Using Okta as SCIM/SAML IdP

Overview

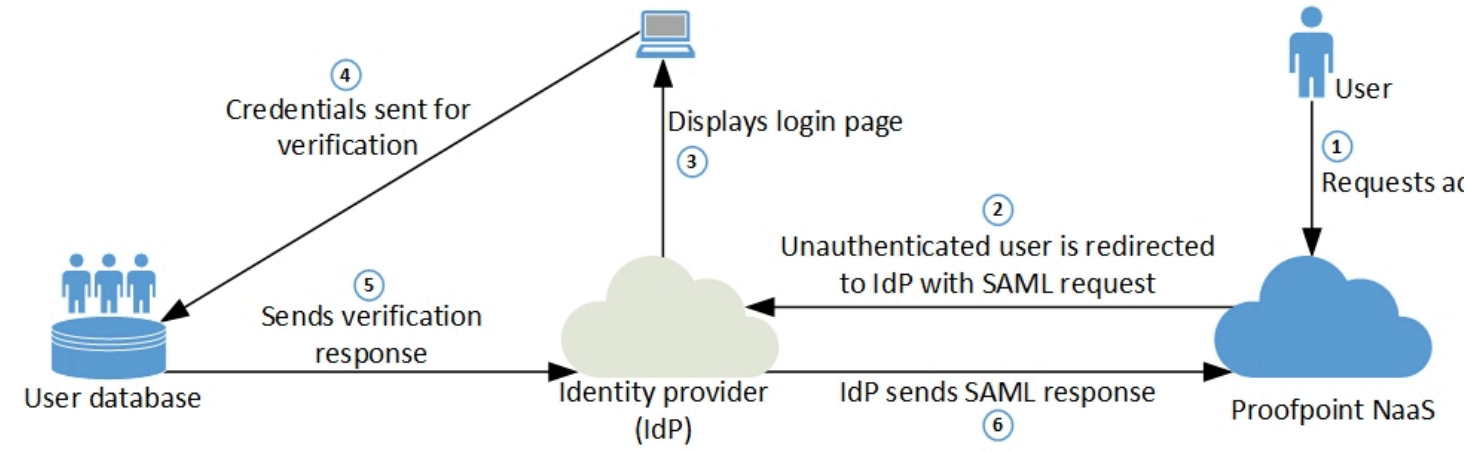
This document describes identity management methods employed by various Proofpoint applications, when integrated with Okta Identity Cl in Okta supports both System for Cross-domain Identity Management (SCIM) and Security Assertion Markup Language (SAML) standards.

SCIM

System for Cross-domain Identity Management is a specification for simplifying user identities management in cloud-based applications an platform. It is designed to build upon existing schemas and deployments, placing specific emphasis on simplicity of development and integr authentication, authorization, and privacy models. Its intent is to reduce the cost and complexity of user management operations by providir model.

SAML/SSO

Proofpoint supports single sign-on (SSO) via Security Assertion Markup Language. When working with Okta Identity Cloud, Okta can be set to Proofpoint Agent, MetaConnect or Proofpoint Admin Console. The diagram below illustrates the flow for application-triggered single sign-



Okta and Proofpoint Integration

Currently, the Okta/Proofpoint integration supports the following functions:

- Creating users – New users created through Okta are duplicated in Proofpoint.
- Updating user attributes – User profile updates in Okta are pushed to Proofpoint.
- Deactivating users – Deactivating the user or disabling user access to resources in Okta also deactivates the user in the Proofpoint ap from Proofpoint user database.
- Pushing groups – Groups and their members can be pushed to Proofpoint. For details, seeManage Group Push.
- Reactivating users – Information about reactivated user accounts in Okta is propagated to Proofpoint as well.

In addition, the following user and user group attributes are synchronized between Okta and Proofpoint:

- User:
  - First name
  - Last name
  - Phone number (work)
- User group:
  - Group name
  - Group member.

> Note
>
> A change in a previously-provisioned user group is not propagated to the Proofpoint user/user group database via Connector applicati synchronization of the modified user group will be suspended.

Before You Begin

Verify that you have the following:

- An administrator account with Okta.
- A Proofpoint account with an administrator role that allows you to configure IdPs.

SCIM Configuration

This section details how configure SCIM parameters in the Proofpoint Admin Console (Admin Console) and Okta dashboard. This procedure

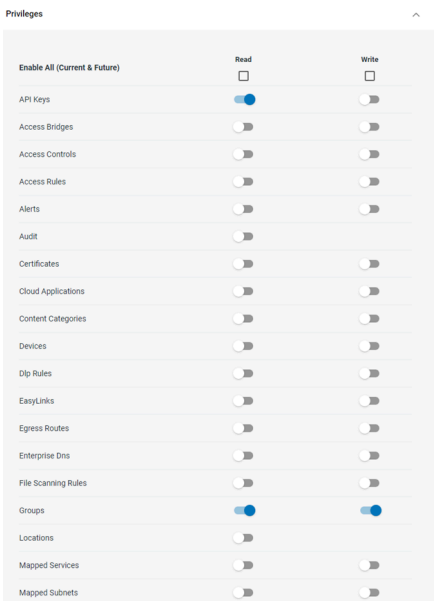
- Adding an API key and creating an IdP instance via Admin Console.
- Adding and configuring Proofpoint application as SCIM endpoint via Okta dashboard.

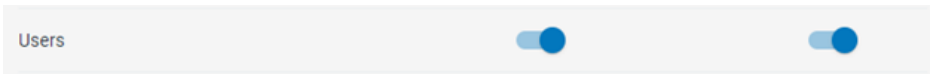
Adding an API Key

You must define an API key to be used for creating an IdP instance via Admin Console, and API secret for authenticating the SCIM API calls i

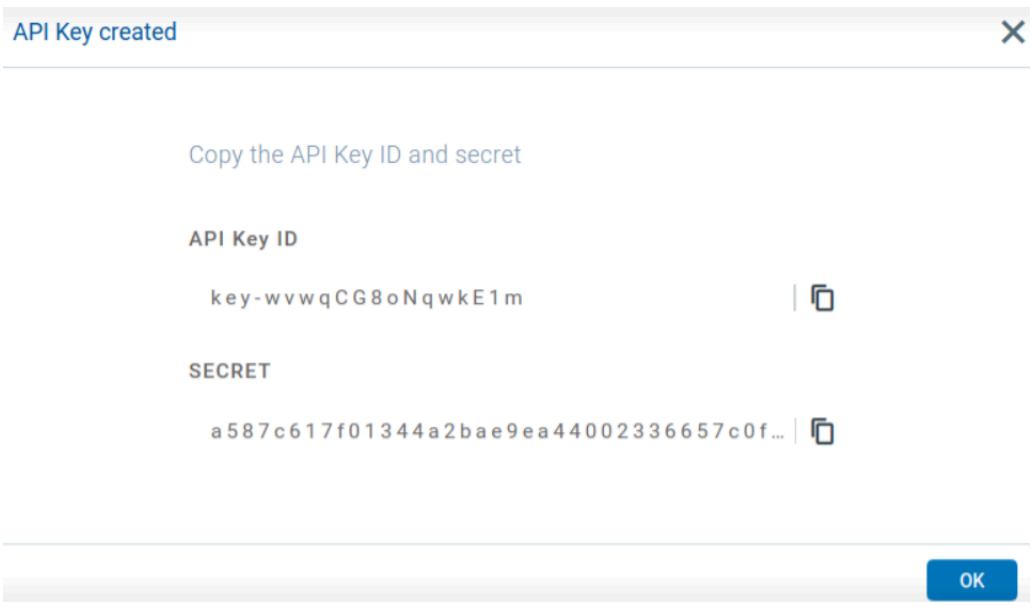
1. Log into Admin Console as administrator.
2. Navigate to**Administration > API Keys**.
3. At the top right-hand corner, click the**+ Create**button to add a new key.
4. In the**General**secton, enter the key name and description.

5. In the**Expiration**section, configure the key to never expire or set its exact expiration date.
6. Enable the relevant privileges for API Key (read), Groups (read/write) and Users (read/write).





7. Click**Save**to finish.



8. Write down the API ID and the secret for the later use.

> **Note**
>
> The API secret disappears after the pop-up window is closed.

Creating an IdP Instance

Add a new IdP instance, which SSO URLs are to be used by the IdP connector application in Okta Identity Cloud.

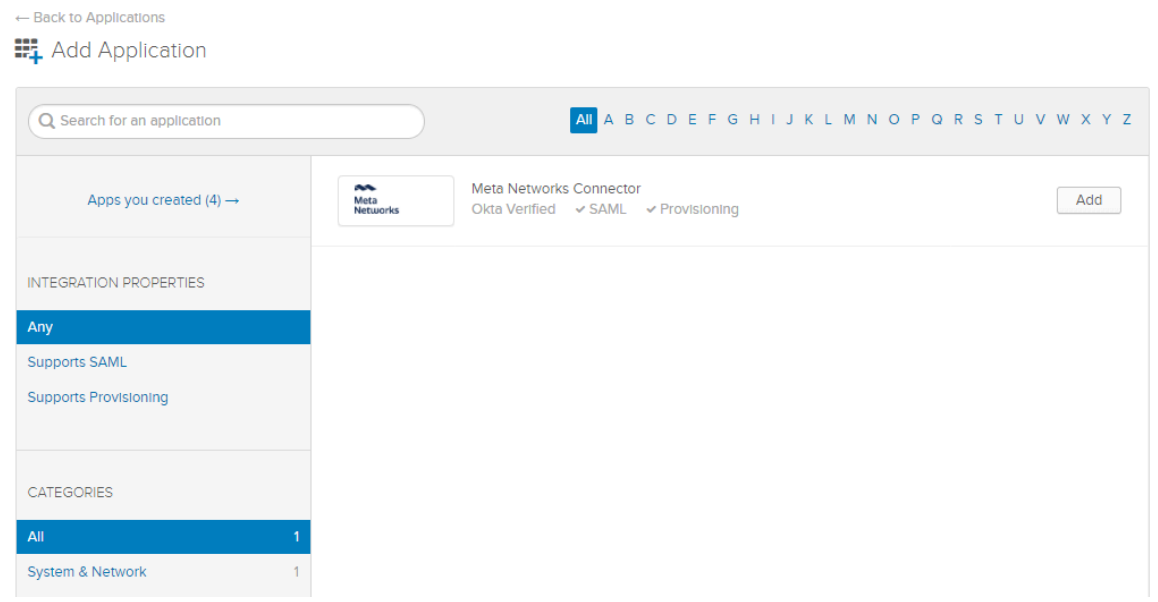
1. Log into Admin Console as administrator.
2. Navigate to**Administration > Identity Providers**.
3. At the top right-hand corner, click the**+ Create**button to add a new IdP.
4. In the**General**section of the**Add Identity Provider**dialog box, add a meaningful name and description to the IdP.
5. Enable the IdP and toggle the**IDP: Visible**switch to make this IdP appear on the main login dialog box.

6. In the Configure SCIM section, enter the previously configured API key (see Adding API Key).
7. Optionally, you can use the Assume Ownership feature to control the way locally-defined users are treated if they also exist in the SCIM users that arrive from the SCIM provider and already exist locally are treated as if provided and controlled by the SCIM provider, and n
8. Click **Save** to finish.

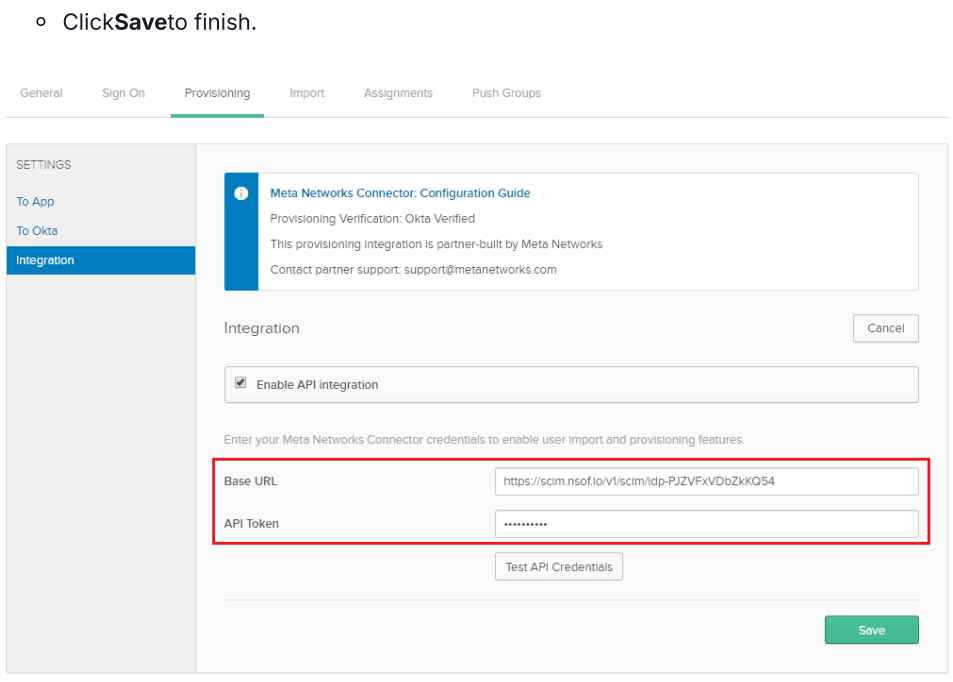
Adding and Configuring Proofpoint Application as SCIM Endpoint in Okta Dashboard

Integrate the relevant Proofpoint applications with Okta.

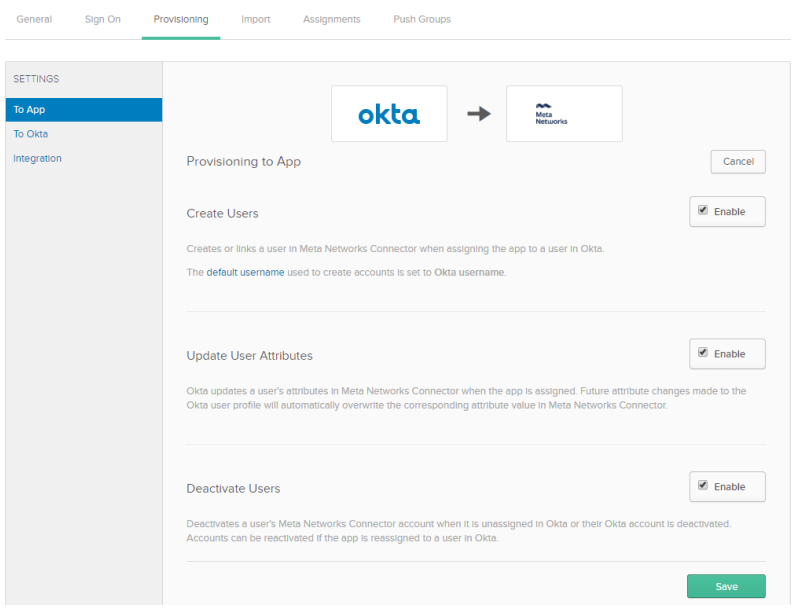
1. Log into Okta Identity Cloud as administrator.
2. Navigate to **Applications** and add the Proofpoint Connector application.



3. Go to **Provisioning and select Integration on the Settings panel**.
4. In the **Integration** dialog box, do the following:
   - Enable API integration.
   - Configure the Base URL parameter – Base/Tenant URL value in the Configure SCIM section of the Admin Proofpoint Edit IDP dial **> Edit IDP**), see see Creating an IDP Instance.
   - Set API Token – API secret, configured in the Admin Proofpoint API Keys menu (see Adding API Key).
   - Click **Test API Credentials** to verify integration of the Proofpoint Connector application.
   - Click **Save** to finish.



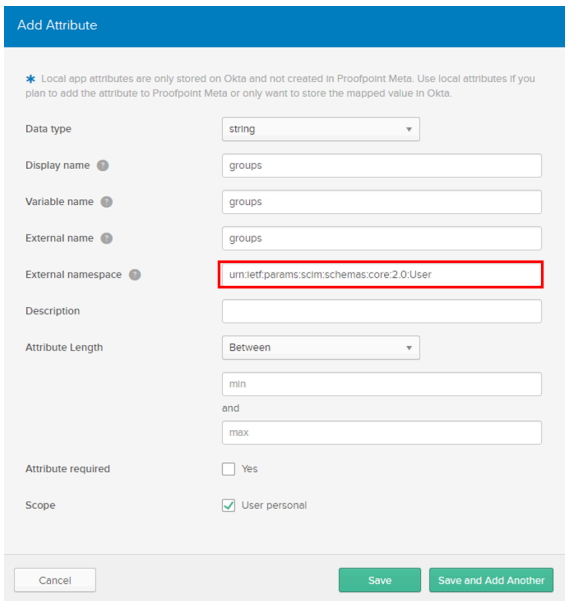
5. Go to **Provisioning and select To App on the Settings panel**.
6. In the **To App** dialog box, enable the required Okta-to-App provisioning features:
   - Creating users.
   - Updating user attributes.
   - Deactivating users.



Mapping Additional Attributes

In order to successfully associate users to their respective groups, an additional custom attribute of the*Data Type*string is required.

1. In the Proofpoint Connector settings, go to**Profile Attributes & Mappings**, and click**Edit Attributes**.
2. Click**Add Attribute**.
3. Fill out the following fields, as illustrated below.

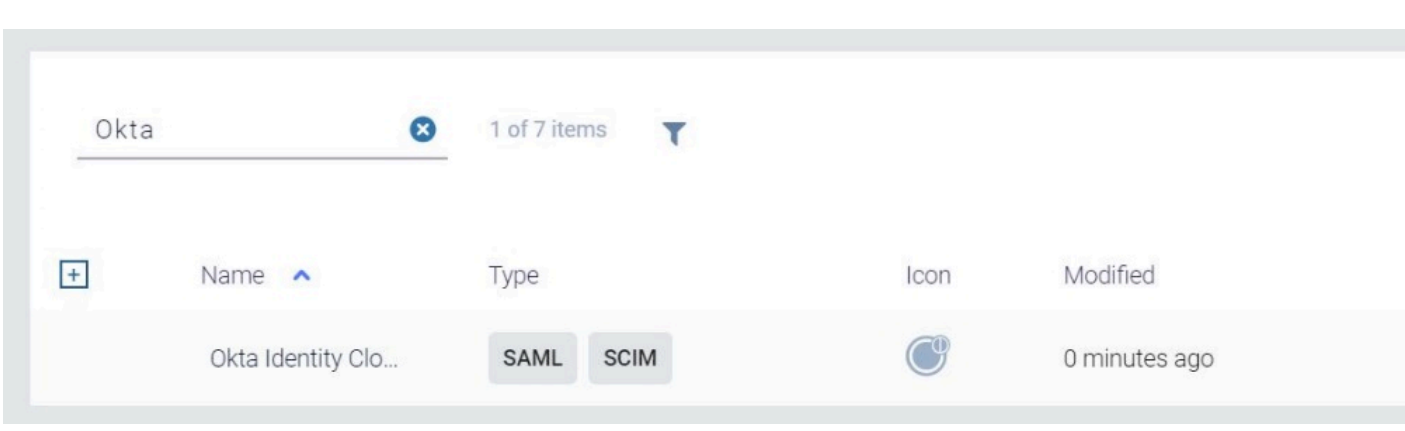


> **Note**
>
> The**External namespace**parameter is mandatory for successful provisioning and correct group membership association. urn:ietf:parar

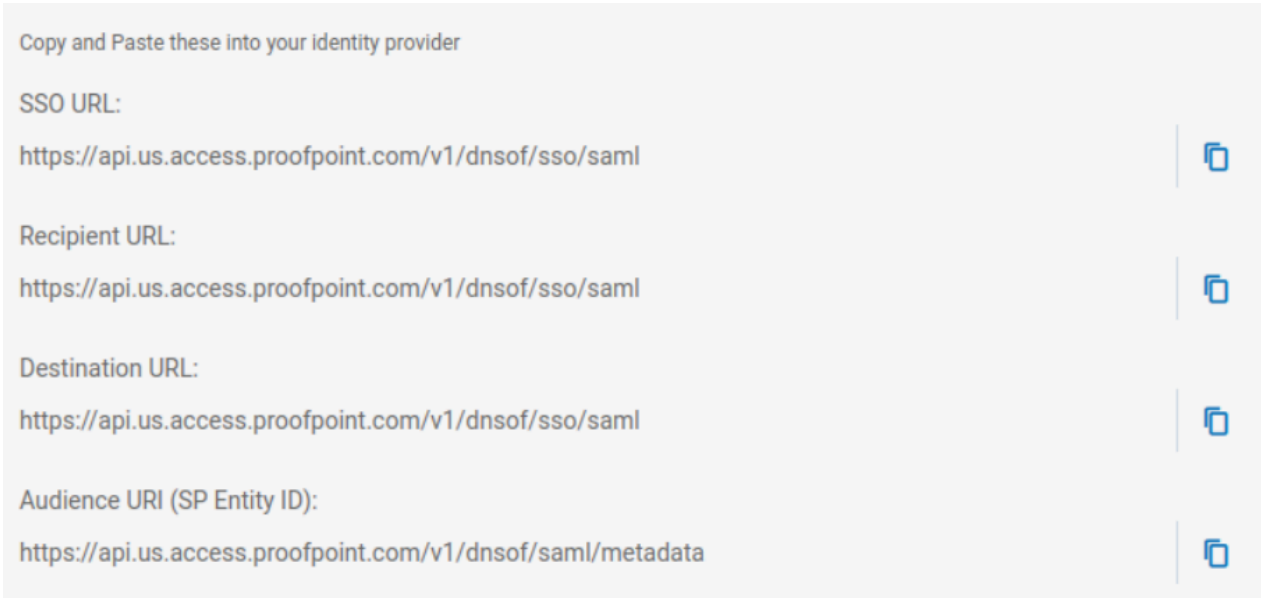
SAML/SSO Configuration

Obtaining SAML/SSO URLs

1. Log into Admin Console as administrator.
2. Navigate to**Administration > Identity Providers**and verify that the previously-created IdP is enabled.

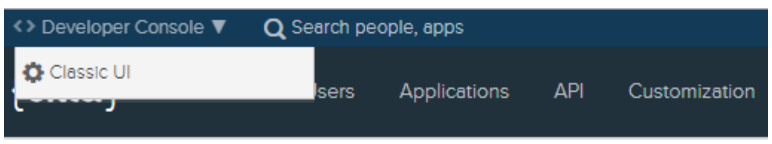


3. Click on the IdP title to display its configuration parameters.
4. Scroll down to display the SSO URLs.

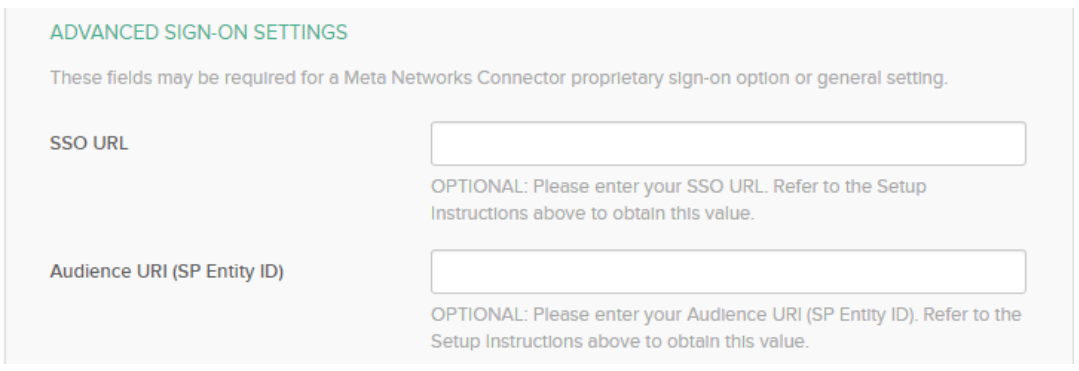


Configuring SAML/SSO in Okta Dashboard

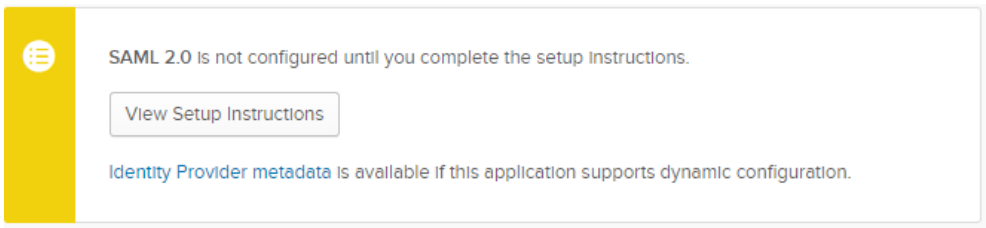
1. Log into Okta Identity Cloud as administrator.
2. Enable the classic Okta dashboard UI, as the relevant SAML settings are available only in this dashboard mode. Click on**Developer Co**



3. In the classic UI of the Okta dashboard, go to**Applications**and select a Proofpoint Connector from the list of active applications.
4. Go to**Sign On**settings and click**Edit**.
5. In the edit mode, scroll down to the**Advanced Sign-on Settings**section.
6. Copy and paste the SSO URL and Audience URI from the Admin Console SSO URLs section.



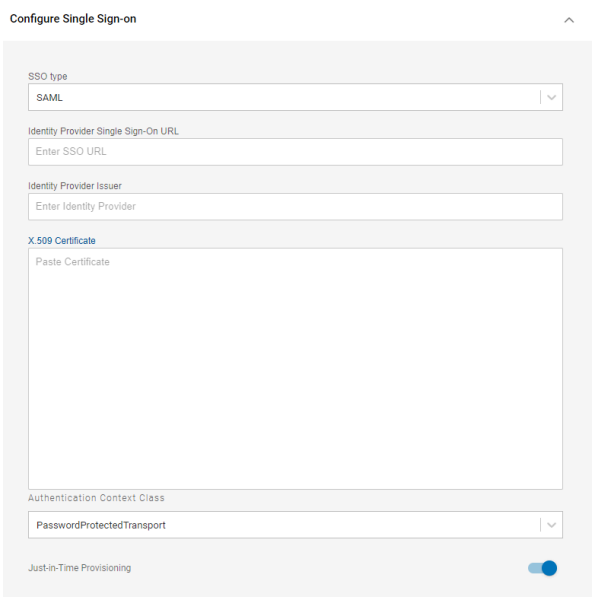
7. Save your changes.
8. Click**View Setup Instructions**to display the relevant SAML 2.0 configuration instructions for the Proofpoint connector.



9. Scroll down to the**Configure SAML Authentication**section and copy the following values to be used during the single sign-on configur
    - **Identity Provider Single Sign-On URL**.
    - **Identity Provider Issuer**.
    - **X.509 certificate**.

Configuring SAML/SSO in Admin Console

1. In the Admin Console, go to**Administration > Identity Providers**and select the IdP to configure.
2. Scroll down to**Configure Single Sign-on**.
3. Paste the following URLs that were copied from the**Configure SAML Authentication**via the Okta dashboard:
    - **Identity Provider Single Sign-On URL**.
    - **Identity Provider Issuer**.
    - **X.509 certificate**.



4. Save your changes, log out of Admin Console and test your SSO access.

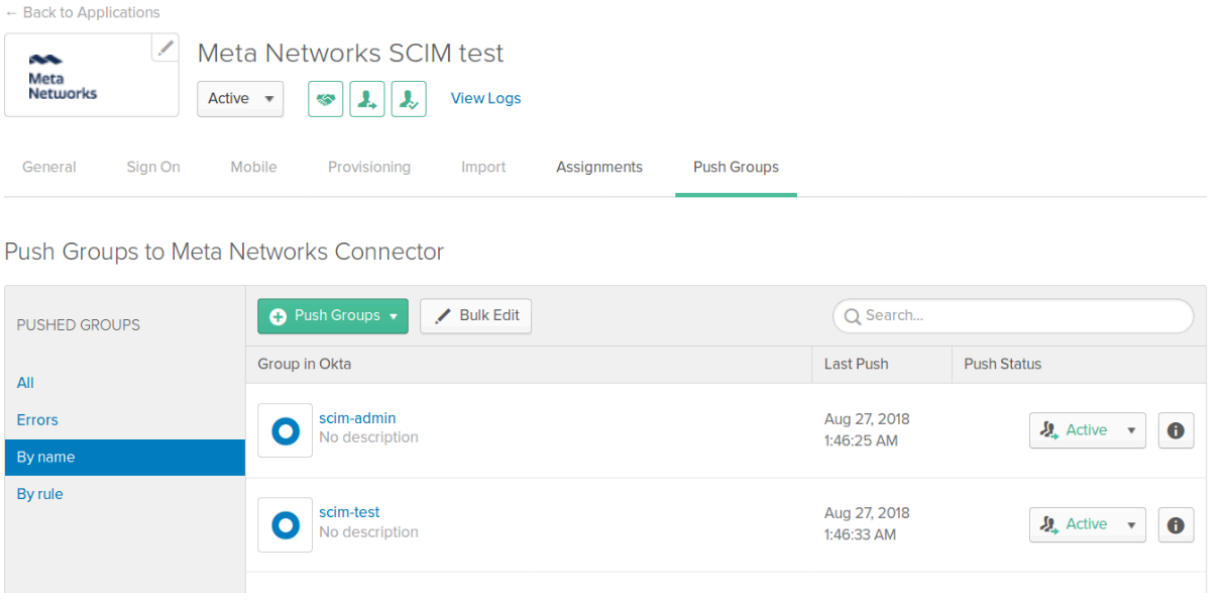
Assigning Users or User Groups in Okta Dashboard

As a security measure, Okta does not issue a token allowing Proofpoint application users to sign into the application unless they have been g granted access directly, or through a group that they are members of.

1. Log into Okta Identity Cloud as administrator.
2. If needed, navigate to**Users > People**, add new users and assign each user to the relevant Proofpoint application.

> Note
>
> User phone numbers must be entered in the E.164 format. Non-compliant phone number are silently discarded.

3. If needed, navigate to**Users > Groups**, assign users to the user group, and then assign the group to the relevant Proofpoint application
4. Navigate to**Applications**and select the required Proofpoint Connector from the list of active applications.
5. Go to**Push Groups**and verify that the user groups assigned to the selected Proofpoint Connector appear in the pushed group list.



The process is complete. On the next login to the Admin Console, Proofpoint Agent or MetaConnect, the SSO sign-in with authentication ag available.