



Examples

FortiManager 8.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 21, 2026

FortiManager 8.0 Examples

02-800-1281557-20260421

TABLE OF CONTENTS

Change Log	5
Introduction	6
Device Manager	7
Exporting a policy package from one FortiManager to another	7
Intrusion prevention	9
Managing IPS signature updates as an IPS administrator	9
View signature details on FortiGuard	9
Configure and install signature overrides	12
Monitor logs for hits to signatures	16
System Settings	23
Configuring and debugging FortiManager HA clusters	23
Configuring the primary FortiManager unit in an HA cluster	23
Configuring backup FortiManager units in an HA cluster	24
Generating and downloading HA debug logs	24
Creating administrator accounts with restricted access	25
Restricting administrator access to ADOMs	25
Restricting administrator access to device groups	27
Restricting administrator access to policy packages	29
Certificate deployment	30
Configuring FortiManager to deploy certificates for admin GUI access	30
Creating the certificate for administrator web access	30
Uploading the certificate to FortiManager	32
Apply the certificate to the FortiGate in FortiManager	32
Install the certificate	32
Verify the certificate was installed correctly	33
Configuring FortiManager to deploy certificates for deep inspection	33
Generate a CA certificate on FortiAuthenticator	33
Generate an intermediate CA certificate	34
Upload the intermediate CA certificate to FortiManager	34
Use the certificate in a policy and install the Policy Package	35
Verify on an endpoint	35
Configuring FortiManager to deploy SAML certificates	36
Create a local CA on the FortiAuthenticator	36
Create the Identity Provider (IdP) certificate used in SAML	39
Create the IdP portal on FortiAuthenticator	39
Allowing IdP service on FortiAuthenticator	40
Defining a local user on the FortiAuthenticator	41
Defining SAML SP settings on FortiManager	41
IdP portal SP settings continued	42
Testing the configuration	42
Using FortiManager to provision the SAML certificates to FortiGates	43
Configure FortiManager to install SAML configuration on the FortiGate	44
Testing the configuration	46
Configuring FortiManager and FortiAuthenticator for SCEP certificate deployment	47

Configuring FortiAuthenticator	47
Configuring FortiManager	50
Verification of certificate deployment	53
Others	57
Managing FortiAnalyzer from FortiManager	57
Adding FortiAnalyzer to FortiManager	57
Viewing managed FortiAnalyzer behavior	61
Centrally configuring FortiGate to send logs to managed FortiAnalyzer	62
Viewing logs and reports for managed FortiAnalyzer units	63
Managing multiple FortiAnalyzer units	64
Troubleshooting managed FortiAnalyzer units	65
Creating a third party blocklist provider workflow	66

Change Log

Date	Change Description
2026-04-21	Initial release.

Introduction

This document serves as a reference guide to common FortiManager 8.0 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 8.0:

- [Device Manager on page 7](#)
- [Managing IPS signature updates as an IPS administrator on page 9](#)
- [System Settings on page 23](#)
- [Certificate deployment on page 30](#)
- [Others on page 57](#)

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](#).

Intrusion prevention

This section contains the following topics:

- [Managing IPS signature updates as an IPS administrator on page 9](#)

Managing IPS signature updates as an IPS administrator

FortiGate receives IPS signature package updates from the FortiGuard Distribution Server (FDS).

The FDS can either be the Fortinet Global FDS service or a FortiManager acting as the FDS. In this example, the FortiManager is acting as the FDS. For information on configuring FortiManager as the FDS, see the [Configuring Devices to use the Built in FDS](#).

The following example also assumes that an IPS restricted administrator is logged in and completing the steps. For more information on restricted administrators, see [Intrusion prevention restricted administrator](#).

This example provides a methodology for managing the release of IPS signature package updates to managed FortiGate devices based on the following steps:

1. [View signature details on FortiGuard on page 9](#)
2. [Configure and install signature overrides on page 12](#)
3. [Monitor logs for hits to signatures on page 16](#)



This example does not present a definitive method, but instead outlines an approach that can be used to build one that aligns with your requirements

View signature details on FortiGuard

To view signature information on FortiGuard:

1. Log in to FortiManager as a restricted IPS administrator.
2. Go to *Intrusion Prevention > FortiGuard Package*.
3. Confirm that the initial *To Be Deployed Version* has been specified for the relevant IPS Signature Database. In this example, the initial version is set to 28.00871, but the *Latest Version* available from FortiGuard is 28.00872.

Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Ver
Industrial Definitions (Industrial)	FortiGate	7.4.0+	Industrial Security	07004000ISDB00105	28.00872 (2024-09-26 00:49:00)	185.97 KB	Latest Change
IPS Engine (64bit)	FortiGate	7.4.0+	IPS	07004000FLEN07600	7.00539 (2024-05-09 17:05:00)	5.98 MB	7.00539 Change
IPS Signature Database (Extended)	FortiManager	6.0.12+	IPS	06000000NIDS02603	28.00872 (2024-09-26 00:53:00)	1.55 MB	28.00871 Change
<input checked="" type="checkbox"/> IPS Signature Database (Slim Extended)	FortiGate	7.4.0+	IPS	07004000NIDS02605	28.00872 (2024-09-26 00:52:00)	1.04 MB	28.00871 Change
Malicious URL Database	UNKNOWN	7.4	IPS	07004000MUDB00103	5.00185 (2024-09-26 13:47:00)	7.18 MB	Latest Change
Signature Meta Data	FortiManager	7.0.0+	IPS	07000000NIDS02600	28.00872 (2024-09-26 00:57:00)	609.86 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	5.4.0+	FortiCare	05004000NIDS02300	28.00872 (2024-09-26 00:57:00)	99.38 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	6.0.9+.6.2.0	FortiCare	05006000APDB00100	28.00872 (2024-09-26 00:51:00)	60.03 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	6.2.1-6.2.8,6.4.0-6.4.1,7.0.0	FortiCare	06000000APDB00100	28.00872 (2024-09-26 00:51:00)	60.03 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	6.2.9+	FortiCare	06002000APDB00100	28.00872 (2024-09-26 00:51:00)	66.24 KB	Latest Change

4. Click on the hyperlink for the *Latest Version* to open the FortiGuard IPS Updates site.

Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Ver
Industrial Definitions (Industrial)	FortiGate	7.4.0+	Industrial Security	07004000ISDB00105	28.00872 (2024-09-26 00:49:00)	185.97 KB	Latest Change
IPS Engine (64bit)	FortiGate	7.4.0+	IPS	07004000FLEN07600	7.00539 (2024-05-09 17:05:00)	5.98 MB	7.00539 Change
IPS Signature Database (Extended)	FortiManager	6.0.12+	IPS	06000000NIDS02603	28.00872 (2024-09-26 00:53:00)	1.55 MB	28.00871 Change
<input checked="" type="checkbox"/> IPS Signature Database (Slim Extended)	FortiGate	7.4.0+	IPS	07004000NIDS02605	28.00872 (2024-09-26 00:52:00)	1.04 MB	28.00871 Change
Malicious URL Database	UNKNOWN	7.4	IPS	07004000MUDB00103	5.00185 (2024-09-26 13:47:00)	7.18 MB	Latest Change
Signature Meta Data	FortiManager	7.0.0+	IPS	07000000NIDS02600	28.00872 (2024-09-26 00:57:00)	609.86 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	5.4.0+	FortiCare	05004000NIDS02300	28.00872 (2024-09-26 00:57:00)	99.38 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	6.0.9+.6.2.0	FortiCare	05006000APDB00100	28.00872 (2024-09-26 00:51:00)	60.03 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	6.2.1-6.2.8,6.4.0-6.4.1,7.0.0	FortiCare	06000000APDB00100	28.00872 (2024-09-26 00:51:00)	60.03 KB	Latest Change
Signature Meta Data (Application Control)	FortiManager	6.2.9+	FortiCare	06002000APDB00100	28.00872 (2024-09-26 00:51:00)	66.24 KB	Latest Change

5. Select the chosen version from the dropdown list, and click *FILTER*. This displays all of the changes and additions that were made since the last package.
- This assumes that a regular release schedule is maintained and that the *Latest Version* is only 1 version ahead of the *To Be Deployed Version*.

FortiGuard Labs | News / Research | Services | Threat Intelligence | Resources | About | FORTINET

Intrusion Protection

Version: 28.872

Released Date: Sep 26, 2024 09:33 | + New (5) | Modified (20) | - Removed (1)

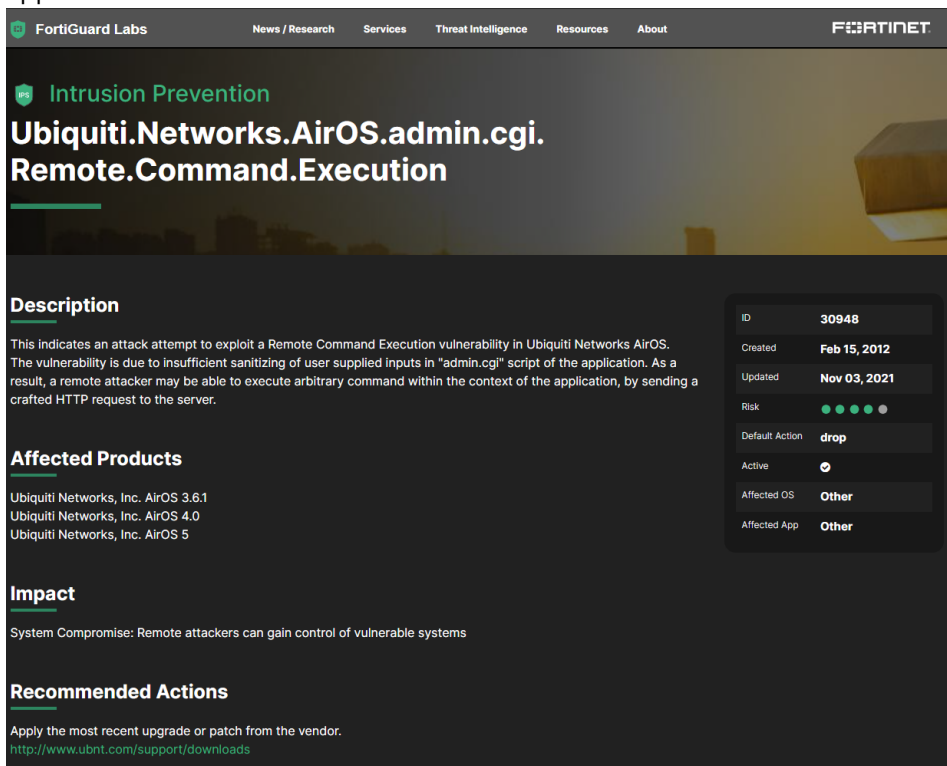
Version: 28.872 | Name: Click to enter a name

FILTER Total: 26

Name	Status	Severity	Update
Corody.CX-E120.Root.Password.Reset.Authentication.Bypass	+ New	●●●●●	
QNAP.QTS.CVE-2017-17033.qpkg.lang.Buffer.Overflow	+ New	●●●●●	

6. Review the signatures that are tagged as *New*, *Modified*, or *Removed*, and evaluate how these signatures may affected protected services.
- Individual signatures can be clicked to view additional details about the signature.
 - Review the *Affected OS*, *Affected App*, and *Default Action* fields, and whether the signature is *Active* or not to determine whether it will be applicable to protected services.
 - If the signature is applicable, review the *Description*, *Risk* score and *CVE* information where available.

- d. An alternative approach is to use an override for all newly added signatures in order to monitor their behavior in production for a specified number of days before removing the override and using the default settings applicable to their signatures. The processes defined here are the same for this approach.



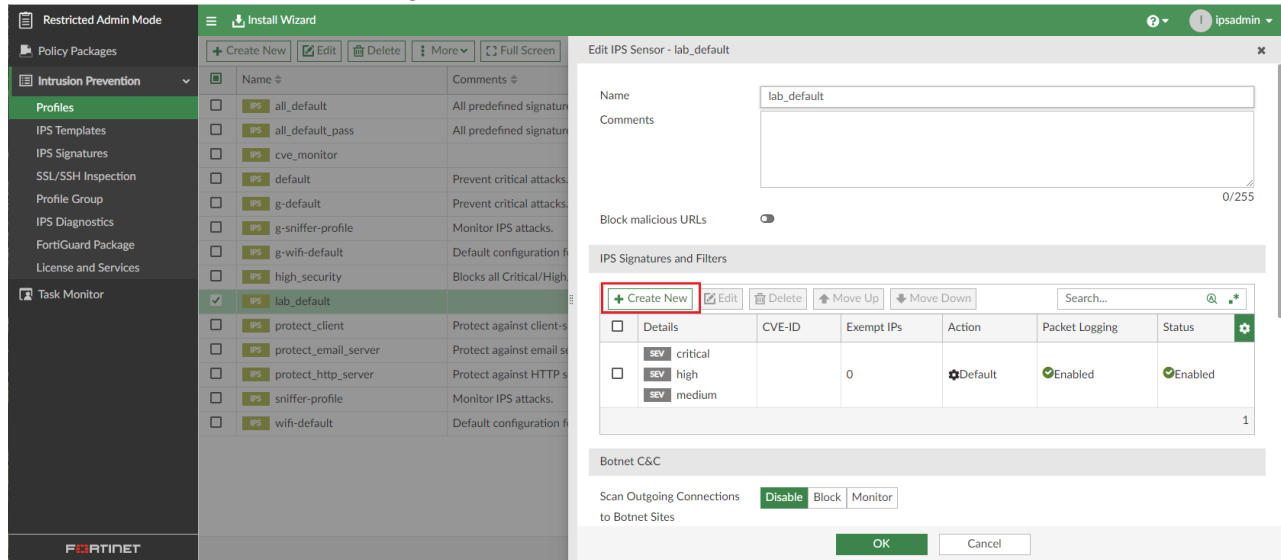
- 7. After completing the review of the signature package changes, return to the FortiManager and if required, create overrides for specific signatures in the new package.

 The new IPS signatures are available to view in FortiManager even though they have not been released to the FortiGates. This allows for administrators to specify overrides before releasing the signatures.

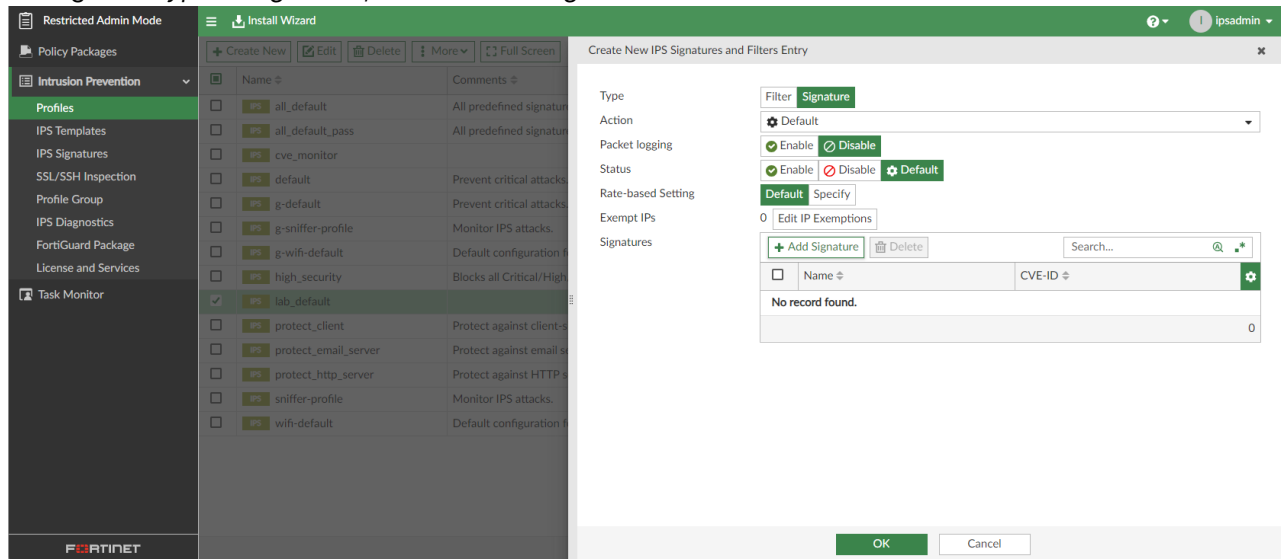
Configure and install signature overrides

To configure signatures on FortiManager:

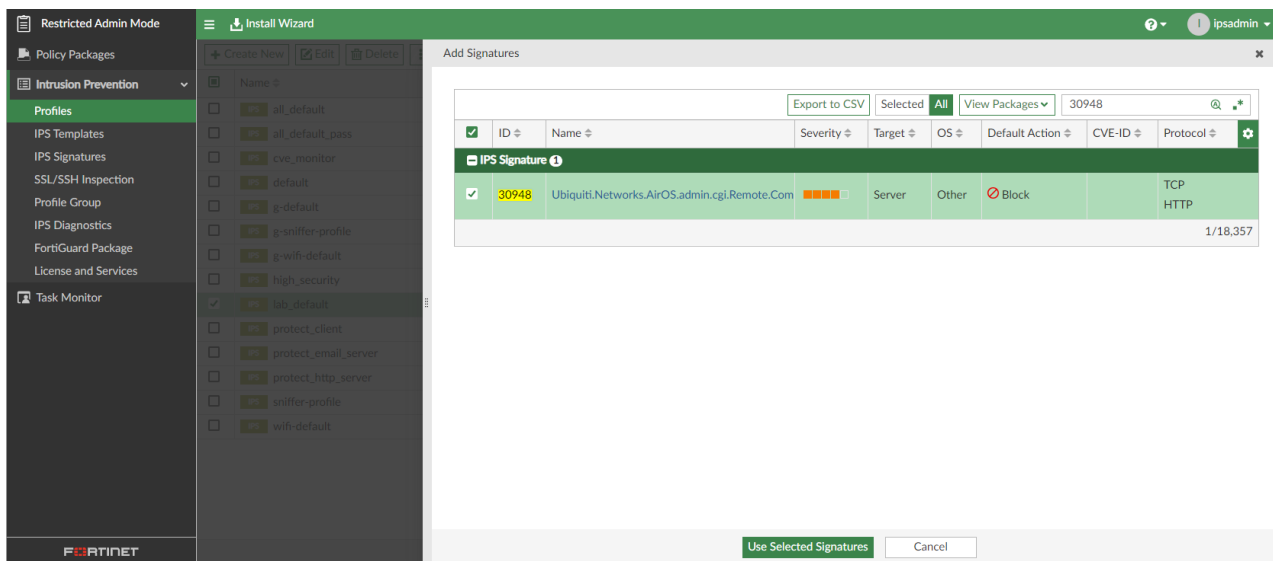
1. Go to *Intrusion Prevention > Profiles* and edit the appropriate IPS Profile(s).
2. Click *Create New* under the *IPS Signatures and Filters* section.



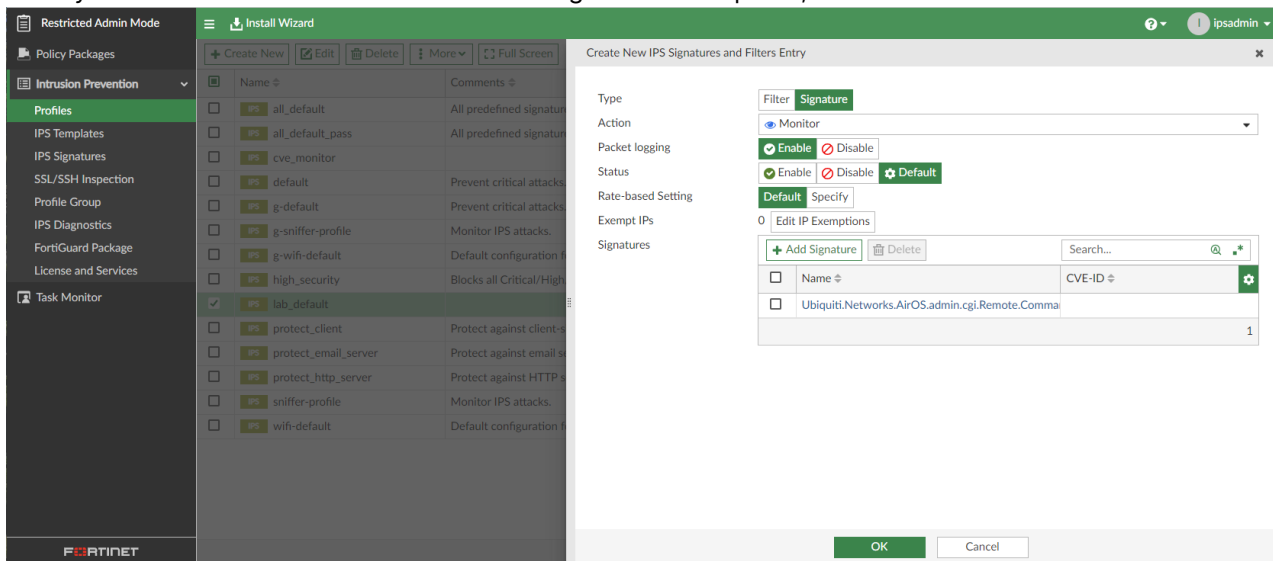
3. Change the *Type* to *Signature*, and click *Add Signature*.



4. Find the required signature(s) by *Name* or *ID*, available from the FortiGuard IPS website. Check the box(es) and click *Use Selected Signature*.



5. Modify the behavior of the FortiGate with this signature as required, and click OK.



Action

The default action is available on [FortiGuard](#).

If the desired approach is to monitor the impact of this signature on production traffic, set this to *Monitor*.

Packet Logging

Determines whether the FortiGate should packet capture the traffic triggering this signature.

This is recommended when using IPS as it provides context as to what triggered the event that pure traffic logs do not.

Status

The default status of the signature is available on [FortiGuard](#).

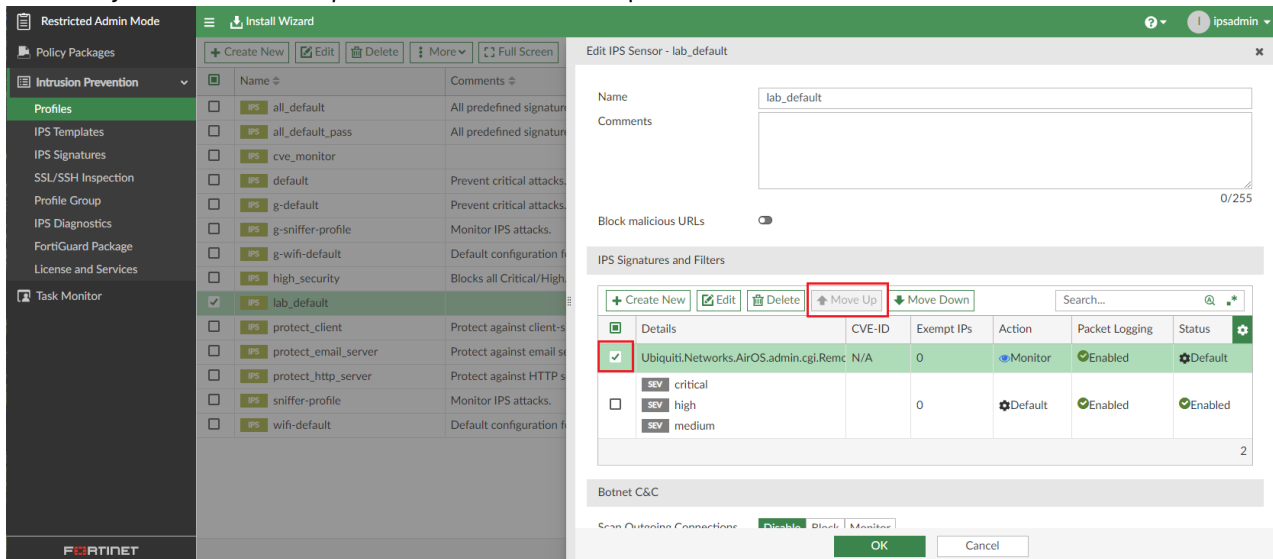
If the signature is set to *Disable* by default, then an override such as described here would only be beneficial if admins wanted to enable a wider range of signatures for an OS/application/protocol/etc. than the defaults but want to monitor the behavior.

In that instance, the *Status* should be set to *Enable*, otherwise *Default* is acceptable as the signature is already enabled.

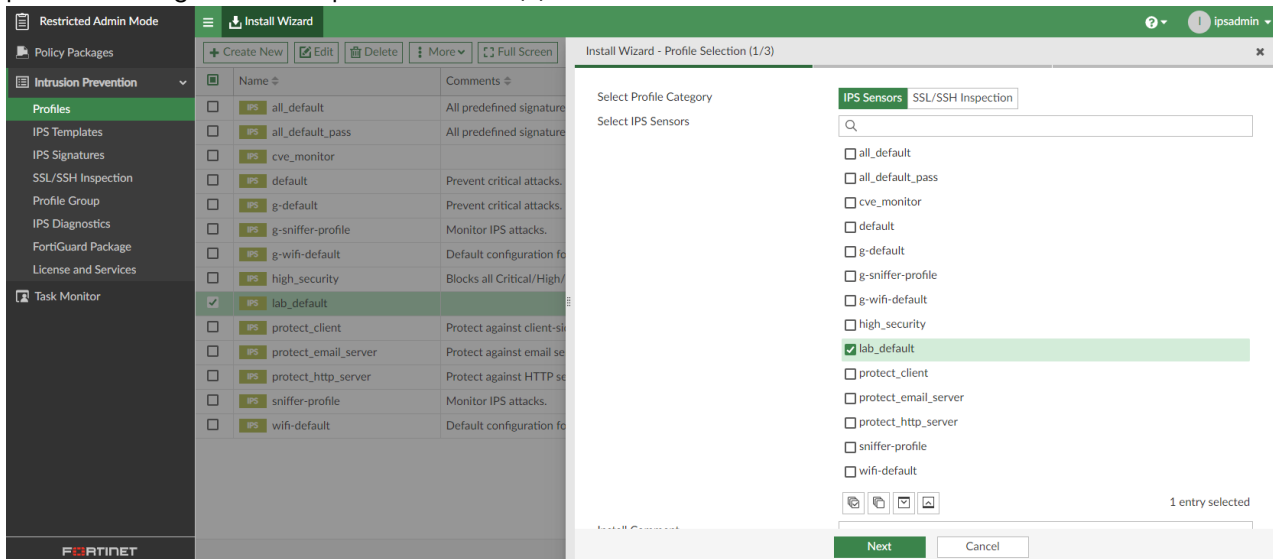
Exempt IPs

This is where administrators can exclude client or server IPs from triggering a signature. This is useful for handling false positive behavior.

- By default, the new profile entries are added to the bottom of the list. As profiles use a top-down/first match approach, the override needs to be located above the general IPS rules in the list. Select the box next to the new entry and click *Move Up* until it is at the desired point in the rule set. Click *OK* to finish.



- This change will need to be installed on the target FortiGates before the IPS package is released. Click *Install Wizard*, select only the profile(s) with the override applied, and complete the install wizard process to push the changes to the required FortiGate(s).



- With the overrides installed, it is time to modify the *To Be Deployed Version* in the *FortiGuard Package* menu. Select the IPS Signature Database appropriate to the deployment and click the *Change* button.

Package Name	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Version
Industrial Definitions (Industrial)	7.4.0+	Industrial Security	07004000ISDB00105	28.00872 (2024-09-26 00:49:00)	185.97 KB	Latest Change
IPS Engine (64bit)	7.4.0+	IPS	07004000FLEN07600	7.00539 (2024-05-09 17:05:00)	5.98 MB	7.00539 Change
IPS Signature Database (Extended)	6.0.12+	IPS	06000000NIDS02603	28.00872 (2024-09-26 00:53:00)	1.55 MB	28.00871 Change
<input checked="" type="checkbox"/> IPS Signature Database (Slim Extended)	7.4.0+	IPS	07004000NIDS02605	28.00872 (2024-09-26 00:52:00)	1.04 MB	28.00871 Change
Malicious URL Database	7.4	IPS	07004000MUDB00103	5.00185 (2024-09-26 13:47:00)	7.18 MB	Latest Change
Signature Meta Data	7.0.0+	IPS	07000000NIDS02600	28.00872 (2024-09-26 00:57:00)	609.86 KB	Latest Change
Signature Meta Data (Application Control)	5.4.0+	FortiCare	05004000NIDS02300	28.00872 (2024-09-26 00:57:00)	99.38 KB	Latest Change
Signature Meta Data (Application Control)	6.0.9+.6.2.0	FortiCare	05006000APDB00100	28.00872 (2024-09-26 00:51:00)	60.03 KB	Latest Change
Signature Meta Data (Application Control)	6.2.1-6.2.8.6.4.0-6.4.1.7.0.0	FortiCare	06000000APDB00100	28.00872 (2024-09-26 00:51:00)	60.03 KB	Latest Change
Signature Meta Data (Application Control)	6.2.9+	FortiCare	06002000APDB00100	28.00872 (2024-09-26 00:51:00)	66.24 KB	Latest Change
Signature Meta Data (Application Control)	6.4.2+	FortiCare	06004000APDB00100	28.00872 (2024-09-26 00:51:00)	66.36 KB	Latest Change
Signature Meta Data (Application Control)	7.0.1+	FortiCare	07000000APDB00100	28.00872 (2024-09-26 00:50:00)	73.78 KB	Latest Change
Signature Meta Data (Application Control)	7.2.1+	FortiCare	07002000APDB00100	28.00872 (2024-09-26 00:50:00)	73.81 KB	Latest Change
Signature Meta Data (Application Control)	7.4.0+	FortiCare	07004000APDB00100	28.00872 (2024-09-26 00:50:00)	73.81 KB	Latest Change
Signature Meta Data (Industrial)	6.0.9+.6.2.0	FortiCare	05006000ISDB00100	28.00872 (2024-09-26 00:50:00)	61.73 KB	Latest Change
Signature Meta Data (Industrial)	6.2.1-6.2.8.6.4.0-6.4.1.7.0.0	FortiCare	06000000ISDB00100	28.00872 (2024-09-26 00:50:00)	68.84 KB	Latest Change
Signature Meta Data (Industrial)	6.2.9+	FortiCare	06002000ISDB00100	28.00872 (2024-09-26 00:50:00)	73.59 KB	Latest Change
Signature Meta Data (Industrial)	6.4.2+	FortiCare	06004000ISDB00100	28.00872 (2024-09-26 00:50:00)	74.16 KB	Latest Change

- Select the reviewed version from the dropdown list for *Change to Version*, then click *OK*. Repeat for all appropriate *IPS Signature Database* options.

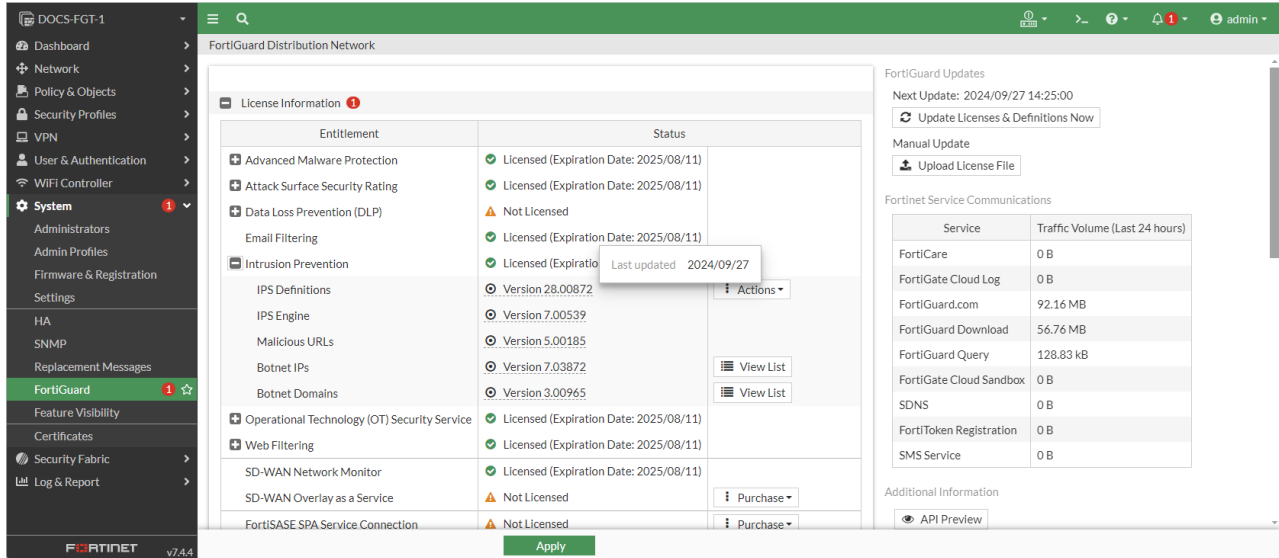
Change Version

Current Version: 28.00871

Change to Version: 28.00872 (2024-09-26 00:52:00)

OK
Cancel

- At this point, the FortiGates being serviced by the FortiManager FDS service will be able to download the approved IPS package from FortiManager. This will occur on the schedule based on the defined settings on the FortiGate.

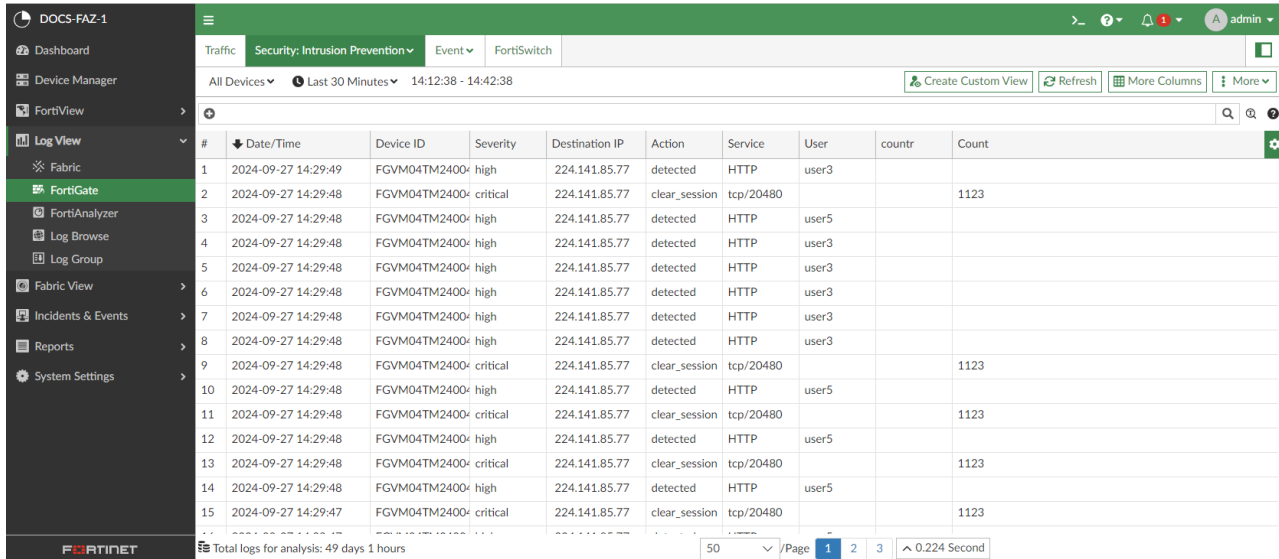


- Once the profile changes have been installed and the IPS packages released, it is recommended to monitor the FortiGate logs to identify any hits against the overridden signatures.

Monitor logs for hits to signatures

To monitor FortiGate logs for hits to overridden signatures:

- Log in to FortiAnalyzer and go to *Log View > FortiGate*, then select the *Security: Intrusion Prevention* menu.



2. In the *Filter*, select *Attack ID* and specify the *ID* of the first overridden IPS signature.

Device ID	Severity	Destination IP	Action	Service	User	count	Count
SVM04TM2400	high	224.141.85.77	detected	HTTP	user3		
SVM04TM2400	critical	224.141.85.77	clear_session	tcp/20480			1123
SVM04TM2400	high	224.141.85.77	detected	HTTP	user5		
SVM04TM2400	high	224.141.85.77	detected	HTTP	user3		
SVM04TM2400	high	224.141.85.77	detected	HTTP	user3		
SVM04TM2400	high	224.141.85.77	detected	HTTP	user3		
SVM04TM2400	high	224.141.85.77	detected	HTTP	user3		
SVM04TM2400	high	224.141.85.77	detected	HTTP	user3		
SVM04TM2400	high	224.141.85.77	detected	HTTP	user3		
SVM04TM2400	critical	224.141.85.77	clear_session	tcp/20480			1123

3. Repeat these steps adding relevant Attack IDs into the filter based on the override signatures and specify an OR operator between them by clicking the AND between the filters.

(Attack ID=30948) AND (Attack ID=37684)



No record found.

4. Review the results to evaluate whether any matches are genuine or potential false positives. The results displayed are for any events matching the signature's attack ID included in the filter.

(Attack ID=30948) OR (Attack ID=37684)

#	Date/Time	Device ID	Severity	Destination IP	Action	Service	User
1	2024-09-27 14:28:10	FGVM04TM2400	high	18.132.130.2	detected	HTTP	

5. Double-clicking the result(s) will provide a more detailed log.

Security	
Level	alert
Threat Level	high
Threat Score	30
General	
Log ID	0419016384
Message	applications3: Ubiquiti.Networks.AirOS.admin.cgi.Remote.Command.Execution
Session ID	3692782
Virtual Domain	root
Source	
Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/537.36
Device ID	[REDACTED]
Device Name	DOCS-FGT-1
Source Country	Reserved
Source IP	172.16.100.100
Source Interface	port2
Source Interface Role	undefined
Source Port	62871
UEBA Endpoint ID	3
UEBA User ID	3
Destination	
Destination Country	 United Kingdom
Destination End User ID	3
Destination Endpoint ID	101
Destination IP	 18.132.130.2
Destination Interface	port1
Destination Interface Role	undefined
Destination Port	80
Host Name	nids.http.ftnt-fsi.com
Action	
Action	detected
Policy ID	1
Policy UUID	d6883c78-568b-51ef-6513-13d12101612e
Threat	8192

Application	
Profile	lab_default
Protocol	6
Service	HTTP
URL	/admin.cgi/sd.css
Data	
Archive	199229444:0 ↓ 🔍 (436 B)
Threat	
Attack ID	30948
Attack Name	Ubiquiti.Networks.AirOS.admin.cgi.Remote.Command.Execution
Direction	outgoing
Incident Serial No.	199229444
Reference	https://fortiguard.fortinet.com/encyclopedia/ips/30948
Severity	high
Type	
Event Type	signature
Sub Type	ips
Type	utm
Others	
CVE ID	
Date	2024-09-27
Date/Time	2024-09-27 14:28:10
Device Time	2024-09-27 14:28:10
Device Time Zone	+0100
Event Time	1727443690547321090
HTTP Method	GET
Referrer URI	http://nids.http.ftnt-fsi.com/test.html
Time	14:28:10
logver	704042662
pktlog	/drive0/private/ips_files/FGVM04TM24004788/root/1727438351/199229444:0

The following is a non-exhaustive list of considerations:

Attack Name & Attack ID	Use the hyperlink(s) to open the FortiGuard page(s) related to the signature and review the attack information.
Source & Destination	Evaluate where the traffic is coming from and going to.
Data Archive	This is the packet capture of the traffic that triggered the signature.

6. By combining the details of the attack from FortiGuard and the PCAP with knowledge of the destination service/application, administrators can determine whether the event is a false positive or not. In this example:
 - a. The PCAP file shows a GET request where the URI includes `"/admin.cgi/sd.css"`.
 - b. The *Destination IP* is known Apache web server.
 - c. The FortiGuard site provides insight into the exploit as being *"The Vulnerability is due to insufficient sanitizing of user supplied inputs in "admin.cgi" script of the application"*.

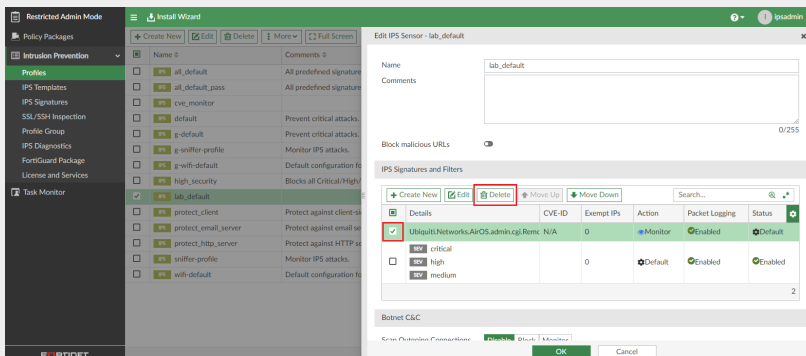
In this example, the Apache web server is known to store the files related to the website in `"/var/www/html"`, with a subdirectory `"/admin.cgi"` used to store the site's CSS file `"sd.css"` (`"/var/www/html/admin.cgi/sd.css"`). This is how the web application has been designed by the administrator and is not a vulnerability, therefore this event represents a false-positive and the server will need to be added to the exemption list.

7. Depending on the review of the log events, there are different options of what to do next:

No log events related to any of the overridden signature

Delete the overrides from the IPS Profile(s) and install the profile changes:

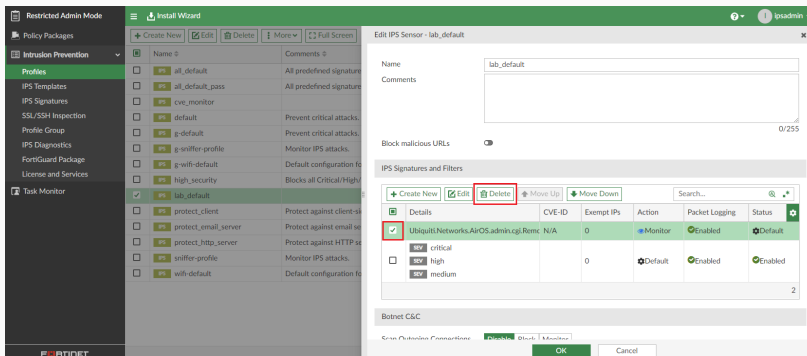
1. Go to *Intrusion Prevention > Profiles*,
2. Edit the profile(s), and select the overridden signatures in the rule list.
3. Click *Delete*, then click *OK*.
4. Use the *Install Wizard* to push the profile changes to the required FortiGates.



Events detected that have been identified as true positive matches

Delete the overrides from the IPS Profile(s) and install the profile changes:

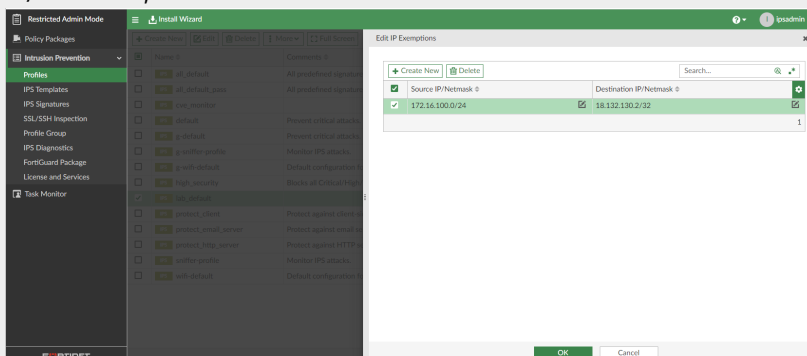
1. Go to *Intrusion Prevention > Profiles*,
2. Edit the profile(s), and select the overridden signatures in the rule list.
3. Click *Delete*, then click *OK*.
4. Use the *Install Wizard* to push the profile changes to the required FortiGates.



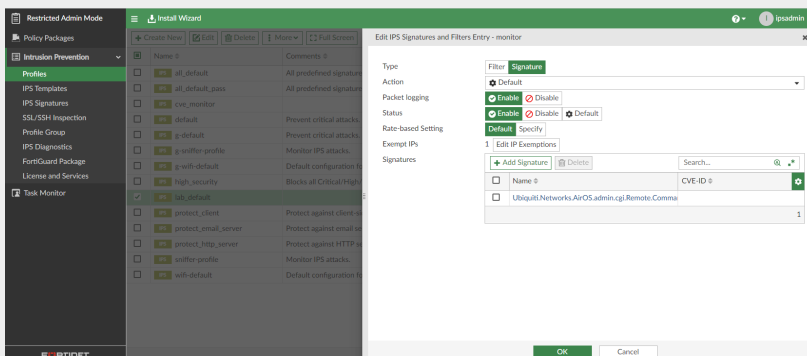
c. Events detected that have been identified as false positive matches

Modify the override to set match the *Action, Packet Logging* and *Status* defined in the main IPS rule:

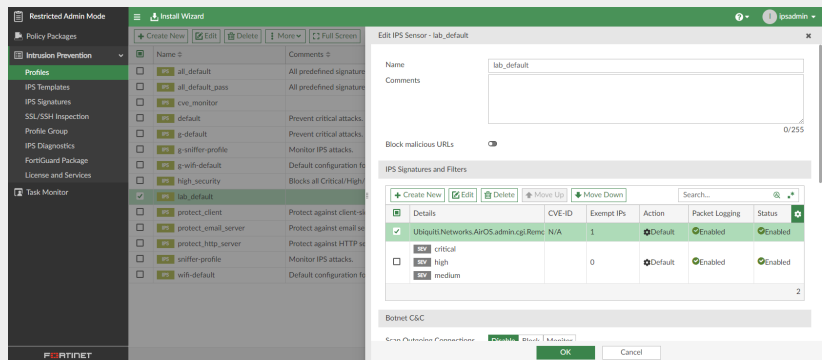
1. Review the main IPS rule settings, in this example they are: *Action – Default, Packet Logging – Enabled, Status – Enabled.*
2. Select the required overridden signature that has triggered false positives, and click *Edit*.
3. Configure the settings to match the main IPS rule, in this example it will be *Action – Default, Packet Logging – Enabled, Status – Enabled.*
4. Click *Edit IP Exemption*, then click *Create New*.
5. Specify appropriate *Source IP/Netmask* and *Destination IP/Netmask* – in this example it would require the LAN IP range for *Source IP/Netmask* and the Apache web server IP for *Destination IP/Netmask*, then click *OK*.



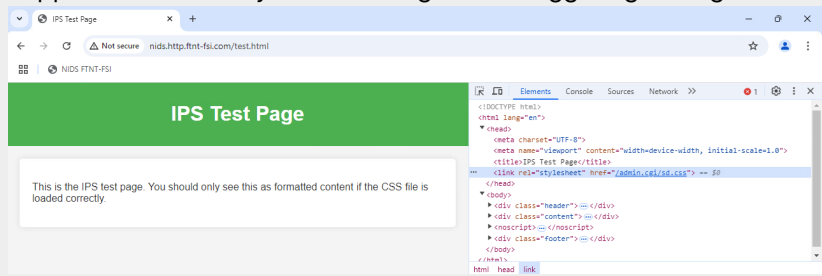
6. Review the configuration for the signature override and if all is correct click *OK*.



7. Modify/remove any additional override signatures as required and click **OK**.



8. Use the *Install Wizard* to push the profile changes to the required FortiGates.
9. Clients connecting to that Apache web server will no longer trigger the Ubiquiti vulnerability as the site is not vulnerable it just so happens the directory structure aligns with triggering the signature.



System Settings

This section contains the following topics:

- [Configuring and debugging FortiManager HA clusters on page 23](#)
- [Creating administrator accounts with restricted access on page 25](#)

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 23](#)
2. Configure one or more backup FortiManager units. See [Configuring backup FortiManager units in an HA cluster on page 24](#)
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 24](#).

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** IPv4 **Peer IP** **Peer SN** +

Cluster ID: (1-64)

Group Password:

File Quota: (2048-20480) MB

Heart Beat Interval: Seconds

Failover Threshold: (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:

1. Go to *System Settings > HA*.
2. Next to *Download Debug Log*, click *Download*.
3. 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 25](#)
- Device groups - see [Restricting administrator access to device groups on page 27](#)
- Policy packages - see [Restricting administrator access to policy packages on page 29](#)

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: [Empty text area]

Admin Type: LOCAL

New Password: [Empty password field]

Confirm Password: [Empty password field]

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: [Toggle Off]

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: ADOM-admin

Avatar: [Add Photo] [Remove Photo]

Description: [Empty text area]

Admin Type: LOCAL

New Password: [Empty password field]

Confirm Password: [Empty password field]

Admin Profile: Restricted_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | **Specify**

Policy Package Access: All Packages | Specify

JSON API Access: None

Administrative Domain Selection:

- root
- 56

2 Entries Selected

[OK] [Cancel]

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

root (5) FortiGate 7.0

56 FortiGate 7.0

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

Administrative Domain List:

- 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:

Buttons: 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 FortiGate 6.4 (Selected)

Test 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.

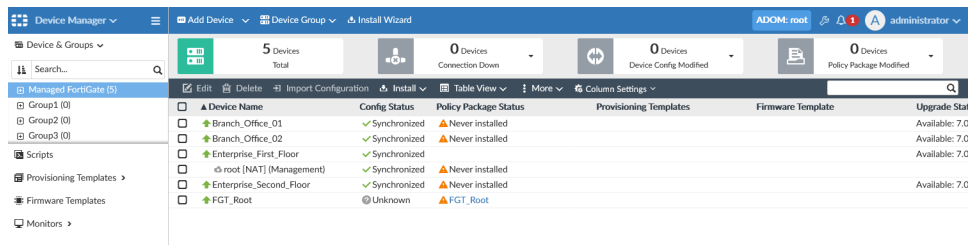
When you create an administrator account, you can specify which ADOMs the account can access, and which device groups can be accessed in those ADOMs.

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

To create a device group:

1. Go to *Device Manager > Device & Groups*.
2. If you are using ADOMs, select the ADOM that you are creating a device group in. Otherwise skip this step.
3. In the *Device Group* dropdown menu, click *Create New Group*.
4. 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.

Create New Administrator

User Name: Devicegrp-admin

Avatar: [Add Photo] [Remove Photo]

Description: [Empty text area]

Admin Type: LOCAL

New Password: [Empty password field]

Confirm Password: [Empty password field]

Admin Profile: Restricted_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | **Specify**

[root] (1 Entry Selected)

Specify Device Group to Access

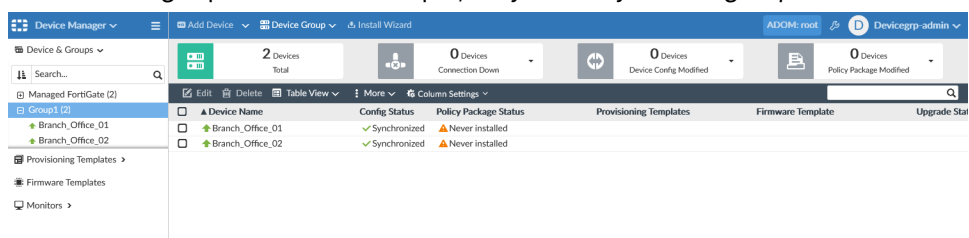
Group1

Policy Package Access: All Packages | Specify

[OK] [Cancel]

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: Package-admin

Avatar: + Change Photo - Remove Photo

Comments: 0/127

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted_User

Administrative Domain: All ADOMs All ADOMs except specified ones Specify

Policy Package Access: All Packages Specify

root:default 60:default

Trusted Hosts: OFF

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 30](#)
- [Configuring FortiManager to deploy certificates for deep inspection on page 33](#)
- [Configuring FortiManager to deploy SAML certificates on page 36](#)
- [Configuring FortiManager and FortiAuthenticator for SCEP certificate deployment on page 47](#)

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 30](#)
2. [Uploading the certificate to FortiManager on page 32](#)
3. [Apply the certificate to the FortiGate in FortiManager on page 32](#)
4. [Install the certificate on page 32](#)
5. [Verify the certificate was installed correctly on page 33](#)

Creating the certificate for administrator web access

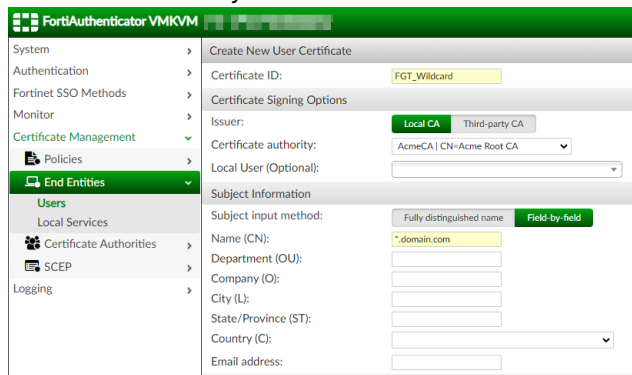
When selecting a certificate to secure HTTPS access, there are a few options you may consider. This example utilizes a wildcard certificate so that it may be applied to several FortiGates in the same domain, such as *FGT1.domain.com*, *FGT2.domain.com*, etc.

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

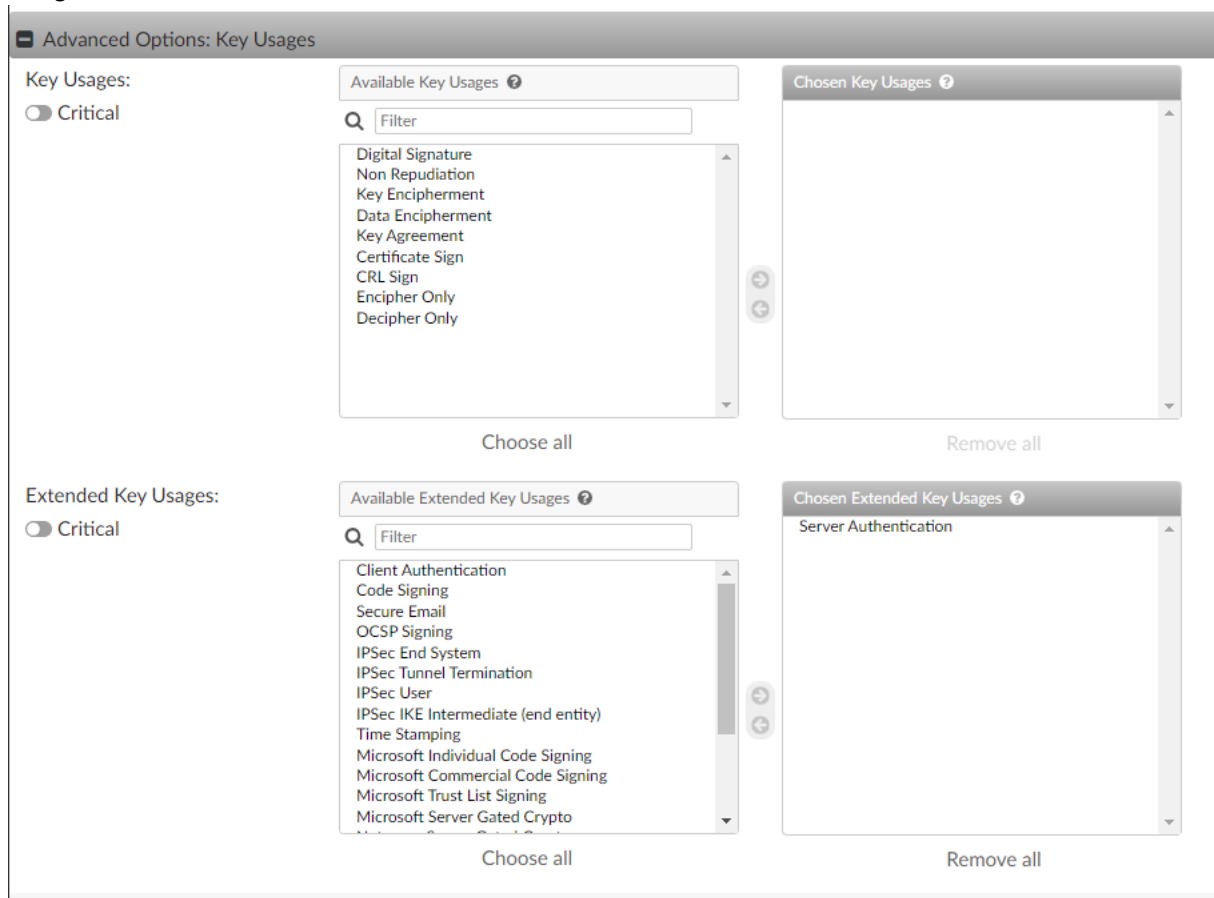
To create the certificate on FortiAuthenticator:

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

3. Provide details for your FortiGate certificate.



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



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 33](#)
2. [Generate an intermediate CA certificate on page 34](#)
3. [Upload the intermediate CA certificate to FortiManager on page 34](#)
4. [Use the certificate in a policy and install the Policy Package on page 35](#)
5. [Verify on an endpoint on page 35](#)

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*.

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.

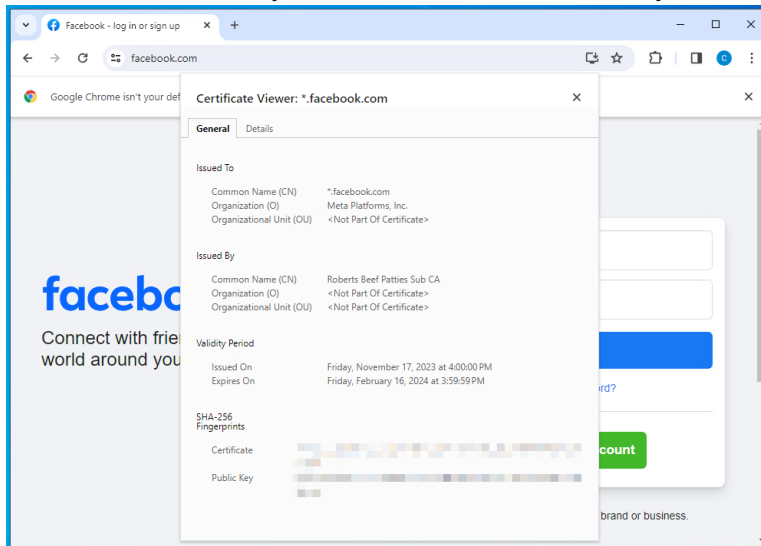
Verify on an endpoint

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.robertsbp.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.robertsbp.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.

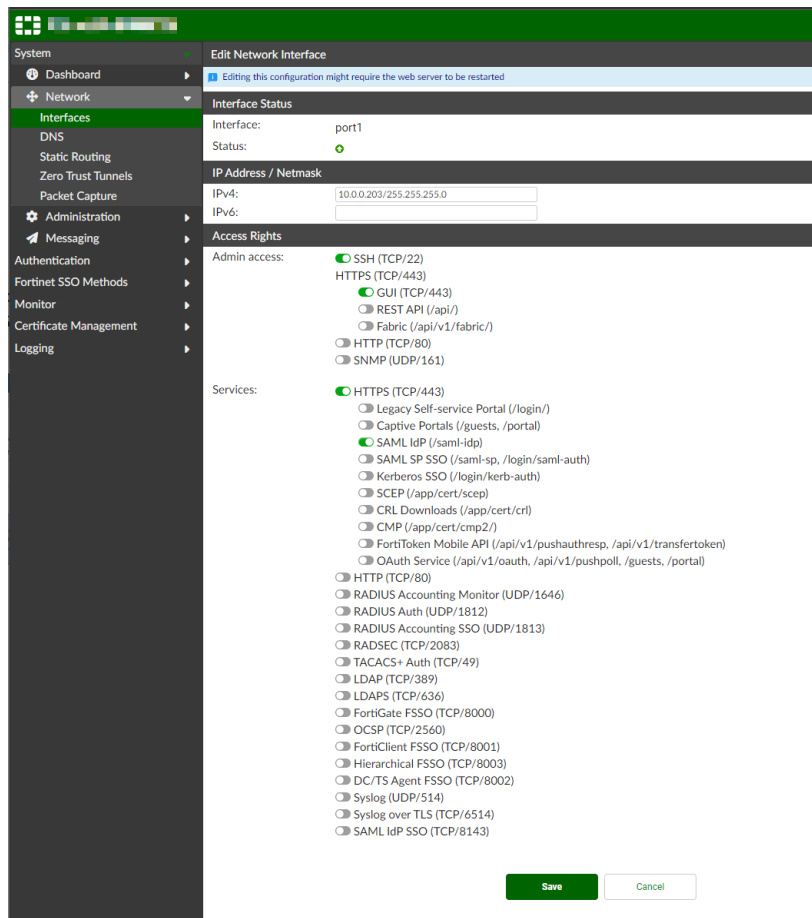
3. Click *Save*, and notice how the *SP Metadata* field appears.
4. Remain in this menu. To complete the SP settings on the IdP, we need to provide the *SP entity ID*, *SP ACS (login) URL*, and the *SP SLS (logout) URL*. These are generated in the upcoming *Defining SAML SP Settings on FortiManager*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



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:

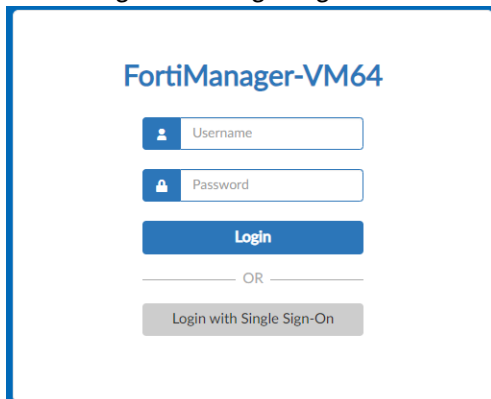
1. In the *SP Metadata* section, provide the three fields copied from the FortiManager:
 - *SP entity ID*
 - *SP ACS (login) URL*
 - *SP SLS (logout) URL*
2. Find the *Assertion Attributes Configuration* section. Notice what configuration already exists.
 - In other products, you will need to ensure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

Testing the configuration

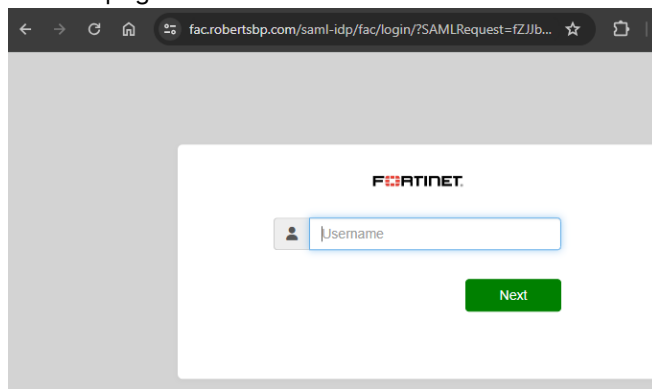
To verify the SAML configuration, attempt to log in to the FortiManager using the local account created on the FortiAuthenticator.

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.



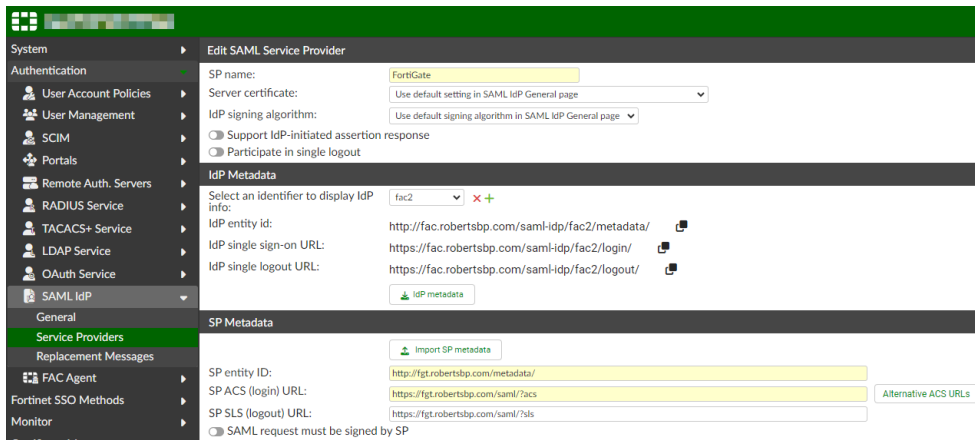
Using FortiManager to provision the SAML certificates to FortiGates

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*.



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.

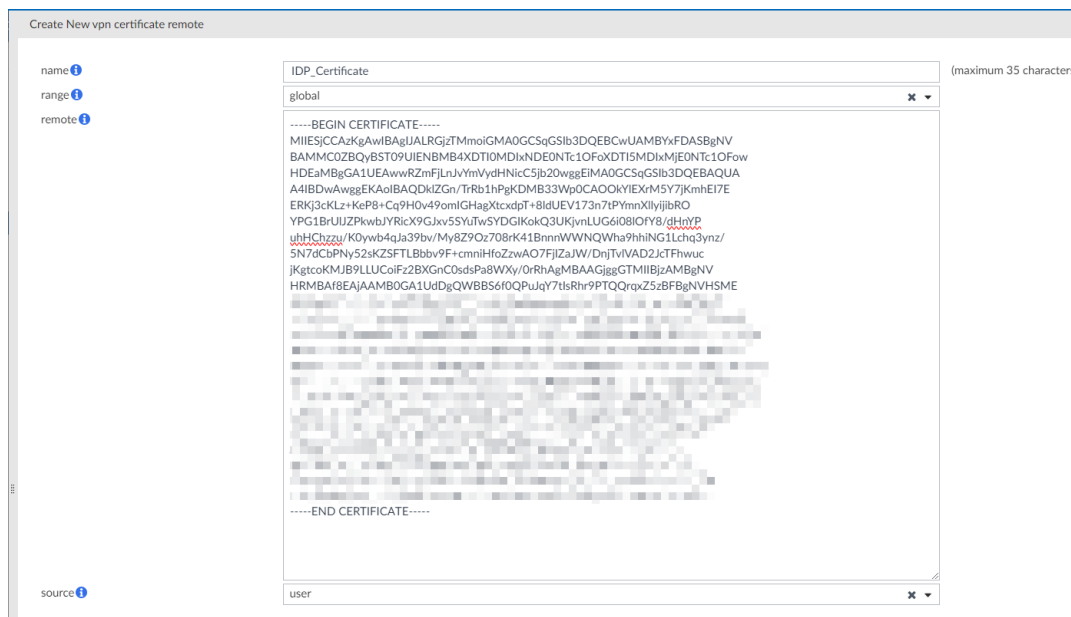
To upload the IdP Certificate to FortiManager:

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.



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:

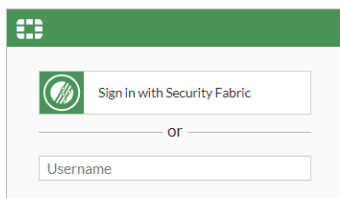
default-profile	super_admin (or your choice)
entity-id	http://fgt.robertsbp.com/metadata/
idp-cert	IDP_Certificate
idp-entity-id	http://fac.robertsbp.com/saml-idp/fac2/metadata/
idp-single-logout-url	https://fac.robertsbp.com/saml-idp/fac2/login/
idp-single-sign-on-url	https://fac.robertsbp.com/saml-idp/fac2/login/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

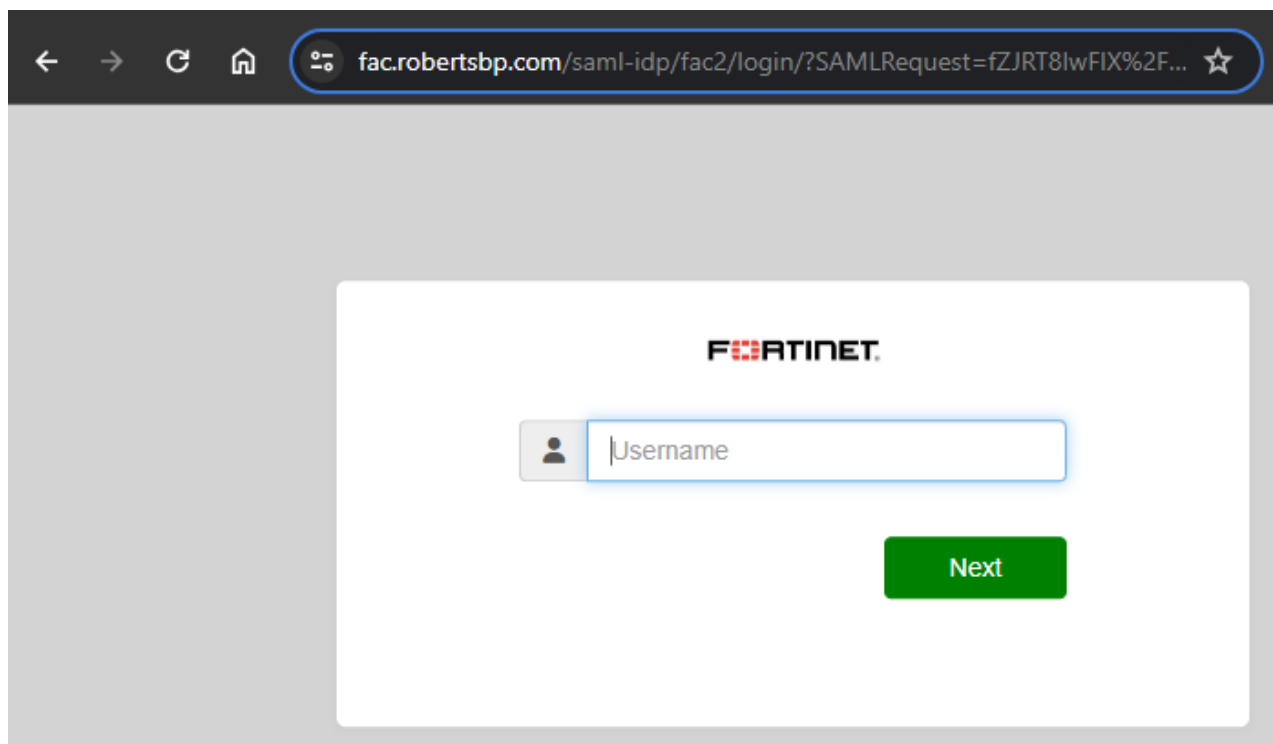
Testing the configuration

To verify the configuration:

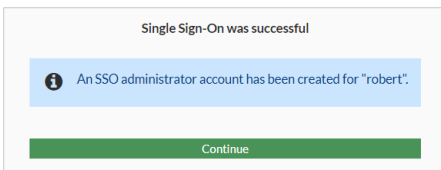
1. To verify the configuration, navigate to the FortiGate's GUI admin page.



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 47](#)
2. [Configuring FortiManager on page 50](#)
3. [Verification of certificate deployment on page 53](#)

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.

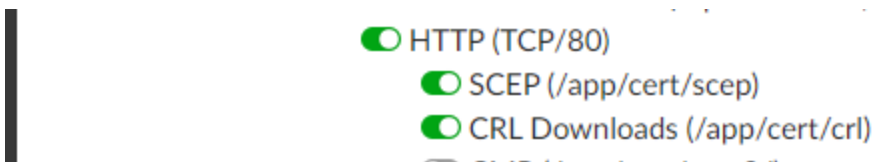
There are three configuration sections for FortiAuthenticator:

1. [Enable SCEP communications on page 47](#)
2. [Select or create a CA certificate on page 48](#)
3. [SCEP configuration on page 49](#)

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*.



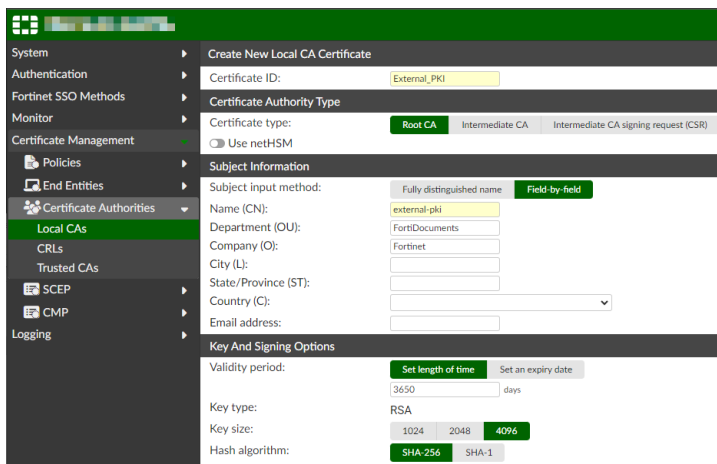
Select or create a CA certificate

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



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.

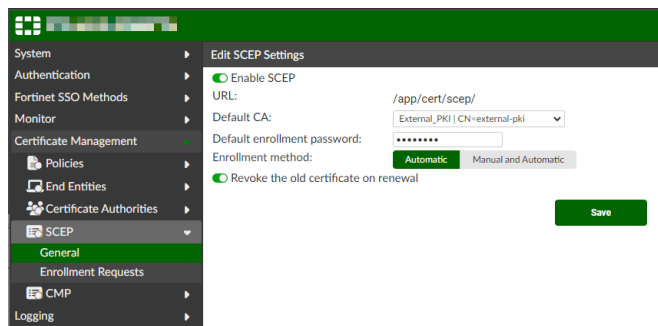


This certificate will need to be uploaded to any device which needs to verify the certificates signed by it. That might mean end user desktops for GUI admin access or deep inspection, or to FortiGates for site-to-site VPN.

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*.



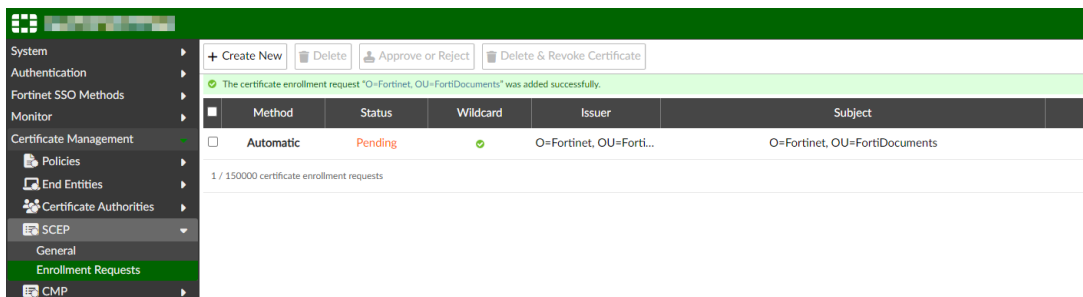
To configure enrollment requests:

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 50](#)
2. [Import the External_PKI CA certificate on page 51](#)
3. [Use the certificate in FortiManager on page 51](#)
4. [Install the certificate to FortiGate on page 52](#)

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.

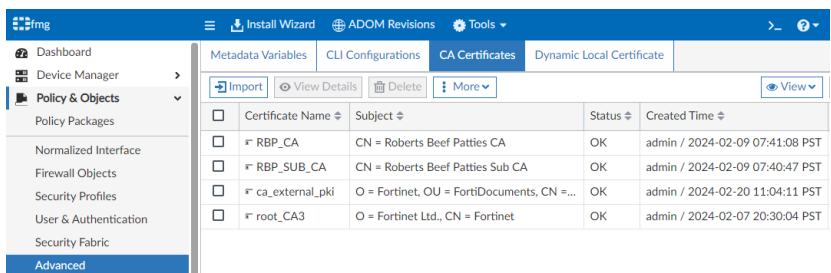
5. Click *OK*.
6. Navigate to *Policy & Objects > Advanced > Dynamic Local Certificate*. Note how there is a new certificate created named *external_pki*. If you edit this certificate, you will notice that there are no per-device mappings. This is expected as the certificate has not yet been requested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



Use the certificate in FortiManager

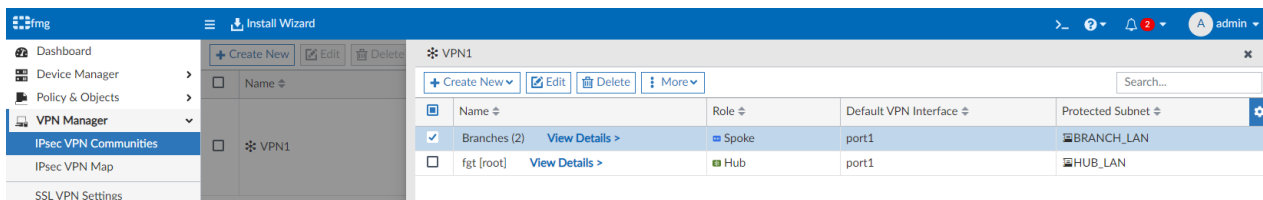
You can now use the certificate in a FortiGate configuration so it will be downloaded and installed to the FortiGate. The certificate may be used in several ways. This example demonstrates how it may be used for IPsec tunnel authentication.



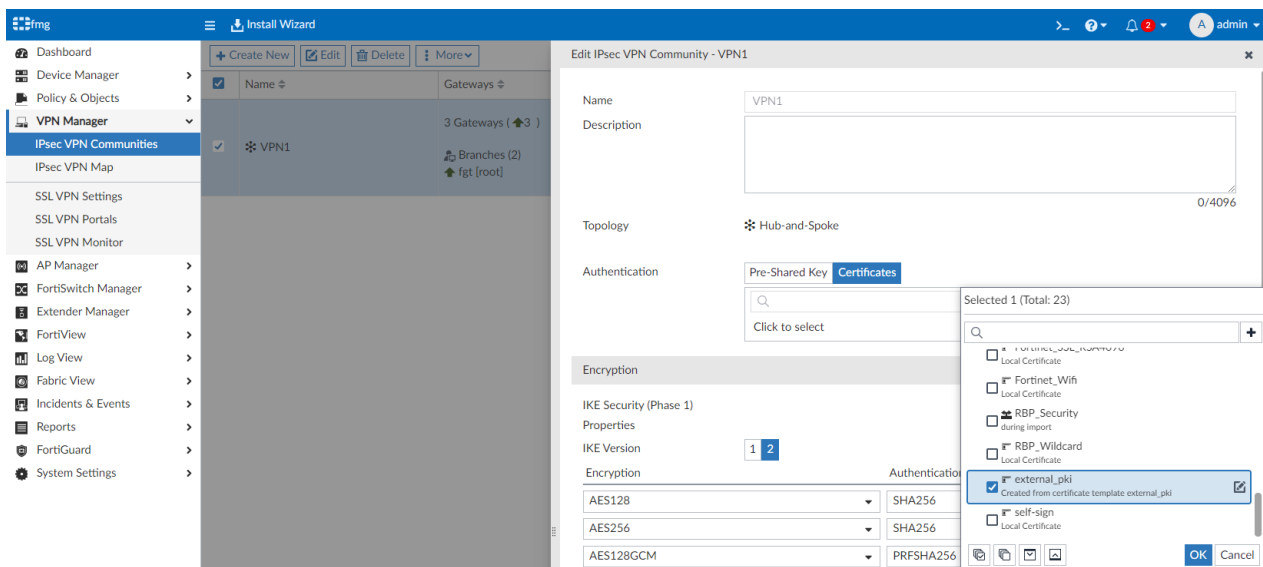
This guide edits an existing hub and spoke VPN set up that is using a PSK for authentication.

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.

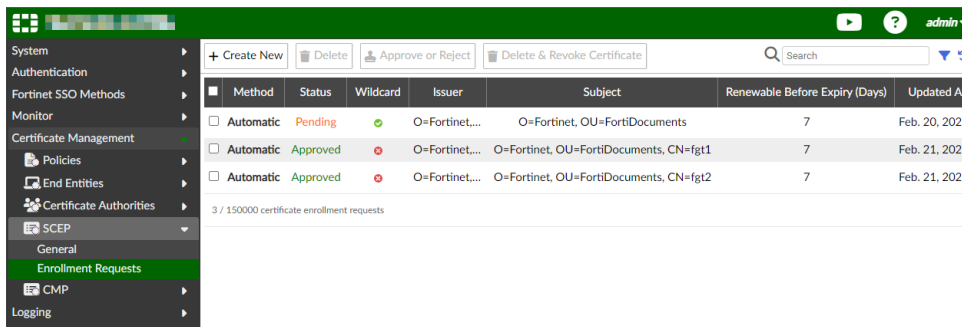
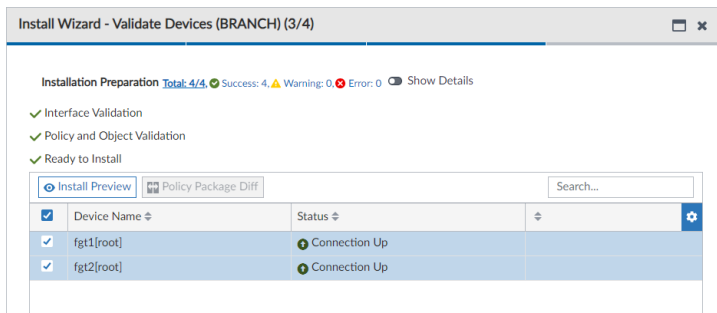


4. Select *OK* to save the community.

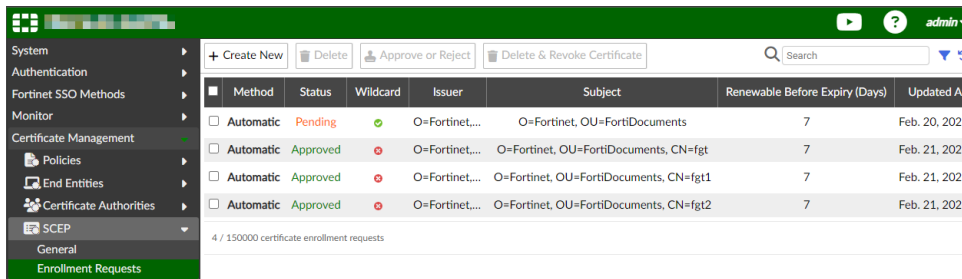
Install the certificate to FortiGate

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.

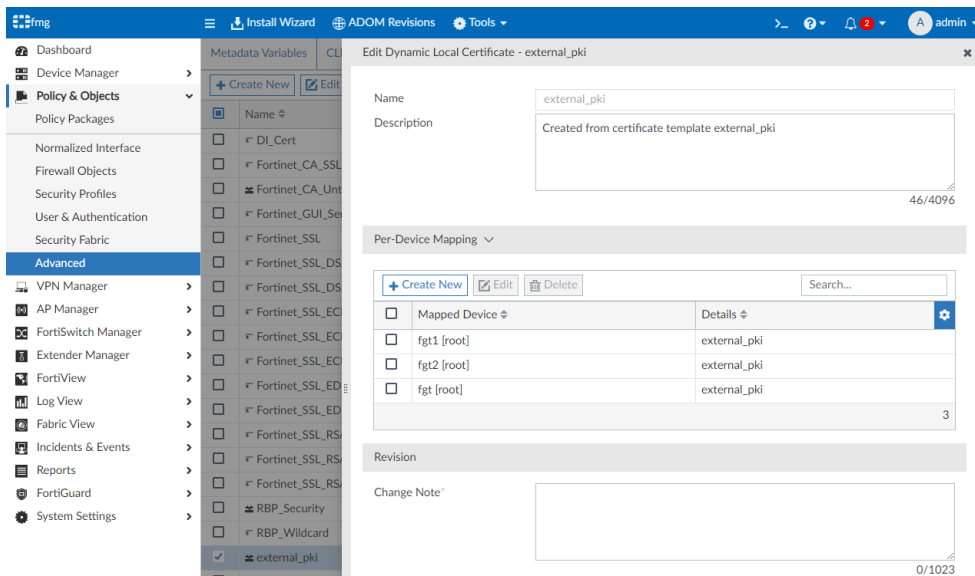
Verification on FortiManager

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.

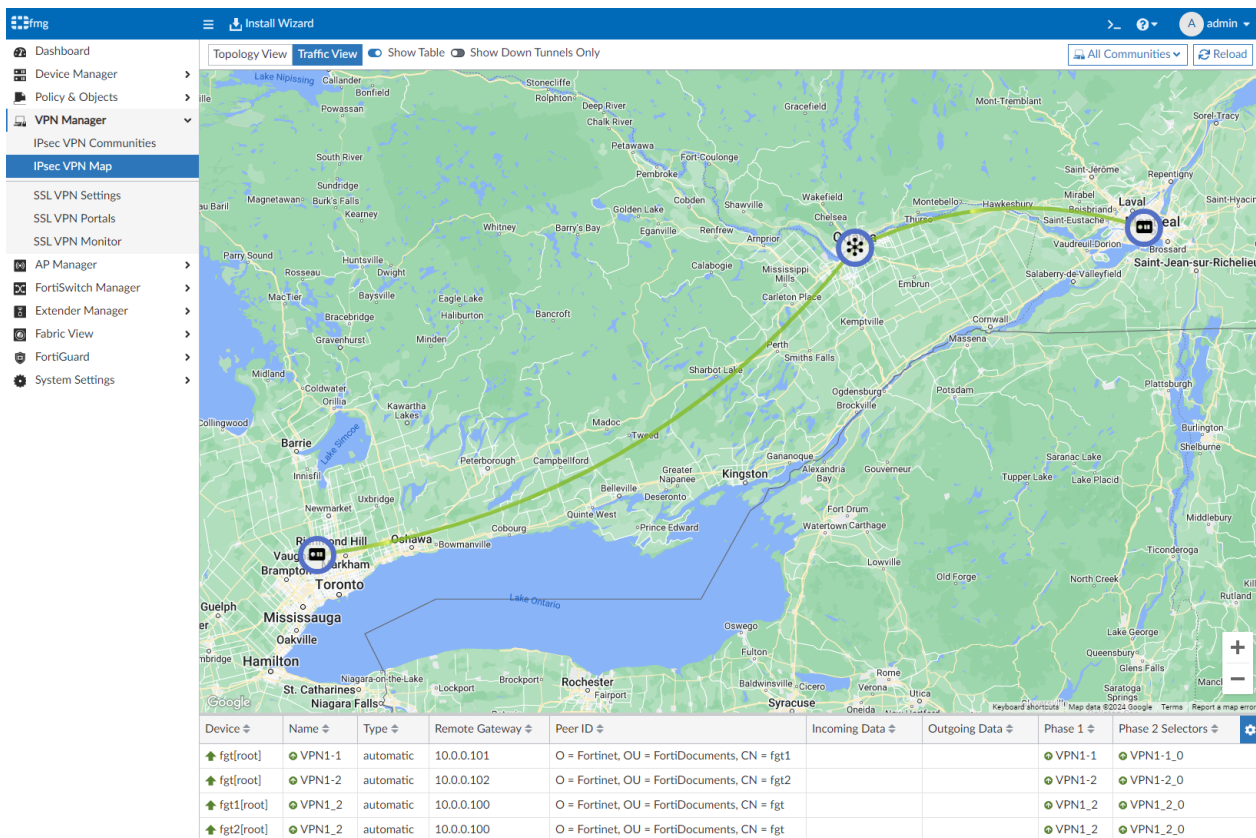
Certificate deployment



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 top screenshot shows the FortiGate web interface with the 'IPsec Tunnels' table. The table has columns for Tunnel, Interface Binding, Status, and Ref. The entries are:

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

The bottom screenshot shows the 'Edit VPN Tunnel' configuration for VPN1-1. The 'Authentication' section is expanded, showing the following details:

- Method: Signature
- Certificate Name: external_pki

A dropdown menu is visible over the 'Certificate Name' field, showing the following options:

- external_pki
- Managed by FortiManager

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.

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 = *robertsbp.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 = fgt	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 57](#)
- [Creating a third party blocklist provider workflow on page 66](#)

Managing FortiAnalyzer from FortiManager

This section contains the following topics:

- [Adding FortiAnalyzer to FortiManager on page 57](#)
- [Viewing managed FortiAnalyzer behavior on page 61](#)
- [Centrally configuring FortiGate to send logs to managed FortiAnalyzer on page 62](#)
- [Viewing logs and reports for managed FortiAnalyzer units on page 63](#)
- [Managing multiple FortiAnalyzer units on page 64](#)
- [Troubleshooting managed FortiAnalyzer units on page 65](#)

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 57](#)
- [Using the wizard to add FortiAnalyzer to FortiManager on page 58](#)
- [Additional information on page 59](#)

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

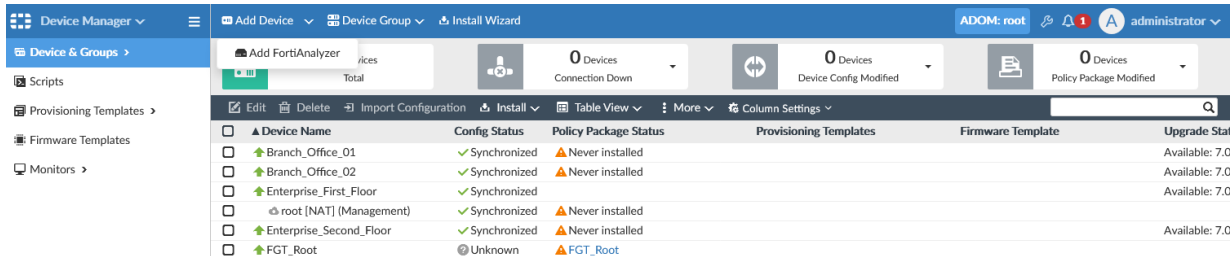
This section describes how to use the *Add FortiAnalyzer* wizard to add FortiAnalyzer to FortiManager.

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
```

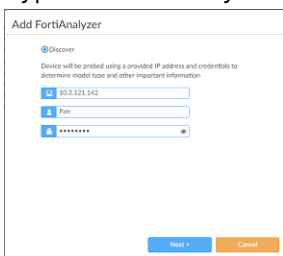
3. Go to *Device Manager*, and select a central management ADOM, such as *manage_remote_faz*. The FortiAnalyzer unit should contain an ADOM of the same name. In this example, both FortiAnalyzer and FortiManager have an ADOM named *manage_remote_faz*.
4. On the *Device & Groups* tab, add the FortiAnalyzer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



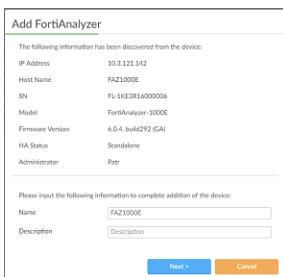
Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Template	Upgrade Status
Branch_Office_01	Synchronized	Never installed			Available: 7.0
Branch_Office_02	Synchronized	Never installed			Available: 7.0
Enterprise_First_Floor	Synchronized	Never installed			Available: 7.0
root [NAT] (Management)	Synchronized	Never installed			
Enterprise_Second_Floor	Synchronized	Never installed			Available: 7.0
FGT_Root	Unknown	FGT_Root			

The *Add FortiAnalyzer* wizard is displayed.

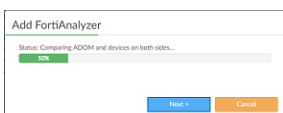
- b. Type the FortiAnalyzer IP address, username, password, and click *Next*.



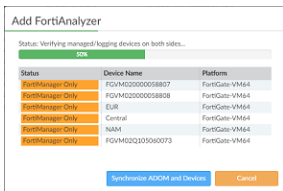
After FortiManager discovers the device, device information is displayed.



- c. Click *Next* to continue.

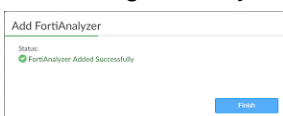


FortiManager automatically compares ADOMs and devices on both FortiAnalyzer and FortiManager and provides the comparison and verification results.



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

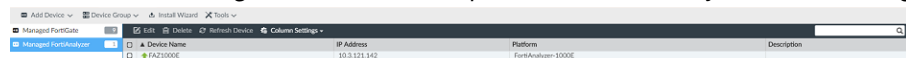
Devices are synchronized between FortiAnalyzer and FortiManager, and FortiAnalyzer is added to FortiManager. The synchronized devices are added to FortiAnalyzer as logging-mode FortiGates.



FortiAnalyzer is added to FortiManager.

- e. Click *Finish*.

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



Additional information

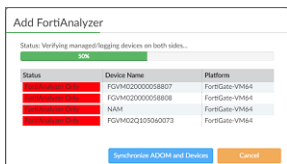
This section describes some of the other scenarios you might encounter when adding FortiAnalyzer units to FortiManager.

Missing ADOM

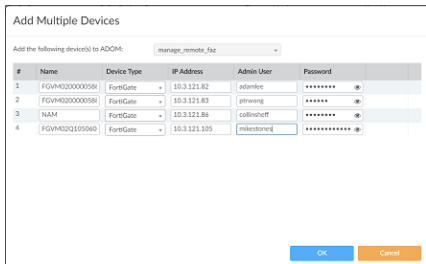
If the current ADOM in FortiManager does not exist on FortiAnalyzer, FortiManager automatically creates an ADOM with same name and version on FortiAnalyzer before starting to synchronize the device list.

Unknown or mismatched FortiGate devices

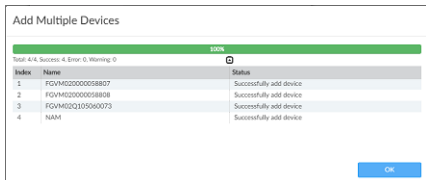
If FortiAnalyzer is receiving logs from FortiGate devices that do not exist on FortiManager, FortiManager identifies the devices.



FortiManager automatically attempts to discover the FortiGates.

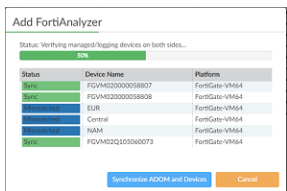


FortiManager can add the FortiGates and retrieve configurations for the FortiGates when adding the FortiAnalyzer unit.

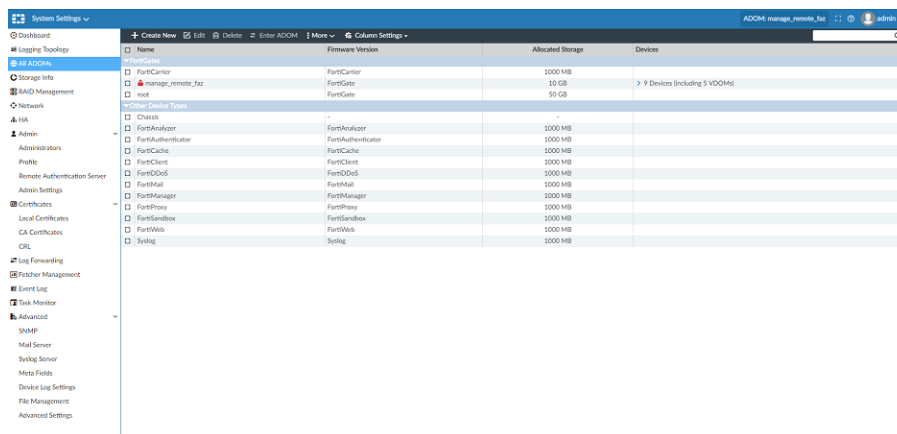


If one device fails to add or retrieve, FortiManager fails to add FortiAnalyzer.

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.



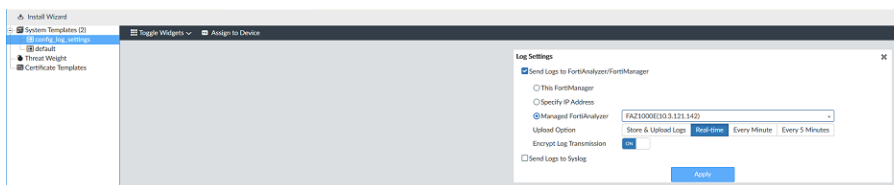
Name	Firmware Version	Allocated Storage	Devices
FortiAnalyzer	FortiAnalyzer	1000 MB	
FortiAuthenticator	FortiAuthenticator	1000 MB	
FortiGate	FortiGate	2000 MB	
FortiClient	FortiClient	1000 MB	
FortiDdOS	FortiDdOS	1000 MB	
FortiMail	FortiMail	1000 MB	
FortiManager	FortiManager	1000 MB	
FortiProxy	FortiProxy	1000 MB	
FortiSandBox	FortiSandBox	1000 MB	
FortiWeb	FortiWeb	1000 MB	
Syslog	Syslog	1000 MB	

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:

- In FortiManager, go to *Device Manager > Provisioning templates*.
- Create a new blank system template.
 - In the content pane, click *Create New*.
 - Type a name for the system template, and click *OK*.
The system template is created.
 - 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.



- In the *Log Settings* widget, select *Send Logs to FortiAnalyzer/FortiManager*.
 - Select *Managed FortiAnalyzer*, and select the unit from the drop-down list.
 - Click *Apply*.
- Assign the system template to FortiGates.
 - 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:

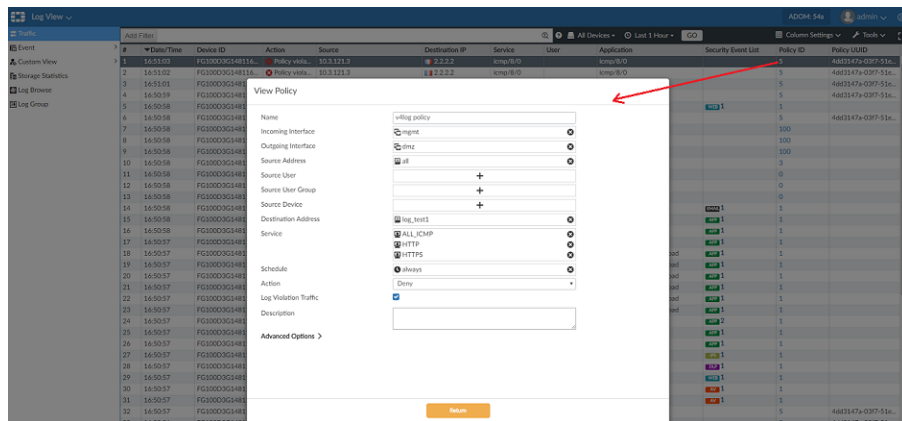
- Importing and exporting a report template
- Importing and exporting a chart
- Importing and downloading a log file

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

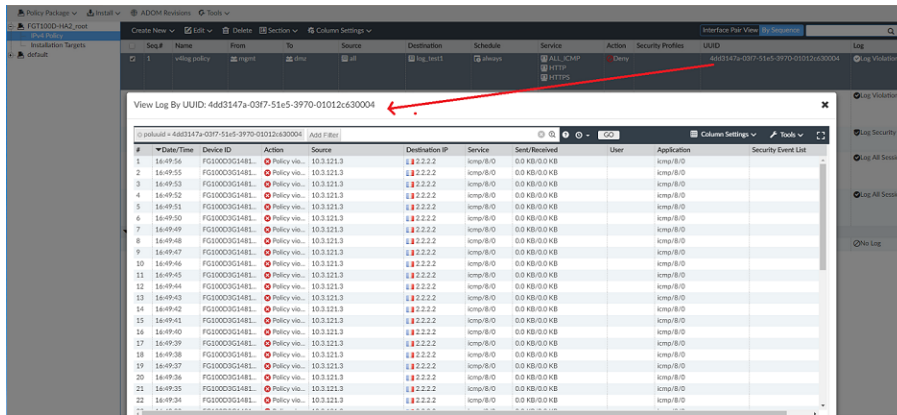
To view logs and reports:

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.



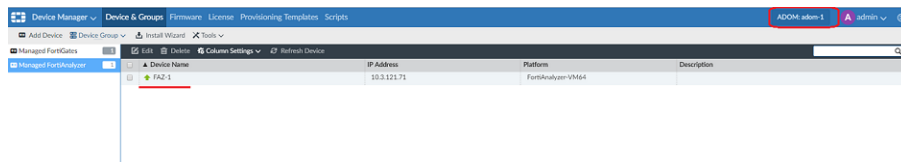
3. Go to *Policy & Objects > Policy Packages*, and right-click the policy UUID to search the related policy logs.



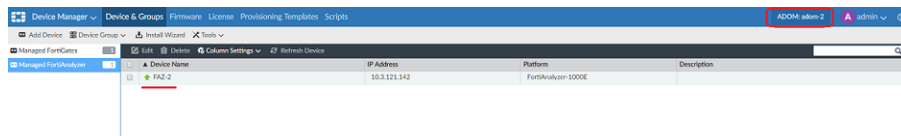
Managing multiple FortiAnalyzer units

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.

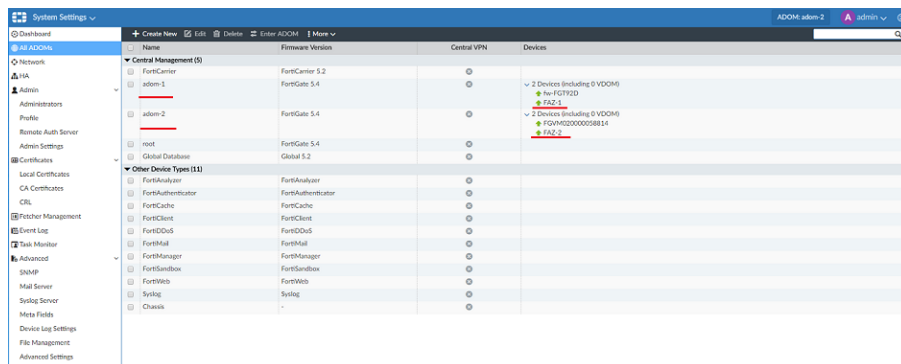
For example, FortiManager can contain the following ADOMs: *adom-1* and *adom-2*, and *adom-1* manages FAZ-1:



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



Following is another view of the ADOMs with FortiAnalyzer units:



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

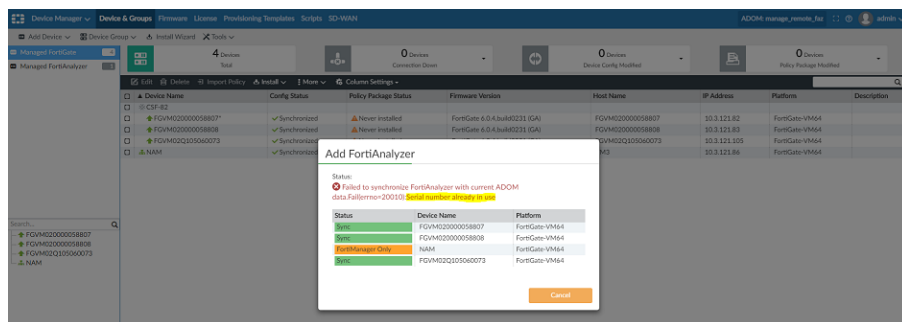
When you delete FortiAnalyzer from FortiManager, the ADOM on FortiAnalyzer should be unlocked. If the ADOM remains locked, you can use the following command on the FortiAnalyzer unit to unlock the ADOM:

```
diagnose dvm adom unlock <adom ADOM name>

diagnose dvm adom unlock remote-faz
---Deleting DVM lock by remote FortiManager succeeded---
```

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.

```

FG380D login: admin
password:
FG380D # diagnose dm device list
--- There are currently 4 devices/vdoms managed ---
TYPE      OID      SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
mg/faz enabled 501    FGVM0200005807  10.3.121.82  FGVM0200005807  manage_remote_faz  6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: not modified; conf: in sync; cmd: OK; ds: retrieved; conn: up
|  vdom[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
FG/faz enabled 51    FGVM0200005808  10.3.121.83  FGVM0200005808  manage_remote_faz  6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: not modified; conf: in sync; cmd: OK; ds: retrieved; conn: up
|  vdom[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
FG/faz enabled 489    FGVM0200005809  10.3.121.85  FGVM0200005809  manage_remote_faz  6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: not modified; conf: in sync; cmd: OK; ds: retrieved; conn: up
|  vdom[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
FG/faz enabled 476    FGVM0200005811 a-p  10.3.121.86  N/A      manage_remote_faz  6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: not modified; conf: in sync; cmd: OK; ds: retrieved; conn: up
|  vdom[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]

HA cluster member: FGVM0200005811 (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 FortiXtender managed ---
--- End device list ---
FG380D #

FAZ100RE login: admin
password:
FAZ100RE # diagnose dm device list
--- There are currently 4 devices/vdoms managed ---
TYPE      OID      SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
faz enabled 273    FGVM0200005807  10.3.121.82  FGVM0200005807  manage_remote_faz  6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: unknown; conf: unknown; cmd: unknown; ds: unknown; conn: unknown
|  vdom[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
faz enabled 274    FGVM0200005808  10.3.121.83  FGVM0200005808  manage_remote_faz  6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: unknown; conf: unknown; cmd: unknown; ds: unknown; conn: unknown
|  vdom[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
faz enabled 272    FGVM0200005809  10.3.121.85  FGVM0200005809  manage_remote_faz  6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: unknown; conf: unknown; cmd: unknown; ds: unknown; conn: unknown
|  vdom[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
faz enabled 308    FGVM0200005811 a-p  10.3.121.86  N/A      root      6.00741 (regular)  6.0 MRD (211)
|  STATUS: dev-db: unknown; conf: unknown; cmd: unknown; ds: unknown; conn: unknown
|  vdom[1]root flags:0 adom:root pkg:[never-installed]

HA cluster member: FGVM0200005811 (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 FortiXtender managed ---
--- End device list ---
FAZ100RE #
    
```

Compare the device list on FMG and FAZ. Both FMG and FAZ have device "FGVM0200005811" but it is in different ADOM (on FMG it is in ADOM "manage_remote_faz" on FAZ it is in ADOM "root"). That is why you see the error "Failed to sync dmdb to FAZ: Serial number already in use".
To solve the problem, manually move the device "FGVM0200005811" 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.

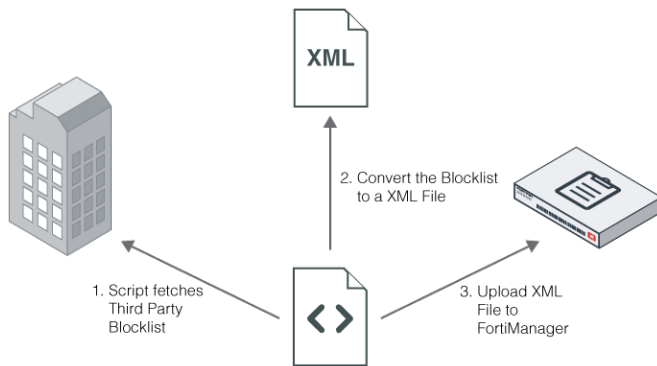
Creating a third party blocklist provider workflow

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 <type> <filename> <server> <port> <directory>
<username> <password>
```

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