmware and General Updates	87.95 KB	
17	FortiOS Virtual Patch Database	FortiGate	7.4	07004000FMVP00105	26.00031 (2026-03-05 01:42:00)	Latest	FortiCare	8.75 KB	
18	IP Geo DB Delta	FortiGate	7.4	07004000IPGO00000	3.00322 (2026-03-04 23:39:00)	Latest	Firmware and General Updates	4.32 MB	
19	IPS Engine (64bit)	FortiGate	7.4	07004000FLEN07600	7.00600 (2026-02-24 23:14:00)	Latest	IPS	5.74 MB	
20	IPS Signature Database (Full Extended)	FortiGate	7.4	07004000NIS02705	36.00179 (2026-03-05 02:33:00)	Latest	IPS	1.73 MB	
21	Industrial Definitions	FortiGate	7.4	07004000ISDB00105	36.00179 (2026-03-05 02:30:00)	Latest	Industrial Security	200.15 KB	

- b. **Downgrade:** Immediately downgrades FortiGate devices on later package versions to the selected preferred package version. The selected version is also set as the preferred version.

Downgrade Package

100%

Success: 1 | Warning: 0 | Error: 0

View Progress Report

#	Name	Time Used	Status
1	FGVM02TM25014290	4s	Push object 07004000APDB00105(35.177) SUCCESS(r=0)

Finish

- c. **Cancel:** Cancel the change.

FortiManager supports importing password-type objects from FortiGate devices with private data encryption

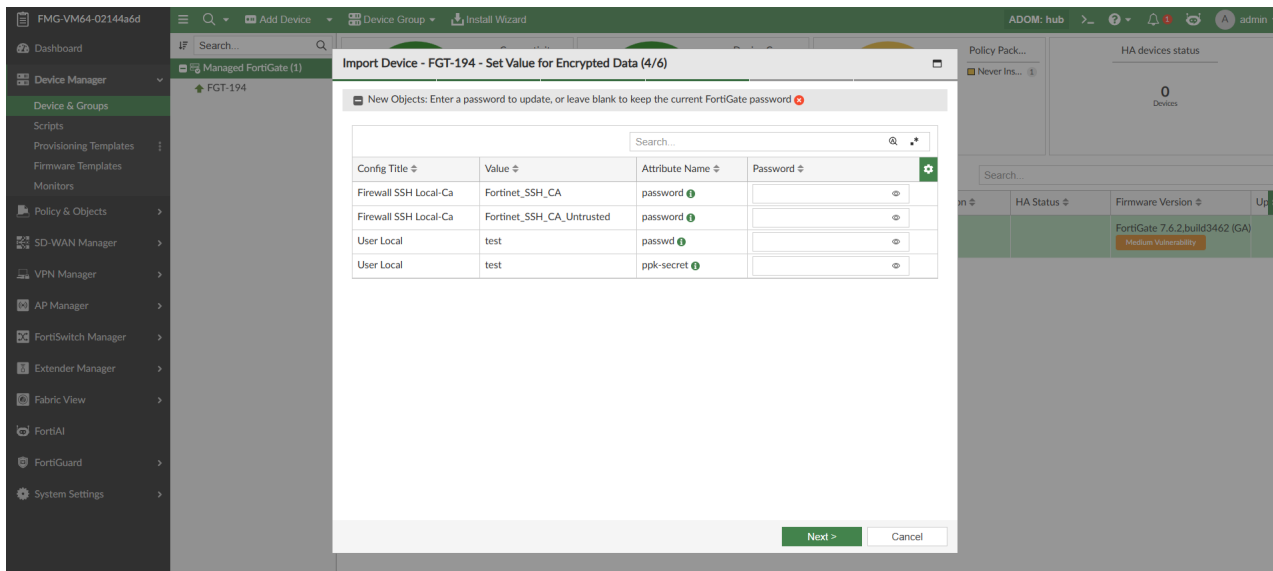


This information is also available in the FortiManager 8.0 Administration Guide:

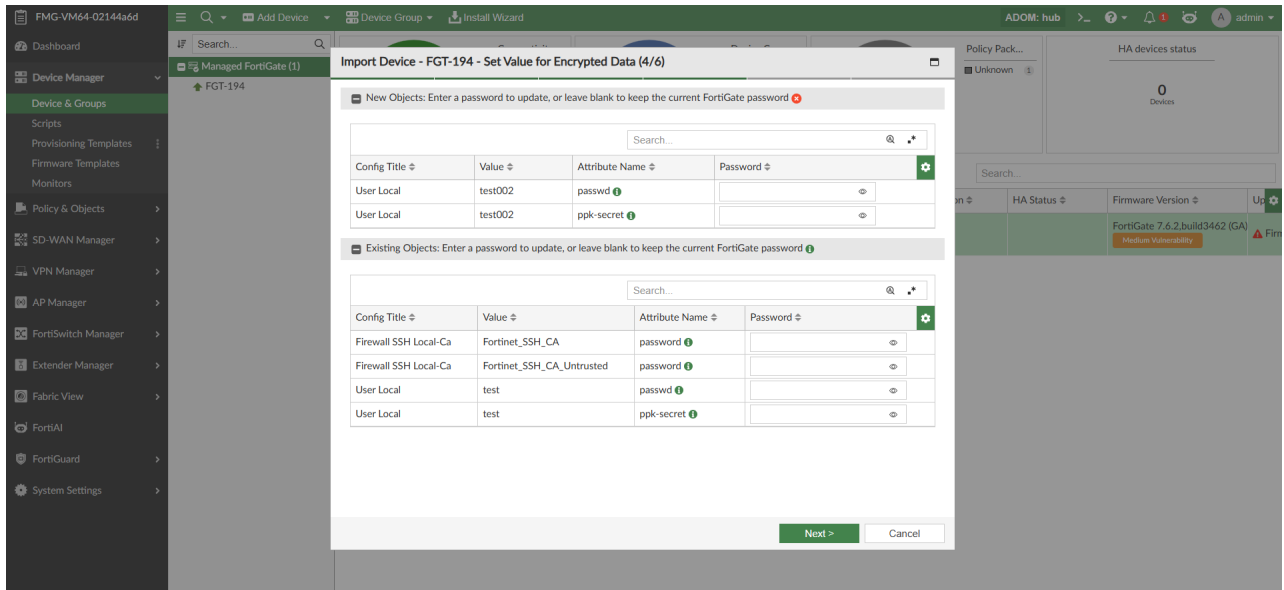
- [Managing FortiGates with private data encryption](#)

Starting in FortiManager 8.0.0, FortiManager can import objects which include password-type attributes from managed FortiGate devices with private data encryption (PDE) enabled.

- When importing new objects with password-type attributes, the *Import Wizard* will prompt the administrator to provide the password for each object as part of the import process.



- When importing objects with password-type attributes that already exist in the ADOM, the Import Wizard will show the existing objects and prompt the user to enter a new password or leave the field blank to keep the current FortiGate password.



Policy and Objects

This section lists the new features added to FortiManager for policy and objects:

- [Policy on page 71](#)

Policy

This section lists the new features added to FortiManager for policies:

- [Local In policies are supported in the Global ADOM and in policy blocks on page 71](#)

Local In policies are supported in the Global ADOM and in policy blocks



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

- [Create a local-in policy](#)

Local In policies are supported in the Global ADOM and in global and local policy blocks, allowing you to apply these policies across multiple policy packages. In previous versions, Local In policies were limited to local ADOM policy packages. This enhancement improves scalability and eliminates repetitive configurations.

This topic contains the following:

- [Managing Local In policies in Global ADOMs on page 72](#)
 - [Creating Local In policies in the Global Database ADOM on page 72](#)
 - [Creating Local In policies in Global policy blocks: on page 73](#)
 - [Assigning Global Local In policies to ADOMs on page 75](#)
 - [Viewing Global Local In policies from the local policy package on page 77](#)
- [Creating Local In policies in local policy blocks on page 78](#)



Local In policies must be selected in *Feature Visibility* before they can be created.

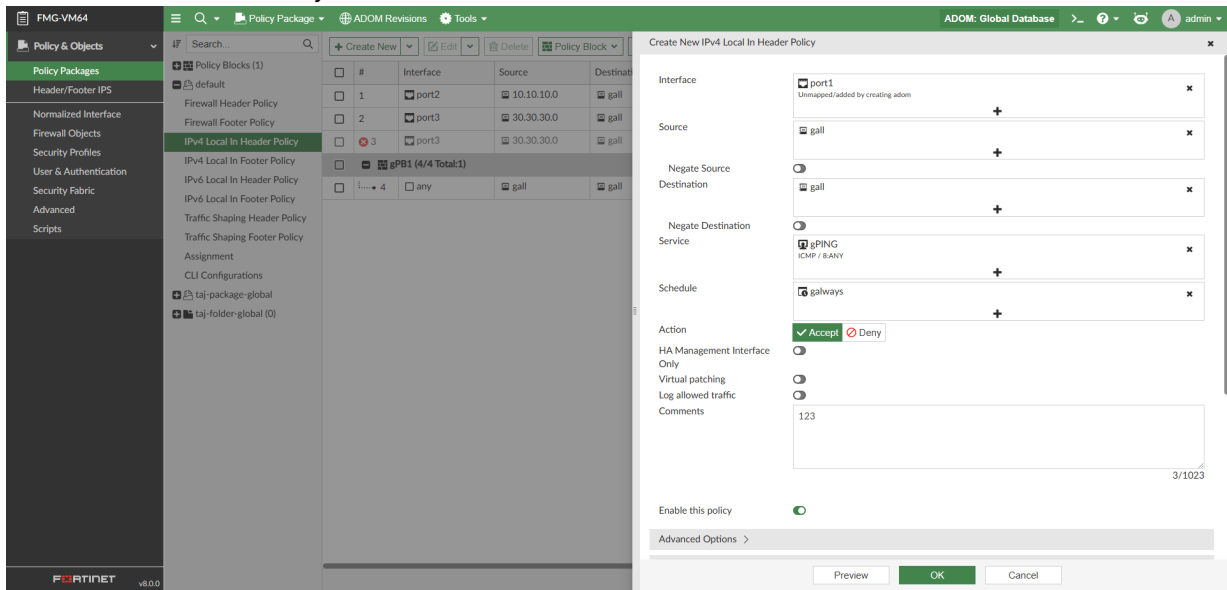
Click *Tools > Feature Visibility* from the *Policy & Objects* toolbar to configure feature visibility.

Managing Local In policies in Global ADOMs

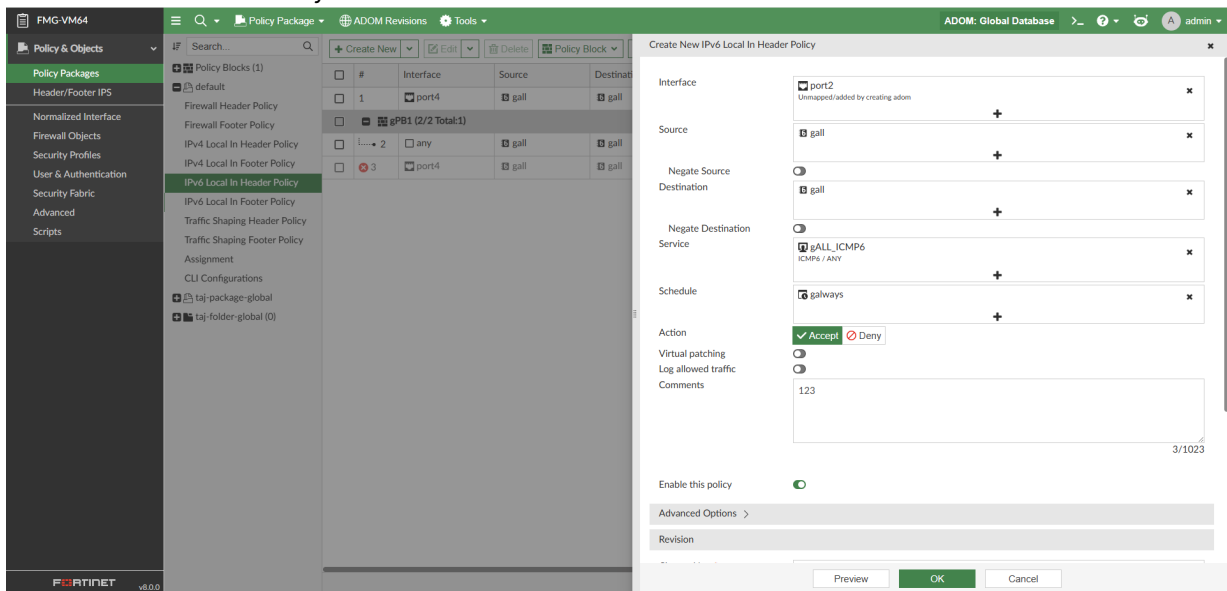
Creating Local In policies in the Global Database ADOM

To create Local In policies in the Global Database ADOM:

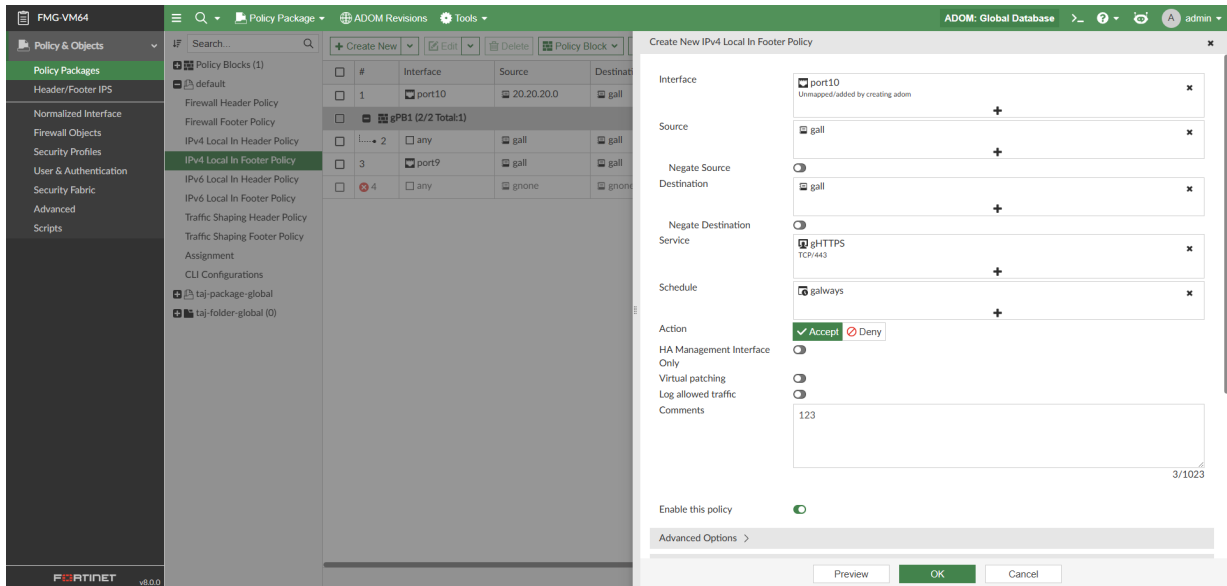
1. Enter the Global Database ADOM.
2. Select a Global policy package from the policy package list (for example, "default").
3. Select the following supported Local In policy types and click *Create New* to create new Local In policies:
 - IPv4 Local In Header Policy



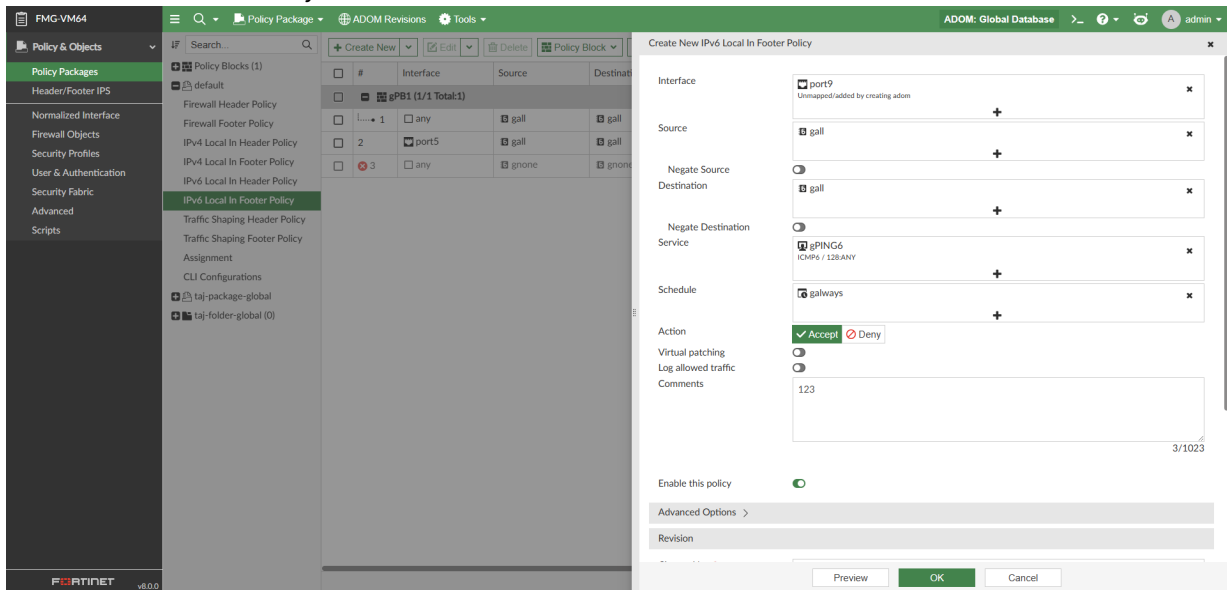
- IPv6 Local In Header Policy



- IPv4 Local In Footer Policy



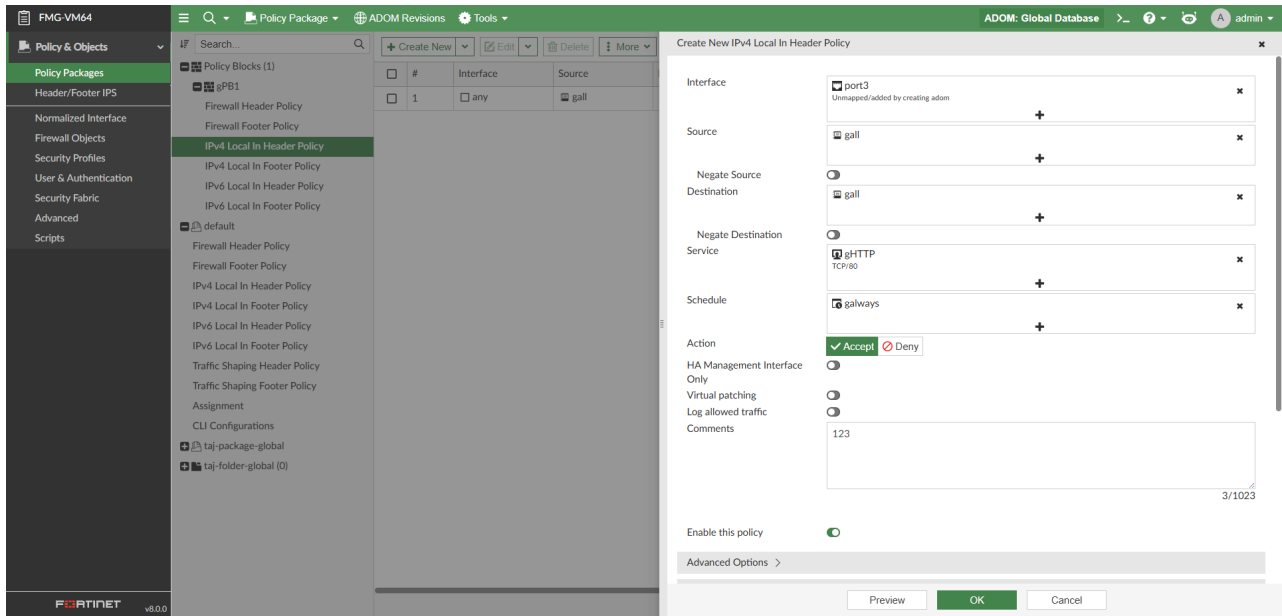
• IPv6 Local In Footer Policy



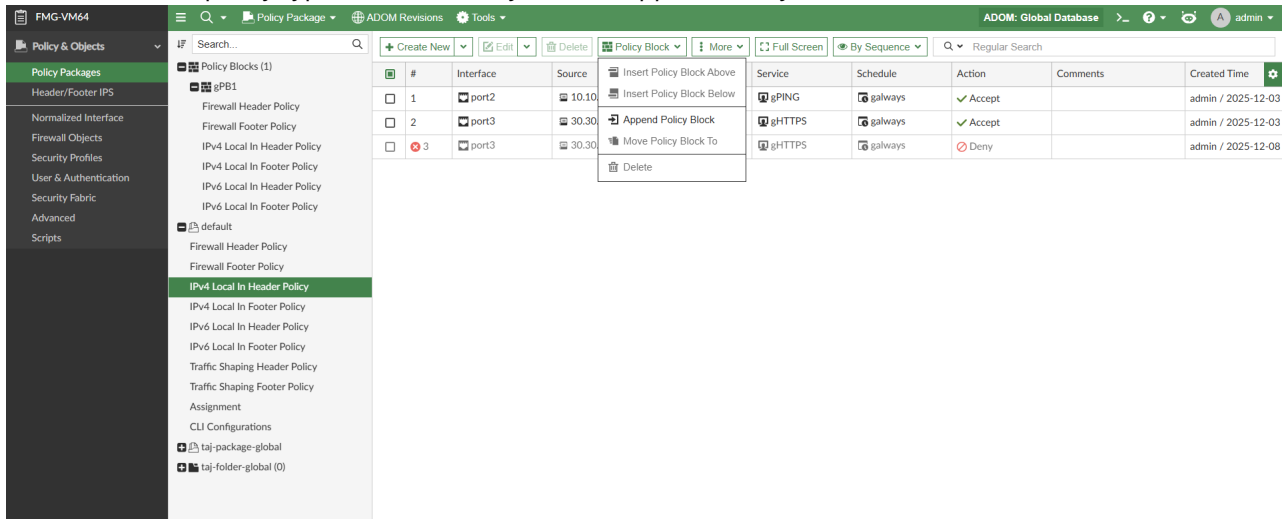
Creating Local In policies in Global policy blocks:

To create Local In policies in Global policy blocks:

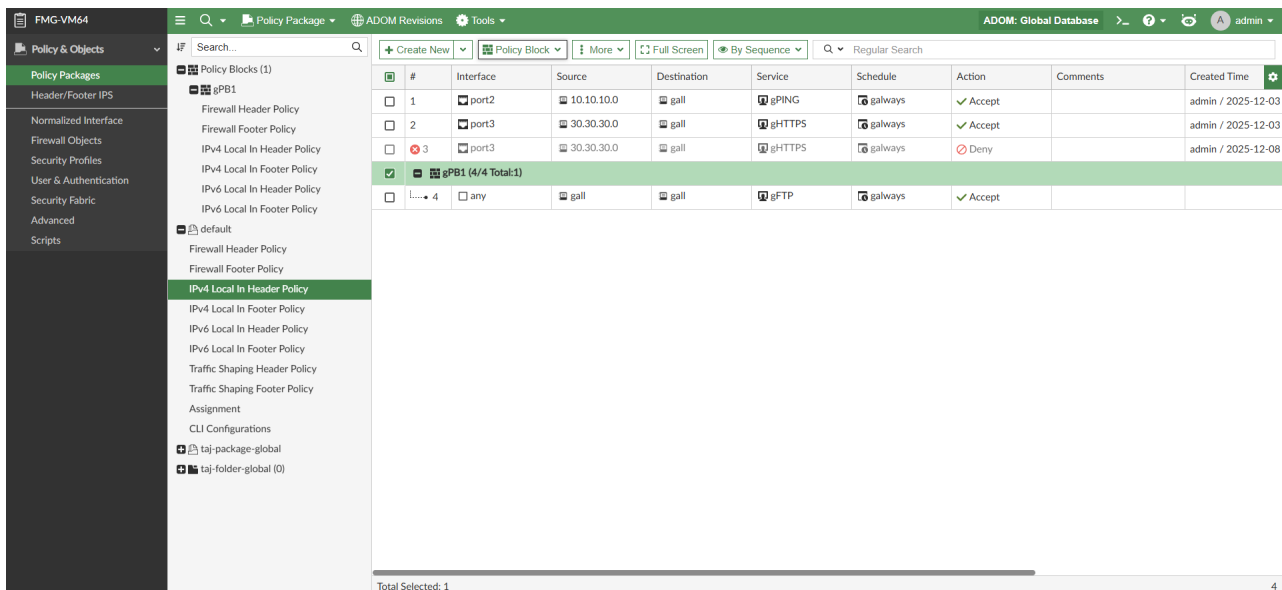
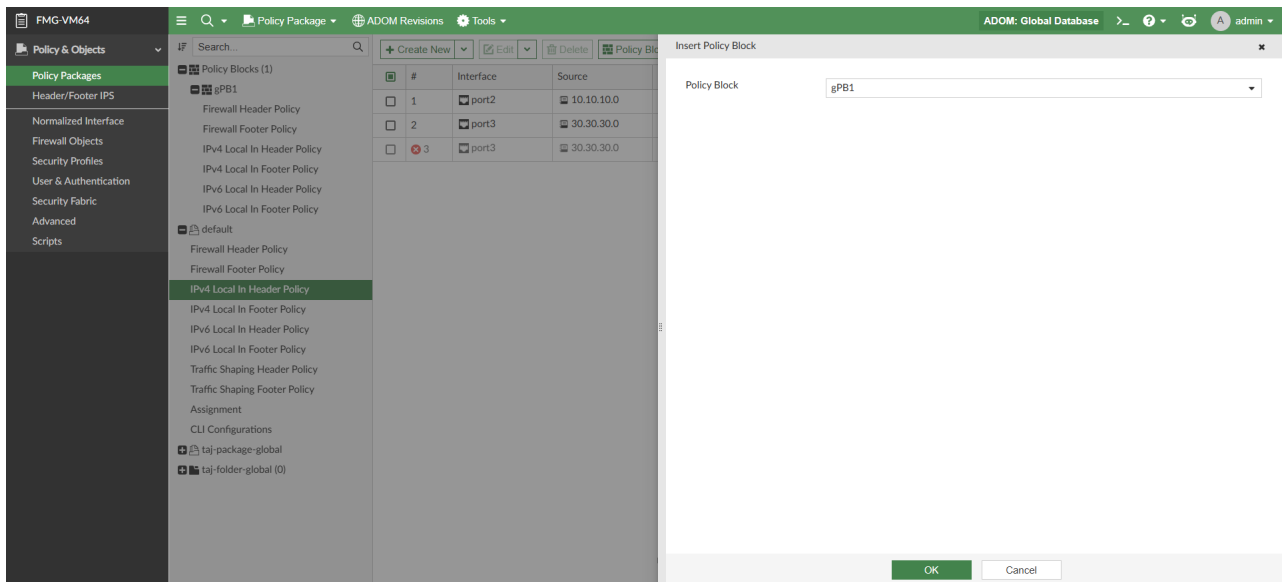
1. Enter the Global Database ADOM.
2. Select *Policy Blocks* in the policy package list and click *Create New* to create a new policy block.
3. Create the desired IPv4 and IPv6 Header and Footer policies in the policy block.



4. Select a Global policy package from the policy packages list (for example, "default") .
5. Select a Local In policy type and click *Policy Block > Append Policy Block* from the toolbar.



6. Select the configured policy block from the dropdown menu, and click *OK* to append it to the policy package.



7. Repeat steps 5-6 for the remaining policy types as needed.

Assigning Global Local In policies to ADOMs

To assign Global Local In policies to ADOMs:

1. Enter the Global Database ADOM.
2. Select the Global policy package which contains the Local In policies (for example, "default").
3. Select *Action* > *Assign* from the toolbar, and configure the assignment options.

Policy and Objects

The screenshot shows the FortiManager interface with the 'Policy & Objects' menu open. The 'Assign' dropdown menu is visible, showing options for 'Assign' and 'Unassign'. The main table lists ADOM objects and their status:

ADOM	Device	Policy Package	Status
ADOM-72	FortiGate 7.4	All Policy Package	Pending changes
ADOM-74	FortiGate 7.4	All Policy Package	Pending changes
ADOM-76	FortiGate 7.6	All Policy Package	Pending changes
ADOM-80	FortiGate 8.0	All Policy Package	Pending changes
ADOM_74to76	FortiGate 7.6	All Policy Package	Pending changes
root	FortiGate 8.0	All Policy Package	Pending changes

The screenshot shows the 'Assign Global Policy Package - default' dialog box. The dialog has the following options:

- Assign USED Objects Only
- Assign ALL Objects
- Automatically Install Policies to ADOM Devices
- Leave Meta Variable As-Is

Buttons at the bottom: Start to Assign, Cancel.

The screenshot shows the 'Assign Global Policy Package - default' progress report dialog box. The progress bar is at 100%. The report shows the following details:

#	Name	Time Used	Status
1	ADOM-74[assign]	2s	Assigning global policy package default to adom ADOM-74 ...
2	ADOM-76[assign]	5s	Assigning global policy package default to adom ADOM-76 ...
3	ADOM-80[assign]	5s	Assigning global policy package default to adom ADOM-80 ...

Buttons at the bottom: Finish.

Viewing Global Local In policies from the local policy package

To view Global Local In policies from the local policy package:

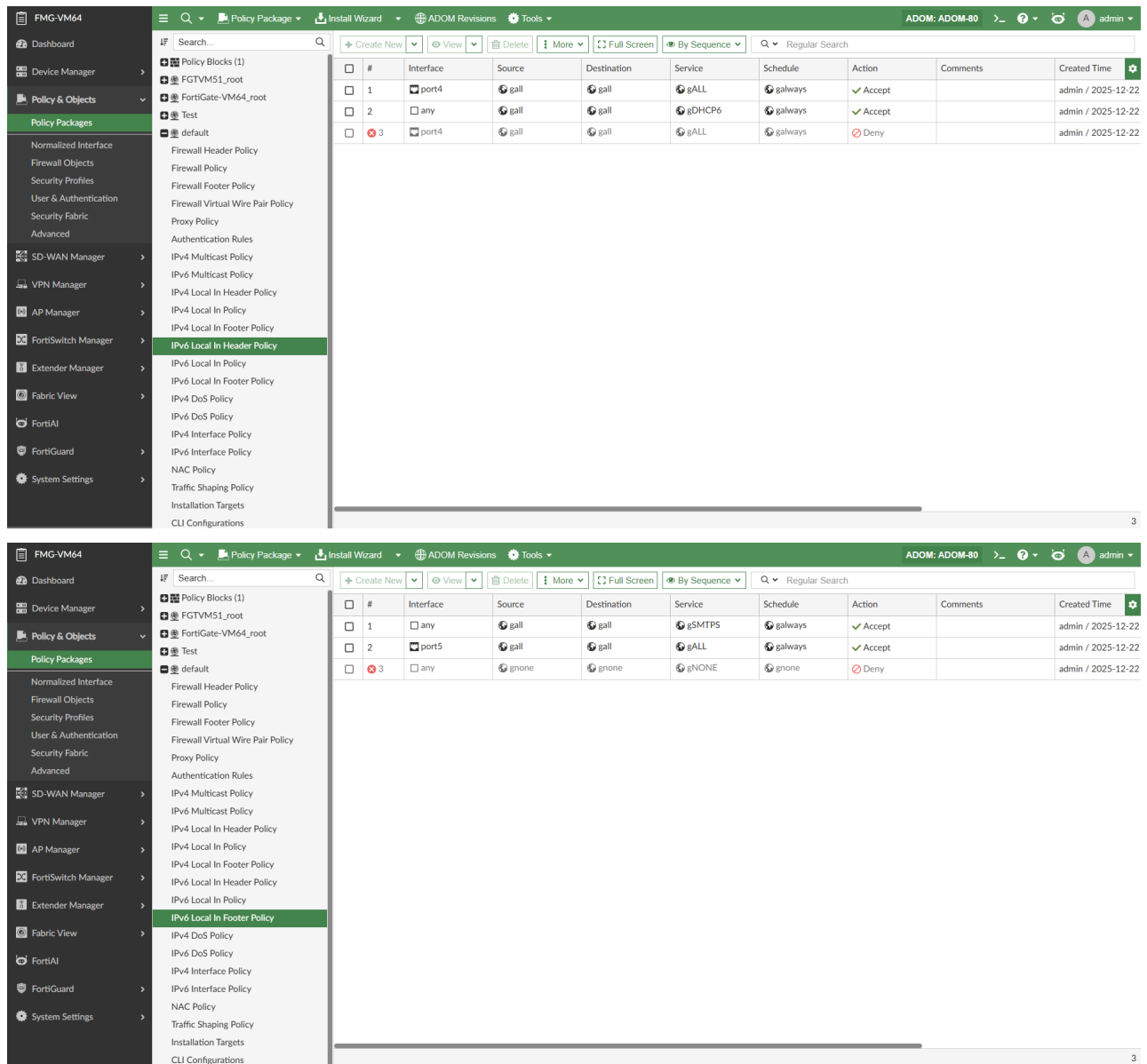
1. Enter the local ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a local policy package (for example, "default").
Policy packages include the global flag icon which indicates that Global policies are assigned to them.
4. View the Global Local In policies in *IPv4 Local In Header Policy*, *IPv4 Local In Footer Policy*, *IPv6 Local In Header Policy*, and *IPv6 Local In Footer Policy*.

The screenshot shows the FortiManager interface for the 'default' policy package. The left sidebar lists various policy types, with 'IPv4 Local In Header Policy' selected. The main area displays a table of policies:

#	Interface	Source	Destination	Service	Schedule	Action	Comments	Created Time
1	port2	10.10.10.0	gall	gPING	galways	✓ Accept		admin / 2025-12-22
2	port3	30.30.30.0	gall	gHTTPS	galways	✓ Accept		admin / 2025-12-22
3	port3	30.30.30.0	gall	gHTTPS	galways	✗ Deny		admin / 2025-12-22
4	any	gall	gall	gFTP	galways	✓ Accept		admin / 2025-12-22

The screenshot shows the FortiManager interface for the 'default' policy package. The left sidebar lists various policy types, with 'IPv4 Local In Footer Policy' selected. The main area displays a table of policies:

#	Interface	Source	Destination	Service	Schedule	Action	Comments	Created Time
1	port10	20.20.20.0	gall	gALL_UDP	galways	✓ Accept		admin / 2025-12-22
2	any	gall	gall	gIMAPS	galways	✓ Accept		admin / 2025-12-22

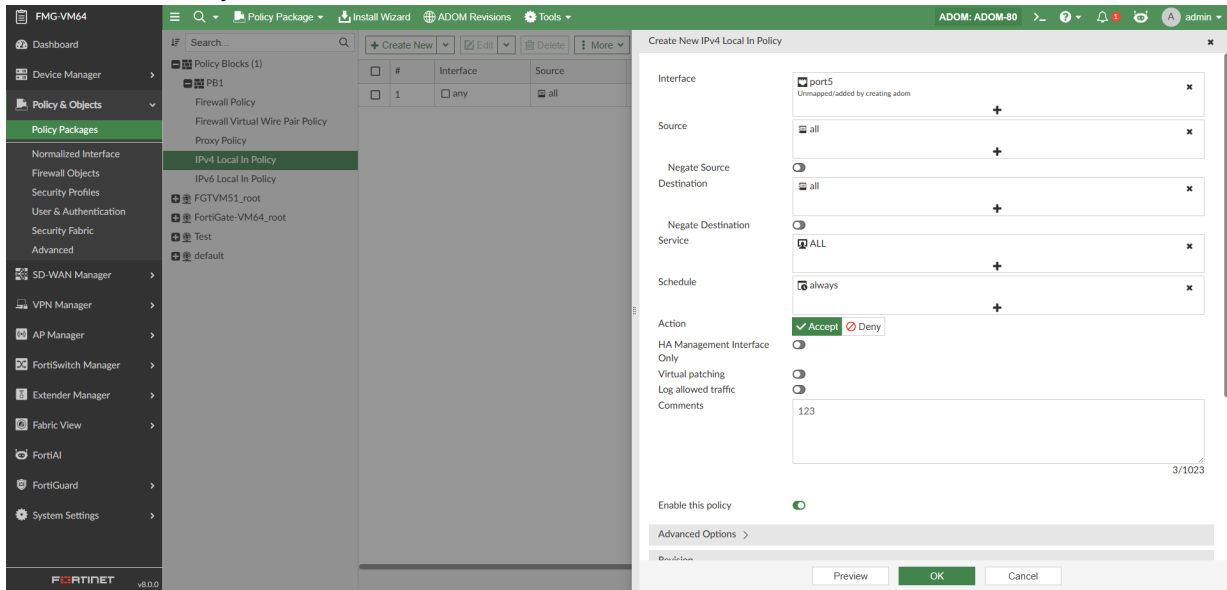


Creating Local In policies in local policy blocks

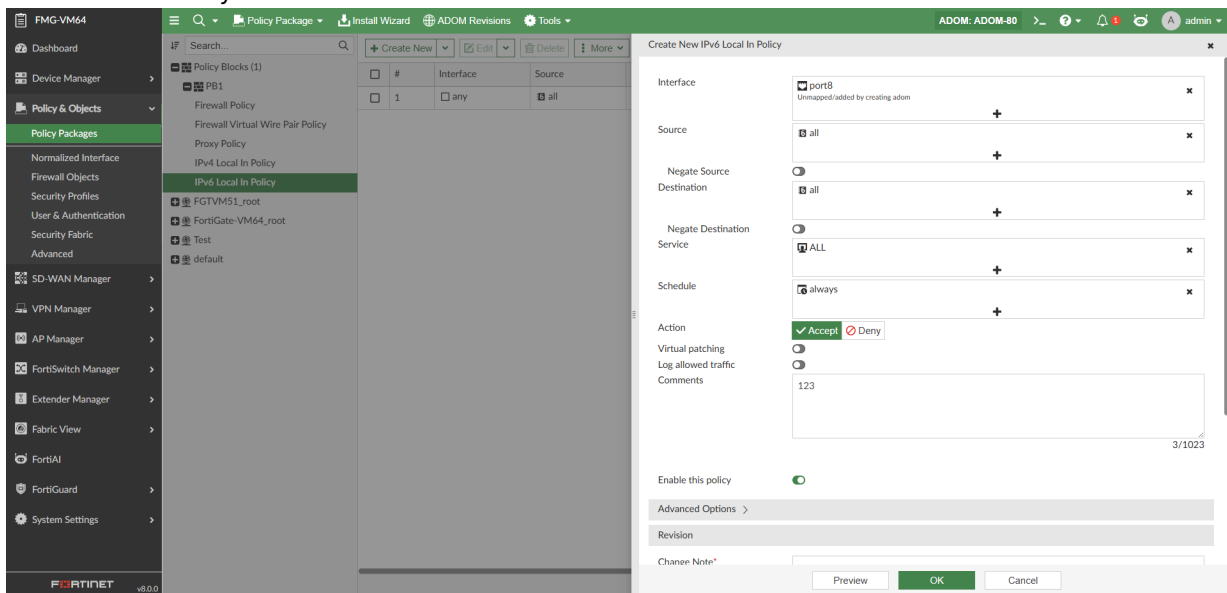
To create Local In Policy in Policy Block:

1. Enter the local ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select *Policy Block* from the policy packages list, and create new IPv4 and IPv6 Local In policies.

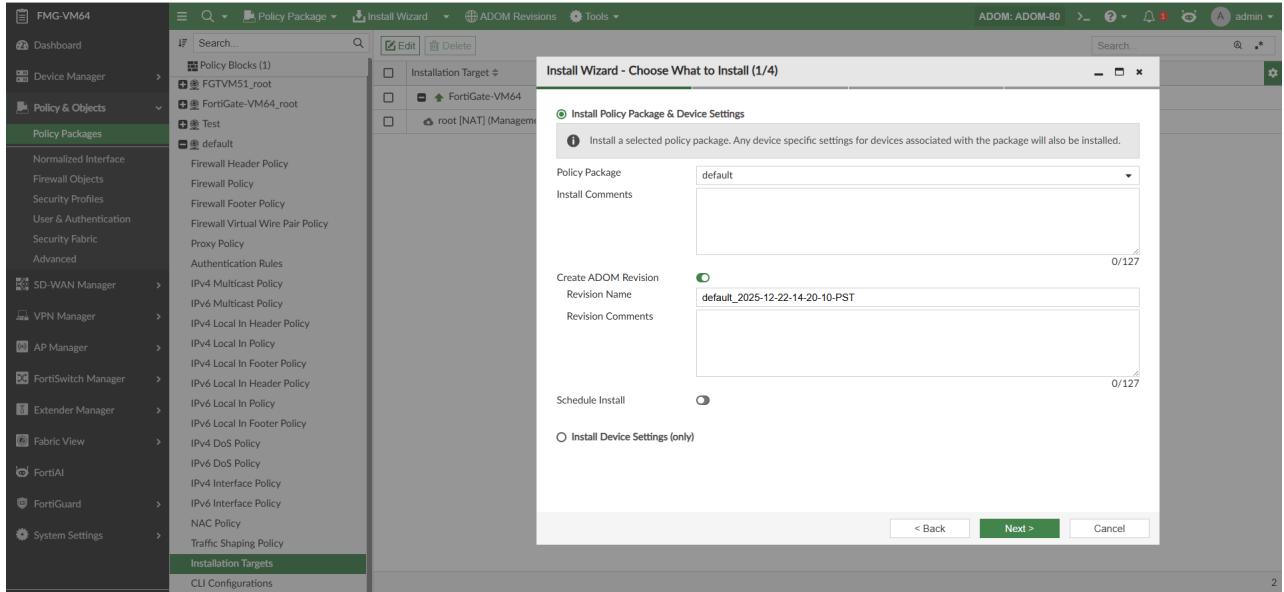
- IPv4 Local In Policy

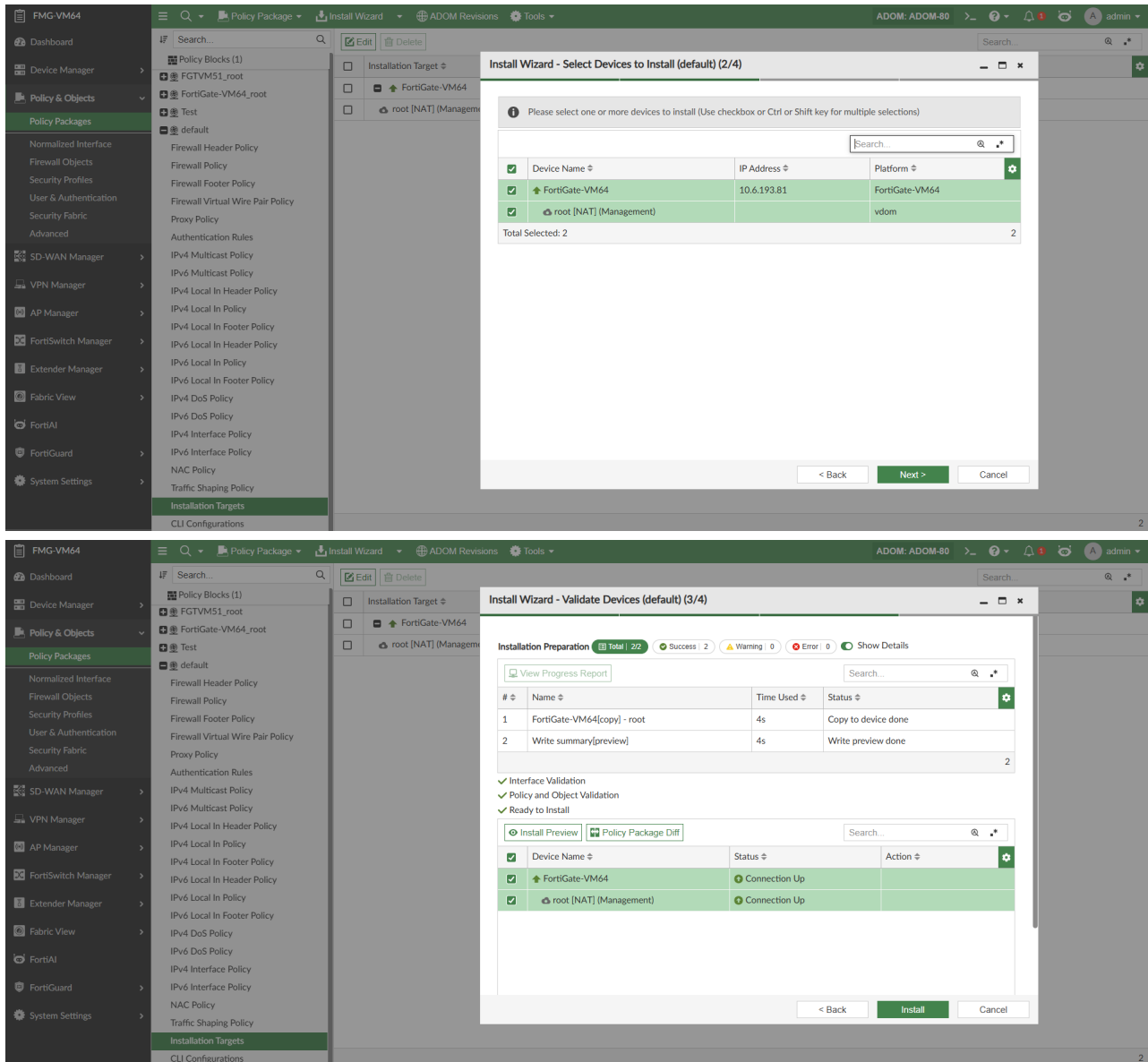


- IPv6 Local In Policy



4. Append the local policy block to a local policy package.
5. Install the policy package to the FortiGate.





Fabric View

This section lists the new features added to FortiManager for Fabric View:

- Connectors on page 82

Connectors

This section lists the new features added to FortiManager for connectors:

- New external connectors: GuardiCore, Microsoft Azure (Proxy Mode), and Application Centric Infrastructure (ACI Proxy Mode) on page 82
- FortiAI Ops connector on page 87
- Central management for ACI features on page 98

New external connectors: GuardiCore, Microsoft Azure (Proxy Mode), and Application Centric Infrastructure (ACI Proxy Mode)



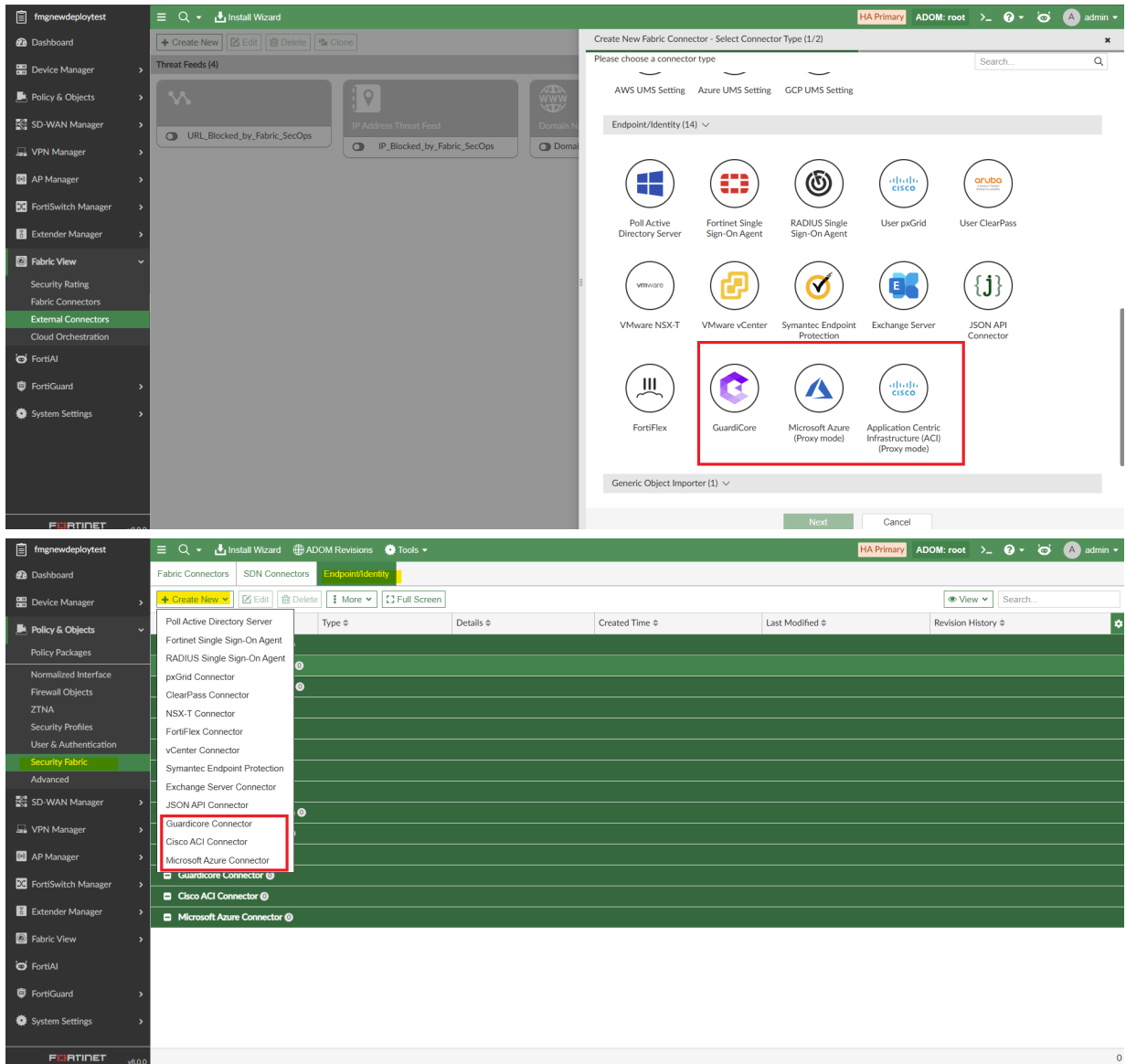
This information is also available in the FortiManager 8.0 Administration Guide:

- Creating Guardicore connectors
- Creating Microsoft Azure connectors
- Creating Application Centric Infrastructure (ACI) connectors

To create Guardicore, ACI and Azure external connectors:

1. Go to *Fabric View > External Connectors* or *Policy & Objects > Security Fabric > Endpoint/Identity*.
2. Click *Create New* and select one of the following connector types:
 - *Guardicore/Guardicore Connector*
 - *Application Centric Infrastructure (ACI)/Cisco ACI Connector*

- Microsoft Azure/Microsoft Azure Connector



3. Configure the connector settings as per your environment and chosen connector type.



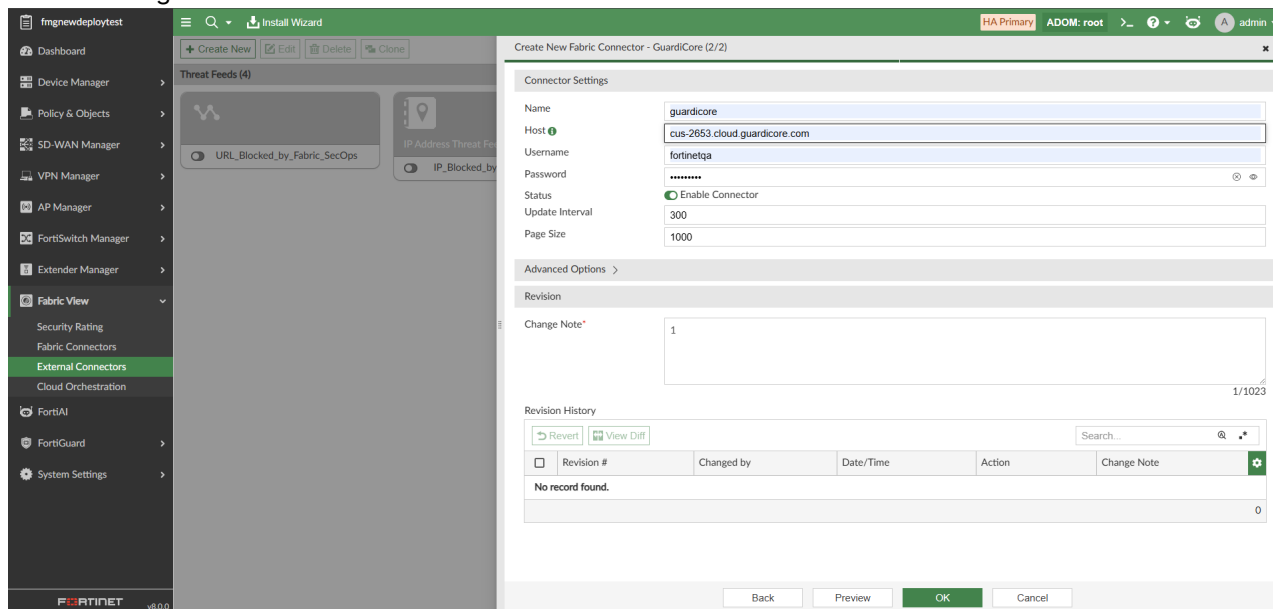
Do not use protocols such as http/https in the hostname for Guardcore and ACI connectors. For example, use "example.com" instead of "https://example.com".

4. Set the *Status* toggle to the *Enable Connector* position.
5. Optionally, you can manually enter the *Update Interval* for FortiManager to communicate with the remote host. The default interval is 300 seconds.
6. Enter a change note and click *OK* to save the connector.

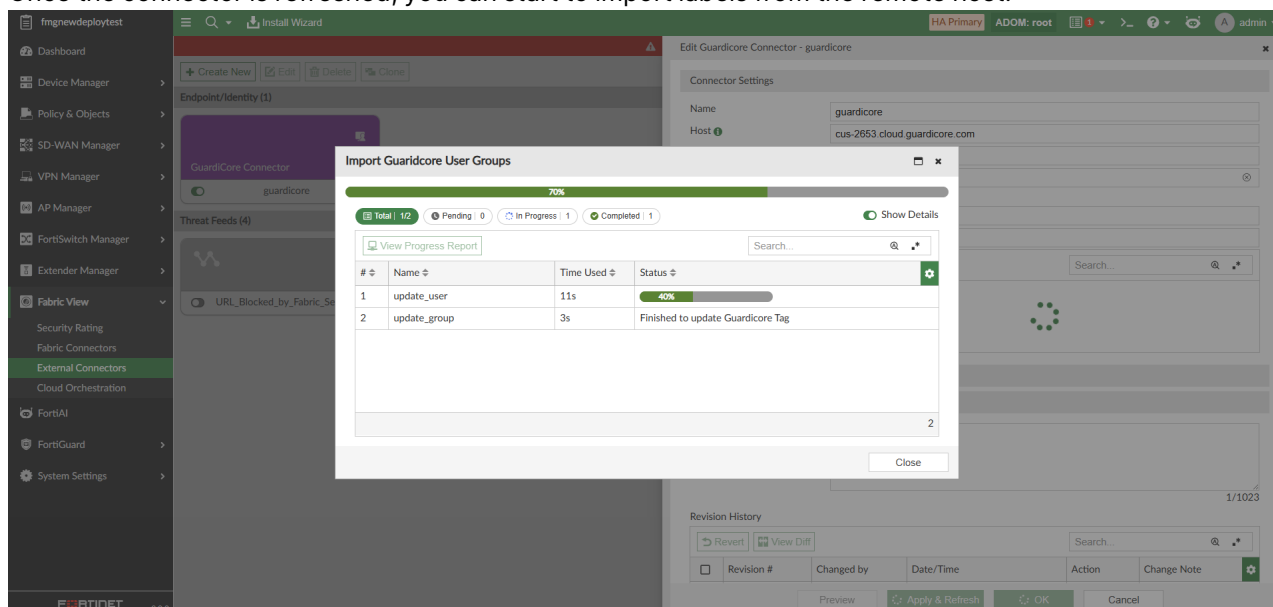
Example: Importing labels from a Guardicore connector

To create a Guardicore connector:

1. Go to *Fabric View > External Connectors*.
2. Click *Create New* and select *Guardicore*.
3. Configure the *Name*, *Host*, *Username*, and *Password* settings.
4. Set the *Status* toggle to the *Enable Connector* position.
5. Enter a change note and click *OK* to save the connector.



6. Edit the connector and click *Apply and Refresh* to import instance objects from the remote host. Once the connector is refreshed, you can start to import labels from the remote host.



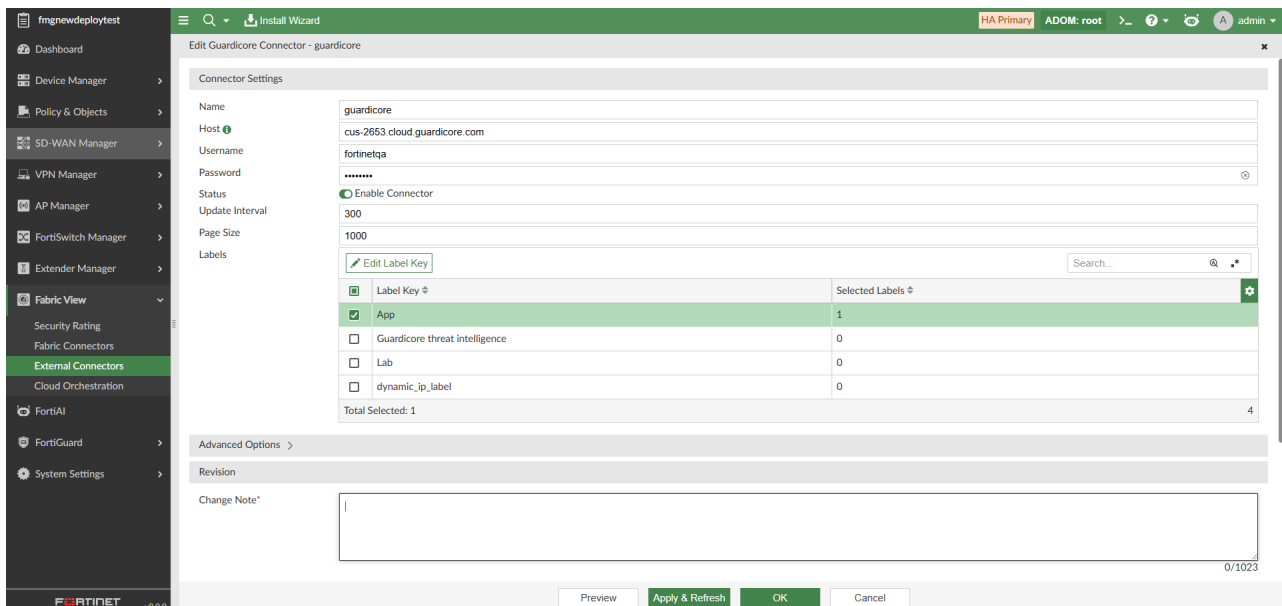
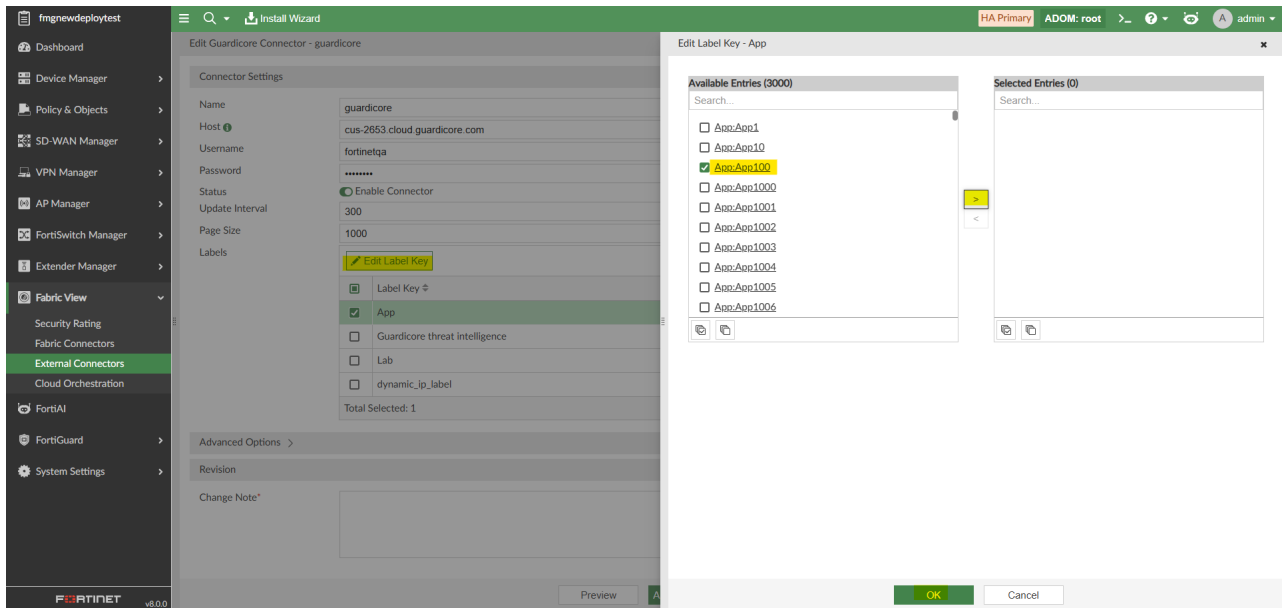
These labels are in the format of Key Value pairs. To import labels, you must input the Key and FortiManager will retrieve the corresponding Key Value pairs, which can then be imported.

7. Click *Edit Label Key* and then select the Key for the FortiManager to retrieve the pairs.

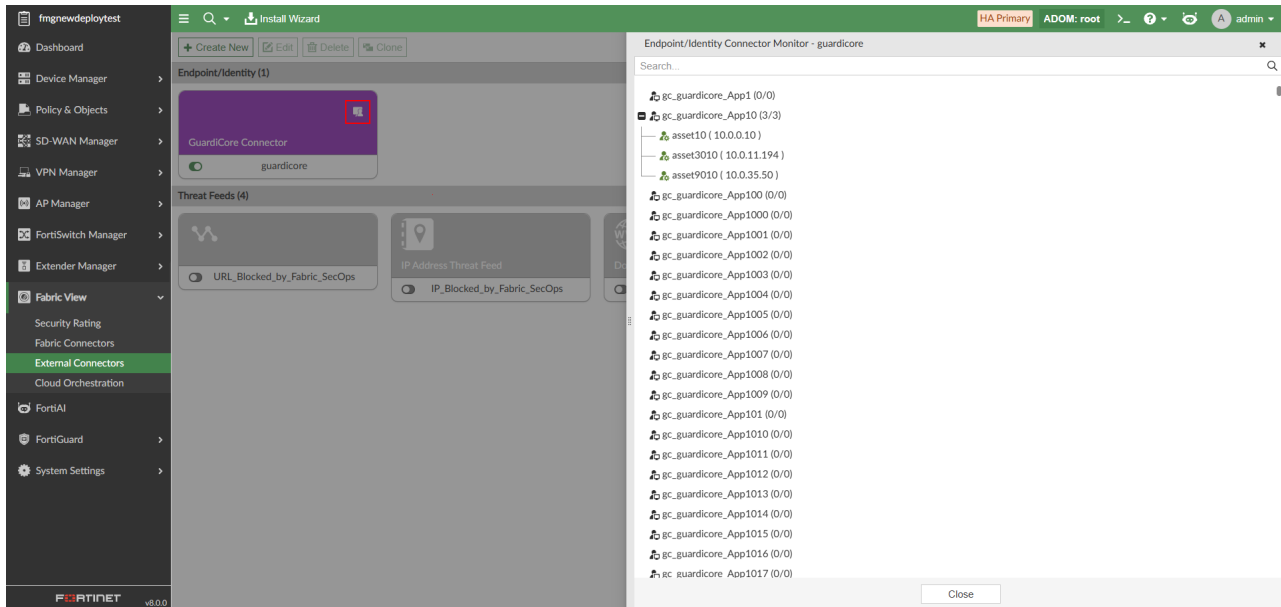
Once you add the Label Key and save it, you can see how many keys have been selected on the connector page.



You can add labels with different Label Keys by repeating this step to add additional Label Keys.



8. Click the top-right icon on the Guardicore connector tile to view matched IP addresses.



Labels imported from the remote host are available as a FSSO adgrp, and are selectable in address objects with the *Dynamic FSSO* type.

To use the imported labels in a firewall policy:

1. Go to *Policy & Objects > Firewall Objects > Addresses* and click *Create New*.
2. Select *Dynamic* as the *Type*.
3. Select *Fortinet Single Sign-On (FSSO)* as the *Sub Type*, and then choose the Guardicore connector as the *FSSO Group*.
4. Click *OK* to save the address object.
5. Create or edit a firewall policy and use the previously configured address object as the *Source*.
You can click *View Matched Addresses* when viewing the object in the policy to see the resolved addresses for Guardicore.
6. Install the policy to your managed FortiGate, and the configuration is pushed to the device.

```
config user adgrp
  edit "gc_guardicore_App10"
    set server-name "FortiManager"
    set connector-source "GUARDICORE"
  next
end

edit "guardicore"
  set uuid c3b0b924-fc82-51f0-9d15-8e5aebcc4cd2
  set type dynamic
  set sub-type fsso
  set fsso-group "gc_guardicore_App10"
next
end

config firewall policy
```

```
edit 1
    set name "test"
    set uuid 9106ec3e-fbea-51f0-e8e4-920fe0d3fc11
    set srcintf "any"
    set dstintf "any"
    set srcaddr "guardicore"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set logtraffic all
next
end
```

FortiAI Ops connector



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

- [Creating a FortiAI Ops connector](#)

FortiManager adds a new fabric connector to FortiAI Ops. The AI Insights dashboard receives updates and information about LAN Edge and SD-WAN managed devices.

This topic includes the following:

- [Prerequisites on page 87](#)
- [Initial configuration on page 87](#)
- [Verifying the connector status on page 92](#)
- [Using the FortiAI Ops Connector on page 94](#)
- [CLI on page 95](#)

Prerequisites

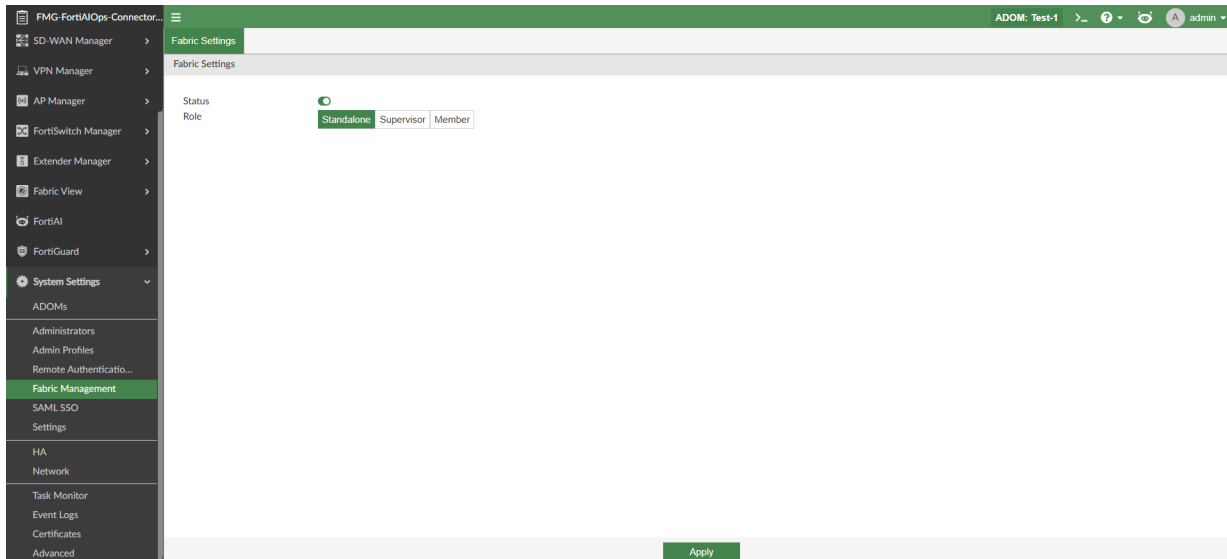
Before you can enable the FortiAI Ops connector, the following prerequisites on FortiManager must be met:

- Enable Fabric Management settings.
- Enable *FortiManager Fabric* Administrative Access for the interface

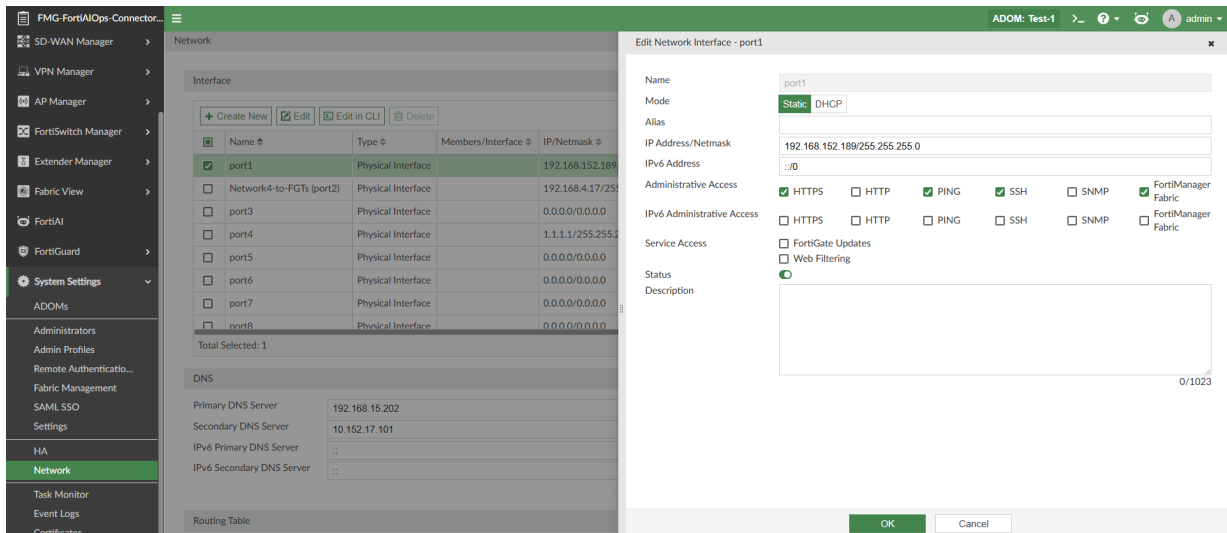
Initial configuration

To use the FortiAI Ops Connector:

1. Enable Fabric Management settings on FortiManager.
 - a. Go to *System Settings > Fabric Management > Fabric Settings*.
 - b. Set the *Status* toggle to the *ON* position.
 - c. Set the *Role* as *Standalone*.



2. Enable FortiManager Fabric Administrative Access for the interface.
 - a. Go to *System Settings > Network*.
 - b. Edit the network interface that FortiAI Ops will use to connect to FortiManager.
 - c. Enable the *FortiManager Fabric* option, and click *OK*.



3. Establish the connection from FortiAI Ops.

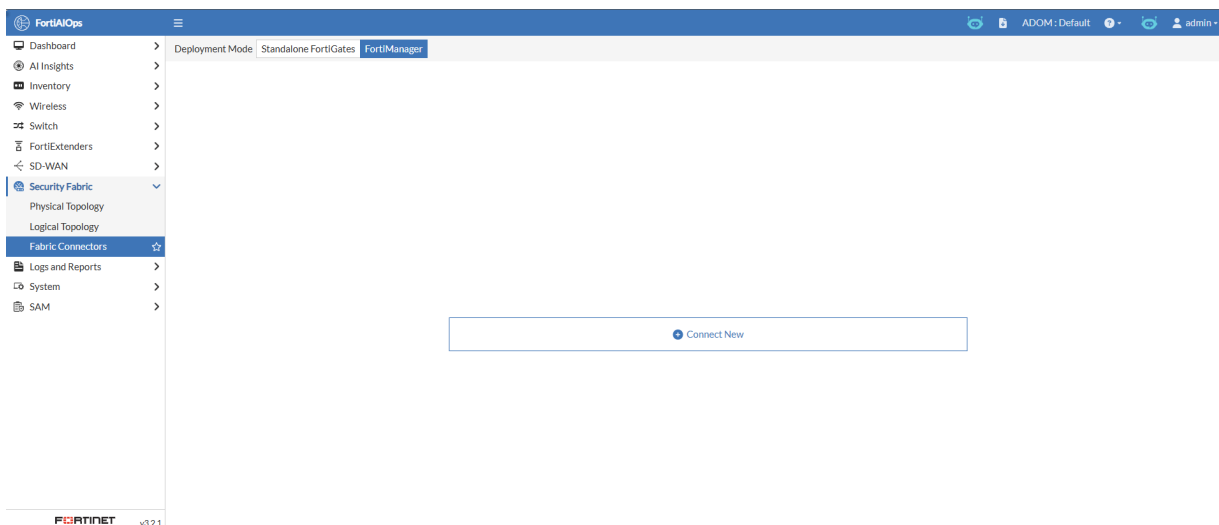
Activating FortiAI Ops from FortiManager

The FortiAI Ops connector cannot be activated on FortiManager without a FortiAI Ops setup request. If you attempt to establish the connection from the FortiManager first, a message is displayed to initiate the authorization through FortiAI Ops.

 Please initiate the Fabric Authorization through your FortiAI Ops.

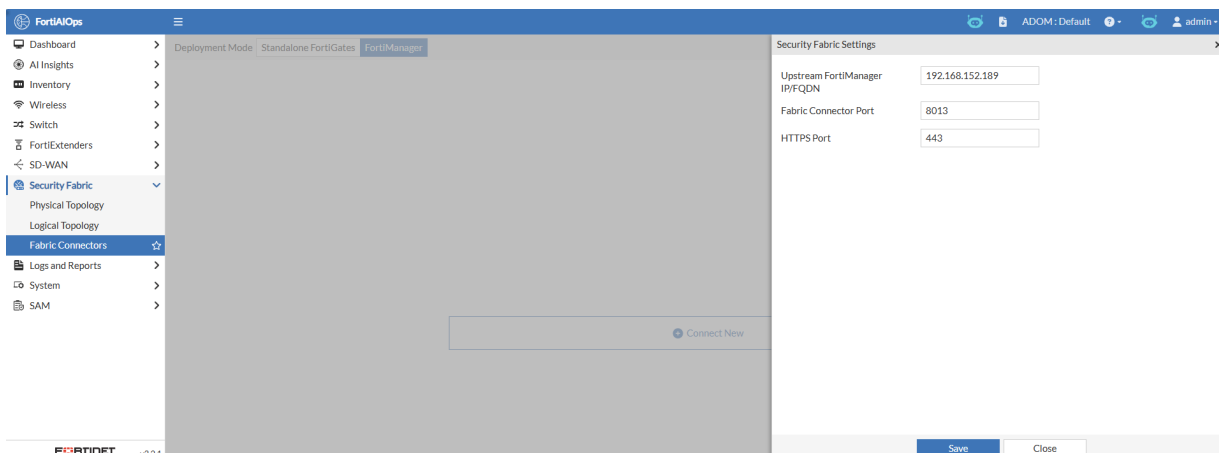
- a. On FortiAI Ops, go to *Security Fabric > Fabric Connectors*.
- b. Select the FortiManager *Deployment Mode*.

c. Click *Connect Now*.



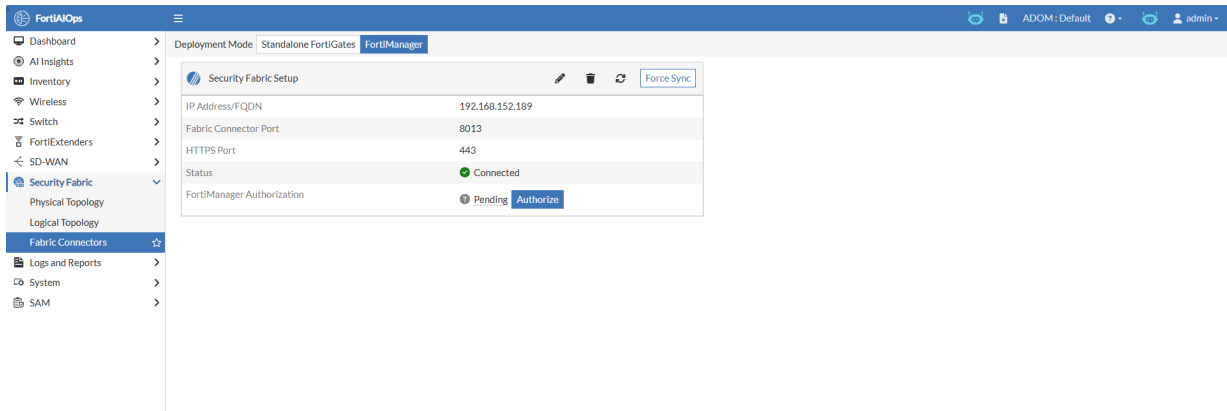
d. Enter the following information from your FortiManager:

Upstream FortiManager IP/FQDN	Enter the IP address or FQDN of the upstream FortiManager.
Fabric Connector port	Enter the Fabric Connector port. The default is 8013.
HTTPS Port	Enter the HTTPS port. The default is 443.

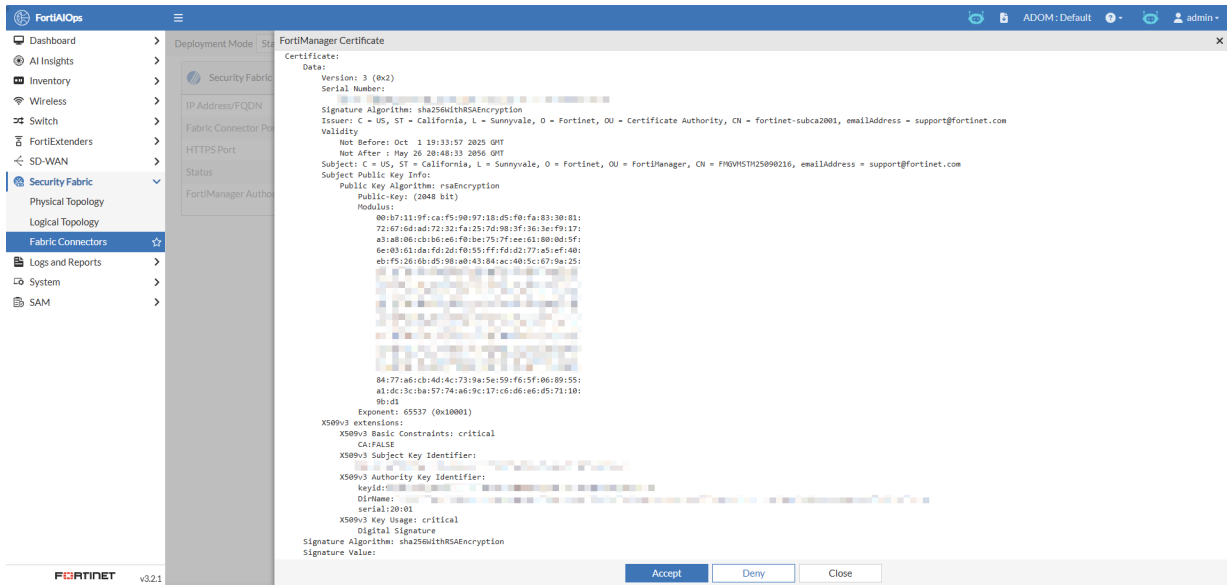


e. Click *Save*. FortiAI Ops will connect to the FortiManager and request authorization.


f. Click *Authorize* to review the FortiManager Certificate.



g. Review the certificate and then click *Accept* or *Deny*.

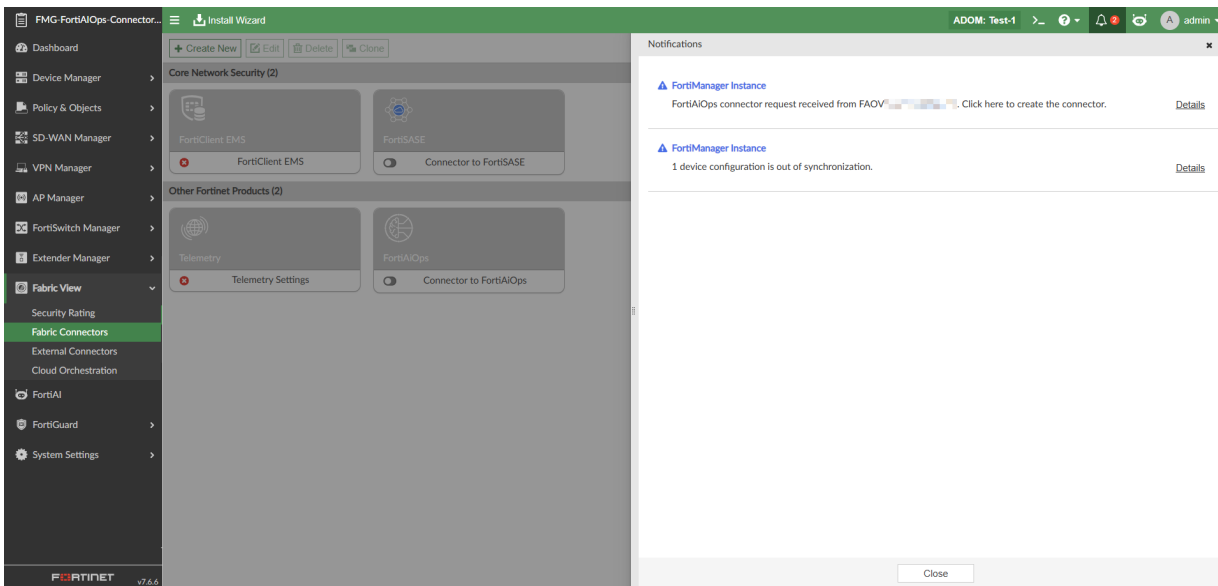


h. If the FortiManager certificate is accepted, the *FortiManager Authorization* status will be set to *Authorized*, and a FortiAI Ops connector setup request will be sent to the FortiManager.

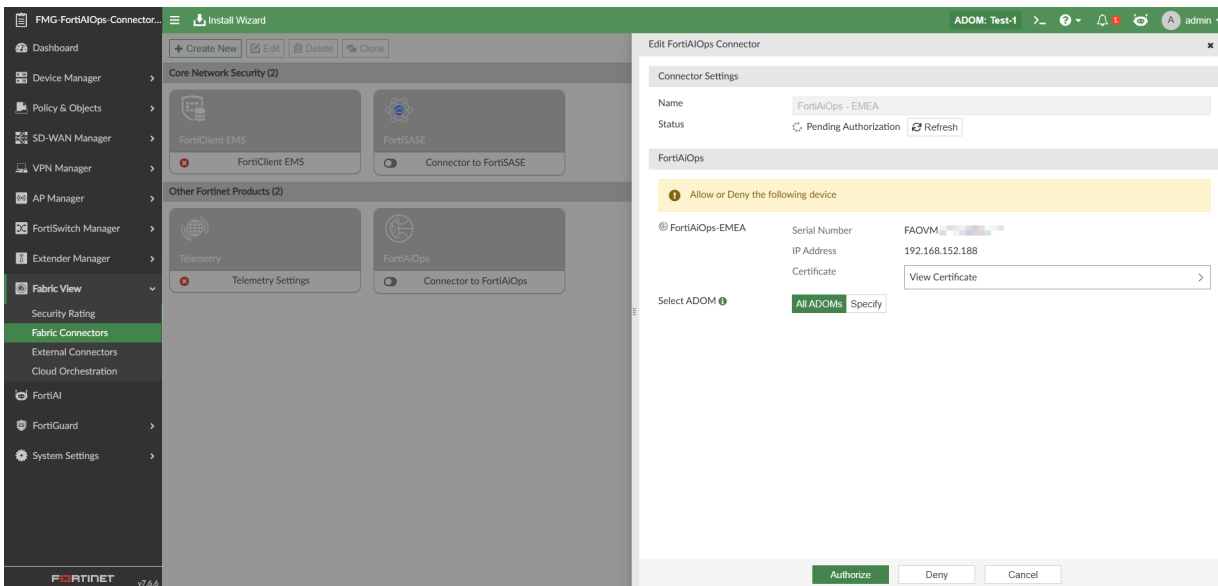
 During the FortiManager-side authorization process, the *FortiAI Ops Authorization* status remains *Pending*.

4. Complete the FortiManager FortiAI Ops Connector establishment process on the FortiManager.

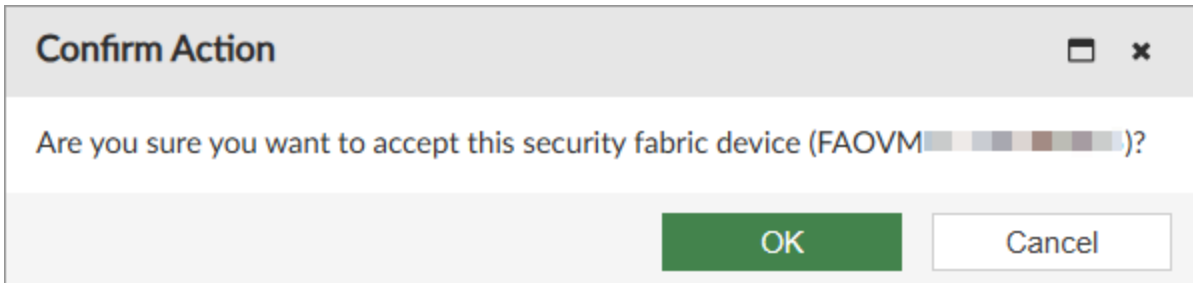
- a. Open the notification drawer on FortiManager to review the FortiAIOPS connector setup request.



- b. Click the *Details* link in the FortiAIOPS connector request notification.
- c. Authorize FortiAIOPS by reviewing its credentials, including the *Serial Number*, *IP address*, and *Certificate*, and select the ADOM list to be shared with FortiAIOPS (*All ADOMs* or *Specify*).



- d. Click *Authorize* to accept the credentials, then click *OK* on the *Confirm Action* dialog to complete the FortiAIOPS Authorization process.





After FortiAI Ops authorization, the *Status* changes from *Pending Authorization* to *On*.

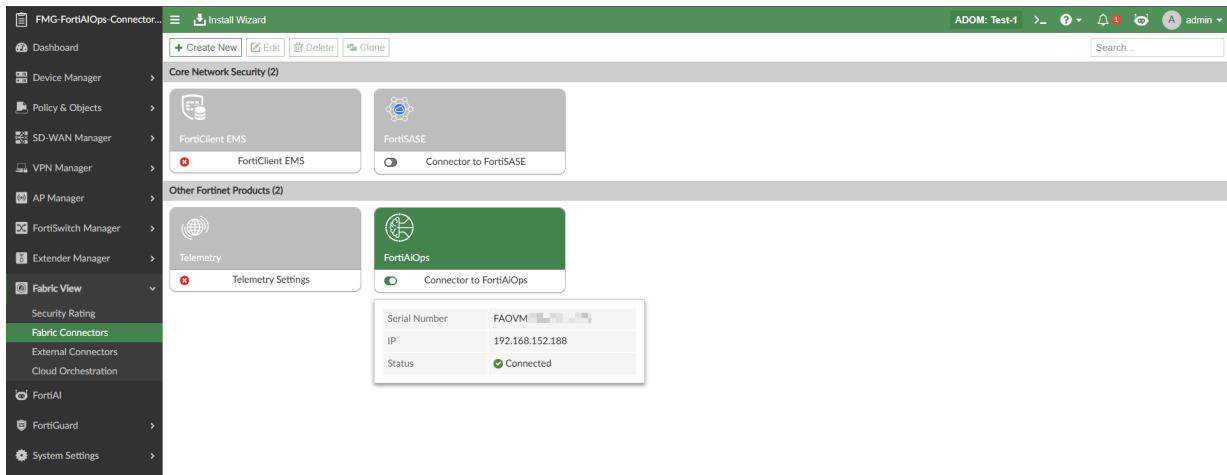
- e. Click **Save** to finalize the FortiAI Ops connector establishment process.

Verifying the connector status

Once a FortiAI Ops connector has been successfully added and authorized, you can verify the connector status by going to *Fabric View > Fabric Connectors*.

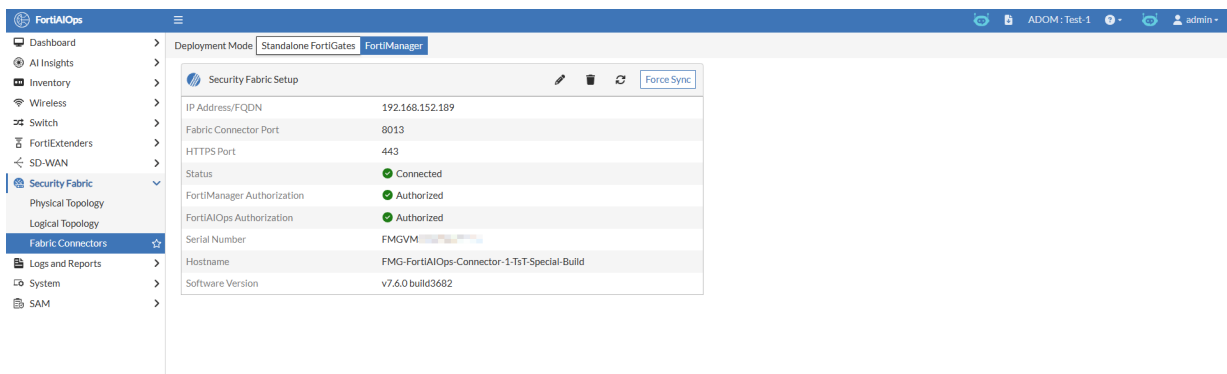
To verify the FortiAI Ops connector status:

1. Verify the FortiAI Ops connector status on FortiManager:
 - a. On FortiManager, go to *Fabric View > Fabric Connectors*.
The FortiAI Ops connector is displayed within the *Other Fortinet Products* category.
 - b. You can view the FortiAI Ops connector details by double clicking the connector, selecting it and clicking *Edit* in the toolbar, or by hovering your mouse over the connector to view the tooltip.

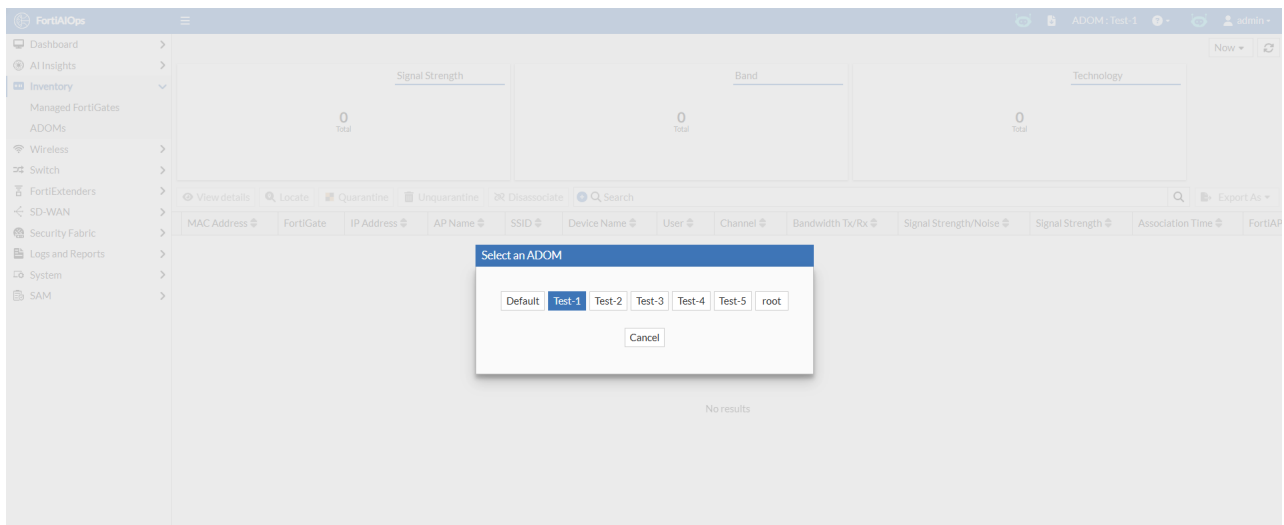
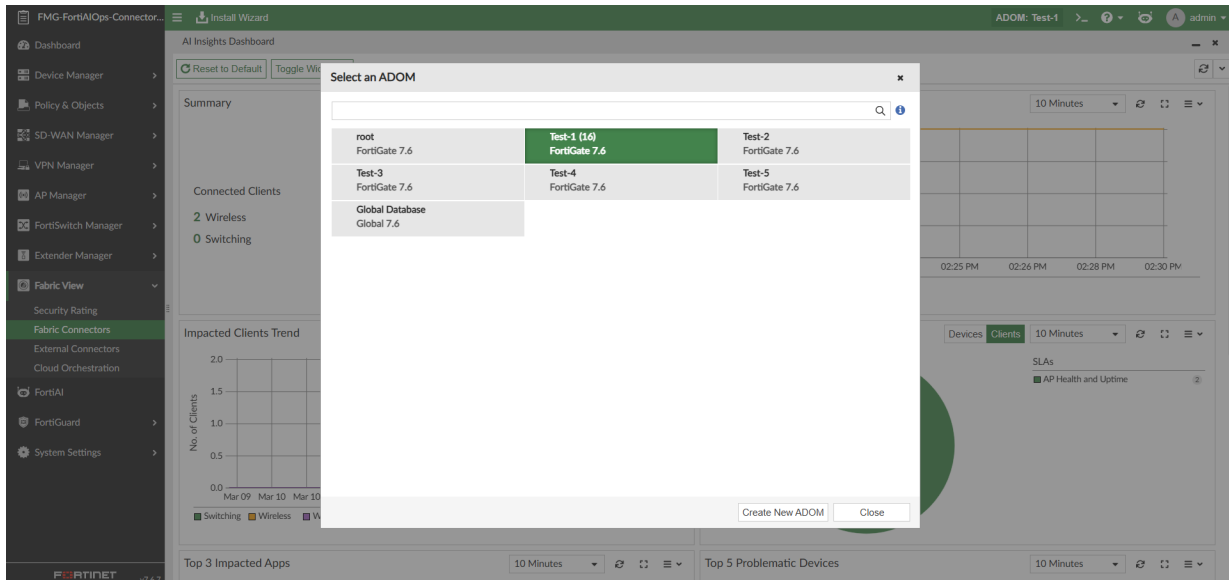


2. Verify the FortiManager Fabric connection on FortiAI Ops.
 - a. On FortiAI Ops, go to *Security Fabric > Fabric Connectors*.

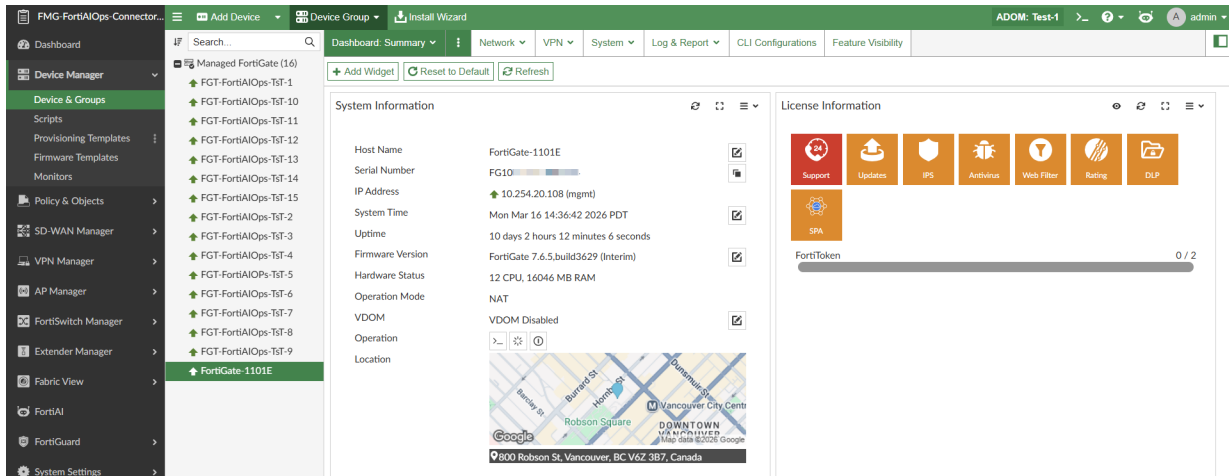
If the configuration was successful, the *Status* field will be displayed as *Connected*, and the *FortiManager Authorization* and *FortiAI Ops Authorization* fields will be displayed as *Authorized*.

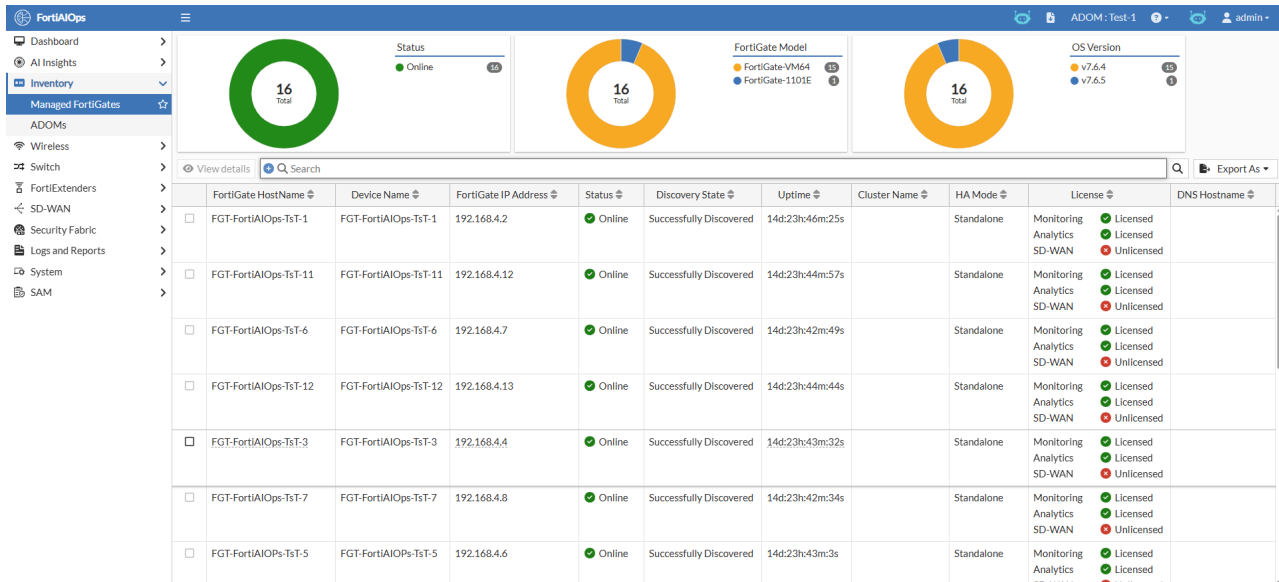


3. Verify that the shared ADOM list is synchronized between FortiManager and FortiAI Ops.



4. Verify that the list of FortiGate devices is synchronized between the FortiManager and FortiAIops.

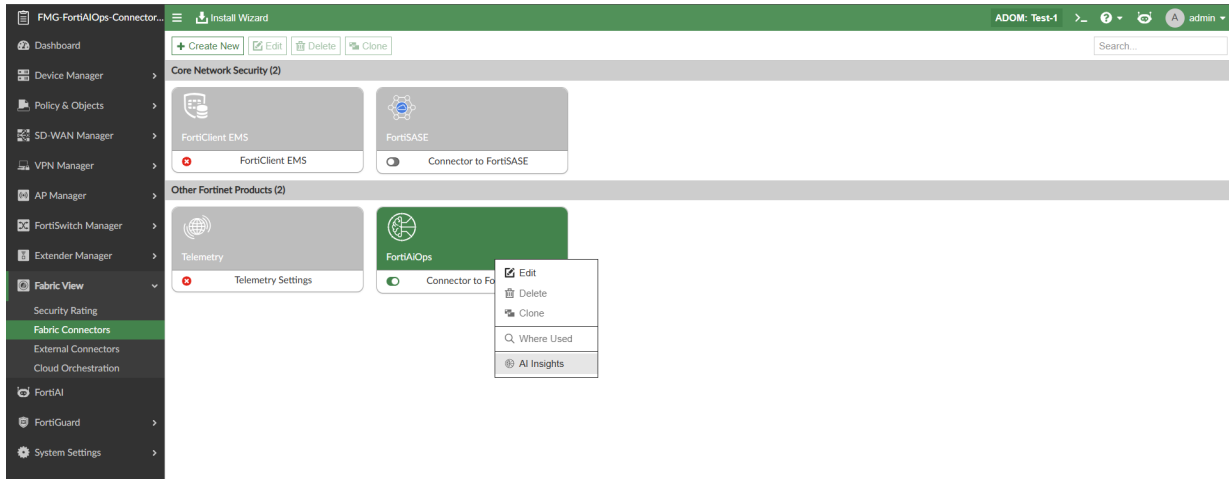




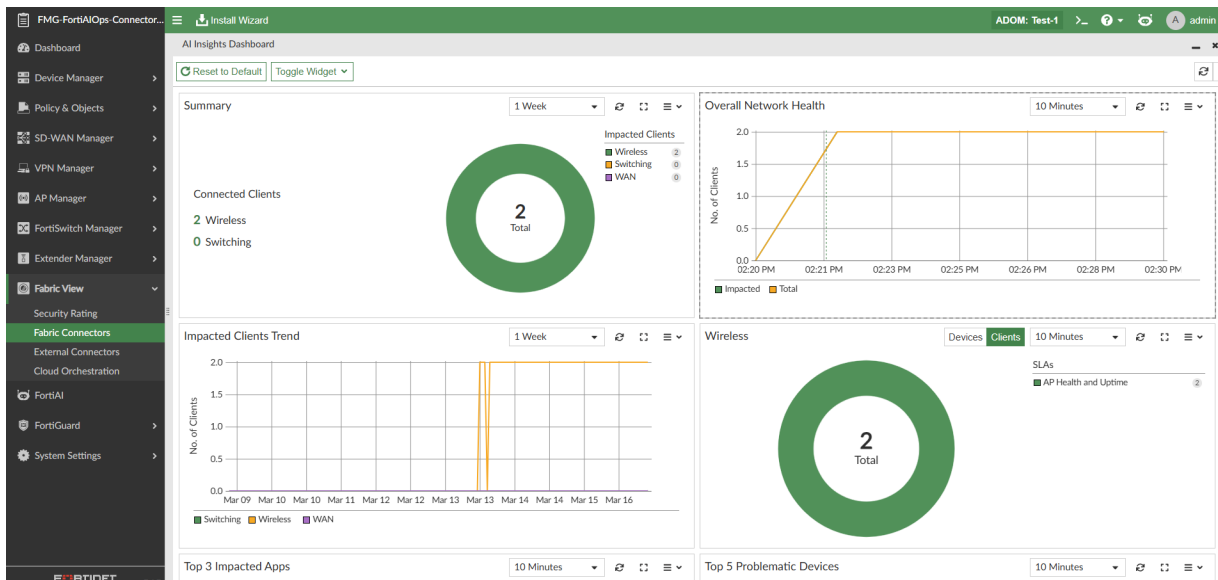
Using the FortiAIOps Connector

To use the FortiAIOps connector on FortiManager:

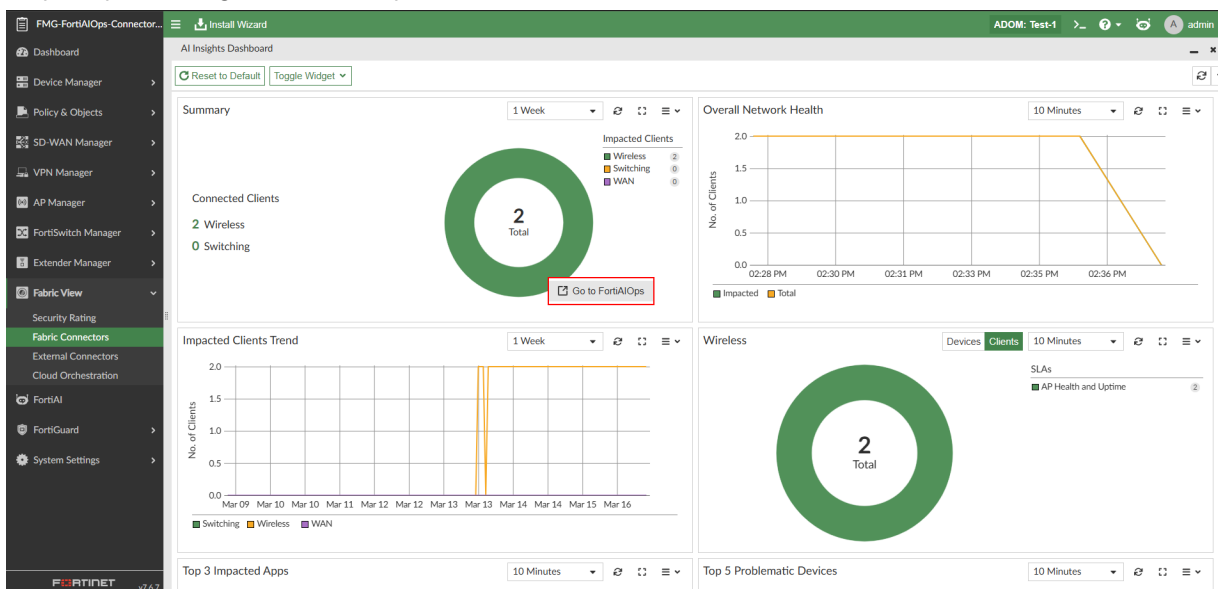
1. Go to *Fabric View > Fabric Connectors*.
2. Right-click the FortiAIOps connector and click *AI Insights*.



The *AI Insights Dashboard* is displayed. The AI Insights dashboard receives updates and information about LAN Edge and SD-WAN managed devices from FortiAIOps.



- The FortiAIops portal can be accessed from the FortiManager *AI Insights* dashboard. Once clicked you will be prompted to log in to FortiAIops.



CLI

FortiAIops data, including the serial number, IP address, and certificate are displayed in the CSF Authorization Pending List once FortiManager is authorized on FortiAIops. This can be verified using the `diagnose system csf authorization pending-list` command.

```
diagnose system csf authorization pending-list
```

Serial Appliance	Path	IP Address	HA-Members

```
-----
FAOVMSTM25000000      192.168.152.188                                fortiaios
FMGVMSTM25090000:FAOVMSTM25000000
```

Certificate:

```
Subject:      C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiAIops, CN =
FAOVMSTM25000000, emailAddress = support@fortinet.com
```

```
Issuer:      C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
Authority, CN = fortinet-subca2001, emailAddress = support@fortinet.com
```

```
Valid from:  2025-10-09 19:04:24 GMT
```

```
Valid to:    2056-05-26 20:48:33 GMT
```

```
Fingerprint: 25:88:13:A4:D8:2A:E7:23:01
```

```
Root CA:    No
```

```
Version:    3
```

```
Serial Num:
```

```
03:ef:d4:a8:06:39:e9:8c:8d:bc:da
```

```
Extensions:
```

```
Name:      X509v3 Basic Constraints
```

```
Critical:  yes
```

```
Content:
```

```
CA:FALSE
```

```
Name:      X509v3 Subject Key Identifier
```

```
Critical:  no
```

```
Content:
```

```
A1:F8:00:78:F4:DA:7A:A9:F2:
```

```
Name:      X509v3 Authority Key Identifier
```

```
Critical:  no
```

```
Content:
```

```
keyid:98:2B:25:3C:30:CA:2C:2B:56
```

```
DirName:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-
ca2/emailAddress=support@fortinet.com
```

```
serial:20:01
```

```
Name:      X509v3 Key Usage
```

```
Critical:  yes
```

```
Content:
```

```
Digital Signature
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIE9DCCA9ygAwIBAgIUUA+/UqAY56YyNvNrG0H4M9ZYN+2MwDQYJKoZIhvcNAQEL
BQAwgasxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQQH
Ew1TdW5ueXZhbGUxETAPBgNVBAoTCEZvcnRpbmV0MR4wHAYDVQQLExVDZXJ0aWZp
Y2F0ZSBDbXR0b3JpdHkxGzAZBgNVBAMTEmZvcnRpbmV0LXN1YmNhMjAwMTEjMCEG
CSqGSIb3DQEJARYUc3VwcG9ydEBmb3J0aW51dC5jb20wIBcNMjUwMDA5MTkwNDI0
WhgPMjA1NjA1MjYyMDQ4MzNaMIGeMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2Fs
aWZvcnRpbmV0MTEwMTEjMCEGCSqGSIb3DQEJARYUc3VwcG9ydEBmb3J0aW51dC5jb20w
MBEGA1UECwwKRm9ydG1BSU9wcZEMBCGA1UEAwwQRkFPVnk1TVE0yNTA5MDAwNTEj
MCEGCSqGSIb3DQEJARYUc3VwcG9ydEBmb3J0aW51dC5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDqtEVB7APBYesNrRbw1jr1EskVRnrqJ+OMbeMF
```

```
wtO3gYPwClWuz7MKFoMgDl+itkGaIs/IIy9Sgi1rPjdcD4kc1YqhMuuUKXIs3djq
uK5eNmH7LUahFaS35In+sKfiucyYIeAM+4zEjIGIH8tbzp6+jWxumWHXSRcwH8LZ
wO5KYpZXsOPnwF66h3zo9Yljgk0zv2ph98pcv1AMhciw9tNCJMy8408XpTVYOnoz
jQZLGpNj3MlmpzDP8s0spbqQT1rdXtwI/WESDdmjOmnE1SRhAgMBAAGjggEXMIIB
EzAMBgNVHRMBAF8EAjAAMB0GA1UdDgQWBBSH+AB49Np6qfL+tdsucyenfKc8GzCB
0wYDVR0jBIHLMIHIIgBSYKYU8MMosK1bn2/xZM7PcPVtq16GBq6SBqDCBpTELMaKG
ZTERMA8GA1UEChMIRm9ydGluZXQxHjAcBgNVBAsTFUNlcnRpZm1jYXRlIEF1dGhv
cm10eTEVMBMGA1UEAxMMZm9ydGluZXQxY2EyMSMwIQYJKoZIhvcNAQkBFhRzdXBw
b3J0QGZvcnRpbmV0LmNvbYICAEwDgYDVR0PAQH/BAQDAgeAMA0GCSqGSIb3DQEB
CwUAA4IBAQDIi15L/PnZehrVIU4i3bnHZZgbXJTLiBovK/I2ZbjFi6IpRnjiHMBk
7vJY5pU9cd3lSNR4dw96yp0mH1rLBMUPnGauX9aUCbkv3Bxw7GA6LLVRBCDITRZ9
C8k3dCzsVlFh37dJ4eQ2d0c16V9mqOuoTxI6wd3MOs1F2RH50e9eAU6Uq1UP619L
BVX2gKnZ7yfCXEzrm5B/QKGdYP4cIudUd3+zLgDkcOhH+mWD85hbyZM3NtrE3WD4
zprjrnXv3ET934tsjHMaqMBb2IG10+eW/jxYtUMzQSD7H49yckSdogFiCOLe5qj
TZi1nVzrNR/7mf/uFA8h36ULDug01rZl
-----END CERTIFICATE-----
```

FortiAIops data, including the name and serial number, are moved from the *CSF Authorization Pending List* to the *CSF Trusted List* once FortiManager authorizes FortiAIops. This can be verified using the following `get system csf` command.

```
diagnose system csf authorization pending-list
Serial          IP Address      HA-Members      Appliance
  Path
-----
-----

FMG-FortiAIops-Connector-1-TsT-Special-Build # get system csf
status          : enable
upstream        : (null)
upstream-port   : 8013
group-name      : (null)
accept-auth-by-cert : enable
authorization-request-type: certificate
certificate      : Fortinet_Local
fabric-workers   : 2
ssl-protocol    : follow-global-ssl-protocol
trusted-list:
  == [ dump ]
  name: dump          serial: dump          ha-members:
  == [ FAOVMSTM25000000 ]
  name: FAOVMSTM25000000
fabric-connector:

*****
```

Central management for ACI features



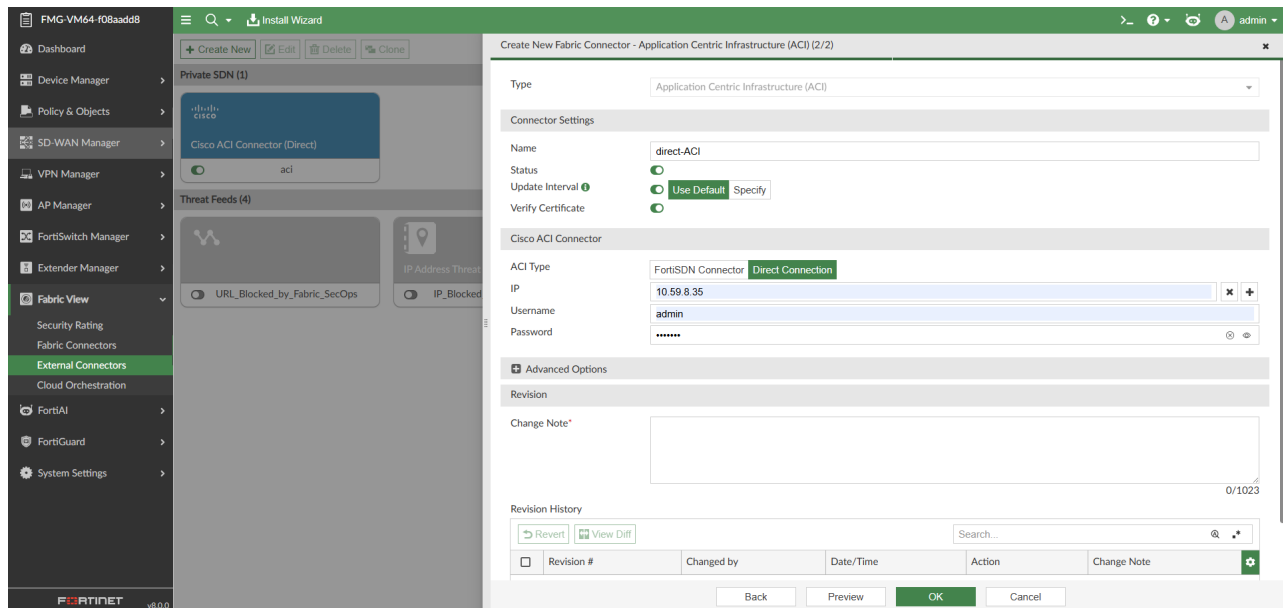
This information is also available in the FortiManager 8.0 Administration Guide:

- Creating ACI SDN Connectors

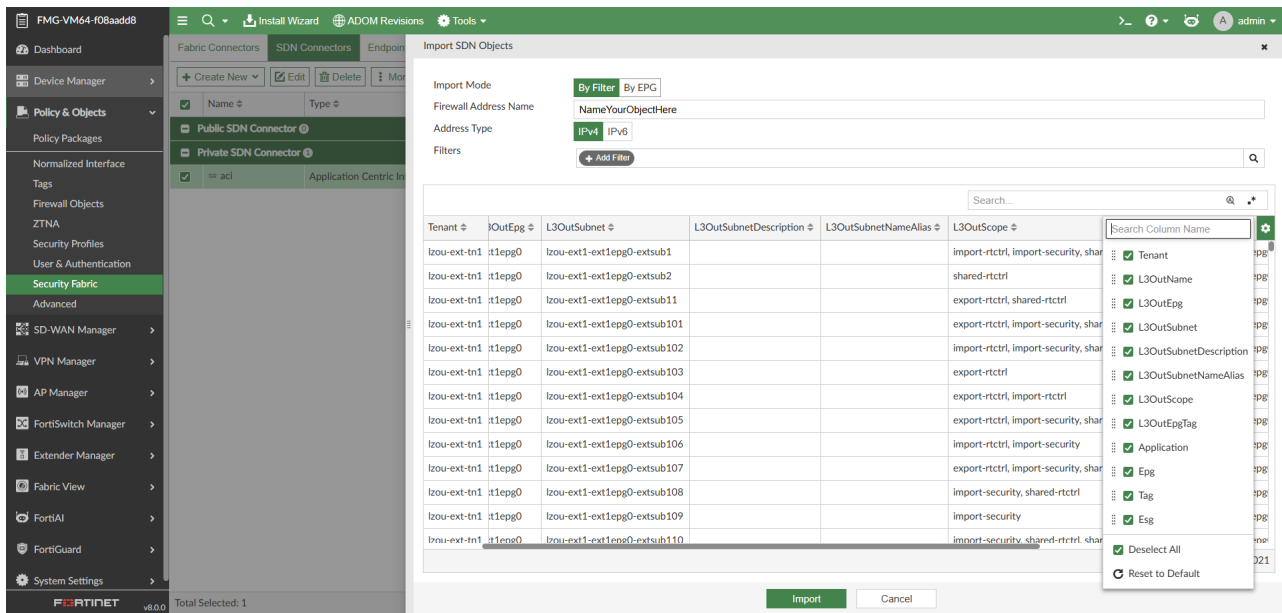
FortiManager can import additional object types from Cisco ACI including L3Out objects and IPv6 objects.

To import objects from Cisco ACI:

1. Go to *Fabric View > External Connectors*.
2. Click *Create New > Cisco ACI Connector*.
3. For *ACI Type* choose *Direct Connection*, configure the connector settings, and click *OK*.

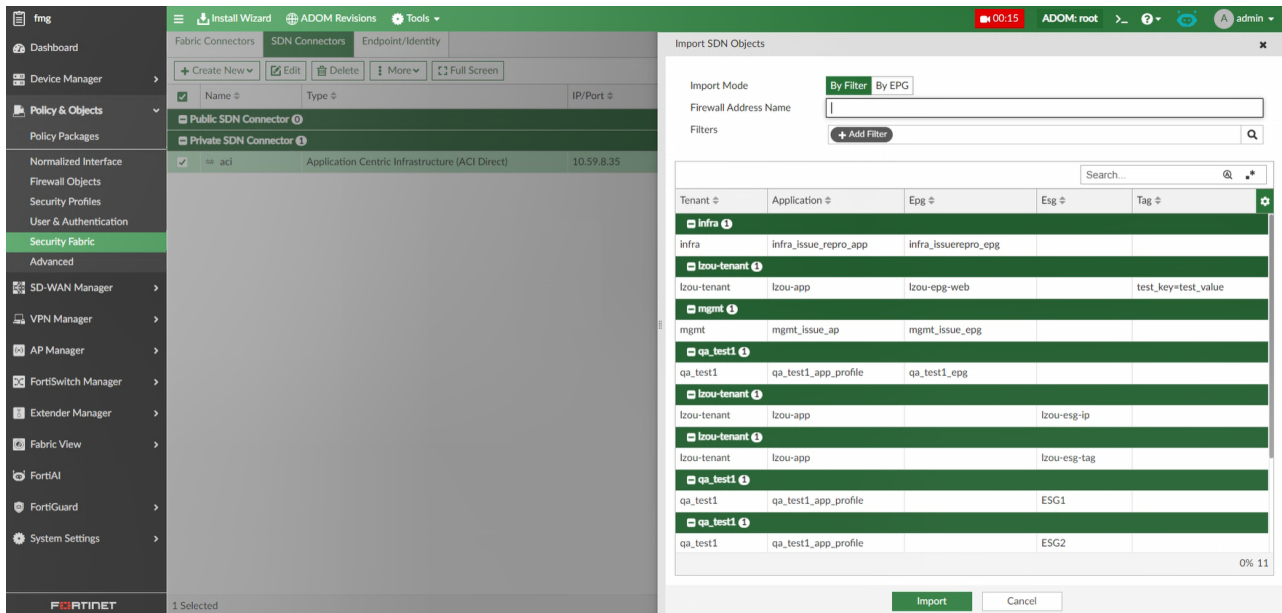


Once the connection is established between FortiManager and Cisco ACI, you can import objects using the *By Filter Import Mode*. Supported object types are displayed in the filtered results.

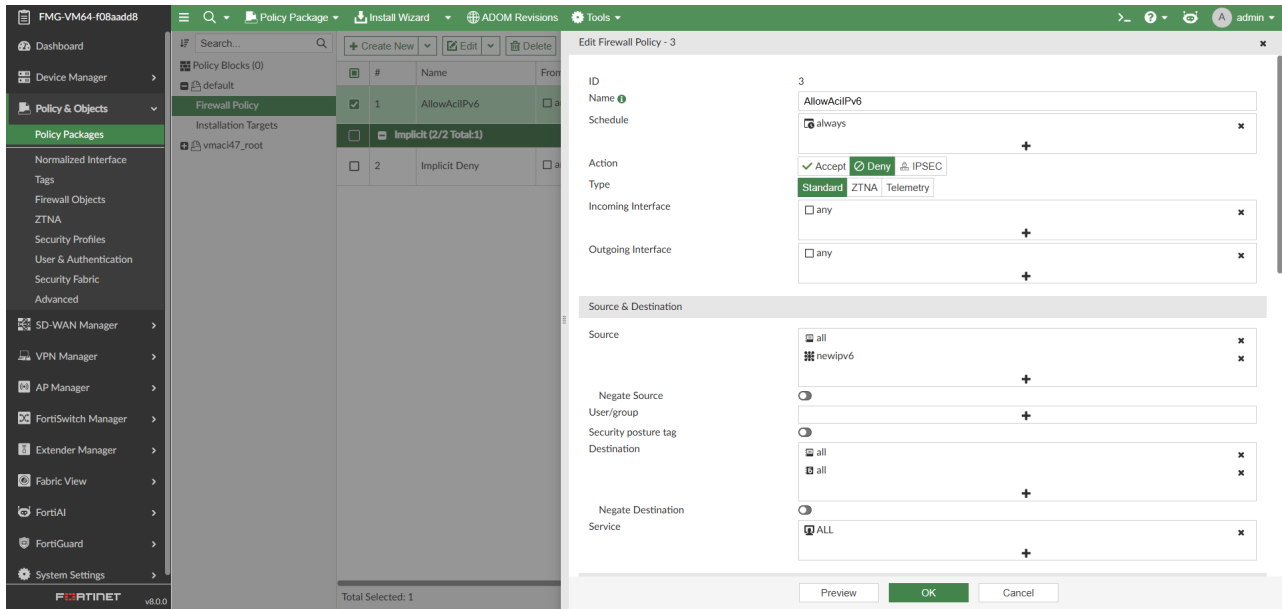


Prior to the implementation of this feature, only *EPG*, *ESG*, and *Tags* were imported. With this release, additional objects are available, for example *L3OutSubnet* and *L3OutSubnetDescription*.

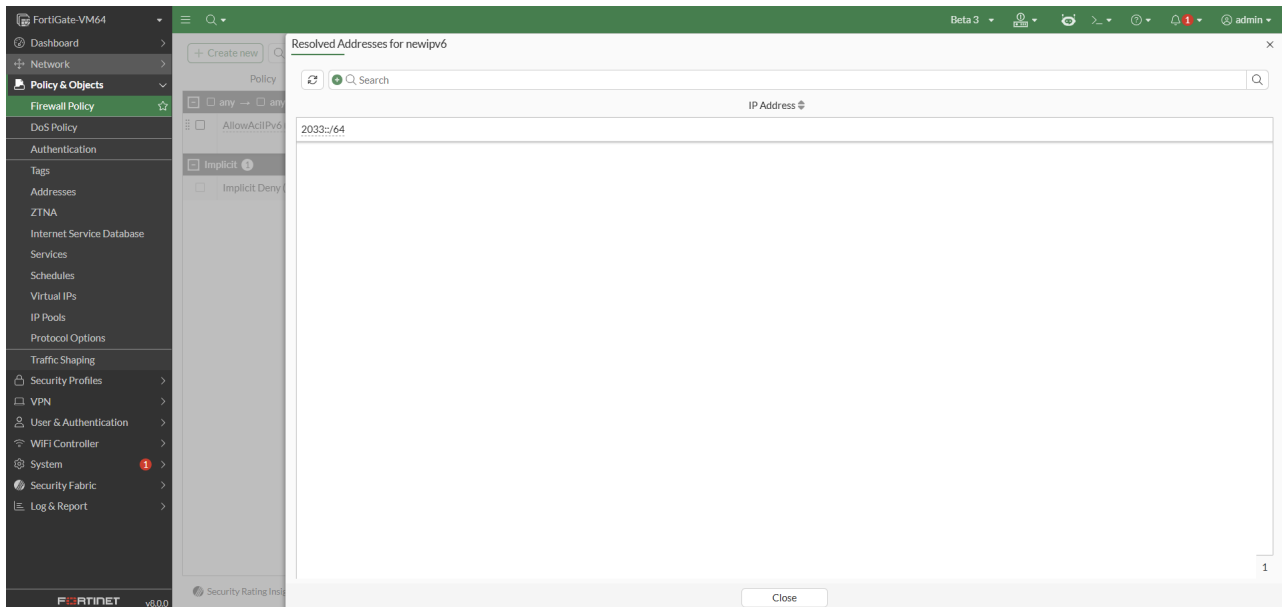
For example, the following image shows the types of objects that could be imported from Cisco ACI connector **before** this feature:



4. Add a Firewall Address Name and click Import to create the corresponding dynamic firewall address.
5. Add the address object to a policy and push the policy package to FortiGate devices.



- Once the policy package is installed, the FortiGate will resolve the IP address from ACI and apply the policy accordingly.



FortiAI

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

- FortiAI can diagnose, troubleshoot, and remediate slow access to cloud or on-premise servers and applications on page 101

FortiAI can diagnose, troubleshoot, and remediate slow access to cloud or on-premise servers and applications

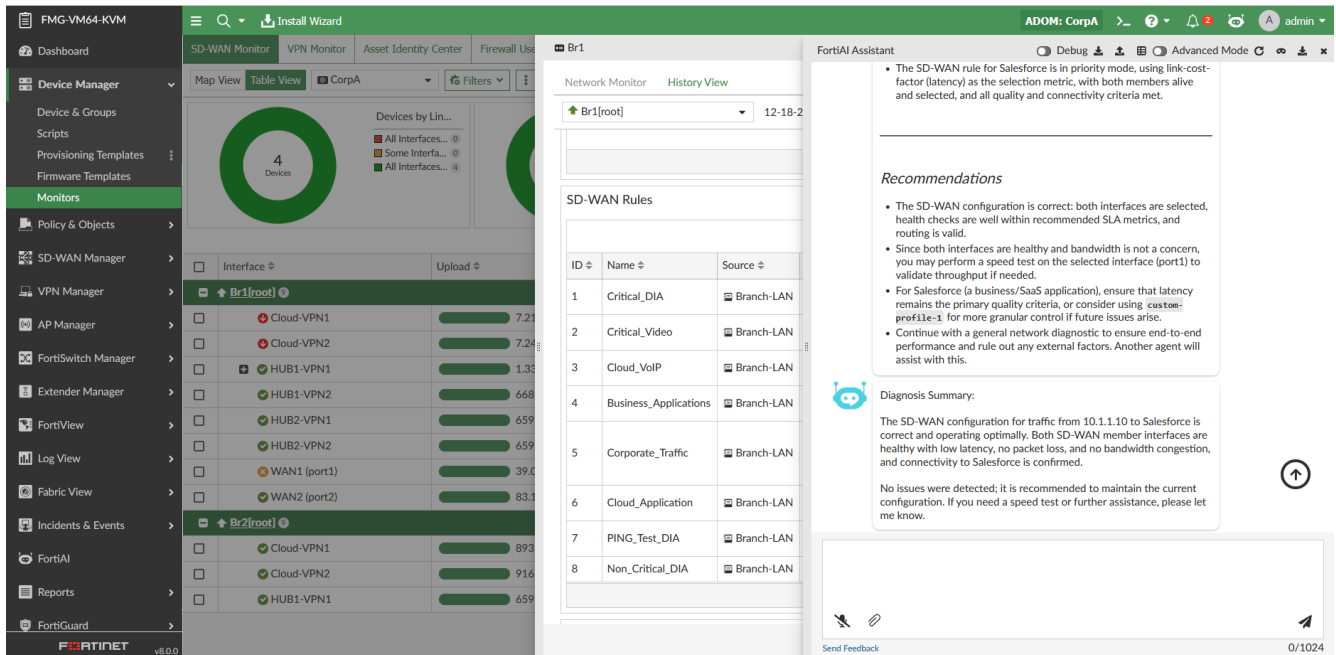


This information is also available in the FortiManager 8.0 Administration Guide:

- Diagnose, troubleshoot, and remediate slow access to cloud or on-premises servers and applications

FortiAI can diagnose, troubleshoot, and remediate slow access to cloud or on-premise servers and applications.

- Example 1: Network is slow from IP 10.1.1.10 to Salesforce application on page 102
- Example 2: Network slow between IP 10.1.1.10 to YouTube on page 104
- Example 3: Network slow between IP 10.1.1.10 to 10.1.2.10 on page 106
- Example 4: Network slow between IP 10.1.1.10 and cloud server 172.20.1.10 on page 108



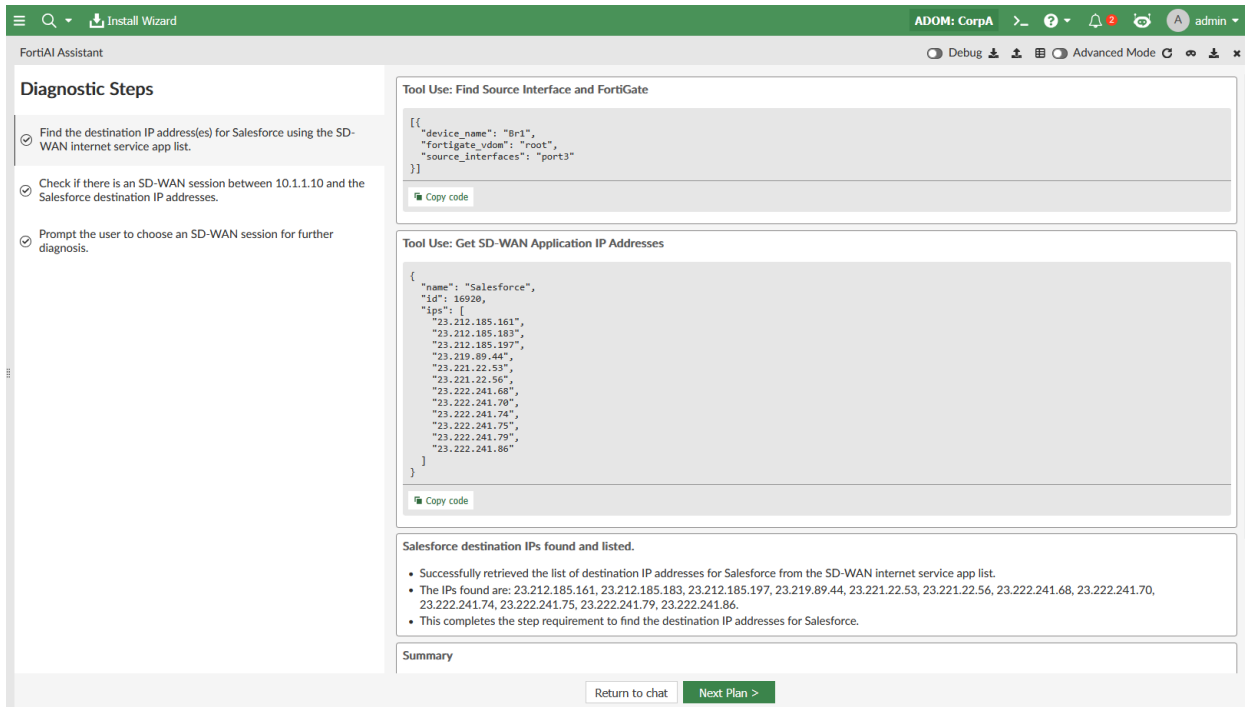
Example 1: Network is slow from IP 10.1.1.10 to Salesforce application

To use FortiAI to diagnose traffic between a user and Salesforce:

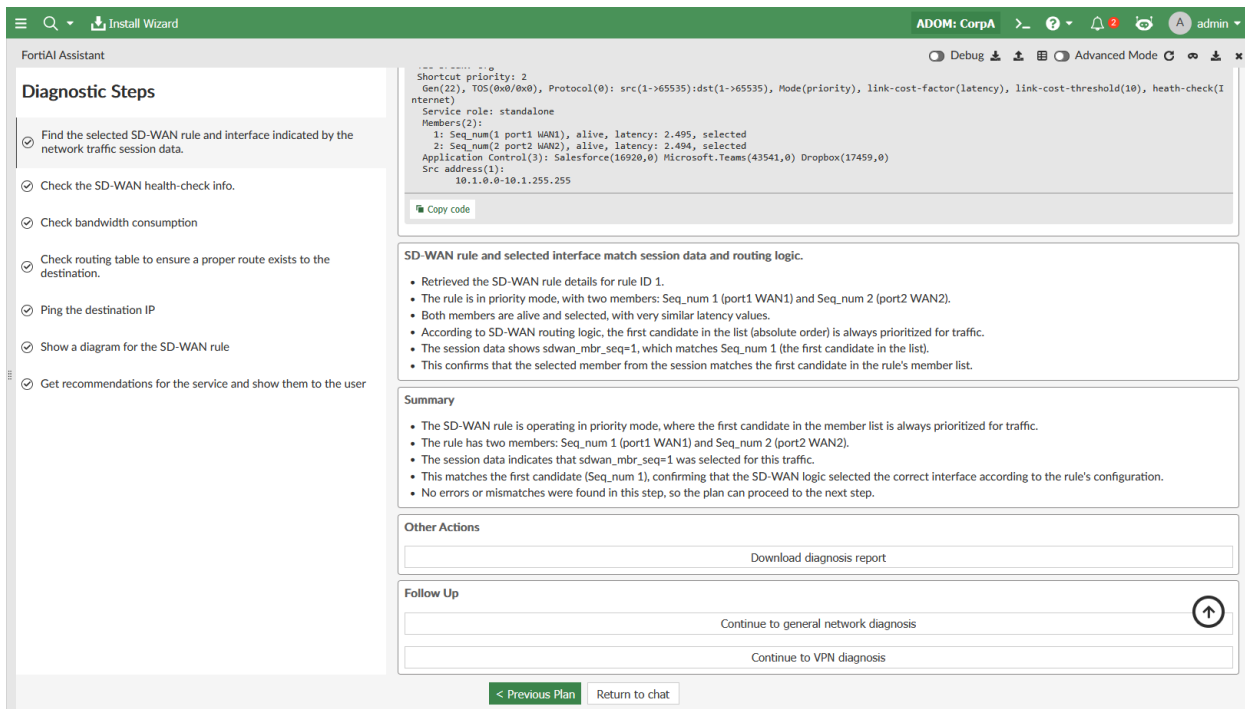
1. FortiAI can be asked to diagnose slow network traffic between a user's IP and applications like Salesforce.
2. FortiAI lists the diagnostic steps that it will follow in order to determine necessary information about the request.

For example, when diagnosing slow network to Salesforce from an internal IP address:

- FortiAI will determine the destination IP address for Salesforce using the SD-WAN internet services app list.
- FortiAI will check if there is an active SD-WAN session between the source and destination IP address.
- FortiAI will prompt the user to select the SD-WAN session for further diagnosis.



3. Once the SD-WAN session is confirmed, FortiAI will continue to diagnose the issue.



4. After the issue has been diagnosed, FortiAI will provide the administrator with its observations, recommendations, and a summary.

Example 2: Network slow between IP 10.1.1.10 to YouTube

1. FortiAI can be asked to diagnose slow network traffic between a user's IP and applications like YouTube.

The screenshot displays the FortiAI interface with several components:

- Network Monitor:** Shows a 'Network Monitor' tab with a dropdown for 'Br1[root]' and a date range of '12-18-2'. Below this is a table of SD-WAN Rules.
- SD-WAN Rules Table:**

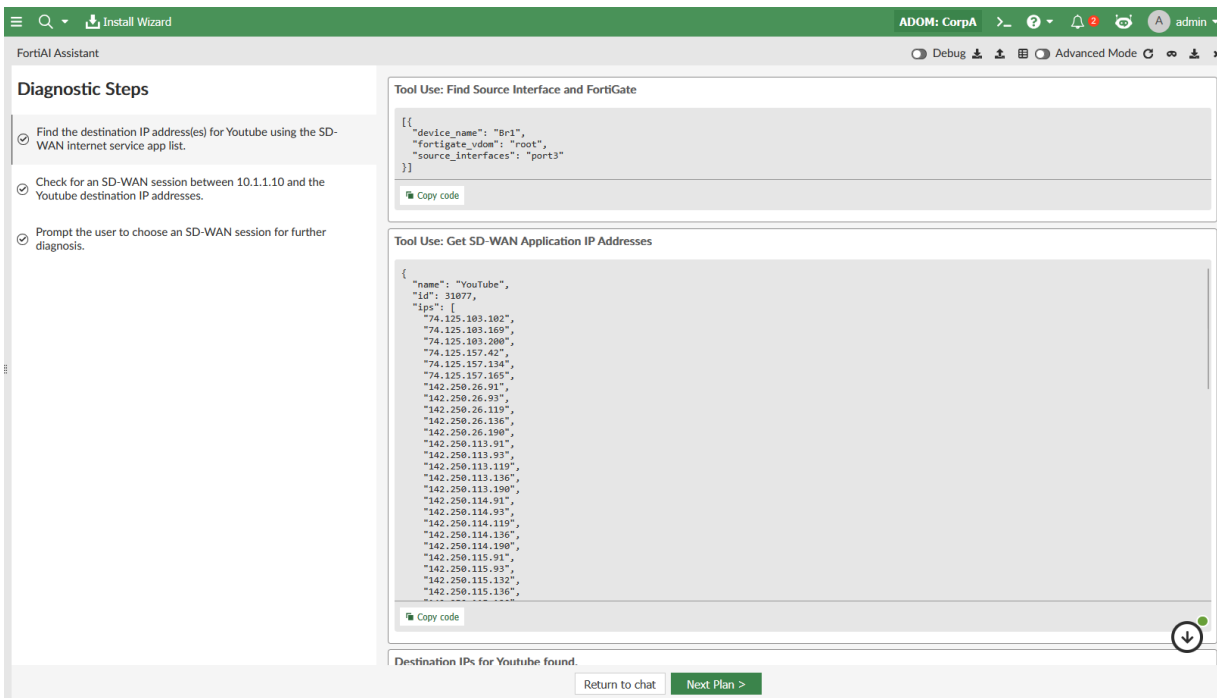
ID	Name	Source
1	Critical_DIA	Branch-LAN
2	Critical_Video	Branch-LAN
3	Cloud_VoIP	Branch-LAN
4	Business_Applications	Branch-LAN
5	Corporate_Traffic	Branch-LAN
6	Cloud_Application	Branch-LAN
7	PING_Test_DIA	Branch-LAN
8	Non_Critical_DIA	Branch-LAN
- FortiAI Assistant:** A chat window on the right side of the interface. It contains a user message: "network slow from 10.1.1.10 to Youtube , can you help to check?". Below this is a "Completed Plan" section with three steps:
 - Find the destination IP address(es) for Youtube using the SD-WAN internet service app list.
 - Check for an SD-WAN session between 10.1.1.10 and the Youtube destination IP addresses.
 - Prompt the user to choose an SD-WAN session for further diagnosis.
 There are buttons for "View details" and "Download diagnosis report". Below the plan is a "Selected session" section with a code block:


```
1. session info: proto=6 proto_state=11 duration=26
9 expire=3595 timeout=3600 refresh_dir=both flags=0
00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=
0/255
```

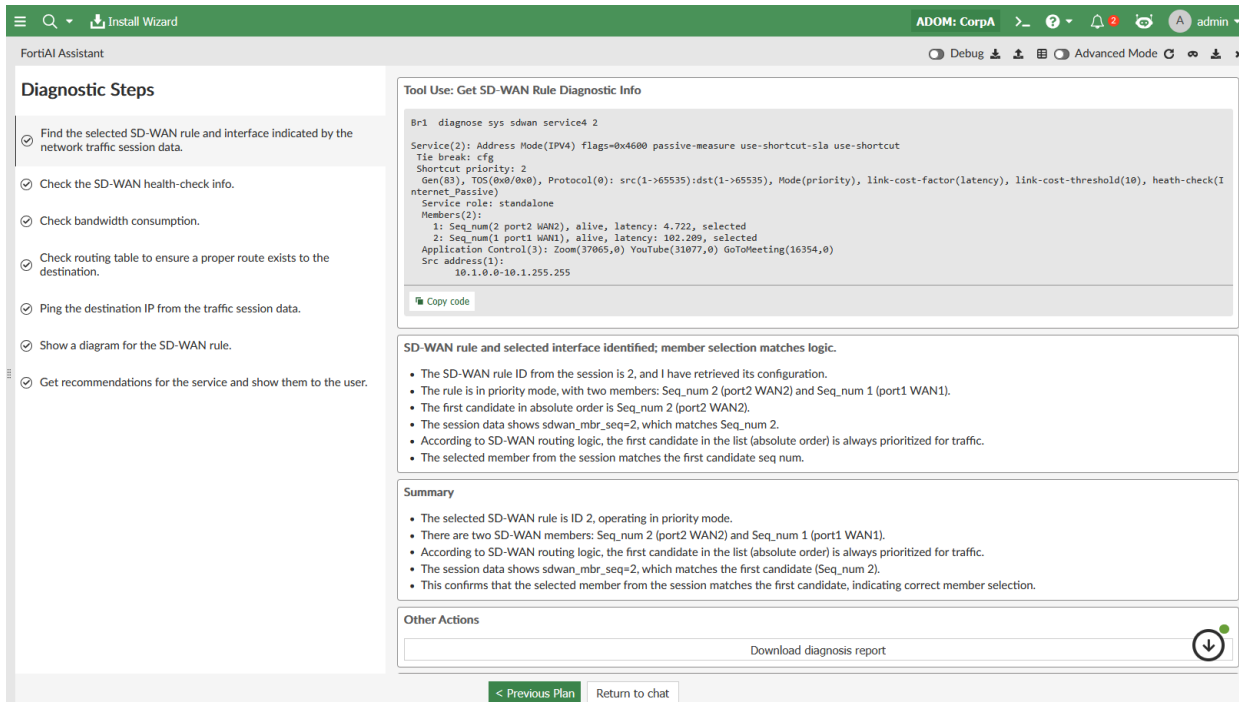
2. FortiAI lists the diagnostic steps that it will follow in order to determine necessary information about the request.

For example, when diagnosing slow network to YouTube from an internal IP address:

- FortiAI will determine the destination IP address for YouTube using the SD-WAN internet services app list.
- FortiAI will check if there is an active SD-WAN session between the source and destination IP address.
- FortiAI will prompt the user to select the SD-WAN session for further diagnosis.



3. Once the SD-WAN session is confirmed, FortiAI will continue to diagnose the issue.



4. After the issue has been diagnosed, FortiAI will provide the administrator with its observations and recommendations. A summary of the diagnosis results is provided to the administrator.

Example 3: Network slow between IP 10.1.1.10 to 10.1.2.10

1. FortiAI can be asked to diagnose slow network traffic between a user's IP and internal IPs like 10.1.2.10.

The screenshot displays the FortiAI dashboard with a chat window on the right. The chat window shows a user asking for help with slow network traffic between IP 10.1.1.10 and 10.1.2.10. The chat interface shows a 'Completed Plan' with two steps: 'Check for SD-WAN session between 10.1.1.10 and 10.1.2.10.' and 'Prompt user to choose an SD-WAN session for further diagnosis.' Below the plan, there is a 'Selected session' section containing a JSON-like diagnostic output.

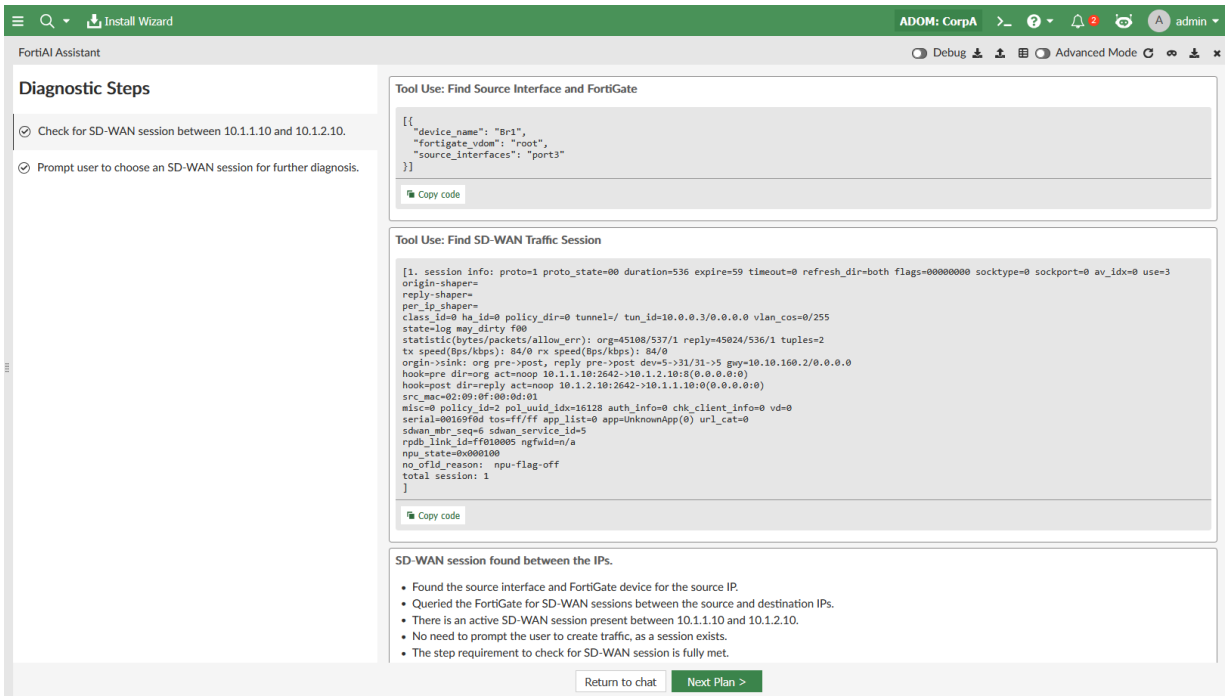
Interface	Upload	Download
Br1[root] (10)		
Cloud-VPN1	4.64 Kbps/0 bps	13.59 Kbps/0 bps
Cloud-VPN2	6.89 Kbps/0 bps	19.57 Kbps/0 bps
HUB1-VPN1	738 bps/0 bps	741 bps/0 bps
HUB1-VPN1_0	7.05 Mbps/0 bps	7.05 Mbps/0 bps
HUB1-VPN2	1.3 Kbps/0 bps	1.31 Kbps/0 bps
HUB2-VPN1	685 bps/0 bps	688 bps/0 bps
HUB2-VPN2	689 bps/0 bps	704 bps/0 bps
HUB2-VPN2_0	3.97 Kbps/0 bps	3.83 Kbps/0 bps
WAN1 (port1)	20.25 Kbps/0 bps	28.37 Kbps/0 bps
WAN2 (port2)	44.43 Kbps/0 bps	385.44 Kbps/0 bps
Br2[root] (10)		
Cloud-VPN1	898 bps/0 bps	648 bps/0 bps

```
hook=pre dir=org act=noop 10.1.1.10:2642->10.1.2.10:2642
hook=post dir=reply act=noop 10.1.2.10:2642->10.1.1.10:2642
src_mac=02:09:0f:00:0d:01
misc=0 policy_id=2 pol_uid_idx=16128 auth_info=0 c
hk_client_info=0 vd=0
serial=00169f0d tos=ffff app_list=0 app=UnknownApp
(0) url_cat=0
sdwan_mbr_seq=6 sdwan_service_id=5
rpdn_link_id=ff010005 ngfwid=n/a
npu_state=0x000100
no_ofld_reason= npu-flag-off
```

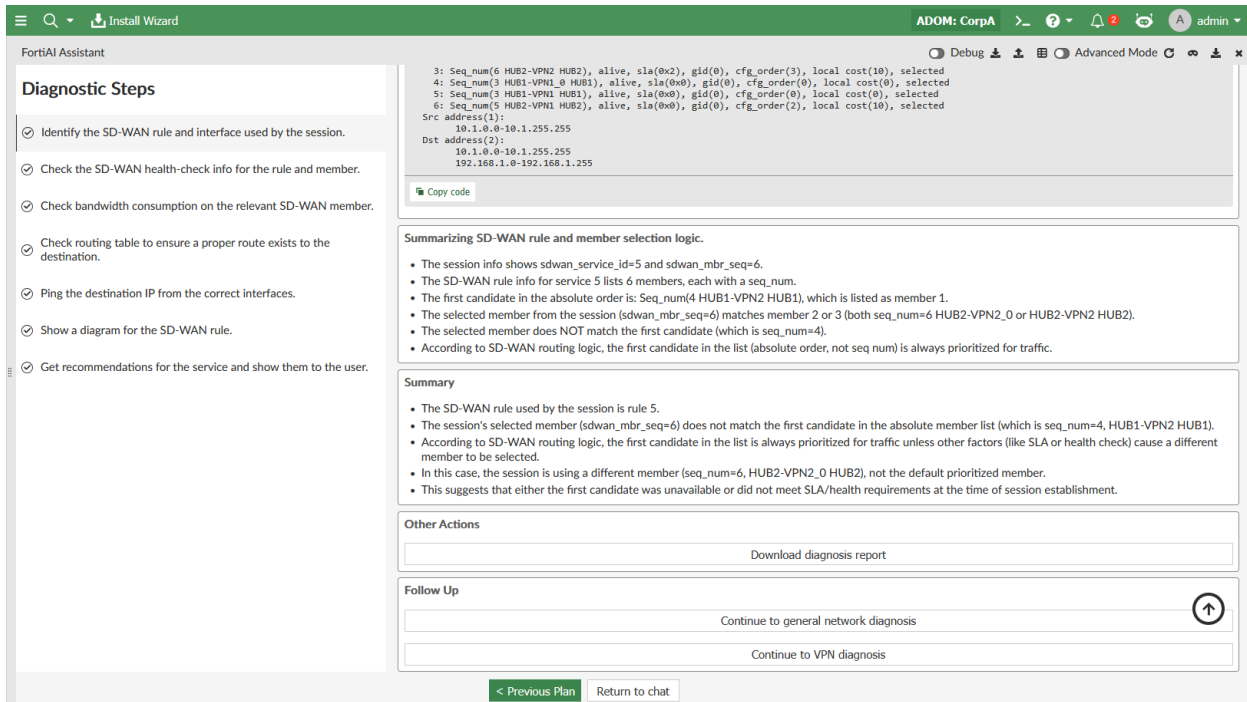
2. FortiAI lists the diagnostic steps that it will follow in order to determine necessary information about the request.

For example, when diagnosing slow network to an internal IP address from an internal IP address:

- FortiAI will check if there is an active SD-WAN session between the source and destination IP address.
- FortiAI will prompt the user to select the SD-WAN session for further diagnosis.



3. Once the SD-WAN session is confirmed, FortiAI will continue to diagnose the issue.



4. After the issue has been diagnosed, FortiAI will provide the administrator with its observations and recommendations. A summary of the diagnosis results is provided to the administrator.

Example 4: Network slow between IP 10.1.1.10 and cloud server 172.20.1.10

1. FortiAI can be asked to diagnose slow network traffic between a user's IP and cloud servers (e.g. IP 172.20.1.10).

The screenshot displays the FortiManager v8.0.0 interface. On the left, the navigation menu includes sections like Device Manager, Monitors, Policy & Objects, SD-WAN Manager, and FortiAI. The main area shows the SD-WAN Monitor for 'Br1' with a 'Table View' of SD-WAN Rules. The FortiAI Assistant chat window is open on the right, showing a user query and a 'Completed Plan' with diagnostic steps.

SD-WAN Rules Table:

ID	Name	Source
1	Critical_DIA	Branch-LAN
2	Critical_Video	Branch-LAN
3	Cloud_VoIP	Branch-LAN
4	Business_Applications	Branch-LAN
5	Corporate_Traffic	Branch-LAN
6	Cloud_Application	Branch-LAN
7	PING_Test_DIA	Branch-LAN
8	Non_Critical_DIA	Branch-LAN

FortiAI Assistant Chat:

Hi admin. How can I help you?

network slow from 10.1.1.10 to Cloud server 172.20.1.10, can you help to check?

Completed Plan

- Check if there is an active SD-WAN session between 10.1.1.10 and 172.20.1.10.
- Prompt the user to choose an SD-WAN session for further diagnosis.

Selected session

```
hook-pre dir=reply act=dnat 172.20.1.10:22759->10.1.1.10:22759
hook-post dir=reply act=noop 172.20.1.10:22759->10.1.1.10:0(0.0.0.0)
src_mac=02:09:0f:00:0d:01
misc= policy_id=1 pol_uid_id=16127 auth_info=0 c
hk_client_info=0 vd=0
serial=000b494c tos=fff app_list=2000 app=Ping ur
l_cat=0
sdwan_mbr_seq=2 sdwan_service_id=0
rpdb_link_id=ff000008 ngfwid=na
```

2. FortiAI lists the diagnostic steps that it will follow in order to determine necessary information about the request.

For example, when diagnosing slow network to a cloud server from an internal IP address:

- FortiAI will check if there is an active SD-WAN session between the source and destination IP address.
- FortiAI will prompt the user to select the SD-WAN session for further diagnosis.

The screenshot shows the FortiAI Assistant interface with the following content:

- Diagnostic Steps:**
 - Check if there is an active SD-WAN session between 10.1.1.10 and 172.20.1.10.
 - Prompt the user to choose an SD-WAN session for further diagnosis.
- Tool Use: Find Source Interface and FortiGate**

```
[[
  "device_name": "Br1",
  "fortigate_vdom": "root",
  "source_interfaces": "port3"
]]
```
- Tool Use: Find SD-WAN Traffic Session**

```
[1. session info: proto=1 proto_state=00 duration=4807 expire=59 timeout=0 refresh_dir=both flags=00000000 socket=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty f00 app_valld
statistic(bytes/packets/allow_err): org=396816/4724/1 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 82/0 rx speed(Bps/kbps): 0/0
origin->link: org pre->post, reply pre->post dev=5->4/4->5 gwy=10.198.2.1/0.0.0.0
hook=pre dir=org act=snat 10.1.1.10:22759->172.20.1.10:8(10.198.2.2:22759)
hook=pre dir=reply act=dnat 172.20.1.10:22759->10.198.2.2:8(10.1.1.10:22759)
hook=post dir=reply act=noop 172.20.1.10:22759->10.1.1.10:8(0.0.0.0:0)
src_mac=02:89:19f:00:8d:01
misc=0 policy_id=1 pol_uid_idx=16127 auth_info=0 chk_client_info=0 vd=0
serial=000b494c tos=ffff app_list=2000 app=ping ur_lcat=0
sdwan_mbr_seq=2 sdwan_service_id=8
rpbk_link_id=ff000000 ngfwid=n/a
npu_state=0x001108
no_ofld_reason: npu-flag-off
total session: 1
]
```
- Active SD-WAN session found between the source and destination.**
 - Found the FortiGate device (Br1) and VDOM (root) for the source IP.
 - Queried for SD-WAN sessions between 10.1.1.10 and 172.20.1.10.
 - An active SD-WAN session exists with relevant session details.
 - The requirement to check for an active SD-WAN session is satisfied.

3. Once the SD-WAN session is confirmed, FortiAI will continue to diagnose the issue.

The screenshot shows the FortiAI Assistant interface with the following content:

- Diagnostic Steps:**
 - Find the selected SD-WAN rule and interface indicated by the network traffic session data.
 - Check the SD-WAN health-check info.
 - Check bandwidth consumption.
 - Check routing table to ensure a proper route exists to the destination.
 - Ping the destination IP.
 - Show a diagram for the SD-WAN rule.
 - Get recommendations for the service and show them to the user.
- Tool Use: Get SD-WAN Rule Diagnostic Info**

```
Br1 diagnose sys sdwan service4 8
Service(8): Address Mode(IPv4) Flags=0x4200 use-shortcut-sla use-shortcut
Tie break: cfg
Shortcut priority: 2
Gen(32), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
Service role: standalone
Members(1):
  1: Seq_num(2 port2 WAN2), alive, selected
Src address(1):
  10.1.0.0-10.1.255.255
Dst address(3):
  192.168.0.0-192.168.255.255
  172.16.0.0-172.31.255.255
  10.0.0.0-10.255.255.255
```
- Summarize SD-WAN rule info and member selection logic.**
 - Retrieved SD-WAN rule info for rule ID 8.
 - Rule is in manual mode, with one member: Seq_num 2 (port2 WAN2), which is alive and selected.
 - The session data shows sdwan_mbr_seq=2, which matches the only member (Seq_num 2).
 - According to SD-WAN routing logic, the first candidate in the list (absolute order) is always prioritized for traffic.
 - In this case, there is only one candidate, so it is both the first and the selected member.
- Summary**
 - The SD-WAN rule identified is rule 8, operating in manual mode.
 - There is only one member for this rule: Seq_num 2 (port2 WAN2), which is alive and currently selected.
 - The session data confirms that sdwan_mbr_seq=2, which matches the first (and only) candidate in the SD-WAN rule member list.
 - According to SD-WAN routing logic, the first candidate in the list (absolute order) is always prioritized for traffic.
 - In this scenario, the selected member does match the first candidate, so the SD-WAN selection is correct and expected.
- Other Actions**
 - Download diagnosis report

4. After the issue has been diagnosed, FortiAI will provide the administrator with its observations and recommendations. A summary of the diagnosis results is provided to the administrator.

System

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

- [Others on page 110](#)

Others

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

- [Legal third party disclosure panel on page 110](#)
- [Custom session labels in FortiManager event logs on page 112](#)

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 FortiManager, 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.

The screenshot displays the FortiManager GUI interface. The top navigation bar shows the user 'admin' and the system name 'ADOM: 76ADOM'. The left sidebar contains various management sections like Dashboard, Device Manager, Policy & Objects, SD-WAN Manager, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, FortiGuard, and System Settings. The main content area is divided into several panels:

- System Information:** Displays host details such as Host Name (FMG-VM64-KVM), Serial Number, Platform Type (FMG-VM64-KVM), HA Status (Standalone), System Time (Thu Feb 19 15:15:50 2026 PST), Firmware Version (v8.0.0 build0063 (Interim)), System Configuration (Last Backup: N/A), Current Admin (admin / 1 in total), and Up Time (2 minutes 24 seconds).
- License Information:** Shows VM License (Valid UUG), FortiCare Subscription (Registered), FortiGuard status (Not Licensed), Management (2 / 10,000 (0.0%) Devices, 1 Used / 10,000 Total ADOMs), and FortiGate (2).
- System Resources:** Features two progress indicators: Average CPU Usage at 16% and Memory Usage at 21% (2.1 GB / 9.6 GB).
- Unit Operation:** Displays a Fortinet logo and a grid of 12 device status icons.
- Alert Message Console:** A table listing system events with columns for Time and Message.
- Connectivity:** A donut chart showing 3 Devices, with a legend for Model Device and Connection Up.

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

The screenshot shows the FortiManager interface for a device named 'FMG-VM64-KVM'. The 'Included Third Party Software' section is active, displaying a table of installed software. An 'Export' dropdown menu is open, showing options for CSV, JSON, and CycloneDX SBOM JSON. A 'MIT License' dialog box is overlaid on the table, containing the following text:

MIT License
Copyright (c) 2020 A Beautiful Site, LLC

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

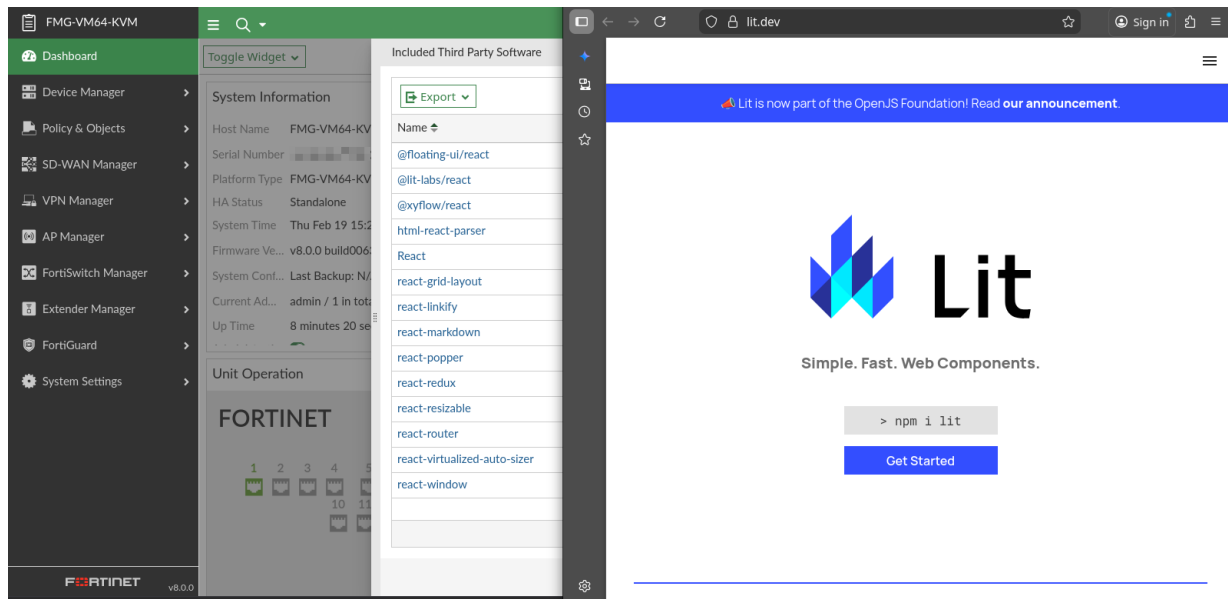
Name	Version	License
3ware-9550sx-u-firmware	2.26	
@dagrejs/dagre	1.1.4	
@dnd-kit/core	6.1.0	
@floating-ui/react	0.27	
@leeoniya/ufuzzy	1.0.1	
@lit-labs/react	1.2.1	
@popperjs/core	2.11	
@reduxjs/toolkit	1.9.7	
@shoelace-style/animations	1.2.0	MIT License
@shoelace-style/shoelace	2.0.0-beta.13	MIT License
@trylona/ts-result	1.0.1	MIT License
@xyflow/react	12.3.6	MIT License
Apache HTTP Server	2.4.25	Apache License 2.0
app-datepicker	4.5.3	MIT License
argparse	2.0.1	Python License 2.0

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

The screenshot shows the FortiManager interface for a device named 'FMG-VM64-KVM'. The 'Included Third Party Software' section is active, displaying a table of installed software. The 'Export' dropdown menu is open, showing options for CSV, JSON, and CycloneDX SBOM JSON. A search bar is visible above the table.

Name	Version	License
CSV		
JSON	2.26.02.007	GNU General Public License v2.0 only
CycloneDX SBOM JSON	1.1.4	MIT License
@dnd-kit/core	6.1.0	MIT License
@floating-ui/react	0.27.16	MIT License
@leeoniya/ufuzzy	1.0.14	MIT License
@lit-labs/react	1.2.1	BSD 3-Clause "New" or "Revised" License
@popperjs/core	2.11.8	MIT License
@reduxjs/toolkit	1.9.7	MIT License
@shoelace-style/animations	1.2.0	MIT License
@shoelace-style/shoelace	2.0.0-beta.13	MIT License
@trylona/ts-result	1.0.1	MIT License
@xyflow/react	12.3.6	MIT License
Apache HTTP Server	2.4.25	Apache License 2.0
app-datepicker	4.5.3	MIT License
argparse	2.0.1	Python License 2.0

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



Custom session labels in FortiManager event logs

FortiManager 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 FortiManager 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.

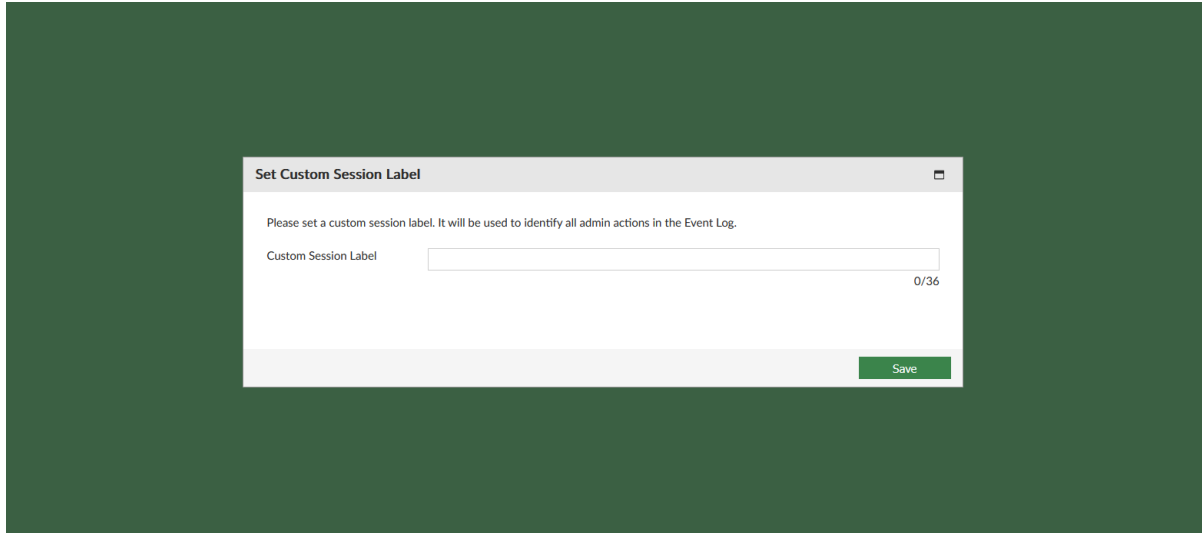
To use custom session labels:

1. Enable custom session labels in the FortiManager CLI:

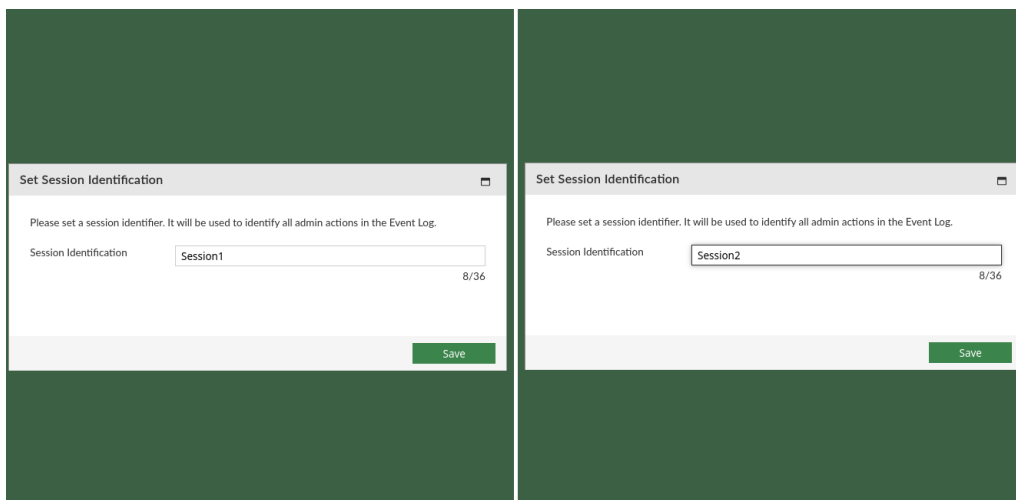
```
config system admin setting
  set custom-session-label enable
  set custom-session-label-mode {changeable | unique-per-session}
end
```

2. Log in to the FortiManager GUI.

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



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.

User Name	Profile	IP Address	Current ADOM	Custom Session Label	Start Time
F admin (Current)	Super_User	GUI(10.100.55.254)	76ADOM	Session 1	Fri Mar 27 12:...
F admin	Super_User	GUI(10.100.55.254)	76ADOM	Session 2	Fri Mar 27 13:...

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

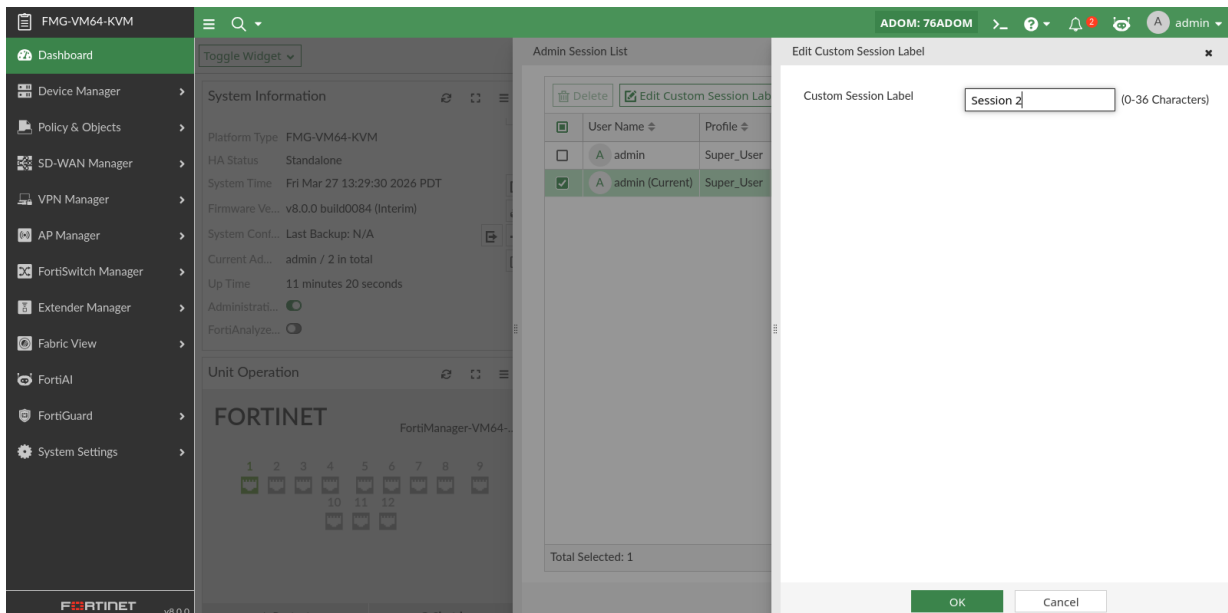
#	Date Time	Level	User	Sub Type	ADOM	Description	Custom Session Label
1	2026-03-27 13:26:06	information	A admin	Device manager event		Device Manager dvm log ...	Session 2
2	2026-03-27 13:25:58	information	A admin	Device manager event	root	Device Manager dvm log ...	
3	2026-03-27 13:25:58	information	A admin	System manager event	root	User login/logout successf...	
4	2026-03-27 13:23:40	information	A admin	Device manager event		Device Manager dvm log ...	Session 1
5	2026-03-27 13:23:29	information	A admin	Device manager event	root	Device Manager dvm log ...	
6	2026-03-27 13:23:29	information	A admin	System manager event	root	User login/logout successf...	
7	2026-03-27 13:23:27	information	A admin	System manager event	76ADOM	User login/logout successf...	
8	2026-03-27 13:23:25	information	A admin	System manager event		User login/logout successf...	
9	2026-03-27 13:23:23	notice	A admin	System manager event		CLI execution info	
10	2026-03-27 13:23:16	information	A admin	System manager event		User login/logout successf...	
11	2026-03-27 13:23:14	information	A admin	Device manager event		Device Manager dvm log ...	
12	2026-03-27 13:23:13	information	A admin	Device manager event	root	Device Manager dvm log ...	
13	2026-03-27 13:23:13	information	A admin	System manager event	root	User login/logout successf...	
14	2026-03-27 13:23:10	information	A admin	System manager event	76ADOM	User login/logout successf...	

Change an active custom session label

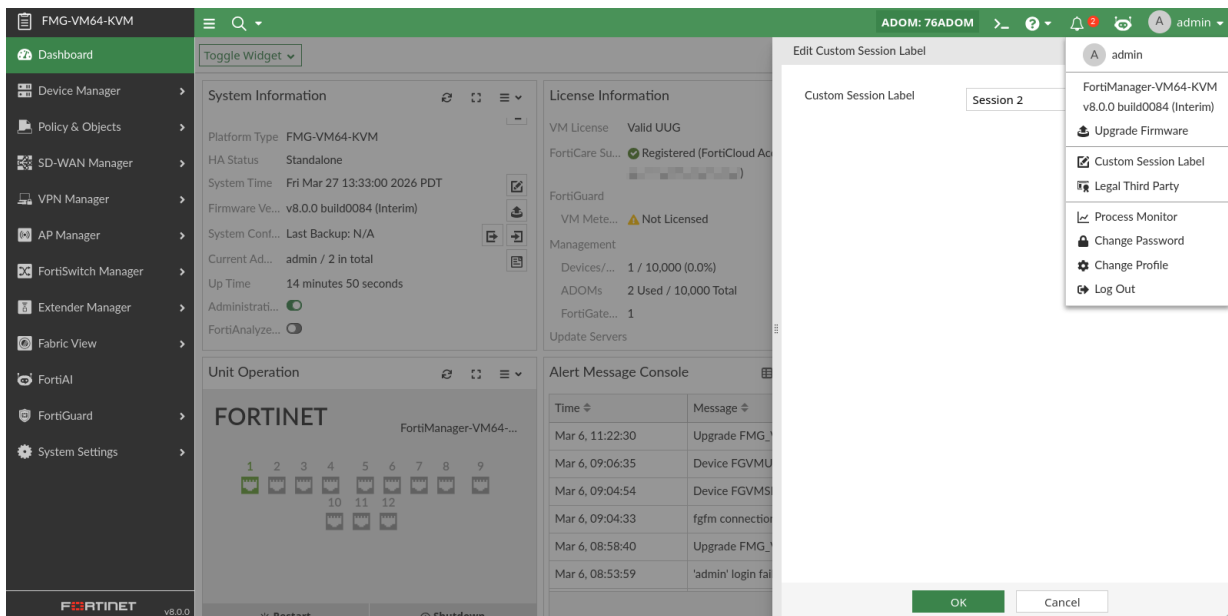
When changeable mode is enabled, administrators can change their custom session label during an active session using one of the following methods.

To change an active session's label:

- 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*.

Index

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

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

- [8.0.0 on page 116](#)

8.0.0

Device Manager

- | | |
|-----------|---|
| Templates | <ul style="list-style-type: none"> • Local certificates lifecycle management (set validity and renew) and expiry notification alerts on page 7 |
|-----------|---|

Central Management

- | | |
|---------------------|--|
| FortiSwitch Manager | <ul style="list-style-type: none"> • FortiSwitch Template adds override option to modify specific port settings on selected devices on page 15 |
| Other enhancements | <ul style="list-style-type: none"> • Workspace Mode supports onboarding new devices and creating new policy packages without ADOM lock on page 19 • Interface-based bandwidth graph uses average bandwidth logic on page 22 • FortiSwitch, FortiAP and FortiExtender templates can be assigned from Fabric Authorization Template on page 23 • Certificate templates can be selected in model device, model HA device, and device blueprint configurations on page 25 • New workflow mode design to control individual admin sessions with selective approvals on page 30 • Factory default IPsec template to configure FortiClient VPN on page 33 • Central monitoring dashboard for Firewall Users with filters for authentication method and user group on page 35 • Maximum length of meta variables value increased to 32768 characters on page 39 • Admin profile adds granular control on device manager (Interface, Log & Report, Security Fabric) and Routing on page 41 • pxGrid connector is enhanced to display Device Type and Session State on page 44 |

- Managing FortiGate registration to FortiCare on page 47
- Enhanced asset details and identity monitoring on page 49
- Administrators can create protected objects on page 61
- FortiManager supports downgrade and roll-back for FortiGuard packages to allow setting a preferred package version for devices on page 66
- FortiManager supports importing password-type objects from FortiGate devices with private data encryption on page 69

Policy and Objects

Policy

- Local In policies are supported in the Global ADOM and in policy blocks on page 71

Fabric View

Connectors

- New external connectors: GuardiCore, Microsoft Azure (Proxy Mode), and Application Centric Infrastructure (ACI Proxy Mode) on page 82.
- FortiAIOps connector on page 87
- Central management for ACI features on page 98

FortiAI

FortiAI

- FortiAI can diagnose, troubleshoot, and remediate slow access to cloud or on-premise servers and applications on page 101

System

Other enhancements

- Legal third party disclosure panel on page 110



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.