

Integration Guide

Integrating Extreme Network Access Control (NAC)

EventTracker v9.x and above

Publication Date:

July 23, 2021

Abstract

This guide provides instructions to configure Extreme Network Access Control to forward Extreme Network Access Control logs via syslog. After EventTracker is configured to collect and parse these logs, dashboard, and reports can be configured to monitor Extreme Network Access Control logs.

Scope

The configurations detailed in this guide are consistent with EventTracker version v 9.x or above and Extreme Management Center version 7.1.

Audience

Administrators who are assigned the task to monitor Extreme Network Access Control events using EventTracker.

Table of Contents

- Table of Contents3
- 1. Overview4
- 2. Prerequisites.....4
- 3. Configuring Extreme Network Access Control4
 - 3.1 Enable syslog/ Remote Logging.....4
- 4. EventTracker Knowledge Pack.....6
 - 4.1 Categories6
 - 4.2 Reports6
 - 4.3 Dashboards.....8
- 5. Importing Extreme Network Access Control Knowledge Pack into EventTracker10
 - 5.1 Categories10
 - 5.2 Token Template.....11
 - 5.3 Reports12
 - 5.4 Knowledge Object.....14
 - 5.5 Dashboard.....15
- 6. Verifying Extreme Network Access Control Knowledge Pack in EventTracker16
 - 6.1 Categories16
 - 6.2 Token Value16
 - 6.3 Knowledge Objects.....17
 - 6.4 Reports17
 - 6.5 Dashboard.....17
- About Netsurion.....19

1. Overview

Extreme Networks Network Access Control (NAC) is a complete standard-based, multi-vendor, interoperable, pre-connect, and post-connect Network Access Control solution for wired and wireless LAN and VPN users. The Extreme Control engine is monitored by Extreme Management Center which provides the analytics for the network.

Log configuration can be achieved via syslog. It will send events like authentication events, user logon events, ethernet connectivity events. With this events EventTracker generate detail reports for user logon activities, ethernet connectivity status, and user authentication activities. Its graphical representation shows login success by username, authentication success by username, ethernet link status, etc.

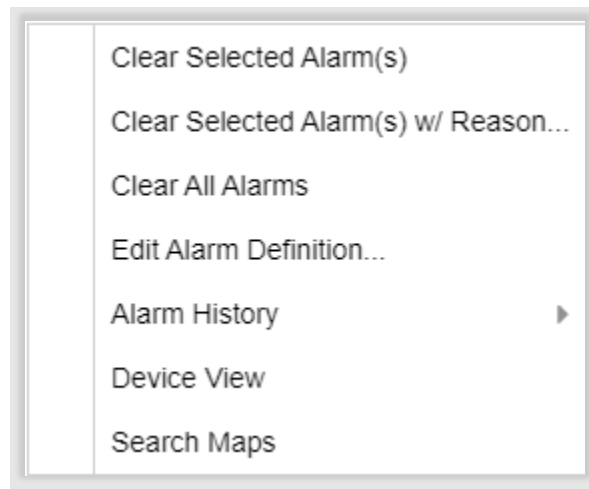
2. Prerequisites

- Admin access to Extreme Network Access Control(NAC).

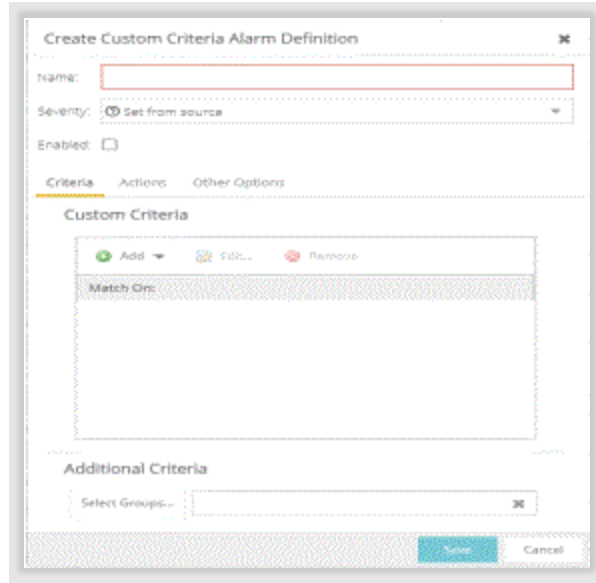
3. Configuring Extreme Network Access Control

3.1 Enable syslog/ Remote Logging.

1. Log in to the Extreme Network Access Control (NAC) web interface with Admin privileges.
2. Navigate to **Alarms tab**, right-click on the alarm or select the **Menu** icon (☰) to display several additional functions.
3. Click on **Edit Alarm Definition**.



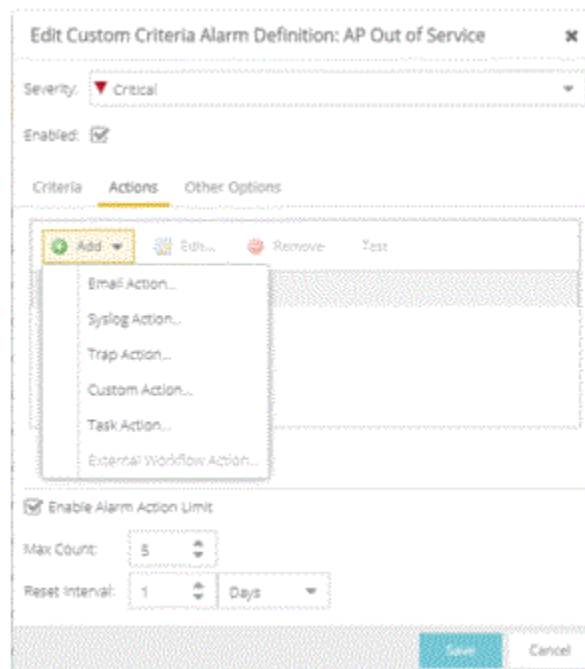
4. Select to open the alarm in the [Alarm Configuration window](#), from which you can edit the criteria which triggers the alarm. The **Create Custom Criteria Alarm Definition** window opens.



5. The severity of the alarm displays in the Severity field. Use the drop-down list to change the alarm severity. The Enabled check box indicates if the custom criteria has been enabled.
 - Select the **Criteria** tab to open the **Custom Criteria** window, where you can Add, Edit or Remove specific criteria details the alarm.

Use the Additional Criteria field to add new criteria. Select the **Select Groups** button to open the Alarm Group Section window.

- Select the **Actions** tab to Add, Edit, Remove actions to the alarm definition. Select the Add button to open the Action drop-down list:



6. Select **Syslog action** from the drop-down list.
 - Syslog Server: Enter EventTracker IP address.
 - Port: Enter syslog server port number 514.
 - Click **Enable** to provide custom log format.

```
Time $time Device $device: alarmName="$alarmName", alarmSource="$alarmSource",
alarmSourceName="$alarmSourceName", alarmSubcomponent="$alarmSubcomponent",
severity="$severity", type="$type", trigger="$trigger", server="$server", Time="$time",
message="$message", eventType="$eventType", eventSeverity="$eventSeverity",
eventCategory="$eventCategory", eventTitle="$eventTitle", eventUser="$eventUser",
eventClient="$eventClient", deviceIP="$deviceIP", deviceIpCtx="$deviceIpCtx",
deviceNickName="$deviceNickName", deviceBootProm="$deviceBootProm",
deviceStatus="$deviceStatus", snmp="$snmp", sysName="$sysName",
sysLocation="$sysLocation", sysUpTime="$sysUpTime", chassisId="$chassisId",
chassisType="$chassisType", trapName="$trapName", trapEnterprise="$trapEnterprise",
trapOid="$trapOid", trapArgs="$trapArgs"
```

Note: We can receive all type of Extreme NAC event logs to EventTracker with above format.

7. Click **Save** changes.

4. EventTracker Knowledge Pack

After logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support **Extreme Network Access Control**.

4.1 Categories

- **Extreme Network Access Control: User login activities** – This saved search provides information related to user login success and user logout events.
- **Extreme Network Access Control: Ethernet port status** – This saved search provides information related to ethernet link goes up and down status.
- **Extreme Network Access Control: User authentication activities** – This saved search provides information related to user try to authenticate for login into Extreme Network Access Control.

4.2 Reports

- **Extreme Network Access Control - User login and logout** – This report is a summary of users try to login and logout into Extreme Network Access Control and it give success status. It contains key field such as log datetime, username, IP address, and logon status.

LogTime	Computer	User Name	Console Type	Server IP address	Client IP Address	Status
07/12/2021 05:43:25 PM	EXTREME_ACCESS_CONTROL-SYSLOG	kenneth	app	10.100.0.4	10.100.0.131	Login
07/12/2021 05:43:25 PM	EXTREME_ACCESS_CONTROL-SYSLOG	maya	ssh	10.100.0.4	10.20.0.11	logout
07/12/2021 05:43:25 PM	EXTREME_ACCESS_CONTROL-SYSLOG	admin	xml	10.100.0.4	10.100.0.18	logout
07/12/2021 05:43:25 PM	EXTREME_ACCESS_CONTROL-SYSLOG	joeb	ssh	10.100.0.4	10.100.0.121	Login
07/12/2021 05:43:25 PM	EXTREME_ACCESS_CONTROL-SYSLOG	maxx	ssh	10.100.0.4	10.100.0.121	logout

- Extreme Network Access Control - User authentication success** – This report is a summary of users trying to authenticate for Extreme Network Access Control and it gives success status or failure status. It contains key fields such as username and IP address.

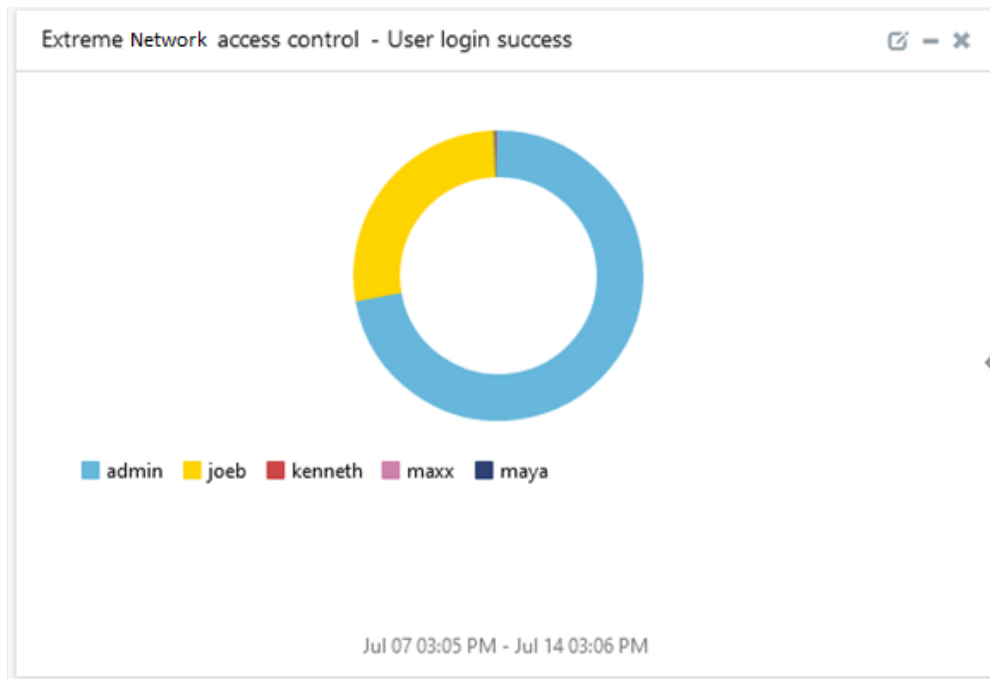
LogTime	Computer	User Name	Client IP Address
07/12/2021 07:50:33 PM	EXTREME_ACCESS_CONTROL-SYSLOG	maya	10.100.0.131
07/12/2021 07:50:33 PM	EXTREME_ACCESS_CONTROL-SYSLOG	admin	10.20.0.12
07/12/2021 07:50:33 PM	EXTREME_ACCESS_CONTROL-SYSLOG	kenneth	10.20.0.12
07/12/2021 07:50:33 PM	EXTREME_ACCESS_CONTROL-SYSLOG	joeb	10.100.0.121

- Extreme Network Access Control – Ethernet link status** – This report is a summary of link port connectivity status goes up or down status. It contains key fields such as ethernet connected port number, ethernet port name, status, and IP address.

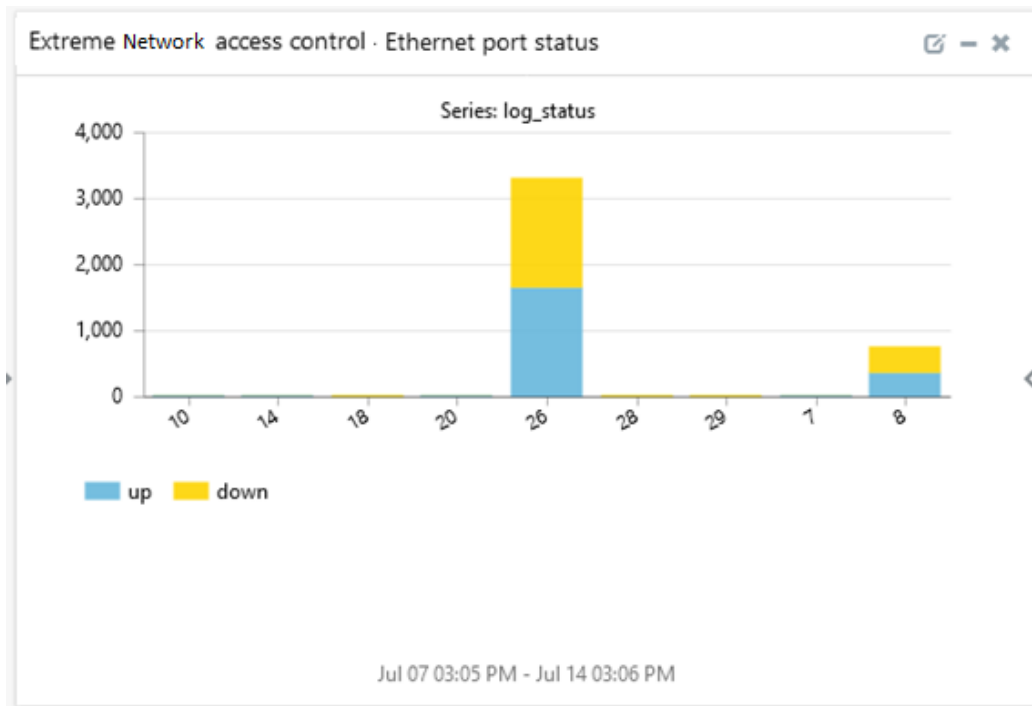
LogTime	Computer	Interface Name	Interface Port	Port Status	IP Address
07/12/2021 07:50:35 PM	EXTREME_ACCESS_CONTROL-SYSLOG	ge	28	Down	10.100.0.10
07/12/2021 07:50:35 PM	EXTREME_ACCESS_CONTROL-SYSLOG	ge	15	Up	10.100.0.11
07/12/2021 07:50:35 PM	EXTREME_ACCESS_CONTROL-SYSLOG	ge	10	Down	10.100.0.21
07/12/2021 07:50:35 PM	EXTREME_ACCESS_CONTROL-SYSLOG	ge	12	Up	10.100.0.14
07/12/2021 07:50:35 PM	EXTREME_ACCESS_CONTROL-SYSLOG	ge	26	Down	10.100.0.1

4.3 Dashboards

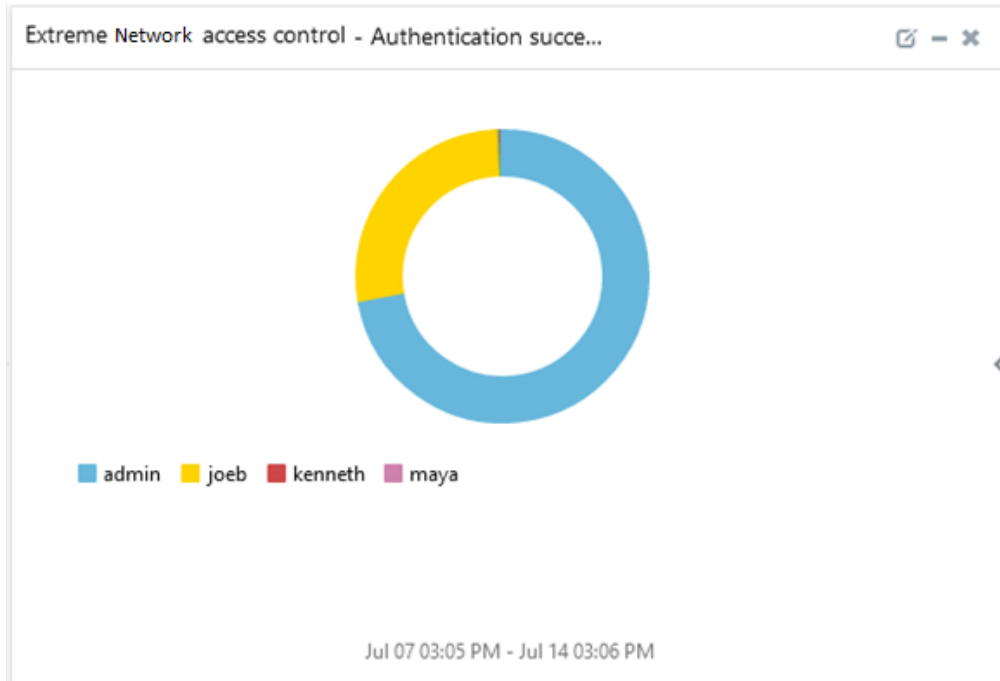
- Extreme Network Access Control - User login success



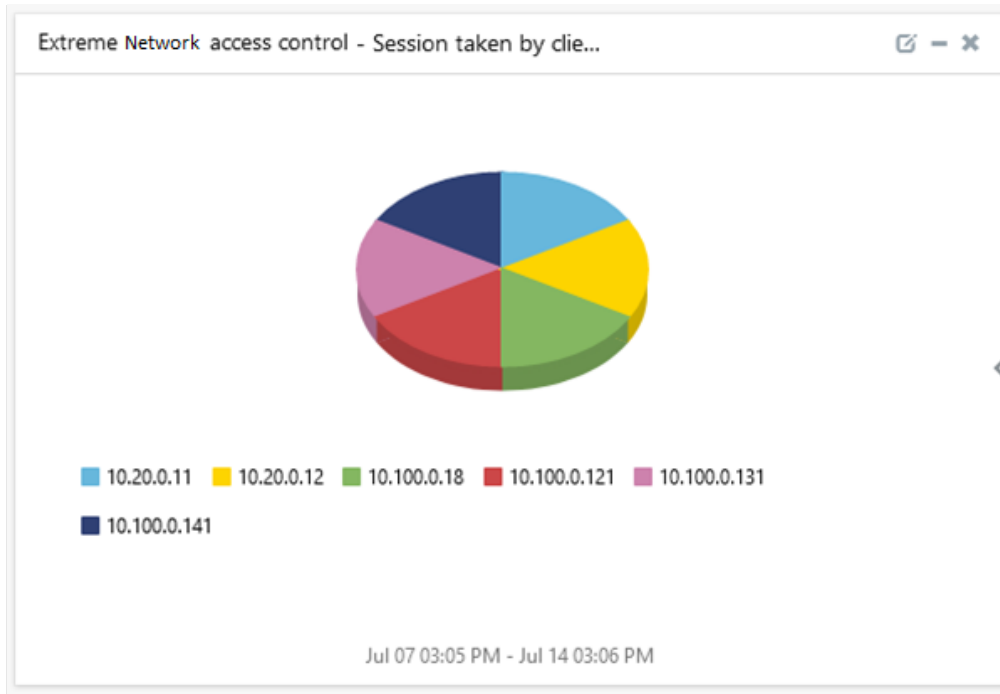
- Extreme Network Access Control - Ethernet port status



- **Extreme Network Access Control - Authentication success by username**



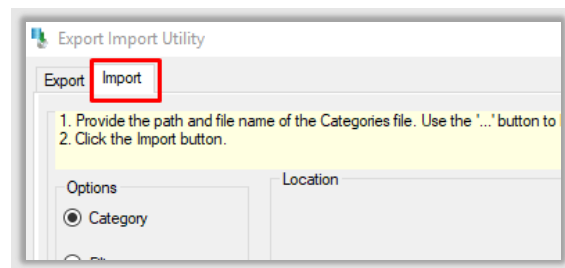
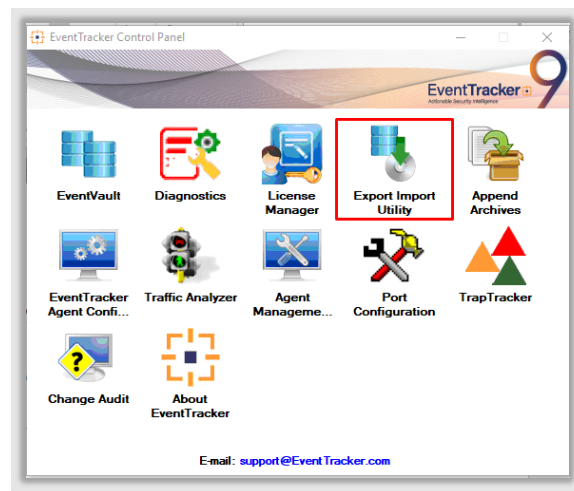
- **Extreme Network Access Control - Session taken by client IP**



5. Importing Extreme Network Access Control Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

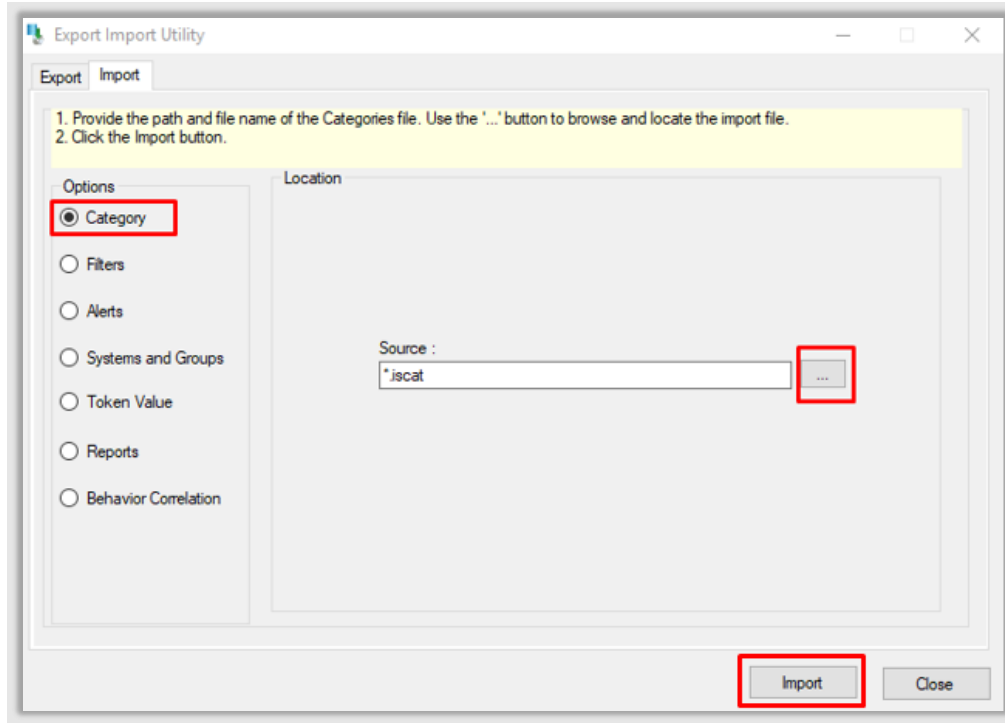
- Categories
 - Token Template
 - Knowledge Objects
 - Flex Reports
 - Dashboard
1. Launch the **EventTracker Control Panel**.
 2. Double click **Export-Import Utility**.



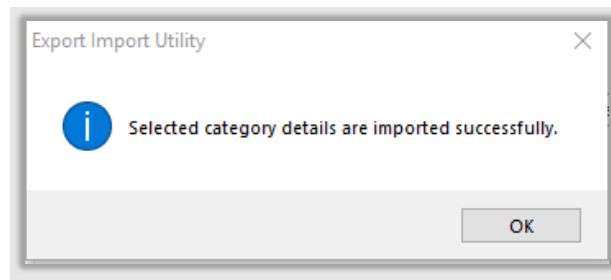
3. Click the **Import** tab.

5.1 Categories

1. After you have opened **Export Import Utility** via **EventTracker Control Panel**, click the **Category** option, and then click Browse .
2. Navigate to the Knowledge Pack folder and select the file with extension **".iscat"**, e.g., **"Categories_Extreme Network Access Control .iscat"** and then click on the **Import** button.



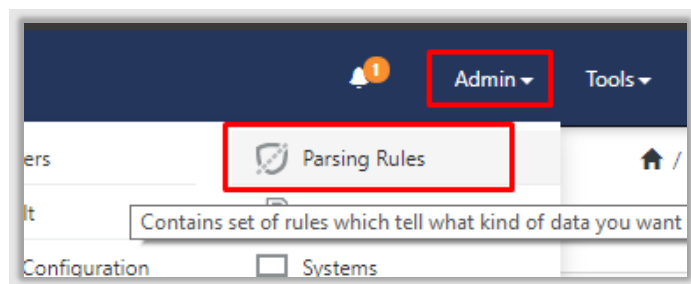
EventTracker displays a success message:



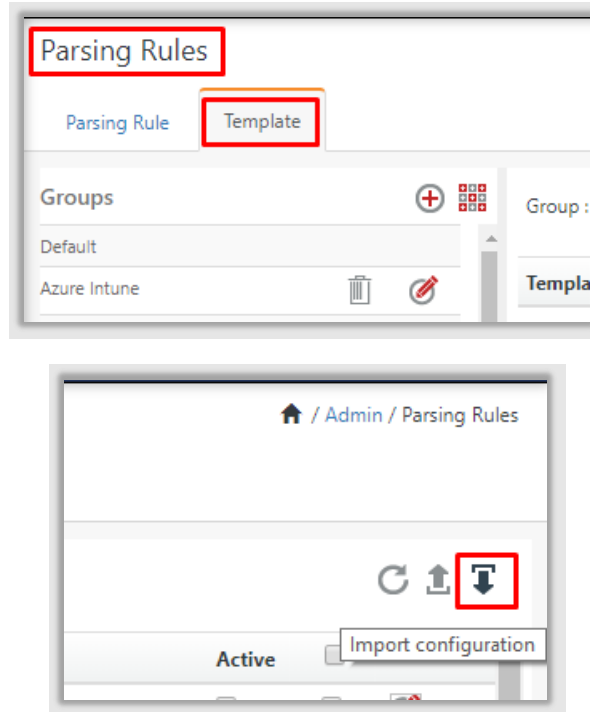
5.2 Token Template

For importing **Token Template**, navigate to **EventTracker manager** web interface.

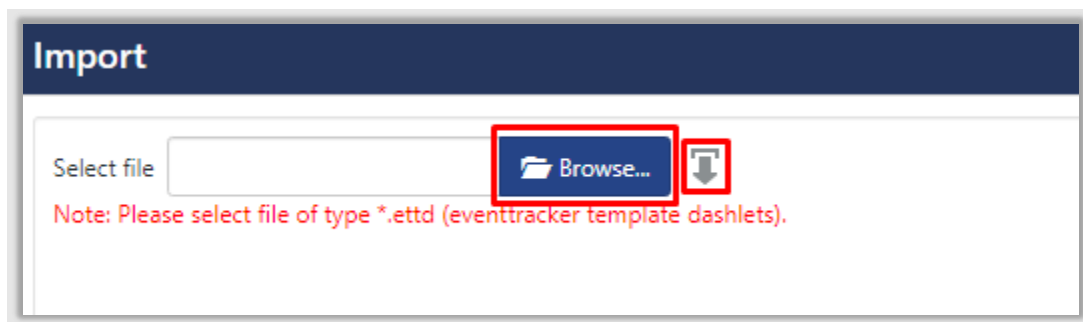
1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.



2. Click the **Template** tab and then click the **Import Configuration** button.

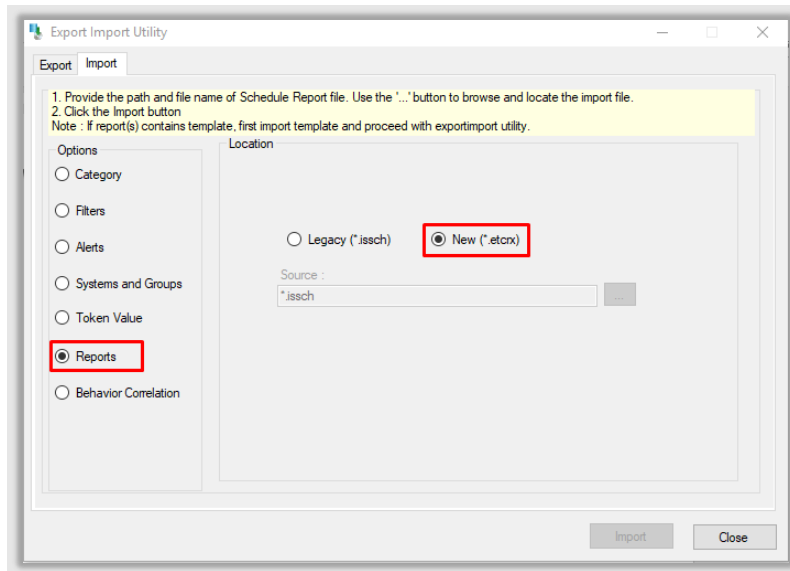


3. Click **Browse** and navigate to the Knowledge Packs folder (type %et_install_path%\Knowledge Packs in navigation bar) where “.ettd”, e.g., “Token Templates_Extreme Network Access Control .ettd” file is located. Wait for few seconds, as templates will be loaded. After you see the templates, click desired template, and click **Import** button.

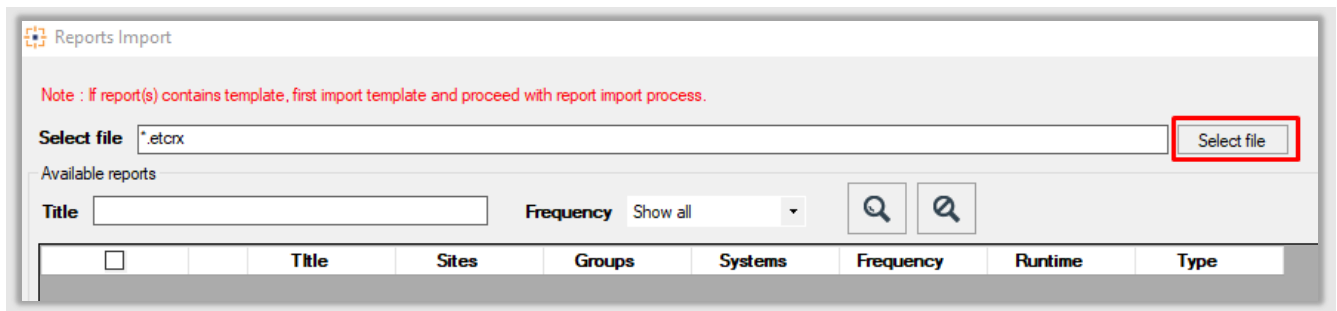



5.3 Reports

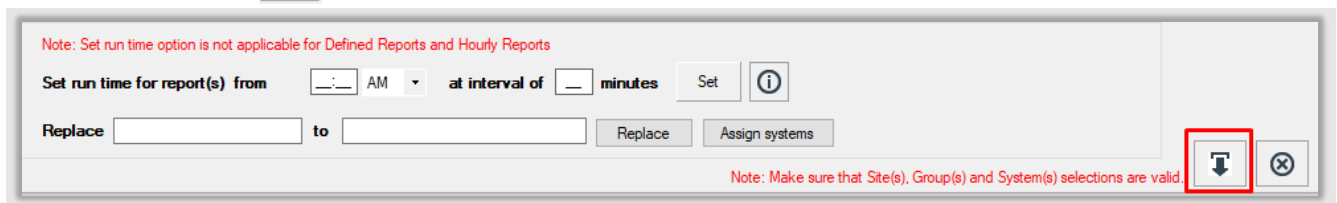
1. In EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Then, click **Reports** option, and Choose **New (*.etcrx)**:



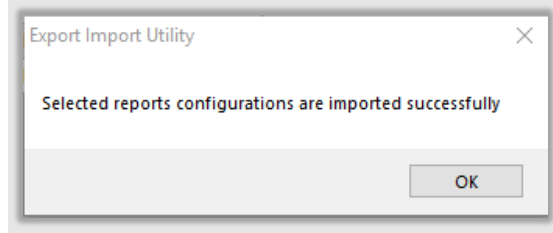
- Once you have selected **New (*.etcrx)**, a new pop-up window appears. Click on the **Select File** button and navigate to the file path with a file having the extension **“.etcrx”**, e.g., **Reports_Extreme Network Access Control .etcrx**.



- Wait while reports are being populated in below tables. Now, select all the relevant reports and then click **Import**  button:

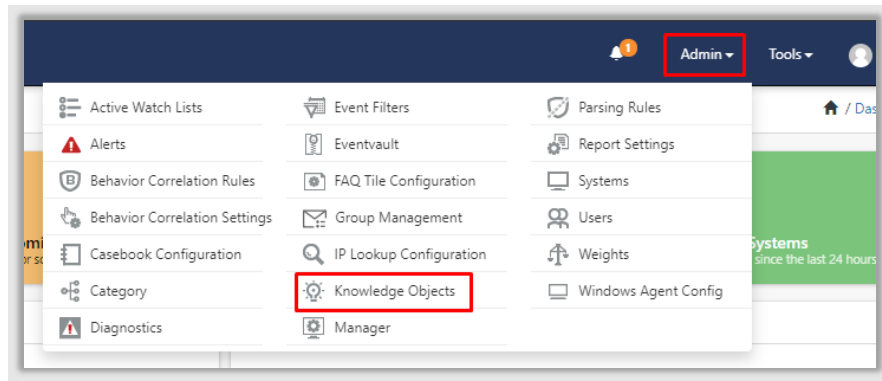


- EventTracker displays a success message:

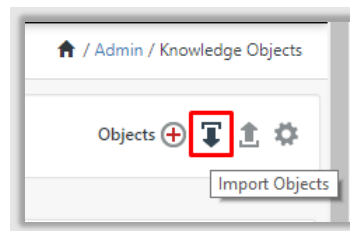


5.4 Knowledge Object

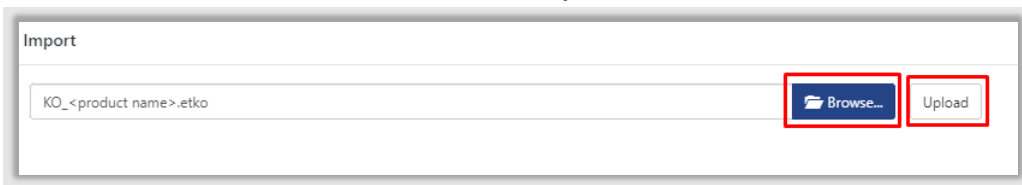
1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager page.



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



3. A pop-up box appears, click **Browse** in that and navigate to knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) with the extension **".etko"**, e.g., **KO_Extreme Network Access Control .etko** and then click **Upload**.

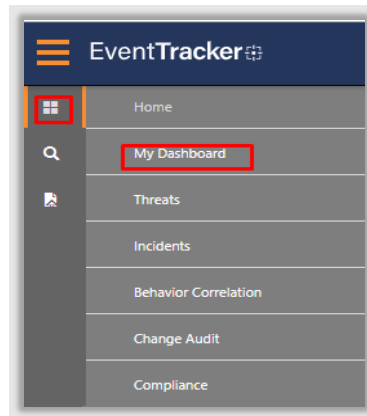


- List of available knowledge object will appear. Select the relevant files and click on **Import** button.

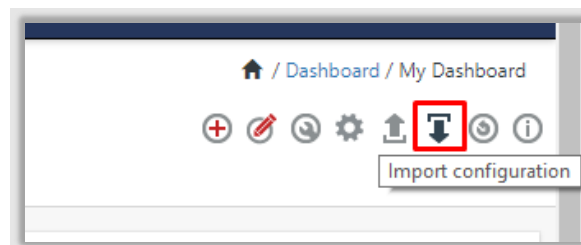


5.5 Dashboard

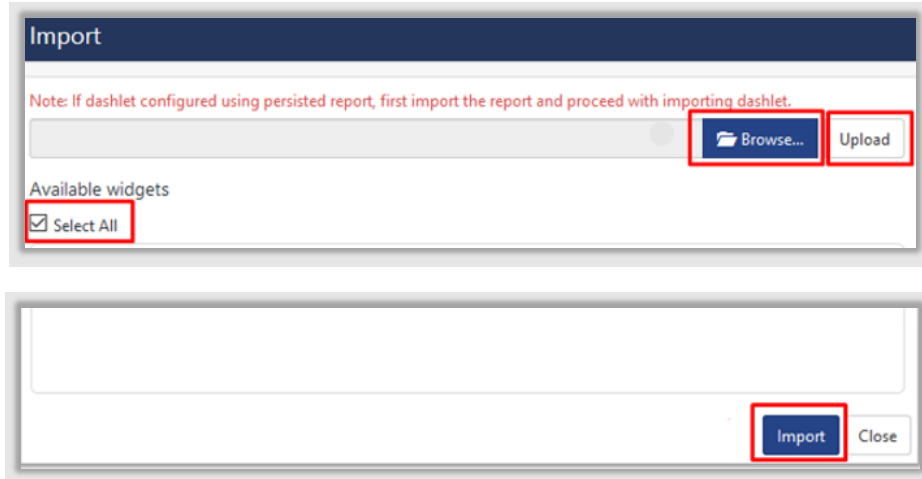
- Login to **EventTracker**.
- Navigate to **Dashboard** → **My Dashboard**.



- In **My Dashboard**, Click on **Import Button**:



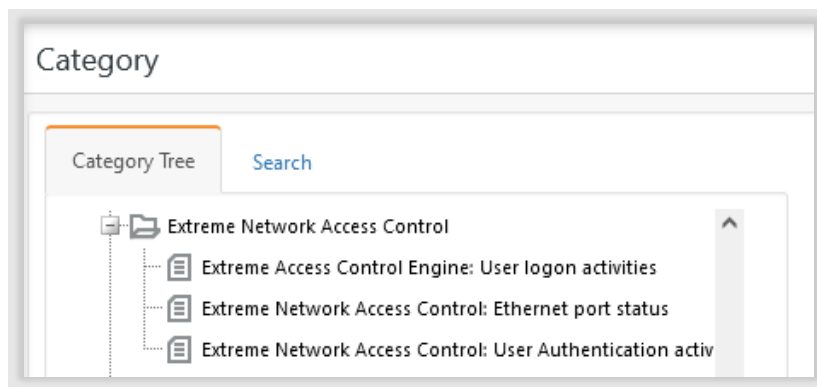
- Select the **browse** button and navigate to Knowledge Pack folder (type `%et_install_path%\Knowledge Packs` in navigation bar) where `.etwd`, e.g., **Dashboards_Extreme Network Access Control .etwd** is saved and click on **Upload** button.
- Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click on **Import** Button.



6. Verifying Extreme Network Access Control Knowledge Pack in EventTracker

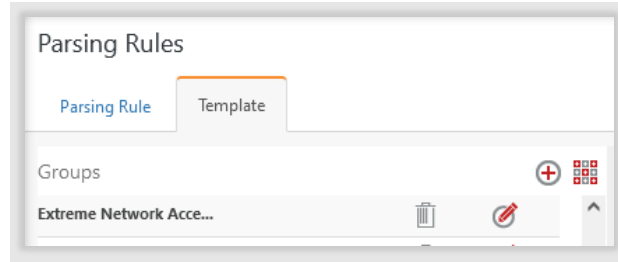
6.1 Categories

1. Login to **EventTracker**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Extreme Network Access Control** group folder to view the imported categories.



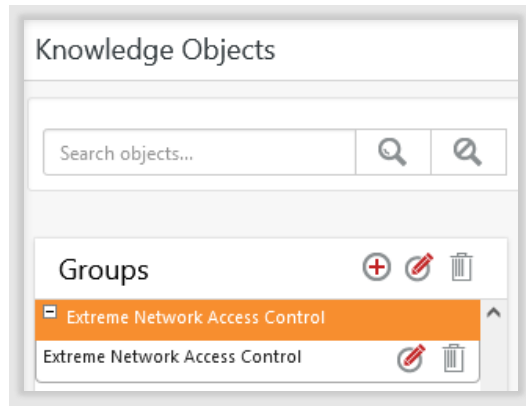
6.2 Token Value

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Template**.
2. In the **Template** tab, click on the **Extreme Network Access Control** group folder to view the imported Token Values.



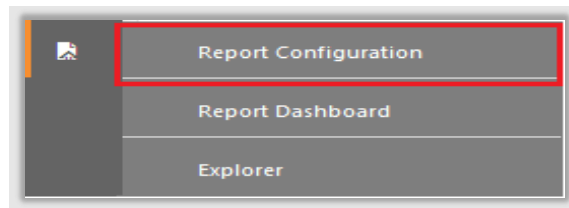
6.3 Knowledge Objects

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

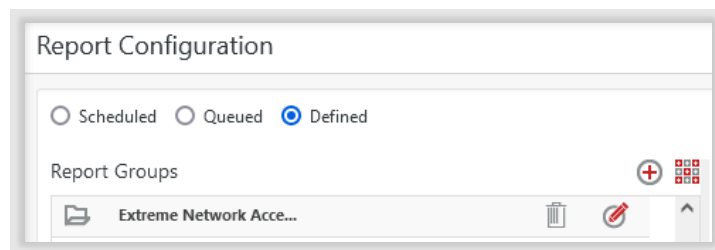


6.4 Reports

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

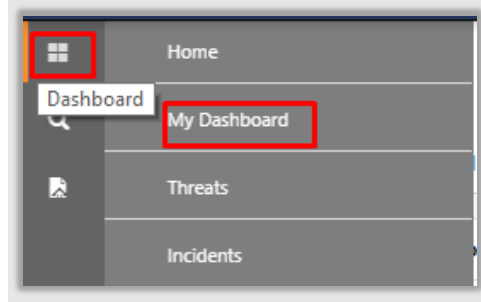


2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Extreme Network Access Control** group folder to view the imported reports.

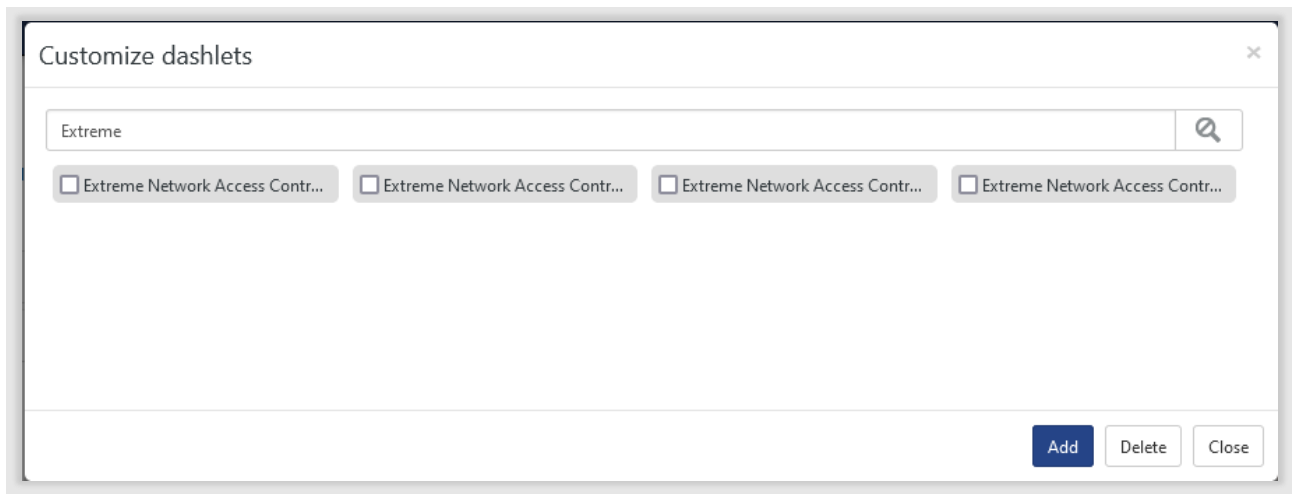
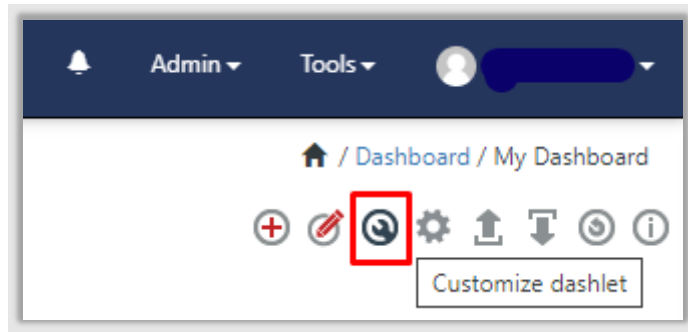


6.5 Dashboard

1. In the **EventTracker** web interface, Click on Home Button  and select **My Dashboard**.



2. Select **Customize daslets**  and type **Ubiquiti** in the search bar.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's [EventTracker](#) cyber threat protection platform provides SIEM, end protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's [BranchSDO](#) delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations.

Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit [netsurion.com](https://www.netsurion.com) or follow us on [Twitter](#) or [LinkedIn](#). Netsurion is #19 among [MSSP Alert's 2020 Top 250 MSSPs](#).

Contact Us

Corporate Headquarters

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

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)

EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)

EventTracker Essentials SOC: 877-333-1433 (Option 4)

EventTracker Software Support: 877-333-1433 (Option 5)

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