Integrate Active Directory Audit

EventTracker v8.x and above

Publication Date: April 7, 2017
Abstract

This guide helps you in configuring Active Directory with EventTracker to receive Active Directory events. In this document you will find the detailed procedures required for monitoring Active Directory.

Audience

Administrators who are assigned the task to monitor and manage Active Directory events 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.

© 2017 EventTracker Security LLC. 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
Audience .................................................................................................................................................................. 1
Overview ............................................................................................................................................................... 3
Prerequisites ............................................................................................................................................................ 3
Enabling of Active Directory Audit events ............................................................................................................. 3
Configure Active Directory to send events to EventTracker .................................................................................. 8
Monitoring Events of Active Directory .................................................................................................................. 8
    EventTracker Knowledge Pack................................................................................................................................ 8
        Flex Reports ..................................................................................................................................................... 8
        Alerts ............................................................................................................................................................... 17
Import Active Directory knowledge pack into EventTracker ...................................................................................... 17
    Parsing Rule....................................................................................................................................................... 18
    Flex Reports ..................................................................................................................................................... 19
    Alerts ............................................................................................................................................................... 20
Verify Active Directory knowledge pack in EventTracker ......................................................................................... 21
    Alerts ............................................................................................................................................................... 21
    Flex Reports ..................................................................................................................................................... 22
Template ................................................................................................................................................................. 23
Create Flex Dashboards in EventTracker ................................................................................................................... 24
    Schedule Reports............................................................................................................................................... 24
    Create Dashlets................................................................................................................................................ 27
Sample Flex Dashboards ......................................................................................................................................... 30
Overview

This guide addresses the Windows default audit policy settings, baseline recommended audit policy settings, and the more aggressive recommendations from Microsoft, for workstation and server products.

The SCM baseline recommendations shown here, along with the settings recommend to help detect compromise, are intended only to be a starting baseline guide to administrators. Each organization must make its own decisions regarding the threats they face, their acceptable risk tolerances, and what audit policy categories or subcategories they should enable. The Administrators without a thoughtful audit policy in place are encouraged to start with the settings recommended here, and then to modify and test, prior to implementing in their production environment.

Prerequisites

- EventTracker v8.x should be installed.
- Active Directory should be installed and configured.
- Recommended Audit Policies by the OS
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2008
  - Windows 8
  - Windows 7

Enabling of Active Directory Audit events

1. Open the Run command window, and run the command `gpedit.msc`

![Image of Run command window](Figure 1)
2. Local group policy editor window will now appear.

![Local Group Policy Editor](image)

Figure 2

3. Click on **Windows Settings** dropdown under Computer Configuration and choose **Security Settings** as shown in the below image.
4. Click on **Security settings** dropdown, and click on **System Audit Policies-Local Group Policy Object**.
5. Double click on the policies that need to be enabled for auditing.

6. Auditing can be enabled for both Success/Failure events.

7. For e.g. if an **Account Logon** auditing for **Kerberos Authentication Service** needs to be enabled for Success/Failure events, highlight the **Account Logon** option and double click on **Kerberos Authentication Service** as shown in the below image.

![Diagram showing Local Computer Policy and Advanced Audit Policy Configuration](image)

**Figure 5**

8. Once double clicked, another window will pop up. Click the checkbox **“Configure the following audit events”** and also the checkbox **Success** and **Failure** options as shown in the below image.

![Another window with checkboxes](image)
9. Click on **Apply** and then **OK**.
10. Now the auditing is enabled for **Kerberos Authentication Services**.
11. In the below **Flex Report** section, detailed **Category** and **Sub category** fields are provided which needs to be enabled for auditing for that specific report.
12. Enabling of auditing can be done for both the Local Computer and User Configuration in the same way as steps given above.
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 EventTracker Enterprise, Active Directory events can be monitored which are as follows:

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

EventTracker Knowledge Pack

Once logs are received into EventTracker, Alerts, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Flex Reports

Below given are the list of reports along with the table that gives the category of Audit events which needs to be enabled.

1. Active Directory- Account logon events: This report provides details about all the successful logon, successful log off, special privileges logon and Logon failures done in Windows Active Directory.

Audit Events that needs to be enabled:
2. **Active Directory-Account management activities**: This report provides all the details about an account if it is created, deleted, changed, enabled or disabled in Windows Active Directory.

**Audit Events that needs to be enabled:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub Category</th>
<th>Event ID</th>
<th>Audit Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon/Logoff</td>
<td>Audit Account Lockout</td>
<td>4740- A User account was locked out</td>
<td>Enable Success/Failure</td>
</tr>
<tr>
<td></td>
<td>An Account was logged off</td>
<td>4634- An account was logged off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Initiated Log off</td>
<td>4647- User initiated logoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Logoff</td>
<td>538- User logoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Special Logon</td>
<td>4672-Special privileges assigned to new logon</td>
<td></td>
</tr>
</tbody>
</table>
3. **Active Directory-Audit detailed directory service replication**: This report provides the details about an Active Directory replica source naming context if it is established, removed, modified or failed.

**Audit Events that needs to be enabled:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Action</th>
<th>Source Account Name</th>
<th>Source Account Domain</th>
<th>Source Security ID</th>
<th>Target account name</th>
<th>Target account domain</th>
<th>Target security ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/30/2017 01:23:43 PM</td>
<td>PNPL-6-KP</td>
<td>A computer account was created.</td>
<td>Administrator</td>
<td>ACME</td>
<td>ACME\Administrator</td>
<td>WS2321$</td>
<td>ACME</td>
<td>S-1-5-21-3108364787-189202583-342365621-1000</td>
</tr>
<tr>
<td>03/30/2017 01:23:43 PM</td>
<td>PNPL-6-KP</td>
<td>A computer account was deleted.</td>
<td>Administrator</td>
<td>ACME</td>
<td>ACME\Administrator</td>
<td>WS2321$</td>
<td>ACME</td>
<td>S-1-5-21-3108364787-189202583-342365621-1000</td>
</tr>
<tr>
<td>03/30/2017 01:23:44 PM</td>
<td>PNPL-6-KP</td>
<td>A user account was enabled.</td>
<td>ACME-FR</td>
<td>ACME-FR\Administrator</td>
<td>John.Locke</td>
<td>ACME-FR</td>
<td>ACME-FR\John.Locke</td>
<td>ACME-FR\John.Locke</td>
</tr>
<tr>
<td>03/30/2017 01:23:44 PM</td>
<td>PNPL-6-KP</td>
<td>A user account was disabled.</td>
<td>Administrator</td>
<td>WIN-R9H529RIO4\Y Administrator</td>
<td>WIN-R9H529RIO4\Y Administrator</td>
<td>Bob</td>
<td>WIN-R9H529RIO4\Y</td>
<td>Bob</td>
</tr>
</tbody>
</table>

---

**Figure 8**
System Audit Policies-Local Group Policy Object

<table>
<thead>
<tr>
<th>DS Access</th>
<th>Audit Detailed Directory Service Replication</th>
<th>4928- An Active Directory replica source naming context was established.</th>
<th>Enable Success/Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>4929- An Active Directory replica source naming context was removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4930- An Active Directory replica source naming context was modified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4931- An Active Directory replica destination naming context was modified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4934- Attributes of an Active Directory object was replicated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4935- Replication failure begins.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4936- Replication failure ends</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4937- A lingering object was removed from a replica.</td>
<td></td>
</tr>
</tbody>
</table>

Directory Services Restore Mode:
5376- Credential Manager credentials were backed up
5377- Credential Manager credentials were restored from a backup

Report Sample:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Action</th>
<th>Destination DRA</th>
<th>Source DRA</th>
<th>Source Address</th>
<th>Naming Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/03/2017 01:39:44 PM</td>
<td>PNPL-8-KP-WINDOWS</td>
<td>An Active Directory replica source naming context was established.</td>
<td>CN=NTDS Settings,CN=WIN-R89529RIO4Y,CN=First-Name,Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local</td>
<td>CN=NTDS Settings,CN=WIN-R857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local</td>
<td>0663afed-1e41-43a3-CN=NTDS</td>
<td>Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local</td>
</tr>
<tr>
<td>04/03/2017 01:39:45 PM</td>
<td>PNPL-8-KP-WINDOWS</td>
<td>An Active Directory replica source naming context was removed.</td>
<td>CN=NTDS Settings,CN=WIN-R89529RIO4Y,CN=First-Name,Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local</td>
<td>CN=NTDS Settings,CN=WIN-R857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local</td>
<td>0663afed-1e41-43a3-CN=NTDS</td>
<td>Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local</td>
</tr>
</tbody>
</table>

Figure 9
4. **Active Directory-Audit directory service changes**: This report provides all the directory configuration changes such as a directory being created, deleted, modified, moved or undeleted.

**Audit Events that needs to be enabled:**

<table>
<thead>
<tr>
<th>System Audit Policies-Local Group Policy Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS Access</td>
</tr>
<tr>
<td>Audit Directory Service Changes</td>
</tr>
<tr>
<td>5136- A directory service object was modified.</td>
</tr>
<tr>
<td>5137- A directory service object was created.</td>
</tr>
<tr>
<td>5138- A directory service object was undeleted.</td>
</tr>
<tr>
<td>5139- A directory service object was moved.</td>
</tr>
<tr>
<td>5141- A directory service object was deleted.</td>
</tr>
<tr>
<td>Enable Success/Failure</td>
</tr>
</tbody>
</table>

**Report Sample:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Action</th>
<th>Source Account Name</th>
<th>Source Account Domain</th>
<th>Directory service name</th>
<th>Directory service type</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/03/2017 02:58:10 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A directory service object was modified.</td>
<td>Administrator</td>
<td>ACME-FR</td>
<td>acme.com</td>
<td>Active Directory Domain Services</td>
</tr>
<tr>
<td>04/03/2017 02:58:10 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A directory service object was created.</td>
<td>Administrator</td>
<td>ACME</td>
<td>acme.local</td>
<td>Active Directory Domain Services</td>
</tr>
<tr>
<td>04/03/2017 02:58:10 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A directory service object was undeleted.</td>
<td>Carlos</td>
<td>CONTOSO</td>
<td>Contoso.com</td>
<td>Active Directory Domain Services</td>
</tr>
<tr>
<td>04/03/2017 02:58:10 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A directory service object was moved.</td>
<td>Administrator</td>
<td>ACME</td>
<td>acme.local</td>
<td>Active Directory Domain Services</td>
</tr>
<tr>
<td>04/03/2017 02:58:10 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A directory service object was deleted.</td>
<td>administrator</td>
<td>ACME</td>
<td>acme.com</td>
<td>Active Directory Domain Services</td>
</tr>
</tbody>
</table>

**Figure 10**

5. **Active Directory- Audit directory service replication**: This report provides all the directory service replication details.

**Audit Events that needs to be enabled:**

<table>
<thead>
<tr>
<th>System Audit Policies-Local Group Policy Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS Access</td>
</tr>
<tr>
<td>Audit Directory Service Replication</td>
</tr>
<tr>
<td>4932- Synchronization of a replica of an Active Directory naming context has begun.</td>
</tr>
<tr>
<td>4933- Synchronization of a replica of an Active Directory naming context has ended.</td>
</tr>
<tr>
<td>Enable Success/Failure</td>
</tr>
</tbody>
</table>
6. **Active Directory-Audit DPAPI activity**: This report provides all Audit DPAPI activity.

**Audit Events that needs to be enabled:**

<table>
<thead>
<tr>
<th>Detailed Tracking</th>
<th>Audit DPAPI Activity</th>
<th>System Audit Policies-Local Group Policy Object</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>4692- Backup of data protection master key was attempted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4693- Recovery of data protection master key was attempted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4694- Protection of auditable protected data was attempted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4695- Un-protection of auditable protected data was attempted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable Success/Failure</td>
</tr>
</tbody>
</table>

**Report Sample:**

![Table showing Active Directory Audit DPAPI activity](image)
7. **Active Directory-Audit process termination**: This report provides all the terminated or exited process details.

**Audit Events that needs to be enabled**:

<table>
<thead>
<tr>
<th>System Audit Policies-Local Group Policy Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed Tracking</td>
</tr>
</tbody>
</table>

**Report Sample**:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Action</th>
<th>Source Account Name</th>
<th>Source Account Domain</th>
<th>Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/04/2017 03:00:00 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A process has exited.</td>
<td>Edward</td>
<td>Contoso</td>
<td>C:\Windows\System32\conhost.exe</td>
</tr>
<tr>
<td>04/04/2017 03:00:00 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A process has exited.</td>
<td>Zoe</td>
<td>Contoso</td>
<td>C:\Program Files (x86)\Microsoft\Tracker\Web\bin\sm.Tracker.ipresolver.exe</td>
</tr>
</tbody>
</table>

**Figure 13**

8. **Active Directory-Audit Kerberos authentication service**: This report provides details about all the Kerberos authentication services.

**Audit Events that needs to be enabled**:

<table>
<thead>
<tr>
<th>System Audit Policies-Local Group Policy Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Logon</td>
</tr>
</tbody>
</table>

**EventTracker**

Actionable Security Intelligence
9. **Active Directory-Audit Kerberos service ticket operation:** This report provides details about all the Kerberos service ticket operations, whether it was requested or renewed.

**Audit Events that needs to be enabled:**

<table>
<thead>
<tr>
<th>System Audit Policies-Local Group Policy Object</th>
<th>Account Logon</th>
<th>Audit Kerberos Service Ticket Operation</th>
<th>4769- A Kerberos service ticket was requested</th>
<th>4770- A Kerberos service ticket was renewed</th>
<th>Enable Success/Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>4769- A Kerberos service ticket was requested</td>
<td>4770- A Kerberos service ticket was renewed</td>
<td></td>
</tr>
</tbody>
</table>

**Report Sample:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Action</th>
<th>Source Account Name</th>
<th>Source Domain Name</th>
<th>Client Address</th>
<th>Service ID</th>
<th>Service ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/15/2017 05:51:42 PM</td>
<td>PNPL-6-KP</td>
<td>A Kerberos authentication ticket (TGT) was requested.</td>
<td>Dave</td>
<td>neon-sw</td>
<td>NEON-SWDAVE</td>
<td>NEON-SWkrtgt</td>
<td>192.168.1.118</td>
</tr>
<tr>
<td>03/15/2017 05:51:42 PM</td>
<td>PNPL-6-KP</td>
<td>A Kerberos authentication ticket request failed.</td>
<td>Basil</td>
<td>Contoso-us</td>
<td>Contoso-us\Basil</td>
<td>krbtgt/contoso-us</td>
<td>172.14.129.56</td>
</tr>
<tr>
<td>03/15/2017 05:51:42 PM</td>
<td>PNPL-6-KP</td>
<td>Kerberos pre-authentication failed.</td>
<td>Administrator</td>
<td>ACME</td>
<td>ACME\Administrator</td>
<td>krbtgt/acme-fr</td>
<td>10.42.42.224</td>
</tr>
</tbody>
</table>

10. **Active Directory-Audit RPC events:** This report provides details about all the RPC events that were attempted.
Audit Events that needs to be enabled:

<table>
<thead>
<tr>
<th>System Audit Policies-Local Group Policy Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed Tracking</td>
</tr>
</tbody>
</table>

Report Sample:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Action</th>
<th>Source Account Name</th>
<th>Source Account Domain</th>
<th>Process Name</th>
<th>Remote IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/04/2017 03:56:54 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A Remote Procedure Call (RPC) was attempted</td>
<td>wewdrr</td>
<td>WERSDF</td>
<td>C:\Windows\Systemroot</td>
<td>192.124.42.32</td>
</tr>
<tr>
<td>04/04/2017 03:56:54 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A Remote Procedure Call (RPC) was attempted</td>
<td>randyor</td>
<td>RFCINL</td>
<td>C:\Windows\Systemroot</td>
<td>192.168.1.118</td>
</tr>
</tbody>
</table>

Figure 16

11. **Active Directory-Audit other accounts logon events**: This report provides details about all the account logon events.

Audit Events that needs to be enabled:

<table>
<thead>
<tr>
<th>System Audit Policies-Local Group Policy Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Logon</td>
</tr>
</tbody>
</table>
Report Sample:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Action</th>
<th>Security ID</th>
<th>Source Account Name</th>
<th>Source Account Domain</th>
<th>Session Name</th>
<th>Mac address</th>
<th>Client Name</th>
<th>Client Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/04/2017 04:59:00 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A session was disconnected to a Window Station.</td>
<td>Administrator</td>
<td>WIN-RSH529R1014Y</td>
<td>RDP-Tcp#0</td>
<td>XPEDIT</td>
<td>10.42.42.21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04/04/2017 04:58:00 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A session was reconnected to a Window Station.</td>
<td>Administrator</td>
<td>WIN-RSH529R1014Y</td>
<td>RDP-Tcp#0</td>
<td>XPEDIT</td>
<td>10.42.42.21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04/04/2017 04:58:01 PM</td>
<td>PNPL-6-KP-WINDOWS</td>
<td>A request was made to authenticate to a wireless</td>
<td>Contoso\Rooney</td>
<td>Contoso</td>
<td>2e:33:d7:ff:8:ac2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 17

Alerts

1. **Active Directory-Account management activities**: This alert is generated when any account is created, deleted, changed, enabled or disabled in Windows Active Directory.
2. **Active Directory-Account logon events**: This alert is generated when any successful logon, successful log off, special privileges logon or Logon failures is done in Windows Active Directory.
3. **Active Directory-Audit detailed directory service replication**: This alert is generated when an Active Directory replica source naming context is established, removed, modified or failed.
4. **Active Directory-Audit Dpapi activity**: This alert is generated when backup or recovery of data protection master key is attempted.
5. **Active Directory-Audit Kerberos authentication**: This alert is generated when a Kerberos authentication ticket is requested or failed.

**Import Active Directory knowledge pack into EventTracker**

**NOTE**: Import knowledge pack items in the following sequence:

- Token templates
- Flex Reports
- Alerts
1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

3. Click the **Import** tab.

**Parsing Rule**

1. Click **Token Value** option, and then click the browse button.
2. Locate the All Active Directory group of Token Value.issch file, and then click the Open button.
3. Click the **Import** button to import the tokens. EventTracker displays success message.

![Export Import Utility](image)

**Figure 19**

**Flex Reports**

1. Click **Reports** option, and then click the browse button.
2. Locate the **All Active Directory group of flex reports.issch** file, and then click the **Open** button.

![Export Import Utility](image)

**Figure 20**
3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

![Figure 21](image1.png)

**Figure 21**

**Alerts**

1. Click **Alerts** option, and then click the browse button.
2. Locate the **All Active Directory.jsalt** file, and then click the **Open** button.

![Figure 22](image2.png)

**Figure 22**
2. To import alerts, click the **Import** button. EventTracker displays success message.

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

**Verify Active Directory knowledge pack in EventTracker Alerts**

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type **Active Directory**, and then click **Go** button.
3. Alert Management page will display the imported **Active Directory** alert.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Figure 26](image)

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.

**Flex Reports**

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter ‘**Active Directory**, and then click the **Search** button.
EventTracker displays Flex reports of ‘Active Directory’.

![Figure 27](image)

**Template**

1. Logon to *EventTracker Enterprise* web interface.
2. Click the *Admin* menu, and then click *Parsing Rules*.
Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.

4. Click on ‘schedule’ to plan a report for later execution.
5. Click Next button to proceed.
6. In review page, check Persist data in EventVault Explorer option.
7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

---

Figure 31

Figure 32
8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

### Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

![Figure 33: Flex Dashboard pane is shown.](image)

2. Navigate to **Dashboard>Flex**.
Flex Dashboard pane is shown.

![Figure 34: FLEX DASHBOARD](image)
3. Fill suitable title and description and click **Save** button.
4. Click 🔄 to configure a new flex dashlet. Widget configuration pane is shown.

![Figure 35](image)

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.

15. Click ‘customize’ 📦 to locate and choose created dashlet.
16. Click ⬆️ to add dashlet to earlier created dashboard.
Sample Flex Dashboards

- **WIDGET TITLE**: Active Directory-Account management Activity
  - **CHART TYPE**: Stacked Column
  - **AXIS LABELS [X-AXIS]**: Account Name
  - **LEGEND [SERIES]**: Action

![Active Directory-Account management Activity](image)

**Figure 38**

- **WIDGET TITLE**: Active Directory-Audit Dpapi activity
  - **CHART TYPE**: Stacked Column
  - **AXIS LABELS [X-AXIS]**: Account Name
  - **LEGEND [SERIES]**: Action

![Active Directory-Audit Dpapi activity](image)

**Figure 39**
- **WIDGET TITLE**: Active Directory-Audit detailed directory services
- **CHART TYPE**: Donut
- **AXIS LABELS [X-AXIS]**: Action

![Donut Chart](image-url)

**Figure 40**
- **WIDGET TITLE:** Active Directory-Audit directory service replication
- **CHART TYPE:** Donut
- **AXIS LABELS [X-AXIS]:** Action
- **LEGEND [SERIES]:** Computer

![Figure 41](image-url)
• **WIDGET TITLE:** Active Directory-Audit directory service changes  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Account Name  
**LEGEND [SERIES]:** Computer

![](image)

*Figure 42*
- **WIDGET TITLE:** Active Directory-Audit Kerberos service ticket operation
- **CHART TYPE:** Stacked Column
- **AXIS LABELS [X-AXIS]:** Account Name
- **LEGEND[SERIES]:** Service Name

![Active Directory-Audit Kerberos service ticket operation](image)

*Figure 43*
• **WIDGET TITLE**: Active Directory-Audit process termination  
**CHART TYPE**: Donut  
**AXIS LABELS [X-AXIS]**: Account Name  
**LEGEND [SERIES]**: Action

![Figure 44](image-url)
- **WIDGET TITLE:** Active Directory-Audit other account logon events
- **CHART TYPE:** Donut
- **AXIS LABELS [X-AXIS]:** Account Name
- **LEGEND [SERIES]:** Source Account Domain

![Active Directory Audit Chart](image)

**Figure 45**