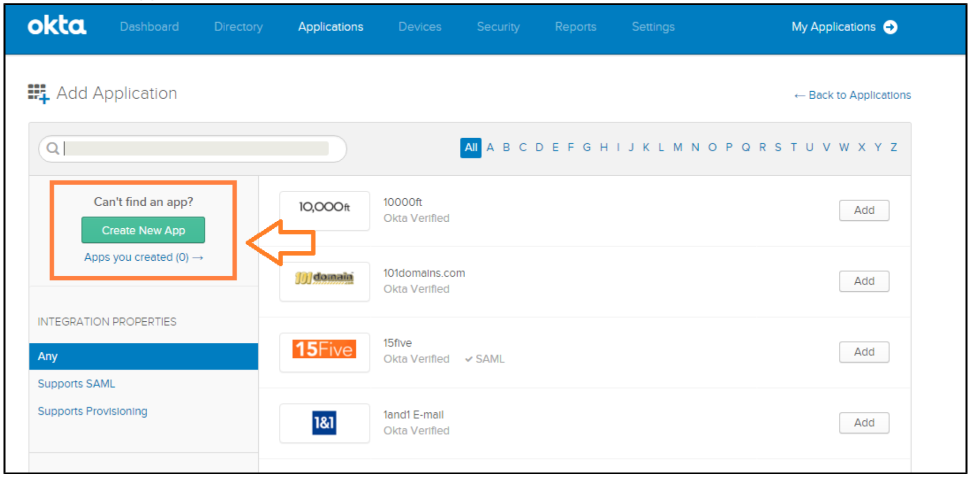
Integrate Okta with FileCloud

ⓘ If you are looking to integrate with Okta browser plugin, please review our configuration guide: Integrate with Okta using browser plugin

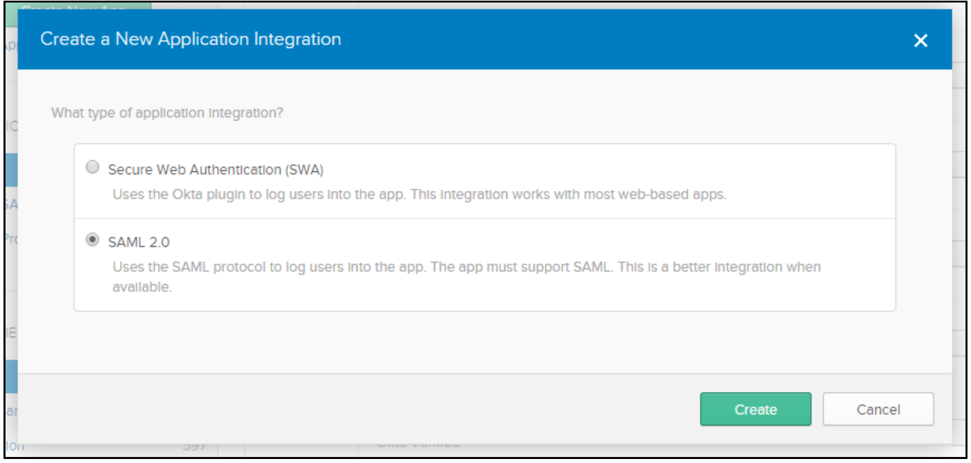
Before completing the following procedures, configure Apache Web Server. See SSO Configuration Steps, Step 1 on the page SAML Single Sign-On Support for configuration instructions.

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



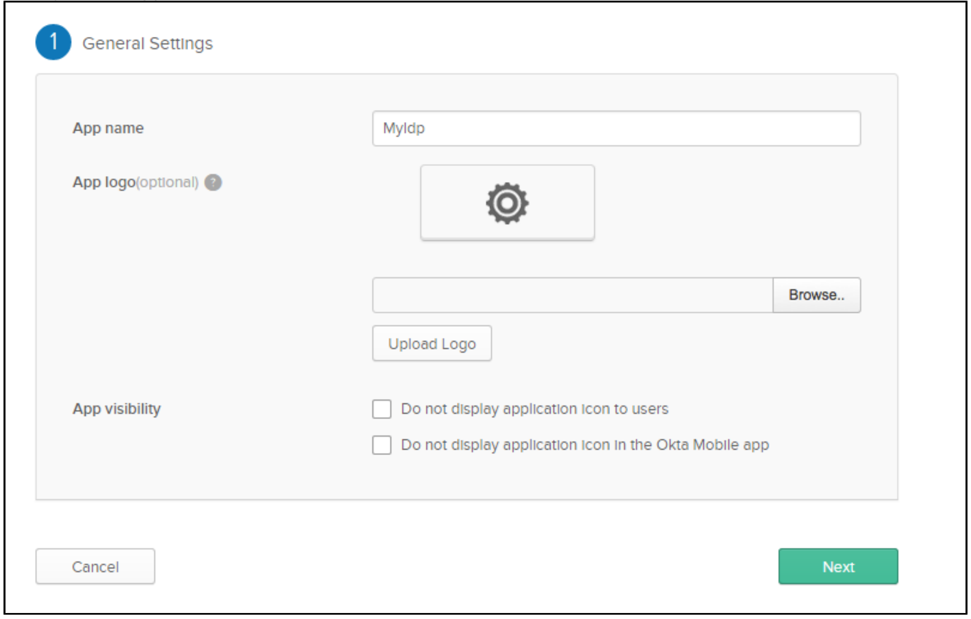
Create a New Application Integration

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.

4. Configure the Application as follows.



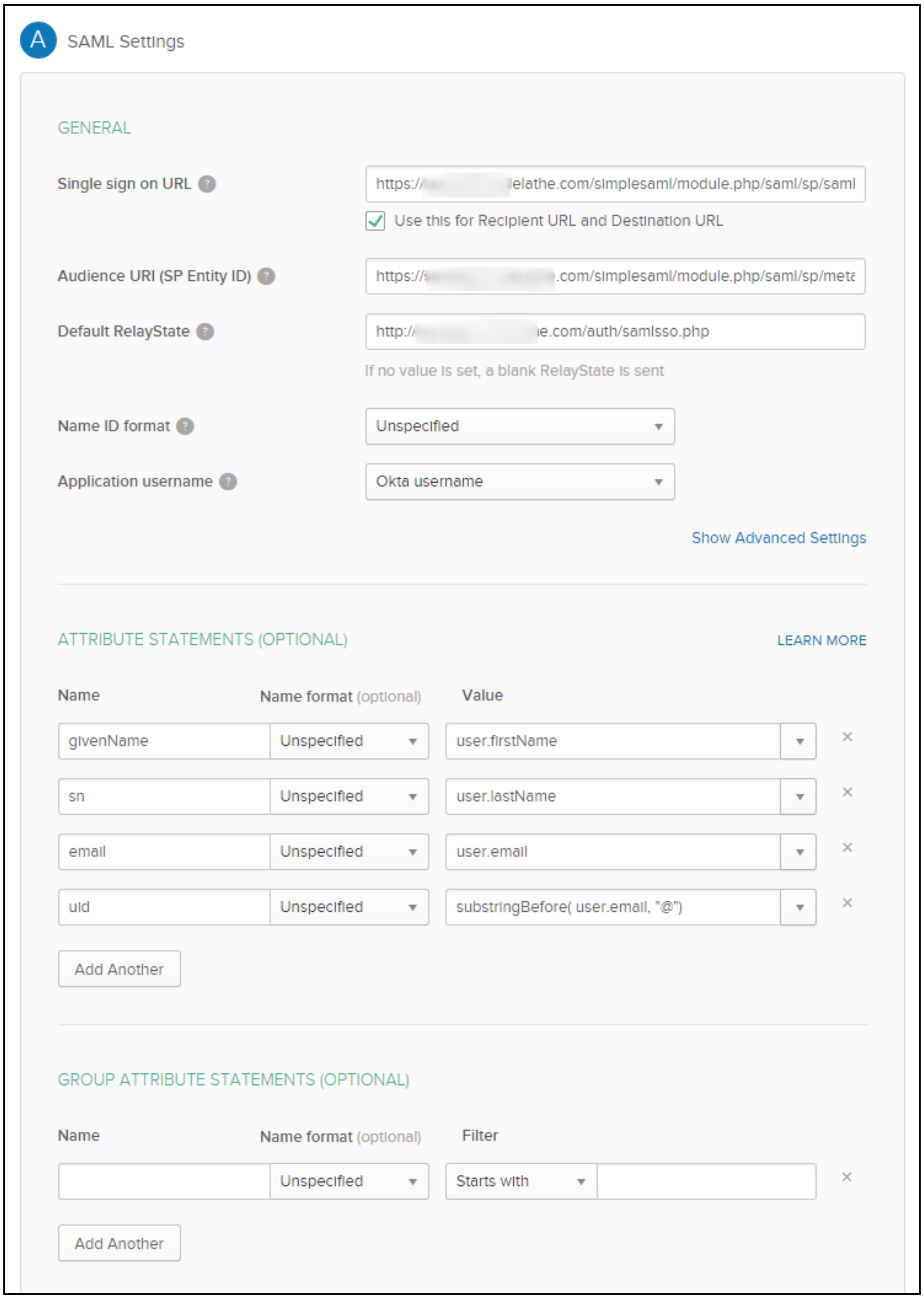
1 General Settings

App name: MyIdp

App logo(optional)

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

   a. Set **Single sign on URL tp** 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/samlsso.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 ?: https://[redacted]elathe.com/simplesaml/module.php/saml/sp/saml

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?: https://[redacted].com/simplesaml/module.php/saml/sp/meta

Default RelayState ?: http://[redacted]e.com/auth/samlsso.php

If no value is set, a blank RelayState is sent

Name ID format ?: Unspecified ▾

Application username ?: Okta username ▾

Show Advanced Settings

ATTRIBUTE STATEMENTS (OPTIONAL) LEARN MORE

Name	Name format (optional)	Value	
givenName	Unspecified ▾	user.firstName ▾	×
sn	Unspecified ▾	user.lastName ▾	×
email	Unspecified ▾	user.email ▾	×
uid	Unspecified ▾	substringBefore(user.email, "@") ▾	×

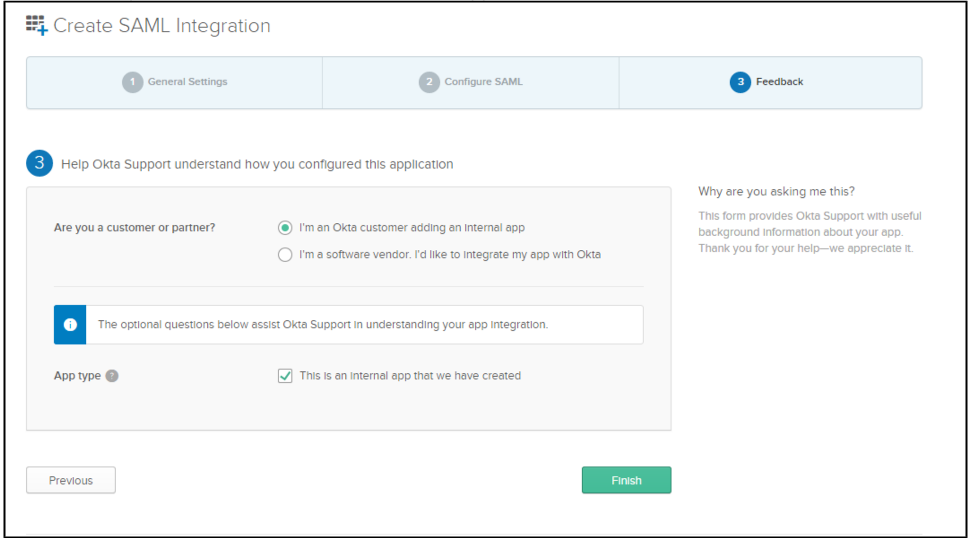
Add Another

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter		
	Unspecified ▾	Starts with ▾		×

Add Another

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



Create SAML Integration

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

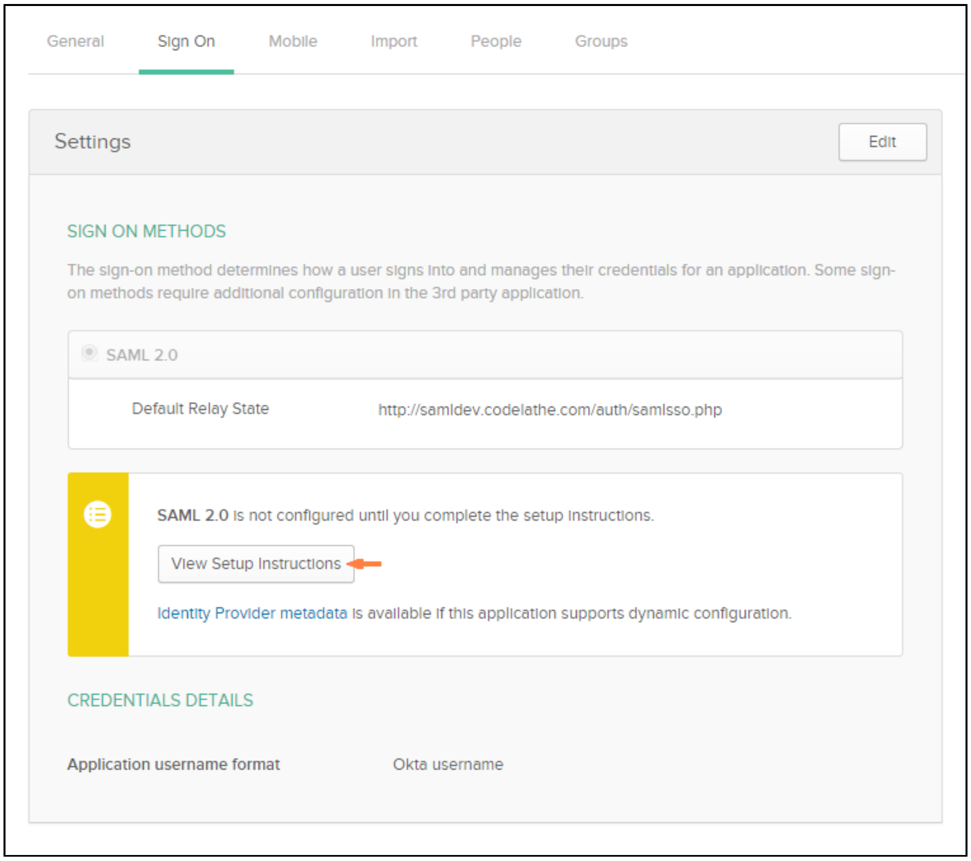
The optional questions below assist Okta Support in understanding your app integration.

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.

6. Click **FInish**.



Settings

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/samlsso.php

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

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

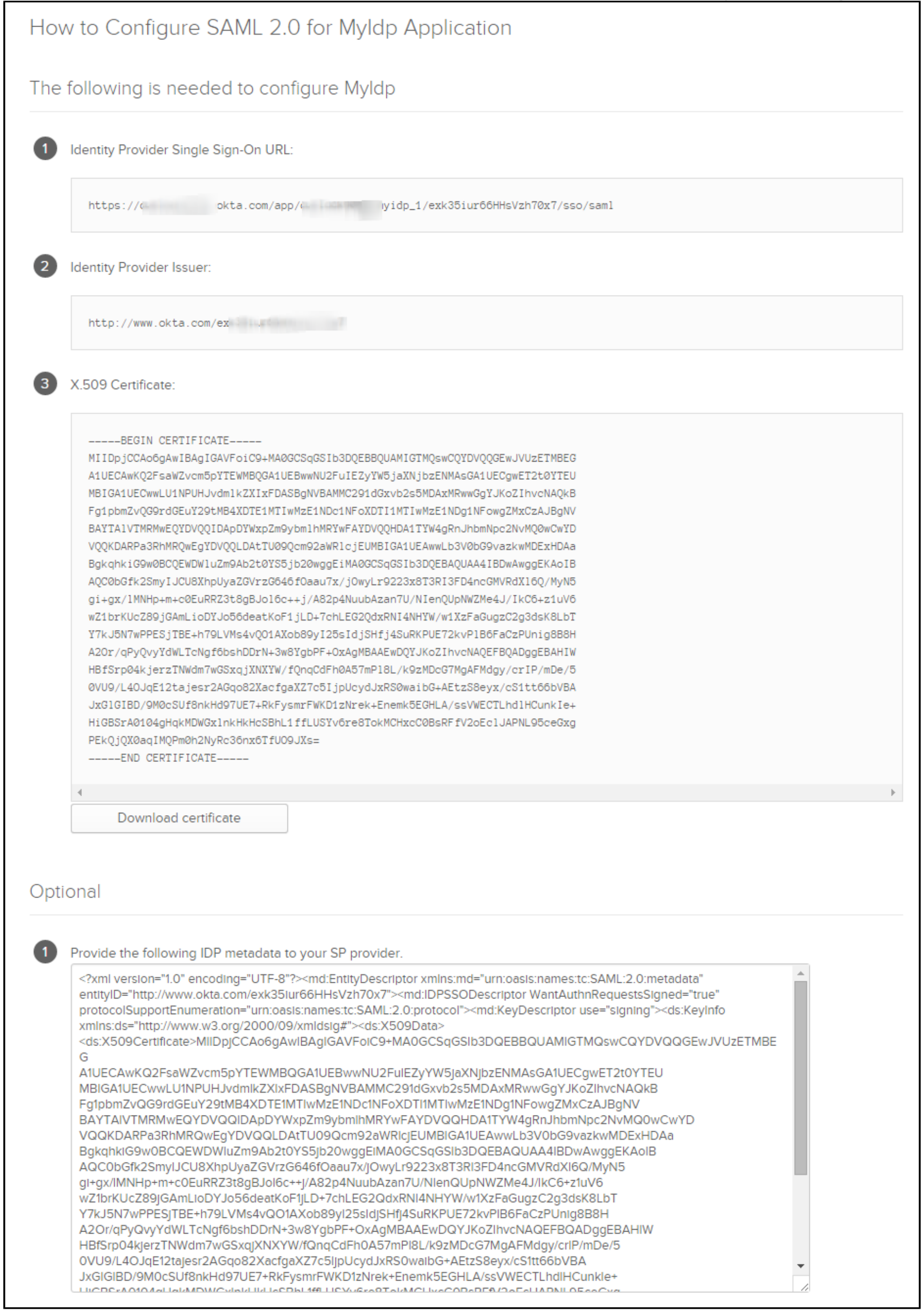
CREDENTIALS DETAILS

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/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 MyIdp Application

The following is needed to configure MyIdp

1 Identity Provider Single Sign-On URL:

```
https://[redacted]okta.com/app/[redacted]yidp_1/exk35iur66HHsVzh70x7/sso/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/ex[redacted]
```

3 X.509 Certificate:

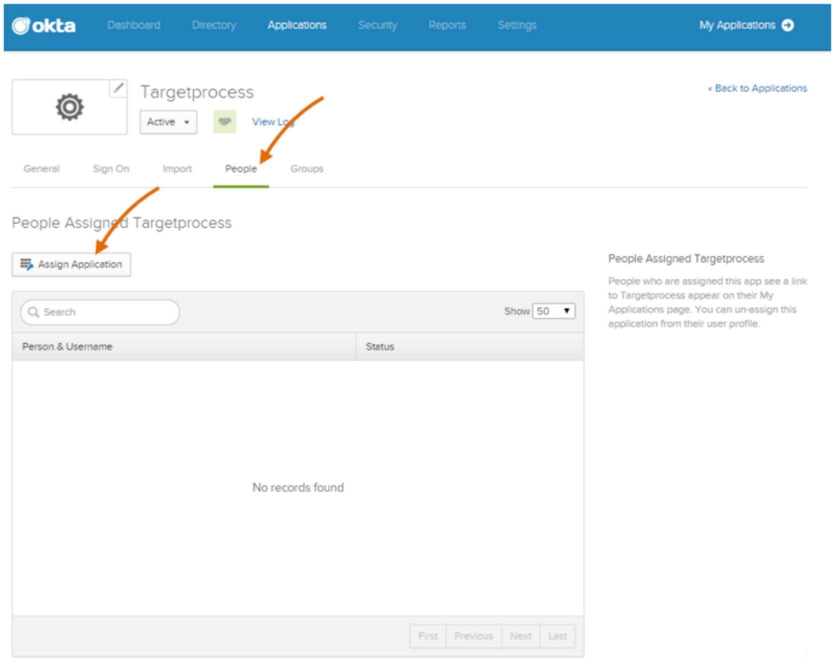
```
-----BEGIN CERTIFICATE-----
MIIDpjCCAo6gAwIBAgIGAVFoiC9+MA0GCSqGSIb3DQEBBQUAMIGTMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFDASBgNVBAMMC291dGxvb2s5MDAxMRwwGgYJKoZIhvcNAQkB
Fg1pbmZvQG9rdGEuY29tMB4XDTE1MTIwMzE1NDc1NFoXDTI1MTIwMzE1NDg1NFowgZMxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0wCwYD
VQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEUMBIGA1UEAwwLb3V0bG9vazkwMDExHDAa
BgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQC0bGfk2SmyIJCU8XhpUyaZGVrzG646fOaau7x/jOwyLr9223x8T3RI3FD4ncGMVRdXl6Q/MyN5
gi+gx/lMNHp+m+c0EuRRZ3t8gBJol6c++j/A82p4NuubAzan7U/NIenQUpNWZMe4J/IkC6+z1uV6
wZ1brKUcZ89jGAmLioDYJo56deatKoF1jLD+7chLEG2QdxRNI4NHYW/w1XzFaGugzC2g3dsK8LbT
Y7kJ5N7wPPESjTBE+h79LVMs4vQO1AXob89yI25sIdjSHfj4SuRKPUE72kvPlB6FaCzPUnig8B8H
A2Or/qPyQvyYdWLTcNgf6bshDDrN+3w8YgbPF+OxAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAHIW
HBfSrp04kjerzTNWdm7wGSxqjXNXYW/fQnqCdFh0A57mPl8L/k9zMDcG7MgAFMdgy/crIP/mDe/5
0VU9/L4OJqE12tajesr2AGqo82XacfgaXZ7c5IjpUcydJxRS0waibG+AEtzS8eyx/cS1tt66bVBA
JxGlGIBD/9M0cSUf8nkHd97UE7+RkFysmrFWKD1zNrek+Enemk5EGHLA/ssVWECTLhdlHCunkIe+
HiGBSrA0104gHqkMDWGxlnkHkHcSBhL1ffLUSYv6re8TokMCHxcC0BsRFfV2oEclJAPNL95ceGxg
PEkQjQX0aqIMQPm0h2NyRc36nx6TfUO9JXs=
-----END 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+MA0GCSqGSIb3DQEBBQUAMIGTMQswCQYDVQQGEwJVUzETMBE
G
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFDASBgNVBAMMC291dGxvb2s5MDAxMRwwGgYJKoZIhvcNAQkB
Fg1pbmZvQG9rdGEuY29tMB4XDTE1MTIwMzE1NDc1NFoXDTI1MTIwMzE1NDg1NFowgZMxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0wCwYD
VQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWRlcjEUMBIGA1UEAwwLb3V0bG9vazkwMDExHDAa
BgkqhkiG9w0BCQEWDWluZm9Ab2t0YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQC0bGfk2SmyIJCU8XhpUyaZGVrzG646fOaau7x/jOwyLr9223x8T3RI3FD4ncGMVRdXl6Q/MyN5
gi+gx/lMNHp+m+c0EuRRZ3t8gBJol6c++j/A82p4NuubAzan7U/NIenQUpNWZMe4J/IkC6+z1uV6
wZ1brKUcZ89jGAmLioDYJo56deatKoF1jLD+7chLEG2QdxRNI4NHYW/w1XzFaGugzC2g3dsK8LbT
Y7kJ5N7wPPESjTBE+h79LVMs4vQO1AXob89yI25sIdjSHfj4SuRKPUE72kvPlB6FaCzPUnig8B8H
A2Or/qPyQvyYdWLTcNgf6bshDDrN+3w8YgbPF+OxAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAHIW
HBfSrp04kjerzTNWdm7wGSxqjXNXYW/fQnqCdFh0A57mPl8L/k9zMDcG7MgAFMdgy/crIP/mDe/5
0VU9/L4OJqE12tajesr2AGqo82XacfgaXZ7c5IjpUcydJxRS0waibG+AEtzS8eyx/cS1tt66bVBA
JxGlGIBD/9M0cSUf8nkHd97UE7+RkFysmrFWKD1zNrek+Enemk5EGHLA/ssVWECTLhdlHCunkIe+
```

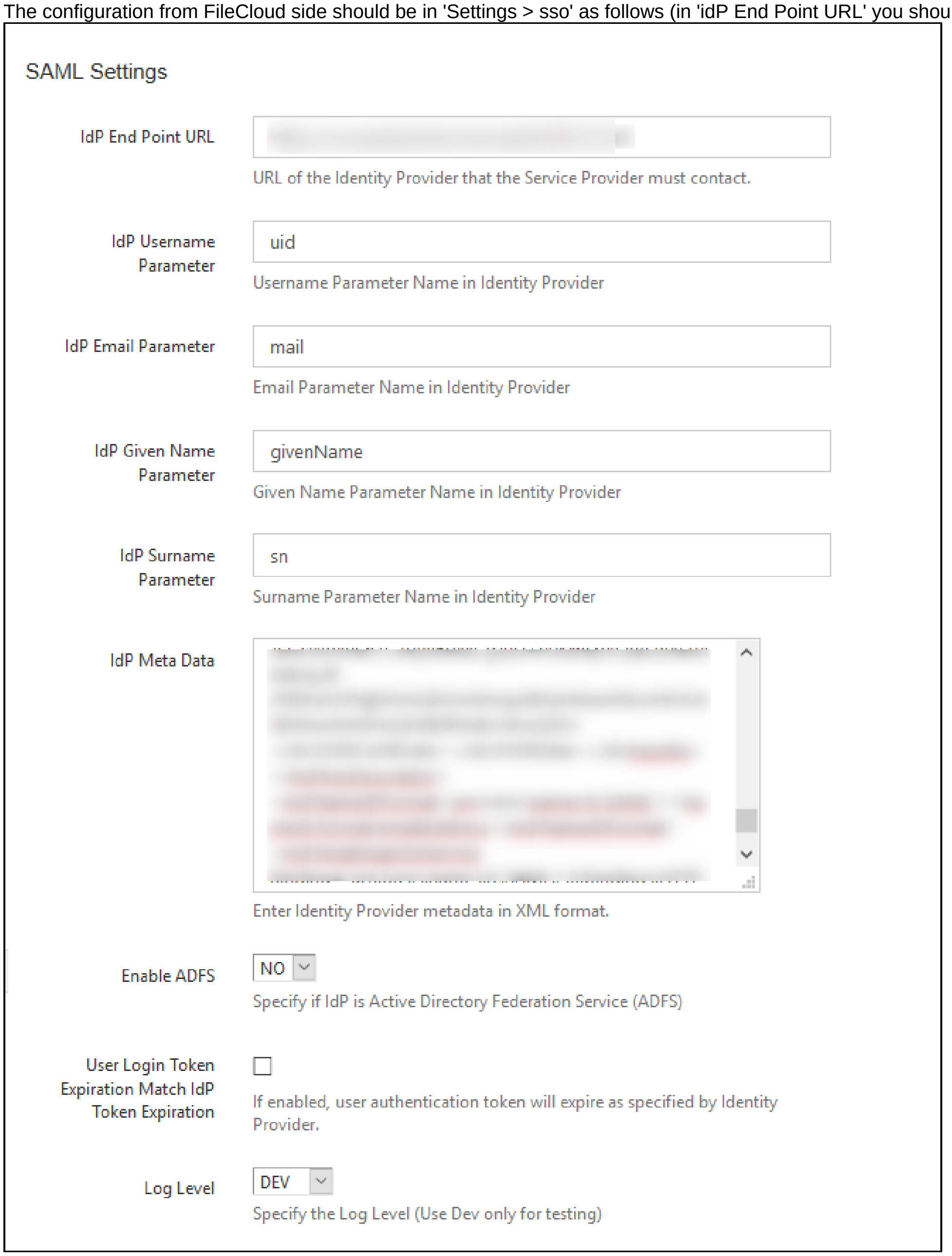
9. Add the user under the **People** tab in Okta.



People Assigned Targetprocess

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.

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: [redacted]
URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter: uid
Username Parameter Name in Identity Provider

IdP Email Parameter: mail
Email Parameter Name in Identity Provider

IdP Given Name Parameter: givenName
Given Name Parameter Name in Identity Provider

IdP Surname Parameter: sn
Surname Parameter Name in Identity Provider

IdP Meta Data: [redacted]
Enter Identity Provider metadata in XML format.

Enable ADFS: NO
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: 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