

Integrate Active Directory

EventTracker v7.x

Publication Date: Aug 27, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks and included in most Windows Server operating systems as a set of processes and services.

An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network - assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.

This guide provides instructions to configure Active Directory to send the event logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and **Win server 2000, Win server 2003, Win server 2008, Win server 2008 R2, Win server 2012 and Win server 2012 R2**.

Audience

Active Directory users, who wish to forward event logs to EventTracker Manager and monitor events using Event Tracker Enterprise.

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.

Table of Contents

- Abstract..... 1
 - Scope 1
 - Audience..... 1
- Active Directory 3
- Prerequisites..... 3
 - Configure Active Directory to send events to EventTracker..... 3
- Monitoring Events of Active Directory 4
- Import Active Directory knowledge pack in EventTracker 5
 - Import Category..... 5
 - Import Alerts..... 6
- Verify Active Directory knowledge pack in EventTracker 7
 - Verify categories..... 7
 - Verify alerts..... 7
- EventTracker Knowledge Pack..... 9
 - Categories 9
 - Alerts 11
- Sample Report 12

Active Directory

Active Directory is a special-purpose database - it is not a registry replacement. The directory is designed to handle a large number of read and search operations and a significantly smaller number of changes and updates. Active Directory data is hierarchical, replicated, and extensible. Because it is replicated, you do not want to store dynamic data, such as corporate stock prices or CPU performance. If your data is machine-specific, store the data in the registry. Typical examples of data stored in the directory include printer queue data, user contact data, and network/computer configuration data. The Active Directory database consists of objects and attributes. Objects and attribute definitions are stored in the Active Directory schema.

Prerequisites

- EventTracker v7.x should be installed
- Windows server 2000 or later should be installed.
- Active Directory should be installed and configured.

Configure Active Directory to send events to EventTracker

Deploy [EventTracker Agent](#) on Active Directory machine. Once the events are triggered, logs will be sent to EventTracker automatically.

Monitoring Events of Active Directory

Monitoring AD events, provides detailed information about what is happening on your Domain. Using Event Tracker Enterprise Active Directory events can be monitored which are as follows:

- **Computers**
- **Group**
- **Group Policy**
- **Local Group**
- **Objects**
- **Organizational Unit**
- **Share Folders**

Import Active Directory knowledge pack in EventTracker

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

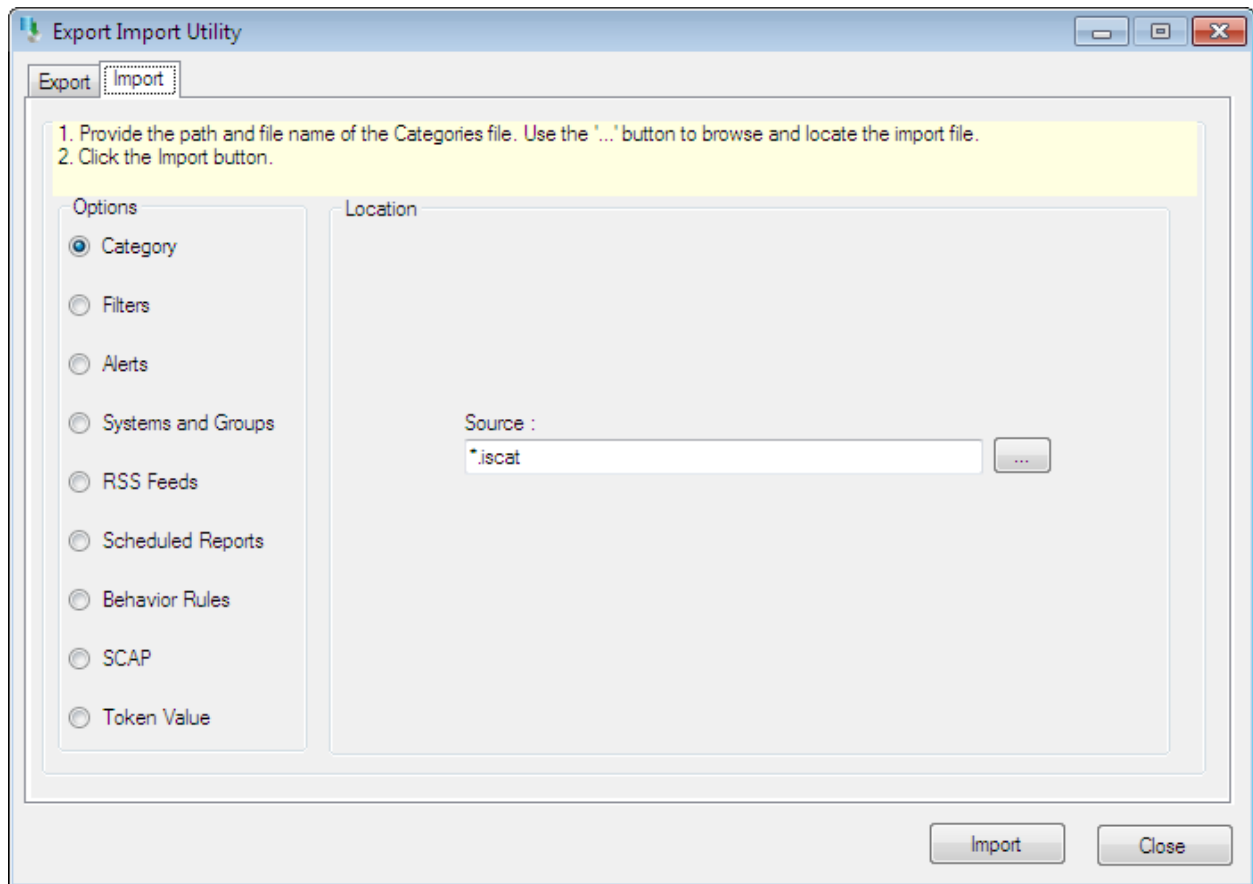


Figure 1

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

Import Category

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

2. Locate **Active Directory.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

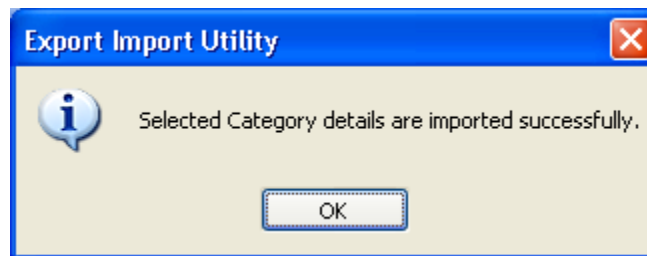



Figure 2

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

Import Alerts

1. Click **Alert** option, and then click the **browse**  button.
2. Locate **Active Directory.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

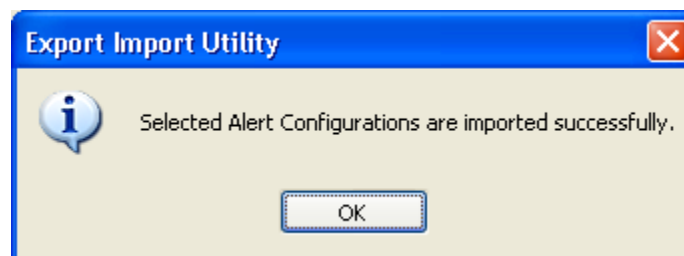


Figure 3

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

Verify Active Directory 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 **Windows**, and then expand **Active Directory** group folder.

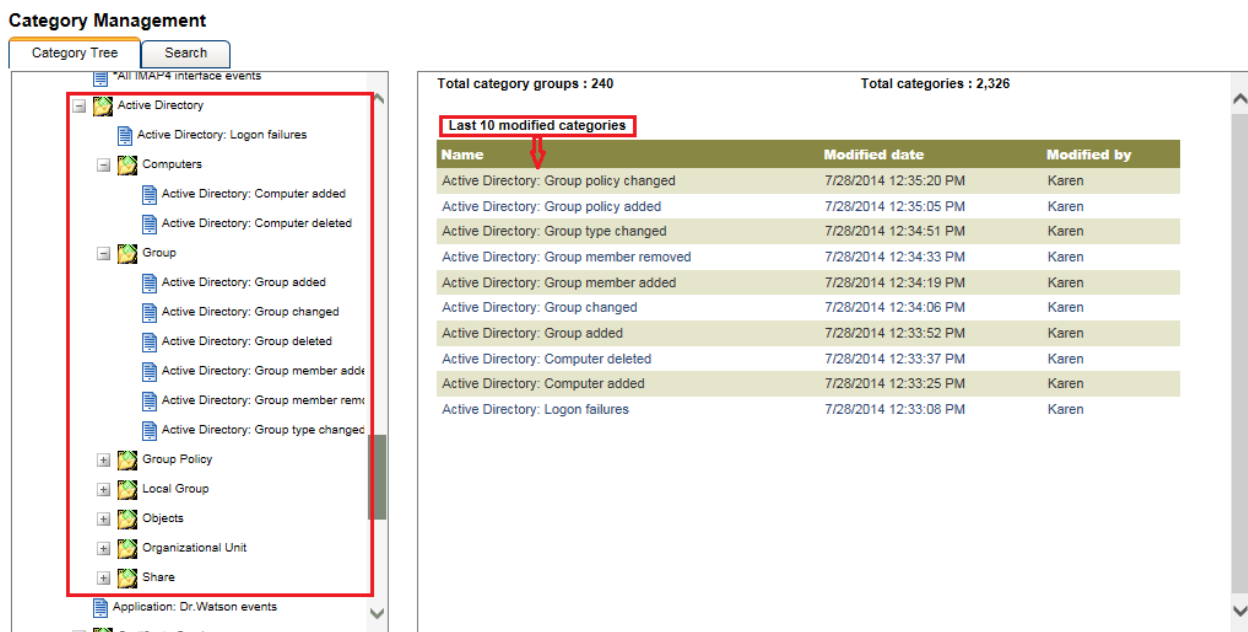


Figure 4

Verify alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** box, type '**Active Directory**', and then click the **Go** button.

Alert Management page will display all the imported alerts.

The screenshot shows the 'Alert Management' interface. At the top, there is a search bar containing 'Active Directory' and buttons for 'Go' and 'Show All'. On the right, the 'Page Size' is set to 25. Below this is a table with the following columns: Alert Name, Threat level, Active, Beep, E-mail, Message, RSS, Forward as SNMP, Forward as syslog, Remedial Action at Console, and Remedial Action at Agent. Three alerts are listed:

Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
Active Directory: Computer deleted	Undefined	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Active Directory: Group policy changed	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Active Directory: Group policy deleted	Undefined	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Below the table, there is a note: '***Click 'Activate Now' after making all changes'. To the right of this note are three buttons: 'Activate Now', 'Add alert', and 'Delete'.

Figure 5

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

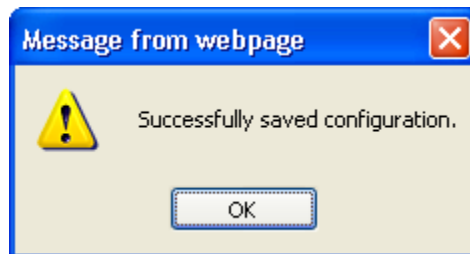


Figure 6

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

EventTracker Knowledge Pack

Categories

- ❖ **Active Directory Changed objects:** This category based report provides information related to Active Directory objects changed. Objects include users, computers, Organizational Units, shared folders, group and group policy.
- ❖ **Active Directory Computer added:** This category based report provides information related to computer added to Windows Active Directory.
- ❖ **Active Directory Computer deleted:** This category based report provides information related to computer deleted from Windows Active Directory.
- ❖ **Active Directory Created objects:** This category based report provides information related to Active Directory objects created. Objects include users, computers, Organizational Units, shared folders, group and group policy.
- ❖ **Active Directory Created share:** This category based report provides information related to share created in Windows environment.
- ❖ **Active Directory Deleted objects:** This category based report provides information related to Active Directory objects deleted. Objects include users, computers, Organizational Units, shared folders, group and group policy.
- ❖ **Active Directory Deleted share:** This category based report provides information related to share deleted.
- ❖ **Active Directory Group added:** This category based report provides information related to group added to Windows Active Directory.
- ❖ **Active Directory Group changed:** This category based report provides information related to any changes made to the group.
- ❖ **Active Directory Group deleted:** This category based report provides information related to group deleted from Windows Active Directory.
- ❖ **Active Directory Group member added:** This category based report provides information related to members added to the group.
- ❖ **Active Directory Group member removed:** This category based report provides information related to members are removed from Active Directory group.

- ❖ **Active Directory Group policy added:** This category based report provides information related to group policy added to Windows Active Directory.
- ❖ **Active Directory Group policy changed:** This category based report provides information related to group policy changed in Windows Active Directory.
- ❖ **Active Directory Group policy deleted:** This category based report provides information related to group policy link deleted or group policy permanently deleted from Windows Active Directory.
- ❖ **Active Directory Local group added:** This category based report provides information related to local group added to Active Directory.
- ❖ **Active Directory Local group deleted:** This category based report provides information related to local group deleted from Active Directory.
- ❖ **Active Directory Local group renamed:** This category based report provides information related to local group renamed in Active Directory.
- ❖ **Active Directory Logon failures:** This category based report provides information related to authentication request failed.
- ❖ **Active Directory Moved objects:** This category based report provides information related to Active Directory objects moved. This event is logged on Windows server 2008 and later operating system.
- ❖ **Active Directory Object Modified:** This category based report provides information related to directory service object was modified.
- ❖ **Active Directory OU added:** This category based report provides information related to Organization Unit added to Active Directory.
- ❖ **Active Directory OU changed:** This category based report provides information related to Organization Unit parameter changed in Active Directory.
- ❖ **Active Directory OU deleted:** This category based report provides information related to Organization Unit deleted from Active Directory.
- ❖ **Active Directory Renamed share:** This category based report provides information related to a share is renamed.
- ❖ **Active Directory Share folder added:** This category based report provides information related to a share folder added.
- ❖ **Active Directory Share folder deleted:** This category based report provides information related to share folder deleted.

- ❖ **Active Directory Sub OU added:** This category based report provides information related to a Sub Organizational Unit Added.
- ❖ **Active Directory Sub OU deleted:** This category based report provides information related to a Sub Organizational Unit deleted.
- ❖ **Active Directory Undeleted objects:** This category based report provides information related to Active directory objects undeleted. This event is logged on Windows server 2008 and later operating system.

Alerts

- ❖ **Active Directory Computer deleted:** This alert is generated when computer is deleted from Windows Active Directory.
- ❖ **Active Directory The Active Directory database is corrupt:** This alert is generated when active directory database is corrupt.
- ❖ **Active Directory Group policy changed:** This alert is generated when group policy is changed in Windows Active Directory.
- ❖ **Active Directory Group policy deleted:** This alert is generated when group policy link is deleted or group policy permanently deleted from Windows Active Directory.
- ❖ **Active Directory Database and log file drive error:** This alert is generated when database or log file drive exceeds the storage limit or is full.
- ❖ **Active Directory Global catalog error:** This alert is generated when specified domain either does not exist or could not be contacted.

Sample Report

The detail of a sample report is given below.

LogTime	EventUser	Computer	AD Object Name	Object Type	AD Object Access type	AD Admin User Name
07/21/2014 03:00:12 AM	MAILSS	SHIELD2	CN=Karen,OU=PNPL,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:12 AM	MAILSS	SHIELD2	CN=Karen,OU=PNPL,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:14 AM	MAILSS	SHIELD2	CN=S,OU=PNPL,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:14 AM	MAILSS	SHIELD2	CN=S,OU=PNPL,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:36 AM	MAILSS	SHIELD2	CN=S,OU=PNPL,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:50 AM	MAILSS	SHIELD2	CN=Jason Smith,OU=PNPL,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:50 AM	MAILSS	SHIELD2	CN=Jason Smith,OU=PNPL,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:51 AM	MAILSS	SHIELD2	CN=Jack,OU=PMI,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:51 AM	MAILSS	SHIELD2	CN=Jack,OU=PMI,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:51 AM	MAILSS	SHIELD2	CN=John,OU=DistGroups,OU=Office365,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:00:53 AM	fury	SHIELD3-DLA	CN=Cloud ETAdmin,OU=CloudUsers,OU=EventTrackerCloud,DC=information,DC=com	user	Write Property	fury
07/21/2014 03:01:02 AM	MAILSS	SHIELD2	CN=Jack,OU=PMI,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:01:02 AM	MAILSS	SHIELD2	CN=Jack,OU=PMI,DC=information,DC=com	user	Read Property	MAILSS
07/21/2014 03:01:02 AM	MAILSS	SHIELD2	CN=Steve Rogers,OU=PMI,DC=information,DC=com	user	Read Property	MAILSS

Figure 7