

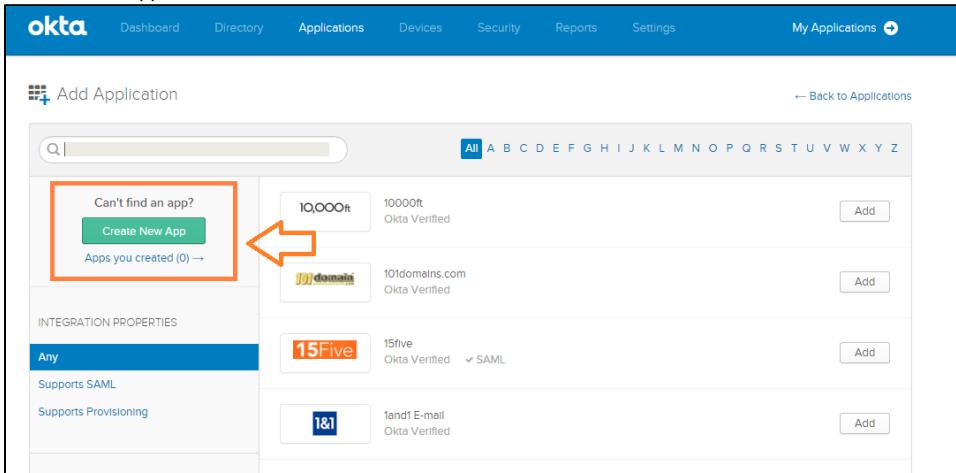
Integrate Okta with FileCloud

 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.

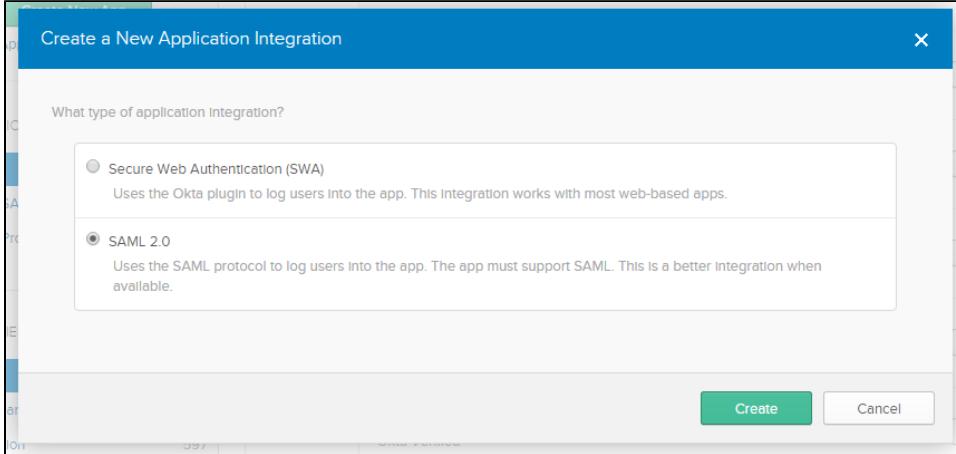
FileCloud can be integrated with OKTA. The Okta must be configured as an Identity Provider (IdP) and FileCloud will act as the Service Provider (SP). The following steps must be followed to configure FileCloud with Okta.

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



The screenshot shows the Okta Admin Console with the 'Add Application' screen. On the left, there's a sidebar with 'INTEGRATION PROPERTIES' set to 'Any'. In the center, there's a search bar and a grid of application cards. One card for '10,000ft' is highlighted with a blue border. An orange arrow points from the 'Create New App' button in the sidebar to the same button in the 'Create a New Application Integration' dialog.

In the application type, select SAML 2.0



The screenshot shows the 'Create a New Application Integration' dialog. It asks 'What type of application integration?' with two options: 'Secure Web Authentication (SWA)' and 'SAML 2.0'. 'SAML 2.0' is selected and highlighted with a blue border. At the bottom are 'Create' and 'Cancel' buttons.

4. Configure the Application as follows.

The screenshot shows the 'General Settings' step of an application configuration wizard. The 'App name' field is filled with 'Myldp'. There is an optional 'App logo' field containing a placeholder gear icon, with a 'Browse...' button and an 'Upload Logo' button below it. Under 'App visibility', two checkboxes are present: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile app'. At the bottom are 'Cancel' and 'Next' buttons.

1 General Settings

App name Myldp

App logo(optional)

Upload Logo

App visibility

Do not display application icon to users

Do not display application icon in the Okta Mobile app

Cancel Next

- a. Set **Single sign on URL** to the FileCloud assertion URL `http://<your domain>/simplesaml/module.php/saml/sp/saml2-acss.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/samlssologin.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.

A

SAML Settings

GENERAL

Single sign on URL ? Use this for Recipient URL and Destination URLAudience 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="button" value="x"/>
<input type="text" value="sn"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>	<input type="button" value="x"/>
<input type="text" value="email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>	<input type="button" value="x"/>
<input type="text" value="uid"/>	<input type="text" value="Unspecified"/>	<input type="text" value="substringBefore(user.email, '@')"/>	<input type="button" value="x"/>

[Add Another](#)

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name

Name format (optional)

Filter

<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>	<input type="button" value="x"/>
----------------------	--	--	----------------------------------

[Add Another](#)

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

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

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

App type This is an internal app that we have created

[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/samlso.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.

- a. 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**.
- b. 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/simplestaml/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/e.../myldp_1/exk35iur66HhsVzh70x7/sso/saml
```

- 2 Identity Provider Issuer:

```
http://www.okta.com/ex.../myldp_1
```

- 3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDpjCAoBgAwIBAgVFoiC9+MA0GCSqGSIb3DQEBCUAMIGTMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTERMBQGA1UEBwwNU2FuIEZyIw5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwLNU1PUHJvdmlkZXIxFDASBgNVBAMC291dGzb2s5MDAxMRwwGgYJKoZIhvcNAQkB
Fg1pbmZvG9rGEuyJ29tMB4XDTE1MTIwMzE1NDc1NFoxDTI1MTIwMzE1NDg1NFowgZMCzA1BgNV
BAYTA1VTRMwEQIDVQQIDA0DYxpZm9ybmlnMRIwFAIDVQQHDA1tIw4gRnJhbmnpc2NMQ0wCwYD
VQQKDARPa3RHQRoEg1DVQQLDArtUO9Qcm92awR1cjeUMBIGA1UEAwLb3V0bG9vazkwMDExHDA
BgkqhkiG9w0BCQEWQDwIuZmAb2t0Y55jb20wgEIMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCoibGfk28my1JCU8XhpUyaZGVrz0646f0aaeu7x/J0wyLr9223x873R13FD4ncGMVRdx16Q/MyN
g1+gx/LMNHpm+c0EUR23t8gBj01c+-+A82p4NuubAzanTU/NienQUpNWZMe4J/IkC6+zuIV6
wZ1brKUc289j0AmL1oDYuJ056deatkoF1JLd+7chLEQ20dxRN14NHw/w1x2FaGugzC2g3dsKLbT
Y7kJ5N7wPPESjTB+e+h7LVLMs4vQO1AXob69yI26sIdjSHfj4S0RKPUET2kvP1B6FaCzPUnig88BH
A2Or/qPyvYdWLJcNgf0bsUDrN+3wYgbF+0xAgMBAEwQZJKoZIhvcNAQFBQA0dgEBAHw
HBfSrpd04kjerzINwdn7wGSxqjXNXYW/f0nqGfPh0A57mP1BL/k0zMDcG7MgAFMdgy/crIP/mDe/5
0VU9/L40JqE12tajesr2AGq082XacfgaXZ7c51jpUcydJxRS0waibG-AEtzS8eyx/cS1t66bVBA
JxG1GIBD/9M0cSUf8nkHd97UE7+RKFysmrFWKD12Nrek+Enemk5EGHLA/ssVWECLhdiHCunkle+
H1GB5SrA0104ghqkMDW31nkHkHcSBhL1fflLUSV6re8tOkMChxc0BsRFvV2oEc1JAPNL95ce6xg
PEKQjQX0aqIMQPm0h2NyRc36nx0Tfu09JXs=
-----END CERTIFICATE-----
```

[Download certificate](#)

Optional

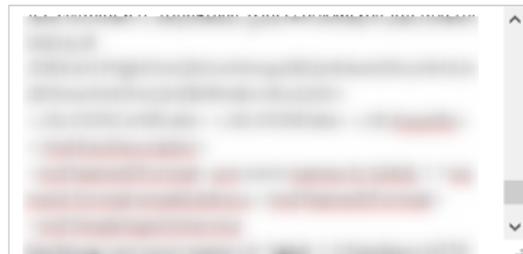
- 1 Provide the following IDP metadata to your SP provider.

```
<?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 WantAuthRequestsSigned="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>MIIDpjCAoBgAwIBAgVFoiC9+MA0GCSqGSIb3DQEBCUAMIGTMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTERMBQGA1UEBwwNU2FuIEZyIw5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwLNU1PUHJvdmlkZXIxFDASBgNVBAMC291dGzb2s5MDAxMRwwGgYJKoZIhvcNAQkB
Fg1pbmZvG9rGEuyJ29tMB4XDTE1MTIwMzE1NDc1NFoxDTI1MTIwMzE1NDg1NFowgZMCzA1BgNV
BAYTA1VTRMwEQIDVQQIDA0DYxpZm9ybmlnMRIwFAIDVQQHDA1tIw4gRnJhbmnpc2NMQ0wCwYD
VQQKDARPa3RHQRoEg1DVQQLDArtUO9Qcm92awR1cjeUMBIGA1UEAwLb3V0bG9vazkwMDExHDA
BgkqhkiG9w0BCQEWQDwIuZmAb2t0Y55jb20wgEIMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCoibGfk28my1JCU8XhpUyaZGVrz0646f0aaeu7x/J0wyLr9223x873R13FD4ncGMVRdx16Q/MyN
g1+gx/LMNHpm+c0EUR23t8gBj01c+-+A82p4NuubAzanTU/NienQUpNWZMe4J/IkC6+zuIV6
wZ1brKUc289j0AmL1oDYuJ056deatkoF1JLd+7chLEQ20dxRN14NHw/w1x2FaGugzC2g3dsKLbT
Y7kJ5N7wPPESjTB+e+h7LVLMs4vQO1AXob69yI26sIdjSHfj4S0RKPUET2kvP1B6FaCzPUnig88BH
A2Or/qPyvYdWLJcNgf0bsUDrN+3wYgbF+0xAgMBAEwQZJKoZIhvcNAQFBQA0dgEBAHw
HBfSrpd04kjerzINwdn7wGSxqjXNXYW/f0nqGfPh0A57mP1BL/k0zMDcG7MgAFMdgy/crIP/mDe/5
0VU9/L40JqE12tajesr2AGq082XacfgaXZ7c51jpUcydJxRS0waibG-AEtzS8eyx/cS1t66bVBA
JxG1GIBD/9M0cSUf8nkHd97UE7+RKFysmrFWKD12Nrek+Enemk5EGHLA/ssVWECLhdiHCunkle+
H1GB5SrA0104ghqkMDW31nkHkHcSBhL1fflLUSV6re8tOkMChxc0BsRFvV2oEc1JAPNL95ce6xg
PEKQjQX0aqIMQPm0h2NyRc36nx0Tfu09JXs=
-----END CERTIFICATE-----
```

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

The screenshot shows the Okta Applications interface. At the top, there's a navigation bar with links for Dashboard, Directory, Applications (which is the active tab), Security, Reports, and Settings. To the right of the Applications link is a "My Applications" button. Below the navigation, the application details for "Targetprocess" are displayed. The application icon is a gear, status is "Active", and there's a "View Log" button. Below the icon are tabs for General, Sign On, Import, People (which is the selected tab, highlighted in green), and Groups. A red arrow points from the "People" tab to the "Assign Application" button. The main content area is titled "People Assigned Targetprocess" and contains a search bar and a table with columns for Person & Username and Status. The table shows "No records found". A red arrow also points to the "Assign Application" button. To the right of the table, there's a note: "People who are assigned this app see a link to Targetprocess appear on their My Applications page. You can un-assign this application from their user profile." At the bottom of the page are "First", "Previous", "Next", and "Last" navigation buttons.

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	<input type="text" value="REDACTED"/>
URL of the Identity Provider that the Service Provider must contact.	
IdP Username Parameter	<input type="text" value="uid"/>
Username Parameter Name in Identity Provider	
IdP Email Parameter	<input type="text" value="mail"/>
Email Parameter Name in Identity Provider	
IdP Given Name Parameter	<input type="text" value="givenName"/>
Given Name Parameter Name in Identity Provider	
IdP Surname Parameter	<input type="text" value="sn"/>
Surname Parameter Name in Identity Provider	
IdP Meta Data	<input type="text" value="REDACTED"/> 
Enter Identity Provider metadata in XML format.	
Enable ADFS	<input type="button" value="NO"/>
Specify if IdP is Active Directory Federation Service (ADFS)	
User Login Token Expiration Match IdP Token Expiration	<input type="checkbox"/>
If enabled, user authentication token will expire as specified by Identity Provider.	
Log Level	<input type="button" value="DEV"/>
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