

Integrate Barracuda Message Archiver

Abstract

This guide provides instructions to configure Barracuda Message Archiver to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later and Barracuda Message Archiver (MA) 650 and later.

Audience

Barracuda Message Archiver users, who wish to forward syslog messages to EventTracker manager.

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

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

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

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract	1
Overview.....	3
Prerequisites.....	3
Configuration.....	3
Barracuda Syslog Server Configuration.....	3
EventTracker Knowledge Pack (KP).....	4
Alerts	4
Categories.....	5
Flex Reports.....	5
Import Barracuda Message Archiver knowledge pack into EventTracker	5
To import Alerts.....	6
To import Category	7
To import Flex Reports	8
Import Template.....	9
To import Knowledge Object	11
Verify Barracuda Message Archiver knowledge pack in EventTracker	13
Verify Barracuda Message Archiver Categories	13
Verify Barracuda Message Archiver Flex Reports	14
Verifying Template	14
Verifying Knowledge Objects	15
Sample Report	16

Overview

The Barracuda Message Archiver is ideal for organizations looking to reduce their email storage requirements and boost user productivity with mobile or desktop access to any email ever sent or received.

The EventTracker supports Barracuda Message Archiver. It monitors and generate reports for inbound, outbound, and internal mails stored and configuration changes for Barracuda Message Archiver. It generates alerts as well as reports for user login failure and report for user login success activity. It also helps us to monitor the mail entities counts (like task, note, contacts, inbound, outbound and internal mails) an hourly, daily and total basis.

Prerequisites

- EventTracker 7.x and later should be installed.
- Barracuda Message Archiver should be installed.
- Administrative access on the EventTracker Enterprise and Barracuda Message Archiver.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.
- Port 514 must be opened on Barracuda Message Archiver Appliance.

Configuration

You must enable and configure logging on Barracuda Message Archiver prior to configuring EventTracker Enterprise.

Barracuda Syslog Server Configuration

1. Login into web console of Barracuda Message Archiver.
2. Go to the **ADVANCED > Syslog** page.
3. In the Syslog section, enter the IP address of **EventTracker** machine in **MAILSYSLOG** and **WEB INTERFACE SYSLOG**.

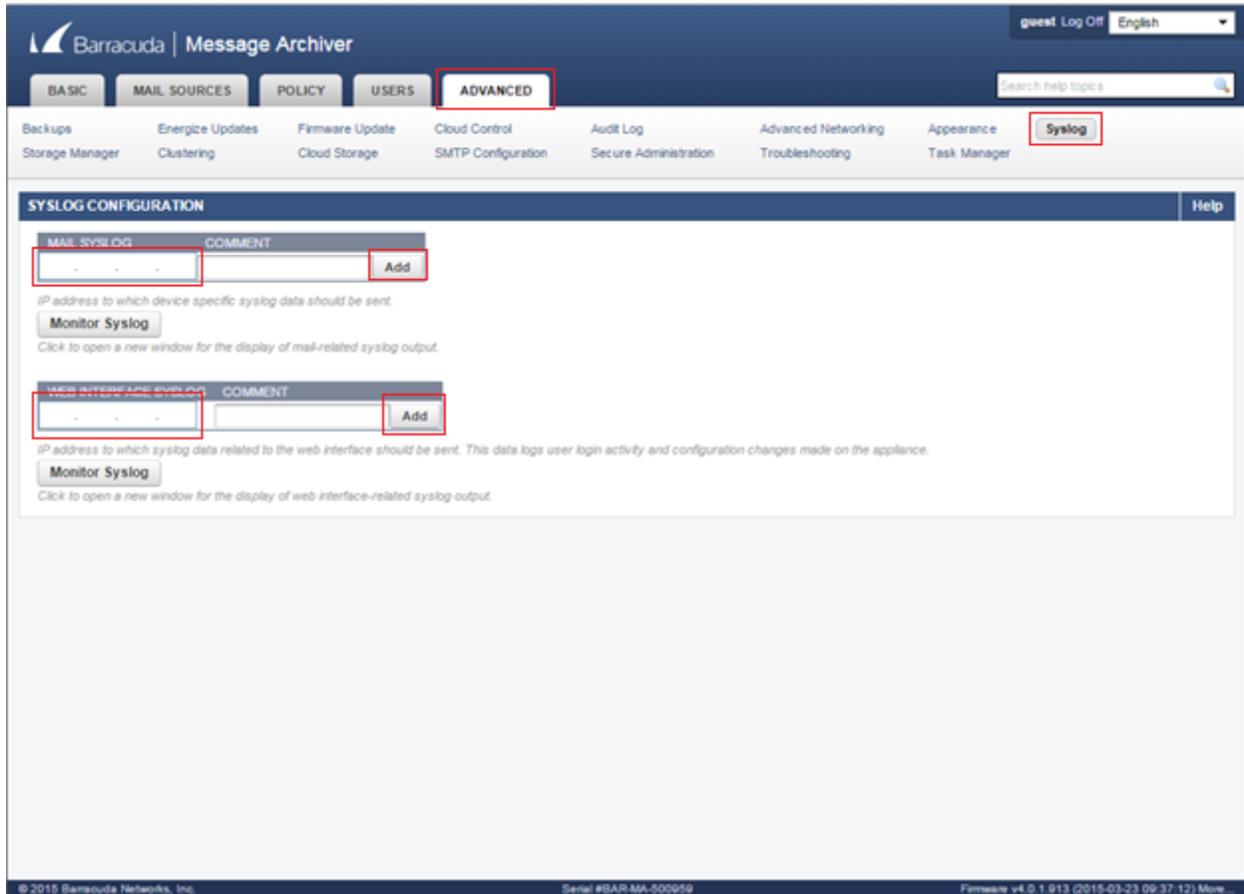


Figure 1

- Click on **Add** button.

EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, categories, reports, alerts and knowledge objects can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Barracuda Message Archiver.

Alerts

- **Barracuda MA: User login failed:** This alert will generate when user authentication fails more than 5 times in 10 second.
- **Barracuda MA: Configuration changed:** This alert will generate when the configuration of Barracuda message archiver changes occurs.

Categories

- **Barracuda MA: User login failed:** All logs generated by the Barracuda Message Archiver when a user failed to login in web interface.
- **Barracuda MA: User login success:** All logs generated by the Barracuda Message Archiver when user login successful in web interface.
- **Barracuda MA: Configuration changes:** All logs generated by the Barracuda Message Archiver when configuration of message archiver changed.
- **Barracuda MA: New mails storage:** All logs generated by the Barracuda Message Archiver when new email stored in message archiver.
- **Barracuda MA: Mail entity count updated:** All logs generated by the Barracuda Message Archiver when changes happen in mails, task, contact and note count.

Flex Reports

- **Barracuda Message Archiver- User login success:** This report provides us the information about the user login successful in the web interface of message archiver.
- **Barracuda Message Archiver- User login failed:** This report provides us the information about the user login failure in the web interface of message archiver.
- **Barracuda Message Archiver- New email storage:** This report provides us the information about the new mails saved in Barracuda Message Archiver with sender, receiver, timestamp and message ID details.
- **Barracuda MA- Configuration change:** This report provides us the information about the changes happened in configuration of Barracuda Message Archiver and by whom configuration is changed.
- **Barracuda MA- Mail entity count change:** This report provide us the count of mail, task, note and contacts on hourly, daily, and total basis in Barracuda Message Archiver.

Import Barracuda Message Archiver knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**. Click **Import** tab.
Import **Alert/Category/Tokens/ Flex Reports/Knowledge Objects** as given below.

To import Alerts

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

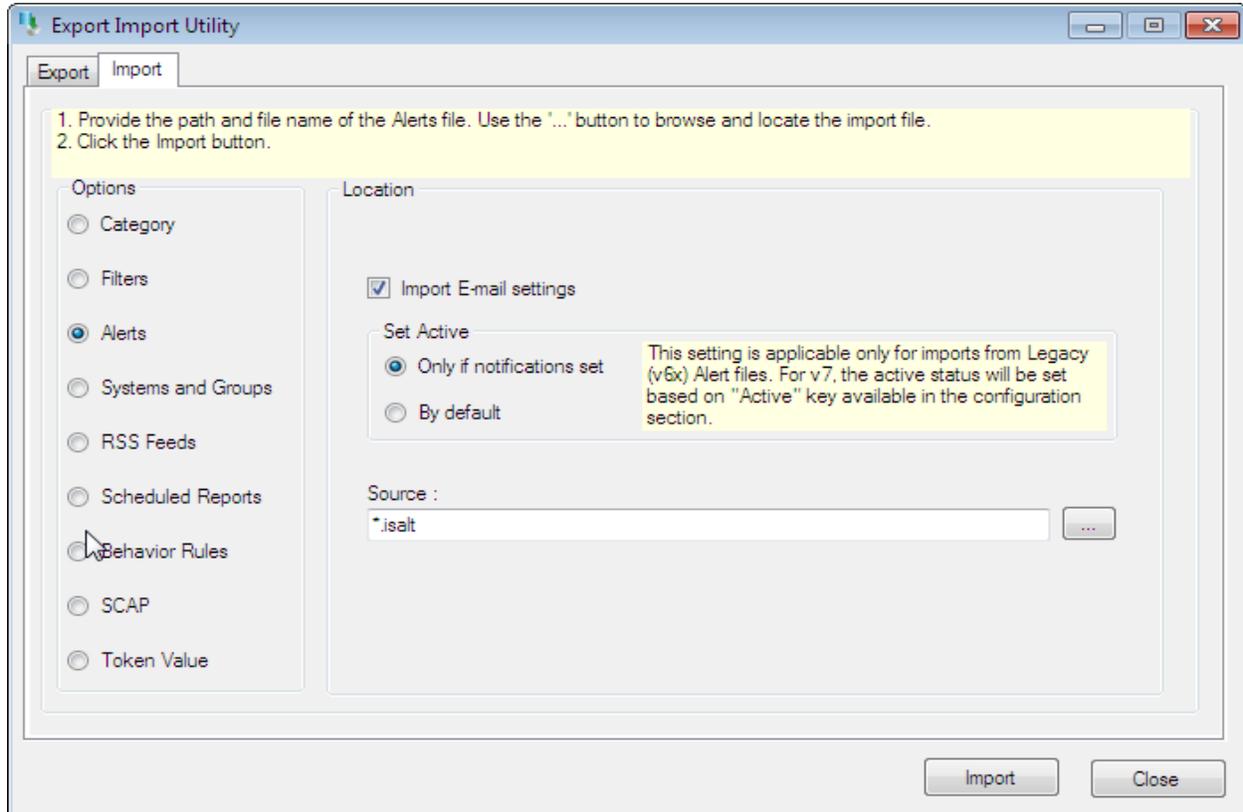


Figure 2

2. Locate **All Barracuda Message Archiver.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
EventTracker displays success message.

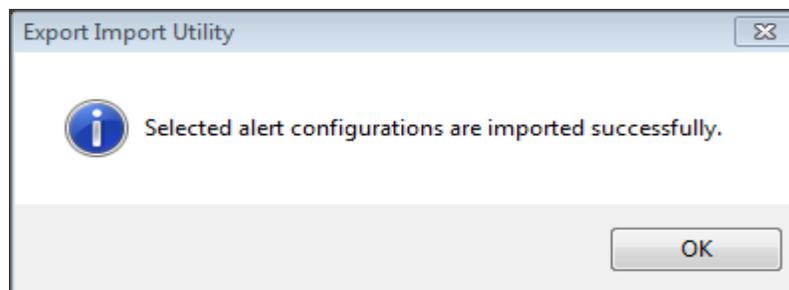


Figure 3

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

To import Flex Reports

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

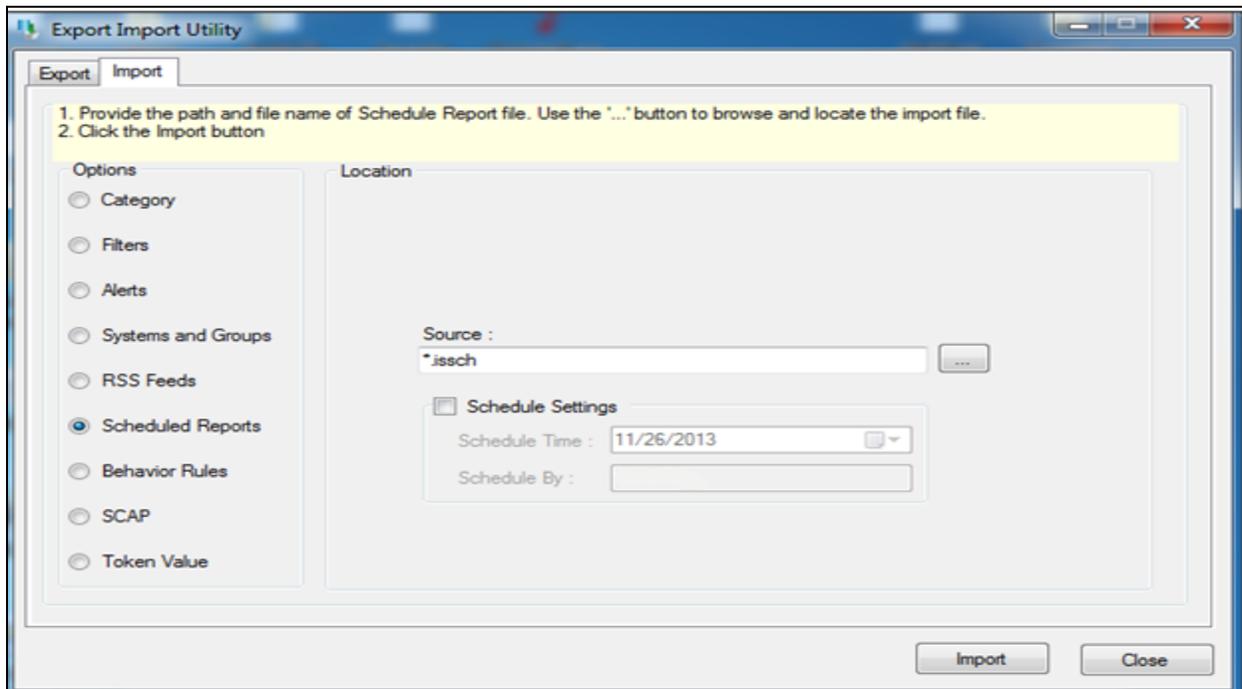


Figure 6

2. Locate the **All Barracuda Message Archiver group of Flex Report.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports. EventTracker displays success message.

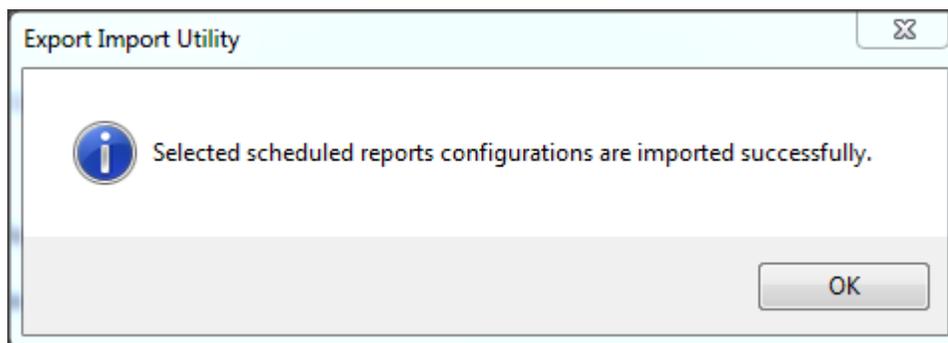


Figure 7

4. Click the **OK** button. Click the **Close** button.

Import Template

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Parsing rule**.
3. Click the **Template** tab.
4. Click the **Import** button, it will open new window. (**Note:** Make sure pop-up is enable for EventTracker)

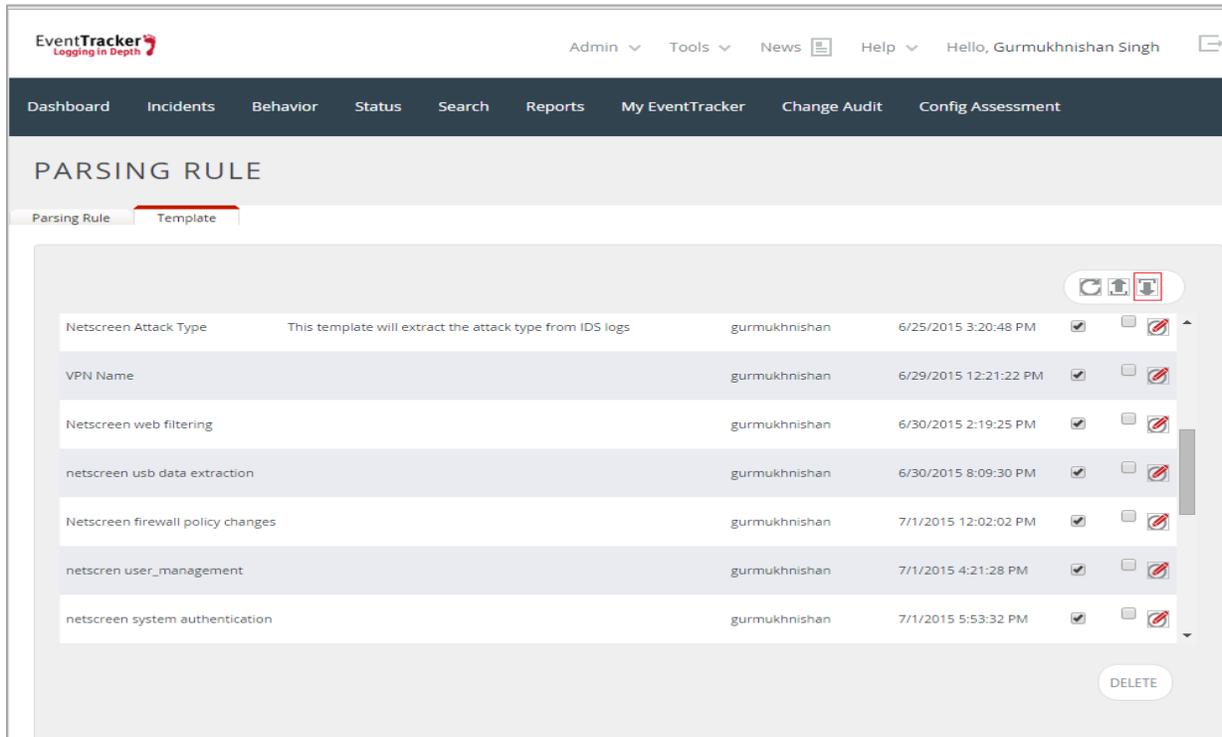


Figure 8

5. Locate and Chose .ETTD file and then click the **Open** button.

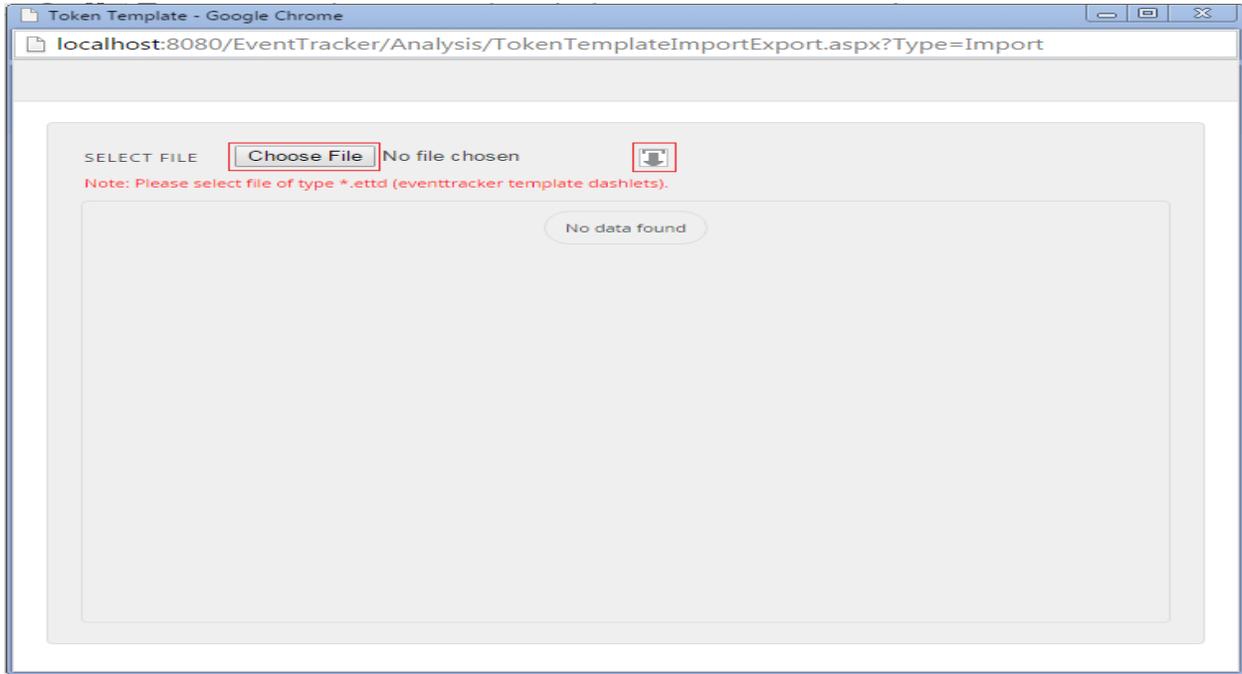


Figure 9

6. Select the template you want to upload.
7. Then click on **Import configuration** button.

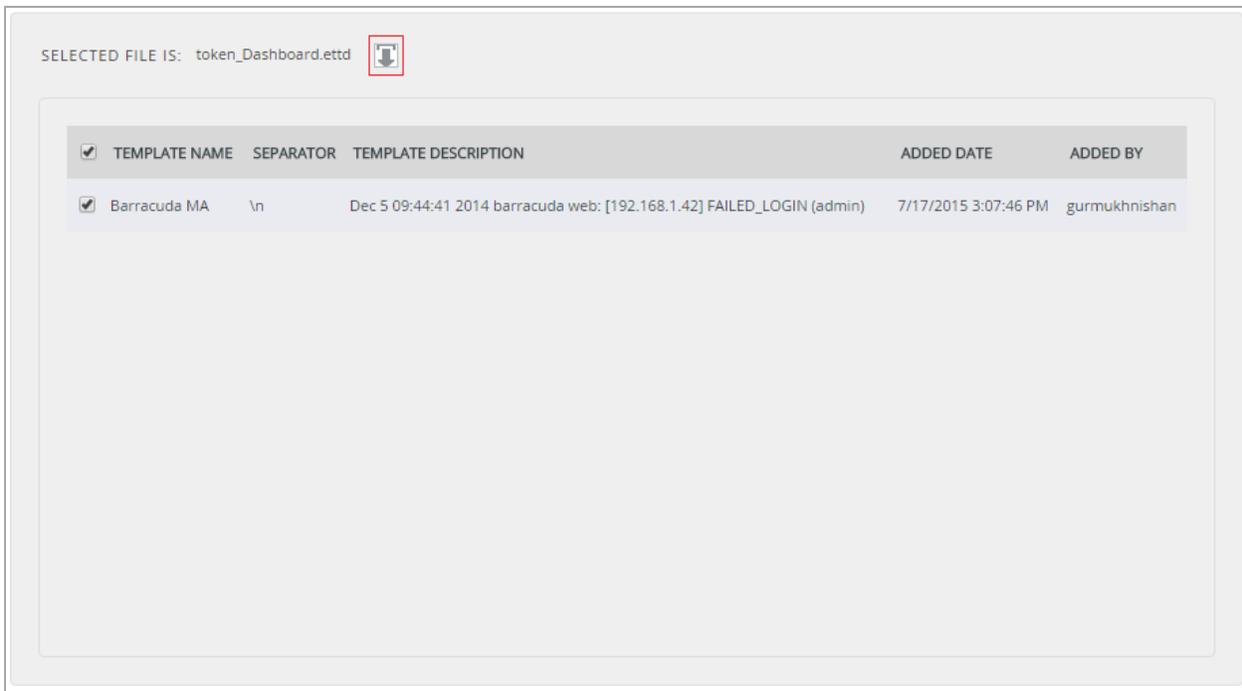


Figure 10

EventTracker displays success message

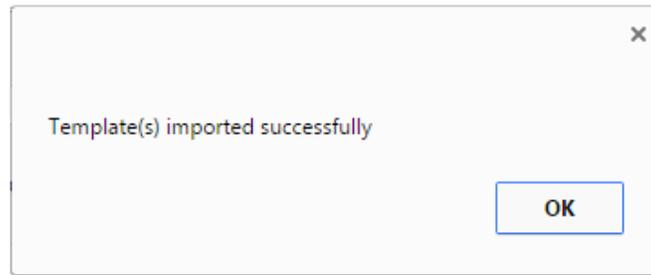


Figure 11

8. Click **OK** it will automatically close the window

To import Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Knowledge Objects**.
3. Click the **Import** button, it will open new window. (Note: Make sure pop-up is enabled for EventTracker.)

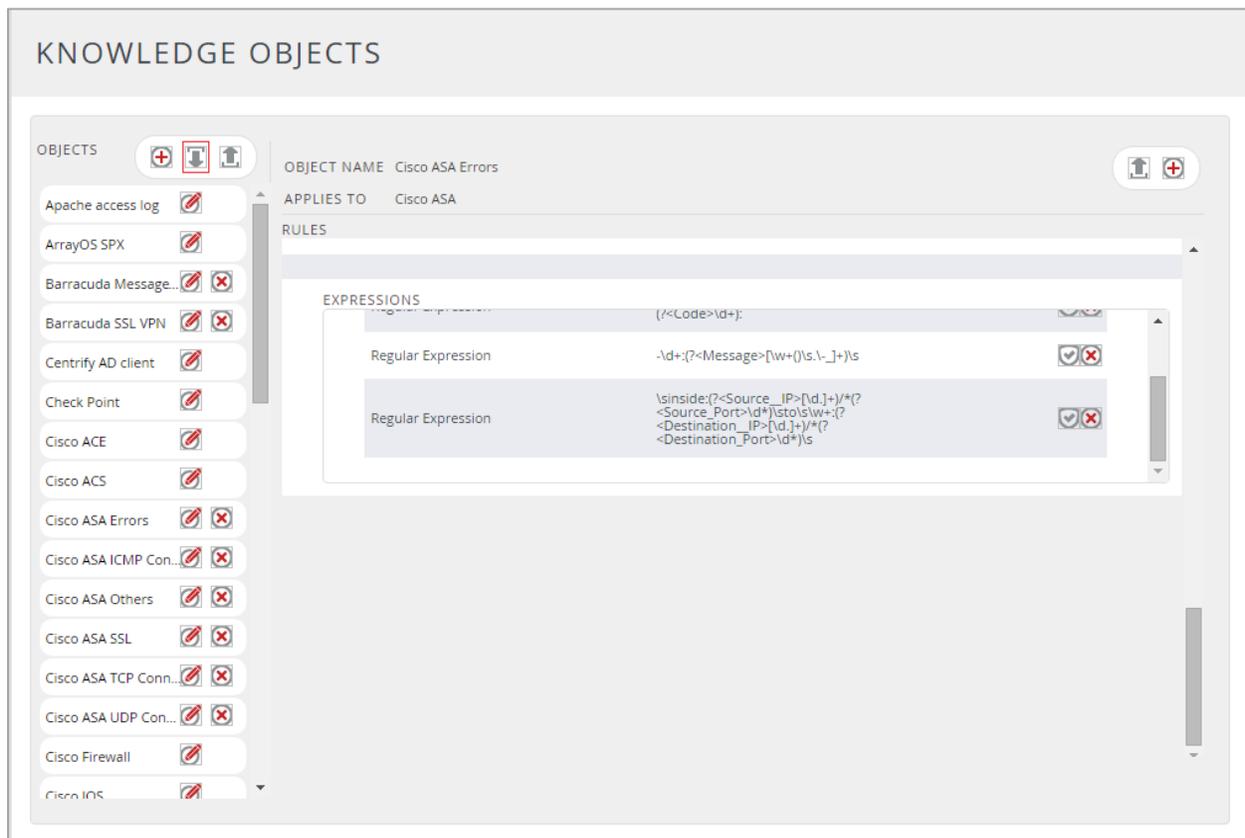


Figure 12

4. Choose the Knowledge object template (.EKTO) files and click on **UPLOAD** button.

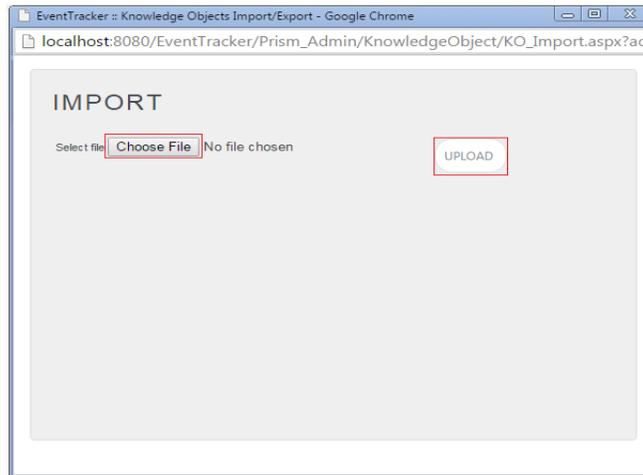


Figure 13

5. Select Knowledge Object and click on **Overwrite or Merge** button.

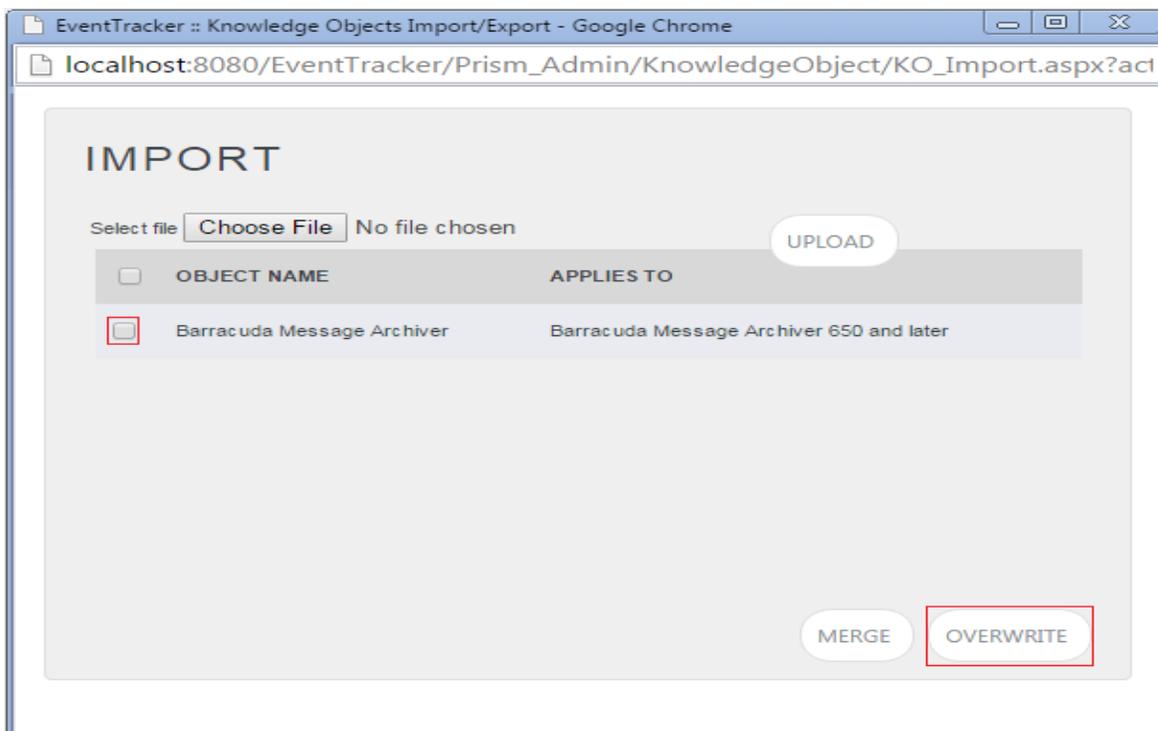


Figure 14

EventTracker displays success message

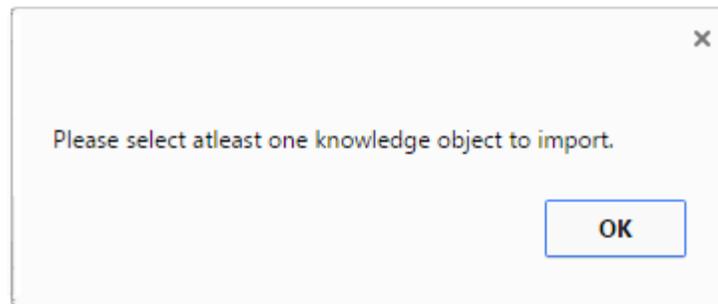


Figure 15

6. Click **OK** it will automatically close the window

Verify Barracuda Message Archiver knowledge pack in EventTracker

Verify Barracuda Message Archiver Categories

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand Barracuda Message Archiever group folder to view the imported categories.

NAME	MODIFIED DATE	MODIFIED BY
Barracuda MA: Count and Configuration Changes	7/20/2015 5:03:56 PM	gurmukhnishan
Barracuda MA: New Mails	7/17/2015 4:16:56 PM	gurmukhnishan
Barracuda MA: Login Success and Failed	7/17/2015 2:32:35 PM	gurmukhnishan
Netscreen: All events	7/15/2015 4:50:52 PM	gurmukhnishan
Netscreen: VPN	7/15/2015 4:50:34 PM	gurmukhnishan
Netscreen: Security device events	7/15/2015 4:49:57 PM	gurmukhnishan
Netscreen: URL allowed	7/15/2015 4:49:35 PM	gurmukhnishan
Netscreen: Web filtering	7/15/2015 4:49:13 PM	gurmukhnishan
Netscreen: Intrusion detection	7/15/2015 4:48:42 PM	gurmukhnishan
Netscreen: Firewall traffic denied	7/15/2015 4:48:12 PM	gurmukhnishan

Figure 16

Verify Barracuda Message Archiver Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports**.
3. Select the **Configuration**.
 - In the **Reports Configuration**, select **Defined** from radio button. **EventTracker** displays **Defined** page.
4. Click the **Barracuda Message Archiver** report group.
5. **EventTracker** displays Flex reports of Barracuda Message Archiver.



REPORTS CONFIGURATION >> BARRACUDA MESSAGE ARCHEIVER

<input type="checkbox"/>	TITLE	CREATED ON	MODIFIED ON			
<input type="checkbox"/>	 Barracuda MA - New Mails	7/17/2015 5:53:58 PM	7/20/2015 10:28:25 AM			
<input type="checkbox"/>	 Barracuda MA - Count and Configuration Changes	7/17/2015 5:50:46 PM	7/20/2015 5:07:53 PM			
<input type="checkbox"/>	 Barracuda MA - Login Success and Failed	7/17/2015 5:47:40 PM	7/20/2015 10:29:29 AM			

Figure 17

Verifying Template

1. Logon to **EventTracker Enterprise**, Go to **Parsing rule**.
2. Click on **Template** tab.
3. Check the template you had uploaded.

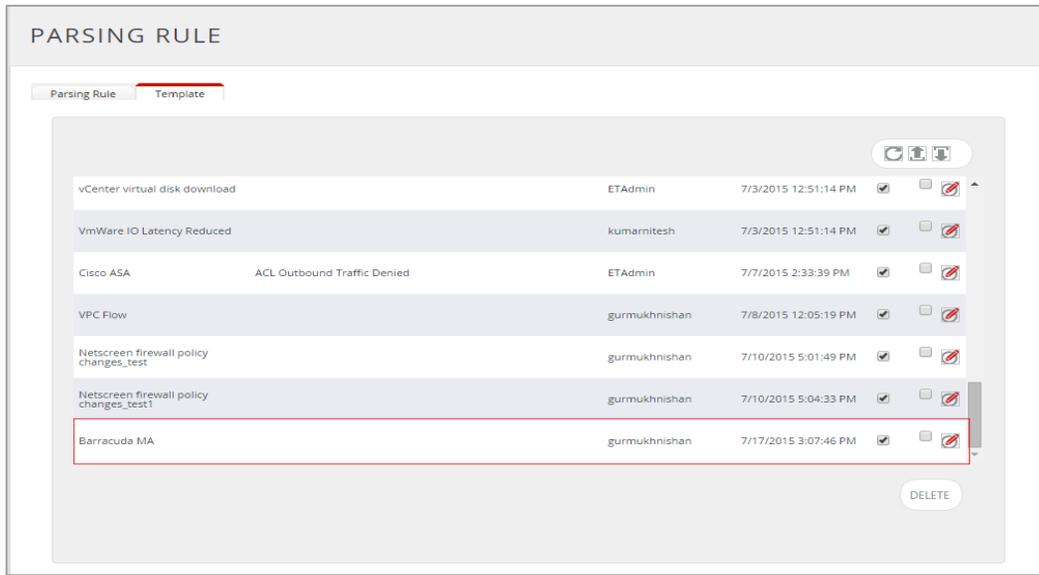


Figure 18

Verifying Knowledge Objects

1. Logon to **EventTracker Enterprise**.
2. Click on **Knowledge Object** option.

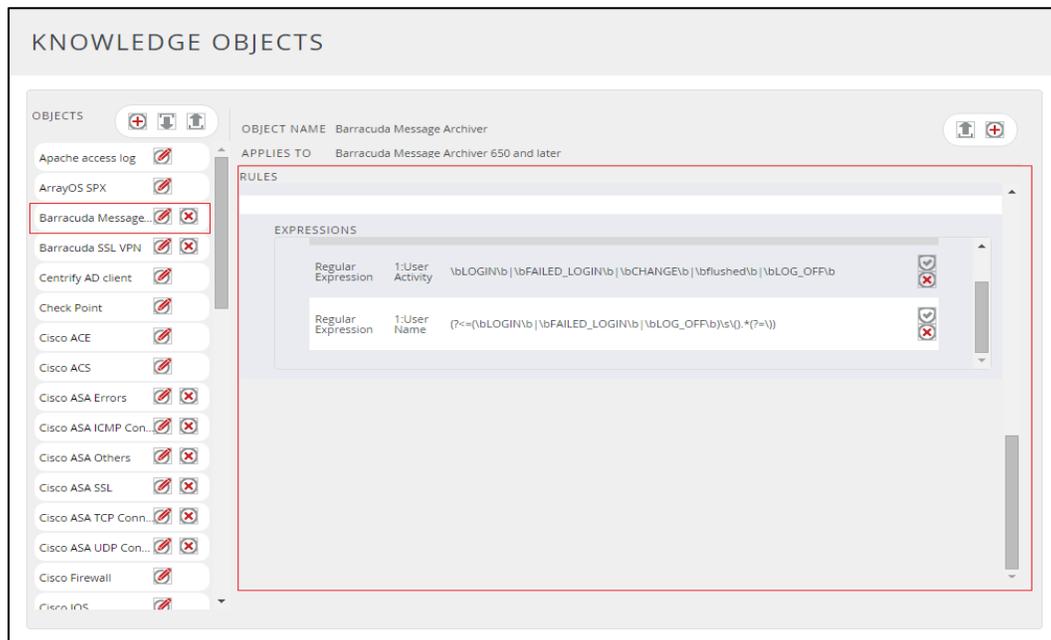


Figure 19

3. Check the Knowledge Object you had imported.

Sample Report

A sample report is shown below.

1. Barracuda MA – Login Success and Failed Reports.

Barracuda MA - Login Success and Failed			
LogTime	Computer	User Name	Action
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:14 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	admin	FAILED_LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	auditor1	LOGIN
07/17/2015 05:35:15 PM	BARRACUDA	auditor1	LOGIN

Figure 20

2. Barracuda MA- New Mails Reports

Barracuda MA - New Mails					
LogTime	Computer	Message ID	From Email	To Email	Email Type
07/17/2015 05:35:12 PM	BARRACUDA	c891af08c5b5464525a46813268b9d03	FRAZIER KRISTE <KFRAZIER@cubx.org>	cphifer@cubx.org	outbound
07/17/2015 05:35:12 PM	BARRACUDA	c891af08c5b5464525a46813268b9d03	FRAZIER KRISTE <KFRAZIER@cubx.org>	cphifer@cubx.org	outbound
07/17/2015 05:35:12 PM	BARRACUDA	80198af453a97162d6c9b3b8d0202a56	Office of Gift Planning <giftplanning@bxamfoundation.com>	cburke@fairlease.org	inbound
07/17/2015 05:35:12 PM	BARRACUDA	c891af08c5b5464525a46813268b9d03	FRAZIER KRISTE <KFRAZIER@cubx.org>	cphifer@cubx.org	outbound
07/17/2015 05:35:12 PM	BARRACUDA	80198af453a97162d6c9b3b8d0202a56	Office of Gift Planning <giftplanning@bxamfoundation.com>	cburke@fairlease.org	inbound
07/17/2015 05:35:12 PM	BARRACUDA	80198af453a97162d6c9b3b8d0202a56	Office of Gift Planning <giftplanning@bxamfoundation.com>	cburke@fairlease.org	inbound
07/17/2015 05:35:12 PM	BARRACUDA	c891af08c5b5464525a46813268b9d03	FRAZIER KRISTE <KFRAZIER@cubx.org>	cphifer@cubx.org	outbound
07/17/2015 05:35:12 PM	BARRACUDA	80198af453a97162d6c9b3b8d0202a56	Office of Gift Planning <giftplanning@bxamfoundation.com>	cburke@fairlease.org	inbound
07/17/2015 05:35:12 PM	BARRACUDA	c891af08c5b5464525a46813268b9d03	FRAZIER KRISTE <KFRAZIER@cubx.org>	cphifer@cubx.org	outbound
07/17/2015 05:35:12 PM	BARRACUDA	80198af453a97162d6c9b3b8d0202a56	Office of Gift Planning <giftplanning@bxamfoundation.com>	cburke@fairlease.org	inbound
07/17/2015 05:35:12 PM	BARRACUDA	c891af08c5b5464525a46813268b9d03	FRAZIER KRISTE <KFRAZIER@cubx.org>	cphifer@cubx.org	outbound
07/17/2015 05:35:12 PM	BARRACUDA	80198af453a97162d6c9b3b8d0202a56	Office of Gift Planning <giftplanning@bxamfoundation.com>	cburke@fairlease.org	inbound
07/17/2015 05:35:13 PM	BARRACUDA	c891af08c5b5464525a46813268b9d03	FRAZIER KRISTE <KFRAZIER@cubx.org>	cphifer@cubx.org	outbound
07/17/2015 05:35:13 PM	BARRACUDA	80198af453a97162d6c9b3b8d0202a56	Office of Gift Planning <giftplanning@bxamfoundation.com>	cburke@fairlease.org	inbound

Figure 21