

Integrating Cisco Aironet Device

EventTracker v7.x

About this Guide

This guide provides instructions to configure Cisco Aironet Device to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and Cisco IOS 12.2(15)JA and later.

Audience

Cisco Aironet Device users, who wish to forward syslog events to EventTracker manager.

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

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2014 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

- About this Guide..... 1
 - Scope 1
 - Audience..... 1
- Overview..... 3
- Pre-requisite..... 3
- Integration of EventTracker with Cisco Aironet..... 3
 - To configure Cisco Aironet to forward the log to EventTracker Enterprise 3
- EventTracker Knowledge Pack (KP) 5
 - Categories 5
 - Alerts 6
- Import Cisco Aironet Knowledge Pack into EventTracker 7
 - To import Category..... 7
 - To import Alerts..... 8
- Verify Cisco Aironet knowledge pack in EventTracker 10
 - Verify Cisco Aironet Firewall Categories 10
 - Verify Cisco Aironet Alerts 10

Overview

Cisco Aironet Access Points (hereafter called access points) provide a secure, affordable, and easy to-use wireless LAN solution. It combines mobility and flexibility with the enterprise-class features required by networking professionals with a management system based on Cisco IOS software.

Pre-requisite

Prior to configuring Cisco Aironet and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker v7.x should be installed.
- Cisco IOS 12.2(15)JA should be running on Aironet device.
- Cisco Aironet devices proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.

Integration of EventTracker with Cisco Aironet

To configure Cisco Aironet to forward the log to EventTracker Enterprise

To configure Cisco Aironet to forward events:

1. Establish a connection to the Cisco Aironet device using one of the following methods
 - Telnet to the wireless access point
 - Access the console
2. Type the following command to access privileged EXEC mode:

enable

3. Type the following command to access global configuration mode:

config terminal

4. Type the following command to enable message logging:

logging on

5. Configure the syslog facility. The default is local7.

logging facility <facility, for example, local7>

6. Type the following command to log messages to your EventTracker Enterprise

logging <IP address of your EventTracker Enterprise >

7. Enable timestamp on log messages:

service timestamp log datetime

8. Return to privileged EXEC mode:

end

9. View your entries:

show running-config

10. Save your entries in the configuration file:

copy running-config startup-config

The configuration is complete. The log source is added to EventTracker Enterprise as Cisco Aironet events are automatically discovered. Events forwarded to EventTracker by Cisco Aironet appliances are displayed on the Log Search tab of EventTracker Enterprise.

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7.x to support Cisco Aironet device tab monitoring.

Categories

- **Cisco Aironet: 802.11 connection error** - This category based report provides information related to 802.11 connection error.
- **Cisco Aironet: Access point error** - This category based report provides information related to access point error.
- **Cisco Aironet: Accounting service error** - This category based report provides information related to accounting service error.
- **Cisco Aironet: Accounting services** - This category based report provides information related to accounting services.
- **Cisco Aironet: ARP error** - This category based report provides information related to ARP error.
- **Cisco Aironet: Authentication failed** - This category based report provides information related to authentication failed.
- **Cisco Aironet: Authentication success** - This category based report provides information related to authentication success.
- **Cisco Aironet: Configuration error** - This category based report provides information related to configuration error.
- **Cisco Aironet: Hot standby error** - This category based report provides information related to Hot standby error.
- **Cisco Aironet: Malicious attack** - This category based report provides information related to malicious attack.
- **Cisco Aironet: Network error** - This category based report provides information related to network error.

- **Cisco Aironet: Rogue detection** - This category based report provides information related to rogue AP detection.
- **Cisco Aironet: Station host** - This category based report provides information related to station host.
- **Cisco Aironet: System error** - This category based report provides information related to system error.
- **Cisco Aironet: VLAN error** - This category based report provides information related to VLAN error.

Alerts

- **Cisco Aironet: Access point error** - This alert is generated when access point error occurs.
- **Cisco Aironet: Authentication failed** - This alert is generated when authentication failure occurs.
- **Cisco Aironet: Configure error** - This alert is generated when configuration error occurs.
- **Cisco Aironet: Malicious attack** - This alert is generated when malicious attack occurs.
- **Cisco Aironet: Rogue detection** - This alert is generated when any rogue AP detected.

Import Cisco Aironet Knowledge Pack into EventTracker

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

To import Category

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

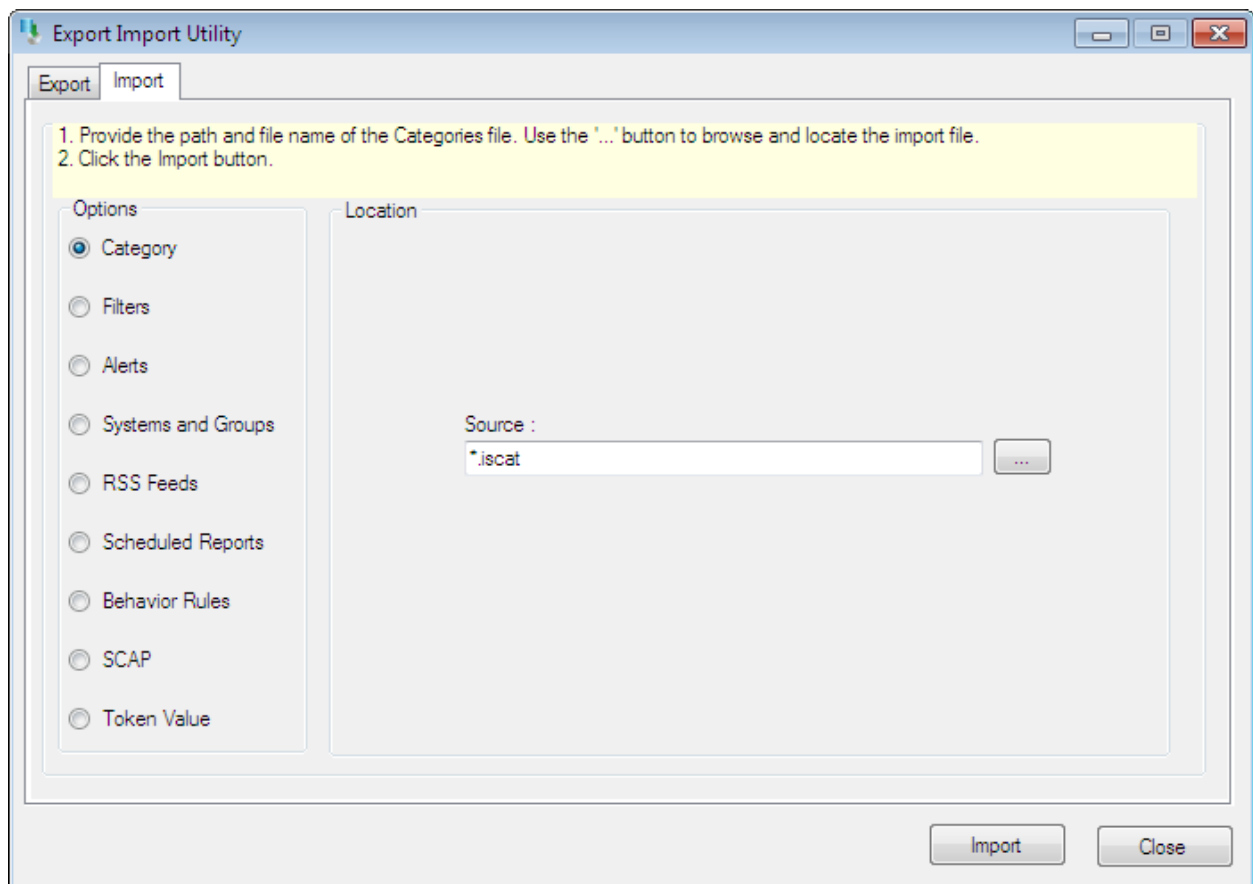


Figure 1

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

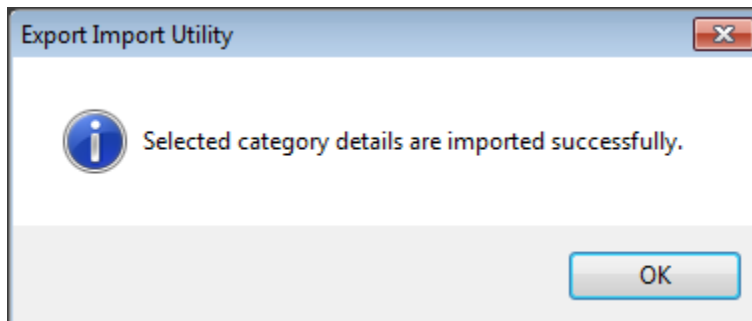



Figure 2

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

To import Alerts

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

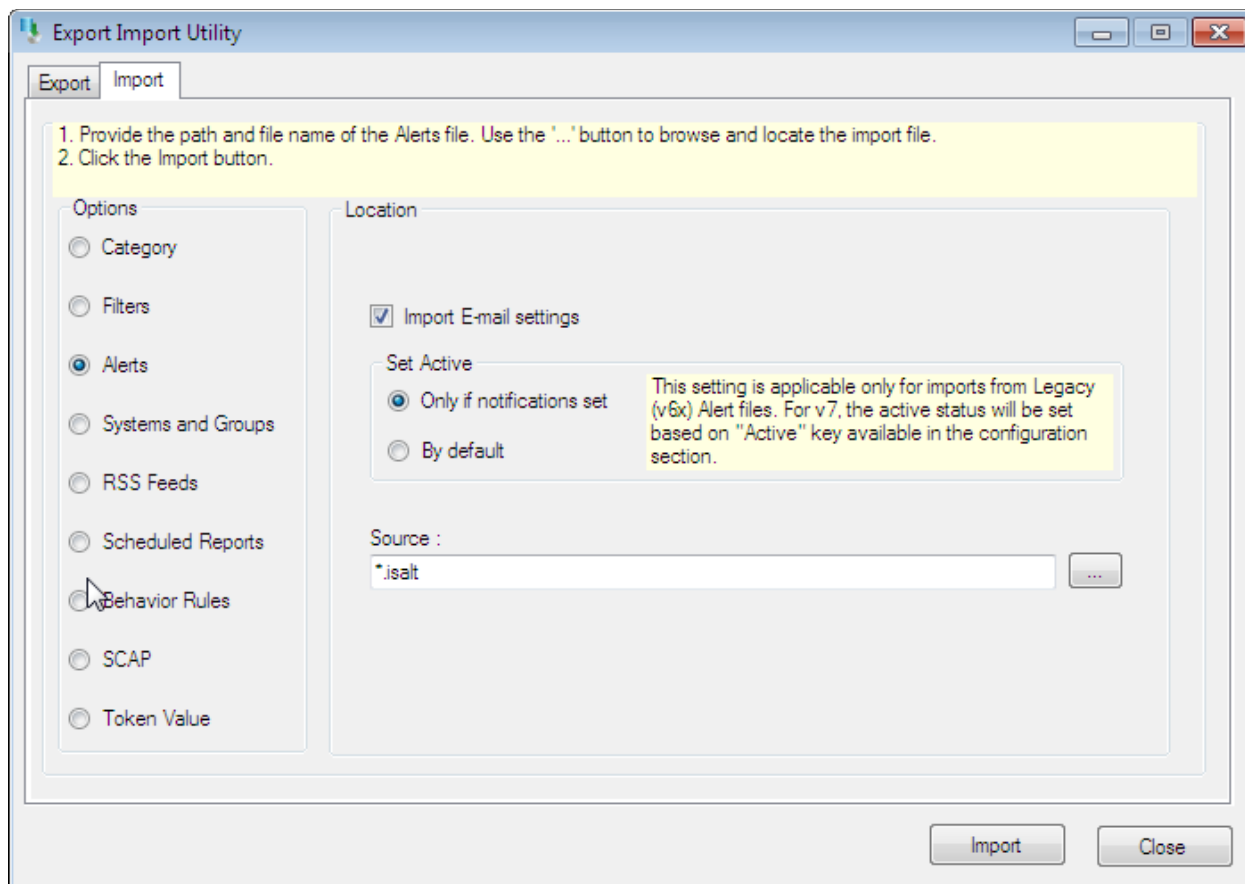


Figure 3

2. Locate **All Cisco Aironet group of Alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.

EventTracker displays success message.

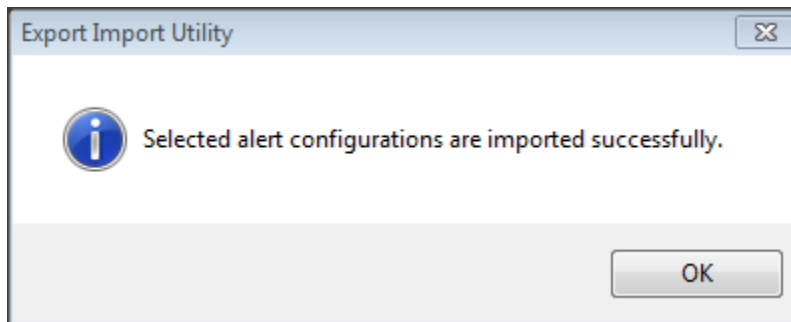


Figure 4

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

Verify Cisco Aironet knowledge pack in EventTracker

Verify Cisco Aironet Firewall Categories

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

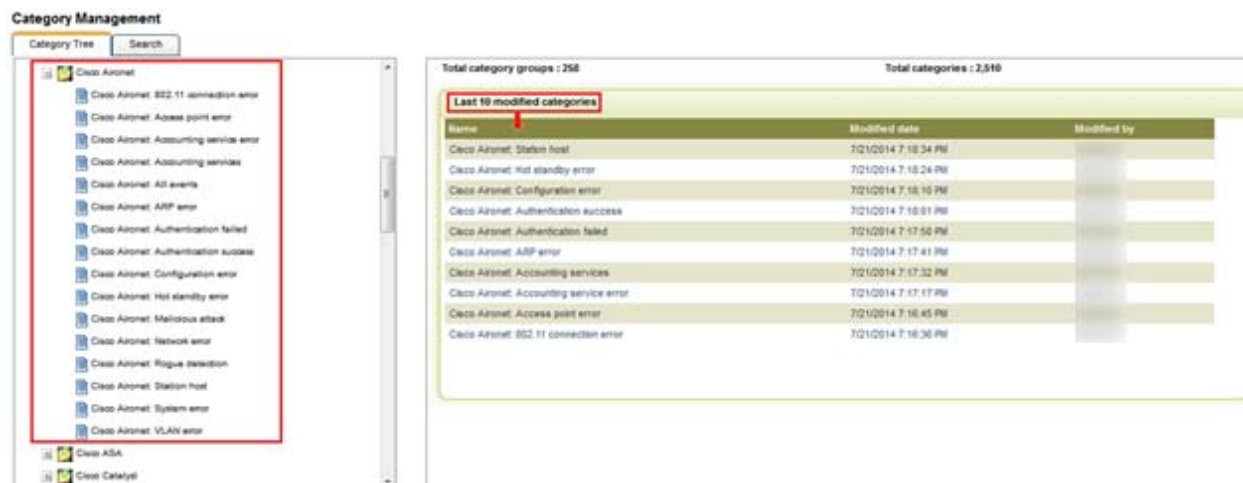


Figure 5

Verify Cisco Aironet Alerts

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



Figure 6

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

EventTracker displays message box.

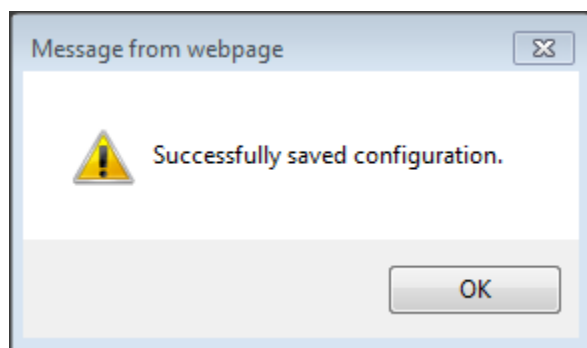


Figure 7

- 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.