Netsurion™ | EventTracker

ARUBA OS

EventTracker v8.x and above

Publication Date: February 25, 2019

Abstract

This guide provides instructions to configure Aruba OS to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and Aruba OS 6.5 and later.

Audience

Aruba OS users, who wish to forward syslog events to EventTracker manager.

Table of Contents

Abstract 1

Scope 1

Audience 1

Overview 3

Pre-requisite 3

Integration of EventTracker with Aruba OS 3

EventTracker Knowledge Pack (KP) 4

Alert 4

Reports 5

Import Knowledge Pack into EventTracker 5

Category 6

Alerts 7

Knowledge Objects 8

Templates 10

Flex Reports 11

Verify Knowledge Pack in EventTracker 14

Category 14

Alerts 14

Knowledge Object 16

Flex Reports 16

Templates 17

Overview

The Aruba OS operating system for Aruba Mobility Controllers, Mobility Access Switches and access points (APs) perform security and system administration, as well as hardware-based routing, switching, firewall and data encryption capabilities.

EventTracker Enterprise supports Aruba OS, the syslog messages can be forwarded to EventTracker Enterprise and based on events, alerts and reports can be configured into EventTracker.

Pre-requisite

Prior to configuring Aruba OS and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker v8.x should be installed.
- Aruba OS should be installed.
- Port 514 must be opened on Aruba OS.
- Port 514 must not be used by other services of Aruba OS.
- An exception should be added into Windows Firewall on EventTracker machine for Syslog port 514.

Integration of EventTracker with Aruba OS

To configure Aruba OS to forward the log to EventTracker Enterprise:

1. Login to the Aruba Mobility Controller using **Web User Interface**.
2. Navigate to the **Configuration > Management > Logging > Servers** page.
3. To add an **EventTracker Enterprise server**, click **New** in the Logging Servers section.
4. Click **Add** to add the **EventTracker Enterprise server** to the list of logging servers. Ensure that the syslog server is enabled and configured on this host.
5. Click on **Apply** button.
6. To select the types of messages you want to log, select the **Levels** tab.
7. Select the category or subcategory to be logged.

8. To select the severity level for the category or subcategory, scroll to the bottom of the page. Select the level from the Logging Level drop-down menu. Click on **Done** button.

Logging Level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical conditions such as a hard drive error.
Error	Error conditions.
Warning	Warning messages.
Notification	Significant events of a non-critical and normal nature.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

The default logging level for all categories is Warning.

9. Click **Apply** to apply the configuration.

The configuration is complete. Aruba Mobility Controller events are automatically discovered in EventTracker Enterprise. Events forwarded to EventTracker by Aruba OS are displayed on the Log Search tab of EventTracker Enterprise.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; alert, reports, knowledge object can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v8.x and later to support Aruba OS monitoring:

Alert

ArubaOS User authentication failure – This alert will trigger whenever user authentication failure happens.

ArubaOS: Attack detected – This alert will trigger whenever association flood DoS attack is detected, ARP-spoofing is detected.

ArubaOS: License expired – This alert will trigger whenever ArubaOS license is expired.

Reports

ArubaOS - User Authentication Failure -This report provides information related to the user authentication failure and authentication server out of service while serving request.

ArubaOS - Connection failure -This report provides information related to the connection failure with the profile manager.

ArubaOS - Attack detected – This report provides information related to the association flood DoS attack detected, detected ARP-spoofing, system detected MAC spoofing and frame dropped.

ArubaOS - User login failure – This report provides information related to the client authentication failure and User de-authenticated.

ArubaOS - User login success - This report provides information related to the Management user authentication completed successfully.

ArubaOS - DHCP activities - This report provides information related to the DHCP client disabled on the specified VLAN, request, release and decline.

ArubaOS - Connection details - This report provides information related to the Assoc connection success, Dis Assoc flood DoS attack detected and Assoc failure.

ArubaOS - User authentication details – This report provides information related to the user de-authenticated, log indicating that a user has been authenticated.

ArubaOS - Firewall messages – This report provides information related to the A firewall rule with log option as hit, as source IP address, source port, destination IP address, destination port details.

Import Knowledge Pack into EventTracker

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

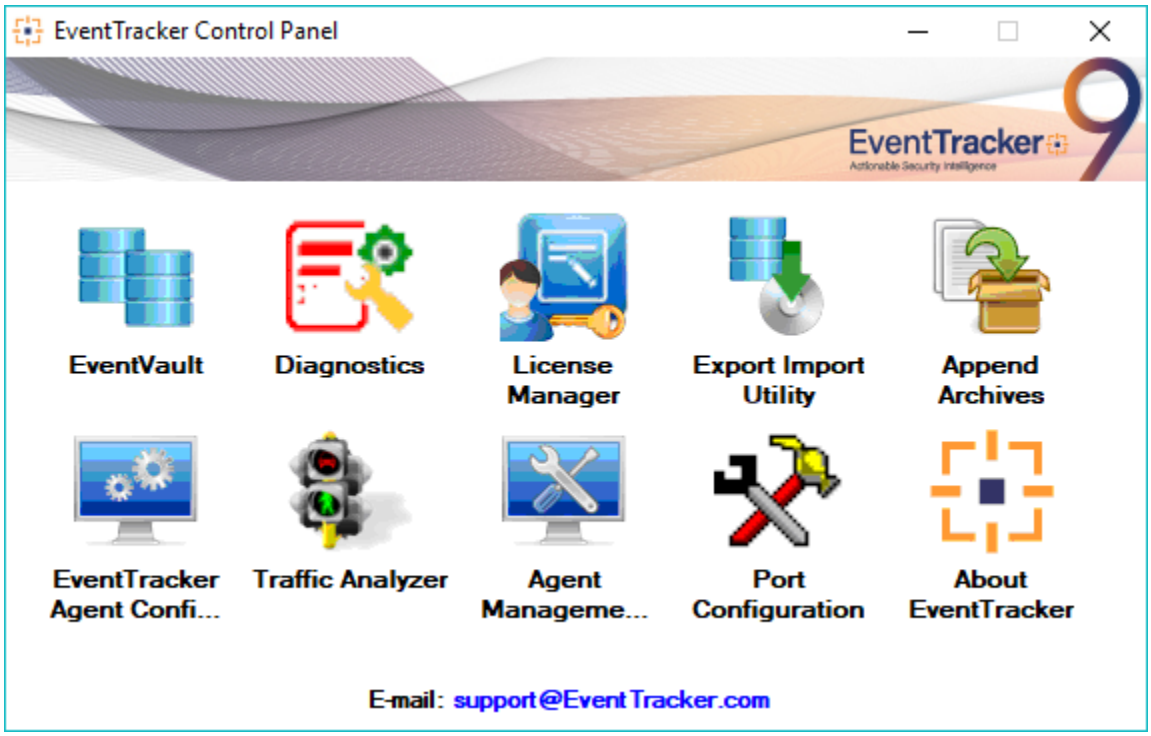

Figure 1

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

Category

1. Click **Category** option, and then click the **browse**  button.

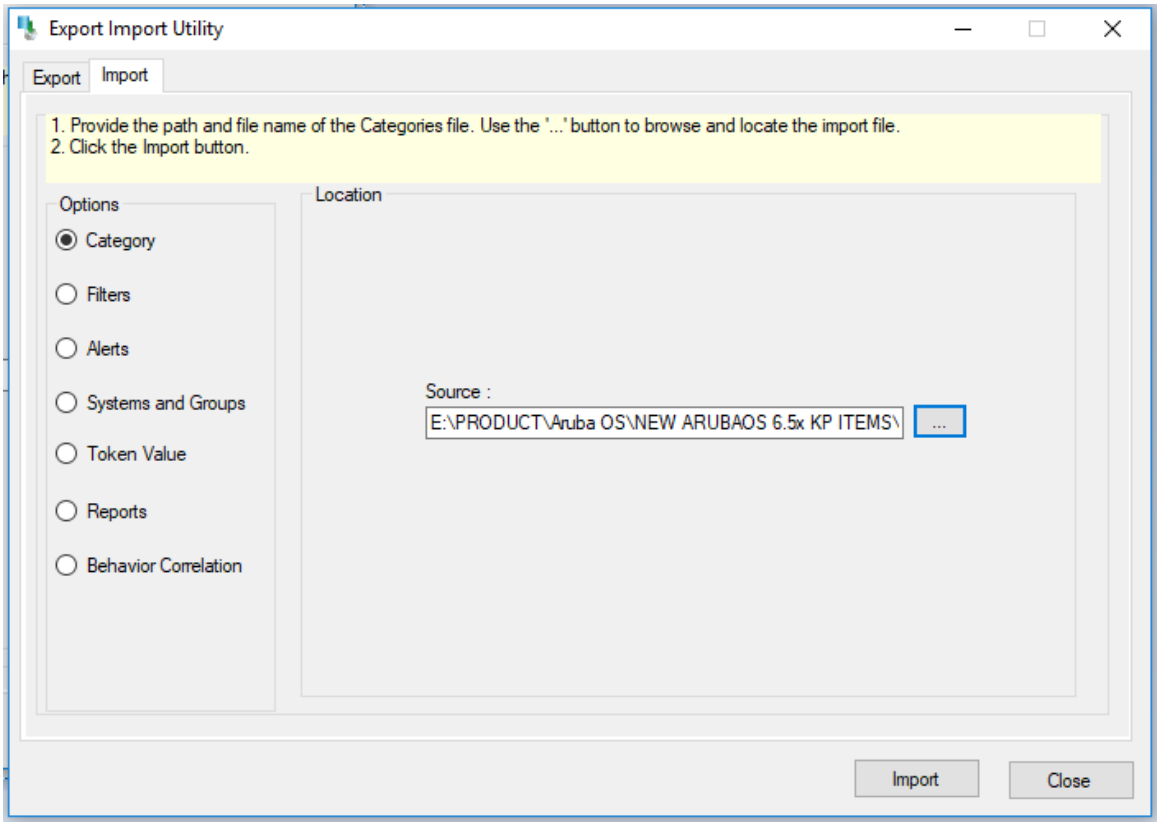

Figure 2

2. Locate **Category_ArubaOS 6.5x.iscat** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.

Figure 3

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

Alerts

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

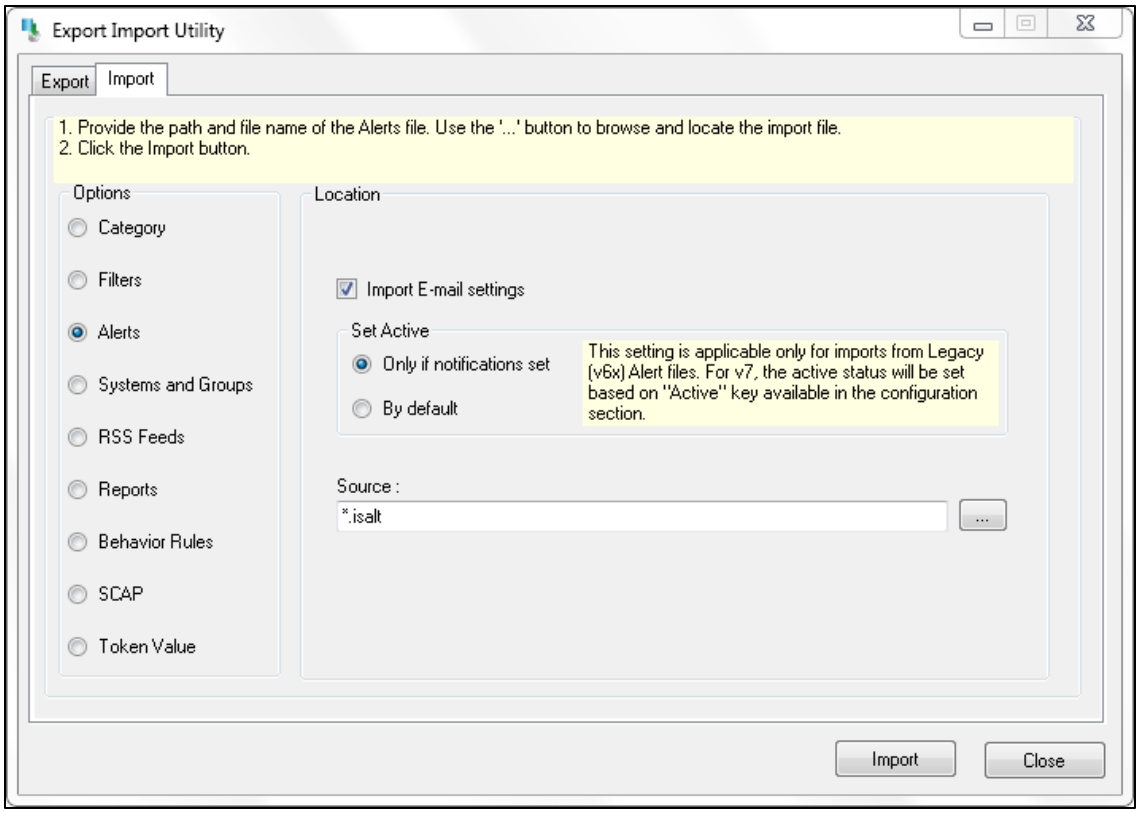

Figure 4

2. Locate **Alerts_ArubaOS 6.5x.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.

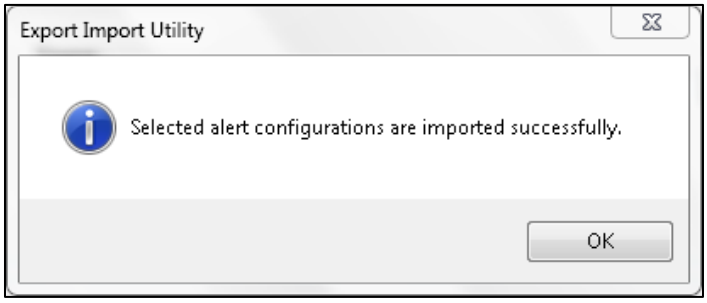

Figure 5

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

Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.
2. Locate the file named **KO_ArubaOS 6.5x.etko**.

Figure 6

3. Now select all the check box and then click on ‘**Import**’ option.

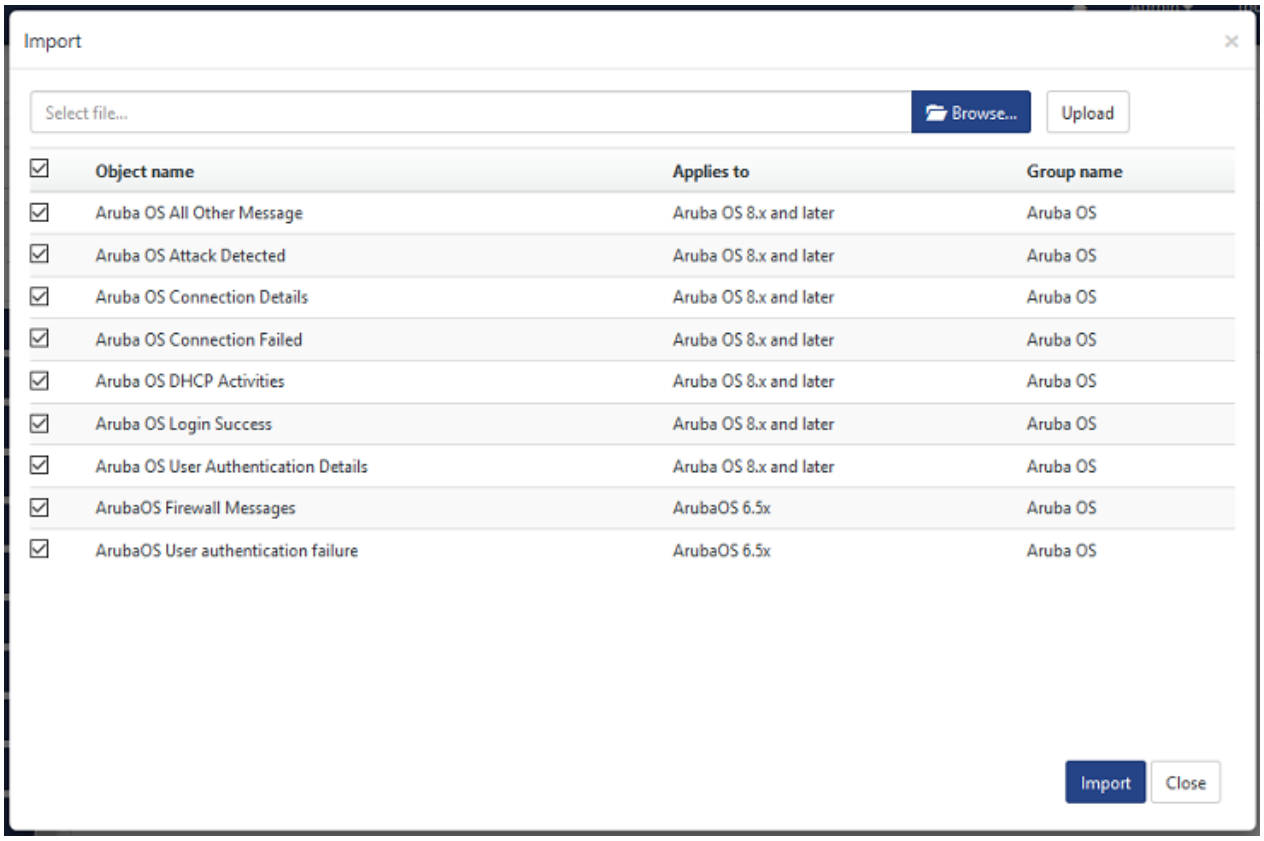

Figure 7

4. Knowledge objects are now imported successfully.

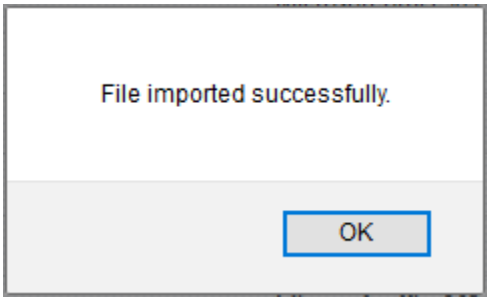

Figure 8

Templates

1. Click **Parsing Rules** option, create group and click Import.
2. Locate the file name **Token_ArubaOS 6.5x.ettd**.

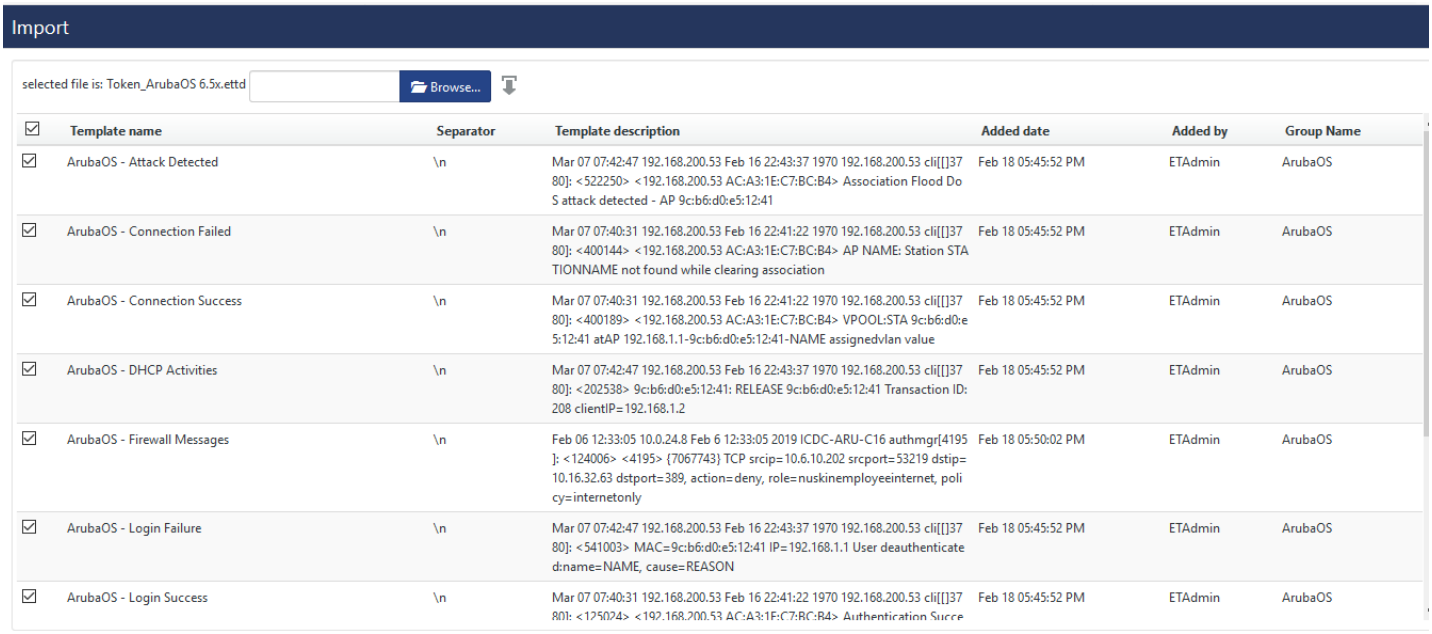

Figure 9

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

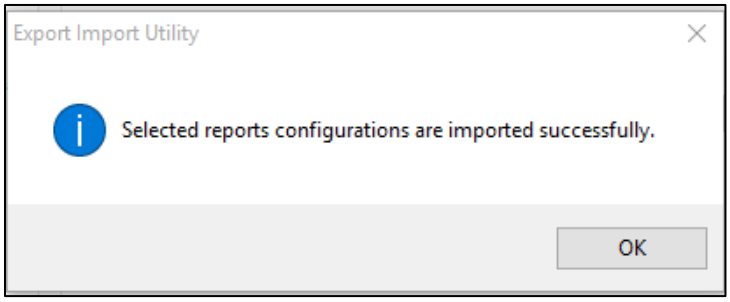

Figure 10

Flex Reports

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

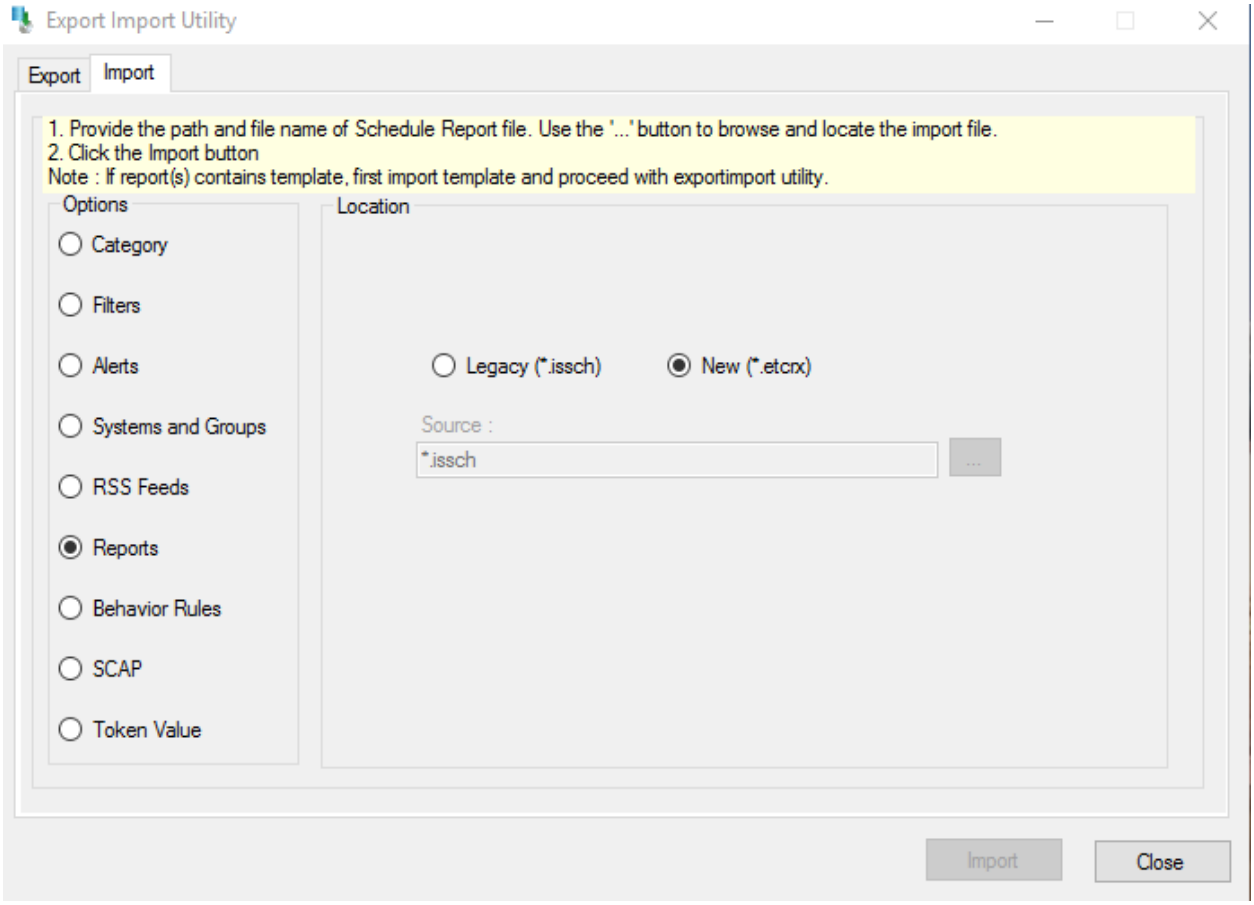

Figure 11

2. Locate the file named **Reports_ArubaOS 6.5x.etcrx** and select all the check box.

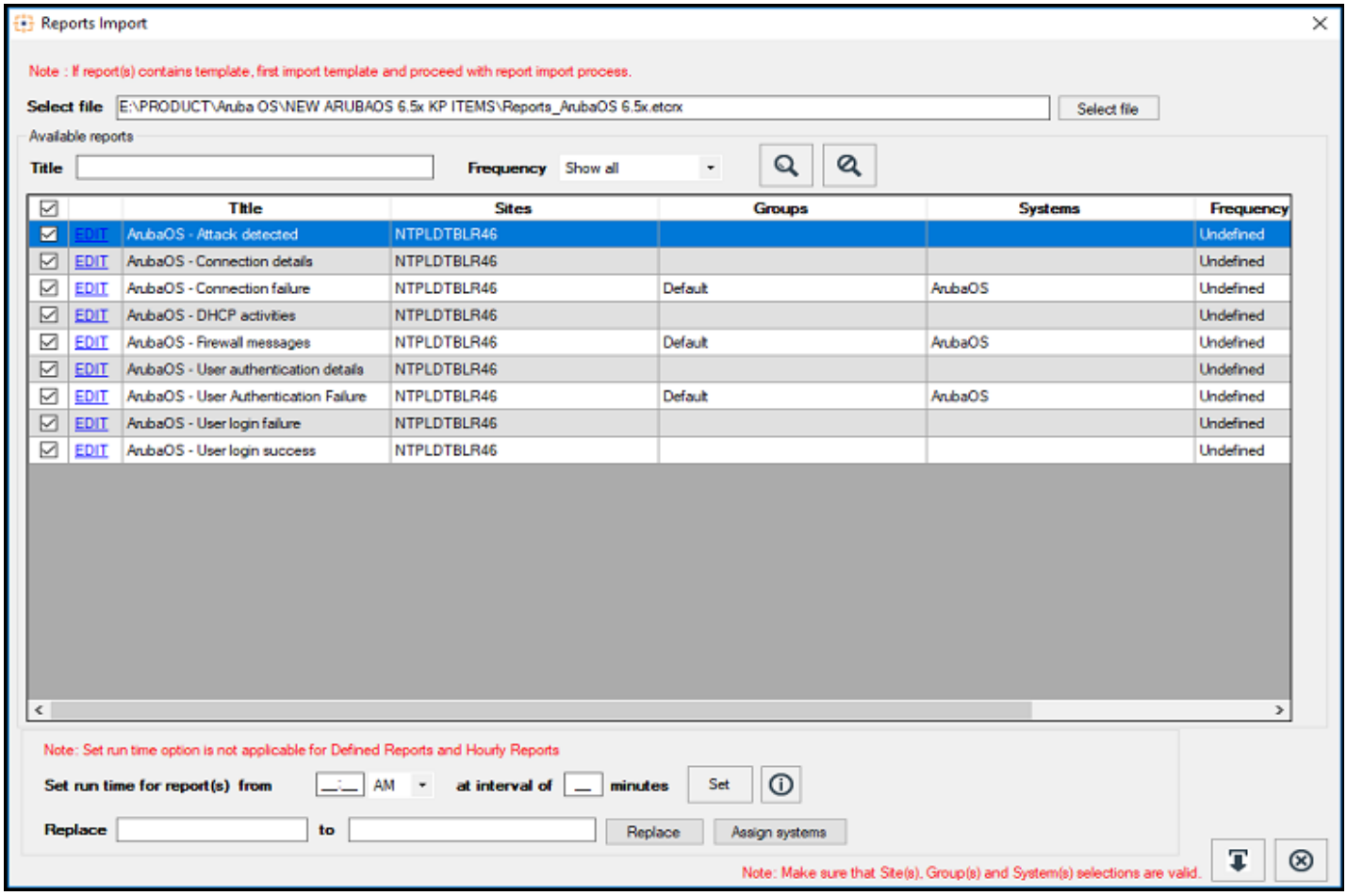

Figure 12

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

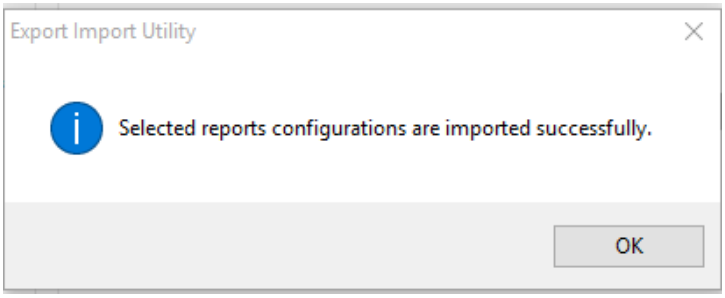

Figure 13

Verify Knowledge Pack in EventTracker

Category

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Category.**

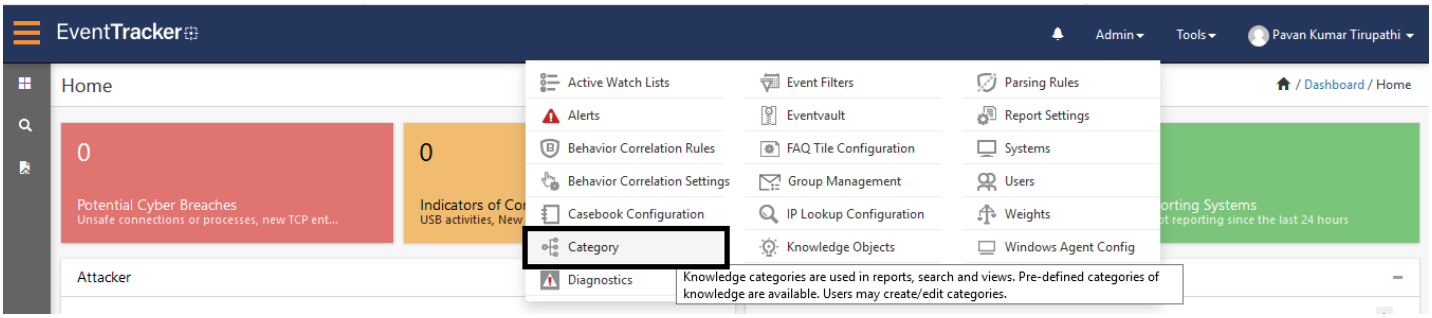

Figure 14

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

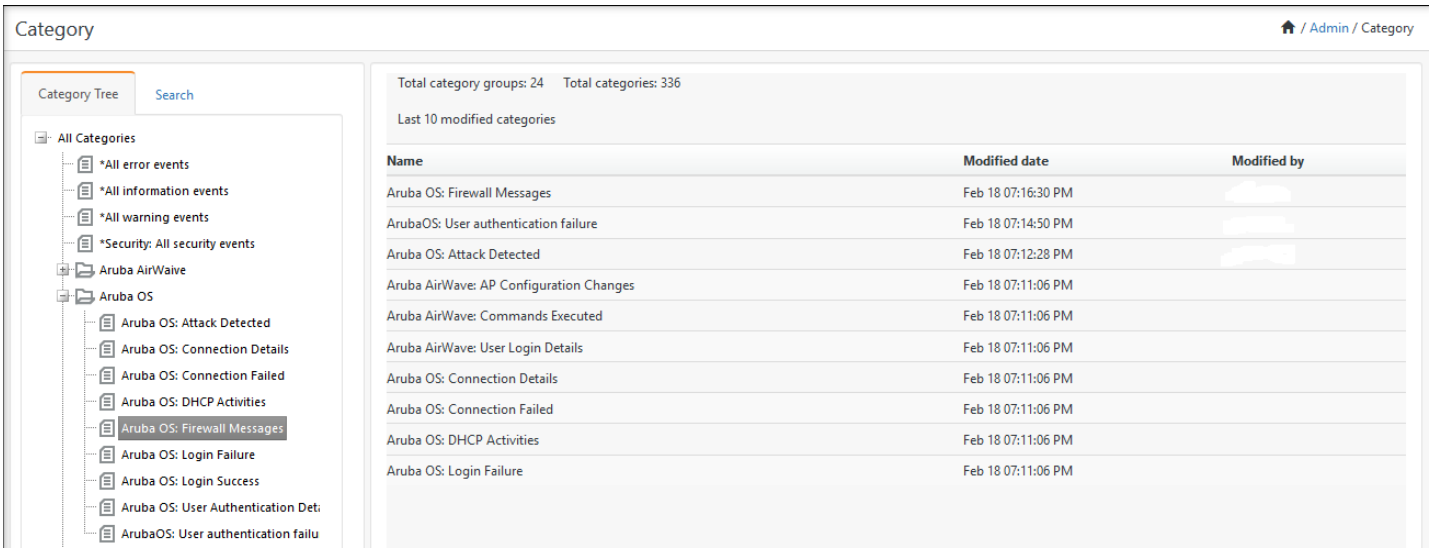

Figure 15

Alerts

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

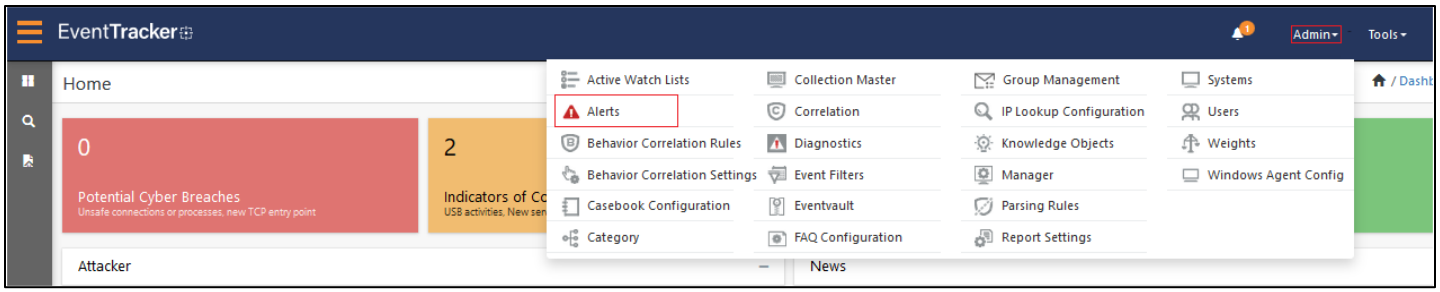

Figure 16

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

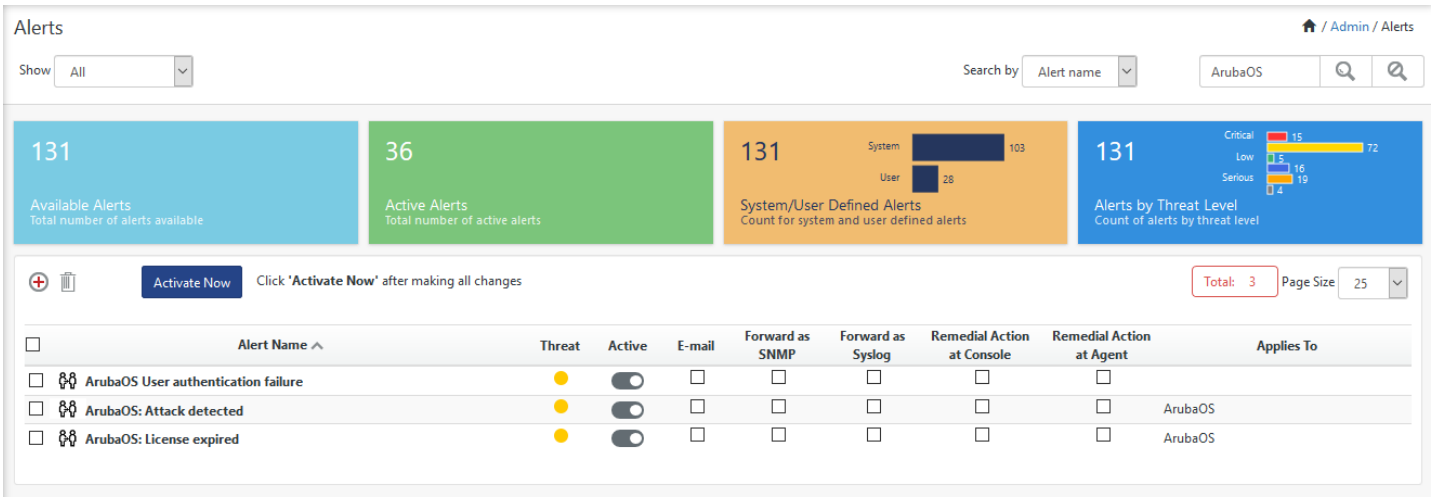

Figure 17

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

   EventTracker displays message box.

Figure 18

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

NOTE: Please specify appropriate **systems** in **Alert configuration** for better performance.

Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Aruba OS** group folder.

Knowledge Object are displayed in the pane.

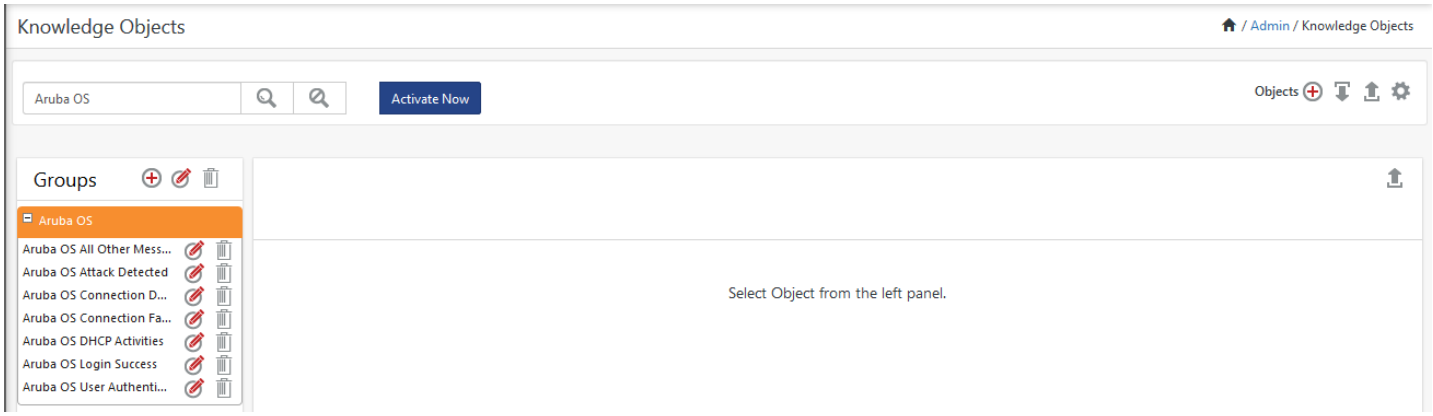

Figure 19

Flex Reports

1. Logon to **EventTracker Enterprise**.
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 **Aruba OS** group folder.

   Reports are displayed in the Reports configuration pane.

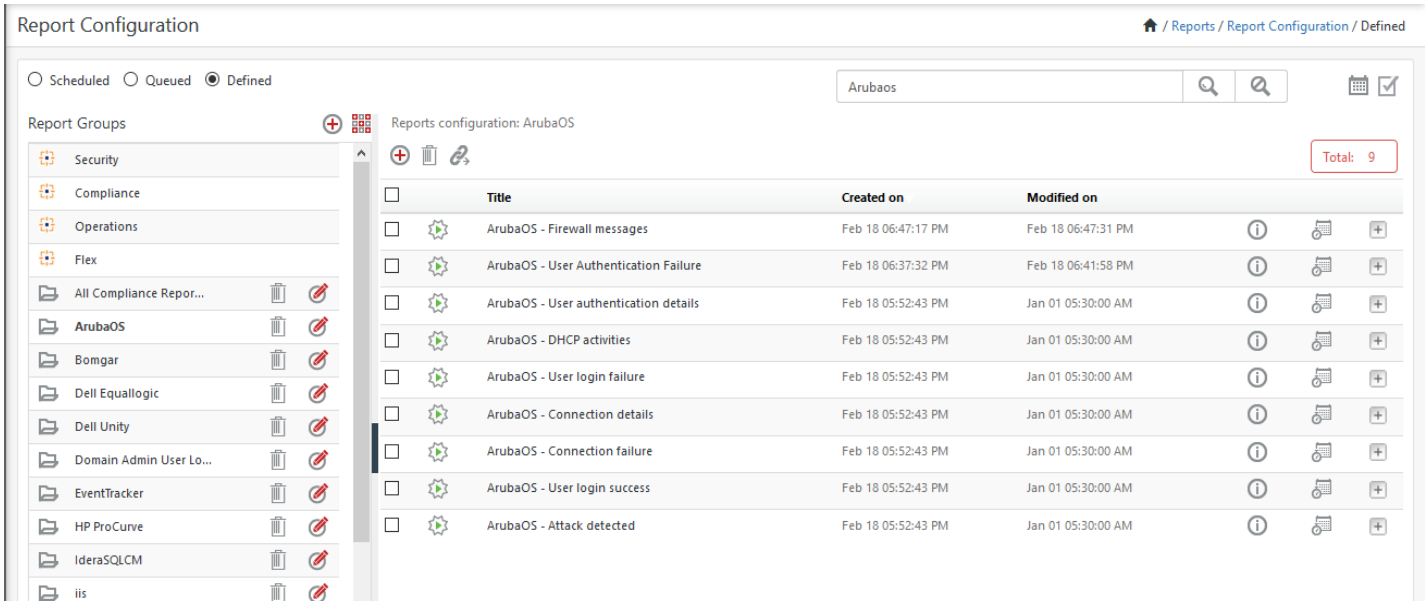

Figure 20

Templates

1. Logon to **EventTracker Enterprise**.
2. Click the **Parsing Rules** menu
3. Select **Template** and choose Group name.
4. In **Template** to view imported Templates, scroll down and click **ArubaOS** group folder.

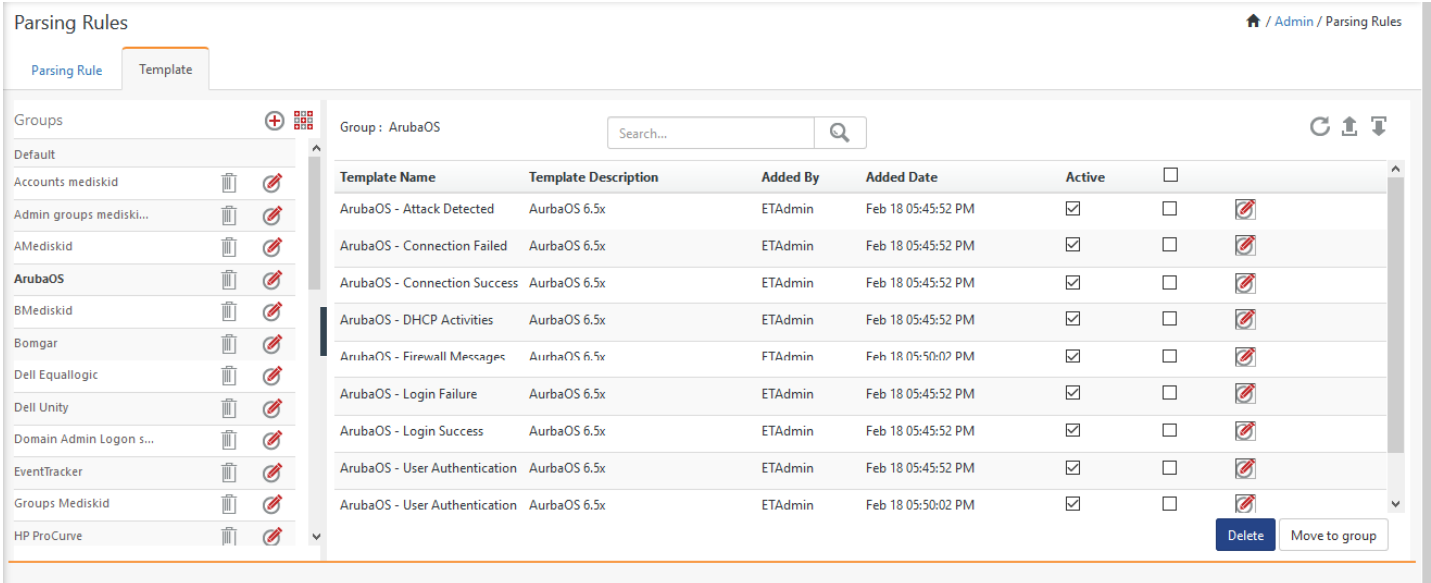

Figure 21