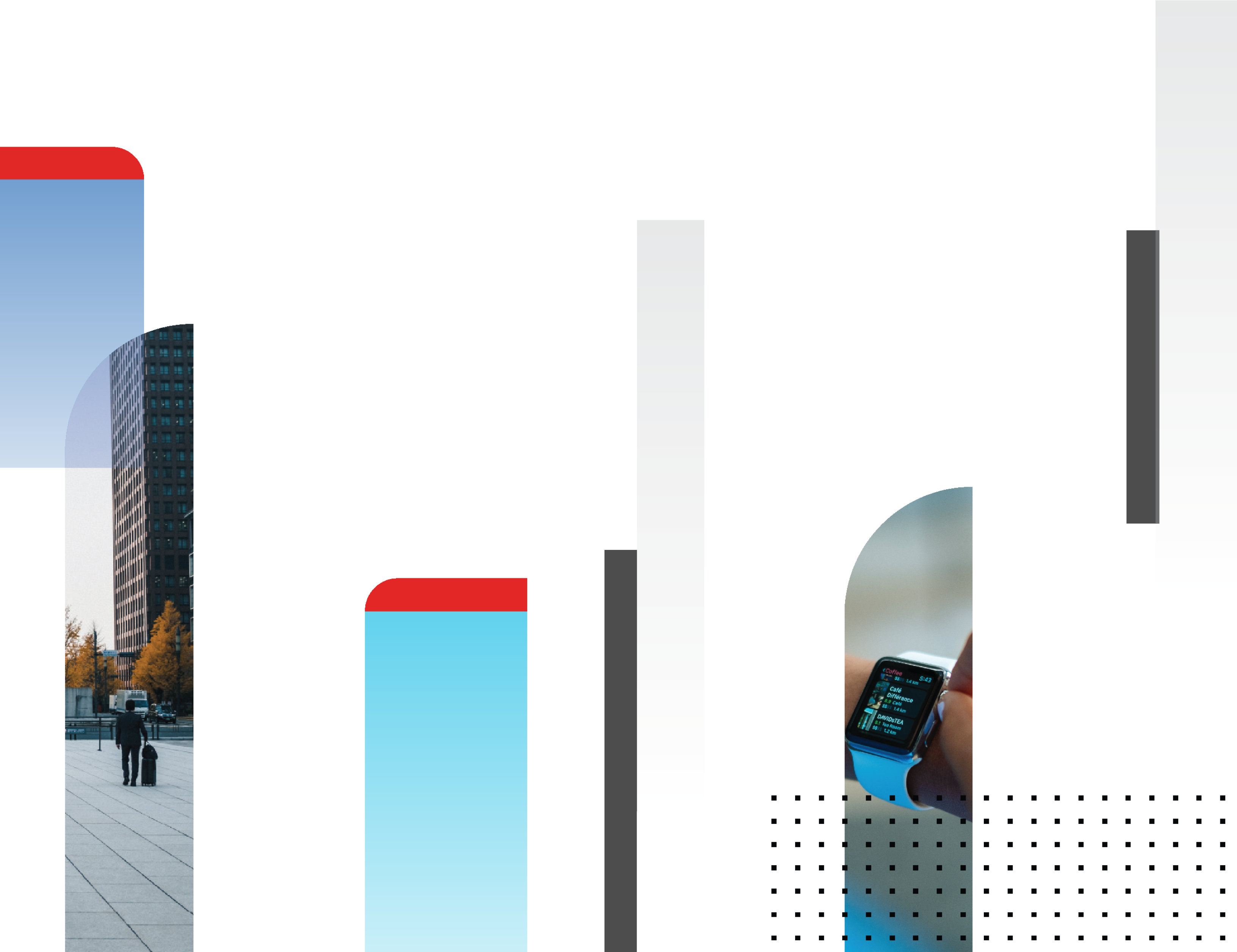
FORTINET

Administration Guide

FortiSigConverter MEA 1.0.0 Beta



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 14, 2022
FortiSigConverter MEA 1.0.0 Beta Administration Guide
02-100-650691-20220214

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-10-22	Initial release of 1.0.0 Beta.
2022-02-14	Updated for release of 1.0.0 Beta 7.

Introduction

When enabled, FortiSigConverter MEA is installed on FortiManager. FortiSigConverter MEA is a management extension application (MEA) that is released and signed by Fortinet to run on FortiManager.

FortiSigConverter MEA requires FortiManager 6.4.3 or later, and you must be in ADOM version 6.4 or later to access FortiSigConverter MEA.

You can use FortiSigConverter MEA to import Snort signature files for FortiManager to use.

Key concepts

Snort is a popular open source Network Intrusion Detection System (NIDS). FortiManager can use Snort signature files after you import them into FortiSigConverter MEA and convert them to Fortinet supported IPS signatures.

ADOM support

FortiSigConverter MEA requires FortiManager 6.4.3 or later, and you must be in ADOM version 6.4 or later to access FortiSigConverter MEA.

FortiManager 6.4.3 to 7.0.1 supports FortiSigConverter MEA only in the root ADOM.

FortiManager 7.0.2 and later supports FortiSigConverter MEA in multiple ADOMs. When ADOMs are enabled, you only need to enable FortiSigConverter MEA once to make it available in all ADOMs. FortiSigConverter MEA is unique in each ADOM.

How FortiSigConverter MEA works with FortiManager

When you import Snort signature files to FortiSigConverter MEA, FortiSigConverter MEA converts them to Fortinet supported IPS signatures. You can push one or more signature rules to FortiManager to make them available as objects that you can select in FortiManager policies.

FortiSigConverter MEA communicates directly with FortiManager by using the API.

Quick start

This section provides a summary of how to get started with FortiSigConverter MEA:

1. Enable FortiSigConverter MEA. See Enabling FortiSigConverter MEA on page 6.
2. Import Snort signature files to FortiSigConverter MEA. See Importing Snort signature files on page 7.
   If you are using FortiManager 7.0.2 or later with ADOMs enabled, ensure you are in the correct ADOM before importing Snort signature files.
3. View converted Snort signature rules. See Viewing converted signature rules on page 9.
4. Push converted signature rules to FortiManager. See Pushing converted signature rules to FortiManager on page 10.
5. View signature rules on the *Policy & Objects* module in FortiManager. See Viewing signature rules on FortiManager on page 11.
   After you push converted signature rules from FortiSigConverter MEA to FortiManager, they are displayed as custom IPS signatures on the *Policy & Objects* module.
6. Export information from FortiSigConverter MEA about imported Snort signature files.
   - For information about imported Snort signature files, see Exporting Snort file lists on page 13.
   - For information about converted signature rules, see Exporting converted signature lists on page 14.
7. View the audit log. See Viewing the audit log on page 14.

You can also delete Snort files and converted signature rules from FortiSigConverter MEA. See Deleting imported Snort files on page 12.

Enabling FortiSigConverter MEA

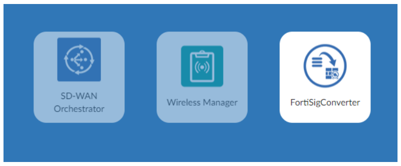
FortiManager provides access to FortiSigConverter MEA that is released and signed by Fortinet.

Only administrators with a *Super_User* profile can enable management extension applications.

A CA certificate is required to install management extension applications on FortiManager.

To enable FortSigConverter:

1. Ensure you are using ADOM version 6.4 or later.
   You must be in the root ADOM, if you are using FortiManager 6.4.3 to 7.0.1.
   If you are using FortiManager 7.0.2 or later, you can enable FortiSigConverter MEA in any ADOM that is version 6.4 or later, if ADOMs are enabled, and FortiSigConverter MEA becomes available for use in all ADOMs.
2. Go to *Management Extensions*.
3. Click the grayed out tile for *FortiSigConverter MEA* to enable the application.
   Grayed out tiles represent disabled Fortinet management extension applications. In the following example, *SD-WAN Orchestrator* and *Wireless Manager* are disabled.



4. Click *OK* in the dialog that appears. It may take some time to install the application.

To enable FortiSigConverter MEA in the CLI:

```
config system docker
   set fortisigconverter enable
end
```

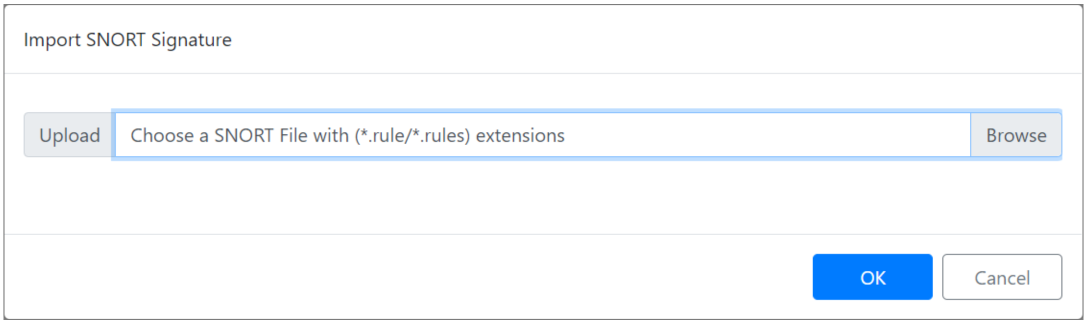
Importing Snort signature files

Use the *IPS Custom Signature* module to import Snort signature files directly into FortiSigConverter MEA. After the signatures are converted to supported IPS signatures, you can use FortiSigConverter MEA to push the signature rules to FortiManager.

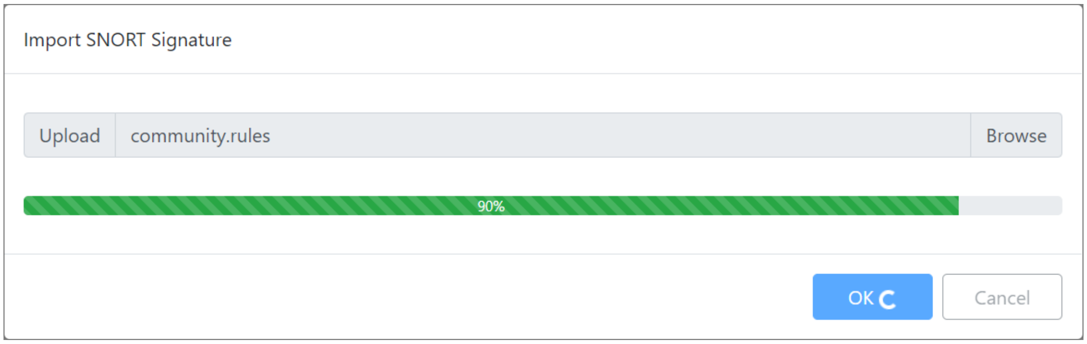
When ADOMs are enabled in FortiManager 7.0.2 and later, you must select the correct ADOM before you import Snort signature files into FortiSigConverter MEA. Because FortiSigConverter MEA is unique in each ADOM, the converted signature rules are only available for use in the same ADOM. If you want to use the same Snort signatures in two or more ADOMs, you must import the Snort signatures into the FortiSigConverter MEA in each ADOM where you want to use the converted signature rules.

To import a Snort signature file:

1. Go to *IPS Custom Signature*, and click *Import SNORT Signature*.
   The *Import SNORT Signature* dialog box is displayed.



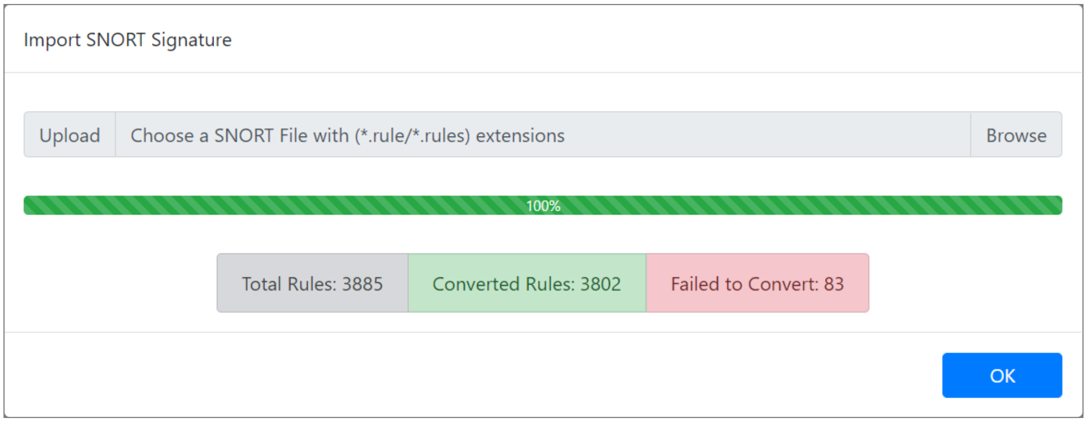
2. Click *Browse* to locate the Snort signature file, and then click *Open*.
   Alternately, you can drag and drop the Snort signature file on to the dialog box.
   The selected Snort signature file is displayed in the *Import SNORT Signature* dialog box.
3. Click *OK*.
   The import process starts, and a progress bar is displayed.



Import SNORT Signature

Upload: community.rules

When the progress reaches 100%, status information about the import process is displayed.

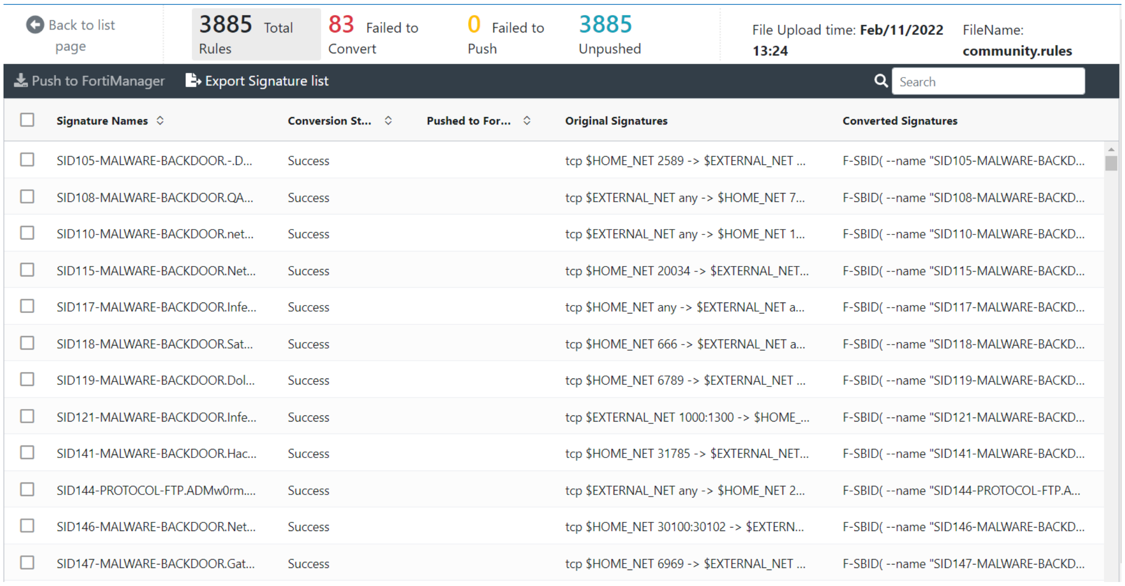


Import SNORT Signature

Upload: Choose a SNORT File with (*.rule/*.rules) extensions

Total Rules: 3885 | Converted Rules: 3802 | Failed to Convert: 83

4. Click *OK* to complete the import process.
   The list of converted signatures is displayed. The *Conversion Status* column displays the status of each converted rule.



3885 Total Rules | 83 Failed to Convert | 0 Failed to Push | 3885 Unpushed

File Upload time: **Feb/11/2022 13:24** FileName: **community.rules**

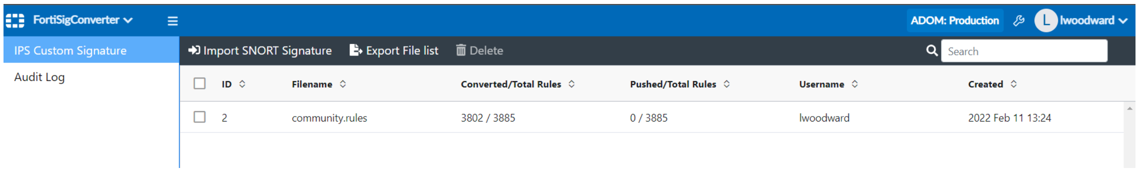
□	Signature Names	Conversion St...	Pushed to For...	Original Signatures	Converted Signatures
□	SID105-MALWARE-BACKDOOR.-.D...	Success		tcp $HOME_NET 2589 -> $EXTERNAL_NET ...	F-SBID(--name "SID105-MALWARE-BACKD...
□	SID108-MALWARE-BACKDOOR.QA...	Success		tcp $EXTERNAL_NET any -> $HOME_NET 7...	F-SBID(--name "SID108-MALWARE-BACKD...
□	SID110-MALWARE-BACKDOOR.net...	Success		tcp $EXTERNAL_NET any -> $HOME_NET 1...	F-SBID(--name "SID110-MALWARE-BACKD...
□	SID115-MALWARE-BACKDOOR.Net...	Success		tcp $HOME_NET 20034 -> $EXTERNAL_NET...	F-SBID(--name "SID115-MALWARE-BACKD...
□	SID117-MALWARE-BACKDOOR.Infe...	Success		tcp $HOME_NET any -> $EXTERNAL_NET a...	F-SBID(--name "SID117-MALWARE-BACKD...
□	SID118-MALWARE-BACKDOOR.Sat...	Success		tcp $HOME_NET 666 -> $EXTERNAL_NET a...	F-SBID(--name "SID118-MALWARE-BACKD...
□	SID119-MALWARE-BACKDOOR.Dol...	Success		tcp $HOME_NET 6789 -> $EXTERNAL_NET ...	F-SBID(--name "SID119-MALWARE-BACKD...
□	SID121-MALWARE-BACKDOOR.Infe...	Success		tcp $EXTERNAL_NET 1000:1300 -> $HOME_...	F-SBID(--name "SID121-MALWARE-BACKD...
□	SID141-MALWARE-BACKDOOR.Hac...	Success		tcp $HOME_NET 31785 -> $EXTERNAL_NET...	F-SBID(--name "SID141-MALWARE-BACKD...
□	SID144-PROTOCOL-FTP.ADMw0rm....	Success		tcp $EXTERNAL_NET any -> $HOME_NET 2...	F-SBID(--name "SID144-PROTOCOL-FTP.A...
□	SID146-MALWARE-BACKDOOR.Net...	Success		tcp $HOME_NET 30100:30102 -> $EXTERN...	F-SBID(--name "SID146-MALWARE-BACKD...
□	SID147-MALWARE-BACKDOOR.Gat...	Success		tcp $HOME_NET 6969 -> $EXTERNAL_NET ...	F-SBID(--name "SID147-MALWARE-BACKD...

Viewing converted signature rules

After Snort signature files are imported to FortiSigConverter MEA, you can view a list of converted signature rules and filter the list by clicking each column heading.

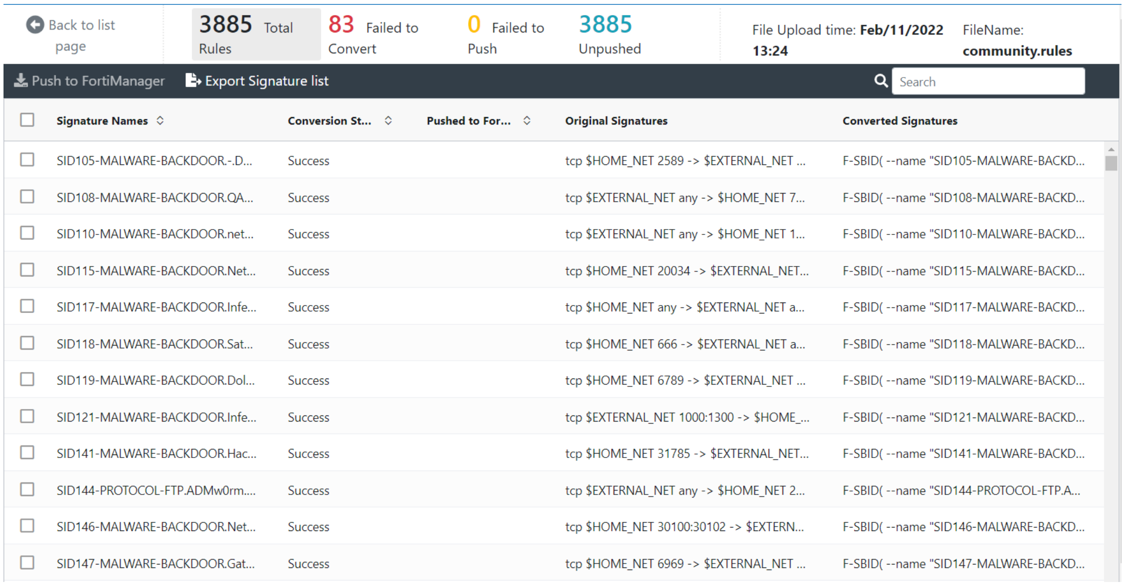
To view imported Snort signature rules:

1. Go to *IPS Custom Signature*.
   The list of imported Snort files is displayed.



□	ID	Filename	Converted/Total Rules	Pushed/Total Rules	Username	Created
□	2	community.rules	3802 / 3885	0 / 3885	lwoodward	2022 Feb 11 13:24

2. Click a Snort file to view its list of converted signature rules.
   By default, the *<number> Total Rules* column is selected, and all signature rules are displayed.



File Upload time: **Feb/11/2022 13:24**
FileName: **community.rules**

□	Signature Names	Conversion St...	Pushed to For...	Original Signatures	Converted Signatures
□	SID105-MALWARE-BACKDOOR.-.D...	Success		tcp $HOME_NET 2589 -> $EXTERNAL_NET ...	F-SBID(--name "SID105-MALWARE-BACKD...
□	SID108-MALWARE-BACKDOOR.QA...	Success		tcp $EXTERNAL_NET any -> $HOME_NET 7...	F-SBID(--name "SID108-MALWARE-BACKD...
□	SID110-MALWARE-BACKDOOR.net...	Success		tcp $EXTERNAL_NET any -> $HOME_NET 1...	F-SBID(--name "SID110-MALWARE-BACKD...
□	SID115-MALWARE-BACKDOOR.Net...	Success		tcp $HOME_NET 20034 -> $EXTERNAL_NET...	F-SBID(--name "SID115-MALWARE-BACKD...
□	SID117-MALWARE-BACKDOOR.Infe...	Success		tcp $HOME_NET any -> $EXTERNAL_NET a...	F-SBID(--name "SID117-MALWARE-BACKD...
□	SID118-MALWARE-BACKDOOR.Sat...	Success		tcp $HOME_NET 666 -> $EXTERNAL_NET a...	F-SBID(--name "SID118-MALWARE-BACKD...
□	SID119-MALWARE-BACKDOOR.Dol...	Success		tcp $HOME_NET 6789 -> $EXTERNAL_NET ...	F-SBID(--name "SID119-MALWARE-BACKD...
□	SID121-MALWARE-BACKDOOR.Infe...	Success		tcp $EXTERNAL_NET 1000:1300 -> $HOME_...	F-SBID(--name "SID121-MALWARE-BACKD...
□	SID141-MALWARE-BACKDOOR.Hac...	Success		tcp $HOME_NET 31785 -> $EXTERNAL_NET...	F-SBID(--name "SID141-MALWARE-BACKD...
□	SID144-PROTOCOL-FTP.ADMw0rm....	Success		tcp $EXTERNAL_NET any -> $HOME_NET 2...	F-SBID(--name "SID144-PROTOCOL-FTP.A...
□	SID146-MALWARE-BACKDOOR.Net...	Success		tcp $HOME_NET 30100:30102 -> $EXTERN...	F-SBID(--name "SID146-MALWARE-BACKD...
□	SID147-MALWARE-BACKDOOR.Gat...	Success		tcp $HOME_NET 6969 -> $EXTERNAL_NET ...	F-SBID(--name "SID147-MALWARE-BACKD...

3. Click each column heading to filter the list of displayed signature rules.
   - Click *<number> Failed to Convert* to display only the signature rules that failed to convert from Snort signature files to Fortinet supported IPS signatures.
   - Click *<number> Failed to Push* to display only the signature rules that failed to be pushed from FortiSigConverter MEA to FortiManager.
   - Click *<number> Unpushed* to display signature rules that have not yet been pushed from FortiSigConverter MEA to FortiManager.
4. Click *<number> Total Rules* to display all signature rules again.

Pushing converted signature rules to FortiManager

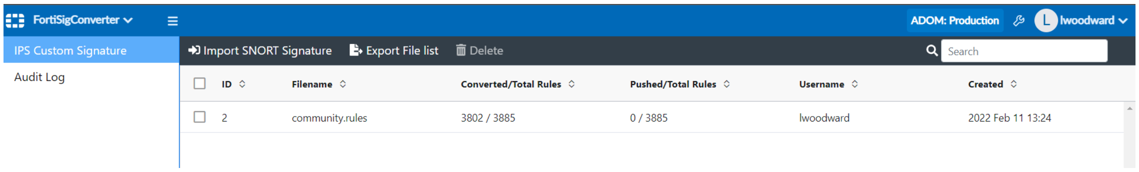
After you import Snort signature files to FortiSigConverter MEA, the signature rules are automatically converted to a Fortinet supported format, and you can push the converted signature rules to FortiManager.

If you are using FortiManager 7.0.2 and later and ADOMs are enabled, ensure you are in the correct ADOM. You can only push converted signature rules to the *Policy & Objects* module in the same ADOM as FortiSigConverter MEA.

After you push converted signature rules from FortiSigConverter MEA to FortiManager, they are displayed as custom IPS signatures on the *Policy & Objects* module.

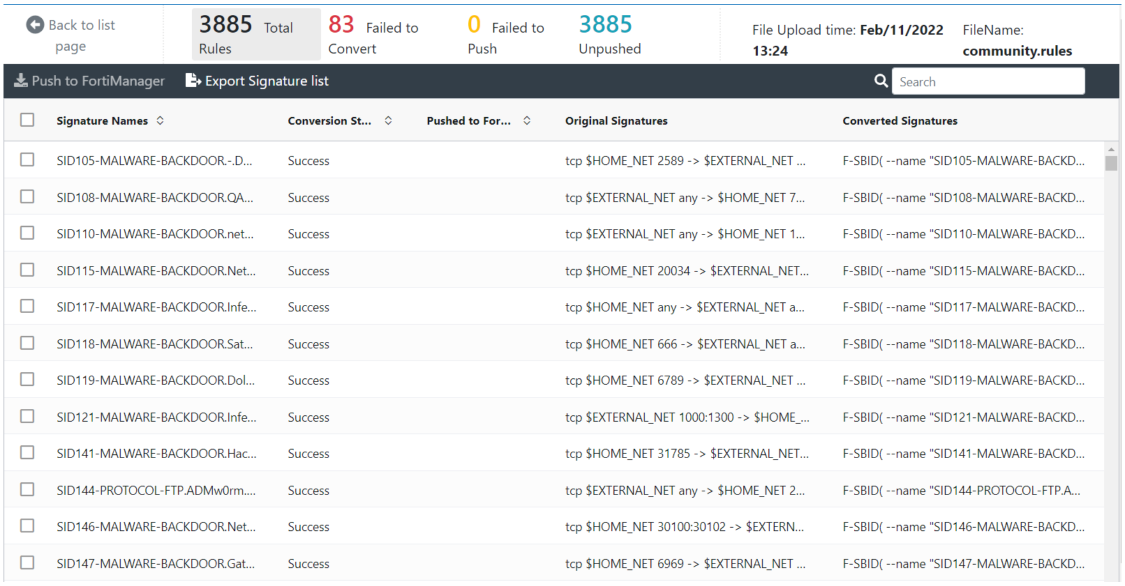
To push converted signature rules:

1. Go to *IPS Custom Signature*.
   The list of imported Snort signature files is displayed.



□	ID	Filename	Converted/Total Rules	Pushed/Total Rules	Username	Created
□	2	community.rules	3802 / 3885	0 / 3885	lwoodward	2022 Feb 11 13:24

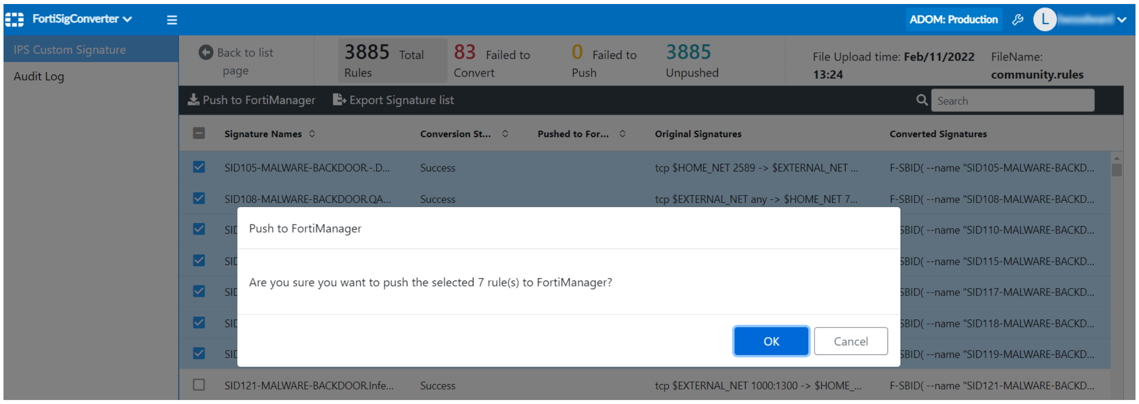
2. Click an imported Snort file to view its list of converted signature rules.



File Upload time: **Feb/11/2022 13:24** FileName: **community.rules**

□	Signature Names	Conversion St...	Pushed to For...	Original Signatures	Converted Signatures
□	SID105-MALWARE-BACKDOOR.-.D...	Success		tcp $HOME_NET 2589 -> $EXTERNAL_NET ...	F-SBID(--name "SID105-MALWARE-BACKD...
□	SID108-MALWARE-BACKDOOR.QA...	Success		tcp $EXTERNAL_NET any -> $HOME_NET 7...	F-SBID(--name "SID108-MALWARE-BACKD...
□	SID110-MALWARE-BACKDOOR.net...	Success		tcp $EXTERNAL_NET any -> $HOME_NET 1...	F-SBID(--name "SID110-MALWARE-BACKD...
□	SID115-MALWARE-BACKDOOR.Net...	Success		tcp $HOME_NET 20034 -> $EXTERNAL_NET...	F-SBID(--name "SID115-MALWARE-BACKD...
□	SID117-MALWARE-BACKDOOR.Infe...	Success		tcp $HOME_NET any -> $EXTERNAL_NET a...	F-SBID(--name "SID117-MALWARE-BACKD...
□	SID118-MALWARE-BACKDOOR.Sat...	Success		tcp $HOME_NET 666 -> $EXTERNAL_NET a...	F-SBID(--name "SID118-MALWARE-BACKD...
□	SID119-MALWARE-BACKDOOR.Dol...	Success		tcp $HOME_NET 6789 -> $EXTERNAL_NET ...	F-SBID(--name "SID119-MALWARE-BACKD...
□	SID121-MALWARE-BACKDOOR.Infe...	Success		tcp $EXTERNAL_NET 1000:1300 -> $HOME_...	F-SBID(--name "SID121-MALWARE-BACKD...
□	SID141-MALWARE-BACKDOOR.Hac...	Success		tcp $HOME_NET 31785 -> $EXTERNAL_NET...	F-SBID(--name "SID141-MALWARE-BACKD...
□	SID144-PROTOCOL-FTP.ADMw0rm....	Success		tcp $EXTERNAL_NET any -> $HOME_NET 2...	F-SBID(--name "SID144-PROTOCOL-FTP.A...
□	SID146-MALWARE-BACKDOOR.Net...	Success		tcp $HOME_NET 30100:30102 -> $EXTERN...	F-SBID(--name "SID146-MALWARE-BACKD...
□	SID147-MALWARE-BACKDOOR.Gat...	Success		tcp $HOME_NET 6969 -> $EXTERNAL_NET ...	F-SBID(--name "SID147-MALWARE-BACKD...

3. Select one or more signature rules, and click *Push to FortiManager*.
   A confirm dialog box is displayed.

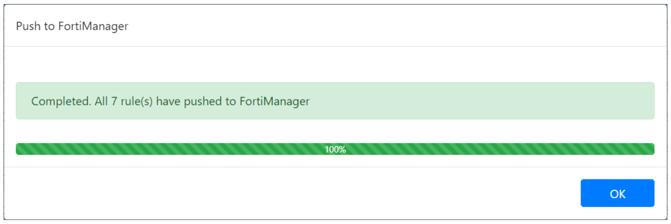


☐	Signature Names	Conversion St...	Pushed to For...	Original Signatures	Converted Signatures
☑	SID105-MALWARE-BACKDOOR.-.D...	Success		tcp $HOME_NET 2589 -> $EXTERNAL_NET ...	F-SBID(--name "SID105-MALWARE-BACKD...
☑	SID108-MALWARE-BACKDOOR.QA...	Success		tcp $EXTERNAL_NET any -> $HOME_NET 7...	F-SBID(--name "SID108-MALWARE-BACKD...
☑	SI				SBID(--name "SID110-MALWARE-BACKD...
☑	SI				SBID(--name "SID115-MALWARE-BACKD...
☑	SI				SBID(--name "SID117-MALWARE-BACKD...
☑	SI				SBID(--name "SID118-MALWARE-BACKD...
☑	SI				SBID(--name "SID119-MALWARE-BACKD...
☐	SID121-MALWARE-BACKDOOR.Infe...	Success		tcp $EXTERNAL_NET 1000:1300 -> $HOME_...	F-SBID(--name "SID121-MALWARE-BACKD...

Push to FortiManager

Are you sure you want to push the selected 7 rule(s) to FortiManager?

4. Click *OK*.
   A progress bar displays the status.



Push to FortiManager

Completed. All 7 rule(s) have pushed to FortiManager

5. When the progress bar displays 100%, click *OK* to complete the process.

Viewing signature rules on FortiManager

After you push converted signature rules from FortiSigConverter MEA to FortiManager, they are displayed as custom IPS signatures on the *Policy & Objects* module.

This section describes how to view custom IPS signatures in the following versions of FortiManager:

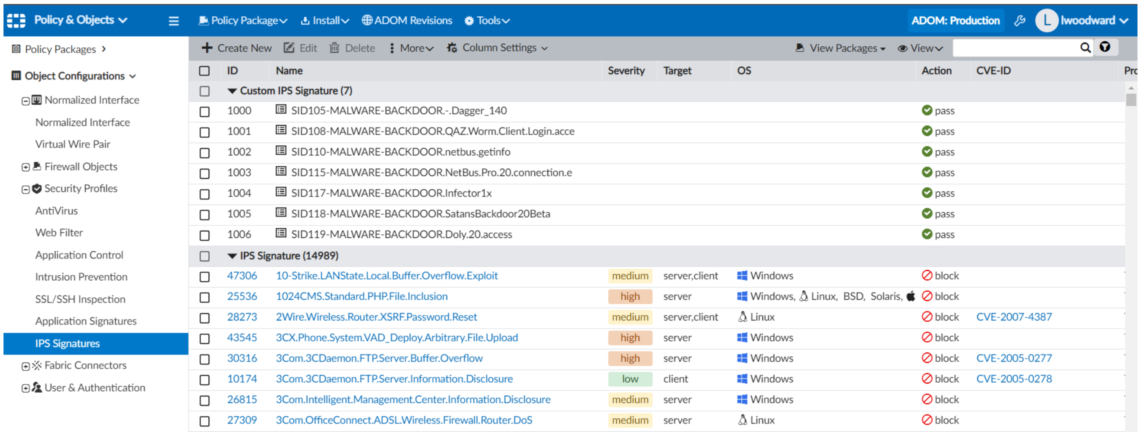
- For FortiManager 7.0, see FortiManager 7.0 on page 11.
- For FortiManager 6.4, see FortiManager 6.4 on page 12.

FortiManager 7.0

In FortiManager 7.0.2 and later, ensure that you are in the correct ADOM, if ADOMs are enabled. You must be in the same ADOM where you imported Snort signature files to FortiSigConverter MEA. FortiSigConverter MEA is unique in each ADOM.

To view custom IPS signatures in FortiManager:

1. In *FortiManager*, go to *Policy & Objects*, and expand *Object Configurations*.
2. In the tree menu, expand *Security Profiles* > *IPS Signature*.
   The custom IPS signatures from FortiSigConverter MEA are displayed in the content pane.



☐	ID	Name	Severity	Target	OS	Action	CVE-ID	Pro
☐	Custom IPS Signature (7)							
☐	1000	SID105-MALWARE-BACKDOOR.-.Dagger_140				✓ pass		
☐	1001	SID108-MALWARE-BACKDOOR.QAZ.Worm.Client.Login.acce				✓ pass		
☐	1002	SID110-MALWARE-BACKDOOR.netbus.getinfo				✓ pass		
☐	1003	SID115-MALWARE-BACKDOOR.NetBus.Pro.20.connection.e				✓ pass		
☐	1004	SID117-MALWARE-BACKDOOR.Infector1x				✓ pass		
☐	1005	SID118-MALWARE-BACKDOOR.SatansBackdoor20Beta				✓ pass		
☐	1006	SID119-MALWARE-BACKDOOR.Doly.20.access				✓ pass		
☐	IPS Signature (14989)							
☐	47306	10-Strike.LANState.Local.Buffer.Overflow.Exploit	medium	server,client	Windows	⊘ block		
☐	25536	1024CMS.Standard.PHP.File.Inclusion	high	server	Windows, Linux, BSD, Solaris,	⊘ block		
☐	28273	2Wire.Wireless.Router.XSRF.Password.Reset	medium	server,client	Linux	⊘ block	CVE-2007-4387	
☐	43545	3CX.Phone.System.VAD_Deploy.Arbitrary.File.Upload	high	server	Windows	⊘ block		
☐	30316	3Com.3CDaemon.FTP.Server.Buffer.Overflow	high	server	Windows	⊘ block	CVE-2005-0277	
☐	10174	3Com.3CDaemon.FTP.Server.Information.Disclosure	low	client	Windows	⊘ block	CVE-2005-0278	
☐	26815	3Com.Intelligent.Management.Center.Information.Disclosure	medium	server	Windows	⊘ block		
☐	27309	3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	medium	server	Linux	⊘ block		

FortiManager 6.4

In FortiManager 6.4.x, you must enable *IPS Custom Signature* display options before you can view signatures from FortiSigConverter MEA in FortiManager.

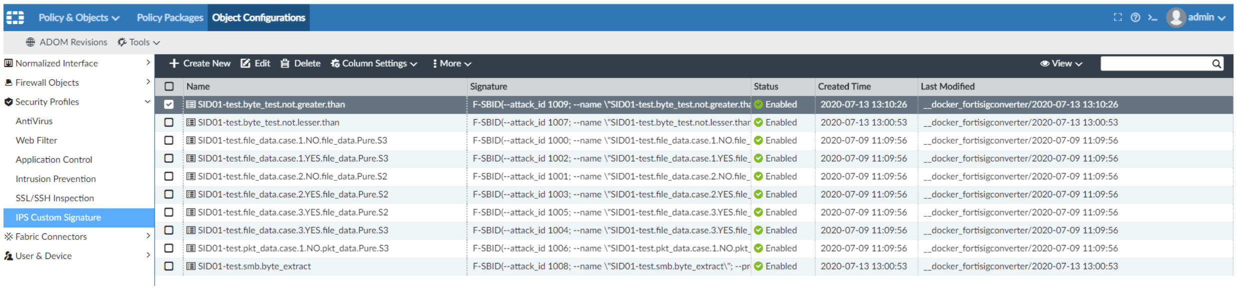
You must be in the root ADOM.

To display custom IPS signatures in FortiManager:

1. In *FortiManager*, go to *Policy & Objects* > *Object Configurations*.
2. In the banner, click *Tools* > *Display Options*.
3. In the *Security Profiles* module, select *IPS Custom Signature*.
4. Click *OK*.

To view custom IPS signatures in FortiManager:

1. In *FortiManager*, go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Security Profiles* > *IPS Custom Signature*.
   The custom IPS signatures from FortiSigConverter MEA are displayed in the content pane.



☐	Name	Signature	Status	Created Time	Last Modified
☑	SID01-test.byte_test.not.greater.than	F-SBID(--attack_id 1009; --name \"SID01-test.byte_test.not.greater.tha	Enabled	2020-07-13 13:10:26	__docker_fortisigconverter/2020-07-13 13:10:26
☐	SID01-test.byte_test.not.lesser.than	F-SBID(--attack_id 1007; --name \"SID01-test.byte_test.not.lesser.thar	Enabled	2020-07-13 13:00:53	__docker_fortisigconverter/2020-07-13 13:00:53
☐	SID01-test.file_data.case.1.NO.file_data.Pure.S3	F-SBID(--attack_id 1000; --name \"SID01-test.file_data.case.1.NO.file_	Enabled	2020-07-09 11:09:56	__docker_fortisigconverter/2020-07-09 11:09:56
☐	SID01-test.file_data.case.1.YES.file_data.Pure.S3	F-SBID(--attack_id 1002; --name \"SID01-test.file_data.case.1.YES.file_	Enabled	2020-07-09 11:09:56	__docker_fortisigconverter/2020-07-09 11:09:56
☐	SID01-test.file_data.case.2.NO.file_data.Pure.S2	F-SBID(--attack_id 1001; --name \"SID01-test.file_data.case.2.NO.file_	Enabled	2020-07-09 11:09:56	__docker_fortisigconverter/2020-07-09 11:09:56
☐	SID01-test.file_data.case.2.YES.file_data.Pure.S2	F-SBID(--attack_id 1003; --name \"SID01-test.file_data.case.2.YES.file_	Enabled	2020-07-09 11:09:56	__docker_fortisigconverter/2020-07-09 11:09:56
☐	SID01-test.file_data.case.3.YES.file_data.Pure.S2	F-SBID(--attack_id 1005; --name \"SID01-test.file_data.case.3.YES.file_	Enabled	2020-07-09 11:09:56	__docker_fortisigconverter/2020-07-09 11:09:56
☐	SID01-test.file_data.case.3.YES.file_data.Pure.S3	F-SBID(--attack_id 1004; --name \"SID01-test.file_data.case.3.YES.file_	Enabled	2020-07-09 11:09:56	__docker_fortisigconverter/2020-07-09 11:09:56
☐	SID01-test.pkt_data.case.1.NO.pkt_data.Pure.S3	F-SBID(--attack_id 1006; --name \"SID01-test.pkt_data.case.1.NO.pkt_	Enabled	2020-07-09 11:09:56	__docker_fortisigconverter/2020-07-09 11:09:56
☐	SID01-test.smb.byte_extract	F-SBID(--attack_id 1008; --name \"SID01-test.smb.byte_extract\"; --pr	Enabled	2020-07-13 13:00:53	__docker_fortisigconverter/2020-07-13 13:00:53

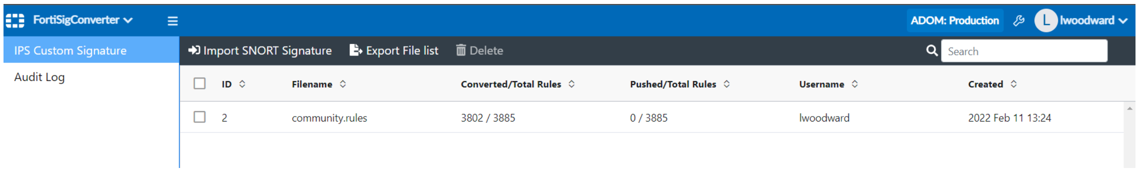
Deleting imported Snort files

After you import Snort files to FortiSigConverter MEA, you can delete the Snort file and all of its converted signature rules from FortiSigConverter MEA.

When you delete a Snort file from FortiSigConverter MEA, the corresponding custom IPS signatures on the *Policy & Objects* module in FortiManager are not automatically deleted. You must manually delete custom IPS signatures from the *Policy & Objects* module in FortiManager.

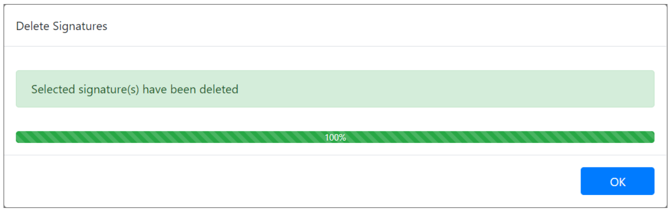
To delete imported Snort files:

1. Go to *IPS Custom Signature*.
   The list of imported Snort files is displayed.



□	ID	Filename	Converted/Total Rules	Pushed/Total Rules	Username	Created
□	2	community.rules	3802 / 3885	0 / 3885	lwoodward	2022 Feb 11 13:24

2. In the *ID* column, select a Snort file, and click *Delete*.
   A confirmation dialog box is displayed.
3. Click *OK*.
   A progress bar is displayed.
4. When the progress reaches 100%, click *OK*.


Delete Signatures

Selected signature(s) have been deleted

The Snort file and all its converted signature rules are removed from FortiSigConverter MEA.

Exporting Snort file lists

You can export a list of Snort files that have been imported into FortiSigConverter MEA. An `export.csv` file of information is downloaded to your computer.

To export a Snort file list:

1. Go to *IPS Custom Signature*.
   The list of imported Snort files is displayed.
2. In the toolbar, click *Export File list*.
   An `export.csv` file is downloaded to your computer.
   The report contains the following information:

ID	The ID number for the Snort file import.
Filename	The name of the Snort signature file imported into FortiSigConverter MEA.
Converted/Total	The number of signature rules converted to Fortinet supported IPS signatures.

Rules	
Pushed/Total Rules	The number of signature rules pushed to FortiManager.
Username	The username of the admin who imported the signature file.
Created	The date the file was imported into FortiSigConverter MEA.

Exporting converted signature lists

After you import a Snort signature file into FortiSigConverter MEA, you can export a list of converted signatures. An `export.csv` file of information is downloaded to your computer.

To export a converted signature list:

1. Go to *IPS Custom Signature*.
   The list of imported Snort files is displayed.
2. Click a Snort file to view its list of converted signatures.
3. In the toolbar, click *Export Signature list*.
   An `export.csv` file is downloaded to your computer and contains the following information:

Signature Names	The IPS signature name.
Conversion Status	The conversion status. TRUE = The conversion was successful. FALSE = The conversion failed.
Pushed to FortiManager	Indicates if the signature rule was pushed to FortiManager. 1 = The signature rule was pushed to FortiManager. -1 = The signature rule was not pushed to FortiManager .
Original Signatures	The Snort signature before it was converted in FortiSigConverter MEA.
Converted Signatures	The signature after it was converted to a supported IPS signature.

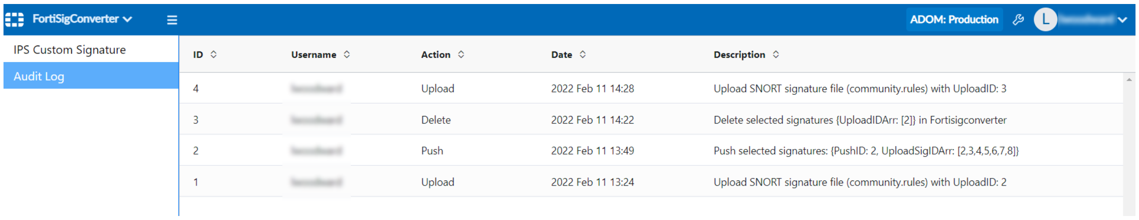
Viewing the audit log

The audit log displays a list of actions performed in FortiSigConverter MEA for the ADOM.

If ADOMs are enabled in FortiManager 7.0.2 or later, you must select the correct ADOM before you can view audit log for FortiSigConverter MEA.

To view the audit log:

1. If ADOMs are enabled, ensure you are in the correct ADOM.
2. Go to *FortiSigConverter MEA > Audit Log*.
   The audit log is displayed.



ID	Username	Action	Date	Description
4	[redacted]	Upload	2022 Feb 11 14:28	Upload SNORT signature file (community.rules) with UploadID: 3
3	[redacted]	Delete	2022 Feb 11 14:22	Delete selected signatures {UploadIDArr: [2]} in Fortisigconverter
2	[redacted]	Push	2022 Feb 11 13:49	Push selected signatures: {PushID: 2, UploadSigIDArr: [2,3,4,5,6,7,8]}
1	[redacted]	Upload	2022 Feb 11 13:24	Upload SNORT signature file (community.rules) with UploadID: 2

More information

FortiSigConverter MEA is available as a management extension application with FortiManager. For information about FortiSigConverter MEA, see the FortiManager page on the Document Library.

www.fortinet.com