Integrating CloudShare with Okta

CloudShare supports Single Sign On (SSO) with Okta.

This guide provides full instructions for how to integrate Okta into CloudShare as a single sign on (SSO) identity provider (IDP). This guide assumes you are an [Okta](#) admin user.

Contents

Overview

Okta provides a template through which you can create a WS-Federation enabled app that enables Okta to handle CloudShare authentication. Using this template, Okta acts as the identity provider (IDP) while CloudShare acts as the service provider (SP) in the following authentication flow:

1. The user browses to the CloudShare login page or clicks a "chicklet" in Okta.

2. CloudShare redirects the user to the configured login URL (Okta's generated app instance URL) sending a passive request.

3. Okta is sent a passive request (assuming you have an existing Okta session).

4. Okta sends a response to CloudShare.

5. CloudShare receives the response and verifies that the claims are correct. A CloudShare session is established.

6. The user is authenticated and receives the assigned CloudShare user role.

Follow the steps in this guide to create the app and assign your users correctly.

Step 1: Contact CloudShare Support

Call CloudShare support to request Okta integration. We will decide together with which of your projects, teams, owning project managers and email domains should be included in the scope of the Okta integration. We will then provide you with an **SSO Provider Name**, which you will use in step 2.

Step 2: Add CloudShare to Okta

In this step, you will add CloudShare to Okta as an application:

1. Login to Okta as a system administrator and click **Admin** to enter the Admin area.

2. From the **Applications** menu, select **Applications** and then click **Add Application**.

3. Search for "Template WS-Fed" and add that application template.
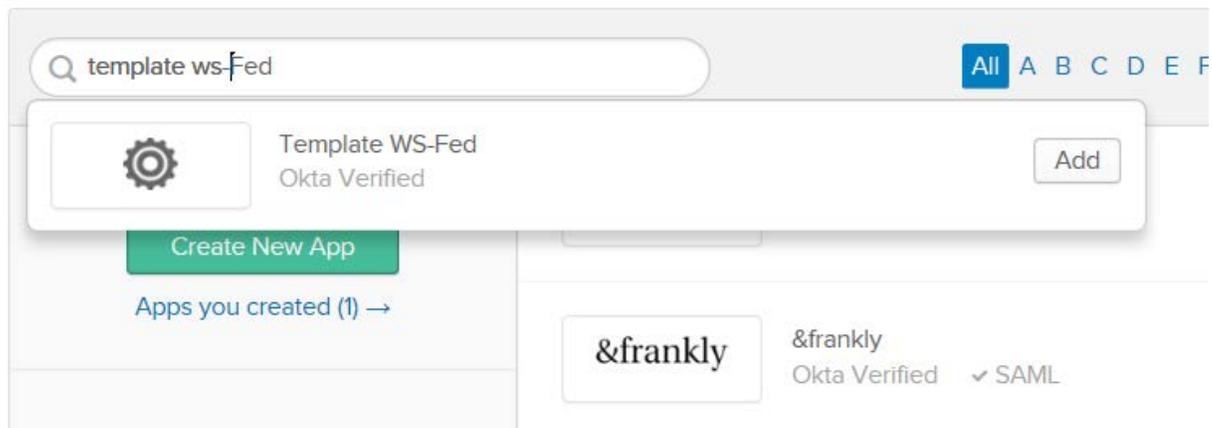
4. In the **Add Template WS-Fed** page, enter the following field values:

In this field…	enter…
Application label	**Cloudshare**
Web Application URL	**https://use.cloudshare.com/Ent/FederatedLogin.mvc?provider=<SSO Provider Name>** *in which <SSO Provider Name> is the unique SSO provider name provided to you by CloudShare* in step 1.
Realm	*Leave this field as is.*
ReplyTo URL	**https://use.cloudshare.com/Ent/FederatedLogin.mvc/SignIn**
Allow ReplyTo Override	*Leave this field as is.*
Name ID Format	*Leave this field as is.*
Audience Restriction	**https://www.cloudshare.com**
Assertion Authentication Context	*Leave this field as is.*
Group Attribute Name (Optional)	*Leave this field as is.*
Group Attribute Value	*Leave this field as is.*
Group filter	**CloudshareCampaign.***
Username Attribute Statements	*Leave this field as is.*
Custom Attribute Statements	**givenname|${user.firstName}|,surname|${user.lastName}|,emailaddress|${user.email}|**
Application Visibility	*Leave this field as is.*

5. Click **Next**, click **Next** again (skip **Assign to People**) and then click **Done**.

The Cloudshare application is added to your active applications.
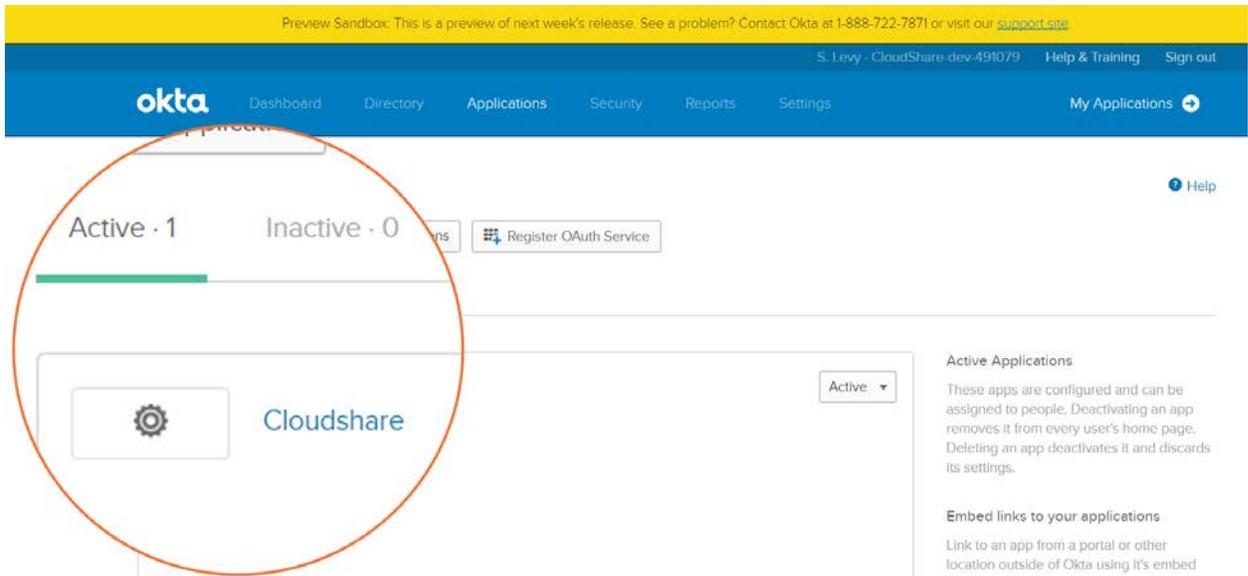
6. Open the **Cloudshare** application you just created.

7. Select the **SignOn** tab, click **View Setup Instructions** and then copy the **Realm (App ID URI)** from the setup instructions page.
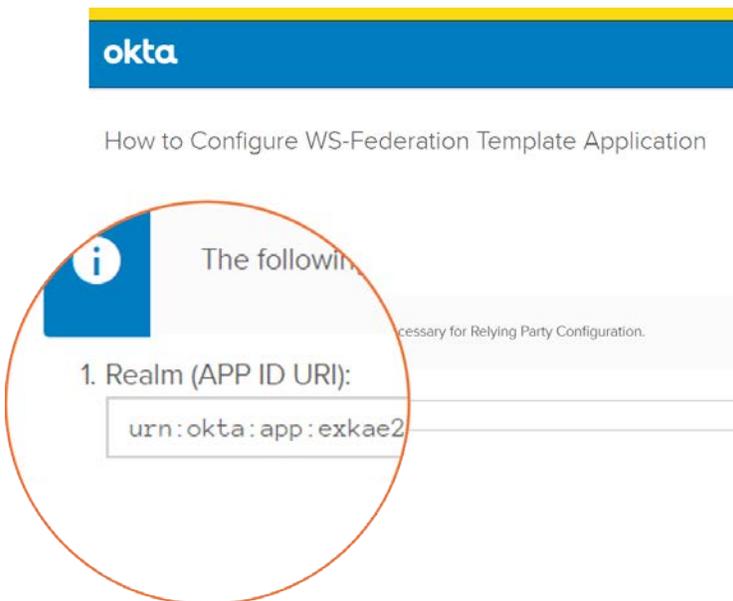
8. Select the **General** tab and paste the value you copied into the **Audience Restriction** field.

Step 3: Assign Users

Each user must have a first name, a last name, and a primary email address defined in Okta. The Okta **primary email address** (and not the Okta **username**) becomes the user's CloudShare username.

For existing Okta users, [check before assigning them that they have the required details and fix if necessary](#).

For any users not defined yet in Okta, [add them as okta users](#) and then assign them.

To assign a user to CloudShare:

1. Open the **Cloudshare** application that you created (From the **Applications** menu, select **Applications**, and then click the application name).

2. Select the **People** tab and then click **Assign to People**.

   The **Assign Cloudshare to People** dialog box appears.

3. Search for a user you want to add and click the **Assign** button for the user.
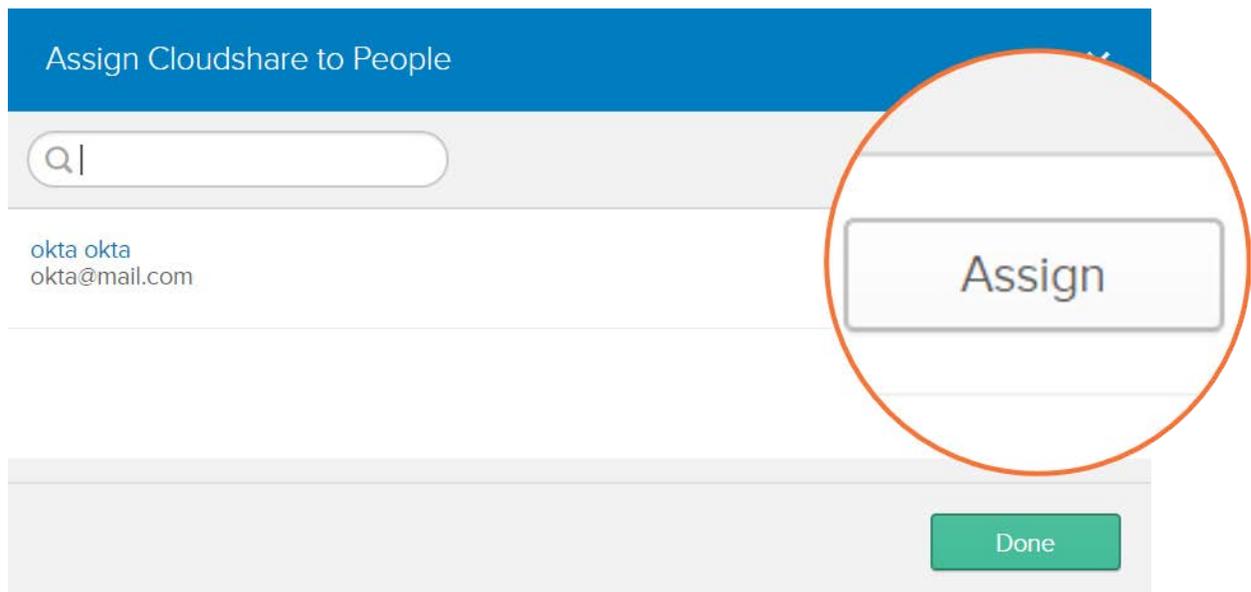
4. Click **Save and Go Back**.

5. Assign more users the same way.

6. Click **Done**.

Checking Okta User Details

To check that an existing Okta user has the required details for CloudShare:

1. Select **People** from the **Directory** menu.

2. Click the user's name and then select the **Profile** tab.

3. On the **Profile** tab, the **First name**, **Last name** and **Primary email** fields must be populated. If not, click **Edit** and add those details.

Adding New Users

To create a new Okta user:

1. From the **Directory** menu, select **People**.

2. Click **Add Person**.

   The **Add Person** dialog box appears.

3. Enter the **First name**, **Last name** and **Primary email**.

4. Select **Send user activation email now**. This will send the user an activation email and enable the user to set a password.

5. Click **Save** (or **Save and Add Another** if you want to add more users).

Step 4: Add Users to Groups

CloudShare user roles are defined per CloudShare project. There are three CloudShare user roles allowed for accessing any CloudShare project:

- Project manager (highest level access)

- Team manager

- Team member (lowest level access)

  The CloudShare-Okta integration applies roles and project access through Okta groups named according to a pre-configured naming convention. Each group you can create enables members to access a specific project with a specific role. For example, adding a user to a group called ***CloudshareCampaign-MyProject-TeamMember*** gives the user access to a project called ***MyProject*** with the ***Team Member*** role

Note: Users who do not belong to a CloudShare group will not be able to sign into CloudShare.

[Create a group](#) for every role you need to assign per project. [Add users](#) to the groups that give them the correct role for the correct project.

Creating Groups

To create a group:

1. From the **Directory** menu, select **Groups**.

2. Click **Add Group**.

3. In the **Name** field, enter:

   CloudshareCampaign-*<Project Name>*-*<Role>*

   <Project Name> is the name of the project. Users who belong to this group will be able to access the specified project.

   <Role> must be one of the following:

   - TeamMember – assigns the team member role.
   - TeamManager – assigns the team manager role.
   - CampaignManager – assigns the project manager role.

   For example, to assign the ***team member*** role for access to a project called ***MyProject***, create a group called ***CloudshareCampaign-MyProject-TeamMember***.

On request, CloudShare Support can customize the role names for you.

4. Click **Add Group**.

The group is created.

Adding Users to Groups

Add each user to a group to grant the user access to a specific project with a specific user role.

To add users to a group:

1. From the **Directory** menu, select **Groups**.

2. Click the group you want to add users to.

3. Click **Manage People** and then add members:

   ▪ Use the search box to find people.
   ▪ To add one person, mouse over the person in the **Not Members** box and then click ⊕
   ▪ To add multiple non-members, click **Add All**.
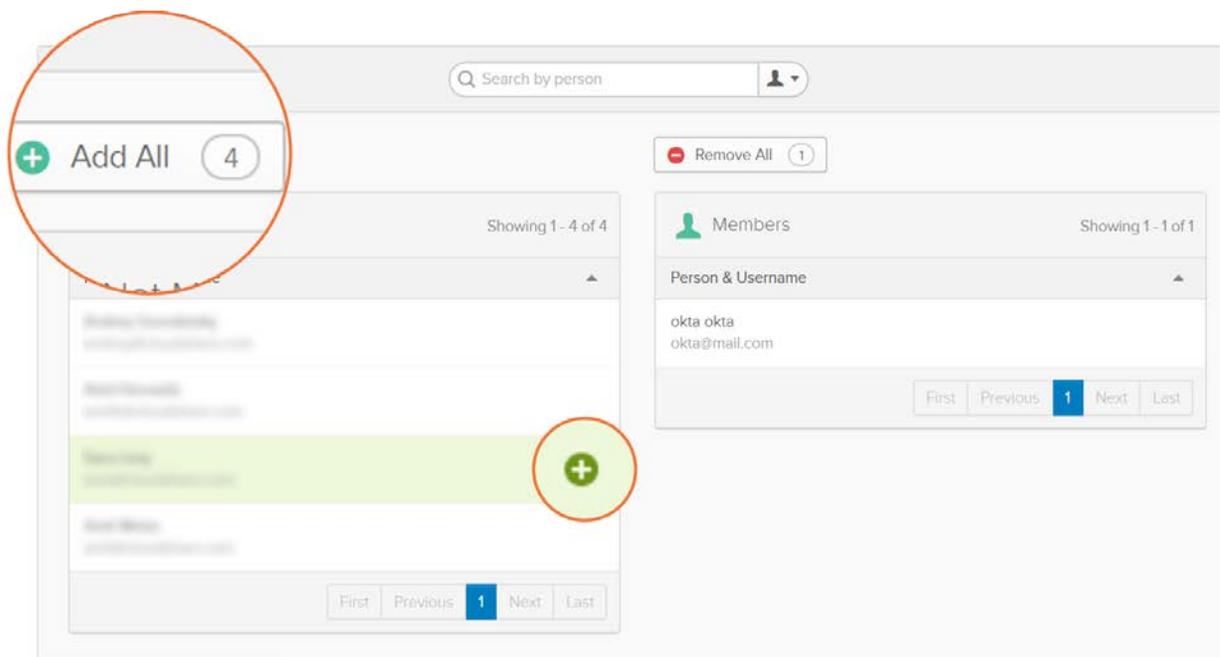
4. Click **Save**.

Step 5: Send Us These Details

To complete the integration:

1. Go to the **Sign On** tab and click the **View Setup Instructions** button.

2. From the page that appears, retrieve the following and provide them to CloudShare support:

   - The Realm (APP ID URI)
   - The Issuer
   - The Passive Endpoint
   - The certificate thumbprint, which you can find in an "<add thumbprint=" element in the **Sample ASP.NET Configuration** code sample.