EventTracker

Actionable Security Intelligence

# Integrate Barracuda Web Application Firewall

Publication Date: July 28, 2014

# Abstract

This guide provides instructions to configure Barracuda Web Application Firewall 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 Firewall 100 and later.

# Audience

Barracuda Web Application Firewall users, who wish to forward syslog events to EventTracker manager.

# Table of Contents

Abstract ..... 1
Overview ..... 3
Prerequisites ..... 3
Integration of EventTracker with Barracuda Firewall ..... 3
EventTracker Knowledge Pack (KP) ..... 5
Categories ..... 5
Alerts ..... 6
Import Barracuda Firewall Knowledge pack into EventTracker ..... 6
To import Category ..... 7
To import Alerts ..... 8
Verify Barracuda Firewall knowledge pack in EventTracker ..... 9
Verify Barracuda Firewall Categories ..... 9
Verify Barracuda Firewall Alerts ..... 9

# Overview

The Barracuda Firewall provides all next-generation application control and user identity functions in an easy-to-use. It outperforms traditional firewalls and UTMs by integrating a powerful next-generation firewall appliance with scalable cloud content security.

While the appliance is optimized for bandwidth-sensitive tasks like packet forwarding and routing, Layer 7 application control, Intrusion Prevention (IPS), DNS/DHCP services, and VPN connectivity, the cloud component handles processor-intensive tasks like virus scanning, content filtering, and reporting.

Syslog can be configured to send to Event Tracker manager, alerts and reports can be configured into EventTracker.

# Prerequisites

Prior to configuring Barracuda Web Application Firewall and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker should be installed.
- Barracuda Web Application Firewall should be installed and proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.

# Integration of EventTracker with Barracuda Firewall

**To configure Barracuda Web Application Firewall to forward all logs to EventTracker Enterprise:**

1. Log in to the Barracuda Web Application Firewall web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Export Logs**.
4. Click **Syslog** Settings.
5. Configure a syslog facility value for the following options:
    - Web Firewall Logs Facility - Select a syslog facility between Local0 and Local7.
    - Access Logs Facility - Select a syslog facility between Local0 and Local7.
    - Audit Logs Facility - Select a syslog facility between Local0 and Local7.
    - System Logs Facility - Select a syslog facility between Local0 and Local7.

    Setting a unique syslog facility for each log type allows the Barracuda Web Application Firewall to divide the logs in to different files.

6. Click **Save Changes**.
7. In the **Name** field, type name of the syslog server.
8. In the **Syslog** field, type IP address of your EventTracker Console or Event Collector.
9. From the **Log Time Stamp** option, select **Yes**.
10. From the **Log Unit Name** option, select **Yes**.
11. Click **Add**.
12. From the **Web Firewall Logs Format** list box, select **Custom Format**.
13. In the **Web Firewall Logs Format** field, type the following custom event format:

    t=%t|ad=%ad|ci=%ci|cp=%cp|au=%au

14. From the **Access Logs Format** list box, select **Custom Format**.
15. In the **Access Logs Format** field, type the following custom event format:

    t=%t|p=%p|s=%s|id=%id|ai=%ai|ap=%ap|ci=%ci|cp=%cp|si=%si|sp=%sp|cu=%cu

16. From the **Audit Logs Format** list box, select **Custom Format**.
17. In the **Audit Logs Format** field, type the following custom event format:

    t=%t|trt=%trt|an=%an|li=%li|lp=%lp

18. Click **Save Changes**.
19. From the navigation menu, select **Basic > Administration**.
20. From the **System/Reload/Shutdown** pane, click **Restart**.

The syslog configuration is complete after your Barracuda Web Application Firewall restarts.

Barracuda Web Application Firewall events are automatically discovered. Events forwarded to EventTracker by Barracuda Web Application Firewall are displayed on the Log Search tab of EventTracker.

# EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and reports can be configured into EventTracker.
The following Knowledge Packs are available in EventTracker v7 to support Barracuda Web Application Firewall monitoring:

## Categories

- **Barracuda: Application platform exploit -** This category based report provides information related to application platform exploit.
- **Barracuda: Authentication hijacking -** This category based report provides information related to authentication hijacking.
- **Barracuda: Buffer overflow attack -** This category based report provides information related to buffer overflow attack.
- **Barracuda: Command injection attack -** This category based report provides information related to command injection attack.
- **Barracuda: Cookie poisoning attack -** This category based report provides information related to cookie poisoning attack.
- **Barracuda: Cross-site scripting attack -** This category based report provides information related to cross-site scripting attack.
- **Barracuda: Denial-of-service attack -** This category based report provides information related to denial-of-service attack.
- **Barracuda: Directory traversal attack -** This category based report provides information related to directory traversal attack.
- **Barracuda: Error message interception -** This category based report provides information related to error message interception.
- **Barracuda: Firewall received messages -** This category based report provides information related to firewall received messages.
- **Barracuda: Firewall scan messages -** This category based report provides information related to firewall scan messages.
- **Barracuda: Firewall sending messages -** This category based report provides information related to firewall sending messages.
- **Barracuda: Forceful browsing attack -** This category based report provides information related to forceful browsing attack.
- **Barracuda: Form tampering attack -** This category based report provides information related to form tampering attack.
- **Barracuda: Malicious file execution attack -** This category based report provides information related to malicious file execution attack.

- **Barracuda: Obfuscation attack -** This category based report provides information related to obfuscation attack.
- **Barracuda: Protocol exploit attack -** This category based report provides information related to protocol exploit attack.
- **Barracuda: SQL injection attack -** This category based report provides information related to SQL injection attack.
- **Barracuda: Traffic allowed -** This category based report provides information related to traffic allowed.
- **Barracuda: Traffic denied-** This category based report provides information related to traffic denied.

### Alerts

- **Barracuda: Authentication hijacking-** This alert is generated when authentication hijacking occurs.
- **Barracuda: Buffer overflow attack-** This alert is generated when buffer overflow attack occurs.
- **Barracuda: Command injection attack-** This alert is generated when command injection attack occurs.
- **Barracuda: Cookie poisoning attack-** This alert is generated when cookie poisoning attack occurs.
- **Barracuda: Cross-site scripting attack-** This alert is generated when cross-site scripting attack.
- **Barracuda: Denial-of-service attack-** This alert is generated when denial-of-service attack occurs.
- **Barracuda: Error message interception-** This alert is generated when error message interception occurs.
- **Barracuda: Malicious file execution attack-** This alert is generated when malicious file execution attack occurs.
- **Barracuda: Obfuscation attack-** This alert is generated when obfuscation attack occurs.

# Import Barracuda Firewall Knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**. Click the **Import** tab.
   Import **Category/Alert** as given below.

# To import Category

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

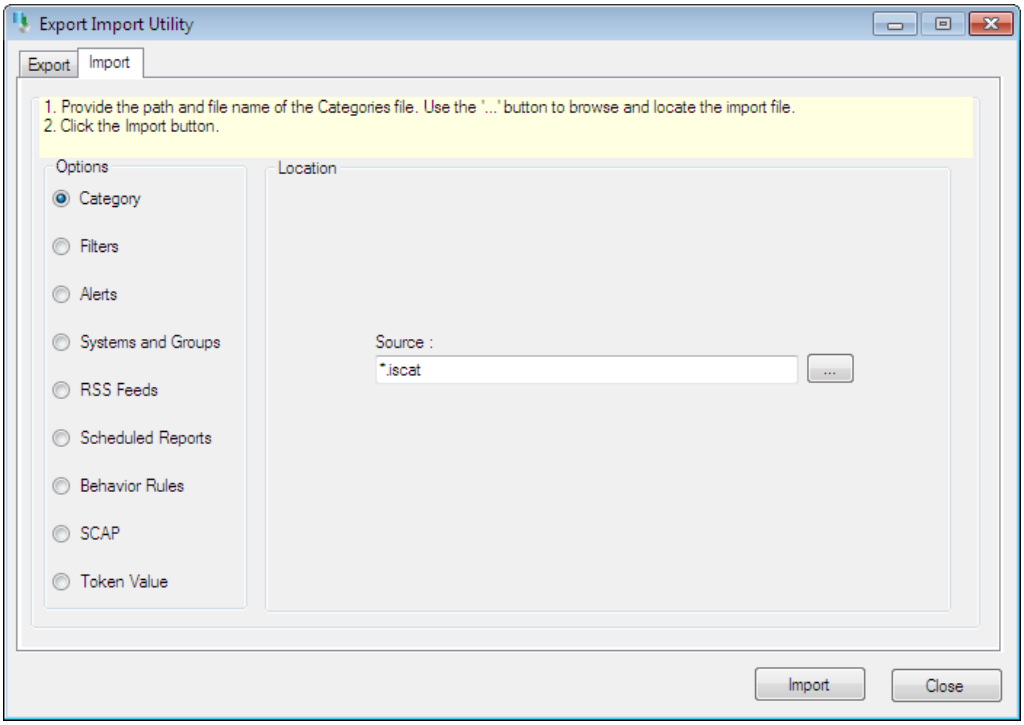


Figure 1

2. Locate **All Barracuda firewall group of Categories.iscat** file, and then click the **Open** button.
3. Click the **Import** button to import the categories.
   EventTracker displays success message.

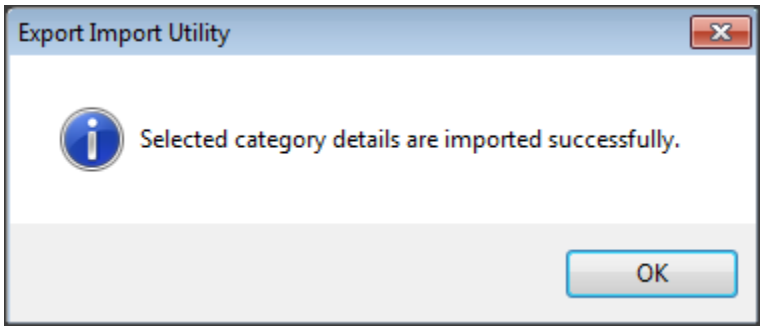


Figure 2

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

# To import Alerts

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

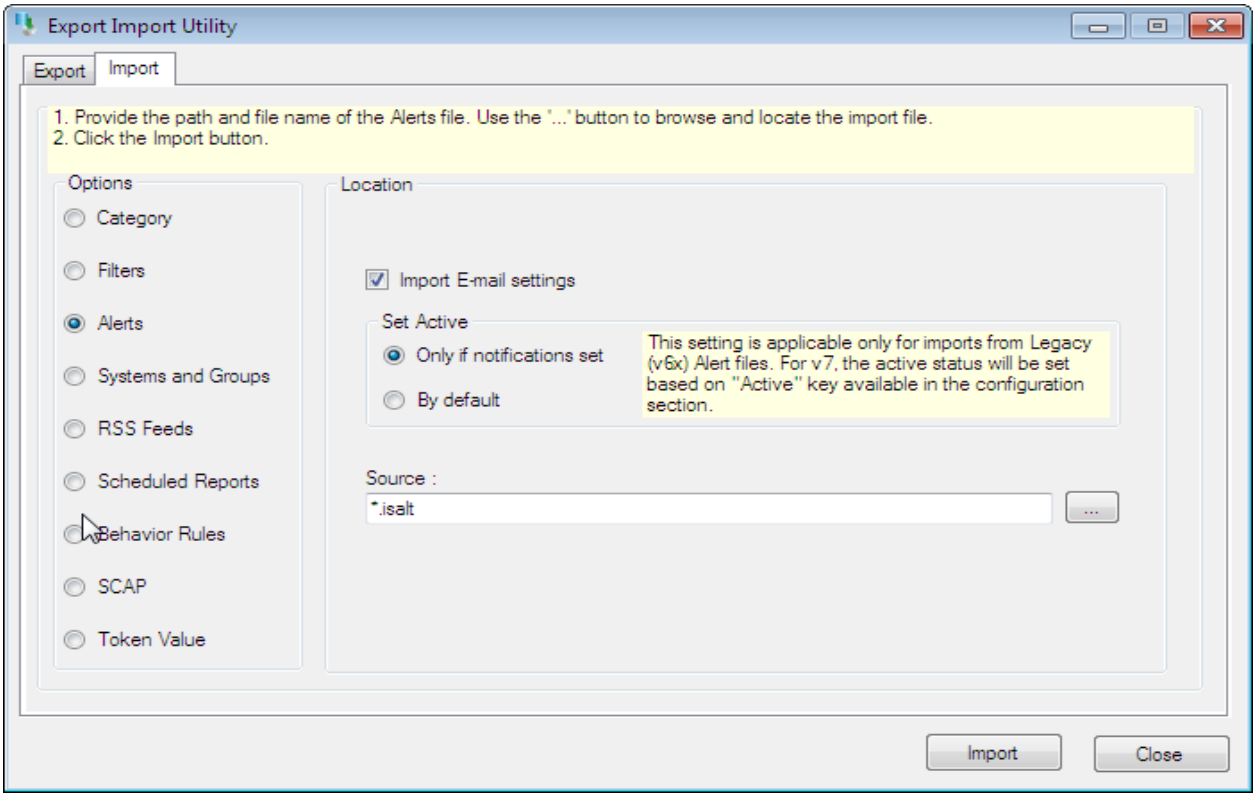


Figure 3

2. Locate **All Barracuda firewall group of Alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.
   EventTracker displays success message.

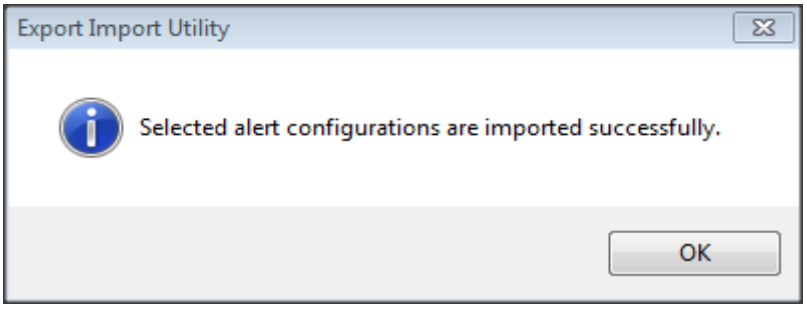


Figure 4

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

# Verify Barracuda Firewall knowledge pack in EventTracker

## Verify Barracuda Firewall Categories

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

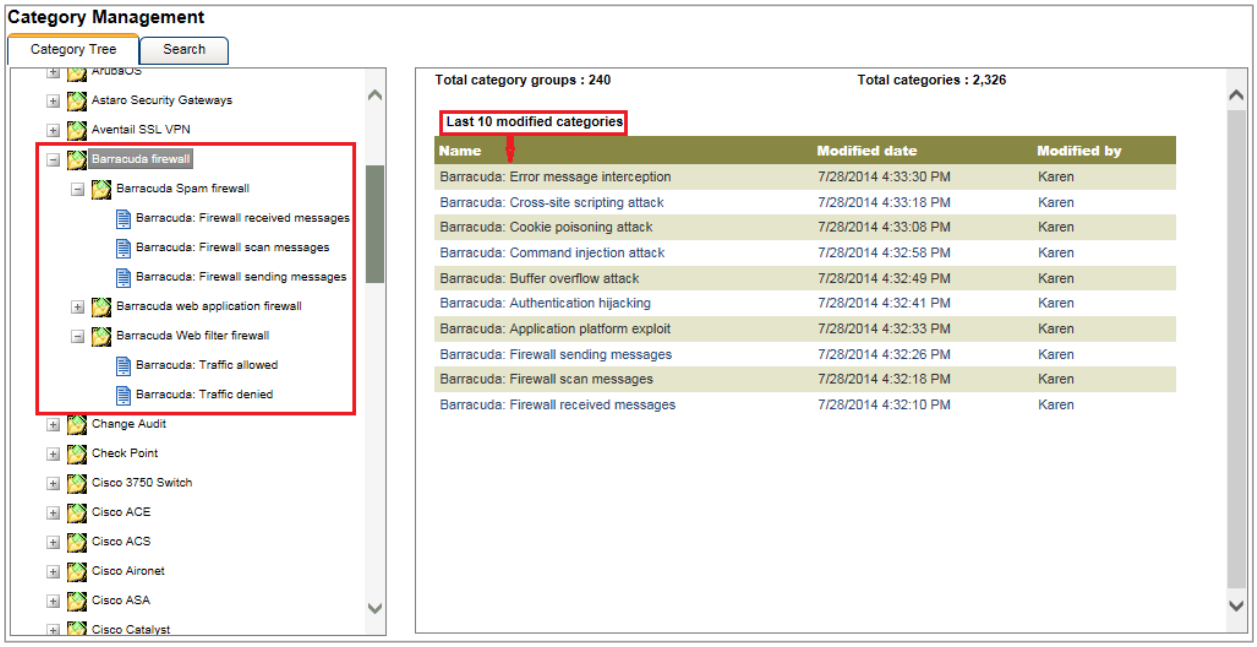


Figure 7

## Verify Barracuda Firewall Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In **Search** field, type '**Barracuda Firewall**', and then click the **Go** button.
   Alert Management page will display all the imported Barracuda Firewall device alerts.

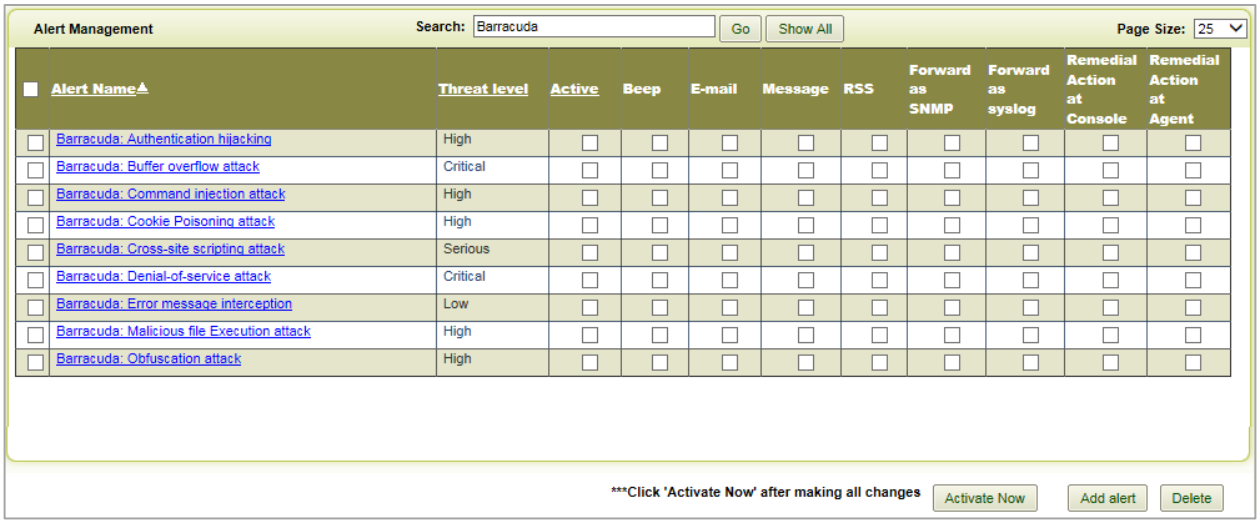


Figure 8

4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

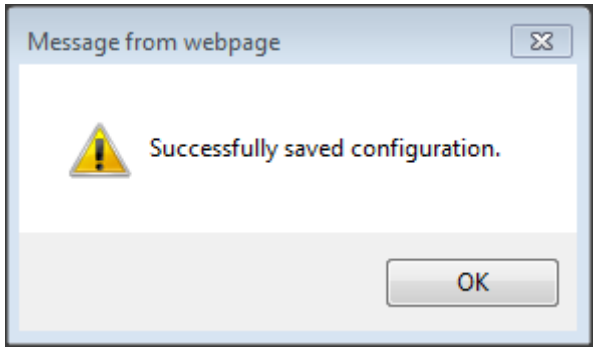


Figure 9

5. Click the **OK** button, and then click the **Activate now** button.
   **NOTE**: You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.