

Integrate Zyxel Firewall

EventTracker v9.2 and later

Abstract

This guide provides instructions to retrieve the **Zyxel firewall** events by syslog. After **EventTracker** is configured to collect and parse these logs, the dashboard and reports can be configured to monitor the **Zyxel firewall**.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Zyxel firewall USG60(W), USG 310, USG110**.

Audience

Administrators who are assigned the task to monitor **Zyxel firewall** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright Zyxel firewall is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Introduction	3
2. Prerequisites	3
3. Configuring Zyxel firewall Syslog logging	3
4. EventTracker Knowledge Pack	4
4.1 Categories	5
4.2 Reports.....	5
4.3 Dashboards	6
5. Importing knowledge pack into EventTracker	8
5.1 Categories	9
5.2 Flex Reports	10
5.3 Knowledge Objects	12
5.4 Dashboards	13
6. Verifying knowledge pack in EventTracker	15
6.1 Categories	15
6.2 Flex Reports	15
6.3 Knowledge Objects	16
6.4 Dashboards	17

1. Introduction

Zyxel firewalls are next-generation firewalls designed to deliver high availability, anti-malware protection, and consolidated policy enforcement for medium to large-sized businesses and campuses.

Zyxel firewall when configured sends events to EventTracker using syslog. Zyxel Firewall sends events like antivirus scan, intrusion detection and prevention, anti-spam, anti-virus, content filtering, unified security policy, IPsec VPN, SSL VPN, and WLAN management. Generates reports on antivirus spam detail, intrusion activities, configuration changes, interface statistics, traffic denied, etc. It contains username, client IP address, status, message, action, file path, file name, and hash. Graphically displays interface statistics, traffic denied by reason, traffic denied by IP address, threat detected by file name, device name, device IP, etc.

2. Prerequisites

- Administrative access on Zyxel firewall Console.
- EventTracker manager IP address.
- Allow port number 514 from the firewall end.

3. Configuring Zyxel firewall Syslog logging

1. Log into the Zyxel Web Interface.
2. Navigate to **Configuration > Log & Report > Log Settings**.

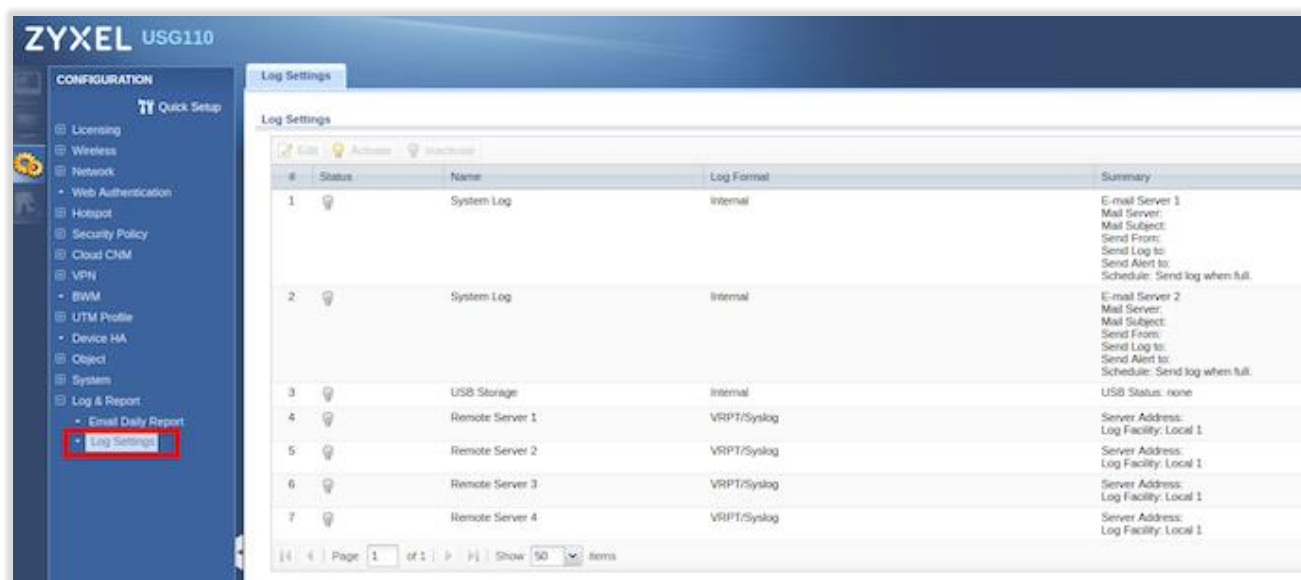


Figure 1

3. Choose a **Remote Server**.
4. Click **Active**.
5. Choose Log Format as **VRPT/Syslog**.
6. Enter the IP address of the **EventTracker**.
7. Select **Local 7** in the **Log Facility** field.
8. Select the **Categories** you want to be logged (normal = default logs, debug = very detailed logs, disable = no logs)

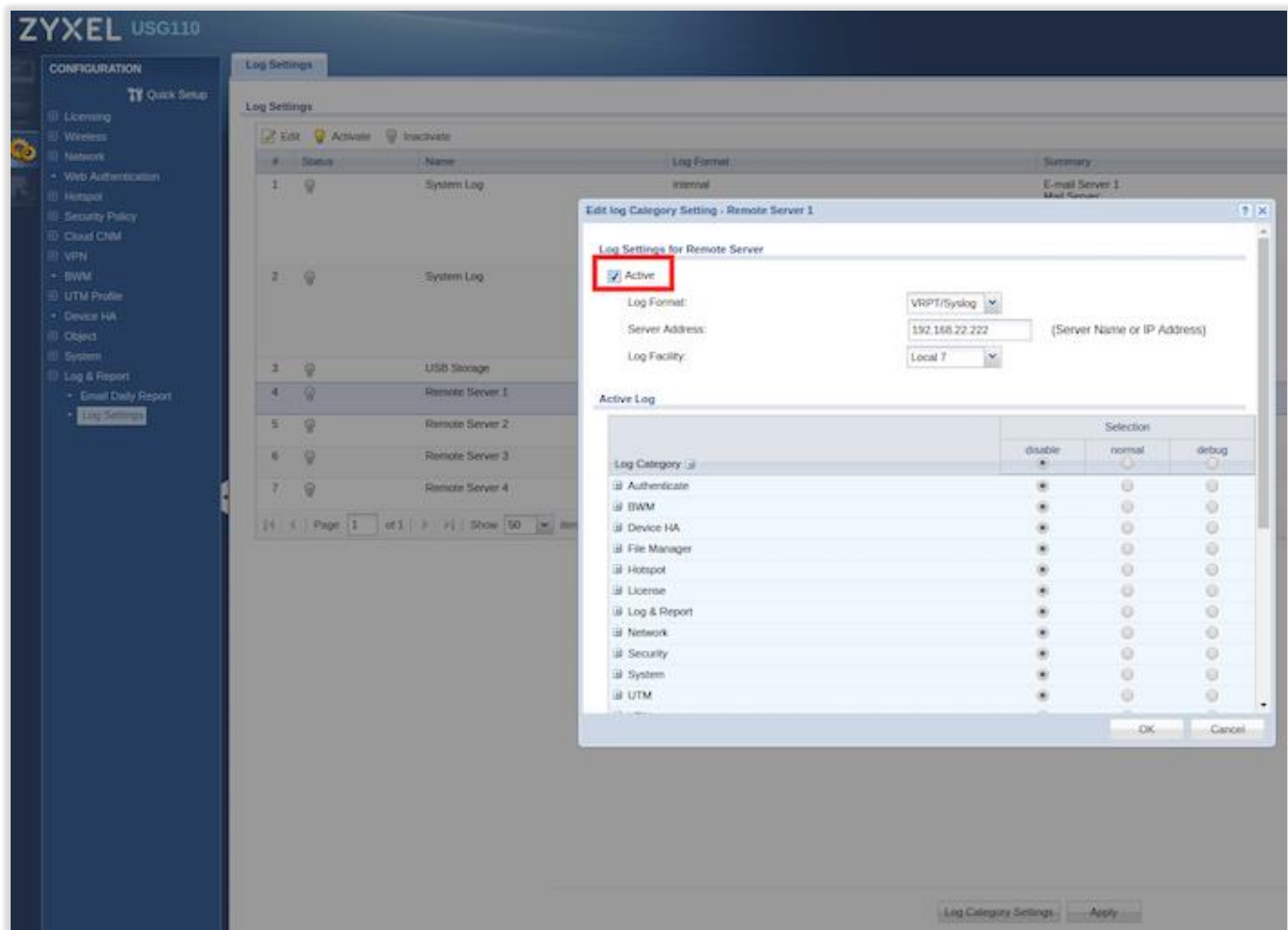


Figure 2

4. EventTracker Knowledge Pack

Once Zyxel firewall events are enabled and Zyxel firewall events are received in EventTracker, alerts and reports can be configured in EventTracker.

The following knowledge packs are available in EventTracker to support Zyxel firewall monitoring.

4.1 Categories

- **Zyxel Firewall: Traffic activities** – This category provides events information related to traffic denied and allowed.
- **Zyxel Firewall: Interface activities** – This category provides events information related to interface statistics like down, active, and inactive.

4.2 Reports

- **Zyxel Firewall – Interface activities** - This report provides information related to interface down, inactive, and active. It provides information like interface port address, packets sent, packets received, device ID, and port status.

Log_Sample

```
Jan 06 12:27:29 Zyxel_Firewall Computer:Zyxel_Firewall, Dec 10 11:08:52 10.10.140.6 Dec 10 11:08:52 2020
FEDC-FWL02 src="0.0.0.0" dst="0.0.0.0"
msg="name=Port1,status=1000M/Full,TxPkts=737059398,RxPkts=1251804984,Colli.=0,TxB/s=94,RxB/s=0,UpTi
me=29292.07:26" note="INTERFACE STATISTICS" user="unknown" devID="107befd06ce6" cat="INTERFACE
STATISTICS"
```

Sample_Report

LogTime	Computer	Device ID	Interface	Status	Packets Sent	Received Packets
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P4_Empty	Inactive	0	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P5_EuroFibr	1000M/Full	33056619092	23795609027
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P4_Empty	Inactive	0	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P3_Managmnt	1000M/Full	5	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P2_Empty	Inactive	0	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	Port6	1000M/Full	537143631	907017725
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	Port4	Down	0	0

Figure 3

- **Zyxel firewall – Traffic denied** – This report provides information related to suspicious traffic denied. It provides information like username, source IP, source port, destination IP, destination port, direction, and reason.

Log_Sample

```
Jan 06 12:27:22 Zyxel_Firewall Computer:Zyxel_Firewall, Dec 10 10:01:53 192.168.101.20 Dec 10 11:01:43 2020
EUDC-ZW310-43L47 src="192.168.8.5:50251" dst="192.168.100.66:8530" msg="Match default rule, DROP"
note="ACCESS BLOCK" user="kenneth" devID="ec43f6fea270" cat="Security Policy Control" class="Access
Control" ob="0" ob_mac="000000000000" dir="ANY:ANY" protoID=6 proto="others"
```

Sample_Report

LogTime	Computer	Device ID	Source IP Address	Source Port	Destination IP Address	Destination Port	Direction	Reason
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.1617.1	52128	192.16.100.50	8080	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.16.17.1	52124	192.16.100.50	8080	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.16.15.5	65387	192.16.100.200	23560	ANY:ANY	abnormal TCP flag attack detected, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.168.15.5	65387	192.168.100.200	23560	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	124.156.245.159	47603	192.168.10.186	5000	ANY:ANY	Match default rule, DNAT Packet, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.241.235.192	56845	194.247.63.253	50070	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	113.187.206.71	64988	89.20.164.162	445	ANY:ANY	Abnormal TCP flag attack detected, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	194.247.42.220	58927	194.247.63.253	445	ANY:ANY	Match default rule, DROP

Figure 4

4.3 Dashboards

- Zyxel Firewall - Interface status**

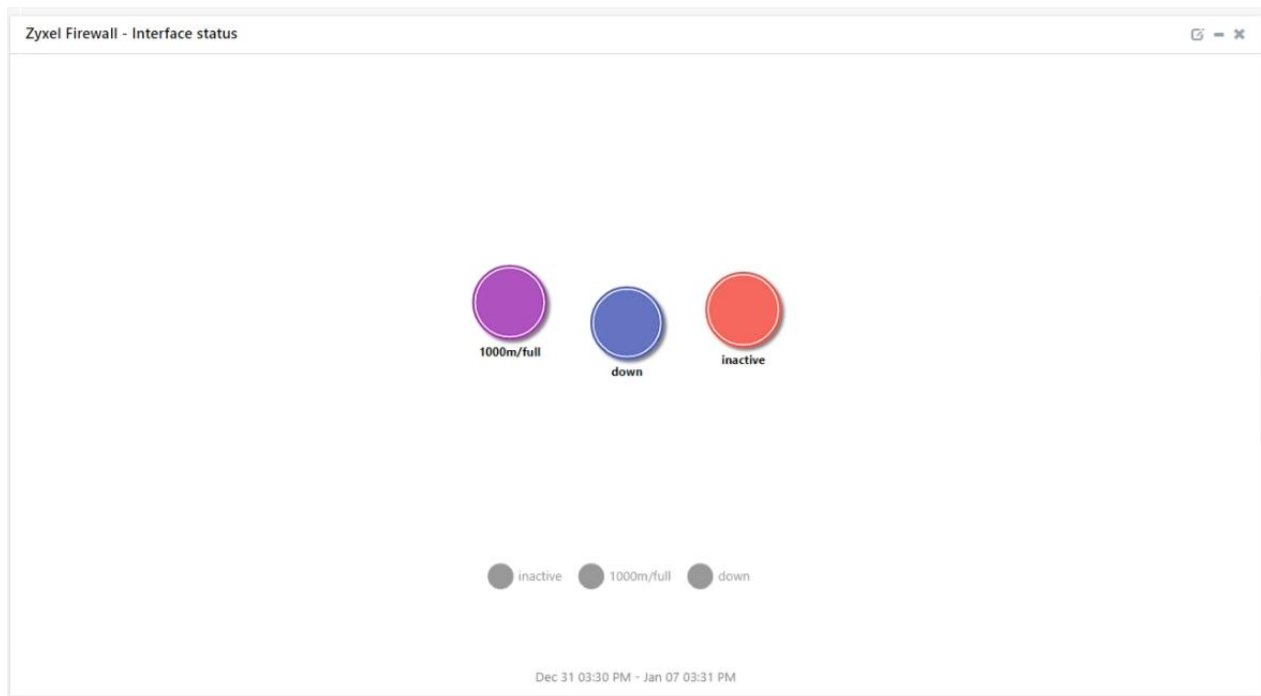


Figure 5

- **Zyxel Firewall - Traffic denied by reason**

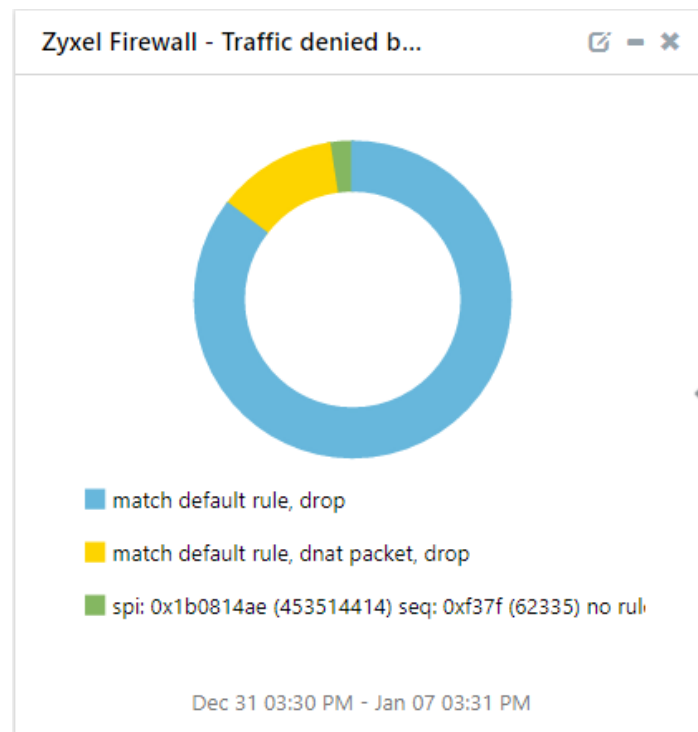


Figure 6

- **Zyxel Firewall - Traffic denied by destination IP**

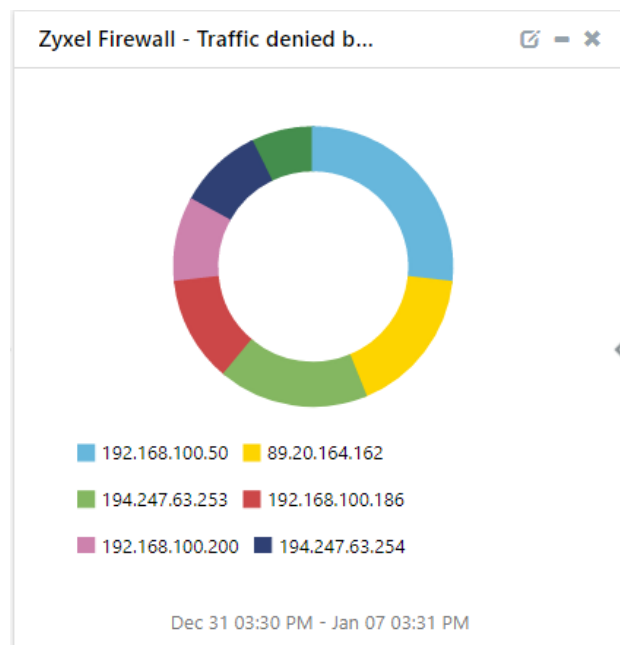


Figure 7

- **Zyxel Firewall - Traffic denied by Source IP**

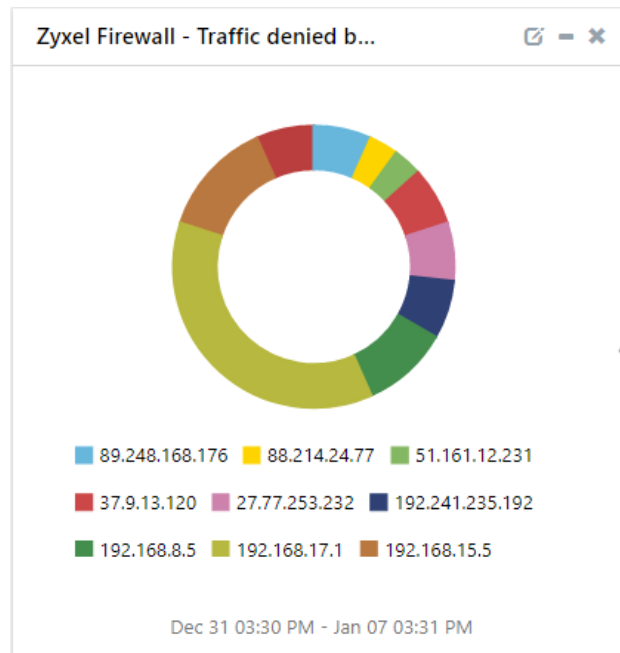


Figure 8

5. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
 - Alerts
 - Flex Reports
 - Knowledge Objects
 - Dashboards
1. Launch the **EventTracker Control Panel**.
 2. Double click **Export-Import Utility**.

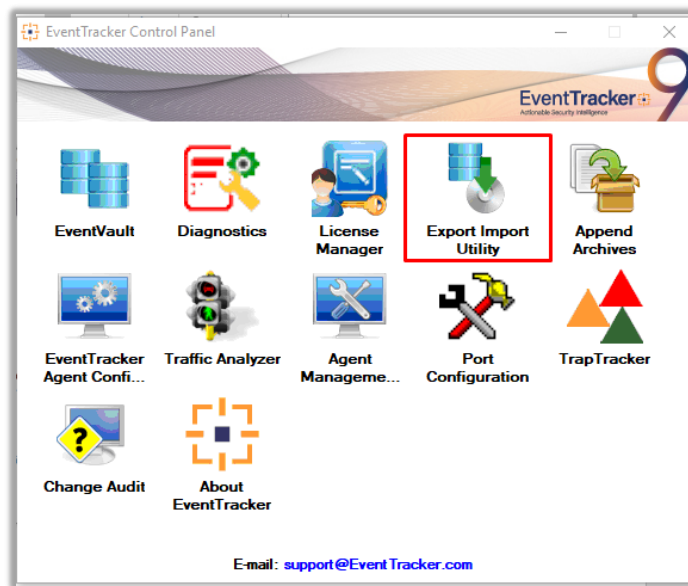


Figure 9

Export-Import Utility window opens.

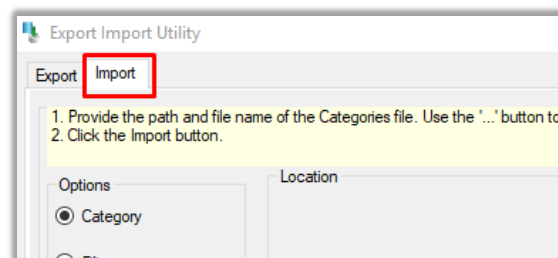



Figure 10

3. Click the **Import** tab.

5.1 Categories

1. In **Export-Import Utility** window, select the **Category** option, and click **Browse** .
2. Navigate to the knowledge pack folder and select the file with the extension **.iscat**, like **"Categories_Zyxel firewall. iscat"** and click **Import**.

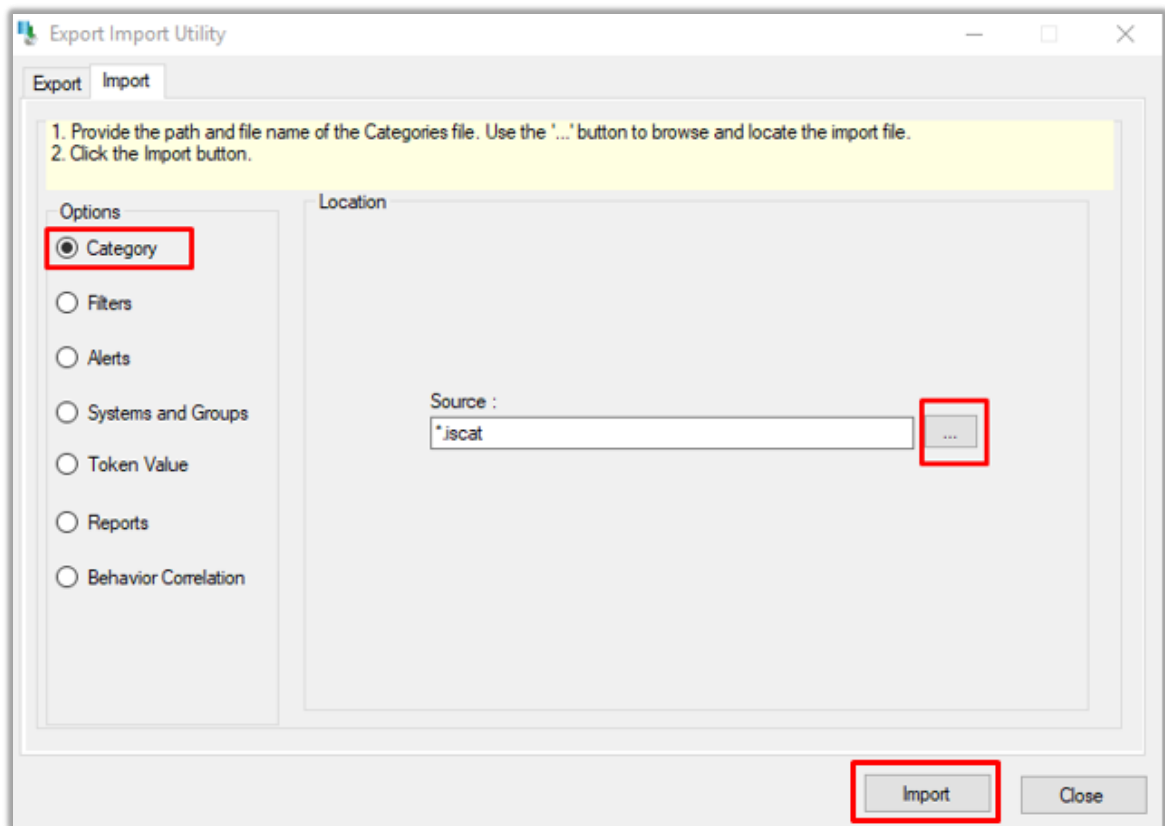


Figure 11

EventTracker displays a success message.

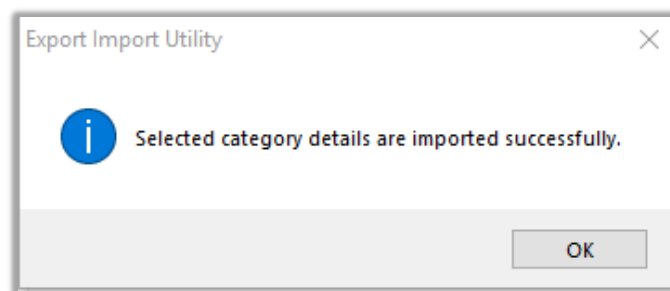


Figure 12

5.2 Flex Reports

1. In **Export-Import Utility** window, select the **Import** tab. Click the **Reports** option, and choose **New (*.etcrx)**.

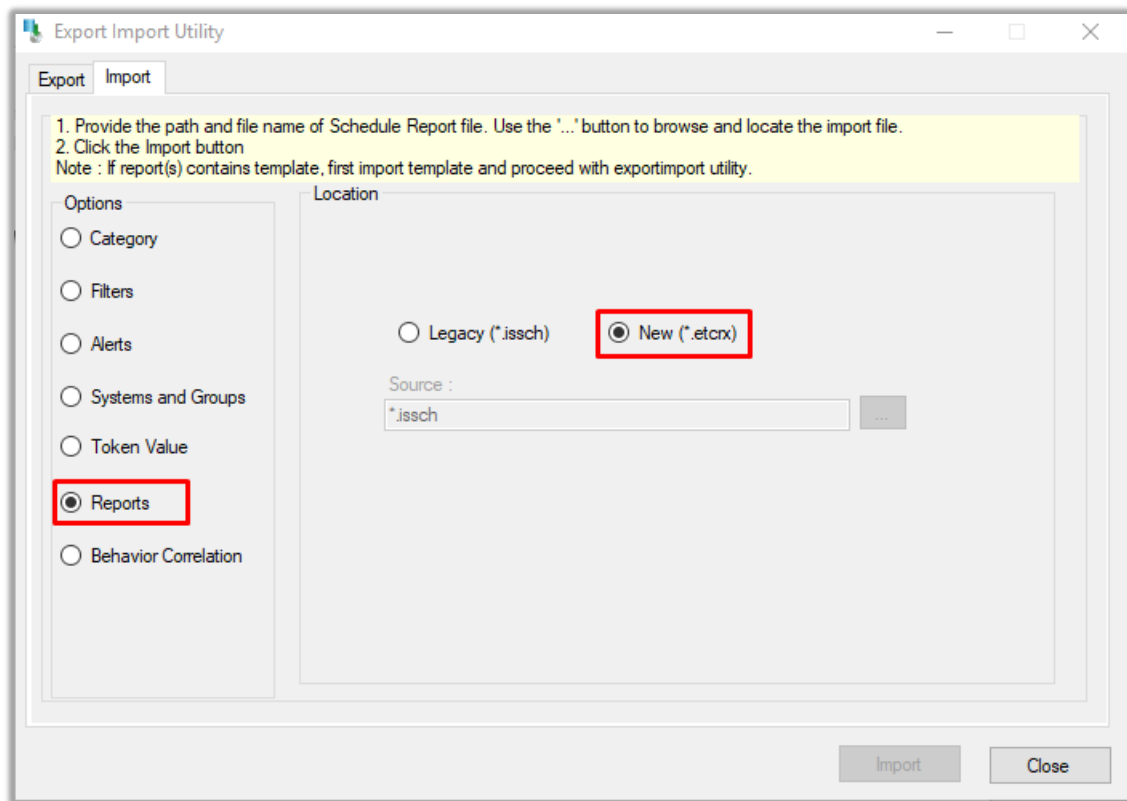


Figure 13

2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension **.etcrx**, e.g. **Reports_Zyxel firewall.etcrx**.

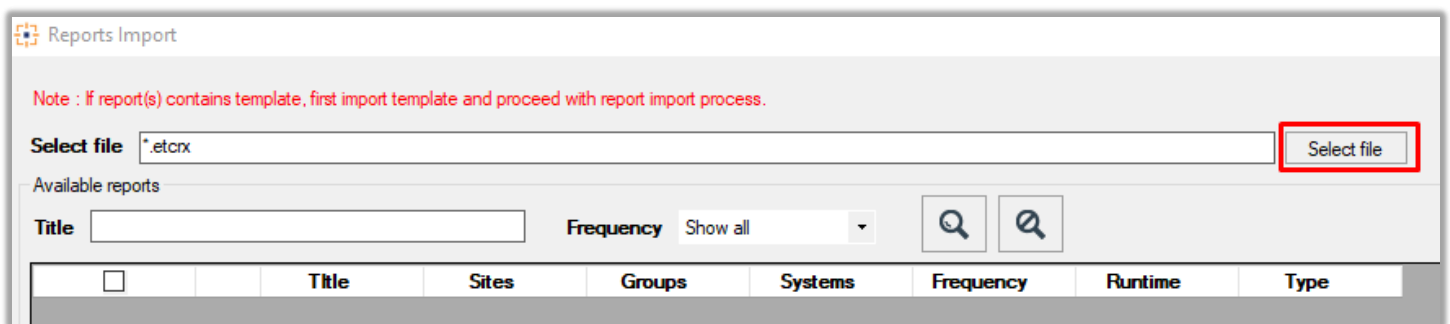



Figure 14

3. Wait while reports populate. Select all the relevant reports and click **Import**  .

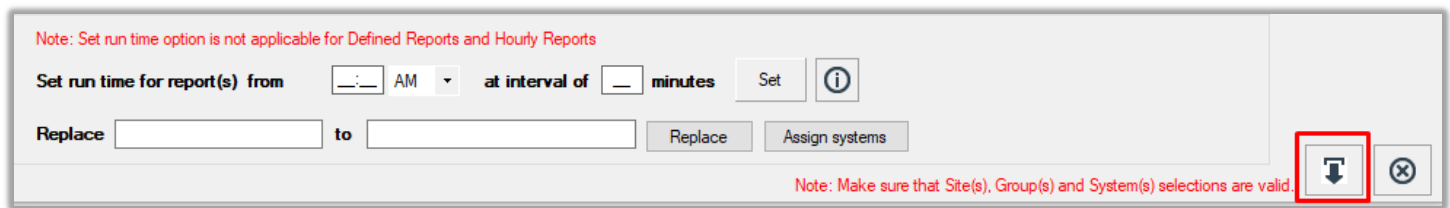


Figure 15

EventTracker displays a success message.

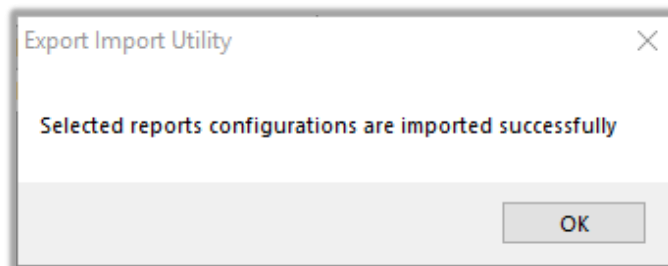


Figure 16

5.3 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

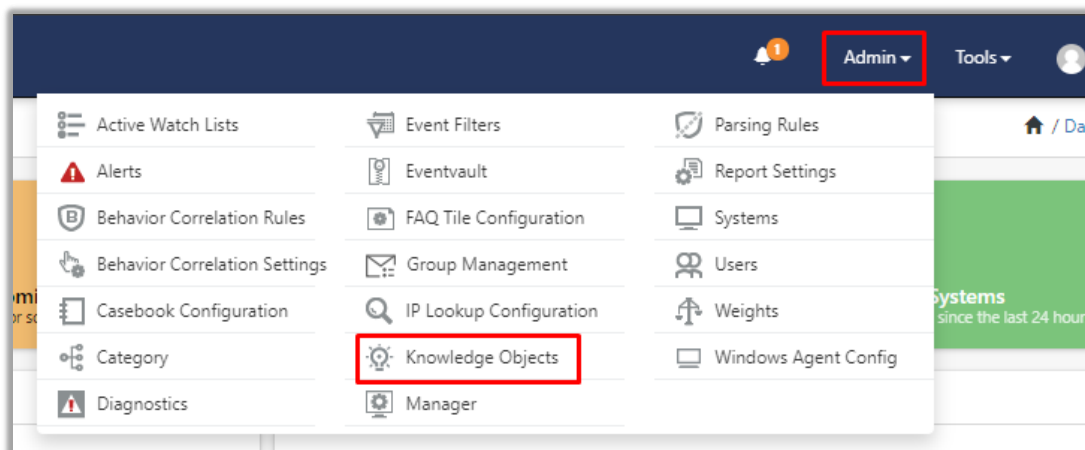


Figure 17

2. Click the **import object** icon.

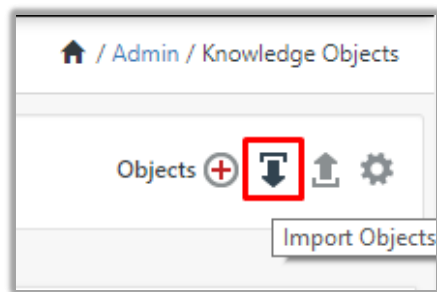


Figure 18

3. A pop-up box appears, click **"Browse"** and navigate to the knowledge packs folder (type **"C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs"** in the navigation bar) with the extension **".etko"**, e.g. **"KO_Zyxel firewall.etko"** and click **"Upload"**.



Figure 19

4. Wait while EventTracker populates all the relevant knowledge objects. After the objects display, select the required ones, and click **Import**.



Figure 20

5.4 Dashboards

1. Login to the **EventTracker** web interface.
2. Navigate to **Dashboard → My Dashboard**.
3. In **My Dashboard**, Click the **Import** button.

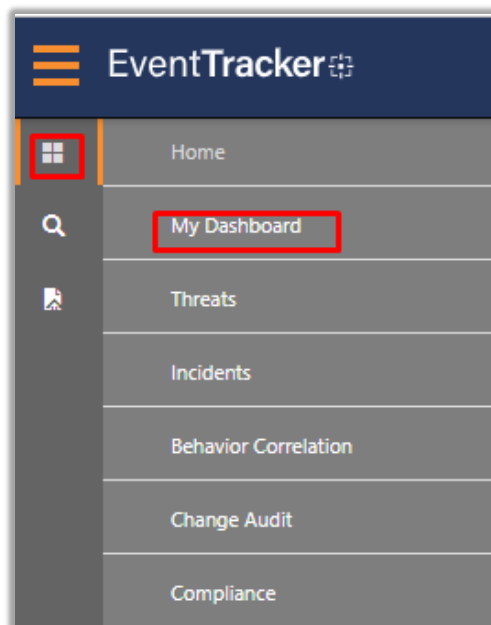


Figure 21

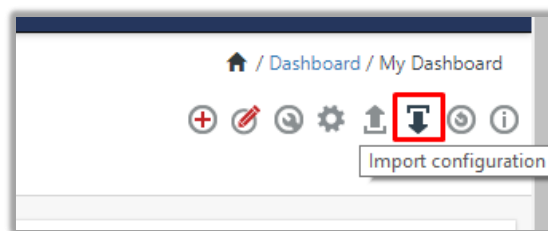


Figure 22

4. Click **Browse** and navigate to the knowledge pack folder (type **C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs** in the navigation bar) where **.etwd**, e.g. **Dashboard_Zyxel firewall.etwd** is saved and click “**Upload**”.
5. Wait while EventTracker populates all the available dashboards. Enable **Select All** and click **Import**.

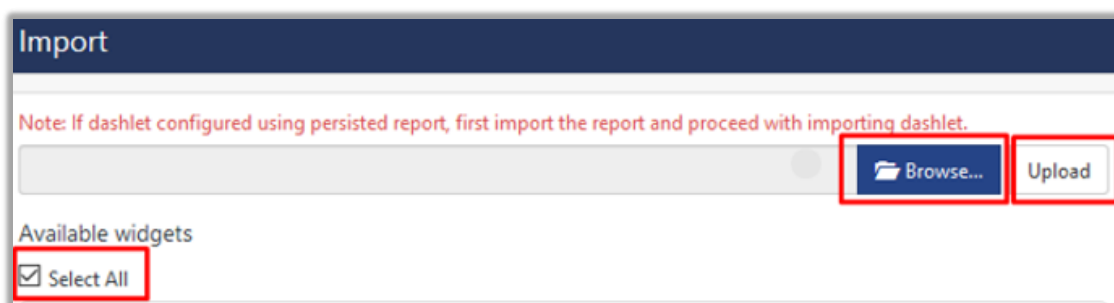


Figure 23

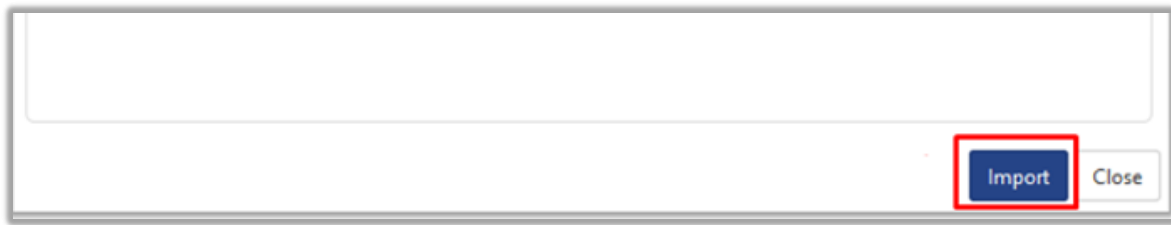


Figure 24

6. Verifying knowledge pack in EventTracker

6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown and click **Categories**.
3. In **Category Tree** to view imported categories, click the **Search** tab and enter **Zyxel firewall** in the search.

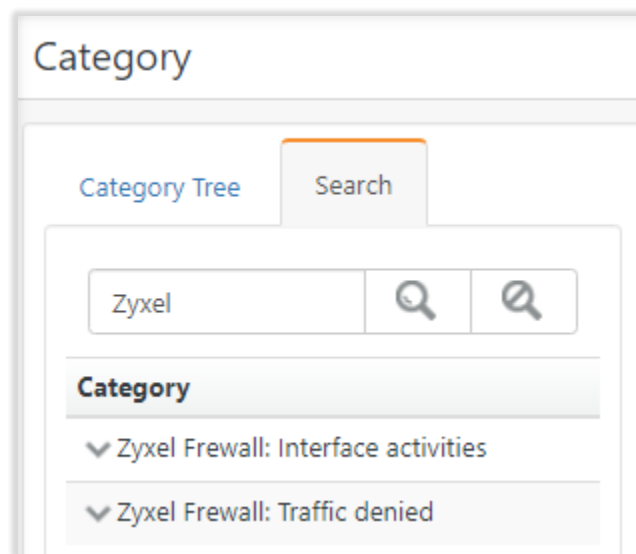


Figure 25

6.2 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.

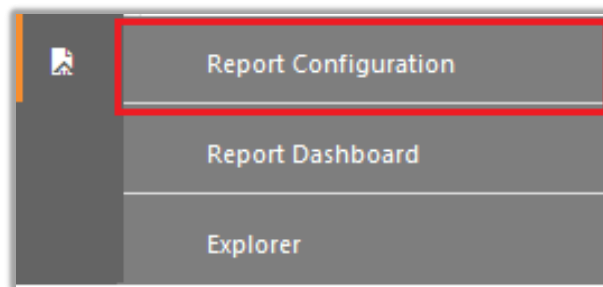


Figure 26

2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Zyxel firewall** group folder to view the imported reports.

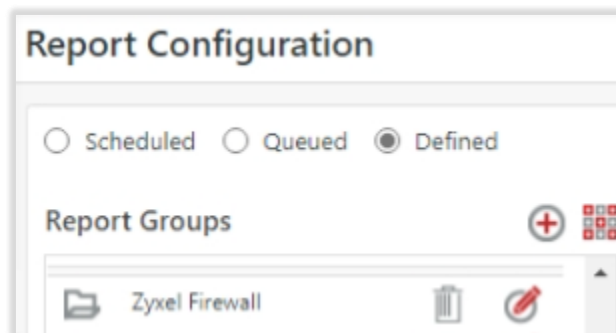


Figure 27

6.3 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.
2. In the **Knowledge Object** tree, expand the **Zyxel firewall** group folder to view the imported Knowledge objects.

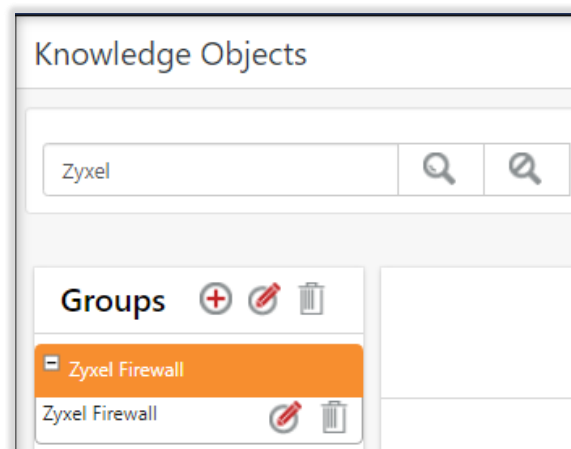


Figure 28

6.4 Dashboards

1. In the EventTracker web interface, Click **Home**  and select “**My Dashboard**”.

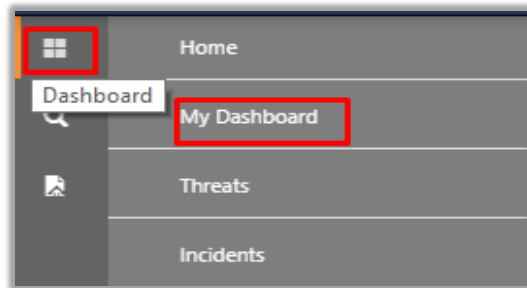


Figure 29

2. In the **Zyxel firewall** dashboard the following screen appears.

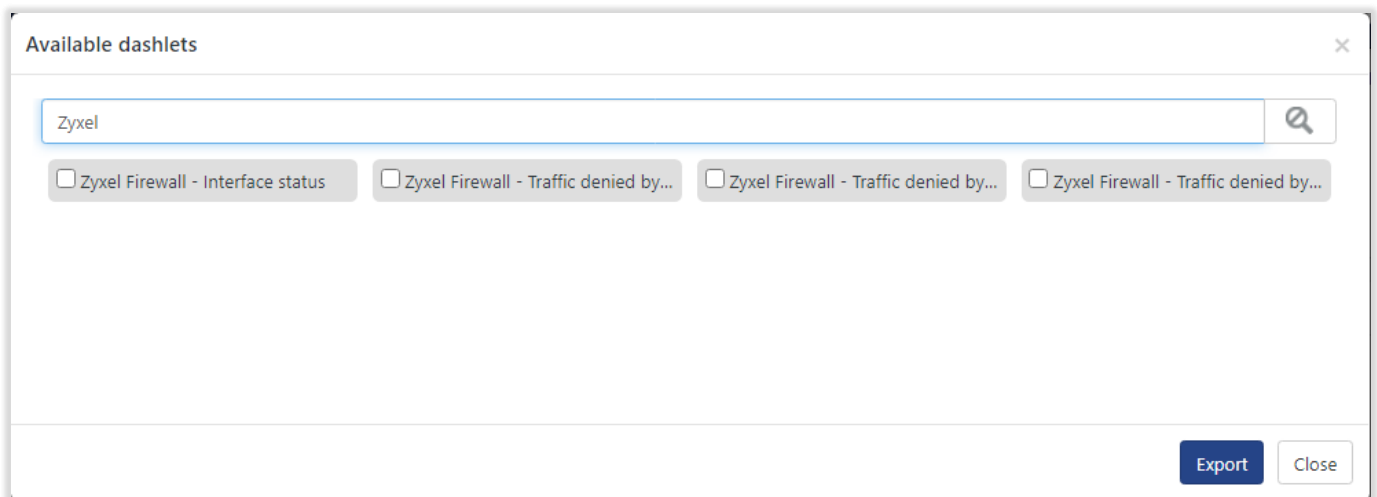


Figure 30