EventTracker

Actionable Security Intelligence

Integrate Astaro Security Gateway

Publication Date: July 24, 2015

Abstract

This guide provides instructions to configure Astaro Security Gateway to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, Astaro Security Gateway v7 and later.

Audience

Administrators who are responsible for monitoring Astaro Security Gateway using EventTracker Manager.

Table of Contents

Introduction

The Astaro Security Gateway is a flexible, full gateway security appliance that can be deployed and configured to fit almost any environment. This product is available as a full hardware appliance, software installation or virtual appliance. The Security Gateway offers firewall and intrusion prevention protection along with application control, web content filtering, gateway anti-virus, email content filtering and anti-spam.

Prerequisites

- EventTracker v7.x should be installed.
- Astaro Security Gateway v7 and later should be installed and configured.

Configure Astaro Security Gateway to send syslog to EventTracker

Enable Logging to a Syslog Host

To configure a remote syslog server, proceed as follows:

1. On the **Remote Syslog Server** tab enable remote syslog.
2. Click **status** icon or the **Enable** button.
   The status icon turns amber and the Remote Syslog Settings area becomes editable.
3. Click the **plus** icon in the **Syslog Servers** box to create a server.
   The Add Syslog Server dialog box opens.
4. Make the following settings:
   Name: Enter a descriptive name for the remote syslog server.
   Server: Add or select the host that should receive log data from gateway.
   Caution - Do not use one of the gateway's own interfaces as a remote syslog host, since this will result in a logging loop.
   Port: Add or select port which is to be used for the connection.
5. Click **Apply**.
   Your settings will be saved.

Monitoring Events of Astaro Security Gateway

Monitoring events provides detailed information about ongoing activities in your network. Astaro Security Gateway events can be monitored using EventTracker Enterprise as follows:

- Antivirus events
- Authentication events
- Clustering events
- Content Filtering events
- Firewall events
- High Availability events
- Intrusion Detection and Prevention events
- Virtual Private Networks events

Import Astaro Security Gateway knowledge pack into EventTracker

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

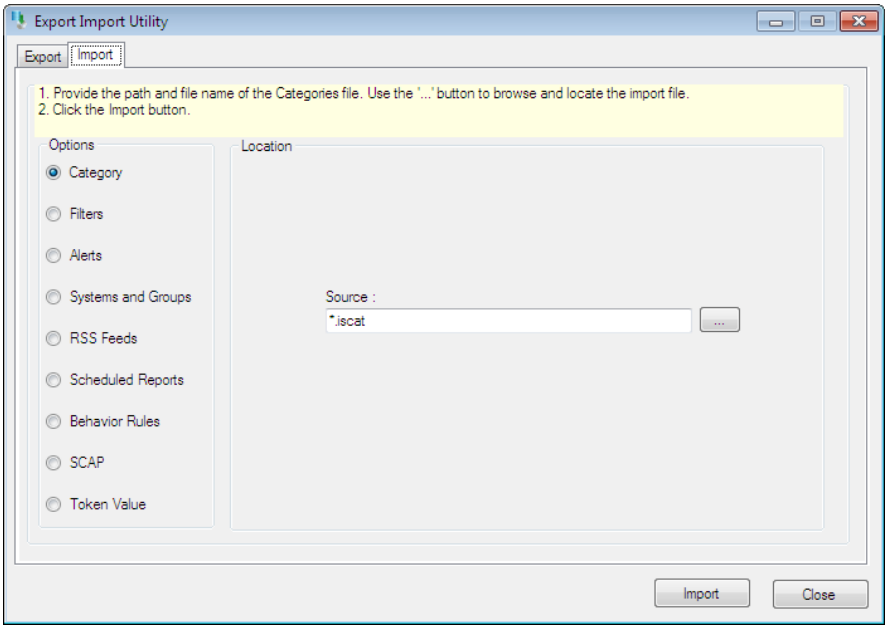

Figure 1

Import **Category/Alert** as given below.

Import Category

1. Click **Category** option, and then click the **browse**  button.
2. Locate **All Astaro Security Gateway group categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.
   EventTracker displays success message.

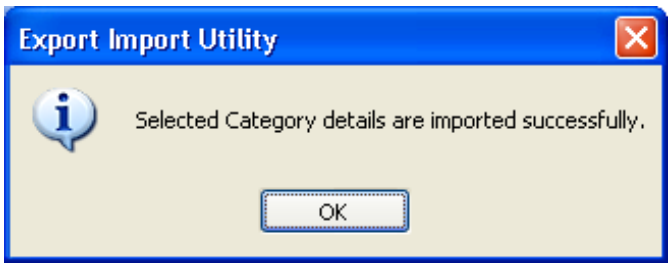

Figure 2

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

Import Alerts

1. Click **Alert** option, and then click the **browse**  button.
2. Locate **All Astaro Security Gateway group alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.

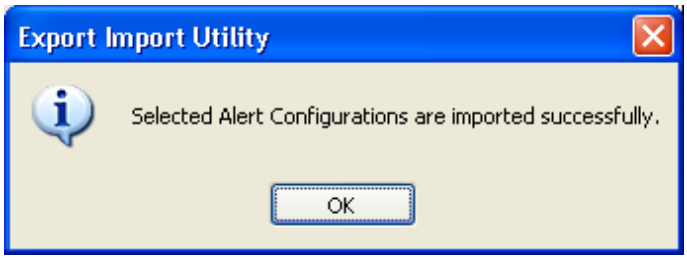

Figure 3

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

Verify Astaro Security Gateway knowledge pack in EventTracker

Verify categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. To view imported categories, in **Category Tree**, expand **Astaro Security Gateways** group folder.

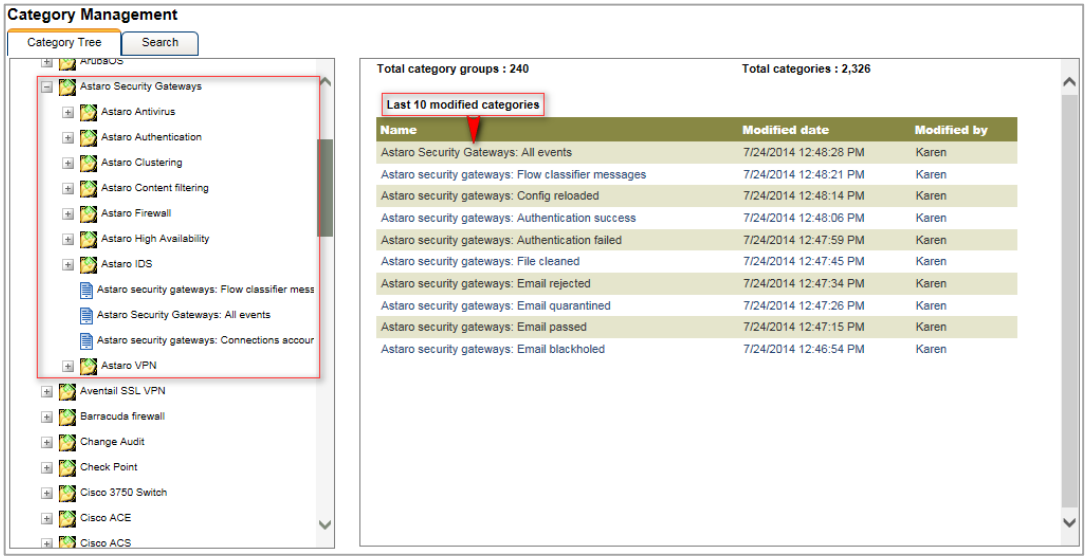

Figure 4

Verify alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type '**Astaro Security Gateway**', and then click the **Go** button.
   Alert Management page will display all the imported alerts.

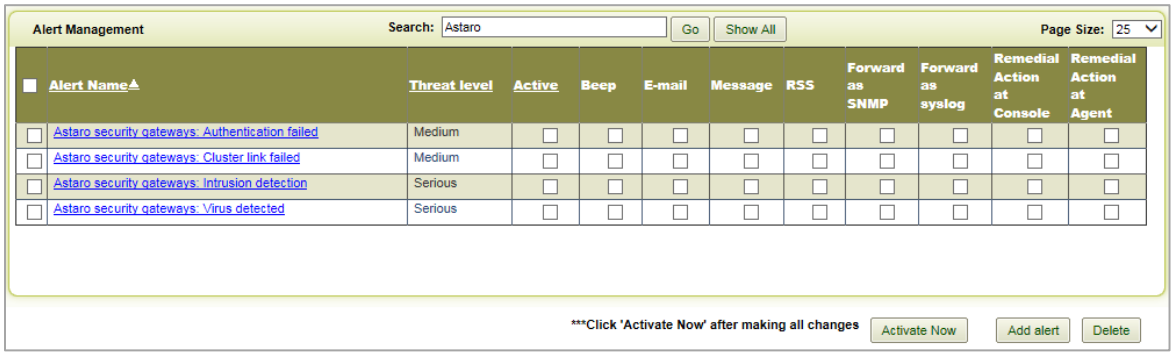

Figure 5

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

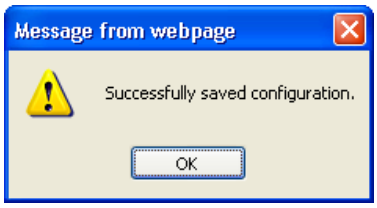

Figure 6

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

EventTracker Knowledge Pack

Categories

EventTracker Categories can alert all critical events such as Virus detection, Login failures etc.
Events which can be monitored using EventTracker are

- **Astaro security gateways Email blackholed -** This category based report provides information related to email blackholed.
- **Astaro security gateways Email passed -** This category based report provides information about e-mail passed.
- **Astaro security gateways Email quarantined -** This category based report provides information about quarantined emails.
- **Astaro security gateways Email rejected -** This category based report provides information about rejected emails.
- **Astaro security gateways File cleaned -** This category based report provides information about the files which has been cleaned.
- **Astaro security gateways File not scanned -** This category based report provides information about the files which are not scanned.
- **Astaro security gateways Virus detected -** category based report provides information about virus detections.
- **Astaro security gateways Authentication failed -** This category based report provides information about authentication failures.
- **Astaro security gateways Authentication success -** This category based report provides information about successful authentications.

- **Astaro security gateways Config reloaded -** This category based report provides information about reloaded configurations.
- **Astaro security gateways Debug message -** This category based report provides information about general debug messages.
- **Astaro security gateways Discarded cache -** This category based report provides information related to discarded cache.
- **Astaro security gateways Informational messages -** This category based report provides information related to informational messages.
- **Astaro security gateways Cluster link failed -** This category based report provides information about cluster link failure.
- **Astaro security gateways Cluster updated successfully -** This category based report provides information about successfully updated clusters.
- **Astaro security gateways Slave dead -** This category based report provides information about worker node goes into slave mode on cluster.
- **Astaro security gateways Web request blocked -** This category based report provides information about blocked web requests.
- **Astaro security gateways Web request delivered -** This category based report provides information about delivered web requests.
- **Astaro security gateways Invalid packet -** This category based report provides information related to invalid packets detections.
- **Astaro security gateways Packet accepted -** This category based report provides information about accepted packets.
- **Astaro security gateways Spoofed packet dropped -** This category based report provides information about spoofed packets dropped.
- **Astaro security gateways Packet logged -** This category based report provides information related to packet logged.
- **Astaro security gateways Packet rejected -** This category based report provides information related to packet rejected.
- **Astaro security gateways Grateful take-over -** This category based report provides information related to grateful takeover of a HA peer.
- **Astaro security gateways Master dead -** This category based report provides information related to master dead.
- **Astaro security gateways Node alive -** This category based report provides information about an alive node detected.
- **Astaro security gateways Node dead -** This category based report provides information about disappeared nodes.

- **Astaro security gateways Preempt slave -** This category based report provides information related to graceful takeover is triggered by preempt Slave.
- **Astaro security gateways Preempt worker -** This category based report provides information related to graceful takeover is triggered by preempt Worker.
- **Astaro security gateways Switching to master mode -** This category based report provides information related to system switches to master mode.
- **Astaro security gateways Switching to slave mode -** This category based report provides information related to the system switches to slave mode.
- **Astaro security gateways Switching to worker mode -** This category based report provides information related to the system switches to worker mode.
- **Astaro security gateways: Flow classifier messages -** This category based report provides information related to flow classifier messages.
- **Astaro Security gateways: All events -** This category based report provides information related to all events of Astaro security gateways.
- **Astaro security gateways: Connection started -** This category based report provides information related to the connection started.
- **Astaro security gateways: Connection terminated -** This category based report provides information related to the connection terminated.
- **Astaro security gateways: Connections accounted -** This category based report provides information related to the connections accounted.
- **Astaro security gateways: ICMP flood detected -** This category based report provides information related to the ICMP flood detected.
- **Astaro security gateways: ICMP redirect -** This category based report provides information related to the ICMP redirect.
- **Astaro security gateways: Intrusion protection alert -** This category based report provides information related to the Intrusion protection alert.
- **Astaro security gateways: Portscan detection:** This category based report provides information related to the portscan detected.
- **Astaro security gateways: Spoofed packet dropped:** This category based report provides information related to spoofed packet dropped.
- **Astaro security gateways: SYN Flood detected -** This category based report provides information related to the SYN Flood detected.
- **Astaro security gateways: UDP flood detected -** This category based report provides information related to the UDP flood detected.

Alerts

- **Astaro security gateways: Authentication failed -** This alert is generated when system or user related authentication fails.
- **Astaro security gateways: Cluster link failed -** This alert is generated when cluster link failed**.**
- **Astaro security gateways: Intrusion detection -** This alert is generated when Intrusion is detected.
- **Astaro security gateways: Virus detected -** This alert is generated when Virus is detected.