

Configuring Okta Provisioning

***This integration with Okta is currently under development and is not available to customers yet. Contact OpenEye support to learn more.**

This document describes how to configure the Okta application to enable automatic user provisioning via SCIM 2.0. The prerequisite to these instructions is a SAML integration already complete or is in progress as described [here](#).

Supported Provisioning Features

- Create Users
- Update User Attributes
- Deactivate Users
- Push Groups by Name

Requirements

Identity Management is enabled for the account and SAML integration is already complete or is in progress.

Step-by-Step Configuration Instructions

Configure identity management provisioning via SCIM (WS)

1. As a web services Administrator, go to Settings->Identity Management.
2. Generate an API Token (SCIM v2 API) via clicking on GENERATE SCIM API TOKEN.

Enable and configure provisioning via Okta Application (Okta)

1. As an Okta user with at least Application Administrator permissions, go to the application referenced by the WS Identity Management page.
2. Go to the Provisioning tab and enable provisioning.
3. Go to the API Integration section of the Provisioning tab and click Edit.
4. Check "Enable API Integration".
5. Copy over the Base URL (SCIM v2 API) from the WS Identity Management page into the Base URL field.
6. Copy over the API Token (SCIM v2 API) from the WS Identity Management page into the API Token field.
7. Save these settings.

Add user and groups via Okta

Users may be added by Assignment and groups by Push Groups. Group permissions will need to be configured on the WS side by an authorized WS user, but groups will maintain their permissions provided they are never removed from Push Groups after their configuration.

Integration Notes and Troubleshooting

- Descriptions for Okta Groups are not synchronized into OWS from Okta. User Group descriptions on the OWS side must be input via OWS and will remain unaffected by the Group description that is in Okta.
- Okta pushed groups ignore users added from the OWS. An OWS admin may manually add users to a User Group on the OWS side in some circumstances. However, this is not a recommended user management practice as Okta will ignore these users when pushing new users from Okta leading to a user management state that is not completely Okta defined. To avoid this, only add or remove users from Groups in Okta.