Netsurion®

Integration Guide

Integrate Forcepoint NGFW with the Netsurion Open XDR platform

Publication Date:

February 27, 2023

Abstract

This guide provides instructions to configure the Data Source Integrations in the Netsurion Open XDR platform to receive the logs from the Forcepoint NGFW. The Data Source Integrations contains alerts, reports, dashboards, categories, and knowledge object.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR platform version 9.3 or later and Forcepoint NGFW version 6.8.8 and later.

Audience

This guide is for the administrators responsible for configuring the Data Source Integration in the Netsurion Open XDR platform.

Product Terminology

The following are the terms used throughout this guide:

- The term “Netsurion’s Open XDR platform” or “the Netsurion Open XDR platform” or “the Open XDR platform” refers to EventTracker.
- The term “Data Source Integrations” refers to Knowledge Packs.

Table of Contents

1 Overview

Forcepoint NGFW supports multiple components which provide services to inspect traffic logs, block malicious attacks, prevents data thefts etc. and all such events can be observed or managed by management console.

Netsurion's Open XDR platform seamlessly combines SIEM, Log Management, File Integrity Monitoring, Machine Analytics, and User Behavior Monitoring. The dashboard, category, alerts, and reports in Netsurion's Open XDR platform benefit in tracking critical activities, security warning activities, and others.

2 Prerequisite

- Configure Forcepoint NGFW to forward logs to Netsurion Managed open XDR.

Note

Refer to How-To guide to configure Forcepoint NGFW to forward logs to Managed open XDR console.

3 The Netsurion Open XDR platform Data Source Integration (DSI)

After Netsurion's Open XDR platform receives the logs, configure the Data Source Integration in the Netsurion Open XDR platform.

The following Data source integration are available in the Netsurion Open XDR platform.

3.1 Category

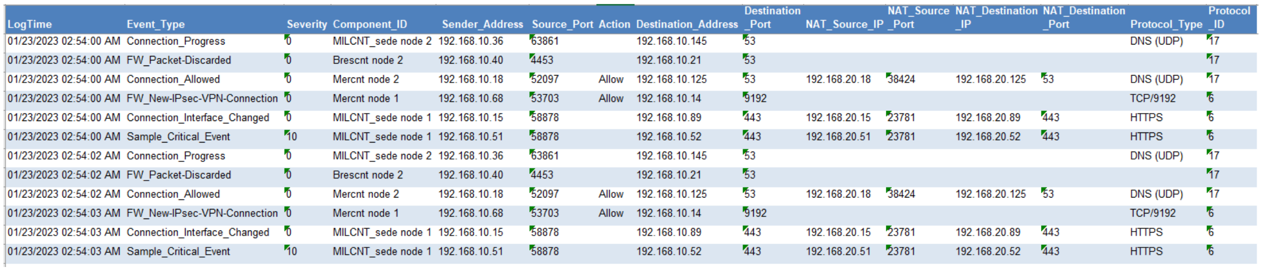
Forcepoint NGFW - Events overview: This category will provide detailed analysis on all events observed on Forcepoint NGFW firewall.

3.2 Alerts

Forcepoint NGFW: Critical events detected: This alert will trigger when a critical level of severity events has been detected by Forcepoint NGFW.

3.3 Reports

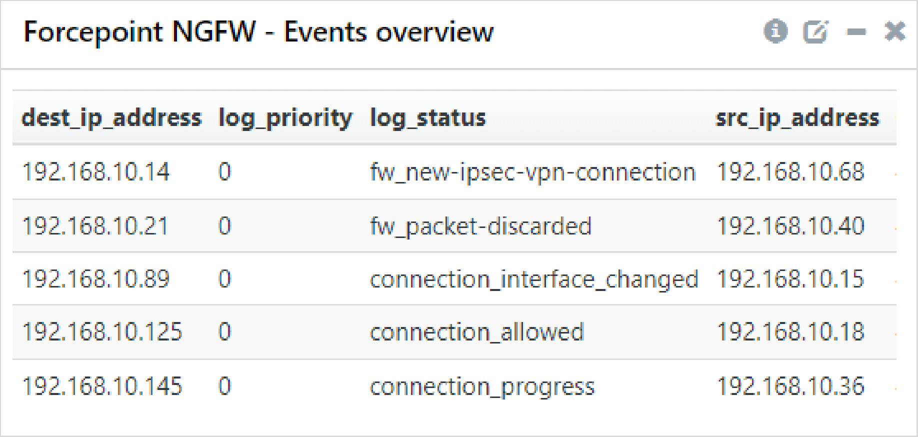
Forcepoint NGFW - Events overview: This report will capture all events performed on Forcepoint NGFW.



LogTime	Event_Type	Severity	Component_ID	Sender_Address	Source_Port	Action	Destination_Address	Destination _Port	NAT_Source_IP	NAT_Source _Port	NAT_Destination _IP	NAT_Destination _Port	Protocol_Type	Protocol _ID
01/23/2023 02:54:00 AM	Connection_Progress	0	MILCNT_sede node 2	192.168.10.36	63861		192.168.10.145	53					DNS (UDP)	17
01/23/2023 02:54:00 AM	FW_Packet-Discarded	0	Brescnt node 2	192.168.10.40	4453		192.168.10.21	53						17
01/23/2023 02:54:00 AM	Connection_Allowed	0	Mercnt node 2	192.168.10.18	52097	Allow	192.168.10.125	53	192.168.20.18	38424	192.168.20.125	53	DNS (UDP)	17
01/23/2023 02:54:00 AM	FW_New-IPsec-VPN-Connection	0	Mercnt node 1	192.168.10.68	53703	Allow	192.168.10.14	9192					TCP/9192	6
01/23/2023 02:54:00 AM	Connection_Interface_Changed	0	MILCNT_sede node 1	192.168.10.15	58878		192.168.10.89	443	192.168.20.15	23781	192.168.20.89	443	HTTPS	6
01/23/2023 02:54:00 AM	Sample_Critical_Event	10	MILCNT_sede node 1	192.168.10.51	58878		192.168.10.52	443	192.168.20.51	23781	192.168.20.52	443	HTTPS	6
01/23/2023 02:54:02 AM	Connection_Progress	0	MILCNT_sede node 2	192.168.10.36	63861		192.168.10.145	53					DNS (UDP)	17
01/23/2023 02:54:02 AM	FW_Packet-Discarded	0	Brescnt node 2	192.168.10.40	4453		192.168.10.21	53						17
01/23/2023 02:54:02 AM	Connection_Allowed	0	Mercnt node 2	192.168.10.18	52097	Allow	192.168.10.125	53	192.168.20.18	38424	192.168.20.125	53	DNS (UDP)	17
01/23/2023 02:54:03 AM	FW_New-IPsec-VPN-Connection	0	Mercnt node 1	192.168.10.68	53703	Allow	192.168.10.14	9192					TCP/9192	6
01/23/2023 02:54:03 AM	Connection_Interface_Changed	0	MILCNT_sede node 1	192.168.10.15	58878		192.168.10.89	443	192.168.20.15	23781	192.168.20.89	443	HTTPS	6
01/23/2023 02:54:03 AM	Sample_Critical_Event	10	MILCNT_sede node 1	192.168.10.51	58878		192.168.10.52	443	192.168.20.51	23781	192.168.20.52	443	HTTPS	6

3.4 Dashboard

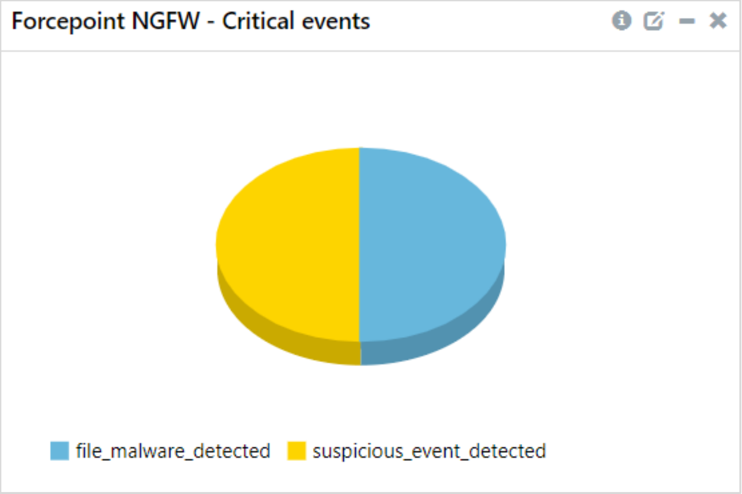
Forcepoint NGFW - Events overview: This dashlets display the different types of events like connection events, VPN events etc. logged by Forcepoint NGFW firewall.



Forcepoint NGFW - Events overview

dest_ip_address	log_priority	log_status	src_ip_address
192.168.10.14	0	fw_new-ipsec-vpn-connection	192.168.10.68
192.168.10.21	0	fw_packet-discarded	192.168.10.40
192.168.10.89	0	connection_interface_changed	192.168.10.15
192.168.10.125	0	connection_allowed	192.168.10.18
192.168.10.145	0	connection_progress	192.168.10.36

Forcepoint NGFW - Critical events: The dashlet will capture critical events like Malware or threat related events etc. detected by Forcepoint NGFW firewall.



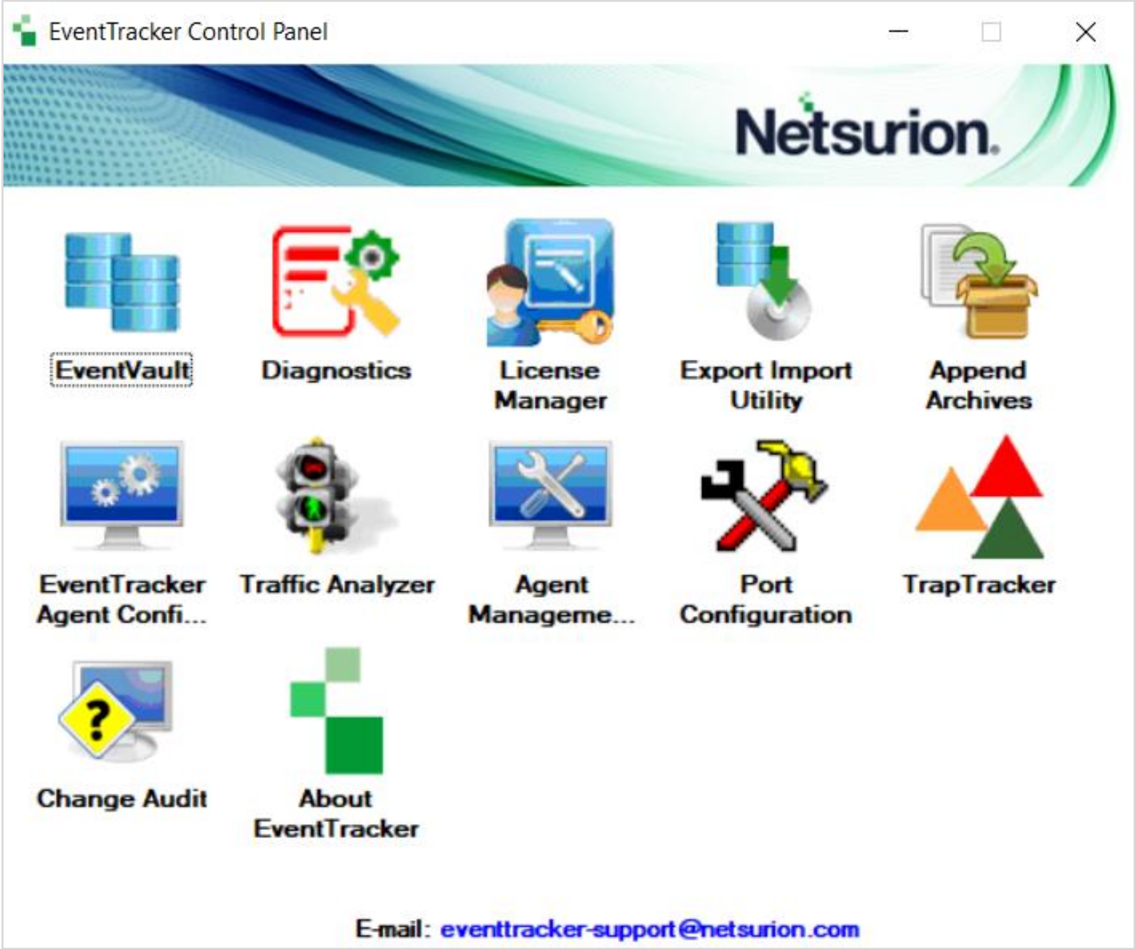
4 Importing Forcepoint NGFW Data Source Integration into the Netsurion Open XDR platform

Import the Data source integration items in the following sequence.

- Category
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards

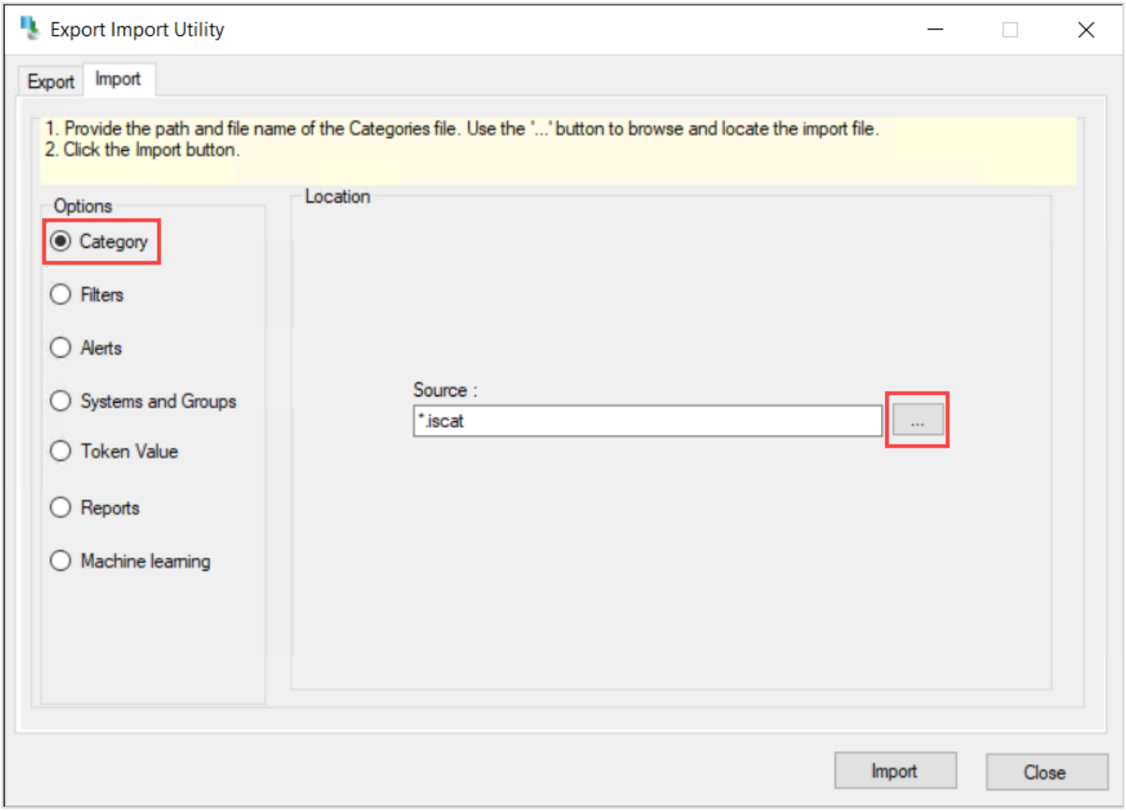
1. Launch the Netsurion Open XDR platform **Control Panel**.

2. Double click on **Export Import Utility** and click the **Import** tab.



4.1 Category

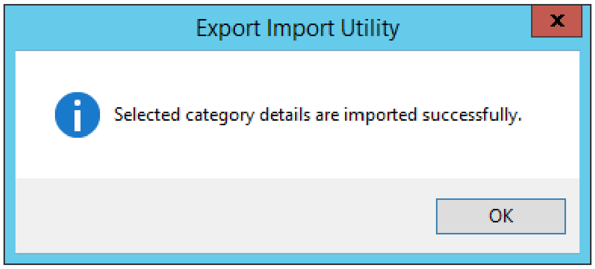
1. In the **Import** tab, choose the **Category** option, and then click the **Browse** ... button to locate the file.



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Source : *.iscat

2. In the **Browse** window, locate the **Categories_ Forcepoint NGFW.iscat** file and click **Open**.
3. To import the categories, click **Import**.
4. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Category**.

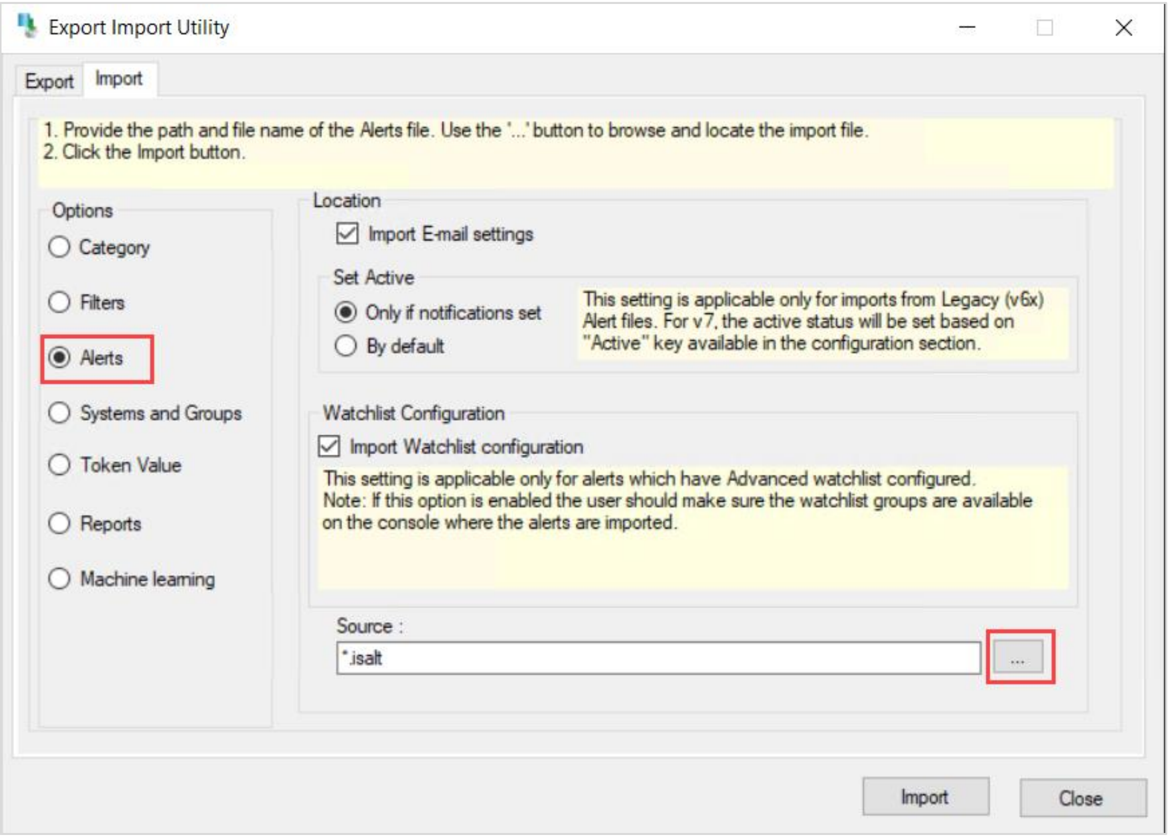


Selected category details are imported successfully.

5. Click **OK** or the **Close** button to complete the process.

4.2 Alerts

1. In the **Import** tab, choose the **Alerts** option, and then click the **Browse** ... button to locate the file.



Export Import Utility

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options: ○ Category ○ Filters ● Alerts ○ Systems and Groups ○ Token Value ○ Reports ○ Machine learning

Location: ☑ Import E-mail settings

Set Active: ● Only if notifications set ○ By default

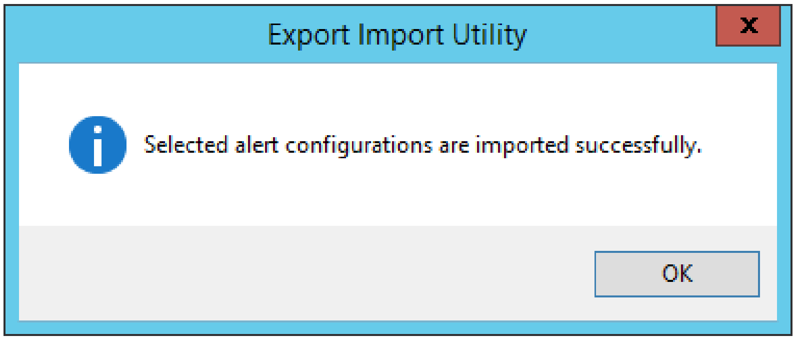
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Watchlist Configuration: ☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt

2. In the **Browse** window, locate the **Alerts_ Forcepoint NGFW.isalt** file, and then click **Open**.
3. To import the alerts, click **Import**.
4. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Alerts**.



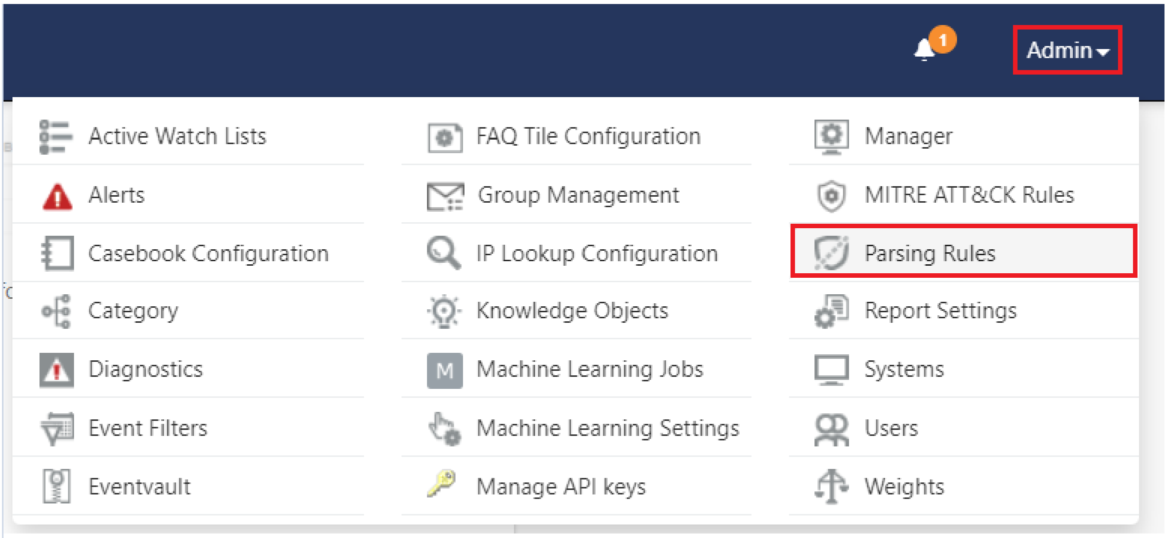
Export Import Utility

Selected alert configurations are imported successfully.

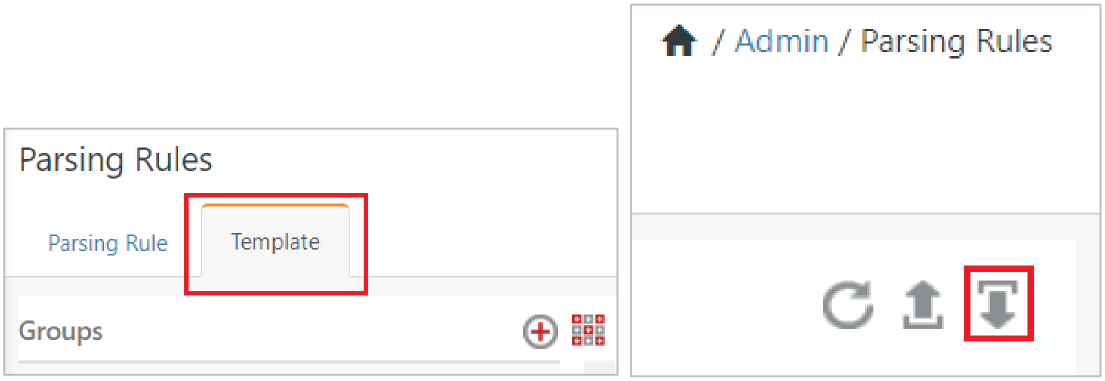
5. Click **OK** or the **Close** button to complete the process.

4.3 Token Template

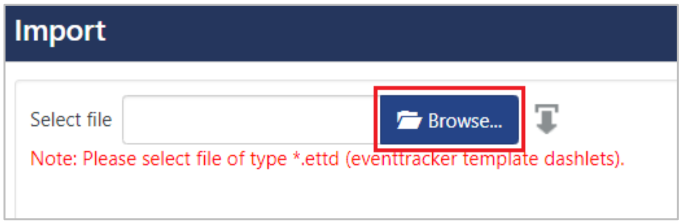
1. In the **Netsurion Open XDR** platform, hover over the **Admin** menu and click **Parsing Rules**.



2. In the **Parsing Rules** interface, click the **Template** tab and then click **Import Configuration**.

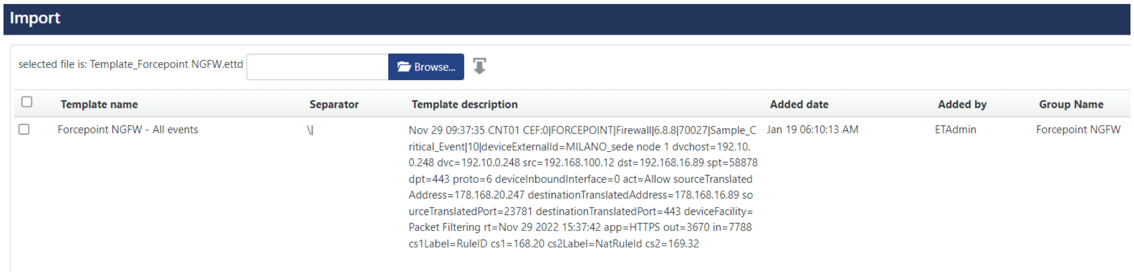


3. In the **Import** window, click **Browse** to search and locate for the **Templates_Forcepoint NGFW.ettd** file.



Note: Please select file of type *.ettd (eventtracker template dashlets).

4. It takes few seconds to load the templates and once templates are displayed, click the appropriate template, and click **Import**.



Import

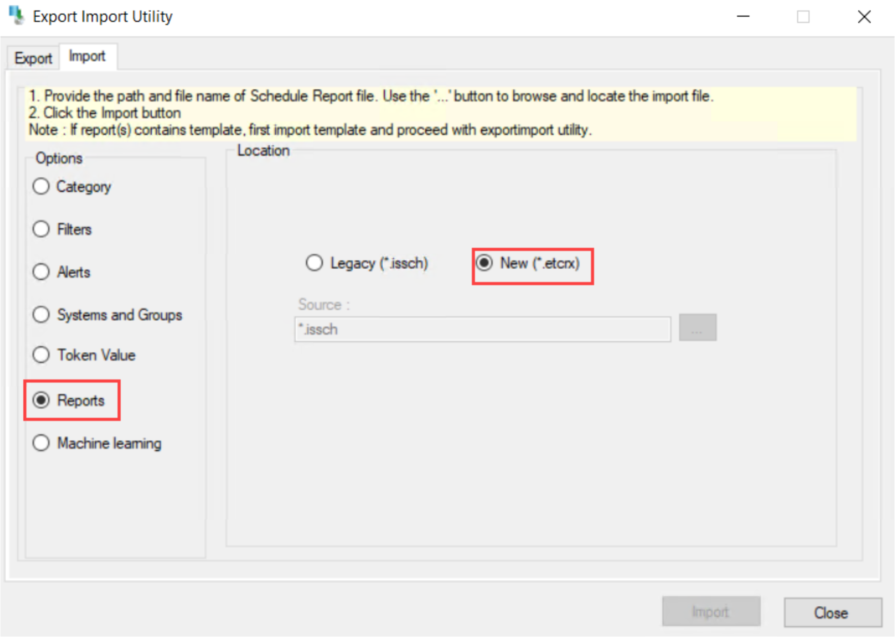
selected file is: Template_Forcepoint NGFW.ettd

<table>
<tr><th>□</th><th>Template name</th><th>Separator</th><th>Template description</th><th>Added date</th><th>Added by</th><th>Group Name</th></tr>
<tr><td>□</td><td>Forcepoint NGFW - All events</td><td>\|</td><td>Nov 29 09:37:35 CNT01 CEF:0|FORCEPOINT|Firewall|6.8.8|70027|Sample_Critical_Event|10|deviceExternalId=MILANO_sede node 1 dvchost=192.10.0.248 dvc=192.10.0.248 src=192.168.100.12 dst=192.168.16.89 spt=58878 dpt=443 proto=6 deviceInboundInterface=0 act=Allow sourceTranslatedAddress=178.168.20.247 destinationTranslatedAddress=178.168.16.89 sourceTranslatedPort=23781 destinationTranslatedPort=443 deviceFacility=Packet Filtering rt=Nov 29 2022 15:37:42 app=HTTPS out=3670 in=7788 cs1Label=RuleID cs1=168.20 cs2Label=NatRuleId cs2=169.32</td><td>Jan 19 06:10:13 AM</td><td>ETAdmin</td><td>Forcepoint NGFW</td></tr>
</table>

5. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Template.**

4.4 Reports

1. In the **Import** tab, choose the **Reports** option and then click **New (*.etcrx)**.



Export Import Utility

1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
● Reports
○ Machine learning

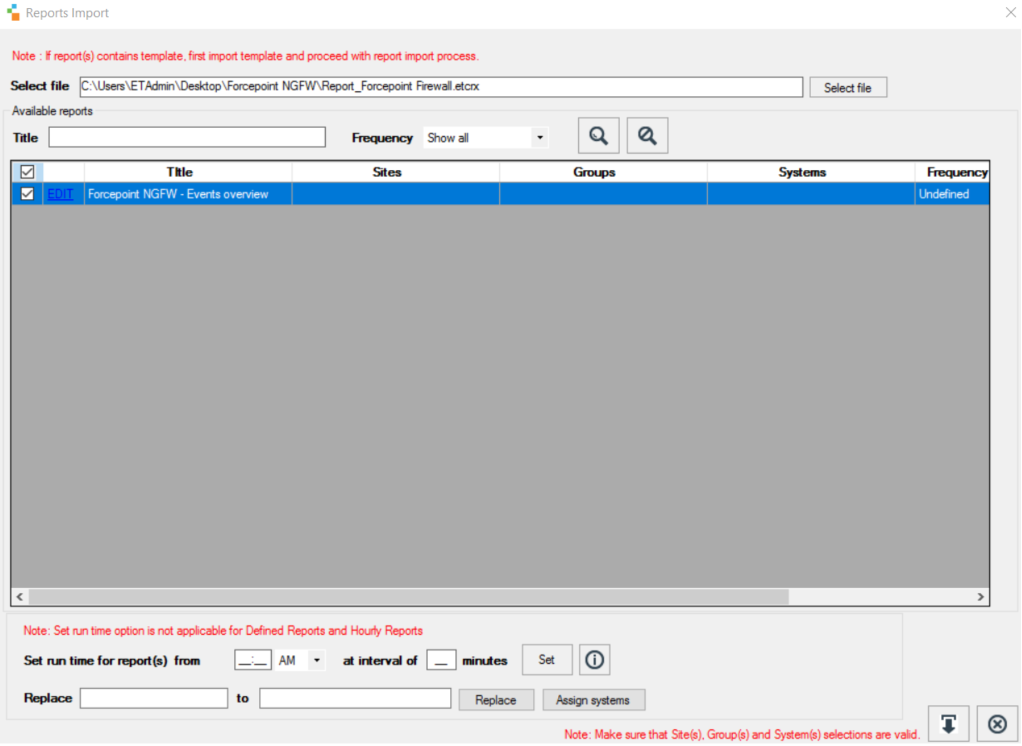
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

2. In the **Reports Import** window, click **Select file** to locate **Reports_ Forcepoint NGFW.etcrx** file.

3. Select the check box of all the files and click the **Import** ⤓ button to import the selected files.



Note : If report(s) contains template, first import template and proceed with report import process.

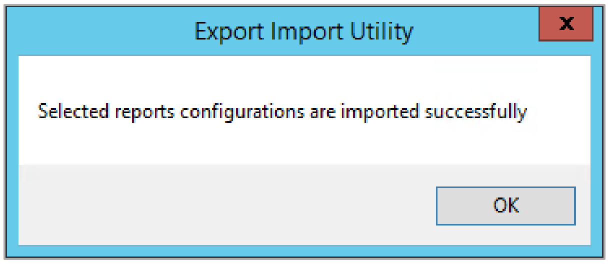
Select file C:\Users\ETAdmin\Desktop\Forcepoint NGFW\Report_Forcepoint Firewall.etcrx Select file

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	Forcepoint NGFW - Events overview				Undefined

Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

4. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Reports**.

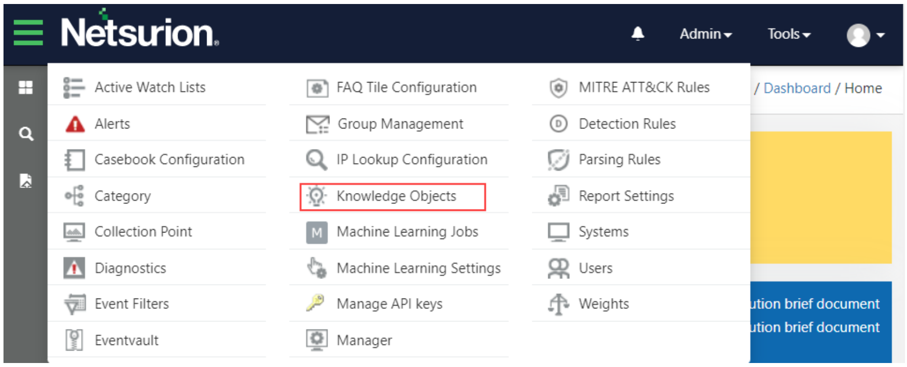


Selected reports configurations are imported successfully

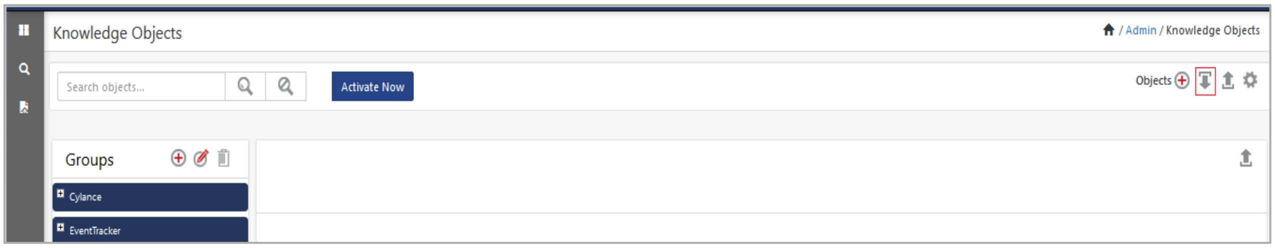
5. Click **OK** or the **Close** button to complete the process.

4.5 Knowledge Objects (KO)

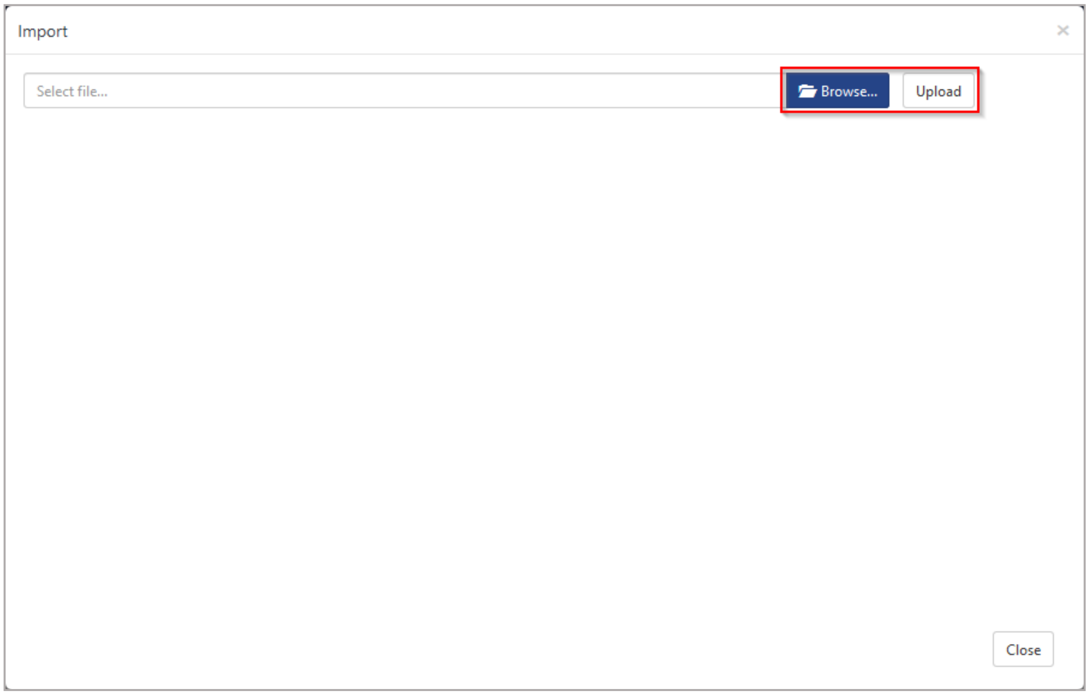
1. In the **Netsurion Open XDR platform**, hover over the **Admin** menu and click **Knowledge Objects**.



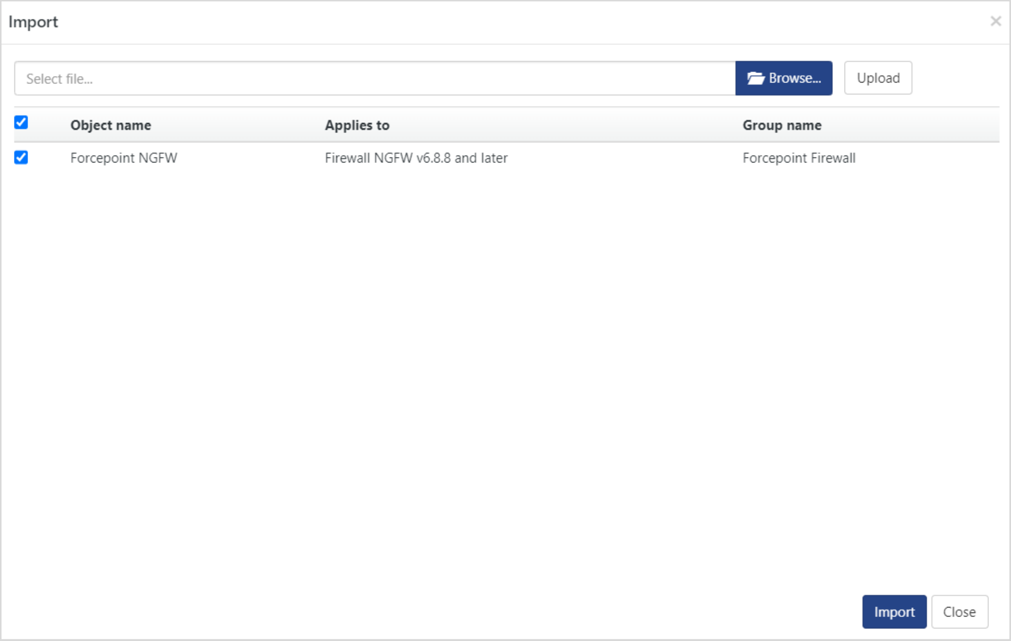
2. In the **Knowledge Objects** interface, click the **Import** ⤓ button to import the KO files.



3. In the **Import** window, click **Browse** and locate the **KO_Forcepoint NGFW.etko** file, and then click **Upload** to upload the file.

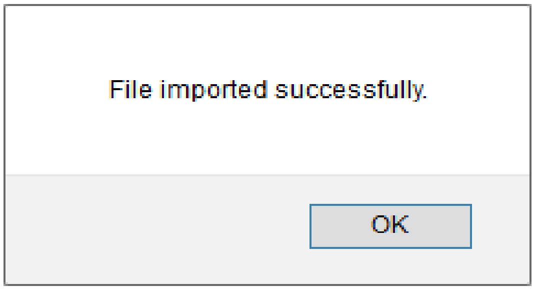


4. Select the check box next to the browsed KO file and then click the **Import** button.



☑	Object name	Applies to	Group name
☑	Forcepoint NGFW	Firewall NGFW v6.8.8 and later	Forcepoint Firewall

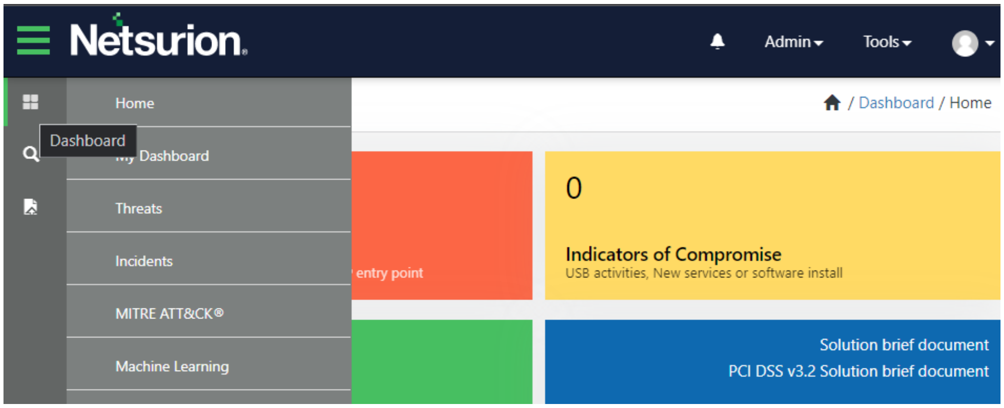
5. The Netsurion Open XDR platform displays a successful message on successfully importing the selected file in **Knowledge Objects**.


File imported successfully.

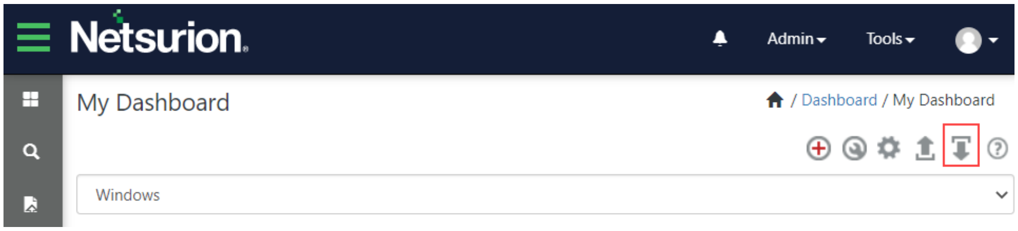
6. Click **OK** or the **Close** button to complete the process.

4.6 Dashboard

1. Log in to the **Netsurion Open XDR platform** and go to **Dashboard** > **My Dashboard**.

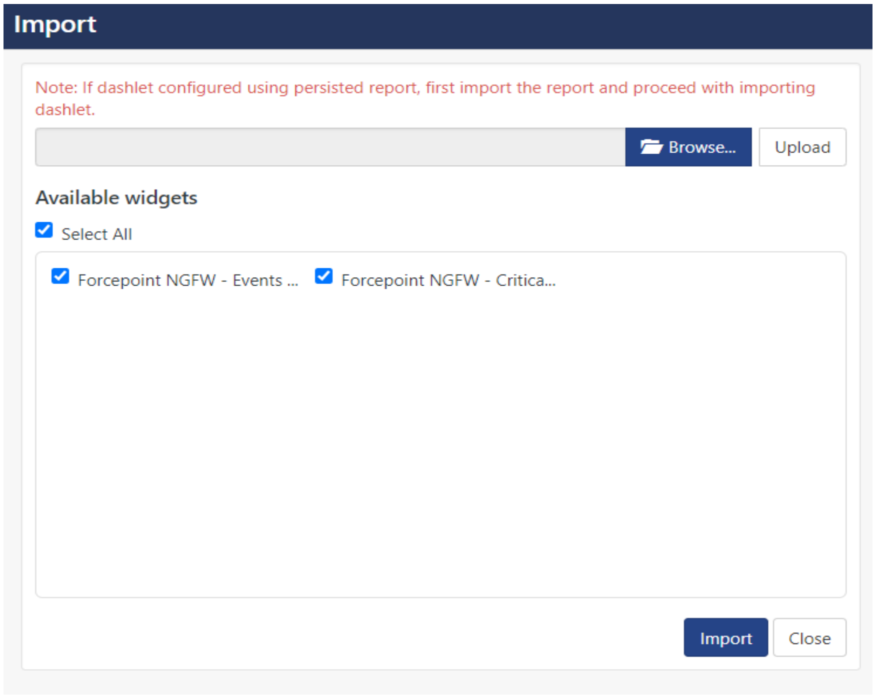


2. In the **My Dashboard** interface, click the **Import** ⤓ button to import the dashlet files.



3. In the **Import** window, click **Browse** to locate the **Dashboards_Forcepoint NGFW.etwd** file and then click **Upload.**

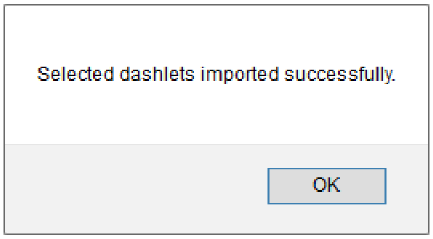
4. Click the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.


Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

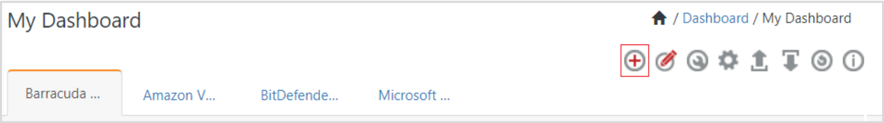
Browse...
Upload
Available widgets
☑ Select All
☑ Forcepoint NGFW - Events ...
☑ Forcepoint NGFW - Critica...
Import
Close

5. The Netsurion Open XDR platform displays the success message on successfully importing the dashlet files.

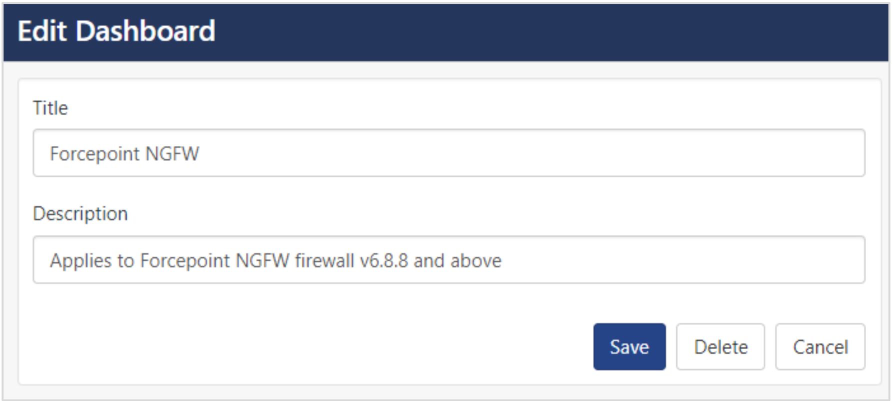


Selected dashlets imported successfully.

6. Then, in the **My Dashboard** interface click the **Add** ⊕ button to add the dashboard.



7. In the **Add Dashboard** interface, specify the **Title** and **Description** and click **Save**.



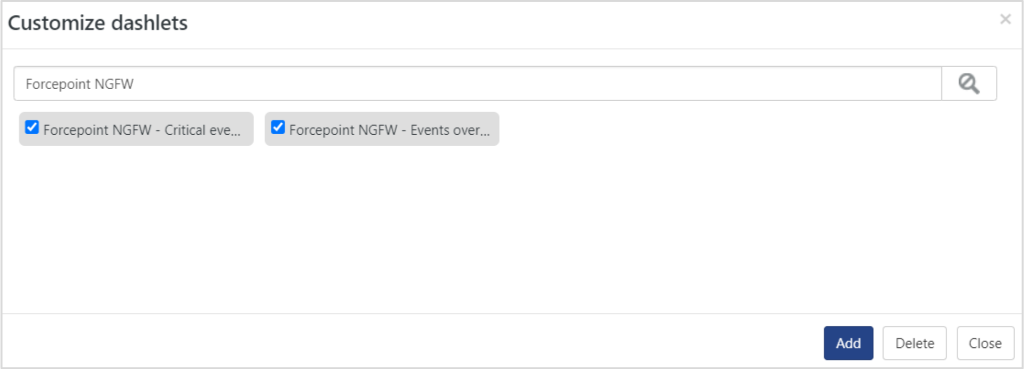
Edit Dashboard

Title: Forcepoint NGFW

Description: Applies to Forcepoint NGFW firewall v6.8.8 and above

8. From the newly created dashboard interface (for example, **Forcepoint NGFW**), click the **Configuration** button to add the Forcepoint NGFW dashlets.

9. Search and select the newly imported dashlets and click **Add**.



Customize dashlets

Forcepoint NGFW

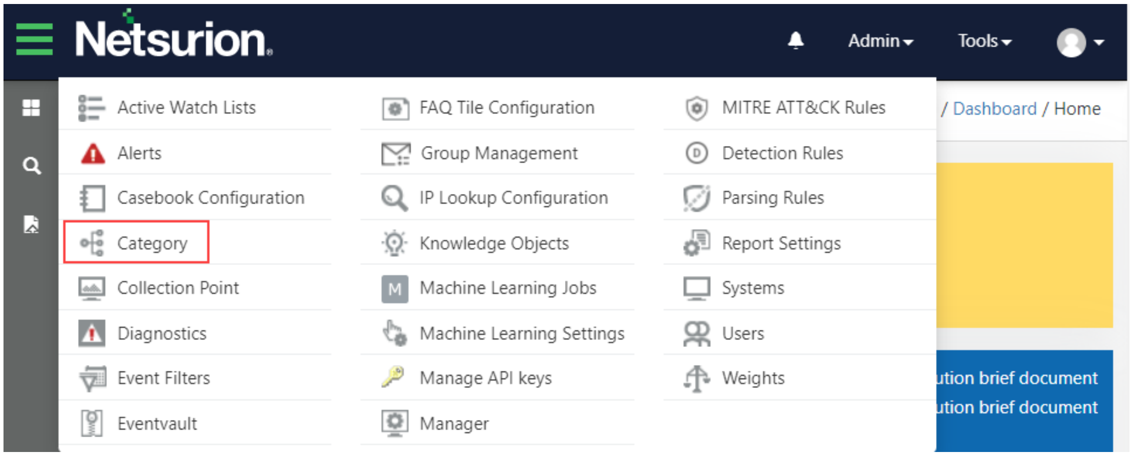
☑ Forcepoint NGFW - Critical eve...

☑ Forcepoint NGFW - Events over...

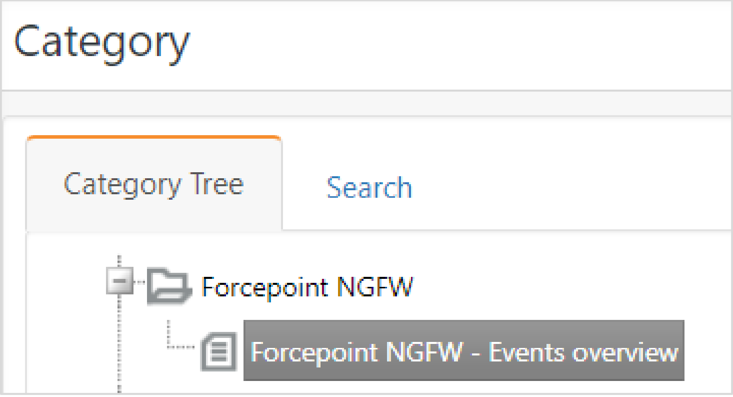
5 Verifying Forcepoint NGFW Data Source Integration in the Netsurion Open XDR platform

5.1 Category

1. In the **Netsurion Open XDR platform**, hover over the **Admin** menu and click **Category**.

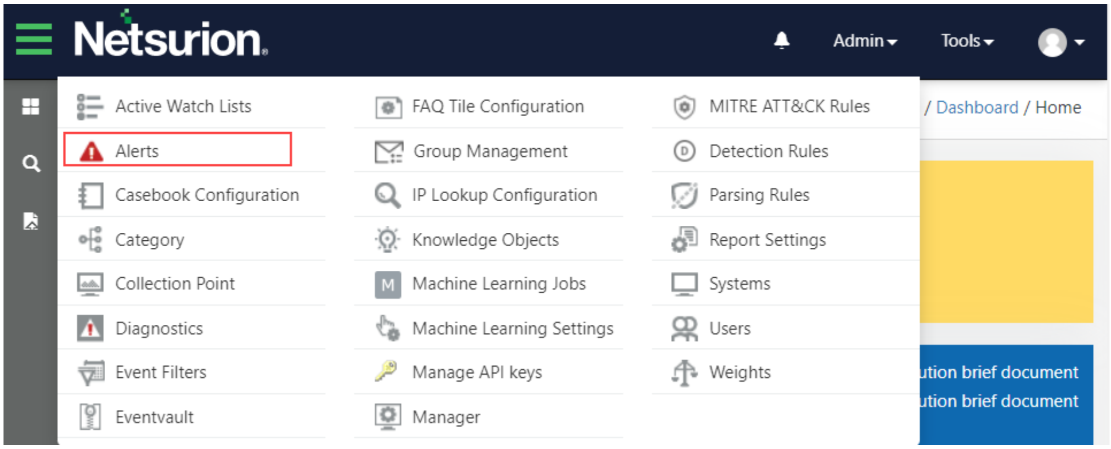


2. In the **Category** interface, under the **Category Tree** tab, click the **Forcepoint NGFW** group folder to expand and see the imported categories.



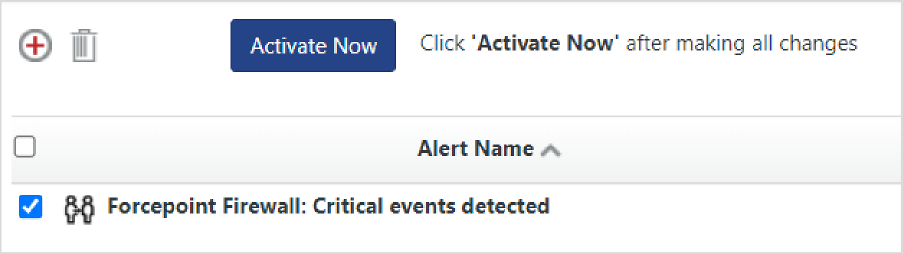
5.2 Alerts

1. In the **Netsurion Open XDR platform**, hover over the **Admin** menu and click **Alerts**.



2. In the **Alerts** interface, type **Forcepoint NGFW** in the **Search** field and click the **Search** button.

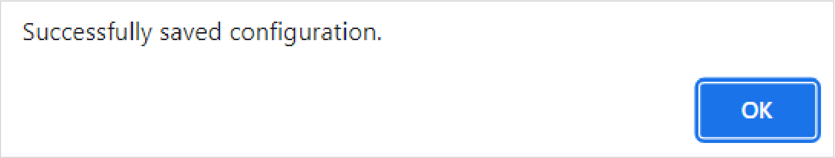
   The **Alerts** interface will display all the imported **Forcepoint NGFW** alerts.



☑ Forcepoint Firewall: Critical events detected

3. To activate the imported alert, toggle the **Active** button, which is available next to the respective alert name.

   Once done, it displays a success message on successfully configuring the alerts.


Successfully saved configuration.

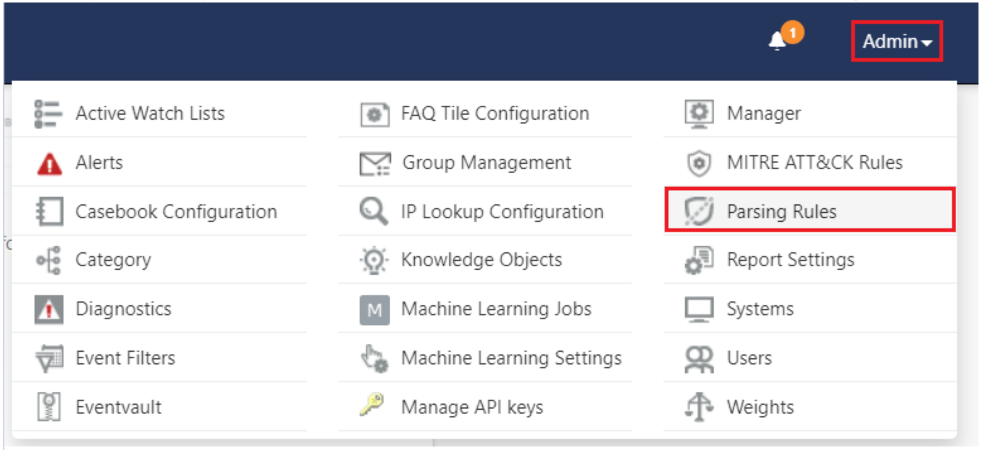
4. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

> **Note**
>
> You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

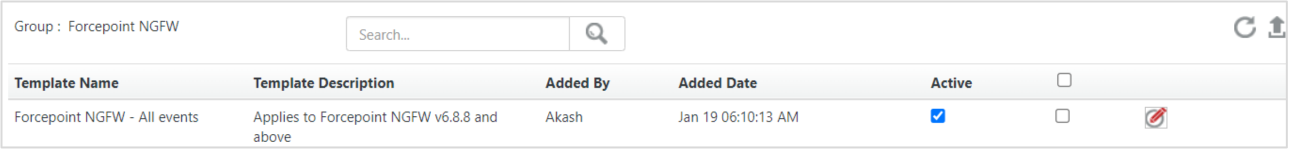
> **Note**
>
> In the **Alert Configuration** interface, specify the appropriate **System** for better performance.

5.3 Token Template

1. In the **Netsurion Open XDR platform**, hover over the **Admin** menu and click Parsing Rules.



2. Go to the **Template** tab and click the **Forcepoint NGFW** group folder to view the imported Token template.

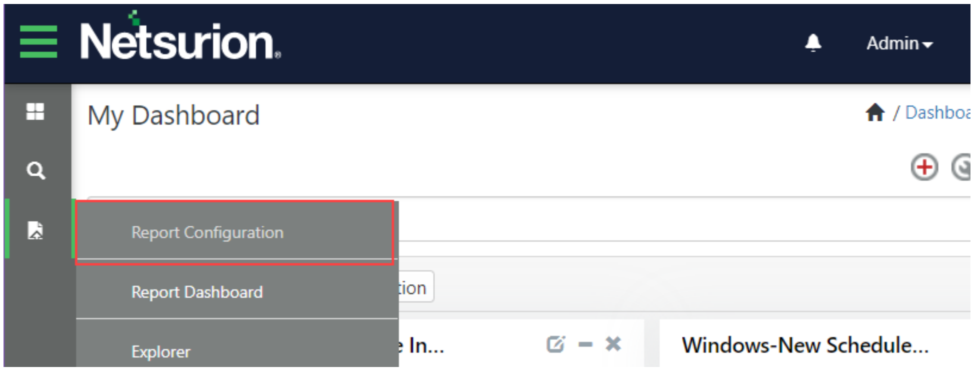


Group : Forcepoint NGFW

Template Name	Template Description	Added By	Added Date	Active	□	
Forcepoint NGFW - All events	Applies to Forcepoint NGFW v6.8.8 and above	Akash	Jan 19 06:10:13 AM	☑	□	

5.4 Reports

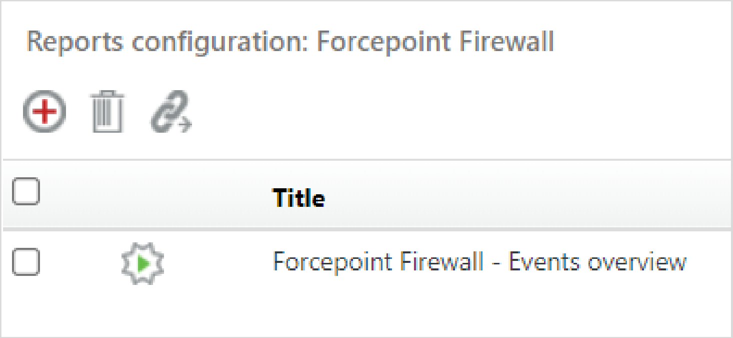
1. In the **Netsurion Open XDR platform**, click the **Reports** menu, and then click **Report Configuration**.



2. In the **Reports Configuration** interface, select the **Defined** option.

3. In the search field, type **Forcepoint NGFW** and click **Search** to search for the Forcepoint NGFW reports.

4. The Netsurion Open XDR platform displays the reports for Forcepoint NGFW.

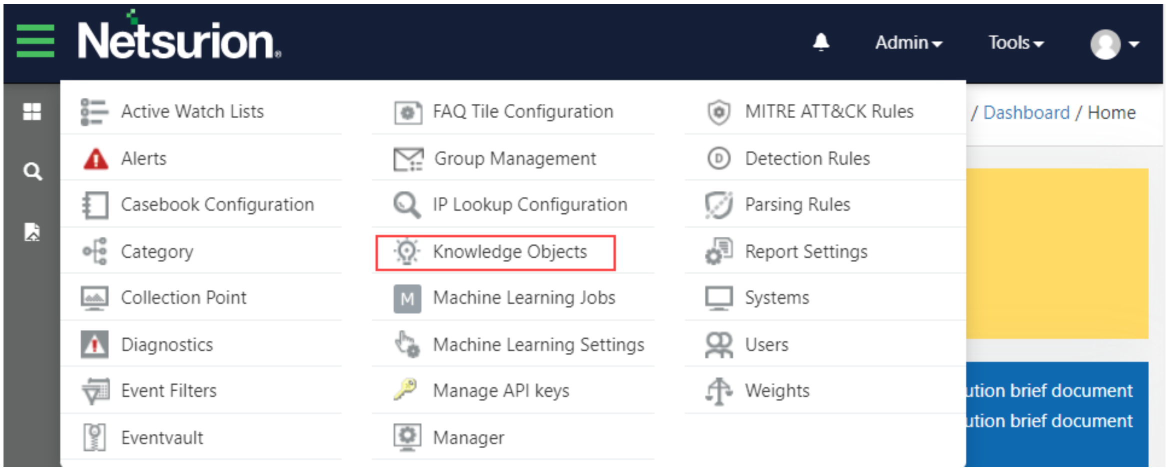


Reports configuration: Forcepoint Firewall

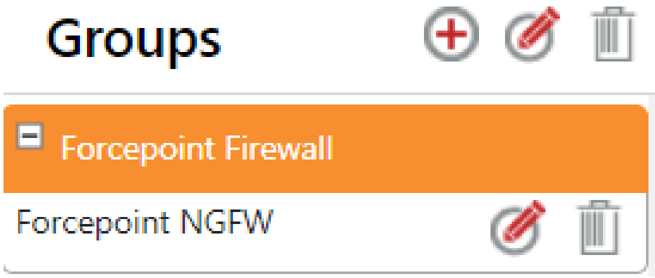
□		Title
□		Forcepoint Firewall - Events overview

5.5 Knowledge Objects (KO)

1. In the **Netsurion Open XDR platform**, hover over the **Admin** menu and click **Knowledge Objects.**



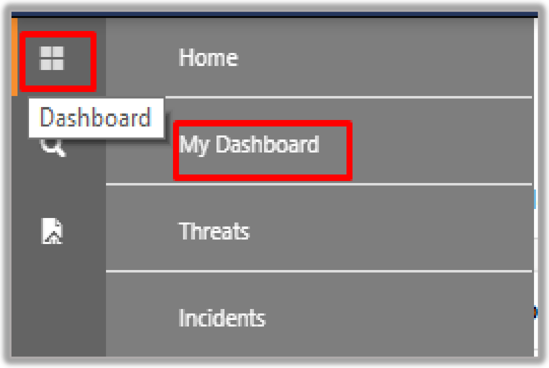
2. In the **Knowledge Object** interface, under **Groups** tree, click the **Forcepoint NGFW** group to expand and view the imported Knowledge objects.



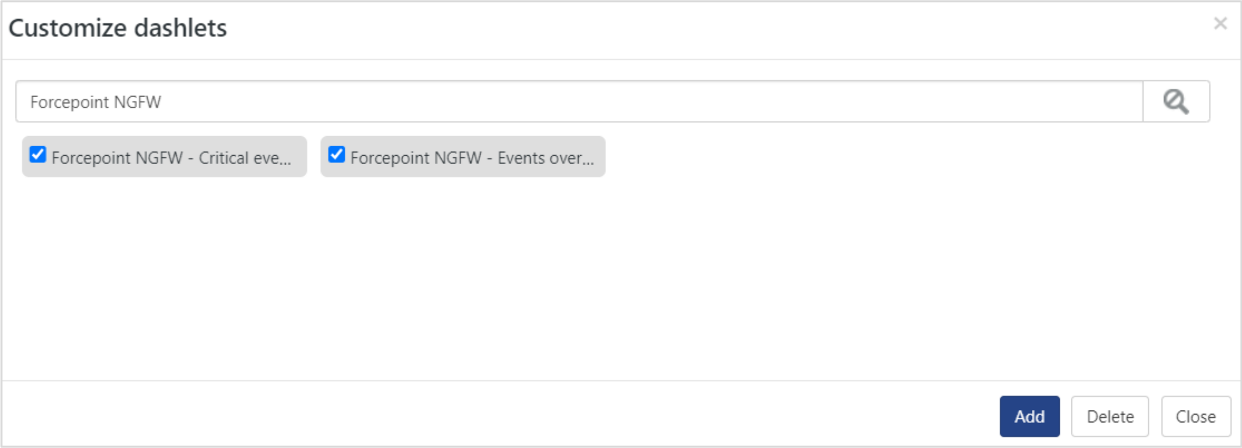
3. Click **Activate Now** to apply the imported Knowledge Objects.

5.6 Dashboard

1. In the **Netsurion Open XDR platform**, go to **Home** > **My Dashboard**, and click the **Customize dashlets** button.



2. In the **Customize dashlets** interface, search for **Forcepoint NGFW** in the search field.
3. The following Forcepoint NGFW dashlet files will get displayed.


Customize dashlets

Forcepoint NGFW

☑ Forcepoint NGFW - Critical eve...
☑ Forcepoint NGFW - Events over...

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

https://www.netsurion.com/eventtracker-support