Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Ubiquiti Access Points with EventTracker

EventTracker v9.x and above

Publication Date:

July 15, 2021

Abstract

This guide provides instructions to configure Ubiquiti UniFi controller to forward Ubiquiti access points logs via syslog. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Ubiquiti access points logs.

Scope

The configuration details in this guide are consistent with EventTracker version v 9.x or above and UAP/USW Firmware 3.7.x and above.

Audience

Administrators who are assigned the task to monitor Ubiquiti access points events using EventTracker.

Table of Contents

1. Overview

Ubiquiti UniFi Access Points provide high-performance Wi-Fi. It is a scalable enterprise access point solution designed to be easily deployed and managed. Ubiquiti Access Points are well managed through Ubiquiti UniFi Controller, which is a wireless network management software solution.

EventTracker helps to monitor events from UniFi Access Point via syslog. EventTracker reports, alerts, and dashboards will help you to analyze the activity logs, such as MAC association, MAC disassociation, connection failed from unknown MAC, etc.

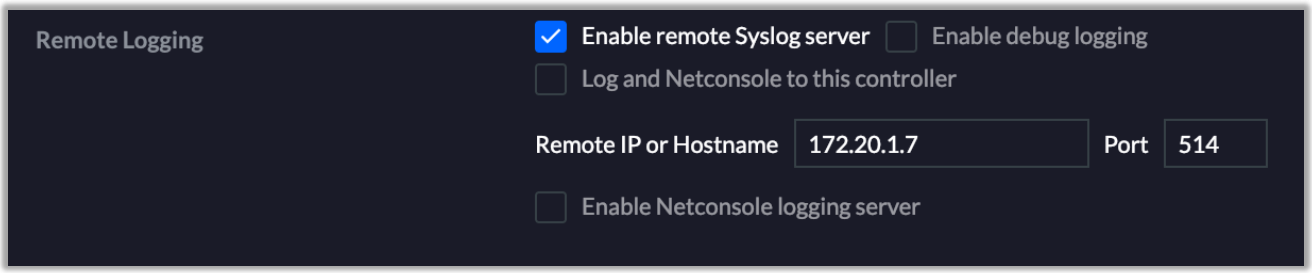
2. Prerequisites

- Admin access to UniFi Controller platform.
- EventTracker server IP address.
- EventTracker server port. E.g. 514.

3. Configuring UniFi Controller

3.1 Enabling Syslog/ Remote Logging.

1. Log in to the UniFi Controller's web interface.
2. Navigate to **Settings > Site**.
3. Navigate to the **Remote Logging** section.
4. Select the checkbox beside **Enable remote syslog server**. Leave the Enable debug logging box unchecked.
5. In the **Remote IP or Hostname**, enter the EventTracker server IP address.
6. In **Port** field, enter the syslog port for EventTracker server, e.g., 514.
7. Click **Apply** changes.



4. System Licensing

Systems are created for as many access points reporting to UniFi controller. The system name format is as follow:

<AP-IP-address>-syslog. e.g., 172.16.12.113-syslog

5. 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 Ubiquiti Access points.

5.1 Alerts

- **Ubiquiti AP - Failed MAC associations** – This alert is triggered when EventTracker receives an event from Ubiquiti flagged as "Probe blocked".

5.2 Reports

- **Ubiquiti AP - Failed MAC Associations** – This report is a summary of failed MAC associations to any access points which is generally flagged as "Probe blocked". It contains key field, such as log datetime, destination MAC address, failure reason, etc.

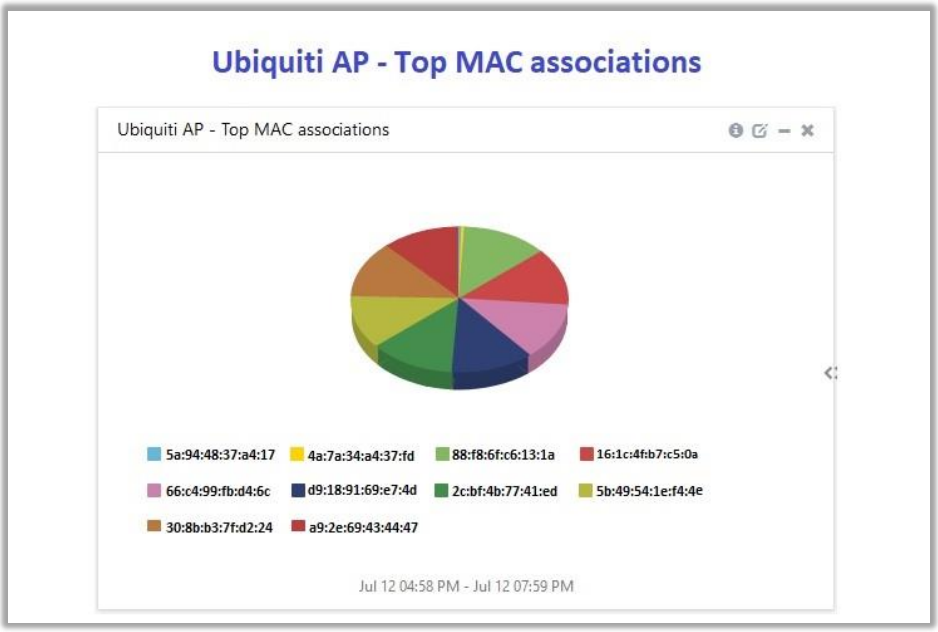
LogTime	Association Status	Auth Type	Device MAC	Device Model	Device Version	Event ID	Event Type	Message Type	Reason	Session Duration	Source MAC
7/6/2021 18:40	2	ath1	b4fbe46e7b8a	U7PG2	v4.0.80.10875	1	failure	STA_ASSOC_TRACKER	ACL	2979281.306	34:01:01:83:b9:cd
7/6/2021 18:40	2	ath0	b4fbe46e7bff	U7PG2	v4.0.80.10875	1	failure	STA_ASSOC_TRACKER	ACL	2980340.429	34:01:01:83:b9:cd
7/6/2021 18:40	2	ath8	b4fbe46e7b8a	U7PG2	v4.0.80.10875	1	failure	STA_ASSOC_TRACKER	ACL	2979283.929	34:01:01:83:b9:cd
7/6/2021 18:40	2	ath7	b4fbe46e7b8a	U7PG2	v4.0.80.10875	1	failure	STA_ASSOC_TRACKER	ACL	2979283.929	34:01:01:83:b9:cd

- **Ubiquiti AP - MAC Associations Activities** – MAC association activities include events in which destination MAC addresses are flagged as "associated" or "disassociated". This includes key information, such as log datetime, destination MAC address, source access points MAC address, access point version number, and association status.

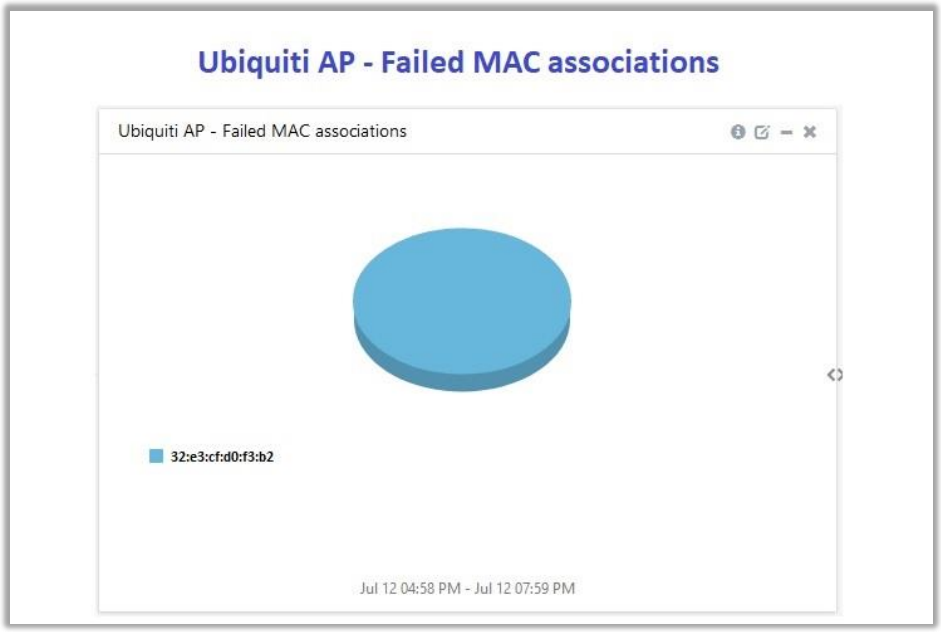
LogTime	Computer	Device MAC	Device Version	Device Model	Source MAC	Association Status
44383.77781	UBIQUITI~NTPLDTBLR48-SYSLOG	b4fbe4e5a21b	v4.0.80.10875	U7LR	3a:6d:8b:f6:4e:53	associated
44383.77781	UBIQUITI~NTPLDTBLR48-SYSLOG	f09fc23be84d	v4.0.80.10875	U7PG2	9a:f2:c7:69:c0:d9	disassociated
44383.77781	UBIQUITI~NTPLDTBLR48-SYSLOG	f09fc23be84d	v4.0.80.10875	U7PG2	9a:f2:c7:69:c0:d9	disassociated
44383.77781	UBIQUITI~NTPLDTBLR48-SYSLOG	b4fbe4e5a21b	v4.0.80.10875	U7LR	3a:6d:8b:f6:4e:53	associated

5.3 Dashboards

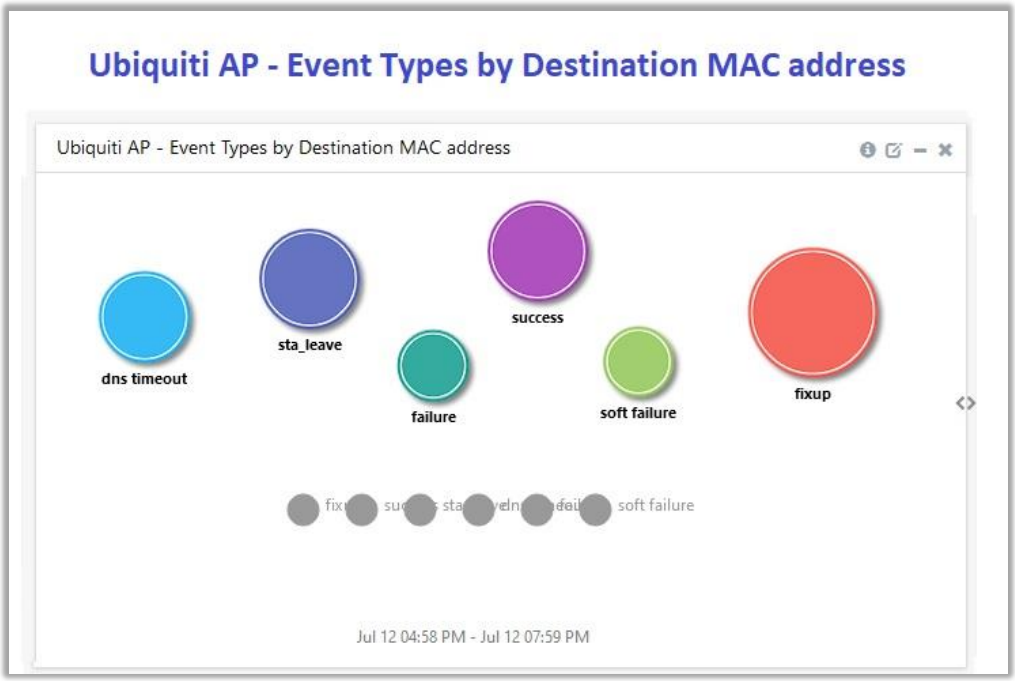
- **Ubiquiti AP - Top MAC associations**



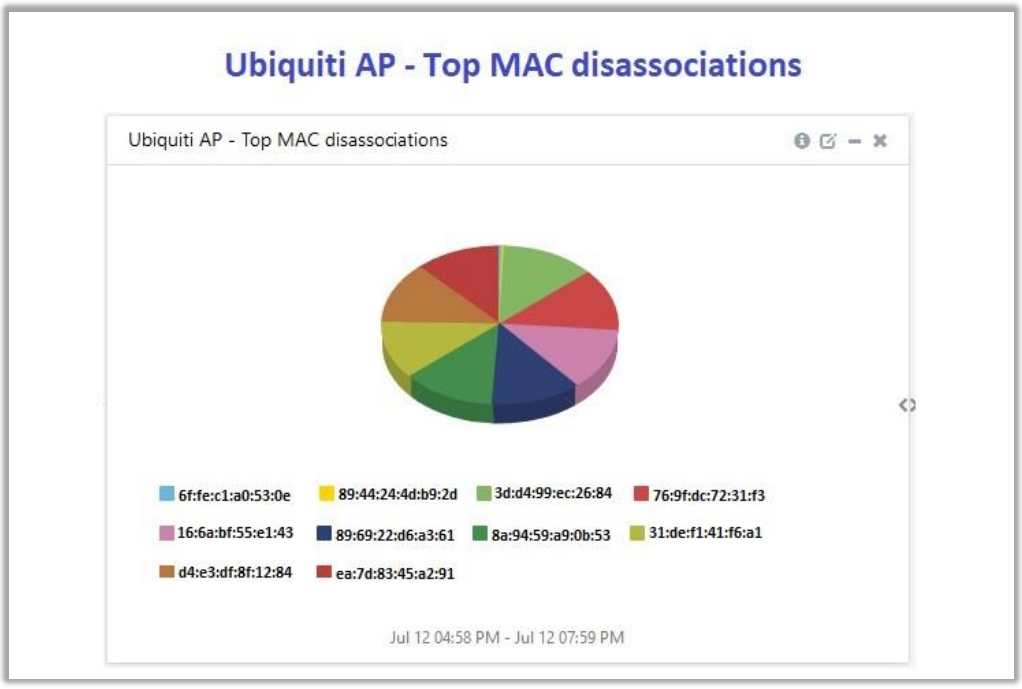
- **Ubiquiti AP - Failed MAC associations**



- **Ubiquiti AP - Event Types by Destination MAC address**



- **Ubiquiti AP: Top MAC disassociations.**

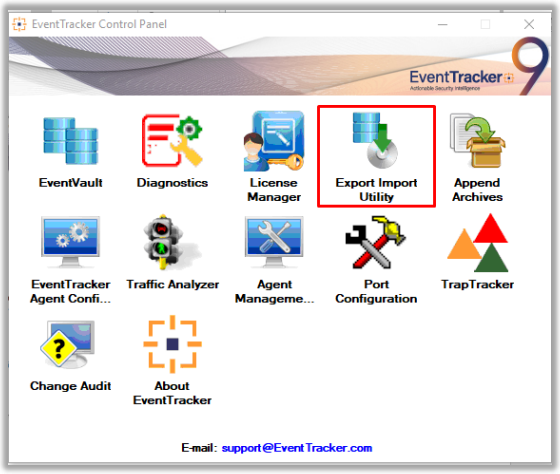


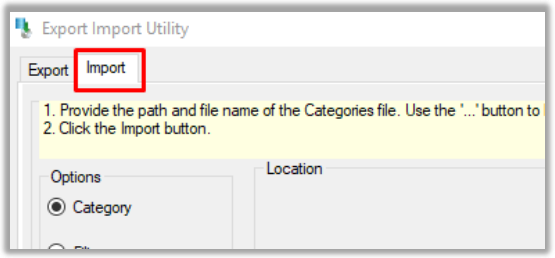
6. Importing Ubiquiti Access Point Knowledge Pack into EventTracker

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**.

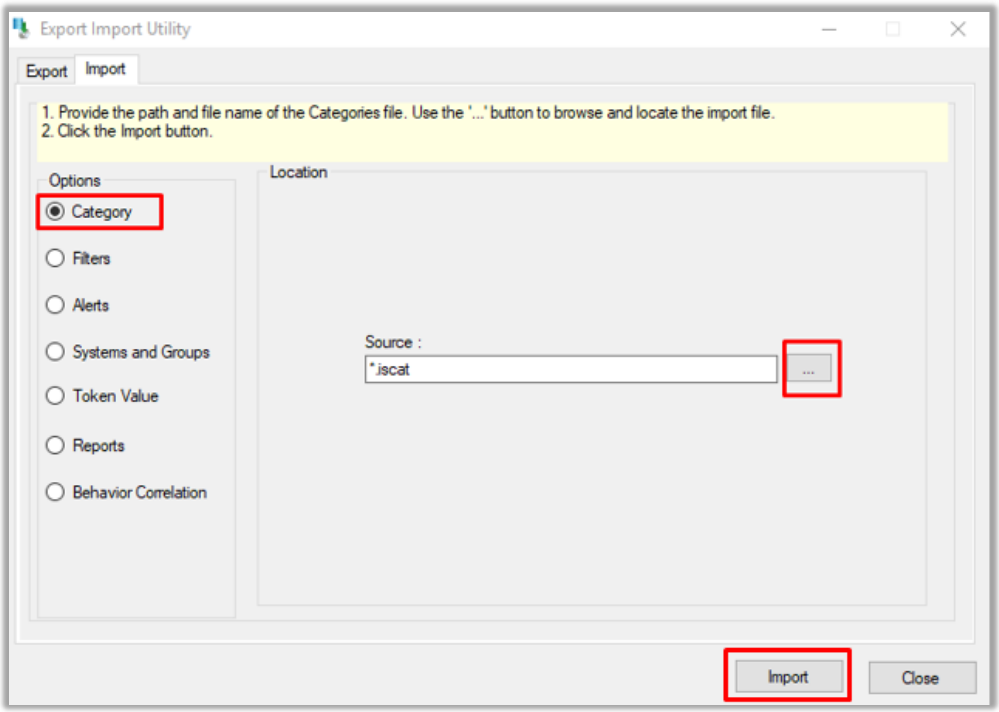




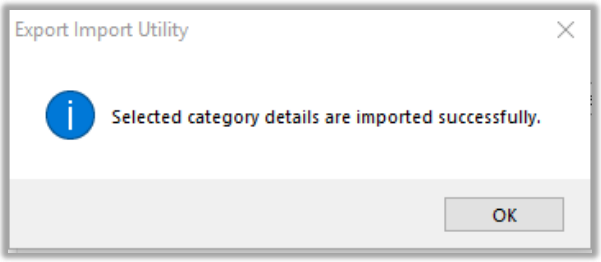
3. Click the **Import** tab.

6.1 Categories

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



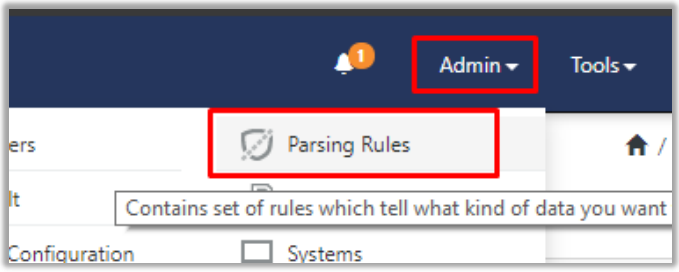
EventTracker displays a success message:



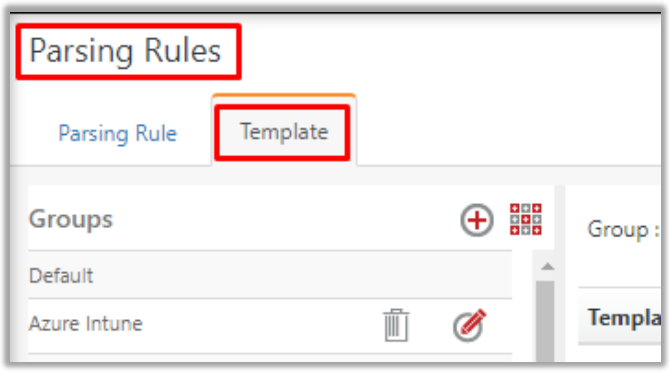
6.2 Token Template

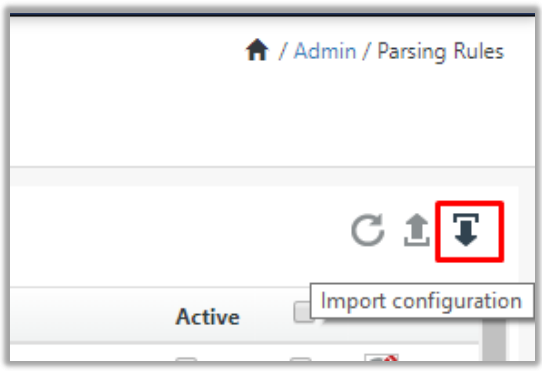
For importing **Token Template**, navigate to **EventTracker manager** web interface.

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

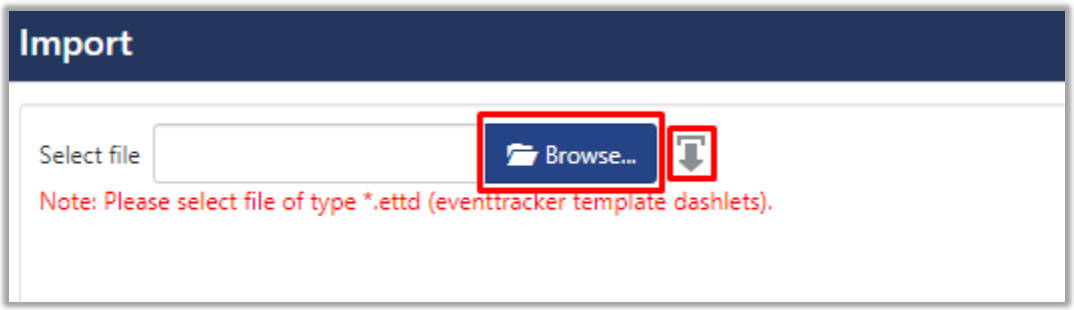


2. Click the **Template** tab and then click the **Import Configuration** button.



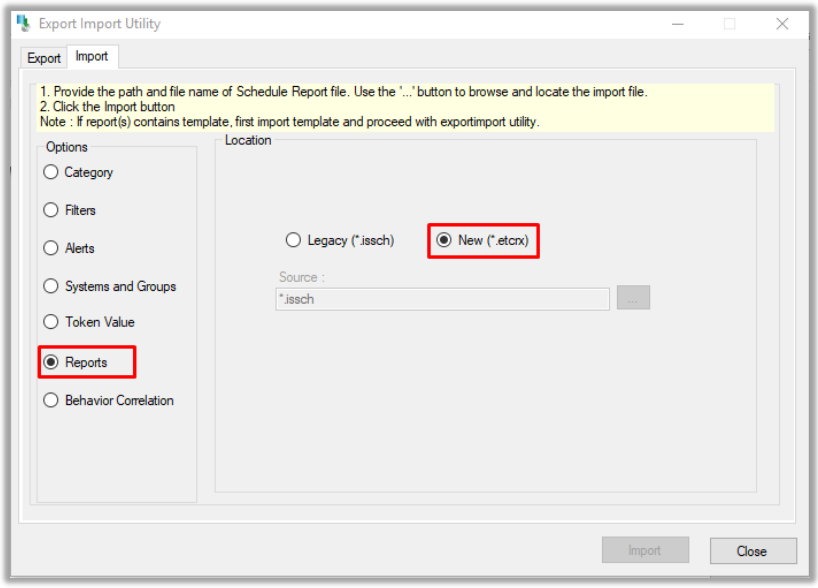


3. Click **Browse** button and navigate to the Knowledge Packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where "**.ettd", e.g. "Token Templates_Ubiquiti Access Point.ettd** file is located. Wait for few seconds, as templates will be loaded. After the templates display, click desired template, and click **Import** button:

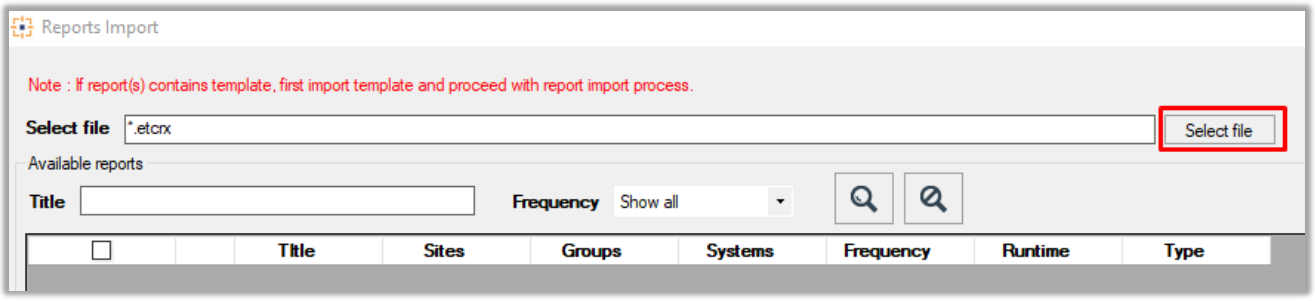


6.3 Reports

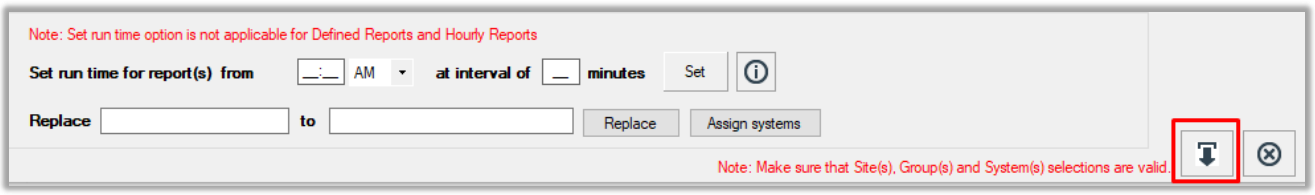
1. In EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Then, click **Reports** option, and Choose **New (*.etcrx)**:



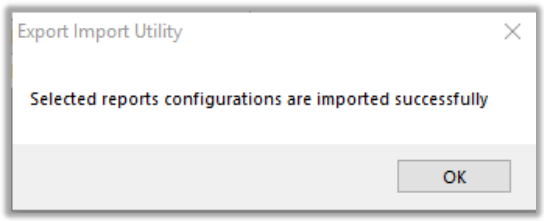
2. After you have selected **New (*.etcrx)**, a new pop-up window will appear. Click on the **Select File** button and navigate to the file path with a file having the extension "**.etcrx", e.g., Reports_ Ubiquiti Access Point.etcrx.**



3. Wait while reports are being populated in below tables. Select all the relevant reports and then click **Import** button:

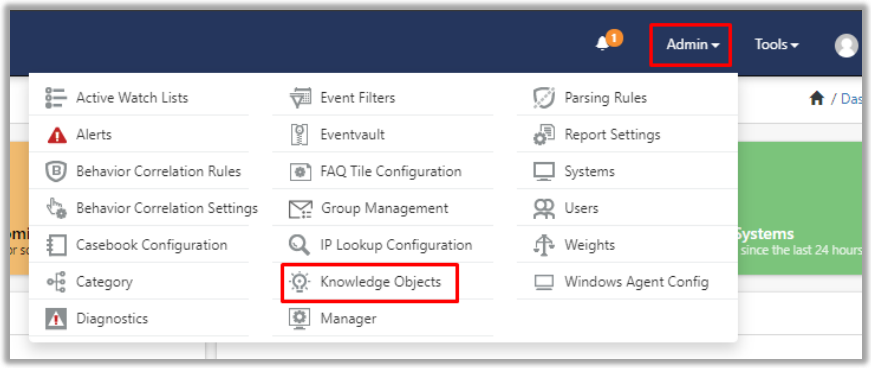


4. EventTracker displays a success message:

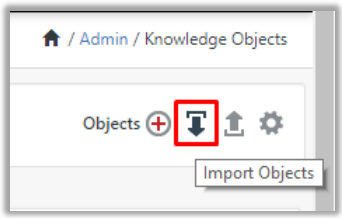


6.4 Knowledge Object

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



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

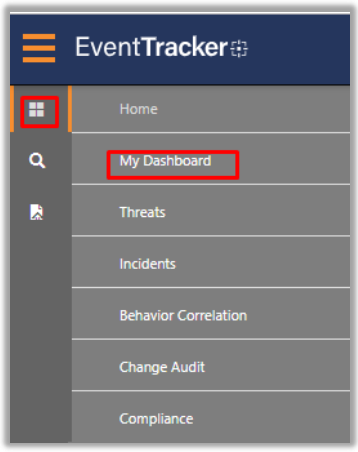


3. A pop-up box appears, click Browse in that and navigate to Knowledge Packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) with the extension **".etko", e.g., KO_Ubiquiti Access Point.etko** and then click **Upload**.

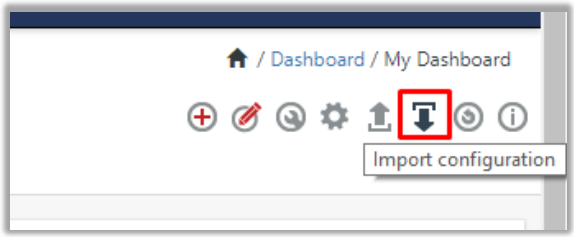
4. List of available Knowledge Object will appear. Select the relevant files and click on **Import** button:

6.5 Dashboard

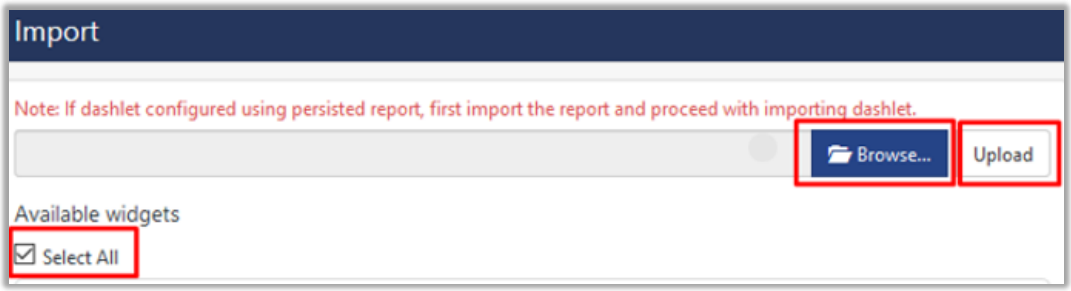
1. Login to **EventTracker**.
2. Navigate to **Dashboard → My Dashboard**.



3. In **My Dashboard**, Click on **Import Button**:



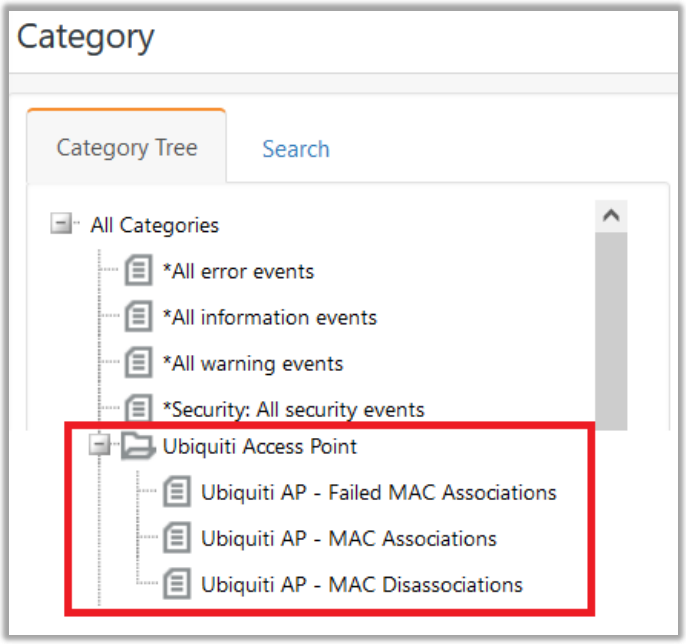
4. Select the **browse** button and navigate to Knowledge Pack folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where **.etwd**, **e.g., Dashboards_Ubiquiti Access Point.etwd** is saved and click **Upload**.
5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click **Import**.



7. Verifying Ubiquiti Access Point Knowledge Pack in EventTracker

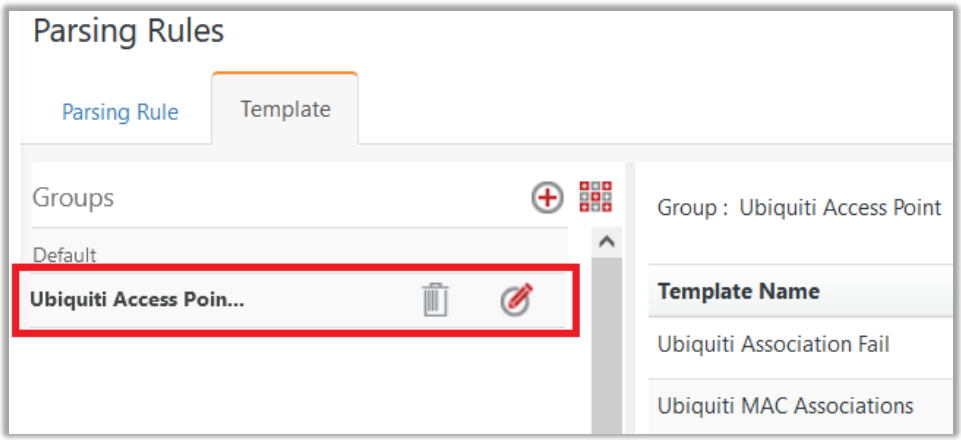
7.1 Categories

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



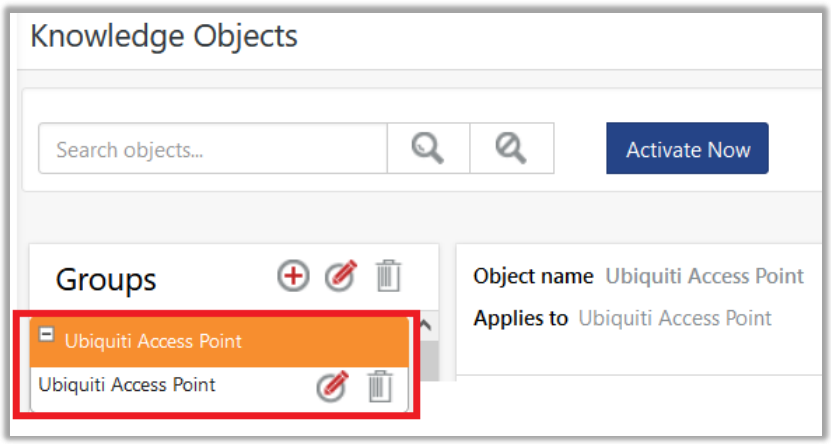
7.2 Token Value

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



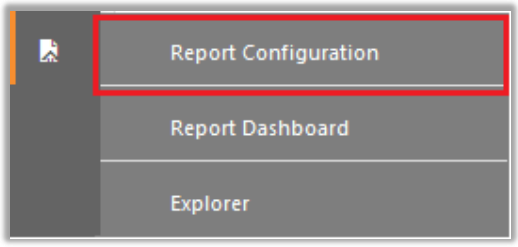
7.3 Knowledge Objects

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

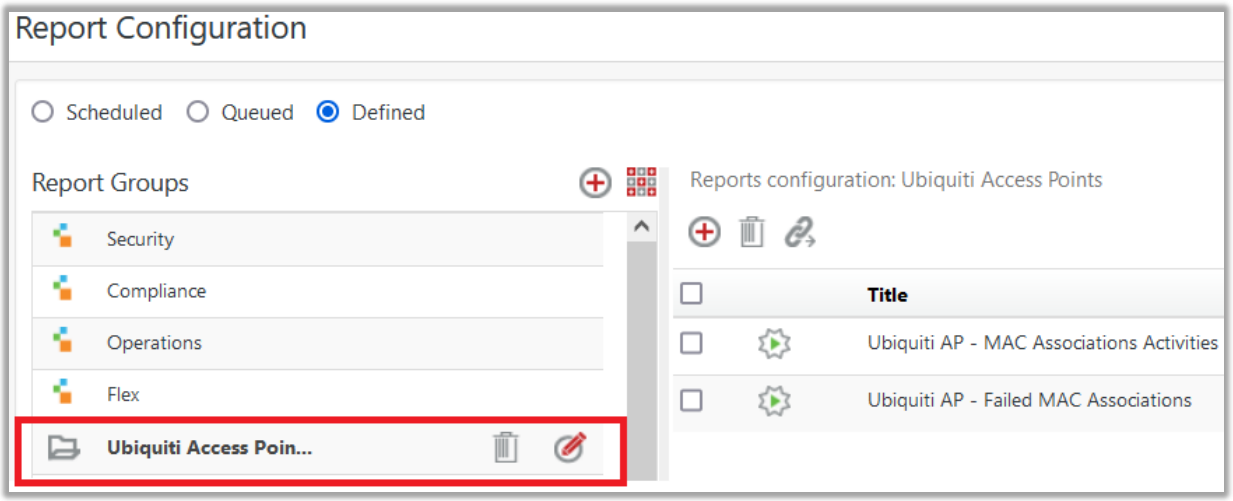


7.4 Reports

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

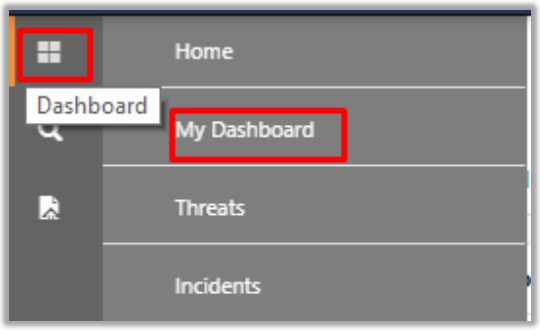


2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Ubiquiti Access Point** group folder to view the imported reports.

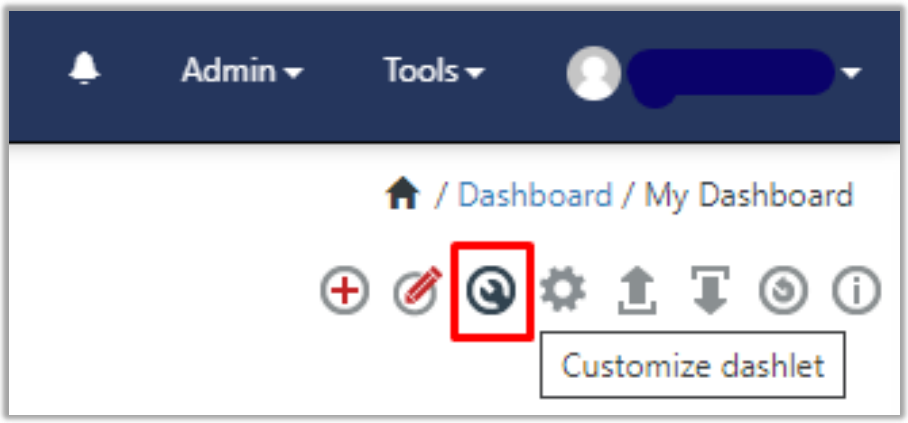


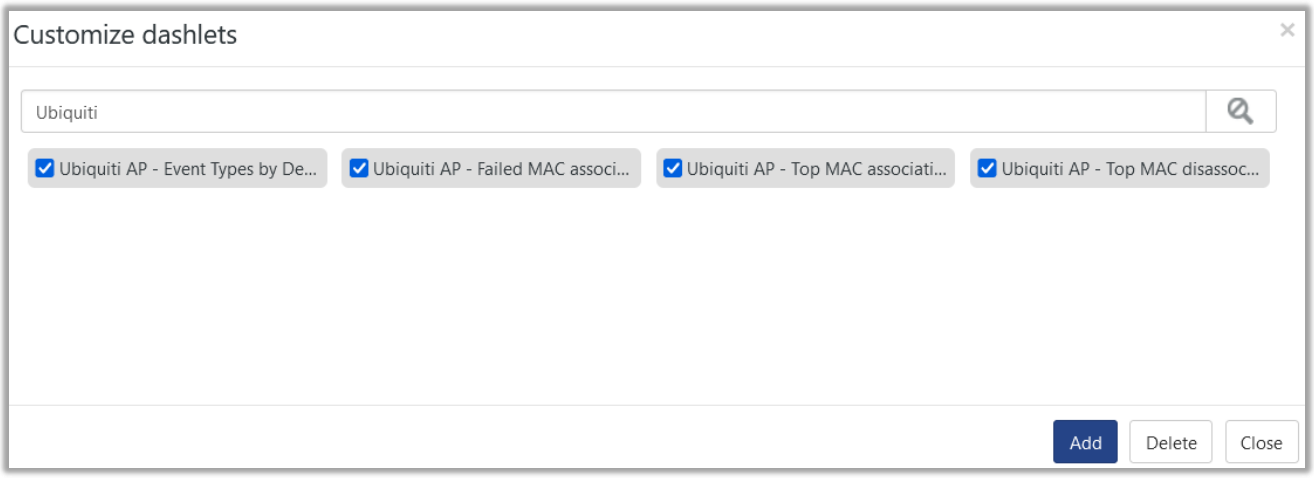
7.5 Dashboard

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, endpoint 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 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