User Provisioning using SCIM in Okta

Costumer

This guide will describe how to setup user provisioning using SCIM through Okta.

Prerequistes

To configure user provisioning the following information is required from CERRIX:

URL to CERRIX	https://customer short name].cerrix.com/
Secret token	A JWT to access the SCIM endpoint. This is a long-lived token which expires after a certain date and needs to be replaced. The date can be negotiated. (In future release of CERRIX the customer should be able to manage these tokens themselves)

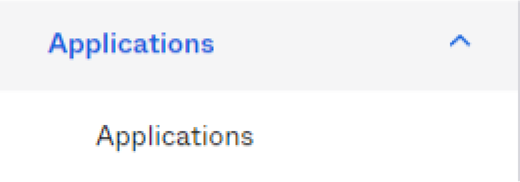
CERRIX requires the following information:

Default organization	Used to specify the default/fallback organization that new users are linked too. Or if an organization identifier is given through user provisioning when no match is found.

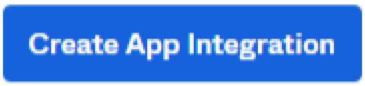
Setting up the SAML integration

We need to create an Okta app integration in which we can configure user provisioning and configure which groups and users are synchronized.

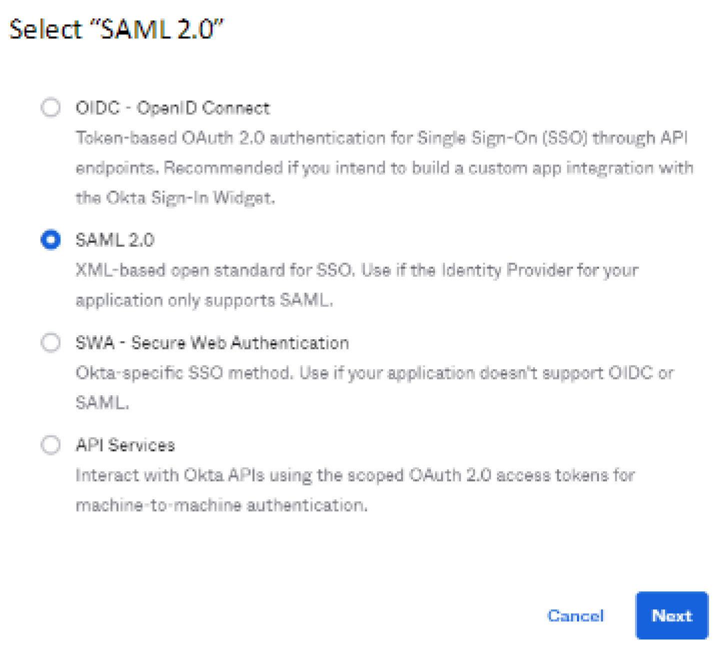
In the side-side menu navigate to “Application”



Select “Create App Integration”



Select “SAML 2.0”



Select "SAML 2.0"

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

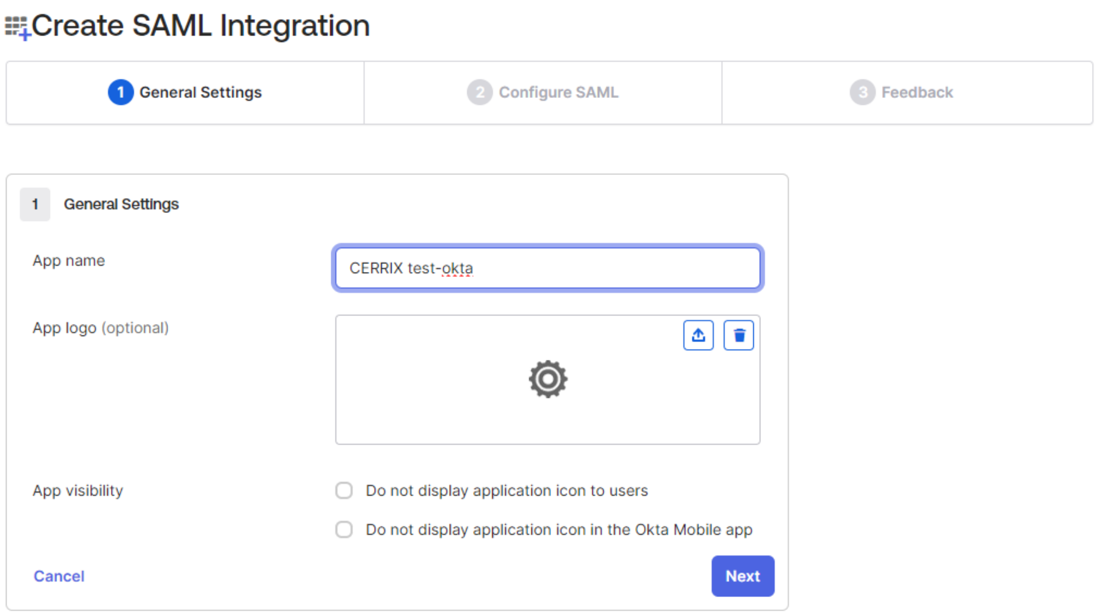
● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Click "Next"

Fill in an App name



Create SAML Integration

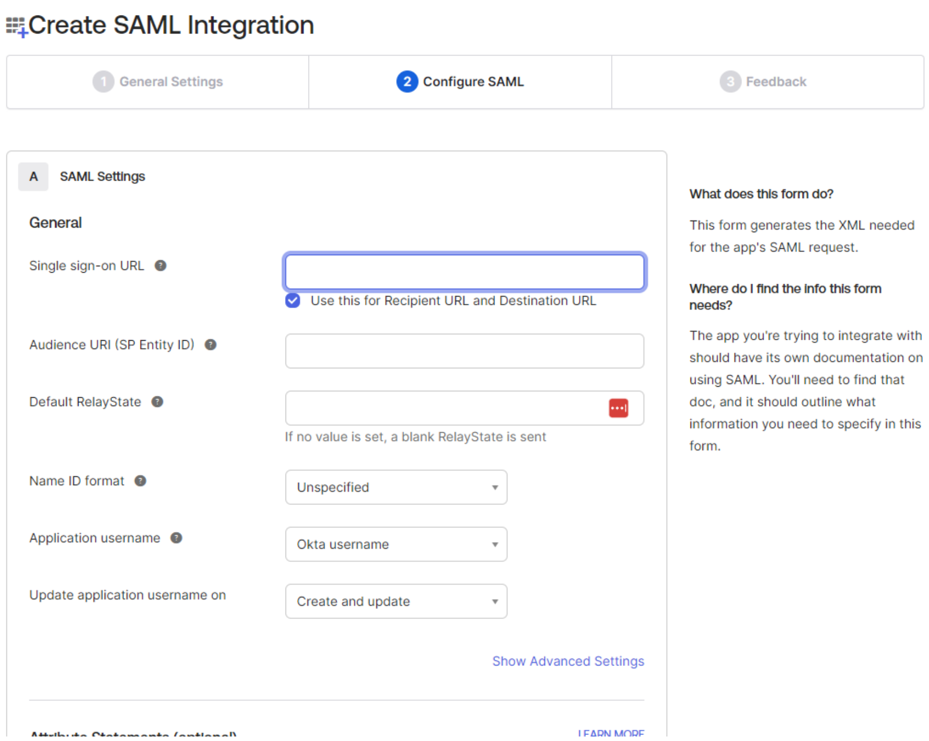
1 General Settings

App name: CERRIX test-okta

App logo (optional)

App visibility
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app

Click "Next"



Create SAML Integration

A SAML Settings

General

Single sign-on URL

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

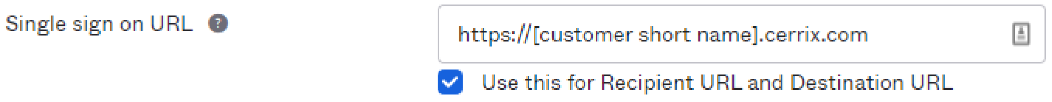
What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

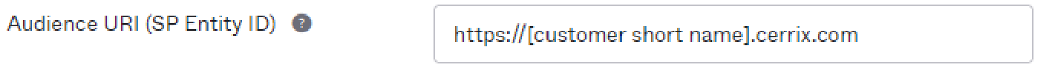
Set “Single sign on URL” to the following value: *https://[customer short name].cerrix.com*



Single sign on URL: https://[customer short name].cerrix.com

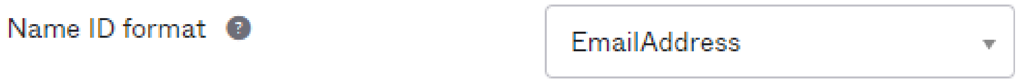
☑ Use this for Recipient URL and Destination URL

Set “Audience URI (SP Entity ID) to the following value: *https://[customer short name].cerrix.com*



Audience URI (SP Entity ID): https://[customer short name].cerrix.com

Set “Name ID format” to “EmailAddress”



Name ID format: EmailAddress

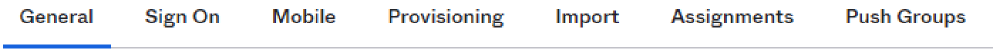
Click “Next”

Click “Finish”

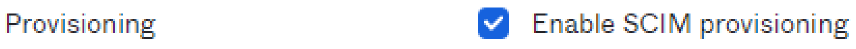
The SAML integration should now be created.

Click on the newly created app

Navigate to the General tab:



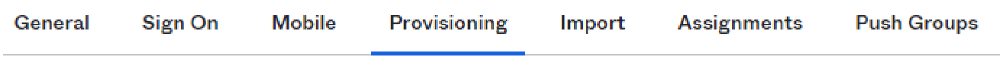
Check “Enable SCIM provisioning”



Provisioning: ☑ Enable SCIM provisioning

Click “Save”

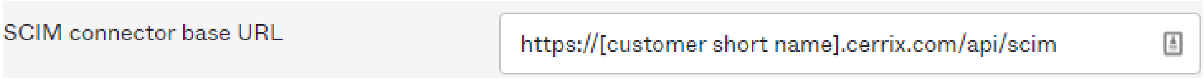
Navigate to the Provisioning tab:



From the side-menu select “Integration”

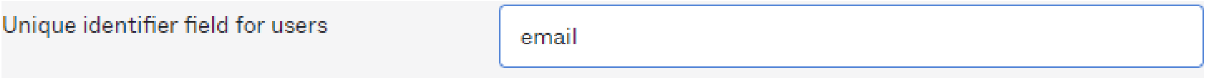
Set “SCIM connector base URL” to the following value:

https://[customer short name].cerrix.com/api/scim



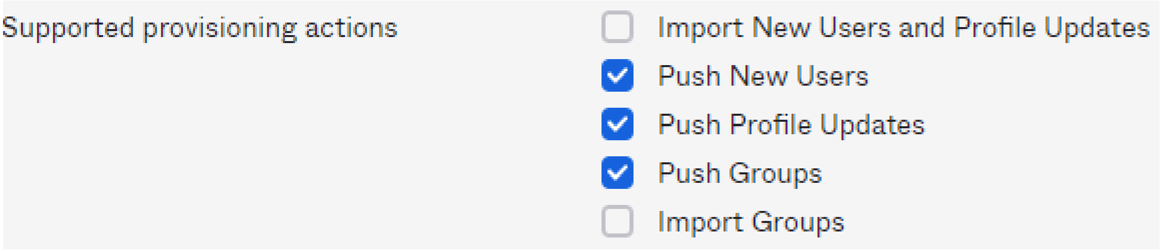
SCIM connector base URL: https://[customer short name].cerrix.com/api/scim

Set “Unique identifier field for users” to the following value: email



Unique identifier field for users: email

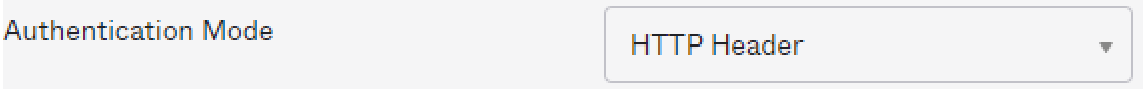
For “Supported provisioning actions select the following:



Supported provisioning actions

- □ Import New Users and Profile Updates
- ☑ Push New Users
- ☑ Push Profile Updates
- ☑ Push Groups
- □ Import Groups

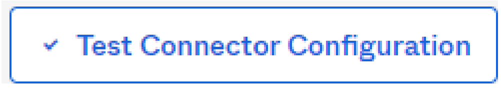
Set “Authentication Mode” to “HTTP Header”



Authentication Mode: HTTP Header

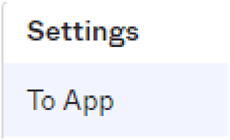
Set the “Bearer token” to the Secret token received from CERRIX

Click “Test Connector Configuration” to make sure everything is filled in correctly.



Click “Save”

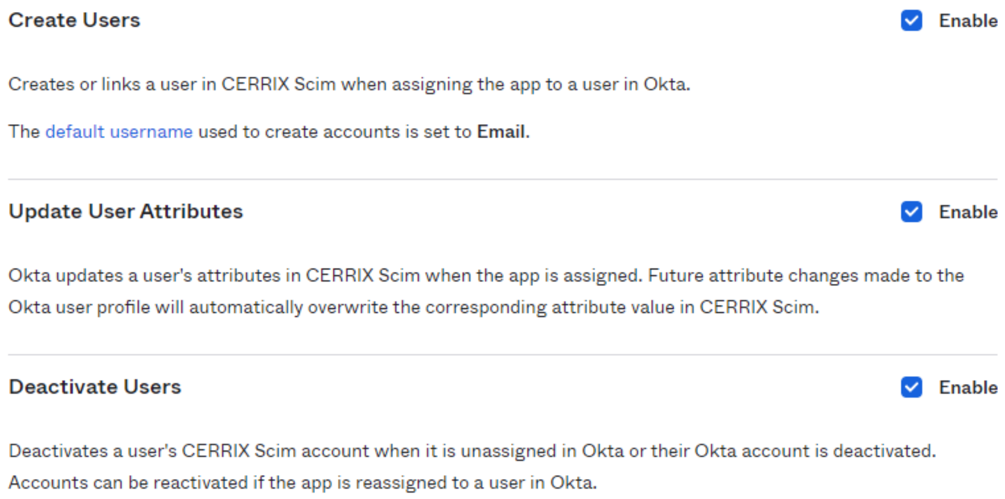
From the side-menu select “To App”



Check the following values:

- “Create Users”

- “Update User Attributes”
- “Deactivate Users”



Create Users ☑ Enable

Creates or links a user in CERRIX Scim when assigning the app to a user in Okta.

The default username used to create accounts is set to **Email**.

Update User Attributes ☑ Enable

Okta updates a user's attributes in CERRIX Scim when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in CERRIX Scim.

Deactivate Users ☑ Enable

Deactivates a user's CERRIX Scim account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Click “Save”

Configuring user provisioning is now finished and can be used with CERRIX.