Integrate OKTA SSO
EventTracker v9.x and above

Publication Date: April 2, 2019
Abstract

This guide provides instructions to configure OKTA SSO to send the event logs to EventTracker Enterprise. Once events are configured to send to EventTracker Manager, alerts, dashboard and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 9.x and later, and OKTA SSO.

Audience

OKTA SSO users, who wish to forward event logs to EventTracker Manager and monitor events using EventTracker Enterprise.
# Table of Contents

Abstract ........................................................................................................................................... 1  
Scope ............................................................................................................................................... 1  
Audience ......................................................................................................................................... 1  
Overview ......................................................................................................................................... 3  
Prerequisites ................................................................................................................................... 3  
Configure OKTA SSO to forward logs to EventTracker ................................................................. 3  
  Get API Key .................................................................................................................................. 3  
  Integration Steps ............................................................................................................................ 5  
EventTracker Knowledge Pack (KP) .................................................................................................. 7  
  Alerts ............................................................................................................................................ 7  
  Reports ......................................................................................................................................... 7  
  Dashboards ................................................................................................................................... 9  
Import Knowledge Pack into EventTracker ..................................................................................... 12  
  Tokens Template ........................................................................................................................... 12  
  Flex Reports ................................................................................................................................. 13  
  Alerts ............................................................................................................................................ 16  
  Knowledge Objects ....................................................................................................................... 17  
  Dashlets ....................................................................................................................................... 18  
Verify Knowledge Pack in EventTracker ........................................................................................... 21  
  Token Template ............................................................................................................................ 21  
  Flex Reports ................................................................................................................................ 21  
  Alerts ............................................................................................................................................ 22  
  Knowledge Object ....................................................................................................................... 23  
  Dashlets ....................................................................................................................................... 24
Overview

OKTA SSO an enterprise-grade, identity management service, is built for the cloud, but compatible with many on-premises applications. With OKTA, IT can manage any employee's access to any application or device. OKTA runs in the cloud, on a secure, reliable, extensively audited platform, which integrates deeply with on-premises applications, directories, and identity management systems.

Prerequisites

- PowerShell 5 or later should be installed on EventTracker Agent workstation.
- Admin credentials on EventTracker Agent workstation.
- Admin credential on OKTA admin console.

Configure OKTA SSO to forward logs to EventTracker

Get API Key

1. Sign-in to the OKTA SSO Admin console.
2. Hover over **Security** and select **API**.

![Figure 2](image)

3. Click **Create Token**.

![Figure 3](image)

4. Give the token a name and click **Create Token** to proceed.

![Figure 4](image)
5. A Token Value will be generated, this is the API key. Copy this, it will be used in the integrator later.

![Create Token](image)

Figure 5

6. Click **OK** to exit.

### Integration Steps

1. Contact [EventTracker Support](#) to download OKTA Integrator.
2. After download, run OKTAIntegrator.exe on EventTracker Agent machine.

![OKTA Integrator](image)

Figure 6
3. Browse the location where you want to extract the OKTA integrator files and click **Install** button.
4. Now, provide the OKTA admin URL and API key which we created in **previous step** and click **Validate Credential**.

![Figure 7](image)

5. If API key and URL is proper it will enable **Finish** button

![Figure 8](image)

6. Click **Finish** button to complete the OKTA integration.

![Figure 9](image)
Once logs are received in EventTracker; alerts, reports and dashboards can be configured in EventTracker.

Following are the KP items available for OKTA SSO:

### Alerts
- **OKTA SSO-Login Failed:** This alert will be triggered whenever the login failure occurs for a user in OKTA SSO.

### Reports
- **OKTA SSO-Application changes:** This report provides information related to application changes.
  - OKTA SSO - Application changes: an alert triggered whenever the login failure occurs for a user in OKTA SSO.
  - OKTA SSO - Application changes: an alert triggered whenever the application associated with a user is changed.
  - OKTA SSO - Application membership changes: an alert triggered whenever the application membership of a user is changed.
  - OKTA SSO - Policy changes: an alert triggered whenever the policy associated with a user is changed.

### Figure 10
![Figure 10](image10.png)

### Figure 11
![Figure 11](image11.png)

### Figure 12
![Figure 12](image12.png)
**OKTA SSO-System events:** This report provides information related to system events.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device IP Address</th>
<th>Action</th>
<th>User Type</th>
<th>User Name</th>
<th>Device Type</th>
<th>Device OS</th>
<th>Browser/Device</th>
<th>Device Country</th>
<th>Target Object Type</th>
<th>Target Object Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:04:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>system로그인_하위</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:04:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>system로그인_하위</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:04:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>Leo</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>system로그인_하위</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:04:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>Bill</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>system로그인_하위</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:04:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>system로그인_하위</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:04:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>system로그인_하위</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

**OKTA SSO-User authentication details:** This report provides information related to user authentication details.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device IP Address</th>
<th>Action</th>
<th>User Type</th>
<th>User Name</th>
<th>Device Type</th>
<th>Device OS</th>
<th>Browser/Device</th>
<th>Device Country</th>
<th>Target Object Type</th>
<th>Target Object Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>Authentication</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>Authentication</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>Leo</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>Authentication</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>Bill</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>Authentication</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>Authentication</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>Authentication</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

**OKTA SSO-User management:** This report provides information related to user management.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device IP Address</th>
<th>Action</th>
<th>User Type</th>
<th>User Name</th>
<th>Device Type</th>
<th>Device OS</th>
<th>Browser/Device</th>
<th>Device Country</th>
<th>Target Object Type</th>
<th>Target Object Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.125</td>
<td>create</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>User이용가능성확인</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.65</td>
<td>create</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>User이용가능성확인</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.125</td>
<td>create</td>
<td>User</td>
<td>Leo</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>User이용가능성확인</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.65</td>
<td>create</td>
<td>User</td>
<td>Bill</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>User이용가능성확인</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.125</td>
<td>create</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>User이용가능성확인</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6:24:00 PM</td>
<td>192.168.1.65</td>
<td>create</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>User이용가능성확인</td>
<td>YouTube</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

**OKTA SSO-User session details:** This report provides information related to user session details.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device IP Address</th>
<th>Action</th>
<th>User Type</th>
<th>User Name</th>
<th>Device Type</th>
<th>Device OS</th>
<th>Browser/Device</th>
<th>Device Country</th>
<th>Target Object Type</th>
<th>Target Object Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>Leo</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>Bill</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.125</td>
<td>login</td>
<td>User</td>
<td>John</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>9:24:00 PM</td>
<td>192.168.1.65</td>
<td>login</td>
<td>User</td>
<td>James</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>userSessionStart</td>
<td>userSessionStart</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

**Figure 13**

**Figure 14**

**Figure 15**

**Figure 16**
- **OKTA SSO-Admin access**: This report provides information related to admin access.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device IP Address</th>
<th>Action</th>
<th>User Type</th>
<th>User Name</th>
<th>Device Type</th>
<th>Device OS</th>
<th>Browser/Device</th>
<th>Device City</th>
<th>Device Country</th>
<th>Target-Object Type</th>
<th>Target-Object Name</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/24/2018 5:43:06 PM</td>
<td>192.168.1.65</td>
<td>Okta admin app accessed</td>
<td>User</td>
<td>Admin</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>India</td>
<td>user-lifecycle-create</td>
<td>user-session-start</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6/24/2018 7:16:42 PM</td>
<td>192.168.1.65</td>
<td>Okta admin app accessed</td>
<td>User</td>
<td>Admin</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>India</td>
<td>user-lifecycle-suspend</td>
<td>user-session-end</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6/24/2018 7:16:42 PM</td>
<td>192.168.1.32</td>
<td>Okta admin app accessed</td>
<td>User</td>
<td>Admin</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>India</td>
<td>user-lifecycle-suspend</td>
<td>user-session-end</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6/24/2018 7:16:42 PM</td>
<td>192.168.1.126</td>
<td>Okta admin app accessed</td>
<td>User</td>
<td>Admin</td>
<td>Computer</td>
<td>Windows 7</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>India</td>
<td>user-lifecycle-clear</td>
<td>user-session-clear</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>6/24/2018 7:16:42 PM</td>
<td>192.168.1.65</td>
<td>Okta admin app accessed</td>
<td>User</td>
<td>Admin</td>
<td>Computer</td>
<td>Windows 10</td>
<td>CHROME</td>
<td>Bengaluru</td>
<td>India</td>
<td>plugin-download</td>
<td>user-session-start</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

**Figure 17**

**Dashboards**

- **OKTA - Login Activities by System Type**

**Figure 18**

- **OKTA - Login Activities by Status**

**Figure 19**
• OKTA - Login Activities by Country

Figure 20

• OKTA - Login Failed by Country

Figure 21
- OKTA - Login Activities by Device Type

![Graph showing login activities by device type.](image)

Figure 22

- OKTA - Login Activities by Browser

![Graph showing login activities by browser.](image)

Figure 23
• OKTA – Activities

![Image of OKTA - Activities](image)

Figure 24

Import Knowledge Pack into EventTracker

Once logs are received in EventTracker; alert, reports and dashboards can be configured in EventTracker. Following are the sequence to upload KP items:

- Token Template
- Flex Report
- Alerts
- Knowledge Object
- Dashboards

Tokens Template

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.
3. Select Template tab, locate the Token_Template_OKTA SSO.ettd file.

![Image of Import](image)

Figure 25
4. Select all the reports by clicking on the check box.

5. Click the **Import** icon.

---

### Import

<table>
<thead>
<tr>
<th>Template name</th>
<th>Separator</th>
<th>Template description</th>
<th>Added date</th>
<th>Added by</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>OKTA SSO All events</td>
<td>$</td>
<td></td>
<td>Jun 21 02:54:18 AM</td>
<td>john</td>
<td>OKTA SSO</td>
</tr>
</tbody>
</table>

---

[Figure 26]

Templates are now imported successfully.

---

[Figure 27]

---

### Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Export/Import Utility**, and then click the **Import** tab.
3. Click **Reports** option, and select new (.etcrx) from the option.
4. Locate the file named **Reports_OKTA SSO.etcrx**, and select all the check box.

![Figure 30](image)

5. Click the **Import** button to import the reports. EventTracker displays success message.

![Figure 31](image)
Alerts

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

![Figure 32](image-url)

2. Locate **Alerts_OKTA SSO.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.
   EventTracker displays success message.

![Figure 33](image-url)

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

1. Click Knowledge objects under Admin option in the EventTracker manager page.
2. Click on ‘Import’ option.
3. Locate the file named KO_OKTA SSO.etko.

4. Now select all the check box and then click Upload.
5. Knowledge objects are now imported successfully.

![Figure 36](image)

**Dashlets**

In EventTracker 9.0, we have added new feature which will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker Enterprise Web console.

![Figure 37](image)
2. Go to **My Dashboard** option.

3. Click import button and select `.etwd` File.
4. Click upload and select Dashboard which you want to import.

5. Click **Import** button. It will upload all selected dashboards.
Verify Knowledge Pack in EventTracker

Token Template

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.
3. In **Template** tab to view imported template, scroll down and click **OKTA SSO** group folder. Templates are displayed in the template pane.

   ![Figure 42](image)

Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **OKTA SSO** group folder.

   Reports are displayed in the Reports configuration pane.
Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search box, type ‘OKTA’, and then click the Go button. Alert Management page will display all the imported alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

   ![](Successfully_saved_configuration.png)

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

**NOTE:** Specify appropriate **systems** in **alert configuration** for better performance.

**Knowledge Object**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **OKTA SSO** group folder.

   Knowledge Objects are displayed in the pane.
Dashlets

1. Logon to EventTracker Enterprise.
2. Click the Dashboard menu, and then My Dashboard.
3. Then click on Customize Dashlet button 🎁 and search for “OKTA”