

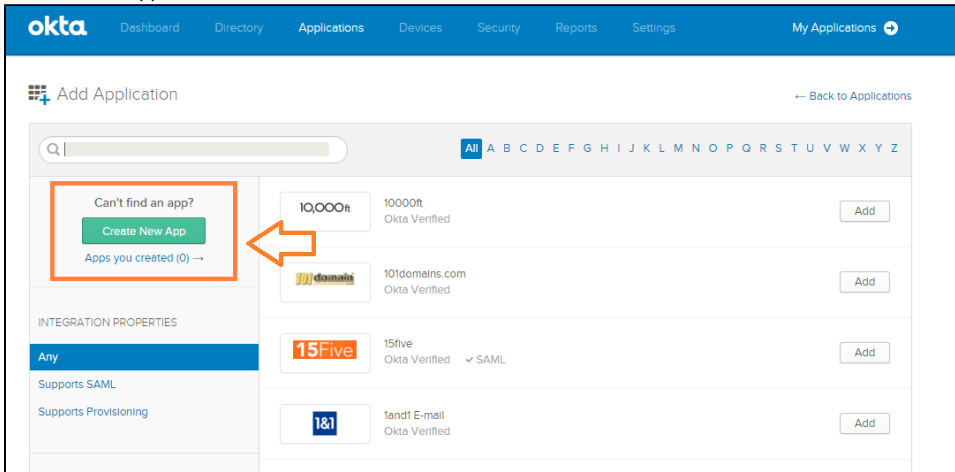
Integrate Okta with FileCloud

 If you are looking to integrate with Okta browser plugin, please review our configuration guide: [Integrate with Okta using browser plugin](#)

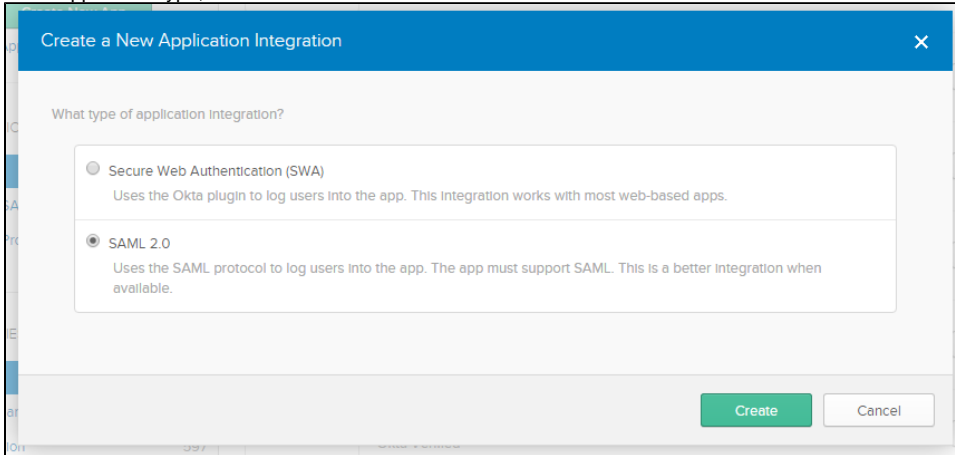
Before completing the following procedures, configure Apache Web Server. See [SSO Configuration Steps, Step 1](#) on the page [SAML Single Sign-On Support](#) for configuration instructions.

FileCloud can be integrated with OKTA. The Okta must be configured as an Identity Provider (IdP) and FileCloud will act as the Service Provider (SP). The following steps must be followed to configure FileCloud with Okta.

1. Log in to your Okta issued URL. <http://yourdomain.okta.com>
2. After successful login to Okta, go to the admin section
3. Create a new application as shown below



In the application type, select SAML 2.0



4. Configure the Application as follows.

The screenshot shows a 'General Settings' configuration window. At the top left, there is a blue circle with the number '1' and the text 'General Settings'. The main content area is a light gray box containing several fields and options:

- App name:** A text input field containing 'MyIdp'.
- App logo(optional):** A section with a gear icon, a text input field, and a 'Browse..' button.
- Upload Logo:** A button below the logo input field.
- App visibility:** Two checkboxes:
 - Do not display application icon to users
 - Do not display application icon in the Okta Mobile app

At the bottom of the window, there are two buttons: 'Cancel' on the left and 'Next' on the right.

- a. Set **Single sign on URL** to the FileCloud assertion URL **`http://<your domain>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp`**
 - b. Set **Audience URI (SP Entity ID)** to **`http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp`**
 - c. Set **Default Relay State** to **`http://<your domain>/auth/saml/so.php`**
- The attribute statements must be set as shown in the screenshot. These attribute names must match the names set in the FileCloud admin screen - Settings SSO parameters for Username, Email, Given Name and Surname.

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 ?

Application username ?

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="givenName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/>	×
<input type="text" value="sn"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>	×
<input type="text" value="email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>	×
<input type="text" value="uid"/>	<input type="text" value="Unspecified"/>	<input type="text" value="substringBefore(user.email, '@')"/>	×

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>	×

5. In the following screen set FileCloud as an Internal App.

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner? I'm an Okta customer adding an internal app I'm a software vendor. I'd like to integrate my app with Okta

1 The optional questions below assist Okta Support in understanding your app integration.

App type This is an internal app that we have created

Why are you asking me this?
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Previous Finish

6. Click **Finish**.

General Sign On Mobile Import People Groups

Settings Edit

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State http://samldev.codelathe.com/auth/samlssso.php

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

Application username format Okta username

7. Click **View Setup Instructions** to get the details to configure FileCloud SSO. The **How to Configure SAML 2.0 for MyIdp Application** screen opens.

8. Get the details for configuring FileCloud from this screen.
- Copy the entity ID field from the Metadata text box on OKTA and use that for **Idp End Point URL** in FileCloud admin UI interface under **Settings > SSO**.
 - Click **Download certificate**, then copy the certificate file and rename to **saml.crt**. Copy this file in the FileCloud server in the following place **<FileCloud WEB ROOT>/thirdparty/simplesaml/cert**

c. The metadata in this screen must match the IdP meta data in FileCloud Admin **Settings > SSO - Idp Meta data**.

How to Configure SAML 2.0 for Myldp Application

The following is needed to configure Myldp

1 Identity Provider Single Sign-On URL:

```
https://c...okta.com/app/...myldp_1/exk35iur66HhSvzh70x7/SSO/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/exk35iur66HhSvzh70x7
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDpJCcAo6GawIBAgI...
-----END CERTIFICATE-----
```

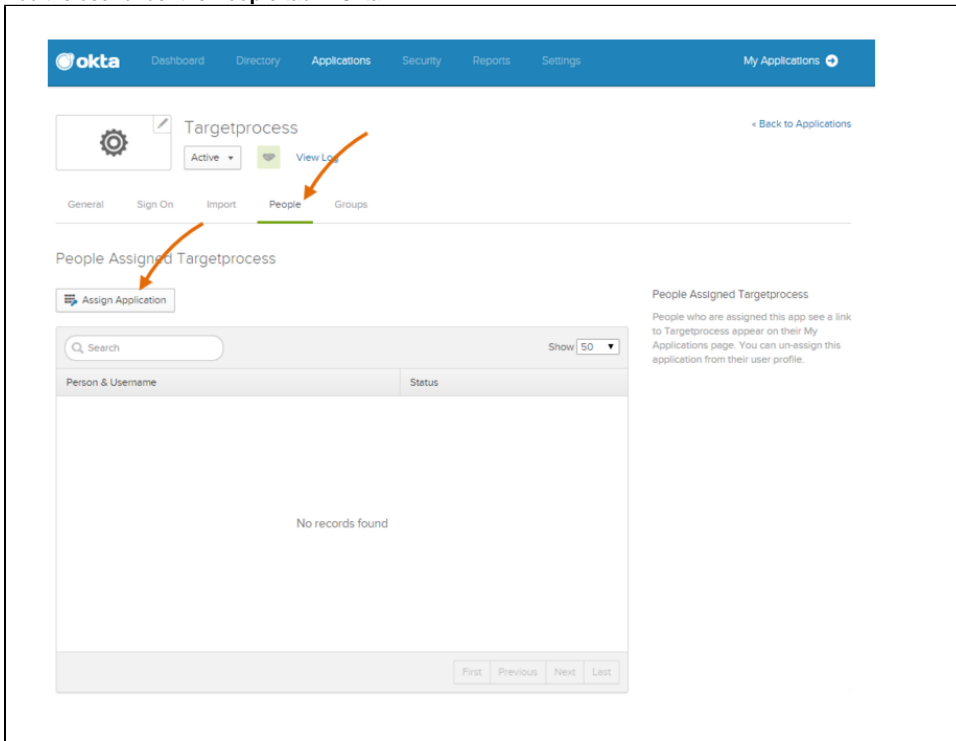
Download certificate

Optional

1 Provide the following IDP metadata to your SP provider.

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exk35iur66HhSvzh70x7"><md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data>
<ds:X509Certificate>MIIDpJCcAo6GawIBAgI...
-----END CERTIFICATE-----
</ds:X509Certificate></md:KeyDescriptor></md:IDPSSODescriptor></md:EntityDescriptor>
```

9. Add the user under the **People** tab in Okta.



The configuration from FileCloud side should be in 'Settings > sso' as follows (in 'idP End Point URL' you should make 'Identity Provider Issuer') :

SAML Settings

IdP End Point URL
URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter
Username Parameter Name in Identity Provider

IdP Email Parameter
Email Parameter Name in Identity Provider

IdP Given Name Parameter
Given Name Parameter Name in Identity Provider

IdP Surname Parameter
Surname Parameter Name in Identity Provider

IdP Meta Data
Enter Identity Provider metadata in XML format.

Enable ADFS
Specify if IdP is Active Directory Federation Service (ADFS)

User Login Token Expiration Match IdP Token Expiration
If enabled, user authentication token will expire as specified by Identity Provider.

Log Level
Specify the Log Level (Use Dev only for testing)

Once the application is created and FileCloud is configured you can start using Single Sign On with Okta from FileCloud