EventTracker

Actionable Security Intelligence

Integrate Aventail SSL VPN

Publication Date: July 24, 2014

Abstract

This guide provides instructions to configure Aventail SSL VPN to send the syslog to EventTracker. Once syslog is being configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, and **Aventail E-class SRA EX6000 and later**.

Audience

Administrators who are responsible for monitoring Aventail E-class SRA EX6000 series appliances using EventTracker.

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.

Table of Contents

Overview

The Aventail SSL VPN appliance provides secure access - including clientless access to Web applications, access to client/server applications, and file sharing - to employees, business partners, and customers. All traffic is encrypted using Secure Sockets Layer (SSL) to protect it from unauthorized users.

The appliance makes applications available from a range of access methods - including a standard Web browser, a Windows client, or a mobile device - on a wide range of platforms including Windows, Macintosh, and Linux.

Prerequisites

- EventTracker v7.x should be installed.
- **Aventail E-class SRA EX6000** and later appliance should be installed and configured.

Configure Aventail appliance to send syslog to EventTracker

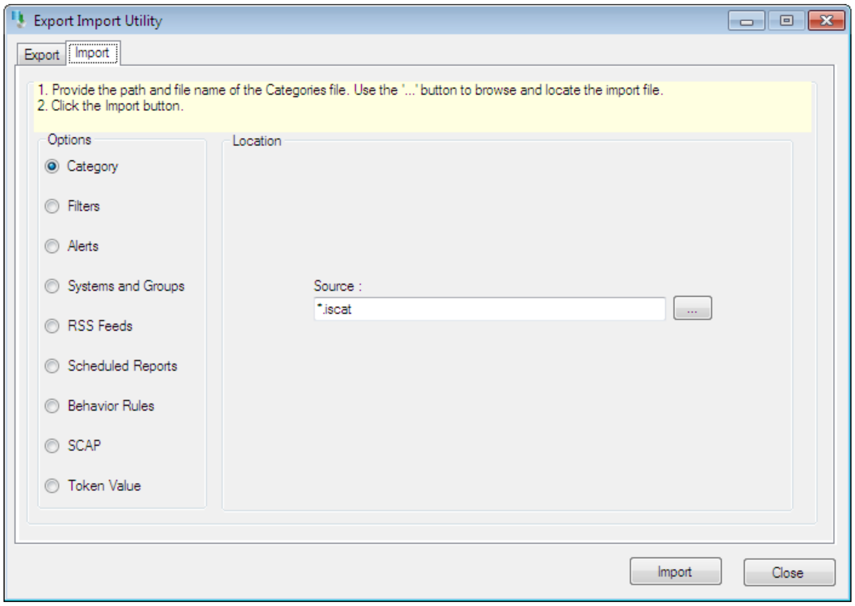
The Aventail appliance can send system logs to a syslog server. Regardless of whether you configure syslog, all system events are logged locally. To avoid flooding the network with log information, the appliance forwards log messages for only the three highest severity levels (fatal, error, and warning).

Enable Logging to a Syslog Host

1. Log in to Management Console
2. From the main navigation menu, click **Logging**.
   The **View Logs** page appears.
3. Click the **Configure Logging** tab.
4. Under **Syslog configuration**, type the IP address and port number of EventTracker Manager.
   The default for the syslog-ng port is *514*, but you can use another port.
5. Match your EventTracker Manager configuration.
6. Use the **Protocol** list to specify whether the appliance will communicate with syslog using the TCP or UDP protocol.
7. Click **Save**.

Import Aventail SSL VPN knowledge pack into EventTracker

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



Export Import Utility

Export | Import

1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

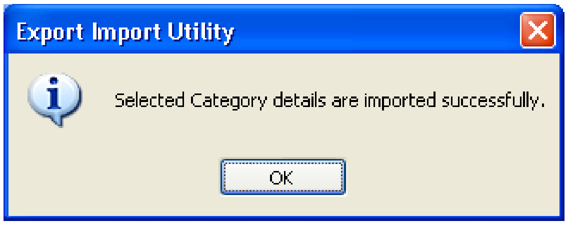
Source : *.iscat

Figure 1

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

Import Category

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



Export Import Utility

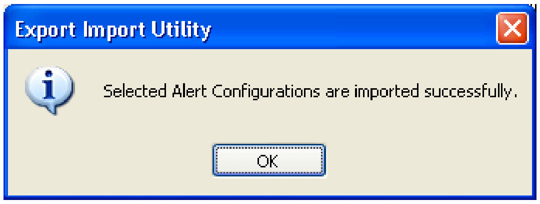
Selected Category details are imported successfully.

Figure 2

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

Import Alerts

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



Selected Alert Configurations are imported successfully.

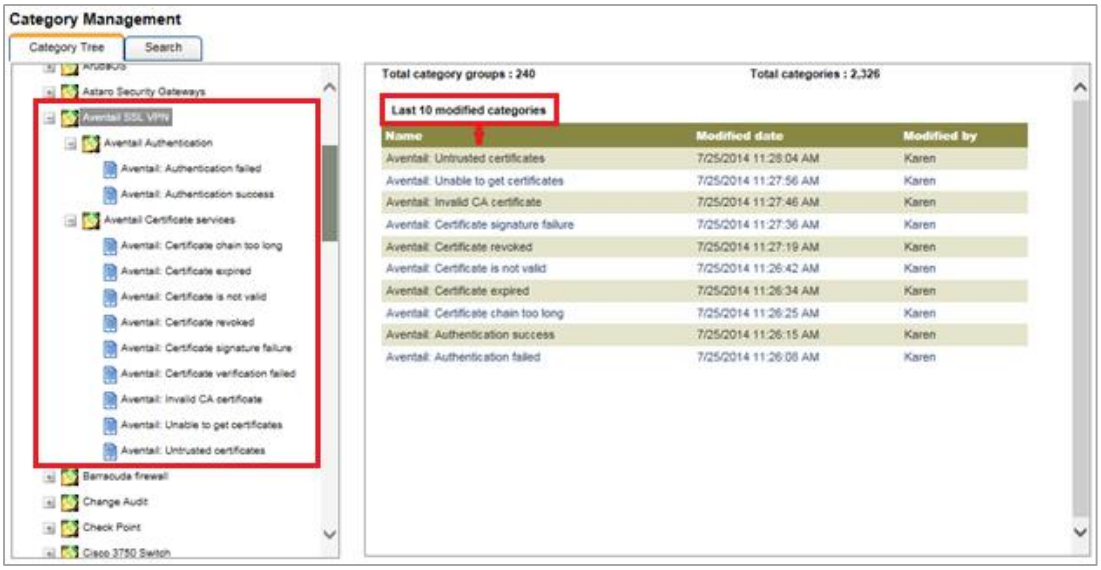
Figure 3

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

Verify Aventail SSL VPN 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 the **Category Tree**, expand **Aventail SSL VPN** group folder.


Category Management
Category Tree
Search
ArubaOS
Astaro Security Gateways
Aventail SSL VPN
Aventail Authentication
Aventail: Authentication failed
Aventail: Authentication success
Aventail Certificate services
Aventail: Certificate chain too long
Aventail: Certificate expired
Aventail: Certificate is not valid
Aventail: Certificate revoked
Aventail: Certificate signature failure
Aventail: Certificate verification failed
Aventail: Invalid CA certificate
Aventail: Unable to get certificates
Aventail: Untrusted certificates
Barracuda firewall
Change Audit
Check Point
Cisco 3750 Switch

Total category groups : 240

Total categories : 2,326

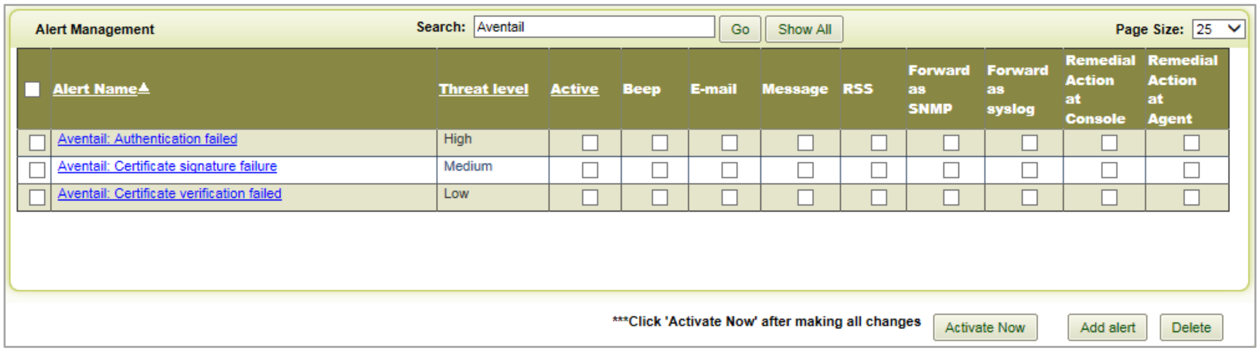
Last 10 modified categories

Name	Modified date	Modified by
Aventail: Untrusted certificates	7/25/2014 11:28:04 AM	Karen
Aventail: Unable to get certificates	7/25/2014 11:27:56 AM	Karen
Aventail: Invalid CA certificate	7/25/2014 11:27:46 AM	Karen
Aventail: Certificate signature failure	7/25/2014 11:27:36 AM	Karen
Aventail: Certificate revoked	7/25/2014 11:27:19 AM	Karen
Aventail: Certificate is not valid	7/25/2014 11:26:42 AM	Karen
Aventail: Certificate expired	7/25/2014 11:26:34 AM	Karen
Aventail: Certificate chain too long	7/25/2014 11:26:25 AM	Karen
Aventail: Authentication success	7/25/2014 11:26:15 AM	Karen
Aventail: Authentication failed	7/25/2014 11:26:08 AM	Karen

Figure 4

Verify alerts

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



Alert Management

Search: Aventail

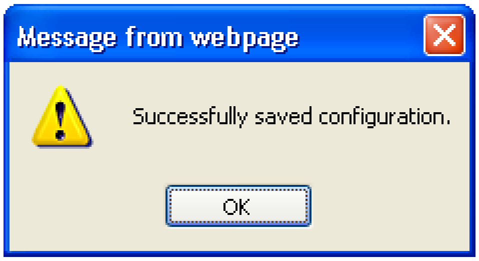
Page Size: 25

□	Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
□	Aventail: Authentication failed	High	□	□	□	□	□	□	□	□	□
□	Aventail: Certificate signature failure	Medium	□	□	□	□	□	□	□	□	□
□	Aventail: Certificate verification failed	Low	□	□	□	□	□	□	□	□	□

***Click 'Activate Now' after making all changes

Figure 5

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



Message from webpage

Successfully saved configuration.

Figure 6

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

EventTracker Knowledge Pack

Categories

Events which can be monitored using Event Tracker:

- **Aventail Authentication failed:** This category based report provides information about authentication failures.
- **Aventail Authentication success:** This category based report provides information about successful authentications.
- **Aventail Certificate chain too long:** This category based report provides information related to certificate chain too long.
- **Aventail Certificate expired:** This category based report provides information about expired certificates.
- **Aventail Certificate is not valid:** This category based report provides information about invalid certificates.
- **Aventail Certificate revoked:** This category based report provides information related to revoked certificates.
- **Aventail Certificate signature failure:** This category based report provides information related to failed signature certificates.
- **Aventail Certificate verification failed:** This category based report provides information about failed certificates verification.
- **Aventail Invalid CA certificate:** This category based report provides information related to CA certificates.
- **Aventail Unable to get certificates:** This category based report provides information of certificates which is unable to get.
- **Aventail Untrusted certificates:** This category based report provides information about untrusted certificates.

Alerts

- **Aventail Authentication failed -** This alert is generated when authentication failed.
- **Aventail Certificate signature failure -** This alert is generated when certificate signature failure occurs.
- **Aventail: Certificate verification failed -** This alert is generated when failed to verify certificate.