


Integrate Okta with FileCloud

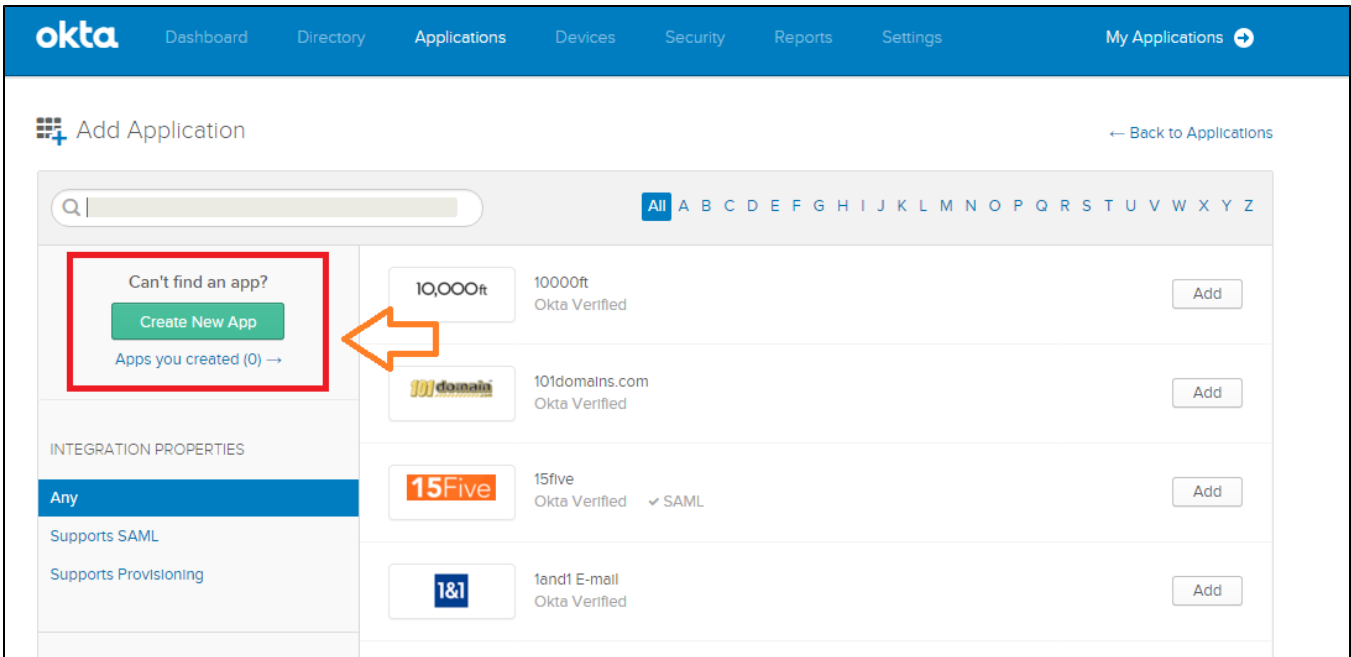
 If you are looking to integrate with Okta browser plugin, please review our configuration guide: [Integrate with Okta using browser plugin](#)

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.

Log in to your Okta issued URL. <http://yourdomain.okta.com>

After successful login to Okta, go to the admin section

Create a new application as shown below



The screenshot shows the Okta Admin Console interface. The top navigation bar includes 'okta', 'Dashboard', 'Directory', 'Applications', 'Devices', 'Security', 'Reports', 'Settings', and 'My Applications'. The main content area is titled 'Add Application' and features a search bar and a list of applications. A red box highlights the 'Create New App' button in the sidebar, and an orange arrow points to it. The list of applications includes:

Application Name	Provider	Integration Type	Action
10,000ft	10000ft	Okta Verified	Add
101domains.com	101domains.com	Okta Verified	Add
15Five	15five	Okta Verified, SAML	Add
1&1	1and1 E-mail	Okta Verified	Add

In the application type, select SAML 2.0

Create a New Application Integration ✕

What type of application integration?

- Secure Web Authentication (SWA)
Uses the Okta plugin to log users into the app. This integration works with most web-based apps.
- SAML 2.0
Uses the SAML protocol to log users into the app. The app must support SAML. This is a better integration when available.

Create Cancel

Configure the Application as follows.

1 General Settings

App name

App logo(optional) ?

Browse..

Upload Logo

App visibility

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

Cancel Next

The single sign on URL is the FileCloud assertion URL <http://<your domain>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp>

Entity ID is set as <http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp>

Default Relay State is set as <http://<your domain>/auth/saml2sso.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 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="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"/>

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"/>

In the following screen set the 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

Click the Finish button. Click "View Setup Instructions" to get the details to configure FileCloud SSO.

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
-----------------------------	---------------

Get the details to configure FileCloud from this screen.

- Idp End Point URL in FileCloud admin (Settings) - Must be the same as the entity ID value from the IDP Meta Data value in the screen (See Screen Shot below)
- Download the Certificate. 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
- The meta data in this screen must match the IdP meta data in FileCloud Admin Settings - SSO - Idp Metadata.

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.

How to Configure SAML 2.0 for MyDp Application

The following is needed to configure MyDp

- 1 Identity Provider Single Sign-On URL:

```
https://c[redacted]okta.com/app/c[redacted]mydp_1/exk35iur66HHsVzh70x7/sso/saml
```

- 2 Identity Provider Issuer:

```
http://www.okta.com/exk35iur66HHsVzh70x7
```

- 3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDpjCCAo6gAwIBAgIGAVFoIC9+MA0GCSqGSIb3DQEBBQUAMIGTMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FueIEZyYW5jaXNjbzENMA5GA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFDASBgNVBAMMC291dGxvbn2s5MDAxMRwwGgYJKoZIhvcNAQkB
Fg1pbmZvQG9rdGEuY29tMB4XDTE1MTIwMzE1NDc1NFoXDTI1MTIwMzE1NDg1NFowZmxCzAJBgNV
BAYTA1VTMRMRwEQYDVQQIDApDYWxpZm9ybmlhMR1wYwYwFAYDQQAHA1Yw4gRnJhbmc2N2NmMQ0wCwYD
VQKQDARPa3RHRMRQwEgYDVQQQLDAtTU09Qcm92aWR1c2EUMBIGA1UEAwwLb3V0bG9vazkwMDExHDAa
BgkqhkiG9w0BCQEWDLiZm9Ab2t0YS5jb20wgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQc0bGfk2SmyIJC8XhpUyaZGVrzG646f0aau7x/jOwyLr9223x8T3R13FD4ncGMVRdX16Q/MyN5
gi+gx/1MNHp+m+c0EURRZ3t8gBj0l6c++j/A82p4NuubAzan7U/NlenQUpNWZMe4J/IkC6+z1uV6
wZ1brKUCz89jGAmLiodyJo56deatKoF1jLD+7chLEG2QdxRNI4NHYYw/w1XzFaGugzC2g3dsK8LbT
Y7kJ5N7wPPESjTBE+h79LVms4vQ01AXob89yI25sIdjSHfj4SuRKPUe72kvPIB6FaCzPUnig8B8H
A2Or/qPyQvyYdWLTcNgf6bshDDrN+3w8YgbPF+OxAgMBAEEwDQYJKoZIhvcNAQEFBQADggEBAHIW
HBfSrp04kjerzTNWdm7wGSxqjXNXyW/fQnqCdFh0A57mPI8L/k9zMDcG7MgAFMdgycrIP/mDe/5
0VU9/L4OJnE12taiesr2AGoo82XacfaaXZ7c5IjpUcYdJxRS0waibG+AetzS8evx/cS1tt66bVBA
JxG1G1Bb/9M0cSuF8nkHd97UE7+RkFysmrFWKD1zNrek+Enemk5EGHLA/ssVWECTLhd1HCunkIe+
HiGBSrA0104gHqkMDW6x1nkHkHcSBhL1ffLUSYv6re8TokMCHxc00BsrfV2oEclJAPNL95ceGxg
PEkQjQX0aaqIMQpm0h2NyRc36nx6TfU09JXs=
-----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>MIIDpjCCAo6gAwIBAgIGAVFoIC9+MA0GCSqGSIb3DQEBBQUAMIGTMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FueIEZyYW5jaXNjbzENMA5GA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFDASBgNVBAMMC291dGxvbn2s5MDAxMRwwGgYJKoZIhvcNAQkB
Fg1pbmZvQG9rdGEuY29tMB4XDTE1MTIwMzE1NDc1NFoXDTI1MTIwMzE1NDg1NFowZmxCzAJBgNV
BAYTA1VTMRMRwEQYDVQQIDApDYWxpZm9ybmlhMR1wYwYwFAYDQQAHA1Yw4gRnJhbmc2N2NmMQ0wCwYD
VQKQDARPa3RHRMRQwEgYDVQQQLDAtTU09Qcm92aWR1c2EUMBIGA1UEAwwLb3V0bG9vazkwMDExHDAa
BgkqhkiG9w0BCQEWDLiZm9Ab2t0YS5jb20wgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQc0bGfk2SmyIJC8XhpUyaZGVrzG646f0aau7x/jOwyLr9223x8T3R13FD4ncGMVRdX16Q/MyN5
gi+gx/1MNHp+m+c0EURRZ3t8gBj0l6c++j/A82p4NuubAzan7U/NlenQUpNWZMe4J/IkC6+z1uV6
wZ1brKUCz89jGAmLiodyJo56deatKoF1jLD+7chLEG2QdxRNI4NHYYw/w1XzFaGugzC2g3dsK8LbT
Y7kJ5N7wPPESjTBE+h79LVms4vQ01AXob89yI25sIdjSHfj4SuRKPUe72kvPIB6FaCzPUnig8B8H
A2Or/qPyQvyYdWLTcNgf6bshDDrN+3w8YgbPF+OxAgMBAEEwDQYJKoZIhvcNAQEFBQADggEBAHIW
HBfSrp04kjerzTNWdm7wGSxqjXNXyW/fQnqCdFh0A57mPI8L/k9zMDcG7MgAFMdgycrIP/mDe/5
0VU9/L4OJnE12taiesr2AGoo82XacfaaXZ7c5IjpUcYdJxRS0waibG+AetzS8evx/cS1tt66bVBA
JxG1G1Bb/9M0cSuF8nkHd97UE7+RkFysmrFWKD1zNrek+Enemk5EGHLA/ssVWECTLhd1HCunkIe+
HiGBSrA0104gHqkMDW6x1nkHkHcSBhL1ffLUSYv6re8TokMCHxc00BsrfV2oEclJAPNL95ceGxg
PEkQjQX0aaqIMQpm0h2NyRc36nx6TfU09JXs=
-----END CERTIFICATE-----
```


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

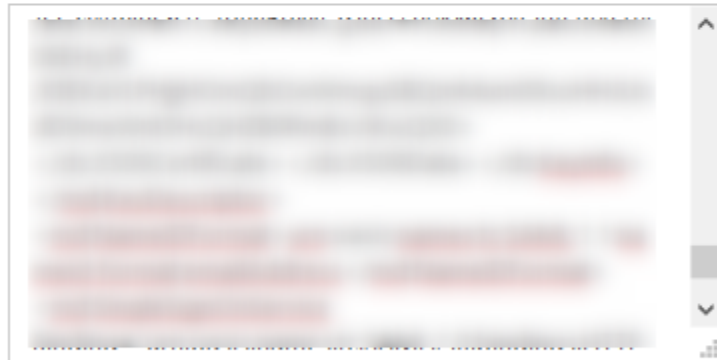
IdP Given Name
Parameter

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 the Single Sign On with Okta from FileCloud