Integrate Cisco Identity Services Engine (ISE) 
EventTracker v7.x
Abstract

This guide provides instructions to configure Cisco Identity Services Engine (ISE) 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 Identity Services Engine (ISE) v1.0.2 and later.

Audience

Cisco Identity Services Engine (ISE) users, who wish to forward syslog messages to EventTracker Manager.
# Table of Contents

Cisco Identity Services Engine (ISE)........................................................................................................... 3  
Prerequisites ............................................................................................................................................. 3  
  Specific Prerequisites for Cisco ISE .................................................................................................... 3  
  General Prerequisites for Cisco ISE .................................................................................................... 3  
Configure Cisco Identity Services Engine ................................................................................................. 4  
EventTracker Knowledge Pack (KP) ........................................................................................................... 5  
  Categories ................................................................................................................................................ 5  
  Alerts ........................................................................................................................................................ 5  
Import ISE knowledge pack in EventTracker ............................................................................................. 6  
  To import Category ................................................................................................................................... 6  
  To import Alerts ...................................................................................................................................... 7  
  To import Tokens ..................................................................................................................................... 8  
  To import Flex Reports ........................................................................................................................... 9  
Verify Cisco ISE knowledge pack in EventTracker .................................................................................. 11  
  Verify Cisco ISE Categories ................................................................................................................ 11  
  Verify Cisco ISE Alerts ......................................................................................................................... 11  
  Verify Cisco ISE Tokens ....................................................................................................................... 12  
  Verify Cisco ISE Flex Reports .............................................................................................................. 13
Cisco Identity Services Engine (ISE)

Cisco Identity Services Engine (ISE) is a security policy management and control platform. It automates and simplifies access control, security compliance for wired, wireless, and VPN connectivity. Cisco ISE is primarily used to provide secure access and guest access, support BYOD initiatives, and enforce usage policies in conjunction with Cisco TrustSec.

The EventTracker supports Cisco ISE Log events. The log subscription policy consists of specific rules enabling access logging used to capture events to a local file where the EventTracker can collect them. These access events are collected and parsed into the EventTracker report tables for later review.

Prerequisites

Prior to integrating Cisco ISE with the EventTracker Enterprise, ensure that you meet the following prerequisites.

Specific Prerequisites for Cisco ISE
- Cisco Identity Services Engine device v1.0.2
- EventTracker Enterprise version 7.X and later

General Prerequisites for Cisco ISE
- Administrative access on the Cisco ISE device
- Administrative access on the EventTracker
Configure Cisco Identity Services Engine

To create Logging Target:

1. From the ISE Administration Interface, select **Administration > System > Logging > Remote Logging Targets**.
2. Click the **Add** button.
3. Configure the following fields:
   - **Name** - Enter the name of the new target.
   - **Target Type** - By default it is set to Syslog. The value of this field cannot be changed.
   - **Description** - Enter a brief description of the new target.
   - **IP Address** - Enter the IP address of the destination machine (EventTracker Enterprise) where you want to store the logs.
   - **Port** - Enter the port number of the destination machine (514 is default for syslog).
   - **Facility Code** - Select the syslog facility code to be used for logging. Valid options are Local0 through Local7.
   - **Maximum Length** - Enter the maximum length of the remote log target messages. Valid options are from 200 to 1024 bytes.
4. Click **Save**.

To edit Logging Categories:

1. From the ISE Administration Interface, select **Administration > System > Logging > Logging Categories**.
2. Click **AAA Audit > Failed Attempts**.
3. Highlight the Remote Logging Target created in the previous step; click the Right Arrow to add it to the **Selected** section.
4. Click **Save**.
5. Repeat for the remaining logging categories.
   - **AAA Audit > Failed Attempts**
   - **AAA Audit > Passed Authentications**
   - **AAA Diagnostics > Policy Diagnostics**
   - **Administrative and Operational Audit**
EventTracker Knowledge Pack ( KP )

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

The following Knowledge Packs are available in EventTracker v7. x to support Cisco ISE monitoring:

Categories

- **Cisco ISE: Administrator authentication failed** - This category based report provides information related to administrator authentication failed.
- **Cisco ISE: Administrator authentication success** - This category based report provides information related to administrator authentication success.
- **Cisco ISE: Administrator session rejected** - This category based report provides information related to administrator session rejected.
- **Cisco ISE: Configuration changed** - This category based report provides information related to configuration changed.
- **Cisco ISE: Configuration deleted** - This category based report provides information related to configuration deleted.
- **Cisco ISE: User password change failed** - This category based report provides information related to user password change failed.
- **Cisco ISE: User password changed** - This category based report provides information related to user password changed.

Alerts

- **Cisco ISE: Administrator authentication failed** - This alert is generated when administrator authentication has failed from Cisco ISE.
- **Cisco ISE: Configuration added** - This alert is generated when configuration is added from Cisco ISE.
- **Cisco ISE: Configuration changed** - This alert is generated when configuration is changed from Cisco ISE.
- **Cisco ISE: Configuration deleted** - This alert is generated when configuration is deleted from Cisco ISE.
- **Cisco ISE: User password change failed** - This alert is generated when a user password change has failed from Cisco ISE.
Import ISE knowledge pack in EventTracker

1. Launch EventTracker Control Panel.
2. Double click Import Export Utility, and then click Import tab.
   Import Category, Alert, Tokens and Flex Report as given below.

To import Category

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

![Figure 1](image)

2. Locate All Cisco ISE group of Categories.iscat file, and then click the Open button.
3. To import categories, click the Import button.
   EventTracker displays success message.
4. Click **OK** and then click the **Close** button.

### To import Alerts

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

2. Locate **All Cisco ISE group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button. EventTracker displays success message.

![Figure 4](image)

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

**To import Tokens**

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

![Figure 5](image)
2. Locate All Cisco ISE group of Tokens.istoken file, and then click the Open button.
3. Click the Import button to import the tokens.
   EventTracker displays success message.

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

To import Flex Reports
1. Click Scheduled Report option, and then click the browse button.
2. Locate All Cisco ISE group of Flex Report.issch file, and then click the Open button.

3. To import the scheduled reports, click the Import button.

   EventTracker displays success message.

4. Click OK, and then click the Close button.
Verify Cisco ISE knowledge pack in EventTracker

Verify Cisco ISE Categories
1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Categories.
3. In the Category Tree, expand Cisco Identity Services Engine group folder to see the imported categories.

Verify Cisco ISE Alerts
1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Alerts.
3. In the Search field, type 'Cisco ISE', and then click the Go button.
   Alert Management page will display all the imported Cisco Identity Services Engine alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Figure 10](image)

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

![Figure 11](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.

---

**Verify Cisco ISE Tokens**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rule**.

Imported Cisco ISE tokens added in Token-Value Groups list at left side of **Parsing rule** tab of EventTracker Enterprise (as shown in below figure).
Verify Cisco ISE Flex Reports

1. Logon to EventTracker Enterprise.
2. Select Reports, and then select Configuration.
3. In Reports Configuration pane, select Defined option.
   EventTracker displays Defined page.
4. In search box enter ‘Cisco ISE’, and then click the Search button.
   EventTracker displays Flex Reports of Cisco ISE.
Here you can find imported defined reports such as ‘Cisco ISE – Configuration changed, User password changed, Admin authentication failed’ report.

**Sample Report**

**Cisco ISE - Configuration changed**

**User Selection:**
- **From Date:** 5/12/2014 2:59:33 PM
- **To Date:** 5/12/2014 3:09:33 PM
- **Limit Time Range:** None
- **Refine:** Regular Expression – Configuration Changes: & & Changed configuration;
- **Filter:** None
- **Categories Selected:** N/A
- **Computers Selected:** CONTOSO:CSOISE:SYSLG
- **Description:** None

**Detail:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Admin Name</th>
<th>Machine IP Address</th>
<th>Configuration Version ID</th>
<th>Config Change Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/12/2014</td>
<td>John</td>
<td>172.16.6.201</td>
<td>13</td>
<td>Identity Policy Configuration='New/Updated'</td>
</tr>
<tr>
<td>05/12/2014</td>
<td>Mike</td>
<td>172.16.6.235</td>
<td>13</td>
<td>Identity Policy Configuration='New/Updated'</td>
</tr>
<tr>
<td>05/12/2014</td>
<td>David</td>
<td>172.16.6.211</td>
<td>11</td>
<td>Authorization Standard Policy Configuration='New/Updated'</td>
</tr>
<tr>
<td>05/12/2014</td>
<td>Johnson</td>
<td>172.16.6.223</td>
<td>10</td>
<td>Authorization Standard Policy Configuration='New/Updated'</td>
</tr>
<tr>
<td>05/12/2014</td>
<td>Alex</td>
<td>172.16.6.245</td>
<td>8</td>
<td>Description='test user'</td>
</tr>
<tr>
<td>05/12/2014</td>
<td>ACSAdmin</td>
<td>172.16.6.200</td>
<td>21</td>
<td>Description='test user'</td>
</tr>
<tr>
<td>05/12/2014</td>
<td>Alex</td>
<td>172.16.6.245</td>
<td>8</td>
<td>Description='test user'</td>
</tr>
</tbody>
</table>