Netsurion™ | EventTracker

Integrate ForeScout CounterAct

EventTracker v9.0 and Above

Publication Date: July 4, 2019

Abstract

This guide provides instructions to configure ForeScout CounterAct to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor the network access control.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and ForeScout CounterAct v8.0.

Audience

IT Admins, ForeScout CounterAct administrator, and EventTracker users who wish to forward logs to EventTracker and monitor events using EventTracker.

Table of Contents

Overview

ForeScout CounterAct gives you network access control. It maintains the policies and network configuration and deploys them to the ForeScout CounterACT appliances.

ForeScout CounterAct can be integrated with EventTracker using syslog. With the help of ForeScout CounterAct KP items, we can monitor the network access control activities, malicious process and mail infection on applications and also trigger the alert whenever any malicious process is running, and mail infection is detected. EventTracker dashboard will help you to visualize the web activities on applications. It can even create a report that helps to collect user activities happening in the applications for a time interval. This will help you to review the different malicious and network activities. EventTracker CIM will help you to correlate from network access control activities, malicious process, and mail infection, etc.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **ForeScout CounterAct v8.0** or latest version should be installed.
- **ForeScout CounterAct core extension module Syslog plugin v3.5** should be installed**.**

Configuring ForeScout CounterAct syslog

Syslog plugin Configuration

This section describes how to configure the syslog plugin. There are two types of messages that you can send to syslog:

- Sending ForeScout event messages.
- Using actions to send endpoint messages.

Sending ForeScout event messages

Select an Appliance to Configure

This section describes how to configure the plugin to ensure that the CounterACT device can properly communicate with syslog servers.

Configuring the syslog plugin

1. In the Modules pane, select **Core Extensions >Syslog** and then select **Appliances**. The syslog - Appliances installed dialog box opens.

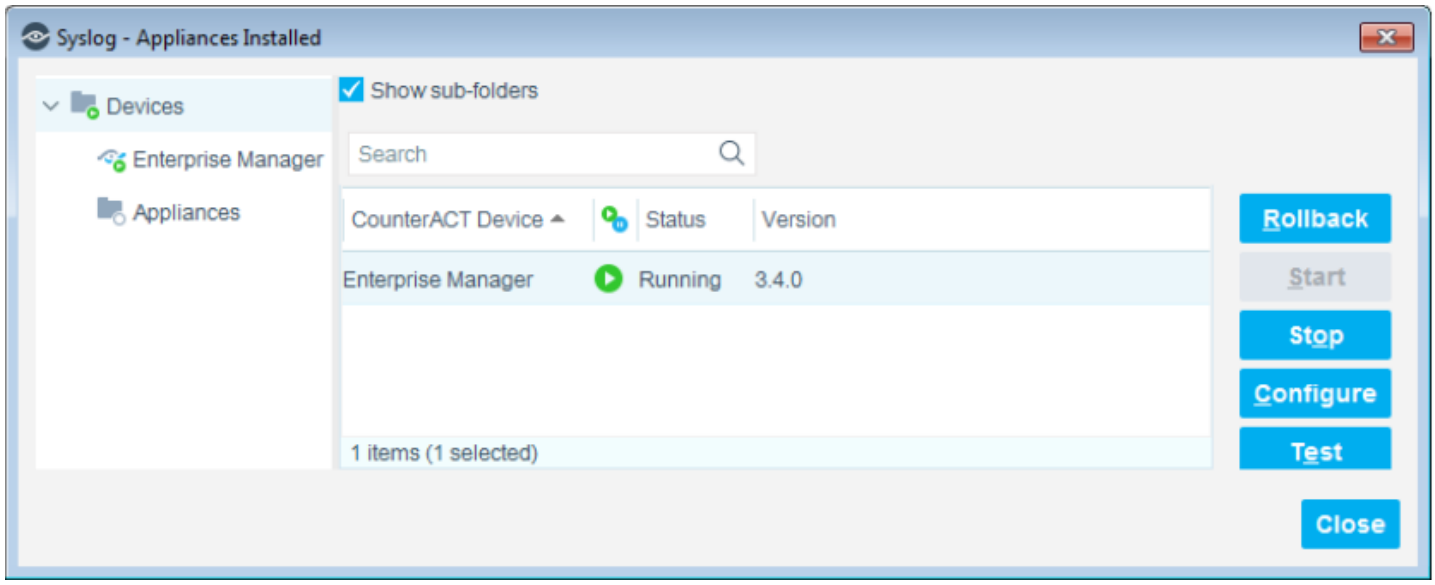

Figure 1

2. Select any appliance or the **Enterprise Manager** and select **Configure**. You cannot configure multiple CounterACT devices simultaneously. The Configuration dialog box opens. Need to configure send events to, syslog triggers, default action configuration for sending logs to the EventTracker.

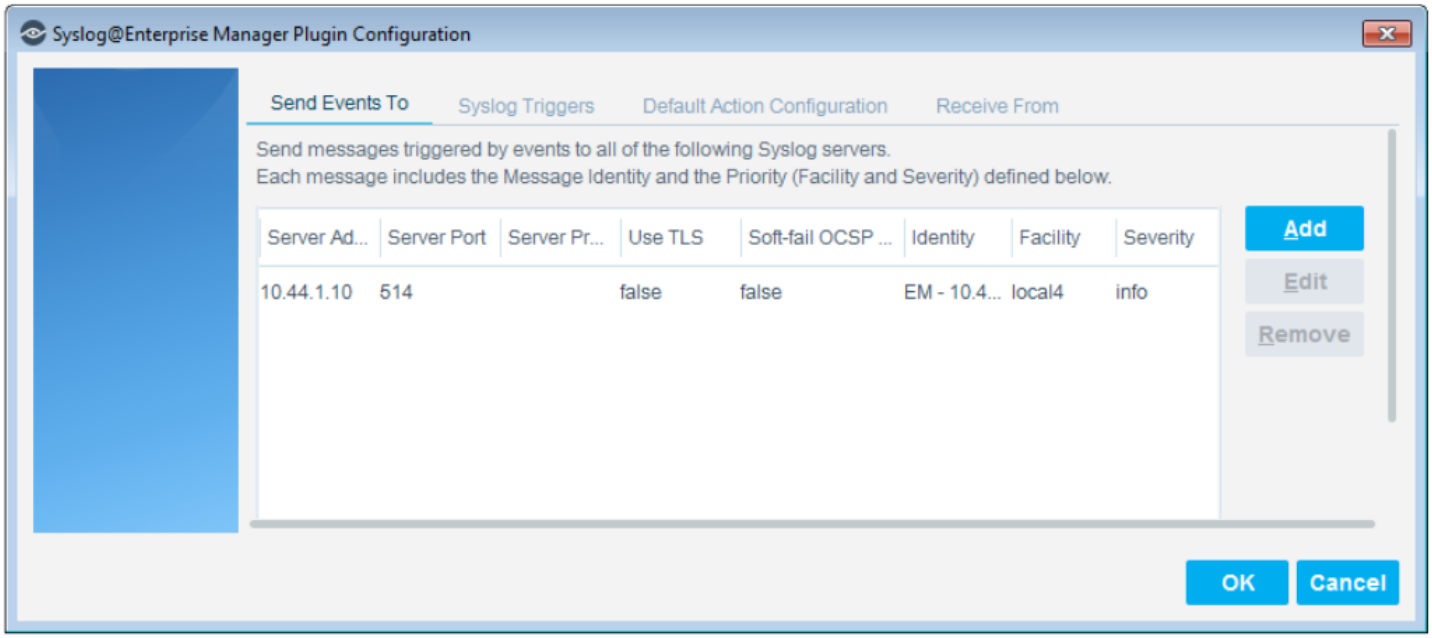

Figure 2

3. When the configuration is complete, select **ok**.

Send Events To

The **Send Events To** tab lists the syslog servers to which the CounterACT device will send messages regarding the event types selected in the syslog triggers tab. For each syslog server, define:

1. In the **Send Events Total**, do one of the following:
   - To define a syslog server not in the table, select **Add**.

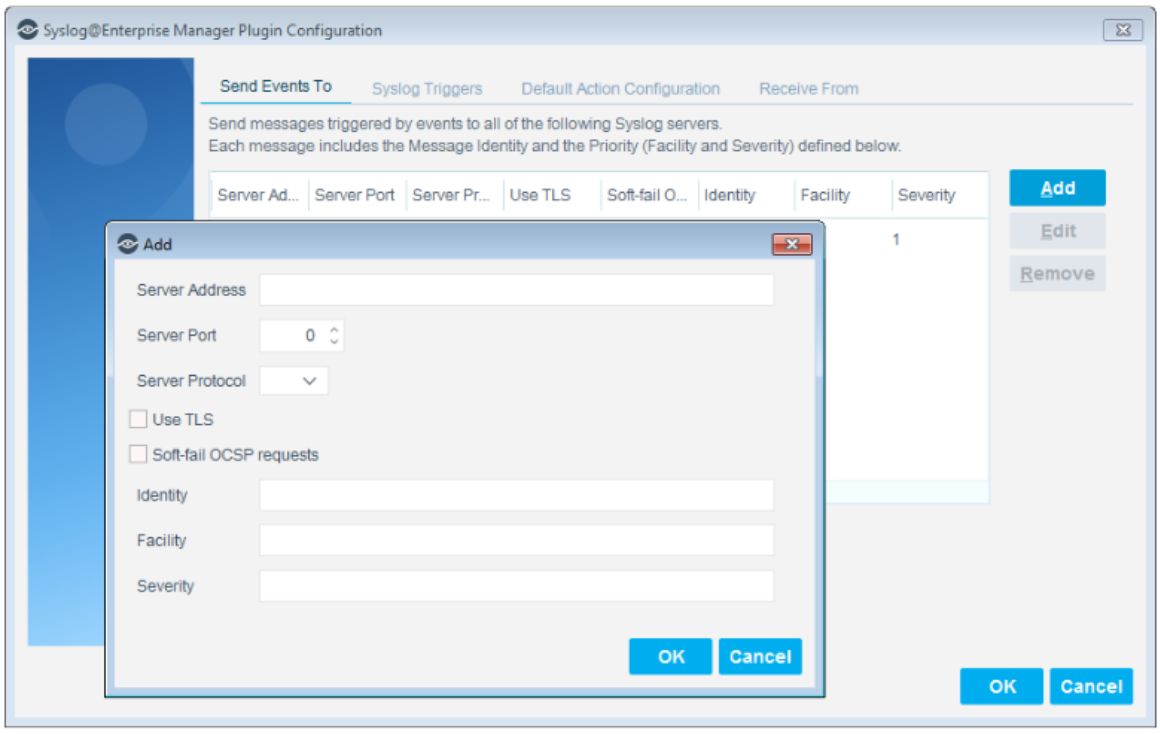

Figure 3

   - To modify the definition of an existing server, select it in the table and select **Edit**.

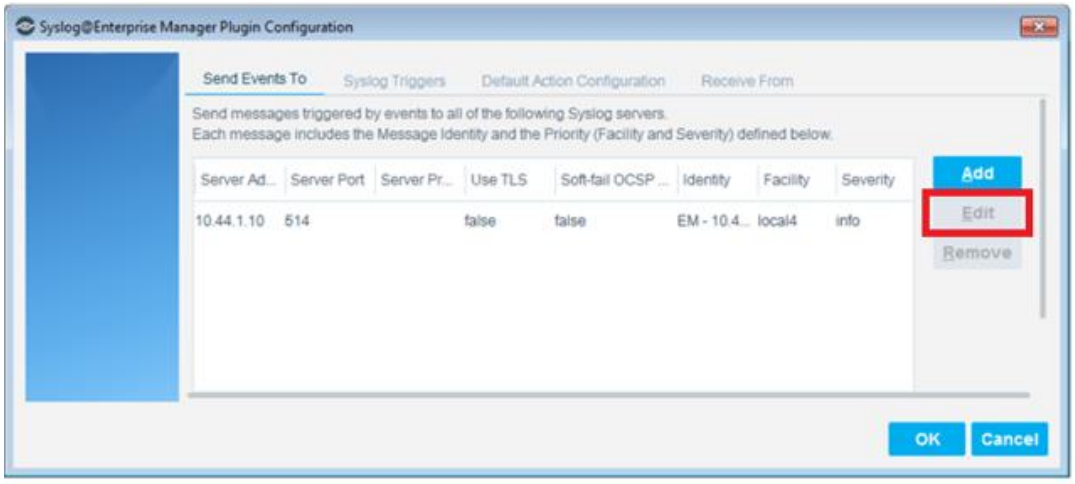

Figure 4

2. Specify the following information for the server:
   - **Server Address**: Provide EventTracker installed host IP address.
   - **Server Port**: Provide syslog (default 514) port.
   - **Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this syslog server.
   - **Identity**: Free-text field for identifying the syslog message.
   - **Facility**: (Optional) Syslog message facility that is transmitted as part of the message Priority field. If the facility value is not mentioned, it is set to **local5**.
   - **Severity**: Mention severity as **Info.**
3. Select OK. The updated server definition appears in the table.

Syslog Triggers

Configure the settings in the syslog triggers tab.

Syslog messages can be generated by Forescout platform policies when endpoints meet conditional criteria.

1. Select "**Include timestamp and CounterACT device identifier in all messages".**

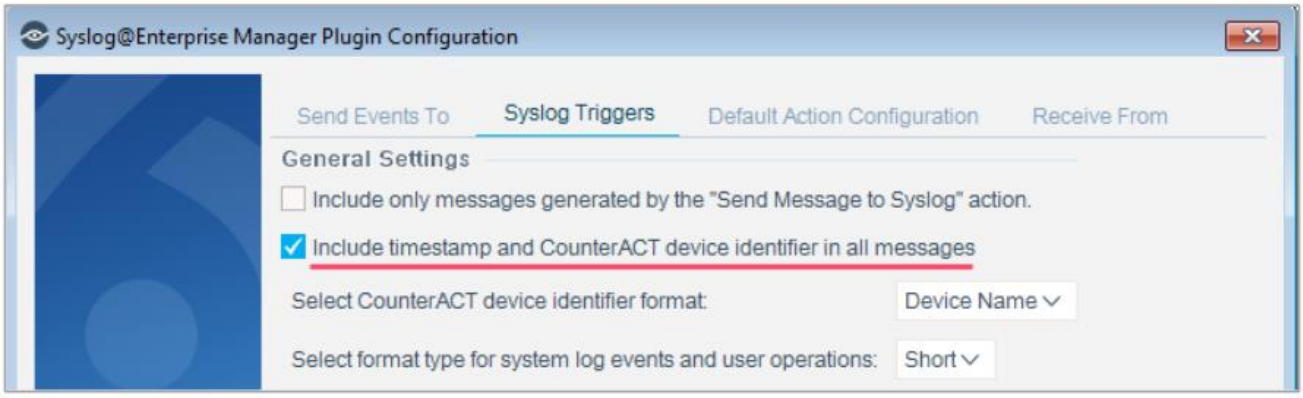

Figure 5

2. Select options in the tab to define which event types trigger syslog messages. Follow below screenshot and click ok.

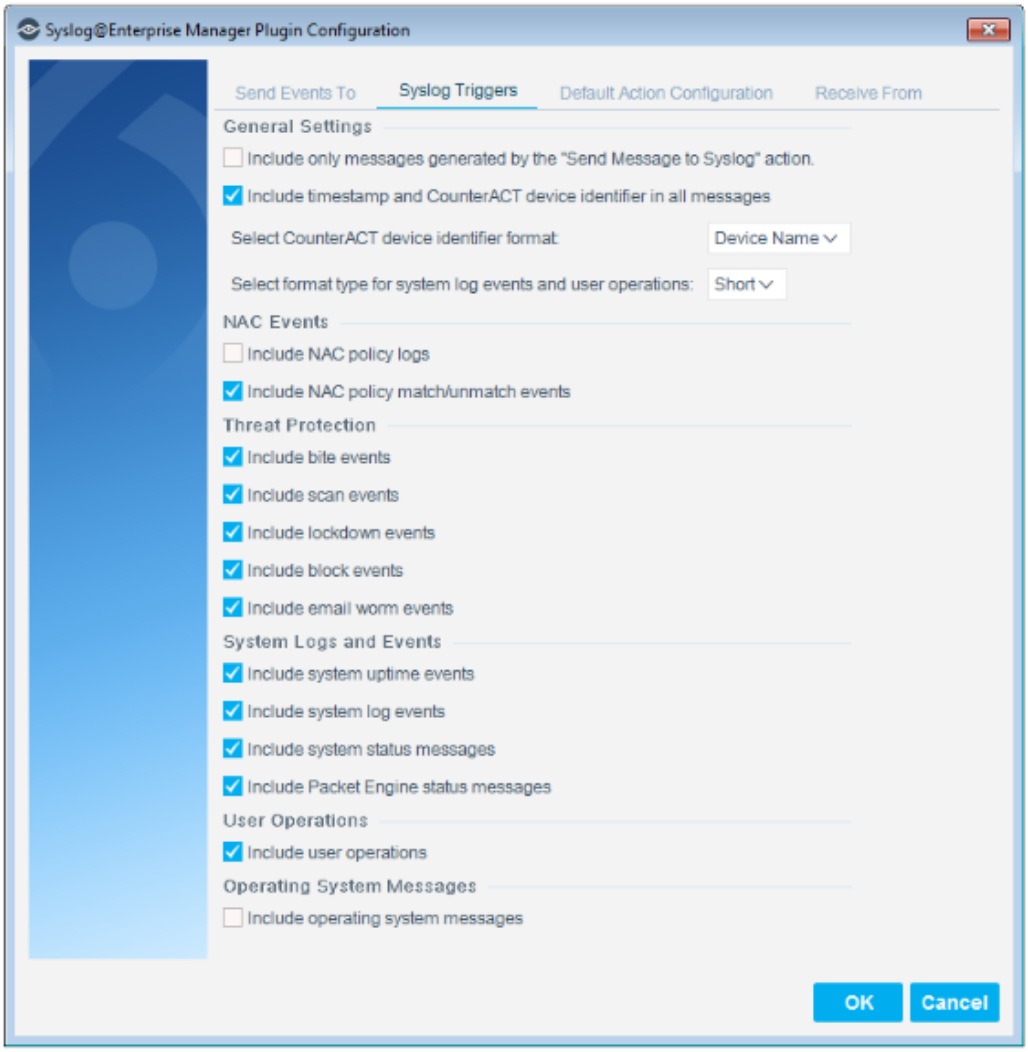

Figure 6

Default Action Configuration

The Default Action Configuration tab allows you to define default values for the **Send Message** to syslog action parameters. These default values are applied to parameters that are not defined in policies. View Send Message to syslog action for details.

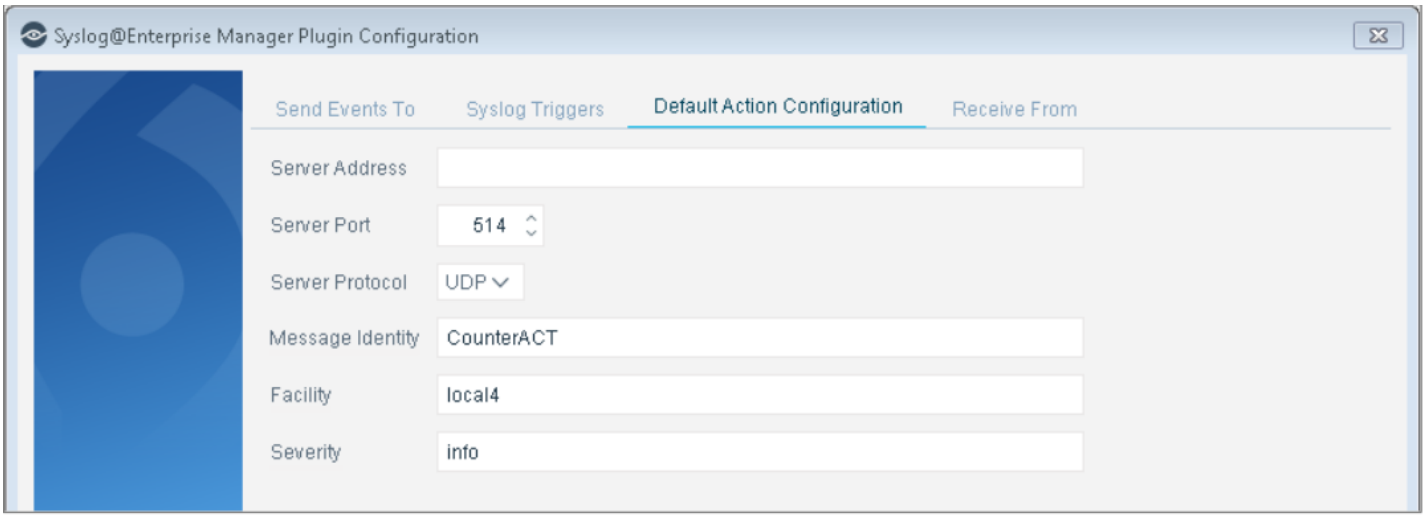

Figure 7

Specify the following values:

1. **Server Address**: Mention EventTracker installed host IP address.
2. **Server Port**: Mention syslog server(default 514) port.
3. **Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this server.
4. **Message Identity**: Free-text field for identifying the syslog message.
5. **Facility**: (Optional) Syslog message facility that is transmitted as part of the message priority field. If the facility value is not mentioned, it is set to **local5**.
6. **Severity**: Mention severity as **Info.**

Using actions to send endpoint messages

Send Message to syslog

The Send Message to syslog action is used by the syslog plugin to send a message to the syslog server. This message overrides syslog plugin configuration options.

1. In the **Policy Manager**, select a policy and select **Edit**. The **Policy Properties** dialog box opens.
2. Next to the **Main Rule** section select **Edit**. The Policy Conditions dialog box opens.
3. Next to the **Actions** section select **Add**. The Action dialog box opens.
4. In the left pane expand the Audit folder.
5. Select **Send Message to syslog**.

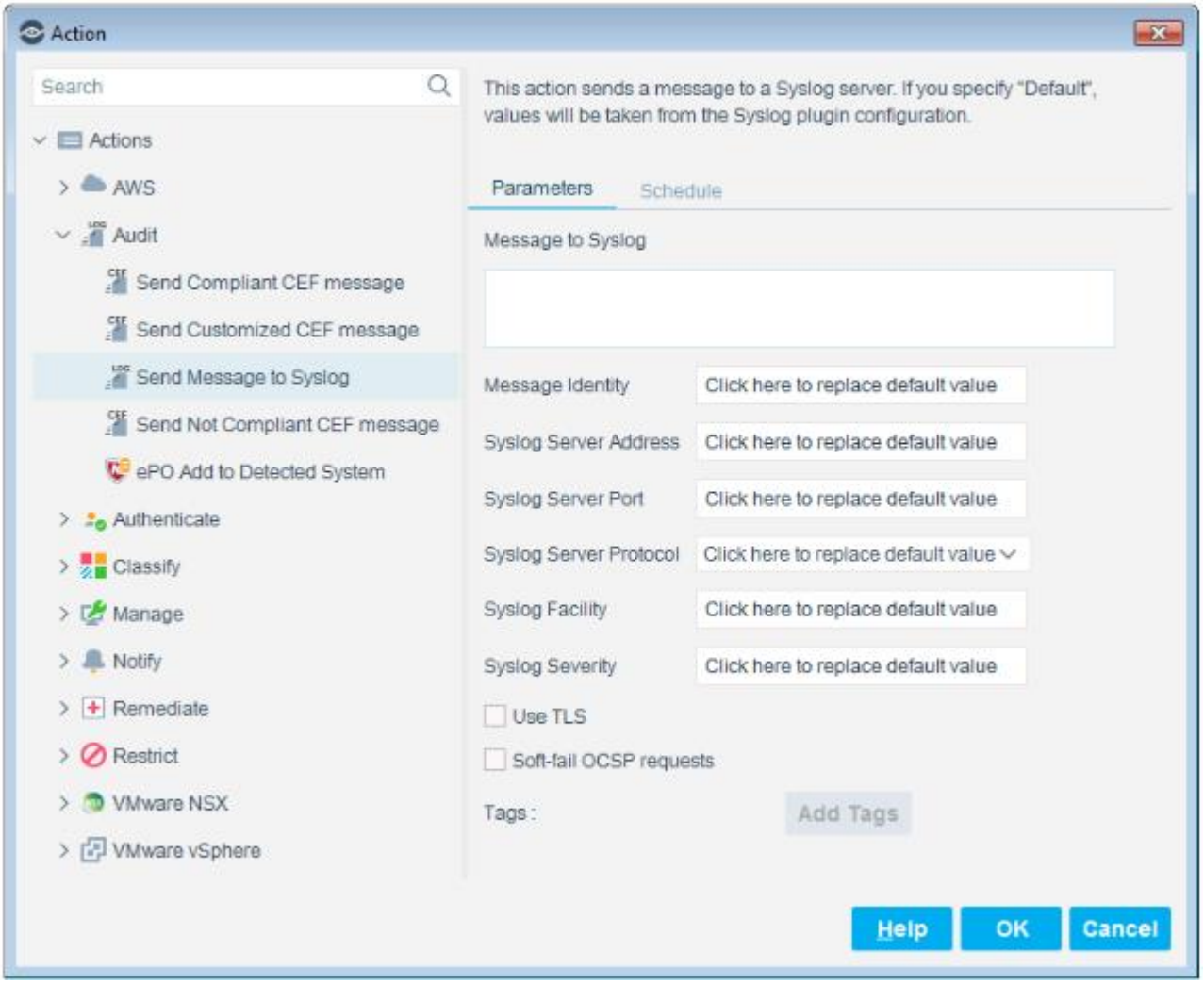

Figure 8

6. Specify the following or use **Default** where applicable to apply the default configuration.

   - **Message to syslog**: Type a message to send to the syslog server when the policy is triggered.
   - **Message Identity**: Free-text field for identifying the syslog message.
   - **Syslog Server Address**: Provide EventTracker installed host IP address.
   - **Syslog Server Port**: Set syslog port number (default is 514).
   - **Syslog Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this server.
   - **Syslog Facility:** (Optional) Syslog message facility that is transmitted as part of the message Priority field. If the facility value is not mentioned, it is set to **local**.
   - **Syslog Priority:** Mention severity as **Info.**
   - **Tags:** Mention tag as ForeScout CounterAct.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; alert, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v9.x and later to support ForeScout CounterAct.

Alert

- **ForeScout CounterAct: Blocked events –** This alert will trigger whenever the IP addresses and ports are blocked.
- **ForeScout CounterAct: Mail infection detected -** This alert will trigger whenever an infection is found in the email attachments.

Reports

- **ForeScout CounterAct – Blocked events –** This report provides information related to the blocked events IP address, port details, firewall blocking status and reason.

LogTime	Log Type	Source IP Address	Port and Service	Destination IP Address	Firewall Blocking	Reason
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:19 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:19 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:20 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:20 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block

Figure 9

- **ForeScout CounterAct – Mail infection activities –** This report provides information related to mail ids of sender and receiver, mail subject and IP address.

LogTime	Log Type	Source IP Address	Mail From	Mail To	Mail Subject
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:19 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:19 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:20 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report

Figure 10

- **ForeScout CounterAct – Network access control activities -** This report provides information related to IP address, rule names, rule message, and reason.

LogTime	Log Type	Source IP Address	Rule Name	Category	Rule Match	Message	Reason
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance"	Not Compliant	AV Not Running:Match	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance"	Not Compliant	AV Not Running:Match	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance"	Not Compliant	AV Not Running:Match	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance"	Not Compliant	AV Not Running:Match	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.

Figure 11

- **ForeScout CounterAct - Threat protection events-** This report provides information related to IP addresses, port bite, scan event, and manual event.

LogTime	Log Type	Sorce IP Address	Destination IP Address	Client Port
06/18/2019 12:51:22 PM	Manual event	10.10.1.123		
06/18/2019 12:51:22 PM	Scan event	106.101.1.23		
06/18/2019 12:51:22 PM	Port bite	120.10.1.23	130.20.3.45	139
06/18/2019 12:51:25 PM	Manual event	10.10.1.123		
06/18/2019 12:51:25 PM	Scan event	106.101.1.23		
06/18/2019 12:51:25 PM	Port bite	120.10.1.23	130.20.3.45	139
06/18/2019 12:51:26 PM	Manual event	10.10.1.123		
06/18/2019 12:51:26 PM	Scan event	106.101.1.23		
06/18/2019 12:51:26 PM	Port bite	120.10.1.23	130.20.3.45	139
06/18/2019 12:51:28 PM	Port bite	120.10.1.23	130.20.3.45	139

Figure 12

- **ForeScout CounterAct - User login and logout-** This report provides information related to user login and logout.

LogTime	User Name	Source IP Address	Client IP Address	Reason	Log Status
06/18/2019 01:01:32 PM	admin	10.23.78.123	21.45.34.89	User admin changed Enterprise Manager Console	Logout succeeded
06/18/2019 01:01:34 PM	admin	10.23.78.123	21.45.34.89	User admin Enterprise Manager Console	Login succeeded
06/18/2019 01:01:36 PM	admin	10.23.78.123	21.45.34.89	User admin changed Enterprise Manager Console	Logout succeeded
06/18/2019 01:11:27 PM	admin	10.21.78.12	22.46.4.189	User admin changed Enterprise Manager Console	Logout succeeded
06/18/2019 01:11:29 PM	admin	10.23.78.123	21.45.34.89	User admin changed Enterprise Manager Console	Logout succeeded

Figure 13

- **ForeScout CounterAct - User activities –** This report provides information about admin changed network configuration, admin changed policy rules.

LogTime	Log Type	Message
06/18/2019 12:51:21 PM	User admin changed Configuration	Paused Network Integrity rules:1.1 Primary Classification
06/18/2019 12:51:21 PM	User admin changed Configuration	Change field lists definition toListsMaaS360 Software Installed -> Application Name: MaaS360 Unauthorized MobileApplicationsNetBIOS Domain: Corporate domain names, Corporate domain names_1VMware Server Product ID: ESXi Server ListWindows Applications Installed -> Name: sqlserverWindows Services Running: Microsoft virtual services
06/18/2019 12:51:21 PM	User admin changed HPS Inspection Engine Configuration	Edited thefollowing Enterprise Manager: :Endpoint Remote Inspection method: Previous Value:wmi_only CurrentValue:wmi_with_fall_back
06/18/2019 12:51:21 PM	User admin changed Configuration	Policy: '1.1 PrimaryClassification'Sub-Rule changes:Sub-Rule Linux\UnixOld Condition:Network Function: Unix Server/Workstation, Linux Desktop/ServerNew Condition:Network Function: Unix Server/Workstation, Linux Desktop/Server OR OpenPorts: 22/TCP
06/18/2019 12:51:24 PM	User admin changed Configuration	Paused Network Integrity rules:1.1 Primary Classification

Figure 14

Dashboards

- **ForeScout CounterAct NAC Activities** – This dashboard shows information network access control activities like IP addresses, firewall action status, and reason.

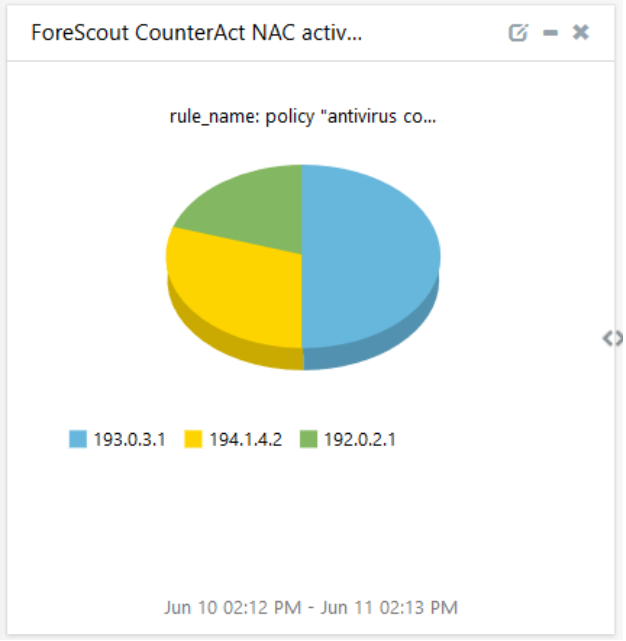

Figure 15

- **ForeScout CounterAct Blocked Events** – This dashboard shows information about suspicious activities blocked by ForeScout CounterAct.

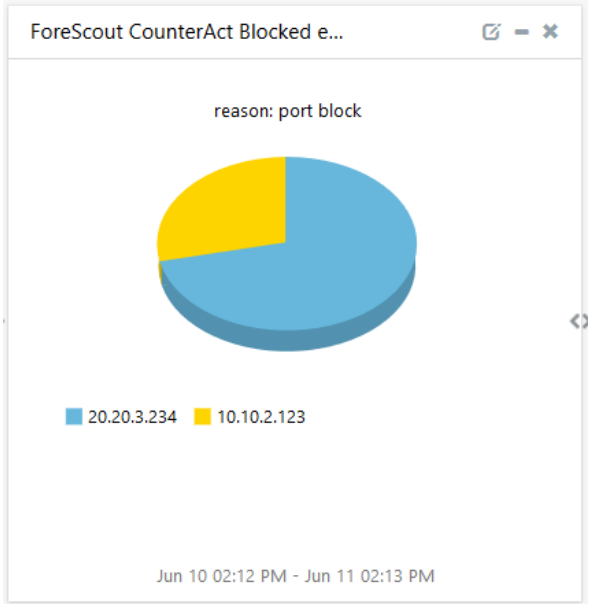

Figure 16

- **ForeScout CounterAct Mail Infection Detected** – This dashboard shows information about mail recipient addresses, IP addresses, and mail subject.

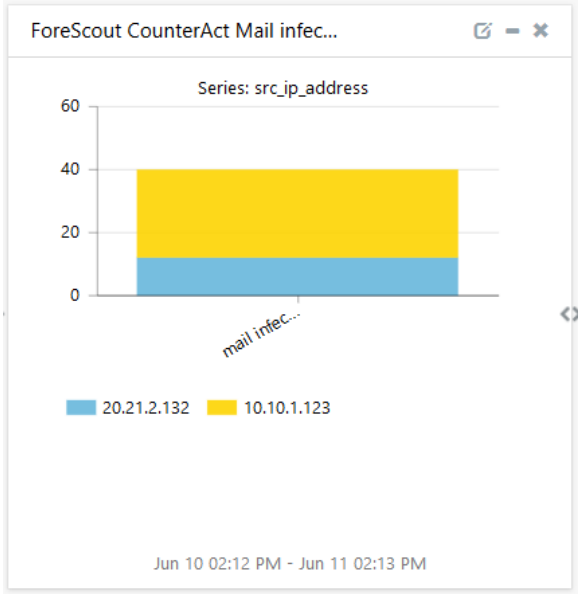

Figure 17

- **ForeScout CounterAct threat protection events** – This dashboard shows information about the IP addresses, port bite, scan event, and manual event.

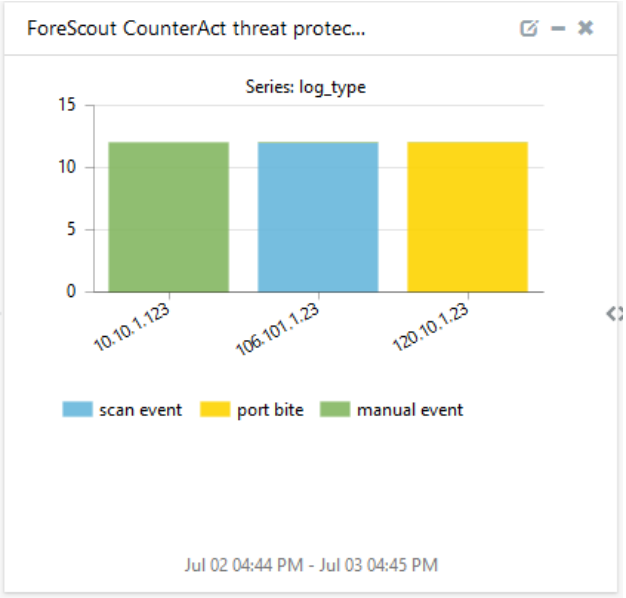

Figure 18

- **ForeScout CouterAct user activities –** This dashboard shows information about admin changes network configuration, admin modified policy rules.

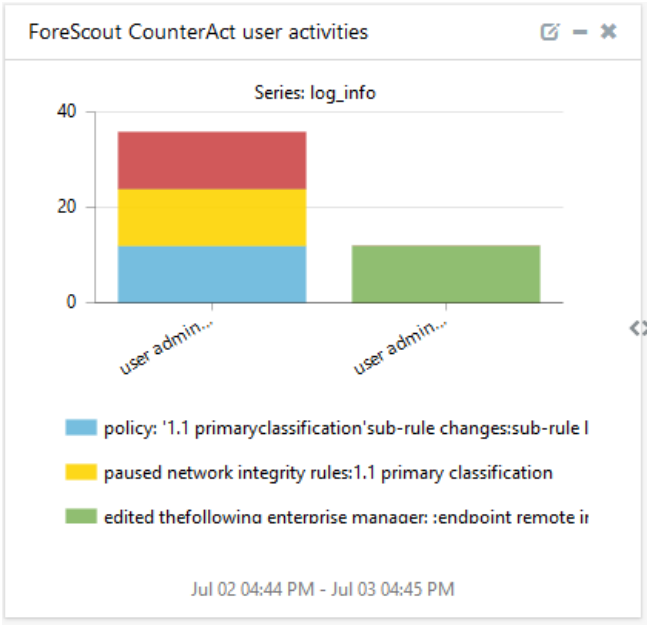

Figure 19

- **ForeScout CounterAct user login and logout –** This dashboard shows information about user login and logout.

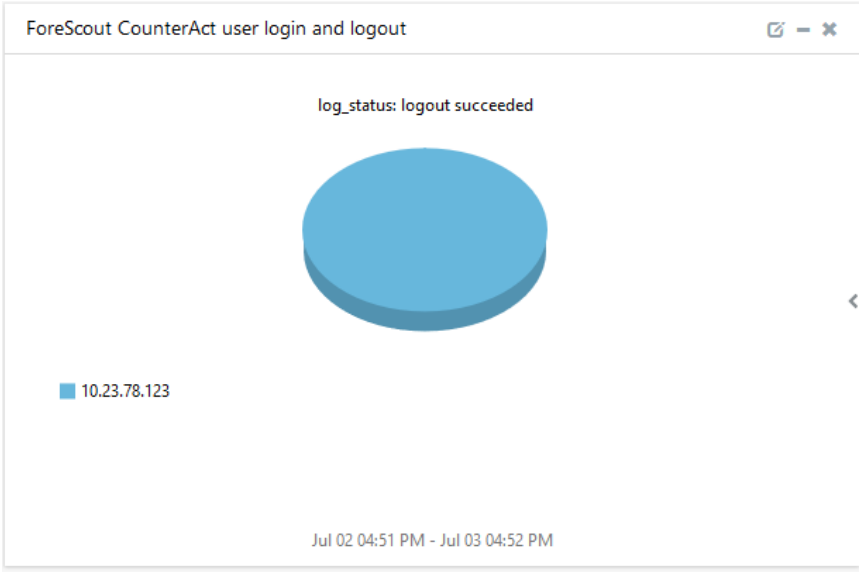

Figure 20

Importing Knowledge Pack into EventTracker

Find the specified knowledge pack in the following sequences-

- Alerts
- Knowledge Objects
- Token Template
- Flex Reports
- Dashlets

1. Launch the **EventTracker Control Panel**.
2. Double click **Export/Import Utility**, and then click the **Import** tab.

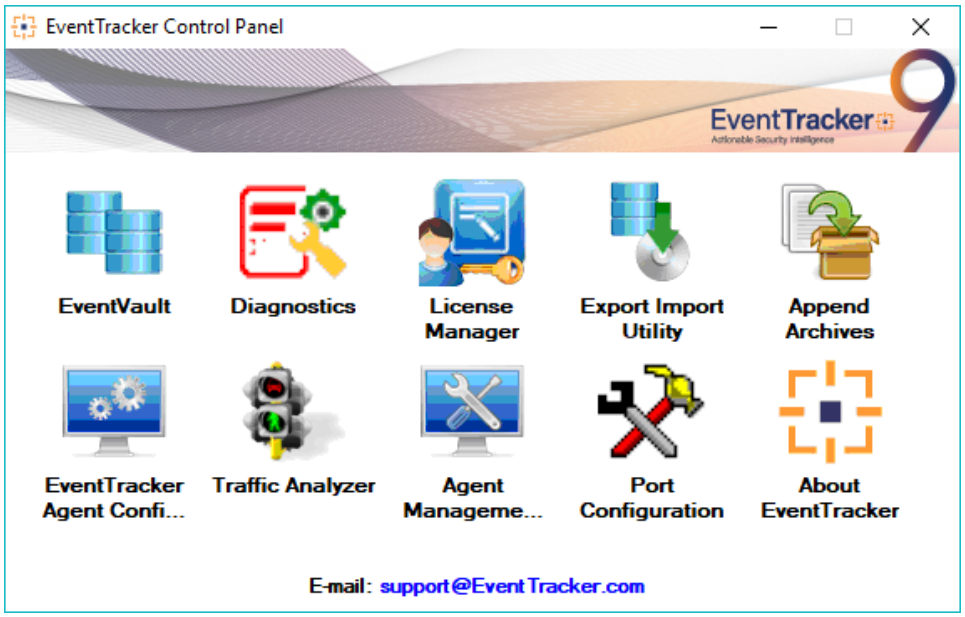

Figure 21

3. Import **Tokens/Flex Reports** as given below.

Alerts

1. Click the **Alert** option, and then click the **Browse** ... button.

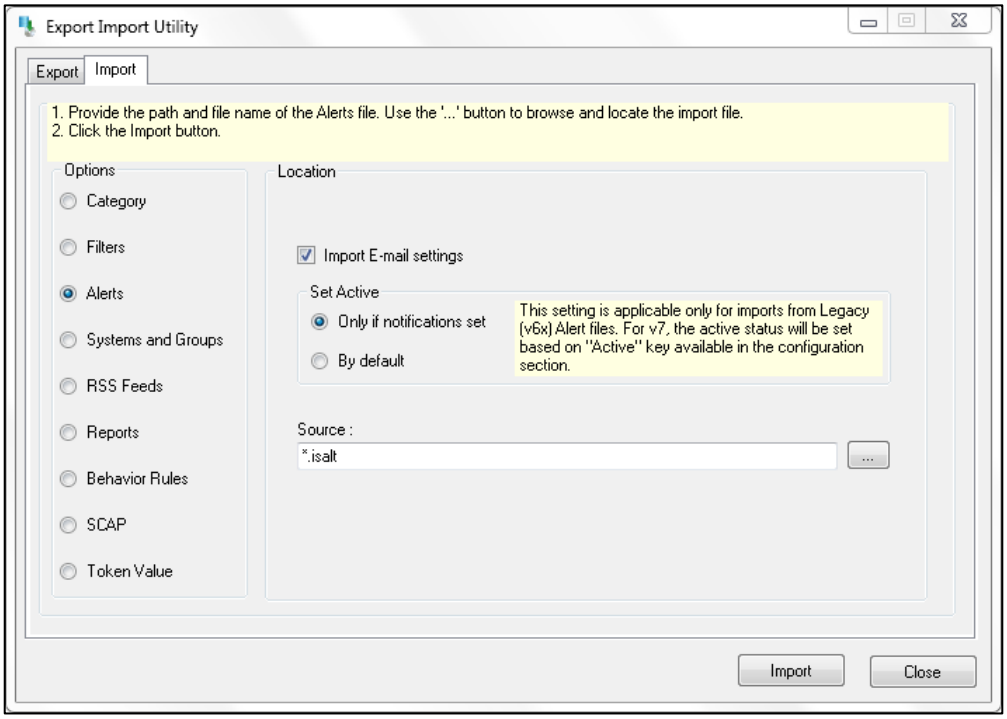

Figure 22

2. Locate the **Alerts_ForeScout CounterAct.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays a success message.

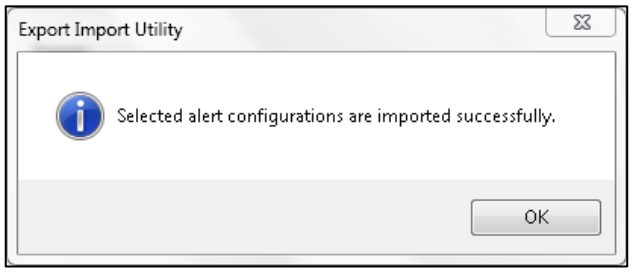

Figure 23

4. Click the **OK** button, and then click the **Close** button.

Knowledge Objects

1. Login into EventTracker and click **Knowledge objects** under the Admin option in the EventTracker page.
2. Locate the file named **KO_ForeScout CounterAct.etko**.

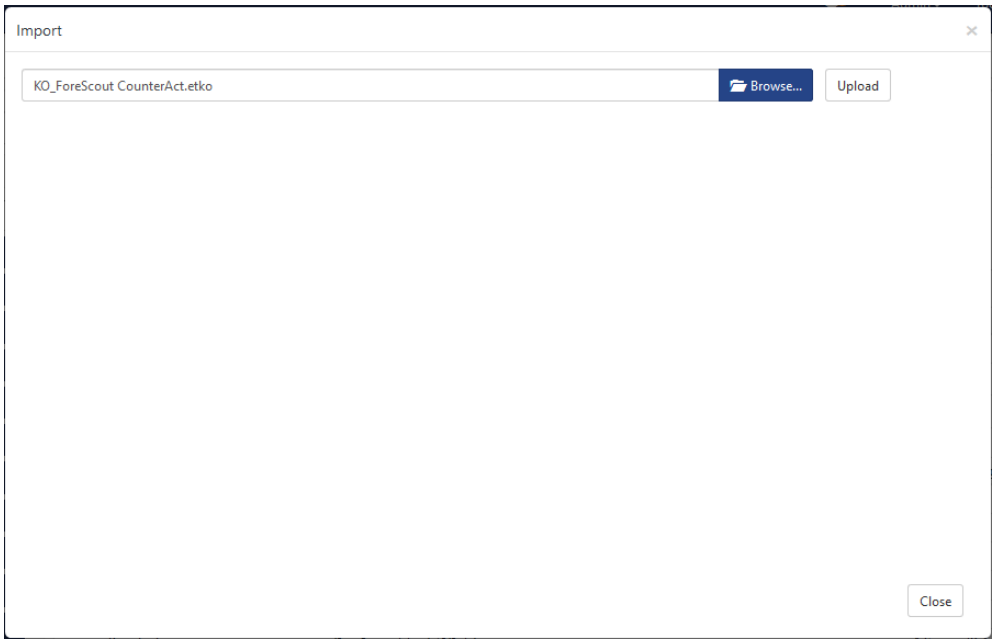

Figure 24

3. Now select all the checkbox and then click on the '**Import**' option.

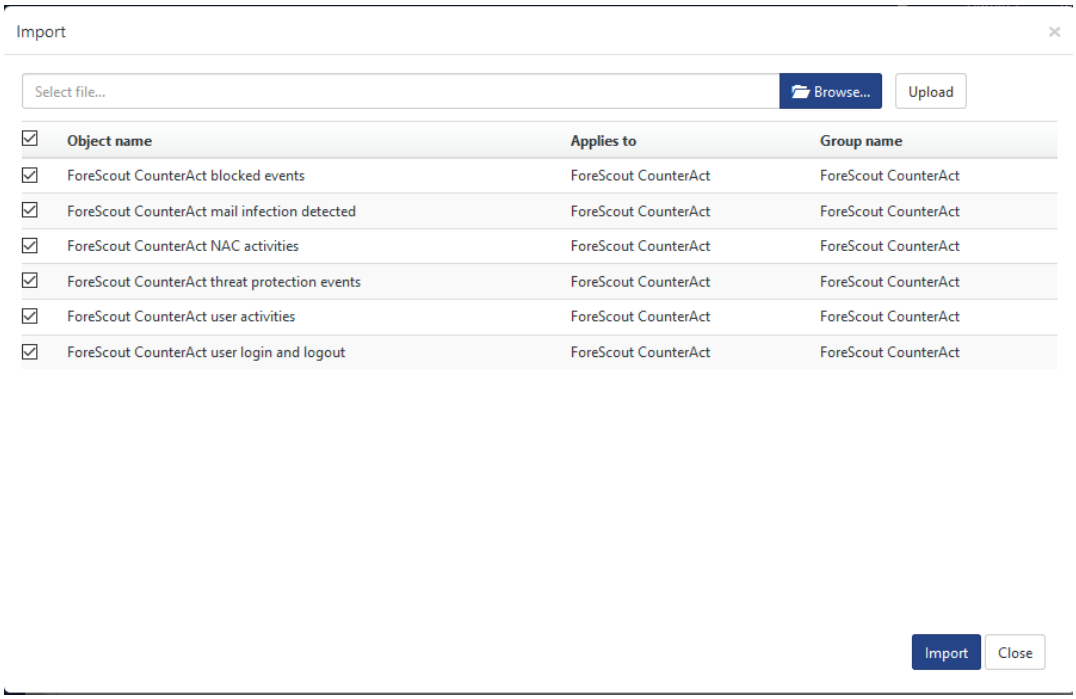

Figure 25

4. Knowledge objects are now imported successfully. Please click **OK** and **Activate Now**.

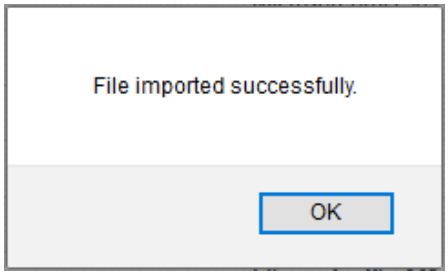

Figure 26

Token Template

1. Login to the **EventTracker**.
2. Click on **Admin >> Parsing Rules**.

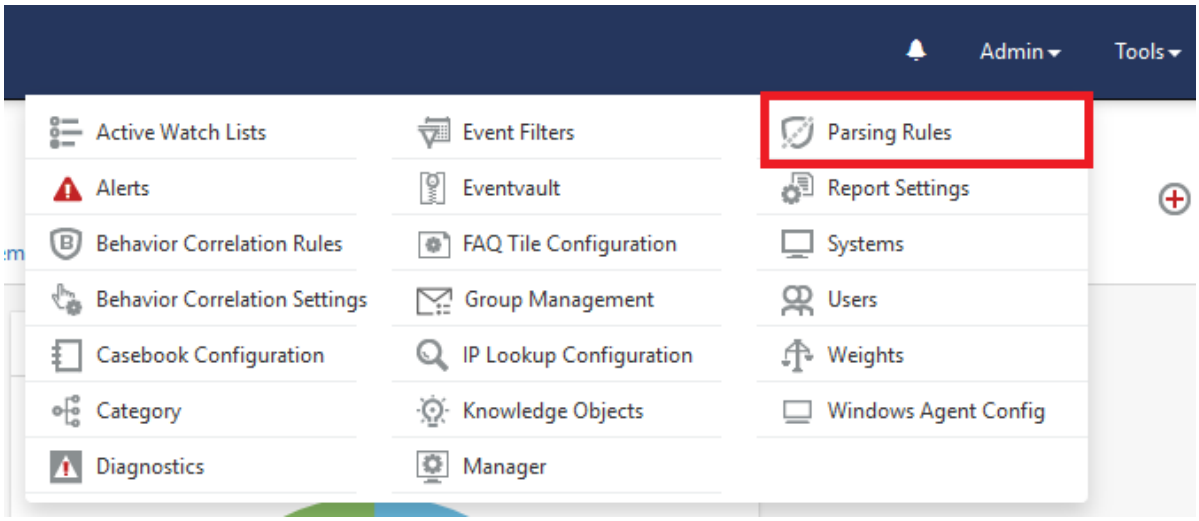

Figure 27

3. Click on **Template** and click **import configuration** Symbol.

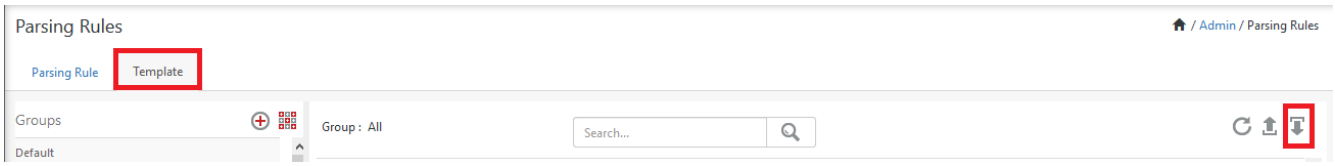

Figure 28

4. Locate the **Template_ForeScout CounterAct.ettd** file and click on **import**.

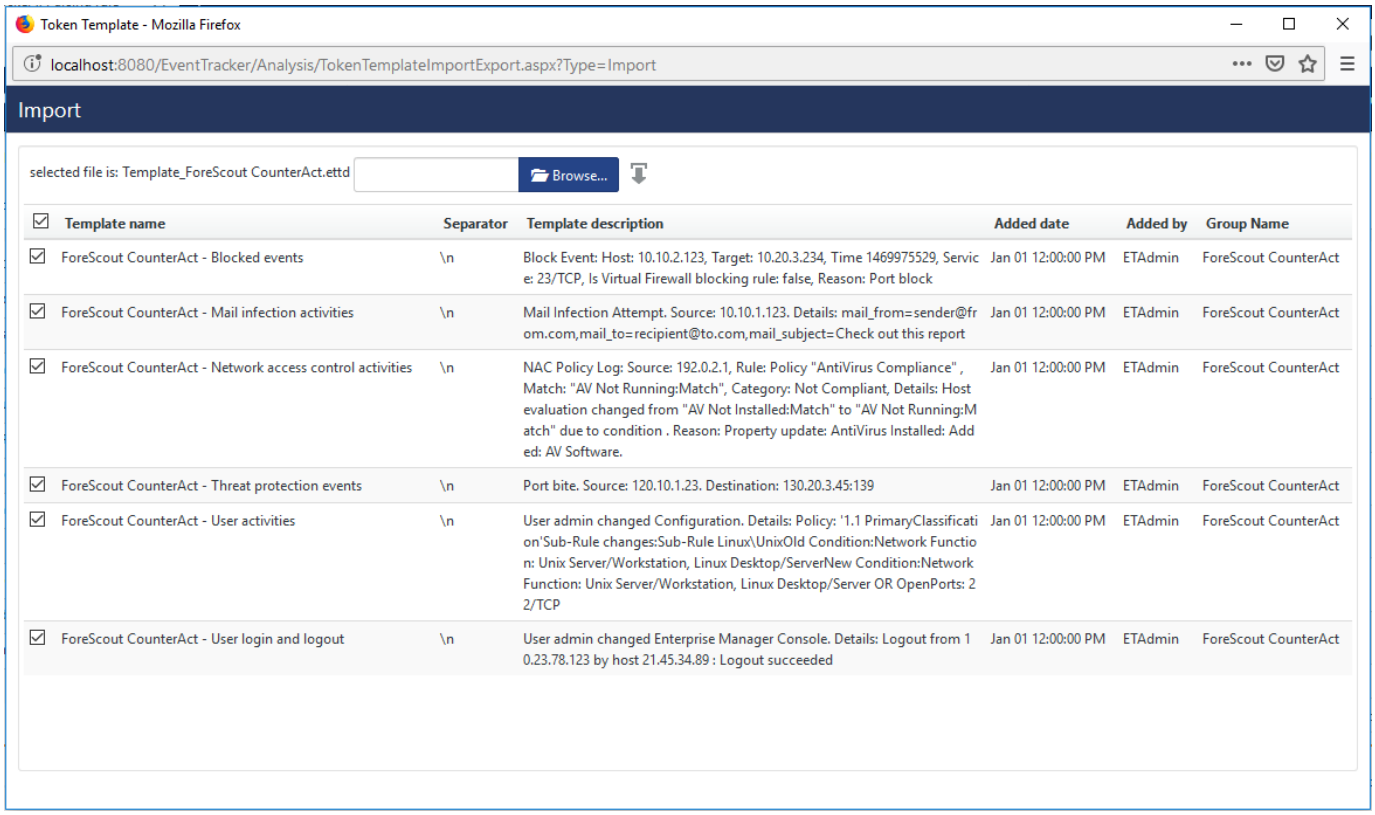

Figure 29

5. Templates are imported now successfully.

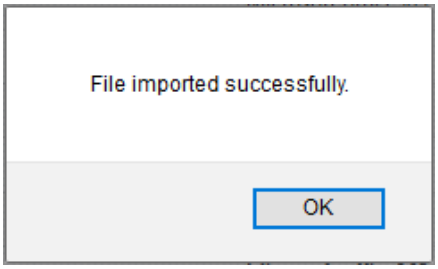

Figure 30

Flex Reports

1. Click **Reports** option and select new (.etcrx) from the option.

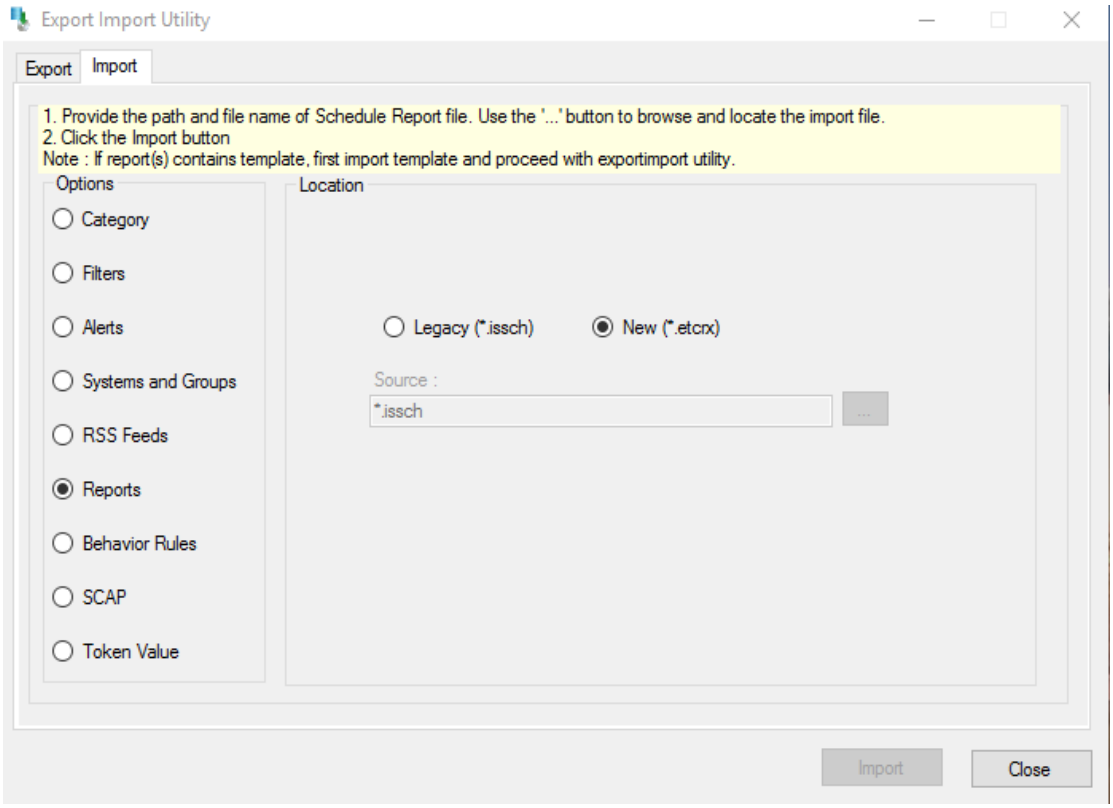

Figure 31

2. Locate the file named **Flex_Reports_ForeScout CounterAct.etcrx** and select all the checkbox.

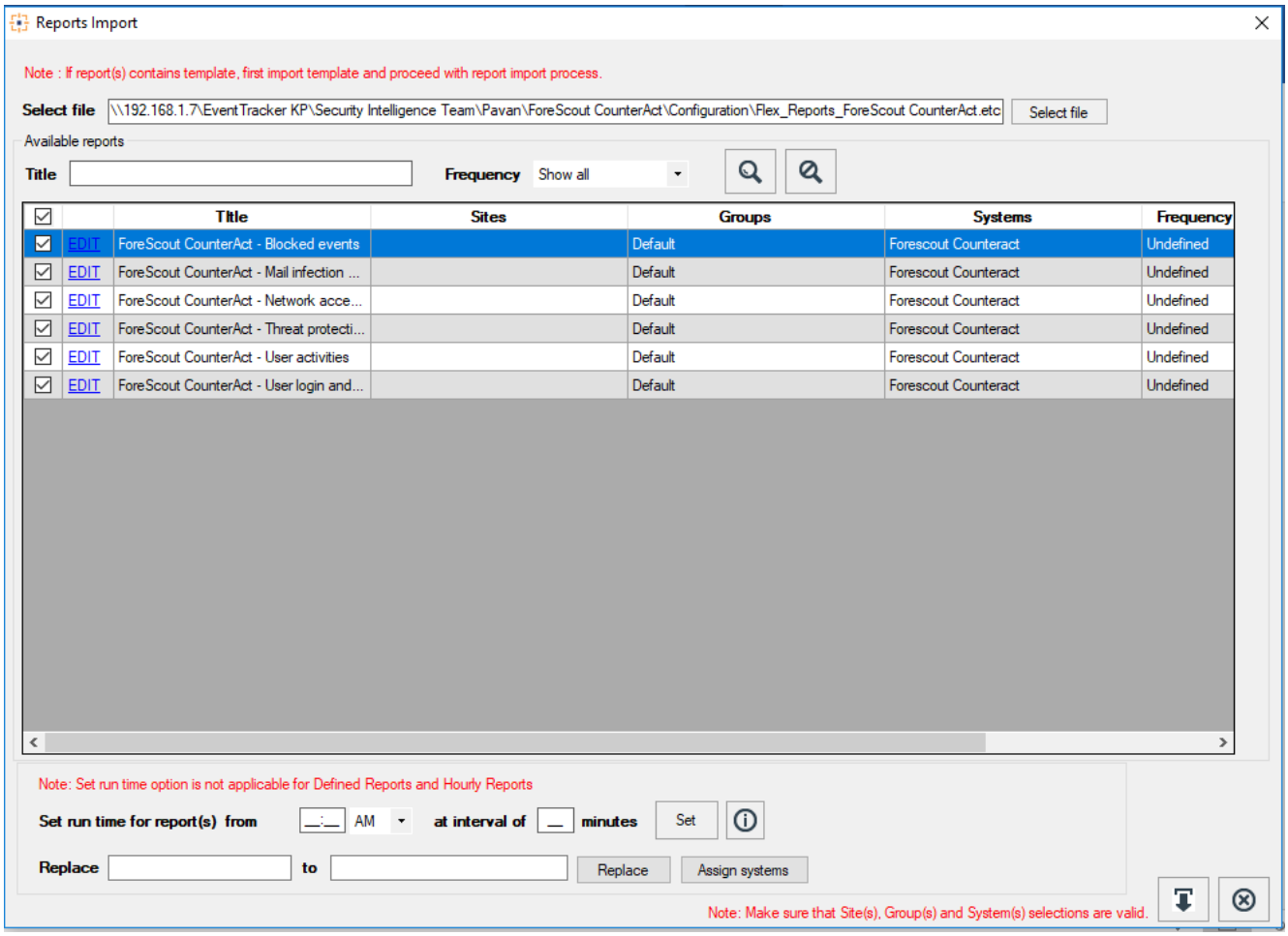

Figure 32

3. Click the **Import** button to import the reports. EventTracker displays a success message.

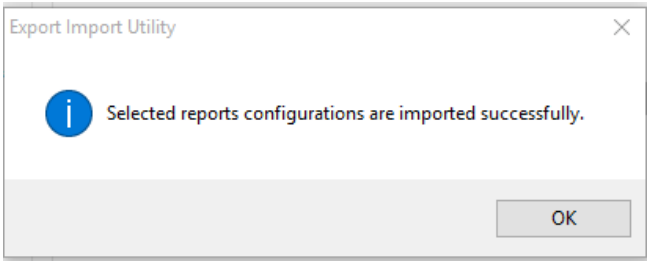

Figure 33

Dashlets

In EventTracker 9.0, we have added a new feature that will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker.

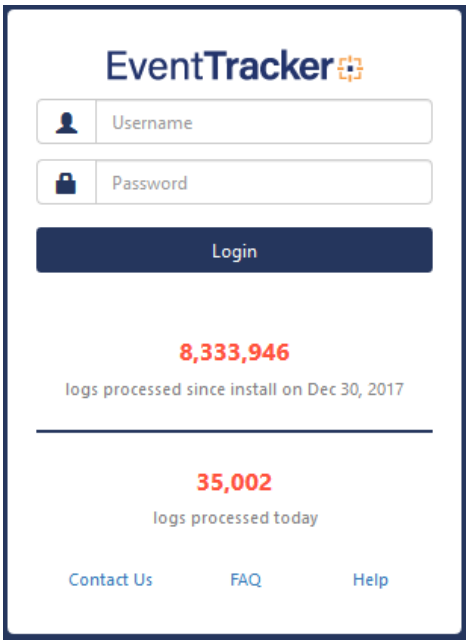

Figure 34

2. Go to **My Dashboard** option.

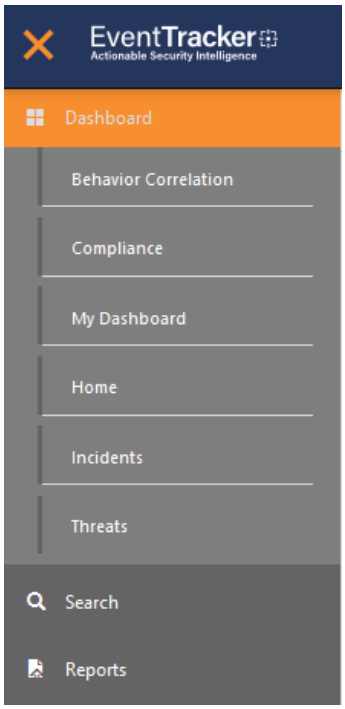

Figure 35

3. Click on the **import** button and select **.etwd** File.

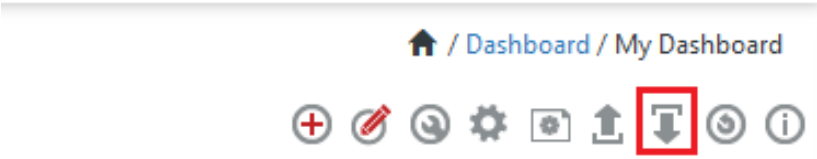

Figure 36

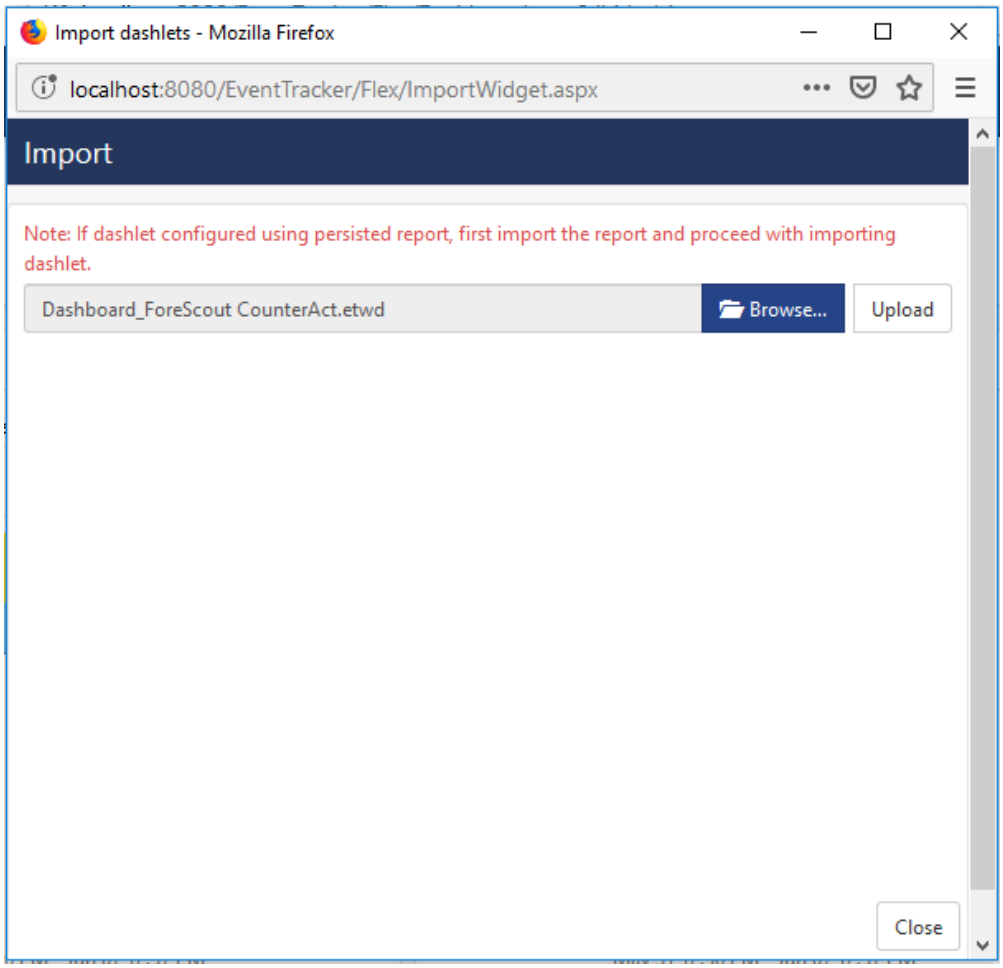

Figure 37

4. Click upload and select Dashboard which you want to import.

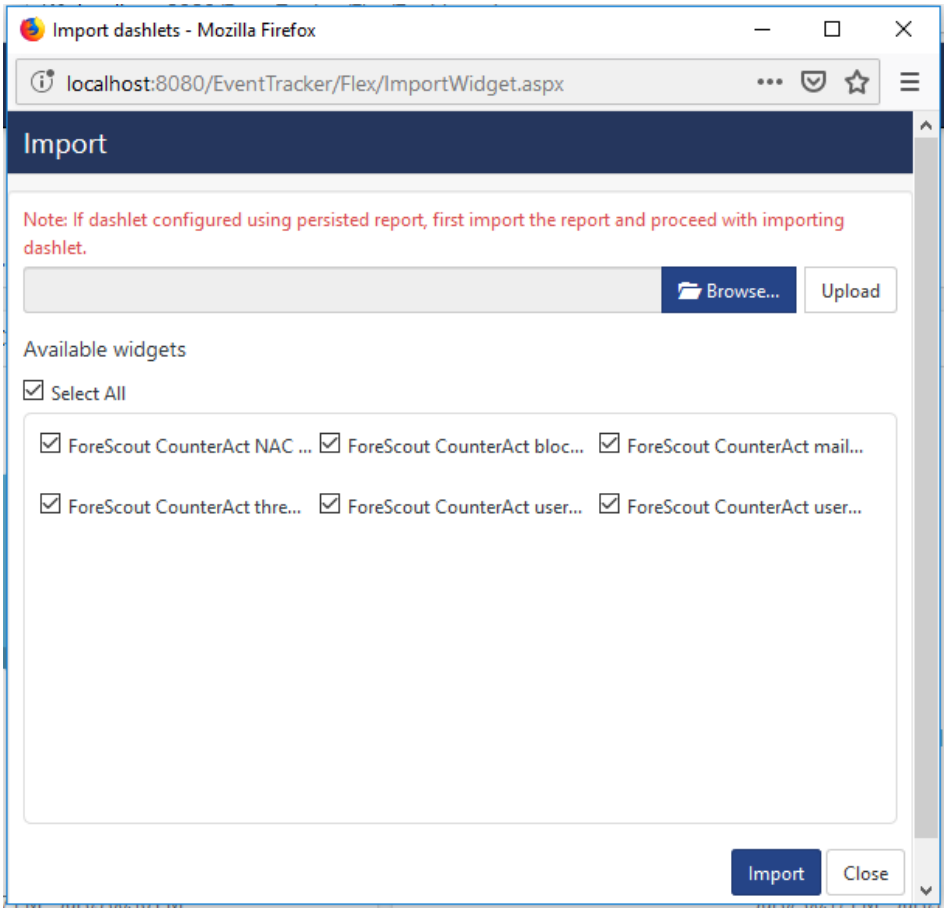

Figure 38

5. Click on the **Import** button. It will upload all selected dashboards.

Verifying Knowledge Pack in EventTracker

Alerts

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.

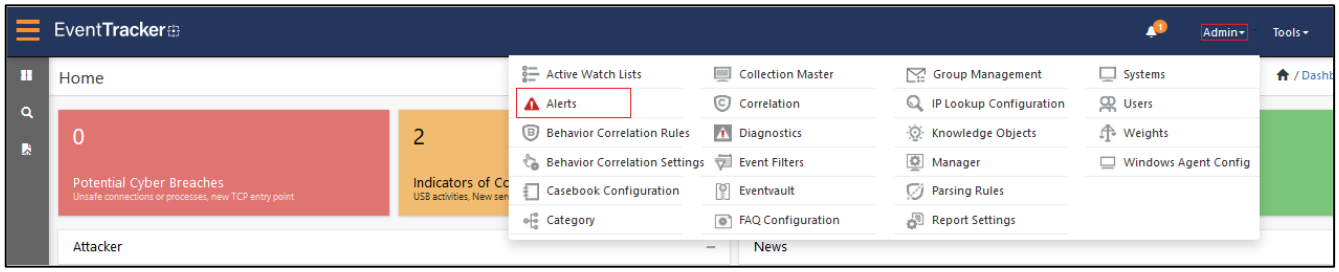

Figure 39

3. In the **Search** box, type **'ForeScout CounterAct'**, and then click the **Go** button.
   Alert Management page will display all the imported alerts.

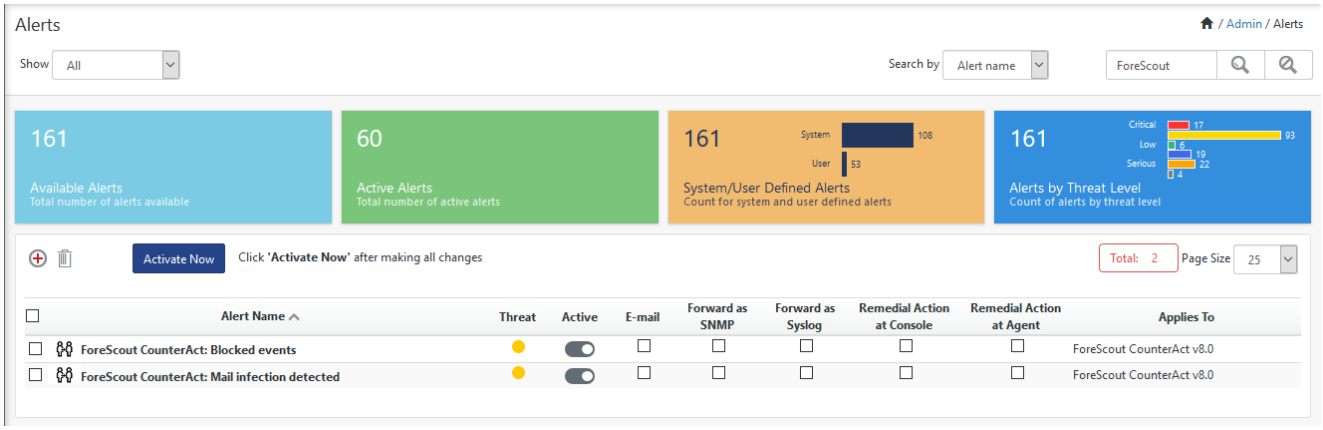

Figure 40

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays a message box.

Figure 41

5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify appropriate **systems** in the **alert configuration** for better performance.

Knowledge Object

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click the **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click the **ForeScout CounterAct** group folder.
4. Knowledge Object is displayed in the pane.

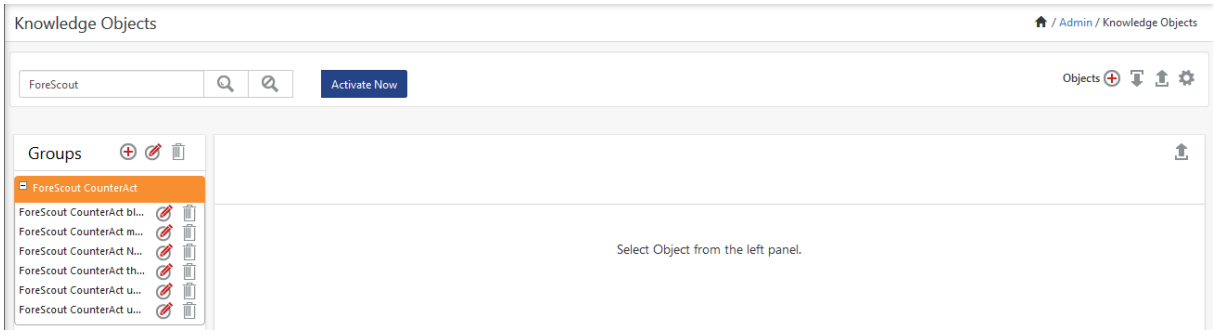

Figure 42

Token Template

1. Login to the **EventTracker**.
2. Click on **Admin >> Parsing Rules**.

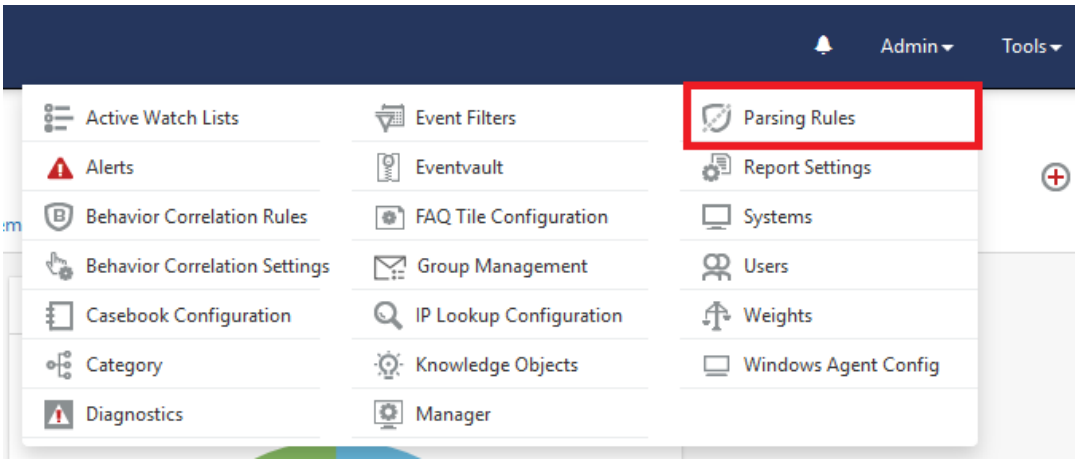

Figure 43

3. Click on **Template** and search for **ForeScout CounterAct.**

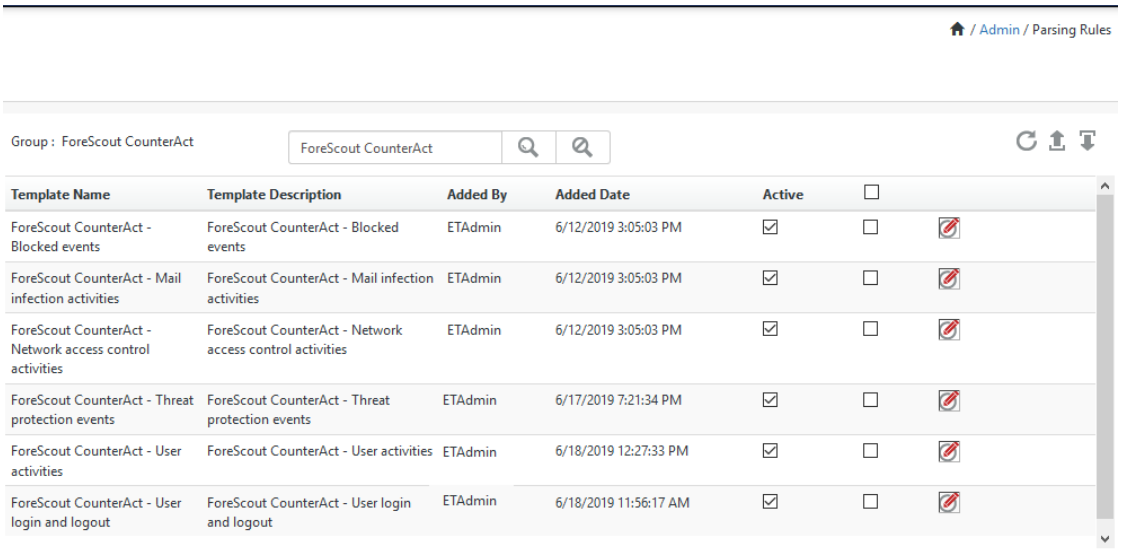

Figure 44

Flex Reports

1. Login to **EventTracker**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click the **ForeScout CounterAct** group folder.

5. Reports are displayed in the Reports configuration pane.

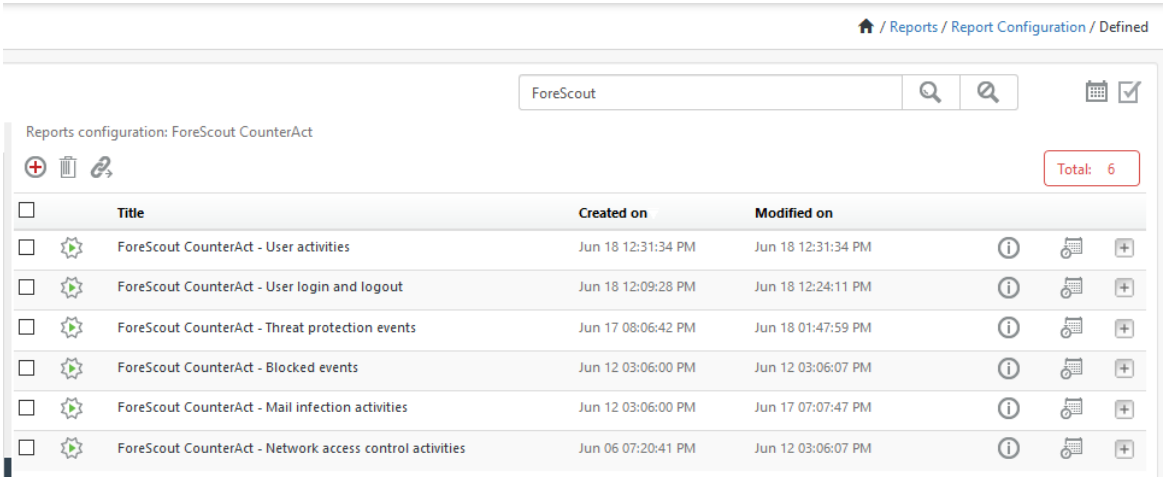

Figure 45

Dashlets

1. Login to **EventTracker**.
2. Click the **Dashboard** menu, and then **My Dashboard.**
3. Then click on **Customize Dashlet** button and search for **"ForeScout CounterAct"**

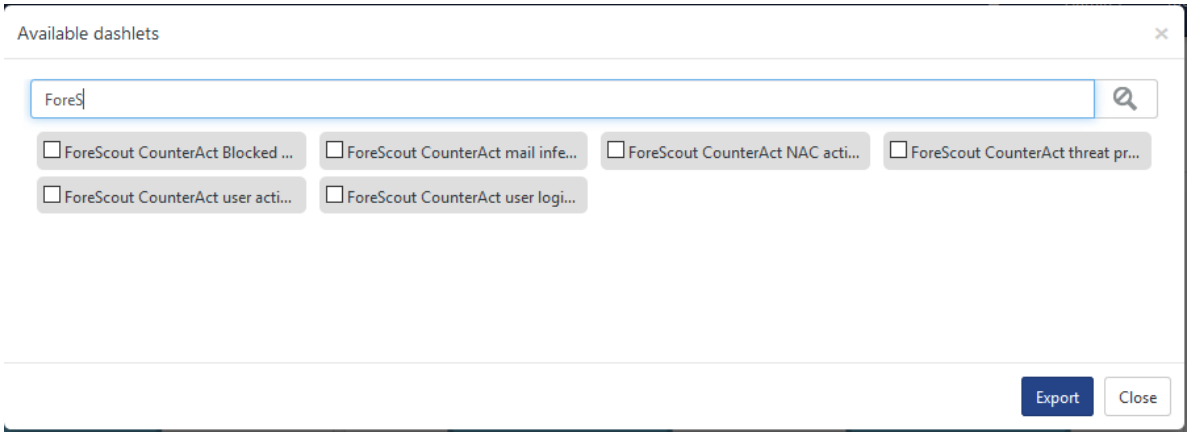

Figure 46