



Examples

FortiManager 7.4.0



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



February 27, 2024

FortiManager 7.4.0 Examples

02-740-909880-20240227

TABLE OF CONTENTS

Change Log	5
Introduction	6
Device Manager	7
Exporting a policy package from one FortiManager to another	7
VPN Manager	9
Configuring a full mesh VPN topology within a VPN console	9
System Settings	15
Configuring and debugging FortiManager HA clusters	15
Configuring the primary FortiManager unit in an HA cluster	15
Configuring backup FortiManager units in an HA cluster	16
Generating and downloading HA debug logs	16
Creating administrator accounts with restricted access	17
Restricting administrator access to ADOMs	17
Restricting administrator access to device groups	19
Restricting administrator access to policy packages	20
Certificate deployment	22
Configuring FortiManager to deploy certificates for admin GUI access	22
Creating the certificate for administrator web access	22
Uploading the certificate to FortiManager	24
Apply the certificate to the FortiGate in FortiManager	24
Install the certificate	24
Verify the certificate was installed correctly	25
Configuring FortiManager to deploy certificates for deep inspection	25
Generate a CA certificate on FortiAuthenticator	25
Generate an intermediate CA certificate	26
Upload the intermediate CA certificate to FortiManager	26
Use the certificate in a policy and install the Policy Package	27
Verify on an endpoint	27
Configuring FortiManager to deploy SAML certificates	28
Create a local CA on the FortiAuthenticator	28
Create the Identity Provider (IdP) certificate used in SAML	30
Create the IdP portal on FortiAuthenticator	30
Allowing IdP service on FortiAuthenticator	31
Defining a local user on the FortiAuthenticator	32
Defining SAML SP settings on FortiManager	32
IdP portal SP settings continued	33
Testing the configuration	33
Using FortiManager to provision the SAML certificates to FortiGates	34
Configure FortiManager to install SAML configuration on the FortiGate	35
Testing the configuration	37
Configuring FortiManager and FortiAuthenticator for SCEP certificate deployment	38
Configuring FortiAuthenticator	38
Configuring FortiManager	41
Verification of certificate deployment	44

Others	48
Managing FortiAnalyzer from FortiManager	48
Adding FortiAnalyzer to FortiManager	48
Viewing managed FortiAnalyzer behavior	52
Centrally configuring FortiGate to send logs to managed FortiAnalyzer	53
Viewing logs and reports for managed FortiAnalyzer units	53
Managing multiple FortiAnalyzer units	54
Troubleshooting managed FortiAnalyzer units	55
Creating a third party blocklist provider workflow	56

Change Log

Date	Change Description
2023-05-15	Initial release.
2024-02-27	Added: <ul style="list-style-type: none">• Configuring FortiManager to deploy certificates for admin GUI access on page 22• Configuring FortiManager to deploy certificates for deep inspection on page 25• Configuring FortiManager to deploy SAML certificates on page 28• Configuring FortiManager and FortiAuthenticator for SCEP certificate deployment on page 38

Introduction

This document serves as a reference guide to common FortiManager 7.4 configuration and deployment scenarios. The scope of this document is to explain specific examples and include information required for those examples to work. The examples rely on the other documents to provide full product information.



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Docs Library](#).

This section includes configuration examples for FortiManager 7.4:

- [Device Manager on page 7](#)
- [VPN Manager on page 9](#)
- [System Settings on page 15](#)
- [Certificate deployment on page 22](#)
- [Others on page 48](#)

Device Manager

This section contains the following topics:

- [Exporting a policy package from one FortiManager to another](#) on page 7

Exporting a policy package from one FortiManager to another

In this example, you will learn how to export a policy package from one FortiManager to another FortiManager.

To export a policy package from one FortiManager to another FortiManager:

1. Select a FortiManager policy package and installation target you want to export:
 - a. Select a FortiManager policy package and its installation target.
For example,
Policy Package: PP_001
Installation Target: Device1
2. Download the latest revision:
 - a. Go to *Device Manager > Device & Groups >* and double-click the installation target device (Device1 in this example).
 - b. Go to *Dashboard > Configuration and Installation > Total Revisions*.
 - c. Download the latest revision (for example, Revision 1).
3. Add the device to the second FortiManager:
 - a. Go to your second FortiManager.
 - b. Go to *Device Manager > Device & Groups >* and click *Add Device*. The Add Device wizard displays.
Its SN must be similar to the one you got the revision from. It can be the same as the original SN, or you can take the SN prefix (the first six characters) and append 10 digits to it.
For example, FG200D12345985242 is the original SN.
Prefix: FG200D
Appended 10 Digits: 0000000001
The new SN will be: FG200D0000000001.
 - c. Select *Add Model Device* and complete the wizard.
4. Import the revision to the second FortiManager:
 - a. On your second FortiManager device, go to *Device Manager > Device & Groups* and double-click the model device. The Device Dashboard displays.
 - b. Go to *Dashboard > Configuration and Installation > Total Revisions*.
 - c. Right-click the empty revision list and select *Import Revision > Revision 1*.
 - d. Go to *Device Manager > Device & Groups*.
 - e. Right-click your model device and select *Import Policy*. The wizard displays.

- f. Complete the wizard.
- g. Go to *Policy & Objects*. The policy package and its used objects are displayed.



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Document Library](#).

VPN Manager

This section contains the following topics:

- [Configuring a full mesh VPN topology within a VPN console on page 9](#)

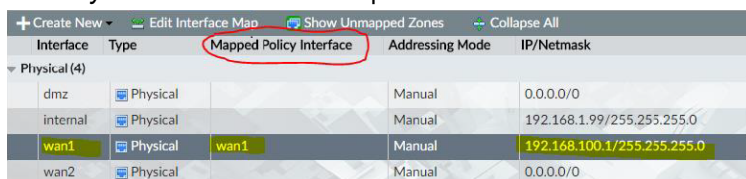
Configuring a full mesh VPN topology within a VPN console

This is an example on how to configure a simple full mesh VPN with:

- Three FortiGate (FGT) devices
- A pre-shared key for authentication
- An auto-up tunnel setting
- Static routes

To configure a full mesh VPN topology within a VPN console:

1. Add FortiGate devices and map all interfaces:
 - a. Go to *Device Manager*. Add three FortiGate devices by clicking *Add Device*. Follow the wizard to add each device.
 - b. Go to *Policy & Objects > Policy Packages* and define the *Zone* interfaces.
 - c. Go to *Device Manager* and select a device.
 - d. Go to *System > Interface* and map the interfaces to the *Zone* interfaces.



Interface	Type	Mapped Policy Interface	Addressing Mode	IP/Netmask
Physical (4)				
dmz	Physical		Manual	0.0.0.0/0
internal	Physical		Manual	192.168.1.99/255.255.255.0
wan1	Physical	wan1	Manual	192.168.100.1/255.255.255.0
wan2	Physical		Manual	0.0.0.0/0

2. Create firewall addresses for protected subnets:
 - a. Go to *Policy & Objects > Firewall Objects > Address* to manage the firewall addresses.
 - b. VPNs only support firewall addresses with the type set to *subnet (IP/Netmask)*. The firewall addresses will be used as protected subnets to generate static routes among the FortiGate devices.
3. Create a VPN community:
 - a. Go to *VPN Manager > IPsec VPN Communities > Create New*.
 - b. Set the *VPN Topology* type to *Site to Site*.
 - c. Define the *Authentication* method with a *Pre-shared Key*.

d. Specify the encryption and hash methods.

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication: Certificates **Pre-shared Key**

☐ Generate(random)
☒ Specify

Encryption

IKE Security (Phase 1) Properties

1-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA-1"/>	+
2-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="MD5"/>	+

IPsec Security (Phase 2) Properties

1-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA-1"/>	+
2-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="MD5"/>	+

< Back Next > Cancel

e. After defining the authentication methods and encryption properties, click *Next*.**f. Configure the *VPN Phase 1* and *Phase 2* settings.**

VPN Topology Setup Wizard

VPN Zone: ON

☒ Create Default Zones
☐ Use Custom Zone

IKE Security Phase 1 Advanced Properties

Diffie Hellman Group(s): ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Exchange Mode: ☐ Aggressive ☒ Main(ID Protection)

Key Life: (120-172800 seconds)

Dead Peer Detection: ON

IPsec Security Phase 2 Advanced Properties

Diffie Hellman Group(s): ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Replay Detection: ON

Perfect Forward: ON

< Back Next > Cancel

- g. For the *IPSec Phase 2* setting, set the tunnel to *Auto-Negotiate*.

VPN Topology Setup Wizard

IPsec Security Phase 2 Advanced Properties

Diffie Hellman Group(s) ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Replay Detection ☒ ON

Perfect Forward Secrecy(PFS) ☒ ON

Key Life ☒ Seconds ☐ KB ☐ Both
 1800 seconds 5120 KB

Autokey Keep Alive ☒ ON

Auto-Negotiate ☐ OFF

NAT-traversal ☒ Enable ☐ Disable ☐ Forced

Keep Alive Frequency 10 (10-900 seconds)

Advanced Options >

< Back Next > Cancel

VPN configuration summary:

Name Full

Description test full mesh

Topology ☒ Full Meshed

Authentication Certificates Pre-shared Key
☐ Generate(random)
☒ Specify

Encryption

IKE Security (Phase 1) Properties

1-Encryption	DES	Authentication	SHA-1	+ -
2-Encryption	DES	Authentication	MD5	+ -

IPsec Security (Phase 2) Properties

1-Encryption	DES	Authentication	SHA-1	+ -
2-Encryption	DES	Authentication	MD5	+ -

VPN Zone ☒ ON
☒ Create Default Zones
☐ Use Custom Zone


IKE Security Phase 1 Advanced Properties


Diffie Hellman Group(s) ☒ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21


4. Add a VPN gateway:
- Go to *VPN Manager > IPsec VPN Communities* and select your VPN community.
 - Right-click the community and select *Add Managed Gateway*.


- c. Add a *Protected Network*. There can be more than one protected networks.


VPN Gateway Setup Wizard - ☒ Full


Protected Network


Device


Default VPN Interface



Local Gateway



Advanced


Protected Subnet


prosub

IP/Netmask:172.19.100.104/255.255.2...

 prosub-172.19.100.2
IP/Netmask:172.19.100.2/255.255.255...

 prosub-172.19.100.3
IP/Netmask:172.19.100.3/255.255.255...

 prosub-172.19.100.4
IP/Netmask:172.19.100.4/255.255.255...

 prosub-172.19.100.5


< Back


Next >


Cancel


- d. Select a *Device*.


VPN Gateway Setup Wizard - ☒ Full


Protected Network


Device


Default VPN Interface


Local Gateway


Advanced

Device

FGT-168-100-100[root]






< Back

Next >

Cancel

- e. Select a *Default VPN Interface*. The default VPN interface should have a valid IP and be mapped.

VPN Gateway Setup Wizard - ☒ Full






    

Protected Network Device **Default VPN Interface** Local Gateway Advanced

Default VPN Interface

- i. Optionally, specify the *Local Gateway*. This option can be left blank in most cases.

VPN Gateway Setup Wizard - ☒ Full

Protected Network Device Default VPN Interface **Local Gateway** Advanced

Local Gateway

- f. Go to *Routing* and select *Automatic* to generate static routes.

VPN Gateway Setup Wizard - ☒ Full

Routing

☐ Manual (via Device Manager)
☒ Automatic

Local ID

Advanced Options ▾

authpasswd

authusr

banner

dns-mode

domain

public-ip

route-overlap

- i. If *Manual* is selected, go to the *Device Manager* to set the IP on the relevant IPSec interfaces and define the routings manually.

VPN gateway configuration settings summary:

Edit Gateway

Protected Subnet	prosub-172.19.100.1
Device	FGT-168-100-1[root]
Default VPN Interface	wan1
Local Gateway	IP Address
Routing	<input type="radio"/> Manual (via Device Manager) <input checked="" type="radio"/> Automatic
Local ID	
Advanced Options >	

5. Create firewall policies:

- a. Go to *Policy & Objects > Policy Package* to create policies among the default VPN zones and protected-subnet interfaces.
- b. Use the *Install On* option to restrict policies applied on specific FortiGate devices.

Seq#	From	To	Source	Destination	Schedule	Service	Action	Log	NAT	Install On
1	vpnmgmt_full_rm	loop1	vpnmgmt_full_rm	all	all	always	ALL	✓ Accept	Log Security Ev	Disabled
2	vpnmgmt_full_rm	loop1	vpnmgmt_full_rm	all	all	always	ALL	✓ Accept	Log Security Ev	Disabled
3	loop1	vpnmgmt_full_rm	prosub-172.19.100.22 prosub-172.19.100.23 prosub-172.19.100.24 prosub-172.19.100.25 prosub-172.19.100.26 prosub-172.19.100.27 prosub-172.19.100.28 prosub-172.19.100.29 prosub-172.19.100.30	all	all	always	ALL	✓ Accept	Log All Sessions	Disabled

- c. Remember to create policies for bi-directional traffic.



For further FortiManager information, refer to the [FortiManager Administration Guide](#) available on the [Fortinet Document Library](#).

System Settings

This section contains the following topics:

- [Configuring and debugging FortiManager HA clusters on page 15](#)
- [Creating administrator accounts with restricted access on page 17](#)

Configuring and debugging FortiManager HA clusters

You can configure two or more FortiManager units in a high availability (HA) cluster. You can also generate and download a debug log for each unit in a FortiManager HA cluster.

The following is an overview of configuring FortiManager units in an HA cluster:

1. Configure the primary FortiManager unit. See [Configuring the primary FortiManager unit in an HA cluster on page 15](#)
2. Configure one or more backup FortiManager units. See [Configuring backup FortiManager units in an HA cluster on page 16](#)
3. If you encounter problems, review the debug log for each unit in an HA cluster. See [Generating and downloading HA debug logs on page 16](#).

Configuring the primary FortiManager unit in an HA cluster

You can configure one FortiManager unit to be the primary unit in a high availability (HA) cluster. You must know the IP address and serial number of the FortiManager units that will be configured as backup (also called secondary or peer) units in the HA cluster to complete this procedure.

To configure the primary FortiManager unit:

1. Go to *System Settings > HA*.
2. Set *Operation Mode* to *Primary*.
3. In the *Peer IP* box, enter the IP address of the backup FortiManager unit.
4. In the *Peer SN* box, enter the serial number of the backup (secondary or peer) FortiManager unit.

- Click + to add additional backup FortiManager units to the HA cluster.

Cluster Settings

Operation Mode

Standalone

Primary

Secondary

Peer IP and Peer SN

IP Type

Peer IP

Peer SN

IPv4

192.168.48.61

FM200D3A15000236

+

Cluster ID

1

(1-64)

Group Password

File Quota

4096

(2048-20480)
MB

Heart Beat Interval

5

Seconds

Failover Threshold

3

(1-255)

Download Debug Log

Download

Apply

- Click *Apply*.

Configuring backup FortiManager units in an HA cluster

You can configure up to four FortiManager units as backup (also called secondary or peer) units in an HA cluster. You must know the IP address and serial number of the primary FortiManager unit in the HA cluster to complete this procedure.

To configure the backup FortiManager unit:

- Go to *System Settings > HA*.
- Beside *Operation Mode*, select *Secondary*.
- In the *Peer IP* box, enter the IP address of the primary FortiManager unit.
- In the *Peer SN* box, enter the serial number of the primary FortiManager unit.
- Click *Apply*.

Generating and downloading HA debug logs

You can run a command to generate a debug log for each FortiManager unit in an HA cluster, and then you can download the logs using the GUI.

To generate a debug log:

- On the primary or backup (secondary) FortiManager unit in an HA cluster, enter the following command:
`diagnose debug application ha 255`

To download a debug log:

- Go to *System Settings > HA*.
- Next to *Download Debug Log*, click *Download*.
- Save the log file (`ha-<date>.log`) to your local computer. It can be opened in a text editor.

Creating administrator accounts with restricted access

When you create an administrator account in FortiManager, by default the account grants access to all ADOMs and all policy packages. However, you can configure administrator accounts with restricted access to the following items:

- ADOMs - see [Restricting administrator access to ADOMs on page 17](#)
- Device groups - see [Restricting administrator access to device groups on page 19](#)
- Policy packages - see [Restricting administrator access to policy packages on page 20](#)

Restricting administrator access to ADOMs


When you create an administrator account, you can specify which ADOMs that users of the account can access. This topic describes the different methods you can use to restrict access.

To create an administrator account and specify ADOM access:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*, and then select the ADOMs that the administrator account can access.

Create New Administrator

User Name: ADOM-admin

Avatar:  +Add Photo -Remove Photo

Description:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted_User

Administrative Domain: All ADOMs All ADOMs except specified

Policy Package Access: All Packages Specify

JSON API Access: None

Theme Mode: Use Global Theme Use Own Theme

Trusted Hosts:

OK

Select Entries (Total: 20)

- ☐ Chassis
- ☐ FortiAnalyzer
- ☐ FortiAuthenticator
- ☐ FortiCache
- ☐ FortiCarrier
- ☐ FortiClient
- ☐ FortiDDoS
- ☐ FortiDeceptor
- ☐ FortiFirewall
- ☐ FortiMail
- ☐ FortiManager
- ☐ FortiNAC

OK Cancel

For example, select only the *root* and 56 ADOMs.

Create New Administrator

User Name	<input type="text" value="ADOM-admin"/>
Avatar	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; background-color: #eee; display: flex; align-items: center; justify-content: center; margin-right: 5px;">A</div> <div> <input type="button" value="+ Add Photo"/> <input type="button" value="- Remove Photo"/> </div> </div>
Description	<div style="border: 1px solid #ccc; height: 40px;"></div>
Admin Type	<div style="border: 1px solid #ccc; padding: 2px;">LOCAL</div>
New Password	<div style="border: 1px solid #ccc; padding: 2px;"></div>
Confirm Password	<div style="border: 1px solid #ccc; padding: 2px;"></div>
Admin Profile	<div style="border: 1px solid #ccc; padding: 2px;">Restricted_User</div>
Administrative Domain	<div style="display: flex; border: 1px solid #ccc; padding: 2px;"> <div style="border-right: 1px solid #ccc; padding: 0 5px;">All ADOMs</div> <div style="padding: 0 5px;">All ADOMs except specified ones</div> <div style="border: 1px solid #007bff; padding: 0 5px; color: #007bff;">Specify</div> </div> <div style="border: 1px solid #007bff; padding: 5px; margin-top: 5px;"> <input style="width: 100%;" type="text"/> <div style="display: flex; justify-content: space-between; padding: 0 5px;"> <div>root</div> <div>✕</div> </div> <div style="display: flex; justify-content: space-between; padding: 0 5px;"> <div>56</div> <div>✕</div> </div> <div style="text-align: center; margin-top: 5px;">2 Entries Selected</div> </div>
Policy Package Access	<div style="display: flex; border: 1px solid #ccc; padding: 2px;"> <div style="border-right: 1px solid #007bff; padding: 0 5px; color: #007bff;">All Packages</div> <div style="padding: 0 5px;">Specify</div> </div>
JSON API Access	<div style="border: 1px solid #ccc; padding: 2px;">None</div>

4. Set the remaining options, and click **OK**.

When the administrator logs in to FortiManager, they can only access the specified ADOMs. In this example, the specified ADOMs are *root* and *56*.

Select an ADOM

<div style="background-color: #007bff; color: white; padding: 5px; border: 1px solid #007bff;">root (5)</div> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">FortiGate 7.0</div>	<div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">56</div> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">FortiGate 7.0</div>
---	--

To create an administrator account and exclude access to specific ADOMs:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *All ADOMs except specified ones*, and then select the ADOMs that you do not want the administrator account to access.
In this example, the *root* and *56* ADOMs are excluded from access.

Edit Administrator

User Name

ADOM-admin

Avatar

A

+ Add Photo

- Remove Photo

Description

Admin Type

LOCAL

Admin Profile

Restricted_User

Administrative Domain

All ADOMs

All ADOMs except specified ones

Specify

root

56

2 Entries Selected

Policy Package Access

All Packages

Specify

JSON API Access

None

Theme Mode

Use Global Theme

Use Own Theme

Trusted Hosts

☐

OK

Cancel

4. Set the remaining options, and click **OK**.

When the administrator logs in to FortiManager, they can access all ADOMs except for the ones specified. In this example, they can access all ADOMs except *root* and *56*.

Select an ADOM

Production

Test

FortiGate 6.4

FortiGate 7.0

Restricting administrator access to device groups

On the *Device Manager* pane, you can create device groups and add devices to the different groups. If you are using ADOMs, select the ADOM, and then create the device group.

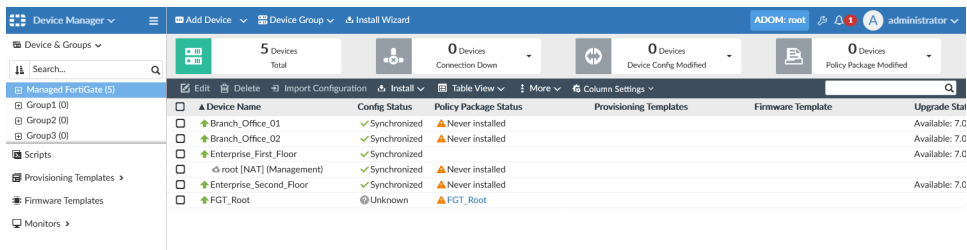
When you create an administrator account, you can specify which ADOMs the account can access, and which device groups can be accessed in those ADOMs.

This topic describes how to create a device group and how to restrict administrator access to device groups.

To create a device group:

- Go to *Device Manager > Device & Groups*.
- If you are using ADOMs, select the ADOM that you are creating a device group in. Otherwise skip this step.
- In the *Device Group* dropdown menu, click *Create New Group*.
- Enter a name for the group and add devices to it, then click **OK**.

In this example, the root ADOM contains *group1*, *group2*, and *group3*.

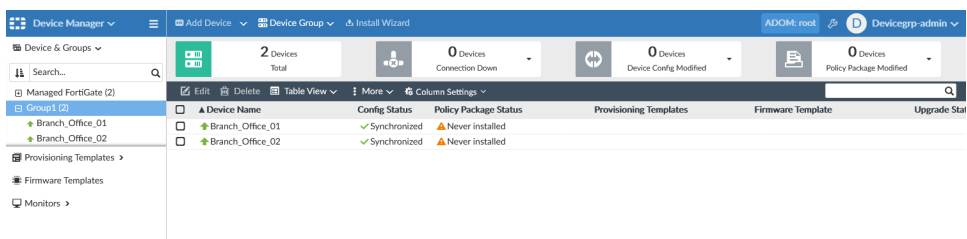


To specify admin access to device groups:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*.
4. Select the ADOM that contains the device group. Select only one ADOM.
5. Select *Specify Device Group to Access*, and then select the device group. In this example, *group1* is specified.

6. Click *OK*.

When the administrator logs in to FortiManager, they can only access the specified device group on the *Device Manager* pane. In this example, they can only access *group1*.



Restricting administrator access to policy packages


When you create an administrator account, you can specify which policy packages that administrator can access.

To specify admin access to policy packages:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.

3. Beside *Policy Package Access*, click *Specify*, and specify which policy packages can be accessed. In the following example, administrators can access the *root* and *60* policy packages.

New Administrator

User Name	<input type="text" value="Package-admin"/>
Avatar	 <input type="button" value="+ Change Photo"/> <input type="button" value="- Remove Photo"/>
Comments	<input type="text" value=""/> 0/127
Admin Type	<input type="text" value="LOCAL"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
Admin Profile	<input type="text" value="Restricted_User"/>
Administrative Domain	<input type="button" value="All ADOMs"/> <input type="button" value="All ADOMs except specified ones"/> <input type="button" value="Specify"/>
Policy Package Access	<input type="button" value="All Packages"/> <input type="button" value="Specify"/> <input type="text" value="✖ root:default"/> <input type="text" value="✖ 60:default"/>
Trusted Hosts	<input type="button" value="OFF"/>
Meta Fields	Meta Fields >

4. Set the remaining options, and click *OK*.
When the administrator logs in to FortiManager, they can only access the specified policy packages. In this example, the specified policy packages are *root:default* and *60:default*.

Certificate deployment

This section includes the following topics:

- [Configuring FortiManager to deploy certificates for admin GUI access on page 22](#)
- [Configuring FortiManager to deploy certificates for deep inspection on page 25](#)
- [Configuring FortiManager to deploy SAML certificates on page 28](#)
- [Configuring FortiManager and FortiAuthenticator for SCEP certificate deployment on page 38](#)

Configuring FortiManager to deploy certificates for admin GUI access

The steps for deploying an end-entity certificate for admin GUI access are as follows:

1. [Creating the certificate for administrator web access on page 22](#)
2. [Uploading the certificate to FortiManager on page 24](#)
3. [Apply the certificate to the FortiGate in FortiManager on page 24](#)
4. [Install the certificate on page 24](#)
5. [Verify the certificate was installed correctly on page 25](#)

Creating the certificate for administrator web access

When selecting a certificate to secure HTTPS access, there are a few options you may consider. This example utilizes a wildcard certificate so that it may be applied to several FortiGates in the same domain, such as *FGT1.domain.com*, *FGT2.domain.com*, etc.

This wildcard certificate is signed by the same CA used to sign the intermediate CA used by SSL/SSH inspection.

To create the certificate on FortiAuthenticator:

1. Navigate to *Certificate Management > End Entities > Users*.
2. Select *+ Create New*.

3. Provide details for your FortiGate certificate.

FortiAuthenticator VMKVM

System > Create New User Certificate

Authentication > Certificate ID: FGT_Wildcard

Fortinet SSO Methods > Certificate Signing Options

Monitor > Issuer: Local CA Third-party CA

Certificate Management > Certificate authority: AcmeCA | CN=Acme Root CA

Policies > Local User (Optional):

End Entities > Subject Information

Users > Subject input method: Fully distinguished name Field-by-field

Local Services > Name (CN): *.domain.com

Certificate Authorities > Department (OU):

SCEP > Company (O):

Logging > City (L):

State/Province (ST):

Country (C):

Email address:

4. Expand *Advanced Options: Key Usages* and add *Server Authentication* to the Chosen Extended Key Usages.

Advanced Options: Key Usages

Key Usages: ☐ Critical

Available Key Usages ?

Filter

Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Certificate Sign
CRL Sign
Encipher Only
Decipher Only

Choose all

Chosen Key Usages ?

Remove all

Extended Key Usages: ☐ Critical

Available Extended Key Usages ?

Filter

Client Authentication
Code Signing
Secure Email
OCSP Signing
IPSec End System
IPSec Tunnel Termination
IPSec User
IPSec IKE Intermediate (end entity)
Time Stamping
Microsoft Individual Code Signing
Microsoft Commercial Code Signing
Microsoft Trust List Signing
Microsoft Server Gated Crypto

Choose all

Chosen Extended Key Usages ?

Server Authentication

Remove all

5. Select *OK* to save the certificate.
6. Select the generated certificate using the checkbox, and click *Export Key and Cert*.
7. Provide a passphrase and click *OK*.
8. Click *Download PKCS#12 file* to download the certificate.

Uploading the certificate to FortiManager

To upload the certificate to FortiManager:

1. Navigate to *Policy & Objects > Advanced*.
2. From the top menu bar, select *Tools > Feature Visibility*, and under *Advanced* enable *Dynamic Local Certificate*.
3. Select *Dynamic Local Certificate* from the top.
4. Select *+Create New* in the top left.
5. Specify a name for the certificate.
6. Expand *Per-Device Mapping* and select *Create New* to create a new mapping.
7. Select the target FortiGate for *Mapped device*.
8. Select *Import* next to *Import Certificate*.
9. Select *Local Certificate* for *Type*.
10. Upload the file by browsing or drag-and-dropping the certificate.
11. Specify the name for the certificate.
12. Select *OK*.



If the newly uploaded certificate does not appear in the dropdown for *Local Certificate*, select *OK*, then select the mapped device and edit once more.

13. Use the *Local Certificate* dropdown to select the newly uploaded certificate.
14. Select *OK* to save the per-device mapping.
15. Provide a change note and select *OK* to save the dynamic local certificate.

Apply the certificate to the FortiGate in FortiManager

To apply the certificate to the FortiGate in FortiManager:

1. Navigate to *Device & Groups*, and select the FortiGate you wish to install the certificate on.
2. Select *System: Settings* from the top menu bar.
3. Under *Administration Settings*, use the dropdown next to *HTTPS Server Certificate* to select the certificate you uploaded in the previous step.
4. Select *Apply*.

Install the certificate

To install the certificate on the FortiGate:

1. Select *Install Wizard* from the top menu bar
2. Select *Install Device Settings (only)* and click *Next*.
3. Select the device you wish to install the certificate on, and click *Next*.
4. If the connection is up, proceed by clicking *Install*.

- You may wish to review the *Install Preview* to ensure all changes are as expected prior to installing.
5. Select *Finish* when the installer completes.

Verify the certificate was installed correctly

To verify the certificate was successfully installed on FortiGate:

1. Navigate to the FortiGate's GUI web page. This should match the *SAN* field of the certificate.
2. Notice how the connection is secure, and the certificate used to secure the connection is the same certificate you configured in the previous steps.

Configuring FortiManager to deploy certificates for deep inspection

FortiManager can be used to deploy certificates to FortiGate devices. These certificates can include Certificate Authority (CA) certificates, commonly used for deep inspection.

The steps for deploying a CA certificate for deep inspection are as follows:

1. [Generate a CA certificate on FortiAuthenticator on page 25](#)
2. [Generate an intermediate CA certificate on page 26](#)
3. [Upload the intermediate CA certificate to FortiManager on page 26](#)
4. [Use the certificate in a policy and install the Policy Package on page 27](#)
5. [Verify on an endpoint on page 27](#)

Generate a CA certificate on FortiAuthenticator

To generate a CA certificate on FortiAuthenticator:

1. On the FortiAuthenticator, go to *Certificate Management > Certificate Authorities > Local CAs*, and select *+Create New*.
2. Specify a *Certificate ID*, leave the *Certificate type* as *Root CA*, and specify a *Name (CN)*.
3. You may provide additional fields as desired.

4. Select OK.

FortiAuthenticator VMKVM

System > Create New Local CA Certificate

Authentication > Certificate ID:

Fortinet SSO Methods > Certificate Authority Type

Monitor > Certificate type: ☒ Root CA ☐ Intermediate CA ☐ Intermediate CA signing request (CSR)

Certificate Management > ☐ Use netHSM

Policies > Subject Information

End Entities > Subject input method: ☐ Fully distinguished name ☒ Field-by-field

Certificate Authorities > Name (CN):

Local CAs > Department (OU):

CRLs > Company (O):

Trusted CAs > City (L):

SCEP > State/Province (ST):

Logging > Country (C):

Email address:

Key And Signing Options

Validity period:

3650 days

Key type: RSA

Key size: ☐ 1024 ☒ 2048 ☐ 4096

Hash algorithm: ☒ SHA-256 ☐ SHA-1

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

Advanced Options: Key Usages

Certificate Revocation List (CRL)

Lifetime: days (1-365)

Re-generate every: days

Generate an intermediate CA certificate

To generate an intermediate CA certificate:

1. From *Certificate Management > Certificate Authorities > Local CAs*, and select **+Create New**.
2. Provide a name for the certificate as *Certificate ID*.
3. For *Certificate type*, select *Intermediate CA*.
4. Use the dropdown for *Certificate authority* to select the certificate created in the previous step.
5. For *CN*, provide a name for the intermediate CA certificate.
6. Click **OK** to save.
7. Use the checkbox to select the generated intermediate CA certificate, then click *Export Key and Cert* in the top navigation bar.
8. Provide a passphrase to secure the private key.
9. Select *Download PKCS#12 file*, then select *Finish*.

Upload the intermediate CA certificate to FortiManager

To upload the intermediate CA certificate to FortiManager:

1. Navigate to *Policy & Objects > Advanced*.
2. From the top menu bar, select *Tools > Feature Visibility*.
3. Under *Advanced*, enable *Dynamic Local Certificate*.
4. Select *Dynamic Local Certificate* from the top.

5. Select **+Create New** in the top left.
6. Specify a name for the certificate.
7. Expand *Per-Device Mapping* and select *Create New* to create a new mapping.
8. Select the target FortiGate for *Mapped device*.
9. Select *Import* next to *Import Certificate*.
10. Select *PKCS#12 Certificate* for *Type*.
11. Upload the file by browsing or drag-and-dropping the certificate.
12. Provide the password used to secure the private key.
13. Specify the name for the certificate.
14. Select *OK*.



If the newly uploaded certificate does not appear in the dropdown for *Local Certificate*, select *OK*, then select the mapped device and edit once more.

15. Use the *Local Certificate* dropdown to select the newly uploaded certificate.
16. Select *OK* to save the per-device mapping.
17. Provide a change note and select *OK* to save the dynamic local certificate.

Use the certificate in a policy and install the Policy Package

To update SSL/SSH inspection to use the uploaded certificate:

1. Navigate to *Policy & Objects > Security Profiles*, and select *SSL/SSH Inspection* from the top menu.
2. Edit *custom-deep-inspection*.
3. For *CA Certificate*, use the dropdown to select the uploaded intermediate CA certificate.
4. Provide a change note and select *OK* to save.
5. Use this security profile, along with a web filtering profile, in a policy assigned to the FortiGate with the certificate mapping.
6. Install the Policy Package.

For more information, see *Deep Inspection* in the FortiGate Administration Guide on the [Fortinet Document Library](#), as you need to install this intermediate CA on endpoints/browsers to enable the certificate rewriting to be trusted.

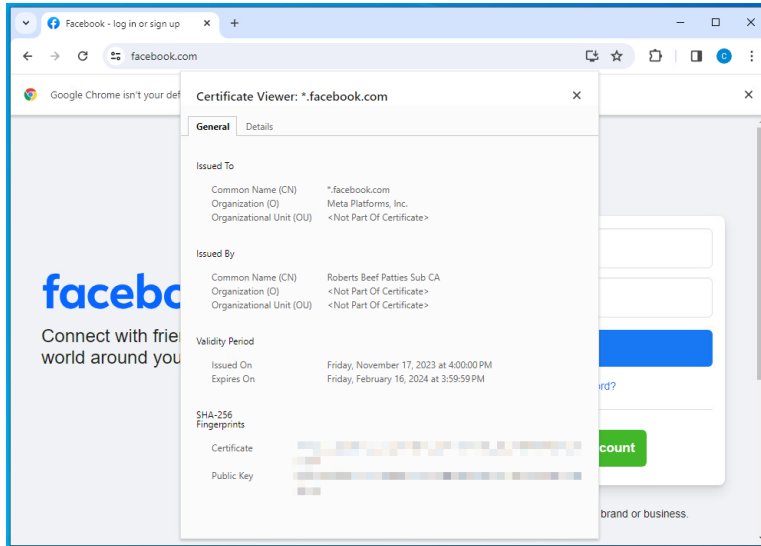
Verify on an endpoint

This guide assumes the certificate used in the deep inspection profile is trusted by the endpoint.

To verify on an endpoint:

1. Navigate to an HTTPS site on an endpoint which would send traffic through the policy you applied the SSL/SSH custom-deep-inspection profile to.
2. When the site loads, inspect the certificate that is being used.

- Note how the certificate is valid.
- Note how the *Issued By* section reflects the certificate you selected for your deep inspection.



Configuring FortiManager to deploy SAML certificates

This topic provides the steps required to generate certificates used for SAML authentication using FortiAuthenticator (version 6.6.0).

These certificates are then used manually to configure SAML authentication using FortiAuthenticator as the Identity Provider (IdP) and a FortiManager (version 7.4.2) as the Service Provider (SP). Then, FortiManager is used to configure a FortiGate (version 7.4.2) to use the FortiAuthenticator as an IdP.

In this example, FortiAuthenticator is used to create two certificates:

- *Root CA certificate*: Used to sign all additional certificates.
- *IdP certificate*: Used in SAML.

More information can also be found in the following guides on the Fortinet Document Library:

- [FortiAuthenticator Administration Guide](#)
- [SAML Interoperability Guide](#)

Create a local CA on the FortiAuthenticator

This certificate will be used to create further certificates used to verify identity between IdP and Service Providers (SP).

To create a local CA on the FortiAuthenticator:

1. Navigate to *Certificate Management > Certificate Authorities > Local CAs*.
2. Select *Create New*.

3. Provide the following info. Optional fields are not specified.

Field	Value	Note
Certificate ID	FAC_ROOT_CA	This is the name of the certificate.
Certificate Type	Root CA	No other certificate may sign this certificate.
CN	FAC ROOT CA	This should reflect the certificate's usage.

Certificate Viewer: *.google.com ×

General Details

Issued To

Common Name (CN)	*.google.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	GTS CA 1C3
Organization (O)	Google Trust Services LLC
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, January 8, 2024 at 10:25:08 PM
Expires On	Monday, April 1, 2024 at 11:25:07 PM

SHA-256 Fingerprints

Certificate	680f8b1123be39f4451430d6267a8159033034403ce0df1abdf11c105031d719
Public Key	271616060e9f67a3804a4b4c326a06d63ebe0d74f8ab16b149014ca71059d745

4. Click **Save**.

Create the Identity Provider (IdP) certificate used in SAML

This certificate will be signed by the CA created in the previous step. Therefore it is also necessary that the SPs trust this CA. This involves installing the root CA on the SPs to create the needed trust.

To create a local certificate on FortiAuthenticator to be used by the IdP:

1. Navigate to *Certificate Management > End Entities > Local Services*.
2. Select *Create New*.
3. Provide the following info. Optional fields are not specified.

Field	Value	Note
Certificate ID	IDP_certificate.	This is the name of the certificate.
Issuer	Local CA	
Certificate Authority	FAC_ROOT_CA CN=FAC ROOT CA	This is the certificate created in the previous step.
Name (CN)	fac.robertsbgp.com	This should match the identity provider's name.

4. At the bottom, expand *Advanced Options: Key Usages*.
5. Add all *Key Usages* and *Extended Key Usages*.
6. Click *OK* when finished.

Export the certificate so that it can be installed on the SP (and IdP when necessary).

To export the certificate:

1. From the same menu as before, select the created certificate using the checkbox on the left.
2. Select *Export Certificate* from the top navigation bar.
3. The certificate will download locally. In this example, the certificate is downloaded as *IDP_certificate.cer*.

Create the IdP portal on FortiAuthenticator

These steps cover the IdP settings which determine whose identity it may verify, as well as the eligible service providers. This example uses FortiAuthenticator as the IdP. As a result, the IdP already has access to the certificate that will be used. If you are using another IdP, you will need to upload the certificate first.

To configure IdP settings:

1. Navigate to *Authentication > SAML IdP > General*.
2. Enable the *SAML Identity Provider Portal*.
3. Provide the following information:
 - a. *Server address*: *fac.robertsbgp.com*.
 - b. *Realms*: *local | Local users*

c. *Default IdP certificate: IDP_certificate | CN=fac.robertsbp.com*

4. Select **Save**.

For this example, FortiManager is added as a service provider within the IdP.

To configure SP settings:

1. Navigate to *Authentication > SAML IdP > Service Providers*.
2. Select *Create New* and provide the following:

Field	Value	Note
SP name	FMG_SP	
Create an identifier for this IdP	fac	Use the + icon to provide this value.

3. Click **Save**, and notice how the *SP Metadata* field appears.
4. Remain in this menu. To complete the SP settings on the IdP, we need to provide the *SP entity ID*, *SP ACS (login) URL*, and the *SP SLS (logout) URL*. These are generated in the upcoming *Defining SAML SP Settings on FortiManager* section, and added in the *IdP portal SP settings continued* section.

Allowing IdP service on FortiAuthenticator

To allow connections to make the SAML request, FortiAuthenticator must be configured to receive these requests.

To allow IdP service on FortiAuthenticator:

1. Navigate to *System > Network > Interfaces*, and edit the interface that will be used for SAML authentication requests.
2. *Enable Services > HTTPS*, then enable *SAML IdP (/saml-idp)*.

3. Click **Save**.

System

Dashboard

Network

Interfaces

DNS

Static Routing

Zero Trust Tunnels

Packet Capture

Administration

Messaging

Authentication

Fortinet SSO Methods

Monitor

Certificate Management

Logging

Edit Network Interface

Editing this configuration might require the web server to be restarted

Interface Status

Interface: port1

Status: ☒

IP Address / Netmask

IPv4: 10.0.0.203/255.255.255.0

IPv6:

Access Rights

Admin access:

☒ SSH (TCP/22)

☒ HTTPS (TCP/443)

☒ GUI (TCP/443)

☐ REST API (/api/)

☐ Fabric (/api/v1/fabric/)

☐ HTTP (TCP/80)

☐ SNMP (UDP/161)

Services:

☒ HTTPS (TCP/443)

☐ Legacy Self-service Portal (/login/)

☐ Captive Portals (/guests, /portal)

☒ SAML IdP (/saml-idp)

☐ SAML SP SSO (/saml-sp, /login/saml-auth)

☐ Kerberos SSO (/login/kerb-auth)

☐ SCEP (/app/cert/scep)

☐ CRL Downloads (/app/cert/crl)

☐ CMP (/app/cert/cmp2/)

☐ FortiToken Mobile API (/api/v1/pushauthresp, /api/v1/transfortoken)

☐ OAuth Service (/api/v1/oaauth, /api/v1/pushpoll, /guests, /portal)

☐ HTTP (TCP/80)

☐ RADIUS Accounting Monitor (UDP/1646)

☐ RADIUS Auth (UDP/1812)

☐ RADIUS Accounting SSO (UDP/1813)

☐ RADSEC (TCP/2083)

☐ TACACS+ Auth (TCP/49)

☐ LDAP (TCP/389)

☐ LDAPS (TCP/636)

☐ FortiGate FSSO (TCP/8000)

☐ OCSP (TCP/2560)

☐ FortiClient FSSO (TCP/8001)

☐ Hierarchical FSSO (TCP/8003)

☐ DC/TS Agent FSSO (TCP/8002)

☐ Syslog (UDP/514)

☐ Syslog over TLS (TCP/6514)

☐ SAML IdP SSO (TCP/8143)

Save Cancel

Defining a local user on the FortiAuthenticator

In order to validate the SAML configuration, we need to define a local user on the FortiAuthenticator, as that is the realm type we specified earlier.

To define a local user on the FortiAuthenticator:

1. Navigate to *Authentication > User Management > Local Users*.
2. Select *Create New* at the top.
3. Provide a username, such as Robert, and specify a password.
4. Click **Save**.

Defining SAML SP settings on FortiManager

Similarly to how we defined the IdP portal on the FortiAuthenticator, we must provide the matching settings on the Service Provider. The following configuration is done on the FortiManager.

To define SAML SP settings on FortiManager:

1. Navigate to *System Settings > SAML SSL*.
2. Specify the Server Address, such as `fmg.example.com`.
3. Select *Service Provider (SP)*.
4. Copy the three generated URLs to a notepad: *SP Entity ID*, *SP ACS (Login) URL*, *SP SLS (Logout) URL*.
5. Enable *Auto Create Admin*. This will create an account after a successful SAML authentication.
6. Specify a *Default Admin Profile* for the accounts created through SAML authentication.
7. Leave the *IdP Type* as *Fortinet*.
8. For *IdP Address*, enter `fac.robertsbp.com`.
9. Enter the *Prefix* which you created on the FAC (fac).
10. Next to *IdP Certificate*, select *Import* to upload the `IDP_certificate.cer` generated on the FAC, then use the dropdown to select this certificate.
11. Select *Apply* to save.



Hover your mouse over the (i) next to *IdP Settings*. Note that it mentions “IdP must send the “username” assertion attribute. This will be important later.

IdP portal SP settings continued

After generating the SP settings, you can provide them to the IdP (FortiAuthenticator in this example) to complete the configuration. Switch back to FortiAuthenticator to resume the IdP portal configuration.

To provide the IdP with the SP settings:

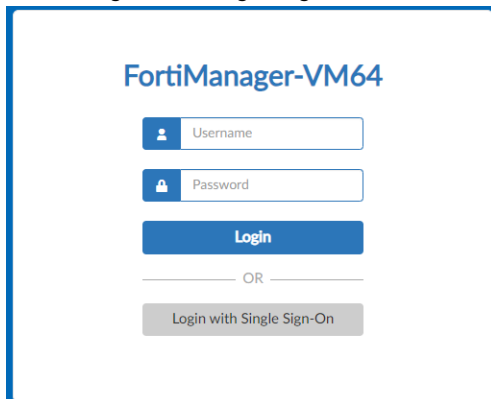
1. In the *SP Metadata* section, provide the three fields copied from the FortiManager:
 - *SP entity ID*
 - *SP ACS (login) URL*
 - *SP SLS (logout) URL*
2. Find the *Assertion Attributes Configuration* section. Notice what configuration already exists.
 - In other products, you will need to ensure that *username* is provided here.
3. Select *Save*.

Testing the configuration

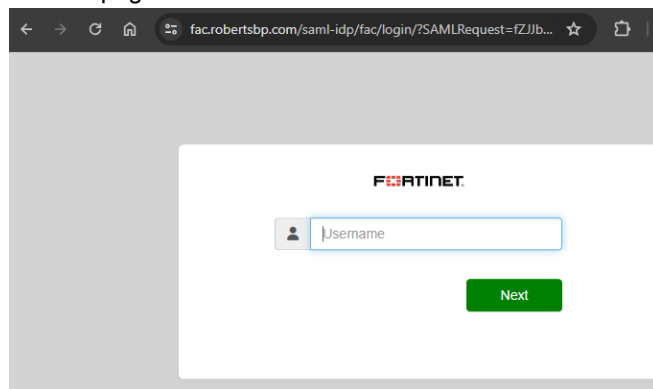
To verify the SAML configuration, attempt to log in to the FortiManager using the local account created on the FortiAuthenticator.

To test the configuration:

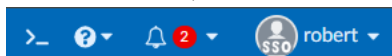
1. Navigate to the FortiManager login page.
2. Select *Login with Single Sign-On*.



The webpage redirects to the FortiAuthenticator address and presents the FortiAuthenticator login menu.



3. Authenticate with the local user you created on FortiAuthenticator.
4. Once successful, the username in the top right shows SSO in the user avatar.



Using FortiManager to provision the SAML certificates to FortiGates

Now that we have a good understanding of the certificates used by the IdP and SP in SAML authentication, we will use FortiManager to configure FortiGates to support SAML. These steps assume you have a managed FortiGate which is synchronized with FortiManager.

To add FortiGate as a Service Provider in the IdP (FortiAuthenticator)

1. Navigate to *Authentication > SAML IdP > Service Providers*, and select *Create New*.
2. Provide a SP name, such as *FortiGate*.
3. Create an identifier for this IdP: *fac2*.
4. Select *Save*.
5. Add the *SP entity ID*, *SP ACS (login) URL*, and *SP SLS (logout) URL* for the FortiGate. These will be similar to the following:

- entity-id `http://<IP-or-FQDN>:<port*>/saml/metadata/`
- single-sign-on-url `https://<IP-or-FQDN>:<port*>/saml/?acs`
- single-logout-url `https://<IP-or-FQDN>:<port*>/saml/?sls`

6. Make sure to specify the port if you are using non-standard HTTP/S ports.
7. Use the dropdown next to *Select an identifier* to display IdP info to select *fac2*.
8. Copy the three IdP URLs provided to a text editor.
9. Select **Save**.

The screenshot shows the FortiGate configuration interface for editing a SAML Service Provider. The left sidebar contains a navigation menu with categories like System, Authentication, User Account Policies, User Management, SCIM, Portals, Remote Auth. Servers, RADIUS Service, TACACS+ Service, LDAP Service, OAuth Service, SAML IdP, General, Service Providers, Replacement Messages, FAC Agent, Fortinet SSO Methods, Monitor, and Certificate Management. The main panel is titled 'Edit SAML Service Provider' and has a tab for 'FortiGate'. It contains several sections: 'SP name' (FortiGate), 'Server certificate' (Use default setting in SAML IdP General page), 'IdP signing algorithm' (Use default signing algorithm in SAML IdP General page), 'Support IdP-initiated assertion response' (checked), and 'Participate in single logout' (checked). Below these is the 'IdP Metadata' section, which includes a dropdown to 'Select an identifier to display IdP info' (set to 'fac2'), and three text fields for 'IdP entity id', 'IdP single sign-on URL', and 'IdP single logout URL', each with a copy icon. At the bottom is the 'SP Metadata' section with an 'Import SP metadata' button, and three text fields for 'SP entity ID', 'SP ACS (login) URL', and 'SP SLS (logout) URL', with an 'Alternative ACS URLs' button. A checkbox for 'SAML request must be signed by SP' is also present.

Configure FortiManager to install SAML configuration on the FortiGate

Here we will add the configuration to the FortiManager so it may be pushed to the FortiGate.

To upload the IdP Certificate to FortiManager:


1. On the FortiManager, navigate to *Policy & Objects > Advanced > CLI Configurations > VPN > Certificate > Remote*.





If the *CLI Only Objects* are not visible under the current view, enable the option *Tools > Feature Visibility*.

2. Select *Create New*.
3. Provide a name, such as *IDP_Certificate*.
4. Change the *range* to *global*.
5. Open the certificate file *IDP_certificate.cer* downloaded from FortiAuthenticator earlier, and open it with a text editor.
6. Copy the contents of the certificate into the remote field on the FortiManager.

Create New vpn certificate remote

name  IDP_Certificate (maximum 35 characters)


range  global

remote 

```

-----BEGIN CERTIFICATE-----
MIIESjCCAzKgAwIBAgIUALRGjZTMmoliGMAOGCsqGSllb3DQEBcUAMBYxFDASBgNV
BAMMCOZBQyBStO9UIENBMB4XDl0MDlxNDE0NTc1OFoXDTI5MDlxMjE0NTc1OFow
HDEaMBGGA1UEAwwRZmFjLnJvYmVydHhNlcC5jb20wggEIMAOGCsqGSllb3DQEBQUA
A4IBDwAwggEKAAQBAQKIZGn/TrRb1hPgKDMB3WpOCAOOkYIEYrM5Y7JkmhEi7E
ERKJ3cKLz+KeP8+Cq9H0v49omlGHagXtcxdt+8ldUEV173n7iPYmnXllyjibRO
YPG1BrUJZPkwbJYRicX9Gjxv5SYUtwSYDGIKokQ3UKjvnLUG6i08iOY8/dH0Yp
uHCHCzzu/K0ywb4qJa39bv/My8Z9Oz708rk41BnnnWWNQWha9hhiNG1Lchq3ynz/
5N7dCbPNy52sKZSFTLBbbv9F+cmnlHfoZzwAO7FJZaJW/DnjTviVAD2jctFhwuc
jKgtcoKMJB9LLUcoIfz2BXGnCOsdsPa8Wxy/OrRhAgMBAAGjggGTMIIIBjzAMBgNV
HRMBAI8EAJAAMBOGA1UdDgQWBBS6fOQPuqY7tIsRhr9PTQqrxZ5z8FBgNVHSMG
-----END CERTIFICATE-----

```

source  user

7. Click **OK**.

To configure the managed FortiGate to use SAML for admin sign-on:

1. Navigate to *Device Manager > Device & Groups*, and select the FortiGate you will be adding SAML authentication to.
2. Select *CLI Configurations* from the top menu bar.
3. Use the search bar and enter "saml" to select *system > saml*, and provide the following:

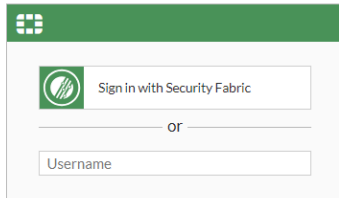
default-profile	super_admin (or your choice)
entity-id	http://fgt.robertsbp.com/metadata/
idp-cert	IDP_Certificate
idp-entity-id	http://fac.robertsbp.com/saml-idp/fac2/metadata/
idp-single-logout-url	https://fac.robertsbp.com/saml-idp/fac2/login/
idp-single-sign-on-url	https://fac.robertsbp.com/saml-idp/fac2/login/
role	service-provider
server-address	fgt.robertsbp.com

4. Select **Apply**.
5. Select *Install Wizard* from the top of the screen.
6. Install the changes to the FortiGate.

Testing the configuration

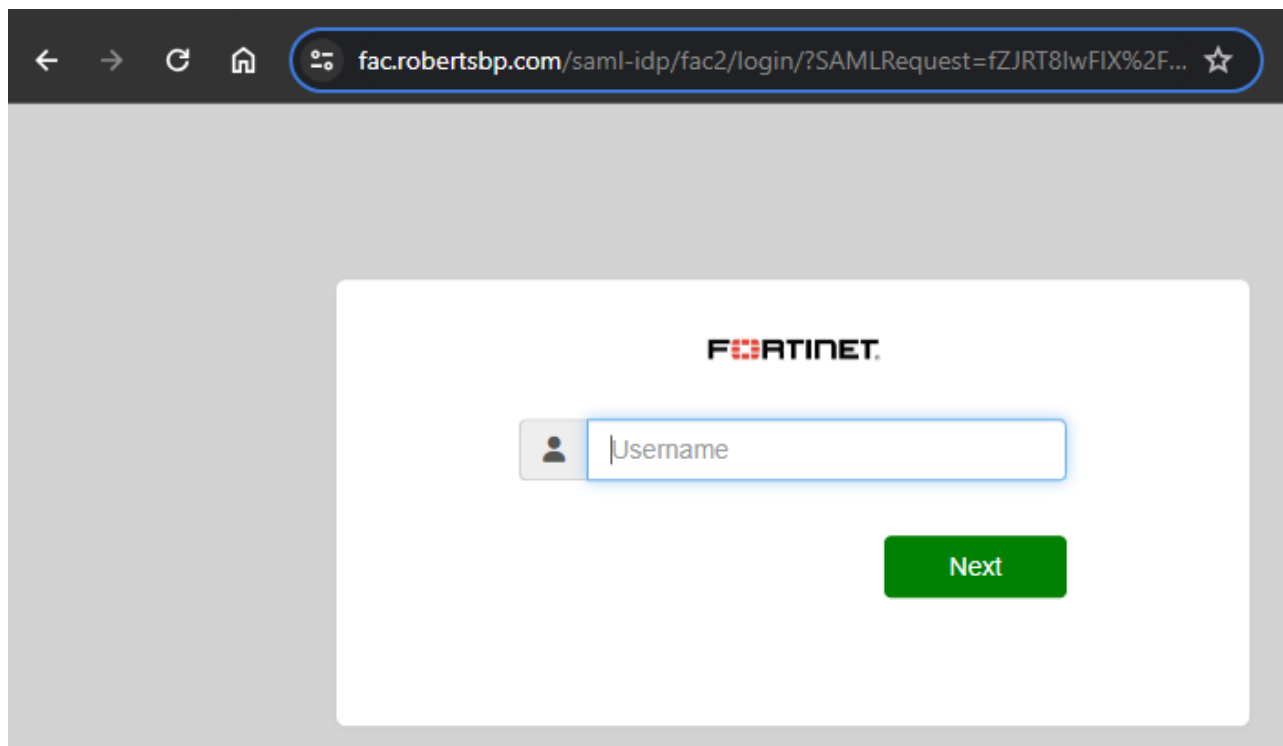
To verify the configuration:

1. To verify the configuration, navigate to the FortiGate's GUI admin page.

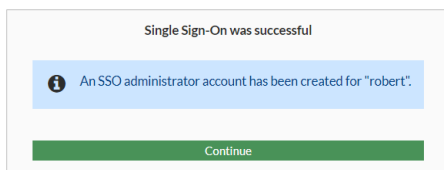


2. Select *Sign in with Security Fabric*.

Your browser redirects you to a new login page, and the URL of this login page is the FortiAuthenticator.



3. Provide the username and password of the local user that was created on the FortiAuthenticator earlier.
4. A window is displayed confirming that an account with the same username was created on the FortiGate. Click *Continue*.



5. Select *Login Read-Only*, as the FortiGate is managed by FortiManager.
The username in the top right shows (SSO) next to the username.



Configuring FortiManager and FortiAuthenticator for SCEP certificate deployment

Simple Certificate Enrollment Protocol (SCEP) is an open source protocol that allows for organizations to manage and deploy certificates in a scalable and secure fashion. This guide covers how to configure FortiAuthenticator as a Certificate Authority (CA) to conditionally sign certificates for FortiGates. These FortiGates will be managed by FortiManager and handles SCEP configuration as well as certificate usage for the FortiGates.

This section includes the following topics:

1. [Configuring FortiAuthenticator on page 38](#)
2. [Configuring FortiManager on page 41](#)
3. [Verification of certificate deployment on page 44](#)

Configuring FortiAuthenticator

The FortiAuthenticator has two roles in this guide: create and act as a Certificate Authority, and participate in the SCEP process as the SCEP server.

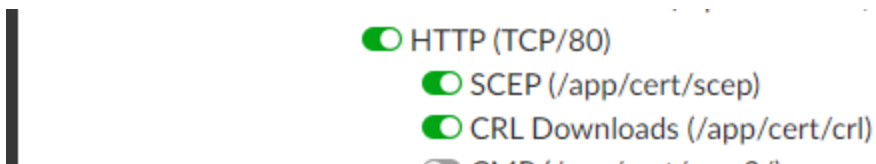
There are three configuration sections for FortiAuthenticator:

1. [Enable SCEP communications on page 38](#)
2. [Select or create a CA certificate on page 39](#)
3. [SCEP configuration on page 40](#)

Enable SCEP communications

To enable FortiAuthenticator for SCEP communications, you must enable the service as follows:

1. Navigate to *System > Network > Interfaces*.
2. Double click on the interface that FortiManager will communicate with the FortiAuthenticator on.
3. In the *Access Rights > Services* section, enable *HTTP*, and then *SCEP* and *CRL Downloads*.



Select or create a CA certificate

Certificate enrollment involves end entities, FortiGates in this example, receiving signed certificates. We will use FortiAuthenticator to generate the CA certificate that will be used to sign these certificates. If you already have a CA on FortiAuthenticator, you may skip this step.

To create a CA certificate on FortiAuthenticator:

1. Navigate to *Certificate Management > Certificate Authorities > Local CAs*.
2. Click *Create New*.
3. Provide the following details to create your CA. You may elect to add more details as you see fit.

Certificate ID	External_PKI
Certificate type	Root CA
Subject input method	Field-by-field
Name (CN)	external_pki
Department	FortiDocuments
Company	Fortinet
Key size	4096
Hash algorithm	SHA-256

The screenshot shows the FortiAuthenticator web interface. On the left is a navigation menu with categories like System, Authentication, Fortinet SSO Methods, Monitor, Certificate Management, Policies, End Entities, Certificate Authorities (selected), Local CAs (selected), CRLs, Trusted CAs, SCEP, CMP, and Logging. The main content area is titled 'Create New Local CA Certificate'. It contains several sections: 'Certificate ID' (External_PKI), 'Certificate Authority Type' (Root CA, Intermediate CA, Intermediate CA signing request (CSR)), 'Subject Information' (Subject input method: Field-by-field, Name (CN): external_pki, Department (OU): FortiDocuments, Company (O): Fortinet, City (L):, State/Province (ST):, Country (C):, Email address:), and 'Key And Signing Options' (Validity period: Set length of time, Key type: RSA, Key size: 4096, Hash algorithm: SHA-256).

4. Click *Save*.
5. Use the checkbox on the left side to select the newly created CA.
6. Select *Export Certificates* at the top to export the CA.

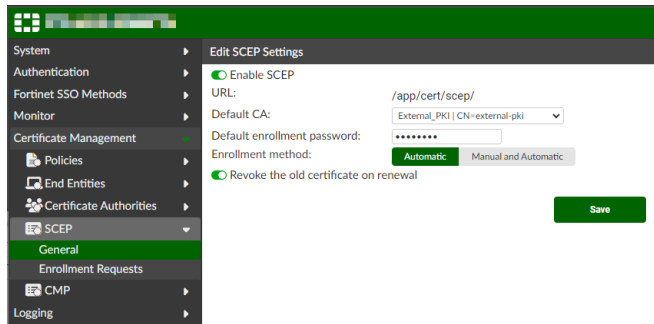


This certificate will need to be uploaded to any device which needs to verify the certificates signed by it. That might mean end user desktops for GUI admin access or deep inspection, or to FortiGates for site-to-site VPN.

SCEP configuration

To enable SCEP:

1. Navigate to *Certificate Management > SCEP > General*.
2. Enable *SCEP*.
3. Ensure *External_PKI* is selected for *Default CA*.
4. Set the *Default enrollment password*.
5. Leave *Enrollment method* on *Automatic*.
6. Leave *Revoke the old certificate on renewal* enabled.
7. Select *Save*.



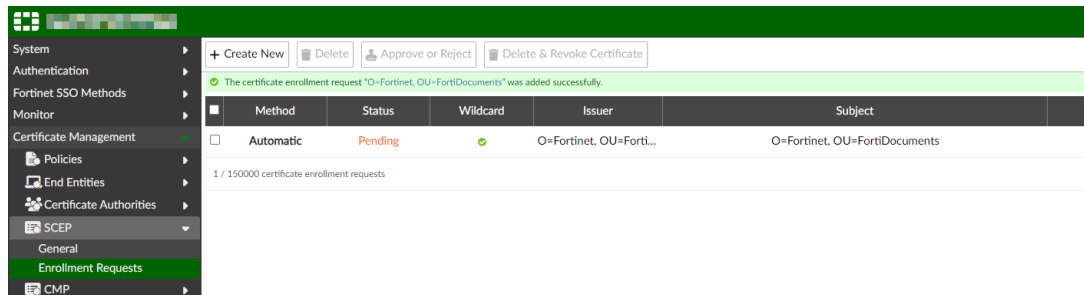
To configure enrollment requests:

1. Select *Certificate Management > SCEP > Enrollment Requests*.
2. Click *Create New*.
3. Provide the following details:

Automatic request type	Wildcard
Certificate authority	External_PKI CN=external-pki
Subject input method	Field-by-field
Department	FortiDocuments
Company	Fortinet
Hash algorithm	SHA-256
Password generation	Default
Allow renewal ____ days before certificate is expired	Enabled, 7
Allow renewal if revoked	Enabled
Allow renewal if expired	Enabled
Add CRL Distribution Points extension	Enabled
Add OSCP Responder URL	Enabled

The wildcard request type allows you to create a single enrollment request to match all requests coming from FortiManager. Hover over the Wildcard option on FortiAuthenticator to learn more about the requirements and caveats.

4. Click **Save**.



Configuring FortiManager

There are four configuration sections for FortiManager:

1. [Creating a certificate template on page 41](#)
2. [Import the External_PKI CA certificate on page 42](#)
3. [Use the certificate in FortiManager on page 42](#)
4. [Install the certificate to FortiGate on page 43](#)

Creating a certificate template

The certificate template is used to define a certificate object for one or more FortiGates. Like most objects in FortiManager, this object can be mapped to many FortiGates so that a common configuration can apply a unique certificate to each managed FortiGate.

To create a certificate template:

1. Navigate to *Device Manager > Provisioning Templates*.
2. Select *Certificate* from the top menu bar.
3. Select *Create New*.
4. Provide the following details:

Type	External
Certificate Name	external_pki
Organization Unit	FortiDocuments
Organization	Fortinet
Key Type	RSA
Key Size	4096
Hash Algorithm	SHA-256

CA Server URL `http://<FAC_IP>/app/cert/scep`

Challenge Password `<The enrollment password created on the FAC>`



The CA Server URL is the URL that the FortiManager can reach FortiAuthenticator on plus the directory that was given after enabling SCEP.

5. Click **OK**.
6. Navigate to **Policy & Objects > Advanced > Dynamic Local Certificate**. Note how there is a new certificate created named `external_pki`. If you edit this certificate, you will notice that there are no per-device mappings. This is expected as the certificate has not yet been requested from FortiAuthenticator, therefore there are no mappings.

Import the External_PKI CA certificate

This certificate will be used by FortiGates to help validate any certificates that this CA certificate has signed. After importing the CA certificate here, it will be included in the next install for FortiGates in the VDOM.

To import the External_PKI CA certificate:

1. Navigate to **Policy & Objects > Advanced**, and select **Tools > Feature Visibility** at the top to enable **Advanced > CA Certificates**.
2. Select **OK** to save the feature visibility.
3. Select **CA Certificates** from the top menu bar.
4. Select **Import** in the top left to provide the following details:
 - a. **Certificate Name**: `ca_external_pki`.
 - b. **Import CA Certificate**: Upload the certificate exported from FortiAuthenticator in an earlier step.
5. Click **OK** to save.

<input type="checkbox"/>	Certificate Name	Subject	Status	Created Time
<input type="checkbox"/>	RBP_CA	CN = Roberts Beef Patties CA	OK	admin / 2024-02-09 07:41:08 PST
<input type="checkbox"/>	RBP_SUB_CA	CN = Roberts Beef Patties Sub CA	OK	admin / 2024-02-09 07:40:47 PST
<input type="checkbox"/>	ca_external_pki	O = Fortinet, OU = FortiDocuments, CN = ...	OK	admin / 2024-02-20 11:04:11 PST
<input type="checkbox"/>	root_CA3	O = Fortinet Ltd., CN = Fortinet	OK	admin / 2024-02-07 20:30:04 PST

Use the certificate in FortiManager

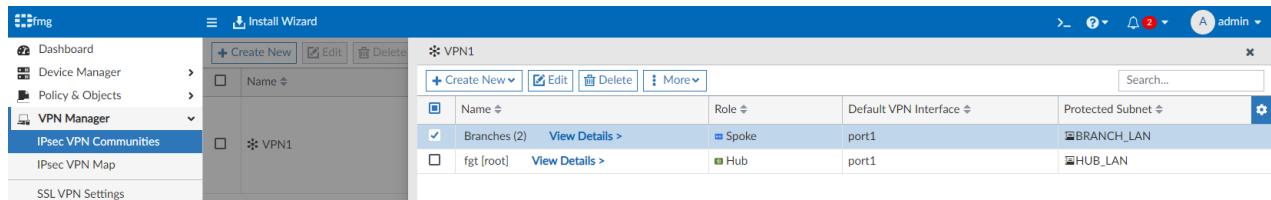
You can now use the certificate in a FortiGate configuration so it will be downloaded and installed to the FortiGate. The certificate may be used in several ways. This example demonstrates how it may be used for IPsec tunnel authentication.



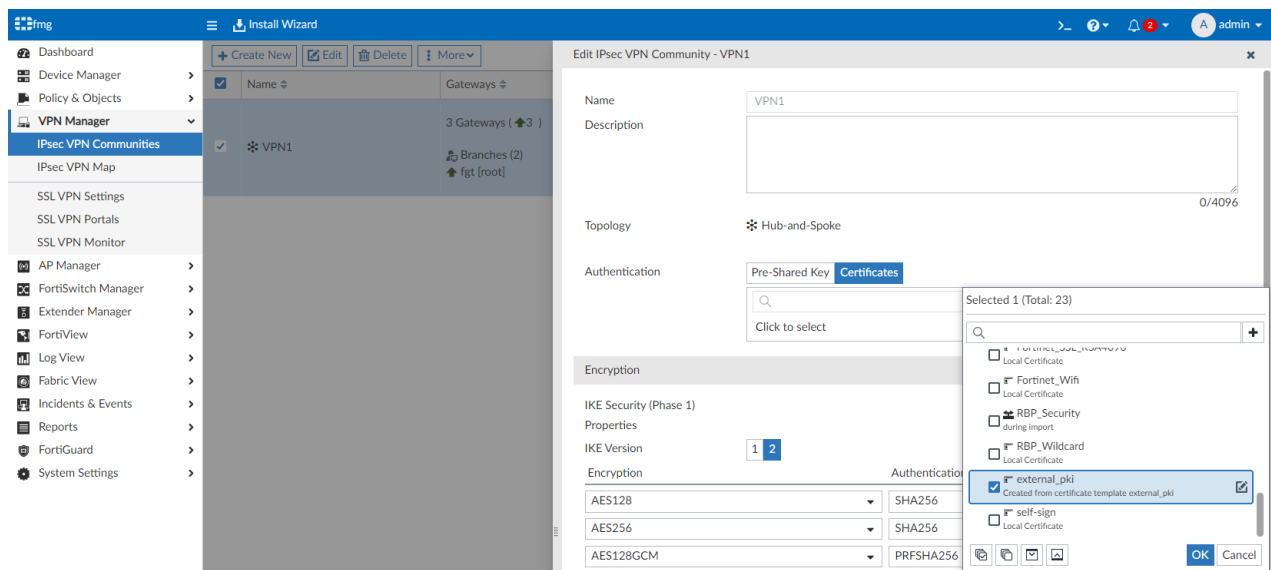
This guide edits an existing hub and spoke VPN set up that is using a PSK for authentication.

To use the certificate in FortiManager:

1. Navigate to *VPN Manager > IPsec VPN Communities*.
2. Select the VPN community you want to update to use automatic certificate enrollment. In this example, the VPN community is *VPN1* and there are three FortiGates in this community: 1 HUB (fgt) and 2 spokes (contained in the *Branches* group: fgt1, fgt2).



3. Edit the community to adjust *Authentication from Pre-Shared Key to Certificates*, and select the *external_pki* certificate created from the certificate template, and select OK to save the selected certificate.

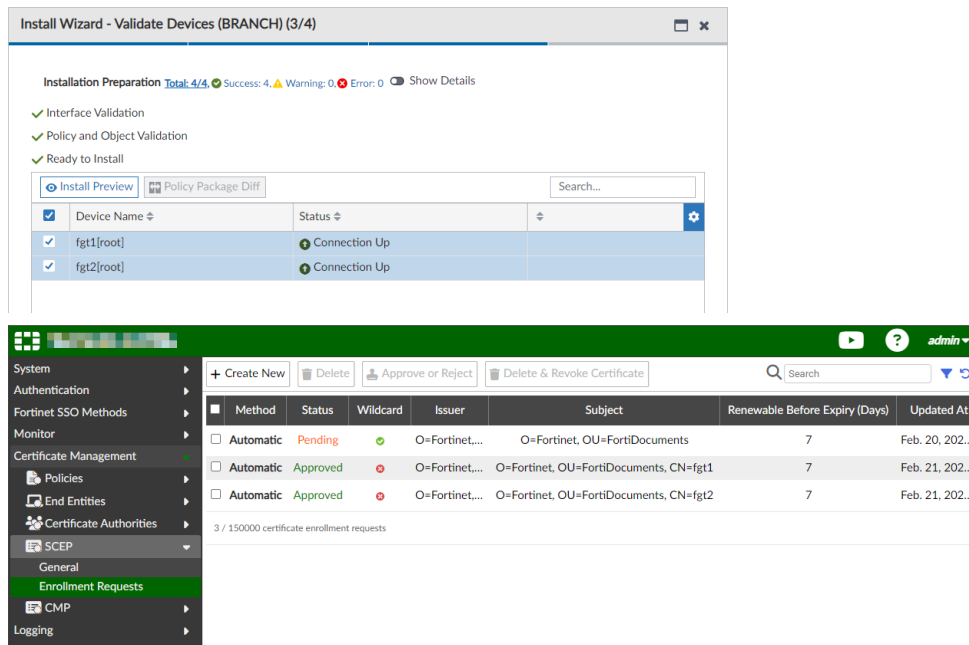


4. Select *OK* to save the community.

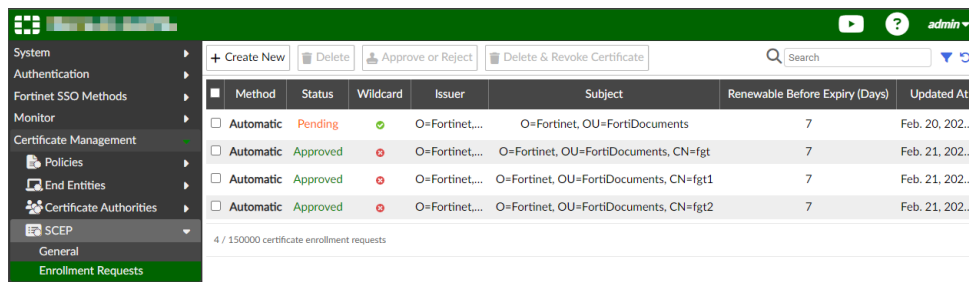
Install the certificate to FortiGate

To install the certificate to a FortiGate:

1. Select *Install Wizard* from the top menu bar.
2. Select the Policy Package for the spoke FortiGates, and select *Next*.
3. Ensure the FortiGates are selected and select *Next*.
4. Once the wizard has completed *Installation Preparation (Validate Devices, step 3/4)*, check the enrollment status on the FortiAuthenticator.



5. Select *Install on FortiManager* to complete the *Install Wizard* and certificate deployment.
6. Repeat the above steps for the HUB FortiGate.



Verification of certificate deployment

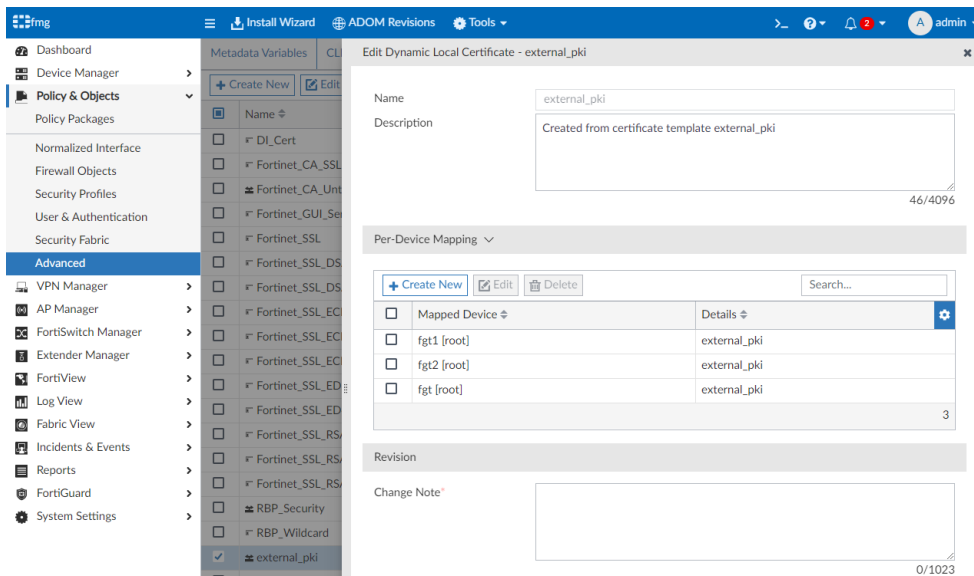
Several certificates will now have been successfully deployed using SCEP. To verify the work, examine the FortiManager and FortiGate configuration.

Verification on FortiManager

On the FortiManager, review the dynamic certificate object, and some VPN monitors.

Dynamic certificate object

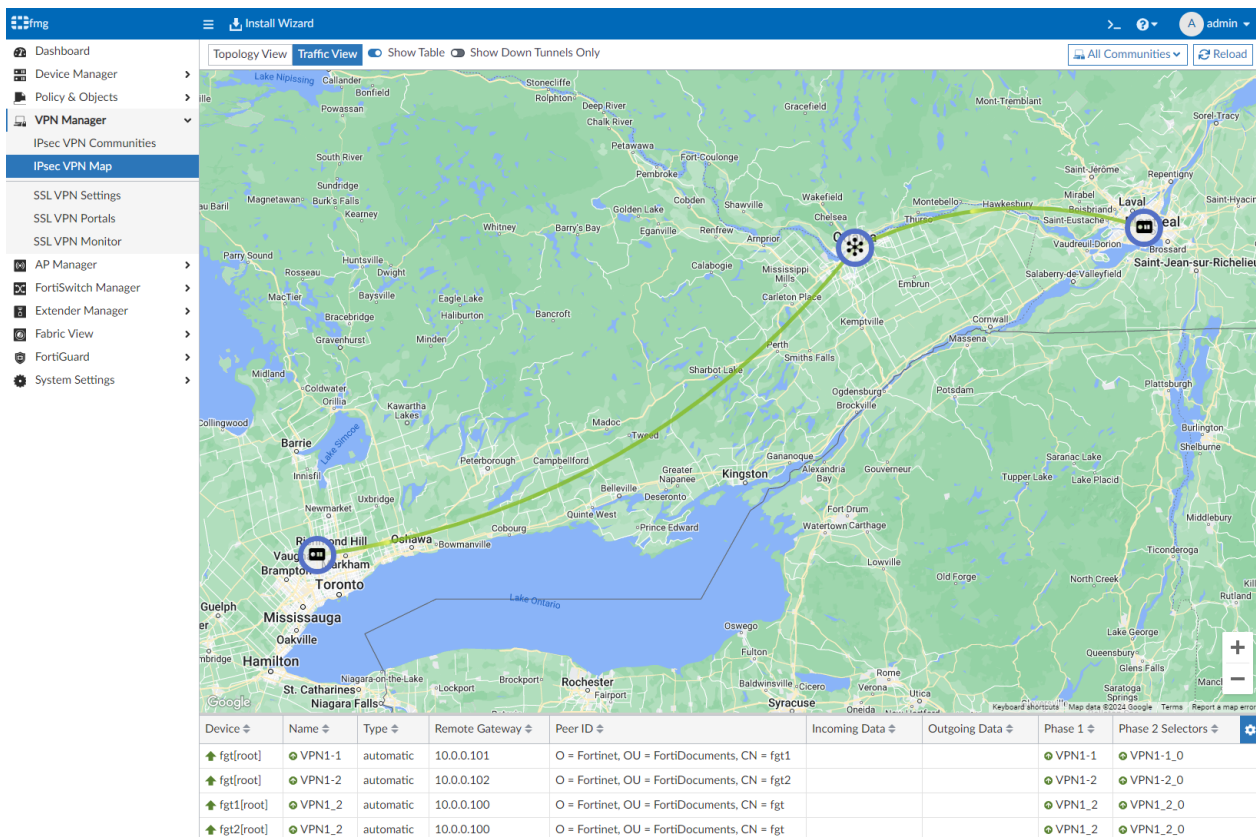
Navigate to *Policy & Objects > Advanced > Dynamic Local Certificate* to examine the *external_pki* certificate. Notice that there are three mappings for the HUB and two branch FortiGates.



You can assign this dynamic certificate to FortiGates without mappings and the SCEP process will automatically generate and deploy a certificate matching the assigned FortiGate.

IPsec VPN map

Review the *VPN Manager > IPsec VPN Map > Topology View* and *Traffic View*. Try enabling *Show Table* on *Traffic View*, and notice the *Peer ID* column. This can be easily used to authenticate.



Verification on FortiGate

Review the certificate and configuration on the FortiGate.

Certificate usage

You can verify the certificate on the FortiGate by navigating to **VPN > IPsec Tunnels**, then double clicking on a tunnel. This shows that a certificate named `external_pki` was used for authentication.

The screenshot displays the FortiGate WebUI interface. The left sidebar shows the navigation menu with 'VPN' and 'IPsec Tunnels' selected. The main content area shows a table of IPsec tunnels. Two tunnels are listed: 'VPN1-1' and 'VPN1-2', both using 'WAN (port1)' as the interface binding and are in 'Up' status. The 'Ref.' column shows the value '3' for both. Below the table, the 'Edit VPN Tunnel' configuration page for 'VPN1-1' is shown. The 'Name' field is 'VPN1-1'. The 'Comments' field contains '[created by FMG VPN Manager]'. The 'Network' section shows 'Remote Gateway: Static IP Address (10.0.0.101), Interface: port1'. The 'Authentication' section shows 'Method' set to 'Signature' and 'Certificate Name' set to 'external_pki'. The 'IKE' section is also visible. On the right side, there is a sidebar with additional information, including 'Managed by FortiManager', 'Additional FortiManager: ::ffff:10.0.0.201', and links to guides and documentation.

Tunnel	Interface Binding	Status	Ref.
VPN1-1	WAN (port1)	Up	3
VPN1-2	WAN (port1)	Up	3

Certificate details

Review the `external_pki` certificate being used in the VPN tunnel.

1. Navigate to **System > Certificates** (enable *Certificates* in *Feature Visibility* if necessary).
2. Notice that the `external_pki` exists in the *Local Certificates* section.

3. Notice that `ca_external_pki` exists in the *Remote CA Certificate* section.

ftg	ftg						
	Edit View Details Download Search						
	Name	Subject	Comments	Issuer	Expires	Status	Source Ref
	Local CA Certificate						
	Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2034/02/09 07:17:54	Valid	Factory 4
	Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2034/02/09 07:17:54	Valid	Factory 4
	Local Certificate						
	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2056/05/26 13:48:33	Valid	Factory 2
	Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2038/01/18 14:34:39	Valid	Factory 0
	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, ...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2026/05/26 10:05:44	Valid	Factory 0
	Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:54	Valid	Factory 0
	Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_SSL_ECDSA512	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:54	Valid	Factory 1
	Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:54	Valid	Factory 1
	Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2026/05/14 08:17:55	Valid	Factory 1
	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert...	This certificate is embedded in the hardware at the factory and is unique...	DigiCert Inc	2024/06/06 16:59:59	Valid	Factory 0
	RBP_Security	CN = Roberts Beef Patties Sub CA		Roberts Beef Patties CA	2034/02/05 11:06:54	Valid	User 1
	RBP_Wildcard	CN = "robertsbg.com		Roberts Beef Patties Sub CA	2025/02/07 11:17:51	Valid	User 0
	SECURITY_RBP_CA	CN = SECURITY RBP CA		Roberts Beef Pattys CA	2034/02/05 07:56:07	Valid	User 0
	external_pki	O = Fortinet, OU = FortiDocuments, CN = ftg	Auto generated by template	Fortinet	2025/02/20 09:24:17	Valid	User 2
	Remote CA Certificate						
	Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:27:39	Valid	Factory 0
	Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2038/01/19 14:34:39	Valid	Factory 0
	Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:48:33	Valid	Factory 0
	Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1		DigiCert Inc	2030/09/23 16:59:59	Valid	Factory 0
	RBP_CA	CN = Roberts Beef Patties CA		Roberts Beef Patties CA	2034/02/05 11:06:55	Valid	User 0
	RBP_SUB_CA	CN = Roberts Beef Patties Sub CA		Roberts Beef Patties CA	2034/02/05 11:06:54	Valid	User 0
	ca_external_pki	O = Fortinet, OU = FortiDocuments, CN = external-pki		Fortinet	2034/02/13 09:02:47	Valid	User 0

4. Double-click either or both certificates to review their details.

Others

This section contains the following topics:

- [Managing FortiAnalyzer from FortiManager on page 48](#)
- [Creating a third party blocklist provider workflow on page 56](#)

Managing FortiAnalyzer from FortiManager

This section contains the following topics:

- [Adding FortiAnalyzer to FortiManager on page 48](#)
- [Viewing managed FortiAnalyzer behavior on page 52](#)
- [Centrally configuring FortiGate to send logs to managed FortiAnalyzer on page 53](#)
- [Viewing logs and reports for managed FortiAnalyzer units on page 53](#)
- [Managing multiple FortiAnalyzer units on page 54](#)
- [Troubleshooting managed FortiAnalyzer units on page 55](#)

Adding FortiAnalyzer to FortiManager

You can add a FortiAnalyzer unit to FortiManager and use FortiManager to manage FortiAnalyzer, but you must add the FortiAnalyzer unit to an ADOM used for central management, which is similar to adding FortiGate units to FortiManager for central management.

You can use the following methods to add FortiAnalyzer units to FortiManager:

- In FortiManager, use the *Add FortiAnalyzer* wizard in the *Device Manager* pane.
- In FortiAnalyzer, enable central management, and then go to FortiManager to authorize the device for central management.

This topic includes the following sections:

- [Preparing to add FortiAnalyzer to FortiManager on page 48](#)
- [Using the wizard to add FortiAnalyzer to FortiManager on page 49](#)
- [Additional information on page 50](#)

Preparing to add FortiAnalyzer to FortiManager

When using FortiManager to manage FortiAnalyzer, it is recommended to use a FortiAnalyzer unit with factory settings or a FortiAnalyzer unit that has been reset to the factory settings (`factory-reset`). A FortiAnalyzer unit with factory settings helps avoid conflicts when FortiManager synchronizes the device database to FortiAnalyzer.

To prepare FortiAnalyzer for management by FortiManager:

1. On the FortiAnalyzer unit, enable fgfm access on the interface used to connect to FortiManager.

```
config system interface
edit "port1"
set ip 10.3.121.142 255.255.0.0
set allowaccess fgfm
next
end
```
2. Create an ADOM with the same name as the ADOM in FortiManager, such as *manage_remote_faz*.
FortiAnalyzer and FortiManager must have an ADOM of the same name. When you add FortiAnalyzer to FortiManager, add it to the ADOM of the same name.
3. Set storage settings for the ADOM.

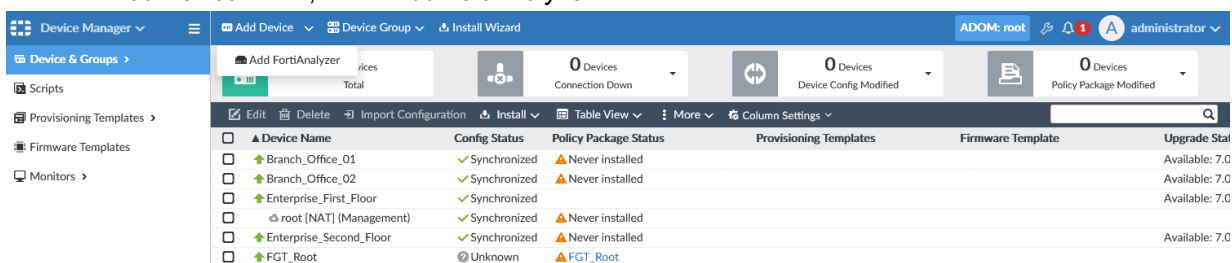
Using the wizard to add FortiAnalyzer to FortiManager

This section describes how to use the *Add FortiAnalyzer* wizard to add FortiAnalyzer to FortiManager.

To add FortiAnalyzer to FortiManager:

1. On FortiManager, ensure that FortiAnalyzer Features are disabled.
 - a. Go to *System Settings > Dashboard*.
 - b. In the *System Information* widget, ensure that *FortiAnalyzer Features* are toggled *Off*.
2. Ensure that the ADOM mode is set to normal by using the following CLI command:

```
config system global
set adom-mode normal
end
```
3. Go to *Device Manager*, and select a central management ADOM, such as *manage_remote_faz*.
The FortiAnalyzer unit should contain an ADOM of the same name. In this example, both FortiAnalyzer and FortiManager have an ADOM named *manage_remote_faz*.
4. On the *Device & Groups* tab, add the FortiAnalyzer unit.
 - a. From the *Add Device* menu, select *Add FortiAnalyzer*.



The *Add FortiAnalyzer* wizard is displayed.

- b. Type the FortiAnalyzer IP address, username, password, and click *Next*.

The screenshot shows the 'Add FortiAnalyzer' wizard. It has a 'Discover' section with a text box for the IP address (10.3.121.142), a text box for the username (root), and a password field (masked with asterisks). There are 'Next' and 'Cancel' buttons at the bottom.

After FortiManager discovers the device, device information is displayed.

Add FortiAnalyzer

The following information has been discovered from the device:

IP Address	10.3.121.142
Host Name	FAZ1000E
SN	FC18E2B1A000004
Model	FortiAnalyzer-1000E
Firmware Version	6.0.4 build2792 (GA)
HA Status	Standalone
Administrator	Pat

Please input the following information to complete addition of the device:

Name:

Description:

- c. Click **Next** to continue.

Add FortiAnalyzer

Status: Comparing ADOM and devices on both sides...

FortiManager automatically compares ADOMs and devices on both FortiAnalyzer and FortiManager and provides the comparison and verification results.

Add FortiAnalyzer

Status: Verifying managed/logging devices on both sides...

Status	Device Name	Platform
FortiManager Only	FGVMD2000008807	FortiGate-VN64
FortiManager Only	FGVMD2000008808	FortiGate-VN64
FortiManager Only	EQH	FortiGate-VN64
FortiManager Only	Central	FortiGate-VN64
FortiManager Only	NAM	FortiGate-VN64
FortiManager Only	FGVMD2010100073	FortiGate-VN64

- d. Click **Synchronize ADOM and Devices** to continue.

Devices are synchronized between FortiAnalyzer and FortiManager, and FortiAnalyzer is added to FortiManager. The synchronized devices are added to FortiAnalyzer as logging-mode FortiGates.

Add FortiAnalyzer

Status: FortiAnalyzer Added Successfully

FortiAnalyzer is added to FortiManager.

- e. Click **Finish**.

5. Go to **Device Manager > Device & Groups** to view FortiAnalyzer in the *Managed FortiAnalyzer* group.

Device Name	IP Address	Platform	Description
FAZ1000E	10.3.121.142	FortiAnalyzer-1000E	

Additional information

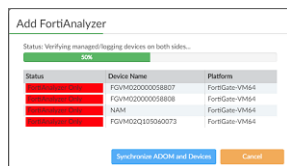
This section describes some of the other scenarios you might encounter when adding FortiAnalyzer units to FortiManager.

Missing ADOM

If the current ADOM in FortiManager does not exist on FortiAnalyzer, FortiManager automatically creates an ADOM with same name and version on FortiAnalyzer before starting to synchronize the device list.

Unknown or mismatched FortiGate devices

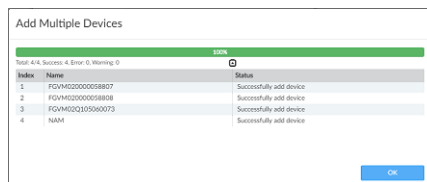
If FortiAnalyzer is receiving logs from FortiGate devices that do not exist on FortiManager, FortiManager identifies the devices.



FortiManager automatically attempts to discover the FortiGates.

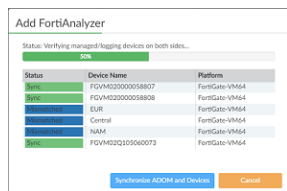


FortiManager can add the FortiGates and retrieve configurations for the FortiGates when adding the FortiAnalyzer unit.

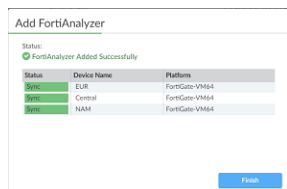


If one device fails to add or retrieve, FortiManager fails to add FortiAnalyzer.

If the same FortiGate device exists on both FortiManager and FortiAnalyzer, but with differences, FortiManager considers the device to be *Mismatched*.



FortiManager tries to synchronize the device settings to FortiAnalyzer.



If any errors occur during the synchronization step, FortiManager fails to add FortiAnalyzer.

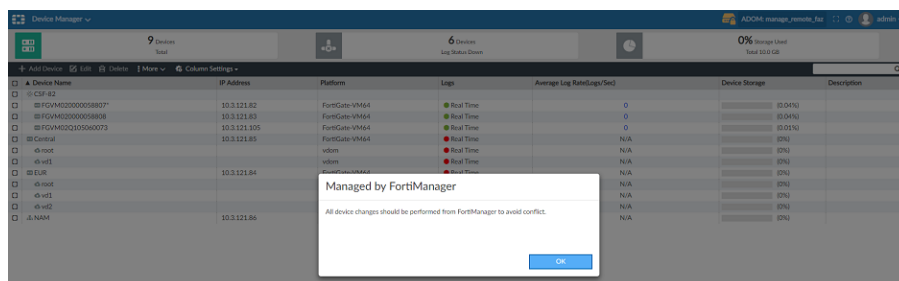
Viewing managed FortiAnalyzer behavior

After FortiManager manages the ADOM with FortiAnalyzer in it, you should use FortiManager to perform changes on all devices in the ADOM. This topic describes the behavior you will view in the GUI for a FortiAnalyzer unit that is managed by FortiManager.

To view managed FortiAnalyzer behavior:

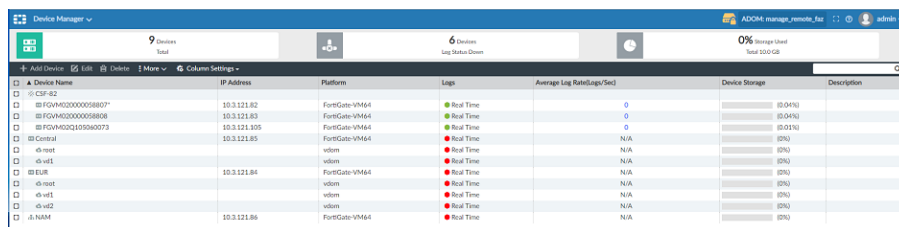
1. Log in to the FortiAnalyzer unit.
2. Go to the *Device Manager* pane.

The *Managed by FortiManager* message is displayed.



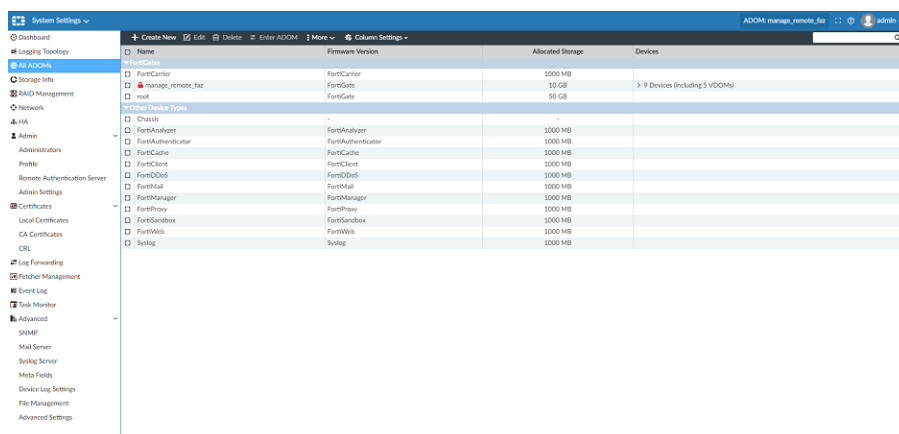
3. Click *OK*.

Notice the *Lock* icon displayed on top bar, and notice that the *Add Device*, *Edit*, and *Delete* buttons are unavailable.



4. Go to *System Settings > All ADOMs*.

Notice the lock icon beside the ADOM that is managed by FortiManager. You can no longer edit devices in the ADOM.

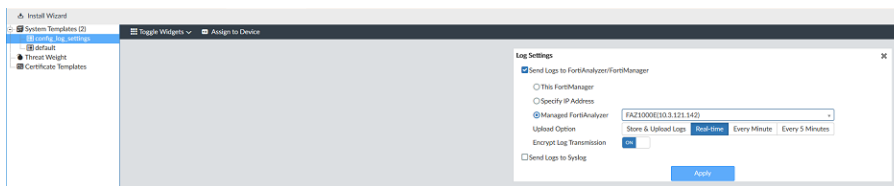


Centrally configuring FortiGate to send logs to managed FortiAnalyzer

After adding FortiAnalyzer to FortiManager, the device list is also synchronized to FortiAnalyzer. To make these FortiGate devices send log to FortiAnalyzer, you can use provisioning templates to centrally configure the log settings for FortiGates.

To centrally configure logging:

1. In FortiManager, go to *Device Manager > Provisioning templates*.
2. Create a new blank system template.
 - a. In the content pane, click *Create New*.
 - b. Type a name for the system template, and click *OK*.
The system template is created.
 - c. Select the system template, and click *Edit*.
The template opens for editing. You can enable the *Log Settings* widget by selecting it from the *Toggle Widgets* dropdown.
- d. In the *Log Settings* widget, select *Send Logs to FortiAnalyzer/FortiManager*.
- e. Select *Managed FortiAnalyzer*, and select the unit from the drop-down list.
- f. Click *Apply*.
3. Assign the system template to FortiGates.
4. Install the system template to FortiGates.



Viewing logs and reports for managed FortiAnalyzer units

After you add FortiAnalyzer to the ADOM in FortiManager, the following FortiAnalyzer panes are available in FortiManager:

- FortiView
- Log View
- FortiSoC
- Reports

All FortiAnalyzer functionality is available, except for the following:

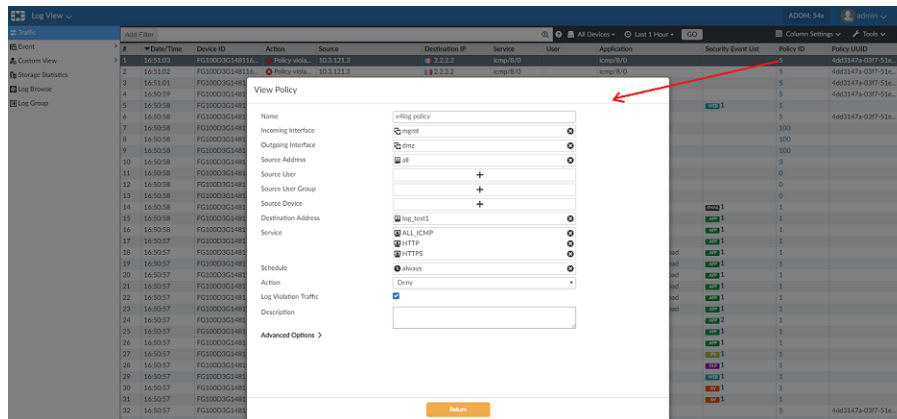
- Importing and exporting a report template
- Importing and exporting a chart
- Importing and downloading a log file

In FortiManager, when you create a report and run it, and the same report is generated in the managed FortiAnalyzer.

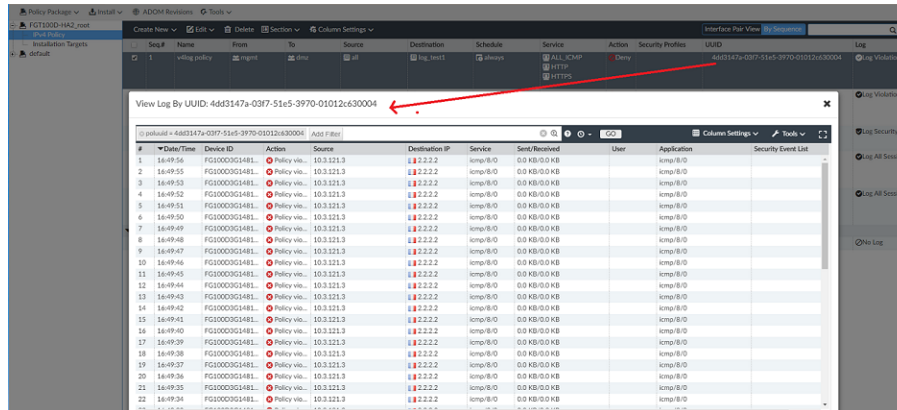
To view logs and reports:

1. On FortiManager, go to **Log View**.
You can view all logs received and stored on FortiAnalyzer.
2. Click the **Policy ID**.
The policy rule opens.

If the policy rule doesn't open, ensure that you have imported the policy rules to the ADOM.



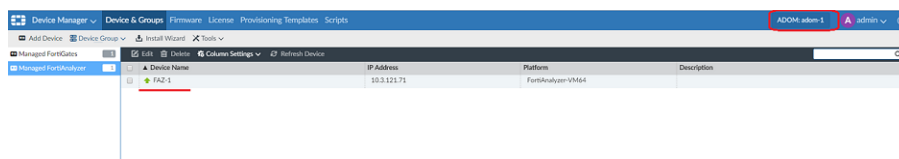
3. Go to **Policy & Objects > Policy Packages**, and right-click the policy UUID to search the related policy logs.



Managing multiple FortiAnalyzer units

FortiManager can manage multiple FortiAnalyzer units, but each FortiAnalyzer must be in its own ADOM. You cannot add a second FortiAnalyzer unit to an ADOM.

For example, FortiManager can contain the following ADOMs: *adom-1* and *adom-2*, and *adom-1* manages FAZ-1:



The other ADOM, *adom-2*, manages FAZ-2:

Device Name	IP Address	Platform	Description
FAZ-2	10.3.121.142	FortiAnalyzer-1000E	

Following is another view of the ADOMs with FortiAnalyzer units:

Name	Firmware Version	Central VPN	Devices
FortiCenter	FortiCenter 5.2		
adom-1	FortiGate 5.4		2 Devices (including 0 VDOMs)
adom-2	FortiGate 5.4		2 Devices (including 0 VDOMs)
root	FortiGate 5.4		
Global Database	Global 5.2		
FortiAnalyzer	FortiAnalyzer		
FortiAuthenticator	FortiAuthenticator		
FortiCache	FortiCache		
FortiClient	FortiClient		
FortiCloud	FortiCloud		
FortiMail	FortiMail		
FortiManager	FortiManager		
FortiSandbox	FortiSandbox		
FortiWeb	FortiWeb		
Swing	Swing		
Chassis	.		

Troubleshooting managed FortiAnalyzer units

This topic describes how to troubleshoot several situations.

Adding FortiAnalyzer failed

If adding FortiAnalyzer failed, enable the following debug command, which will provide error or information in a debug log, and then try adding FortiAnalyzer again.

```
diagnose debug application depmanager 255
diagnose debug enable
```

example: add_faz_dep_debug.txt

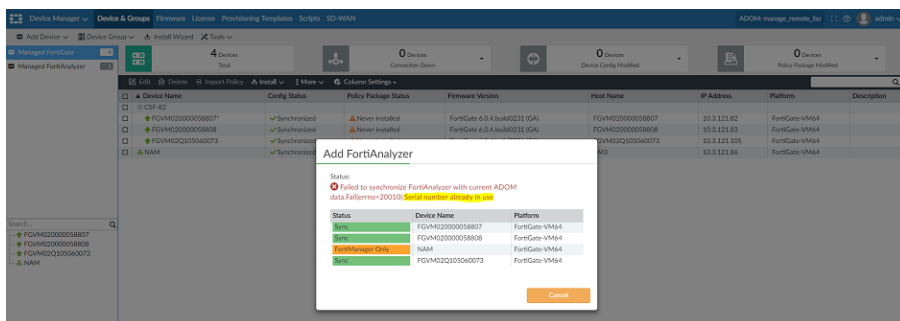
ADOM remains locked on FortiAnalyzer

When you delete FortiAnalyzer from FortiManager, the ADOM on FortiAnalyzer should be unlocked. If the ADOM remains locked, you can use the following command on the FortiAnalyzer unit to unlock the ADOM:

```
FAZ1000E # diag dvm adom unlock
adom ADOM name.
FAZ1000E # diag dvm adom unlock remote-faz
---Deleting DVM lock by remote FortiManager succeeded---
FAZ1000E#
```

Serial number already in use

The Alert console might display the *Serial number already in use* message. FortiManager might also display the *Serial number already in use* message after failing to add FortiAnalyzer.



You can use the `diagnose dvm device list` command on the FortiAnalyzer unit and on the FortiManager unit to see if the same FortiGate unit already exists on the FortiAnalyzer unit, but in different ADOM.

```

FGM000 Login: admin
Password:
FGM000 # diagnose dvm device list
... There are currently 4 device/adoms managed ...

TYPE      QID  SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
mgmt/faz  501  FQVM020000058807  10.3.121.82  FQVM020000058807  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz  513  FQVM020000058808  10.3.121.83  FQVM020000058808  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz  489  FQVM020105060073  10.3.121.105  FQVM020105060073  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz  476  FQVM020000058811  10.3.121.88  N/A      manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
HA cluster member: FQVM020000058811 (master)
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
... There are currently 0 FortiAP managed ...
... There are currently 0 FortiSwitch managed ...
... There are currently 0 FortiExtender managed ...
... End device list ...
FGM000 #

FAZ000 Login: admin
Password:
FAZ000 # diagnose dvm device list
... There are currently 4 device/adoms managed ...

TYPE      QID  SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
mgmt/faz  273  FQVM020000058807  10.3.121.82  FQVM020000058807  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz  271  FQVM020000058808  10.3.121.83  FQVM020000058808  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz  272  FQVM020105060073  10.3.121.105  FQVM020105060073  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/faz  308  FQVM020000058811  10.3.121.88  N/A      root      6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
HA cluster member: FQVM020000058811 (master)
|- vdom:[1]root flags:0 adom:root pkg:[never-installed]
... There are currently 0 FortiAP managed ...
... There are currently 0 FortiSwitch managed ...
... There are currently 0 FortiExtender managed ...
... End device list ...
FAZ000 #

Compare the device list on FGM and FAZ. Both FGM and FAZ
have device "FQVM020000058811" but it is in different
ADOM (on FGM it is in ADOM "manage_remote_faz" on
FAZ it is in ADOM "root"). That is why we saw the error
"Failed to sync devdb to FAZ: Serial number already in
use".
To solve the problem, manually move the device
"FQVM020000058811" to ADOM "manage_remote_faz"
on FAZ. You may need to rebuild the DB if want to view the
old log after move the device.

```

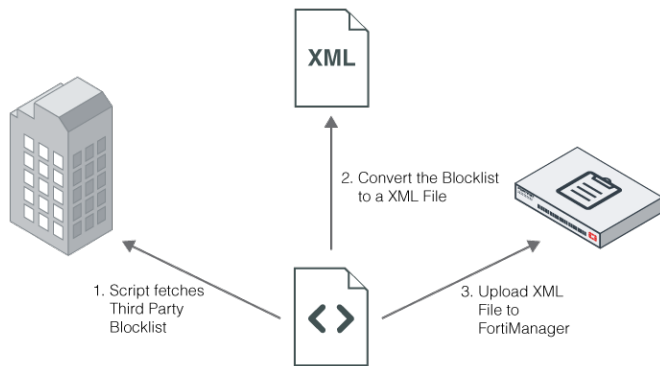
Creating a third party blocklist provider workflow

In this example, you will learn how to use your FortiManager to create a third party blocklist provider workflow.

Overview

You must create a script that will handle the entire workflow. Make sure the script can convert the third party blocklist into a FortiManager XML file.

From an external server, you must schedule the periodic execution of that script. Using the communication tools provided by the third party blocklist provider, the script will fetch the blocklist from the third party.



To create a script to handle a third party blocklist provider workflow:

1. Convert the blocklist to a FortiManager XML file:

The script will convert the blocklist to a FortiManager XML file. This XML file allows you to assign a category to each URL in the list, in addition to a default category. The default category is used as the return value when there is no match.

Example of the FortiManager XML file format:

```
<custom_url_list version="1.0">
  <head>
    <default_cate>142</default_cate>
    <description>the description</description>
  </head>
  <body>
    <url_entry>
      <url>http://www.url-0000001.com</url>
      <cate>79</cate>
    </url_entry>
    <url_entry>
      <url>http://www.url-0000001.com</url>
      <cate>28</cate>
    </url_entry>
  </body>
</custom_url_list>
```

The category value in `<cate></cate>` could be either a normal web filter category or a local category.

2. Upload the XML file into FortiManager:

The script uses SSH to connect to FortiManager and upload the XML file.

CLI command:

```
execute fmupdate <ftp|scp|tftp> import custom-url <xml filename> <ftp|scp|tftp details>
```

Example:

```
# execute fmupdate scp import custom-url 20M-custom-url.xml 000.000.000.000 00
  tmp/FORTIGUARD my_login my_password
```

This operation will replace the current <custom-url> package!

Do you want to continue? (y/n)y

Start getting file from remote SCP Host...

SCP transfer successful.

Packing installation is in process...This could take some time.

lccclient command result:Response=202|

Update successfully

In this example, FortiManager will upload the file from the following file:

```
scp://my_login:my_password@000.000.000.000:00/temp/FORTIGUARD/20M-custom-url.xml
```

3. Configure FortiManager to only use its local FortiGuard database or local blocklist database:

a. Select one of the following:

- Local FortiGuard database
- Local blocklist database
- Or both

```
config fmupdate custom-url-list
  set db_selection <fortiguard-db|custom-url|both>
end
```

4. Test custom URLs managed by FortiManager:

a. Use the CLI in FortiManager to send categorization requests for custom URLs managed by FortiManager.

Example of the CLI command set:

```
# diagnose fmupdate fgd-url-rating FGT SN 1 www.foo.com
url rating flags: 0x2 (2:EXACT_MATCH, 1:PREFIX_MATCH)
rates according to url: 0x37 0x00 0x00 0x00
rates according to ip: 0x00 0x00 0x00 0x00
num_dots:-1, num_slash:-1
database version: 16.45562
0 ms
```

The *FGT SN* can be any FortiGate SN.

The returned category is in a hexadecimal output: *0x37*.

In decimal format, the category is *56* or *Web Hosting*.



The memory capacity of the unit determines the number of URLs FortiManager can manage.

5. Specify FortiManager as the FortiGuard server in FortiGate

a. Go to your FortiGate CLI console and execute the following commands:

```
config system centralmanagement
  set type fortimanager
  set {<IP_address> | <FQDN_address>}
  config serverlist
    edit 1
      set servertype
      update rating
      set serveraddress {<IP_address> | <FQDN_address>}
    next
  end
  set includedefaultservers disable
end
```



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Document Library](#).



www.fortinet.com

Copyright© 2024 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 General Counsel, 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.