

Content Collaboration: Single Sign-On Configuration Guide

Okta

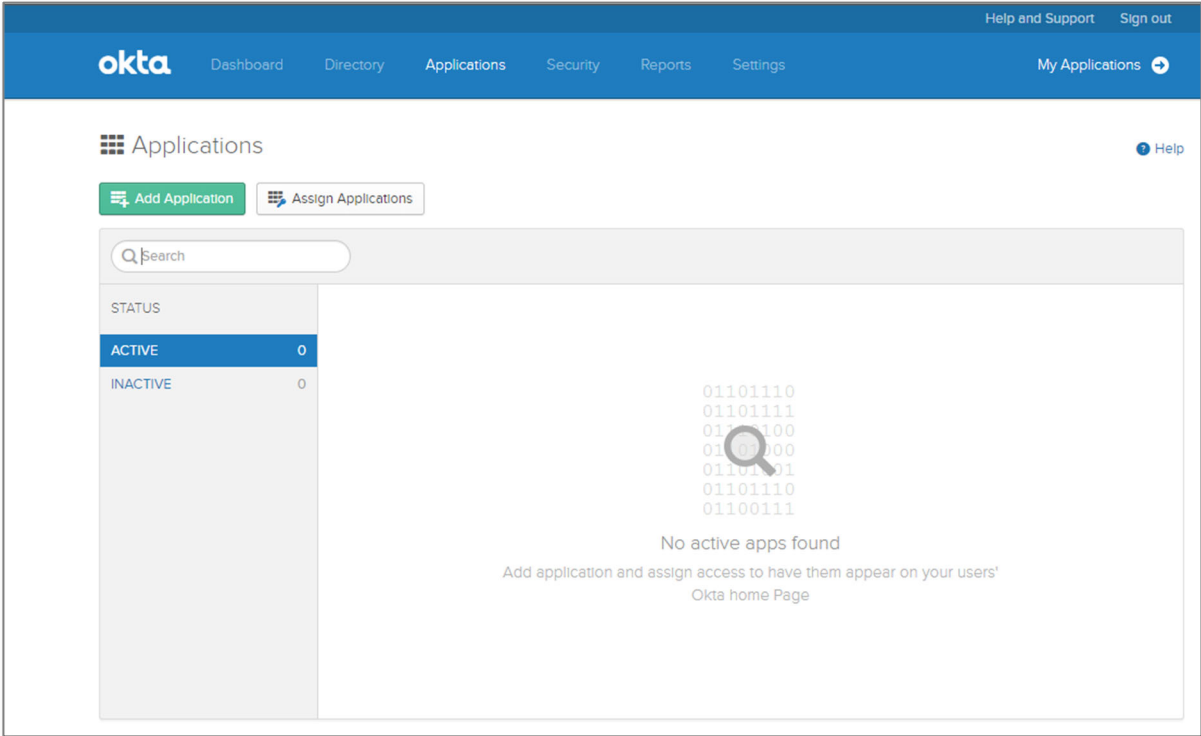
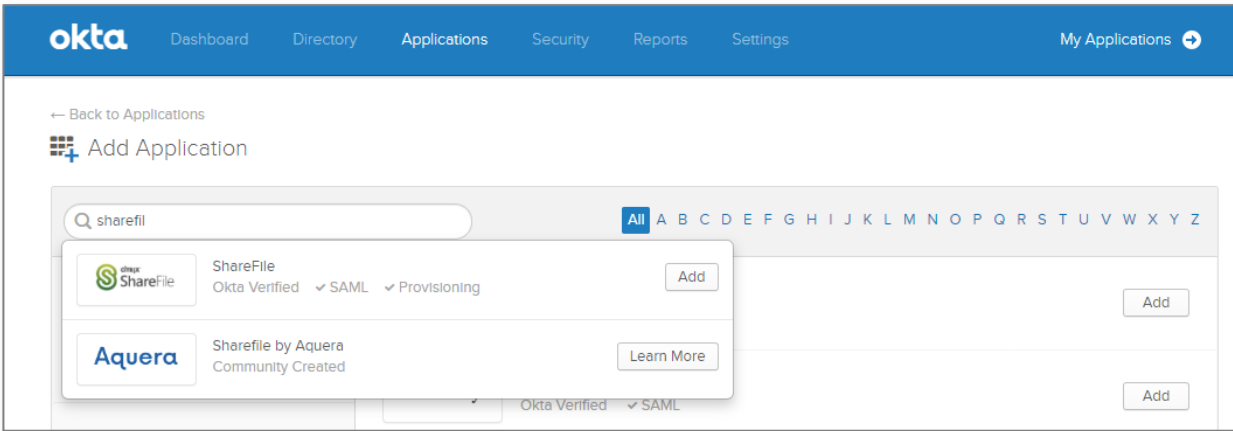


Last Revised: May 2019

LEGAL NOTICE

This document is furnished "AS IS" without warranty of any kind. This document is not supported under any Citrix standard support program. Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix Systems, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc. This document and the software may be used and copied only as agreed upon by the Beta or Technical Preview Agreement.

Copyright © 2019 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Content Collaboration, and ShareFile are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Steps	Description
1.	<p>Log in to the Okta site.</p> <p>For example, login to https://company-admin.okta.com.</p>
2.	<p>Click on Applications, click Add Application.</p>  <p>The screenshot shows the Okta Applications management interface. At the top, there is a navigation bar with 'okta' logo and links for Dashboard, Directory, Applications, Security, Reports, and Settings. Below the navigation bar, there are buttons for 'Add Application' and 'Assign Applications'. A search bar is present with the text 'Search'. On the left, there is a table with columns 'STATUS', 'ACTIVE' (0), and 'INACTIVE' (0). The main content area displays a message: 'No active apps found. Add application and assign access to have them appear on your users! Okta home Page'.</p>
3.	<p>In the Search field, type in ShareFile. Choose Add for the ShareFile SAML app.</p>  <p>The screenshot shows the 'Add Application' page in Okta. The search bar contains 'sharefil'. Below the search bar, there are two search results. The first result is 'ShareFile' by Okta Verified, with options for 'SAML' and 'Provisioning', and an 'Add' button. The second result is 'Sharefile by Aquera' by Community Created, with an 'Add' button. There is also a 'Learn More' button for the Aquera result.</p>
4.	<p>Enter the Base URL as your ShareFile account URL. For example, https://subdomain.sharefile.com</p>

okta Dashboard Directory Applications Security Reports Settings My Applications

Add ShareFile

1 General Settings 2 Sign-On Options

General Settings - Required






Application label	<input type="text" value="ShareFile"/>	General settings All fields are required to add this application unless marked optional.
	<small>This label displays under the app on your home page</small>	
Base URL	<input type="text" value="https://subdomain.sharefile.com"/>	
	<small>Enter Base URL, for example https://org.sharefile.com.</small>	
Application Visibility	<input type="checkbox"/> Do not display application icon to users	
	<input type="checkbox"/> Do not display application icon in the Okta Mobile App	
Browser plugin auto-submit	<input checked="" type="checkbox"/> Automatically log in when user lands on login page	

5.

Choose **SAML 2.0**

← Back to Applications

ShareFile

Active      [View Logs](#)

General **Sign On** Provisioning Import Assignments Push Groups

Settings Cancel

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.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

 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.


Secure Web Authentication

CREDENTIALS DETAILS

Application username format

Update application username on

Password reveal Allow users to securely see their password (Recommended)

 Password reveal is disabled, since this app is using SAML with no password.

[Save](#)

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

You can sync passwords to this app

If you enable provisioning and password push, you can automatically synchronize Okta passwords to ShareFile.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

6. Click on **View Setup Instructions** for specific URLs to configure your ShareFile account.

Settings
Cancel

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.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

☰

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.

Secure Web Authentication

7. **Setup instructions URL (Okta authenticated):** https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-ShareFile.html?baseAdminUrl=https://company-admin.okta.com&app=sharefile&instanceId=0opg2v8wYOUgWM48E356
- Setup instructions URL (Not authenticated):** https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-ShareFile.html

How to Configure SAML 2.0 for ShareFile

Contents

- [Supported Features](#)
- [Configuration Steps](#)
- [Notes](#)

Supported Features

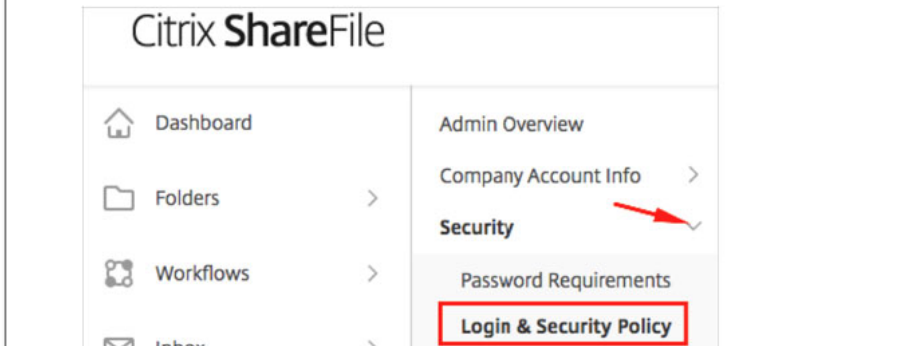
The Okta/ShareFile SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO

For more information on the listed features, visit the [Okta Glossary](#).

Configuration Steps

- 1 Sign into your ShareFile account.
- 2 Navigate to **Settings > Admin Setting > Security > Login & Security Policy**:



Use these settings to configure your ShareFile account.

8. Go to your ShareFile account: <https://subdomain.sharefile.com> > Login with Administrator account > **Settings > Admin Settings > Security > Login & Security Policy** > scroll down on this page to **Single sign on / SAML 2.0 Configuration**.

Use OKTA Setup instructions to configure **Single sign on / SAML 2.0 Configuration:**

Basic Settings

- **Enable SAML:** Select **Yes**
- **ShareFile Issuer / Entity ID:** Leave default value. Make a copy of this value (i.e. *subdomain.sharefile.com*) to validate Okta has the same Entity ID
- **Your Issuer / Entity ID:** Copy and paste from Okta Setup Instructions
- **X.509 Certificate:** Click **Change**, then copy and paste the certificate from Okta Setup instructions:

- **X.509 Certificate:** Click **Change**, then copy and paste the following:

```
-----BEGIN CERTIFICATE-----
MIIDeDCCApigAwIBAgIGANh4xIgsMA0GCSqGSIb3DQEBCwUAMIGYMQswCQYDVQQGEwJVUzETMBEG
A1UECAwRQ2FsaWZvcmlkZm91b250YXN0aW50YXN0aW50YXN0aW50YXN0aW50YXN0aW50YXN0aW50
MBIGA1UECwwLU1NPUHJvdmlkZm91b250YXN0aW50YXN0aW50YXN0aW50YXN0aW50YXN0aW50YXN0
9w0BCQEWLW1uZm9Ab2t0YS5jb20wHhcNMjkwNDA3MTcwNjAzWWhcMjkwNDA3MTcwNzAzWjCB
MAwGA1UEBhMCVVMxZzARBgNVBAglCidThbG1mb3JuaWEuZm91b250YXN0aW50YXN0aW50YXN0aW50
DjALBgNVBAMcZm91b250YXN0aW50YXN0aW50YXN0aW50YXN0aW50YXN0aW50YXN0aW50YXN0aW50
-----END CERTIFICATE-----
```

- **Login URL:** Copy and paste from Okta Setup Instructions (i.e. <https://domain.okta.com>)
- **Logout URL:** Leave blank is recommended (When users log out of ShareFile, they will be redirected to ShareFile login page <https://subdomain.sharefile.com>.)

Basic Settings

Enable SAML: ?

Yes No

ShareFile Issuer / Entity ID: ?

subdomain.sharefile.com

Your IDP Issuer / Entity ID: ?

http://www.okta.com/yours1v8wkXtyu6no73!

X.509 Certificate: ?

Saved [Change](#)

Login URL: ?

https://domain.okta.com/app/sharefile/yours:

Logout URL: ?

9.

Optional Settings

- **Require SSO Login:** *Optional*

After single-sign-on is successfully validated, checking **Yes** for this option will require all non-admin Employees to log in using Okta.

Admins will have the choice to login using Okta (on the left) or their email address as the username and a native ShareFile password (on the right).

- **SSO IP Range:** *Optional*

(Limit requiring non-admin Employees to login from a specific IP range. Employees outside of this specified range will not be required to use Okta to login.)

- **SP-initiated SSO Certificate:** Select **HTTP Redirect with no signature**

- **Enable Web Authentication:** **Yes** (Choose **No** when you do not want to allow logins via a web browser. This means Windows authentication will need to be available).

- **SP-initiated Auth Context:** Select **Password Protected Transport**.

- **Active Profile Cookies:** Leave blank

○ Click **Save**

Optional Settings

Require SSO Login: (?)

Yes No

SSO IP Range: (?)

SP-Initiated SSO certificate: (?)

HTTP Redirect with no signature ▾

Enable Web Authentication: (?)

Yes No

SP-Initiated Auth Context: (?)

Password Protected Transport ▾

Minimum ▾

Active Profile Cookies: (?)

Save

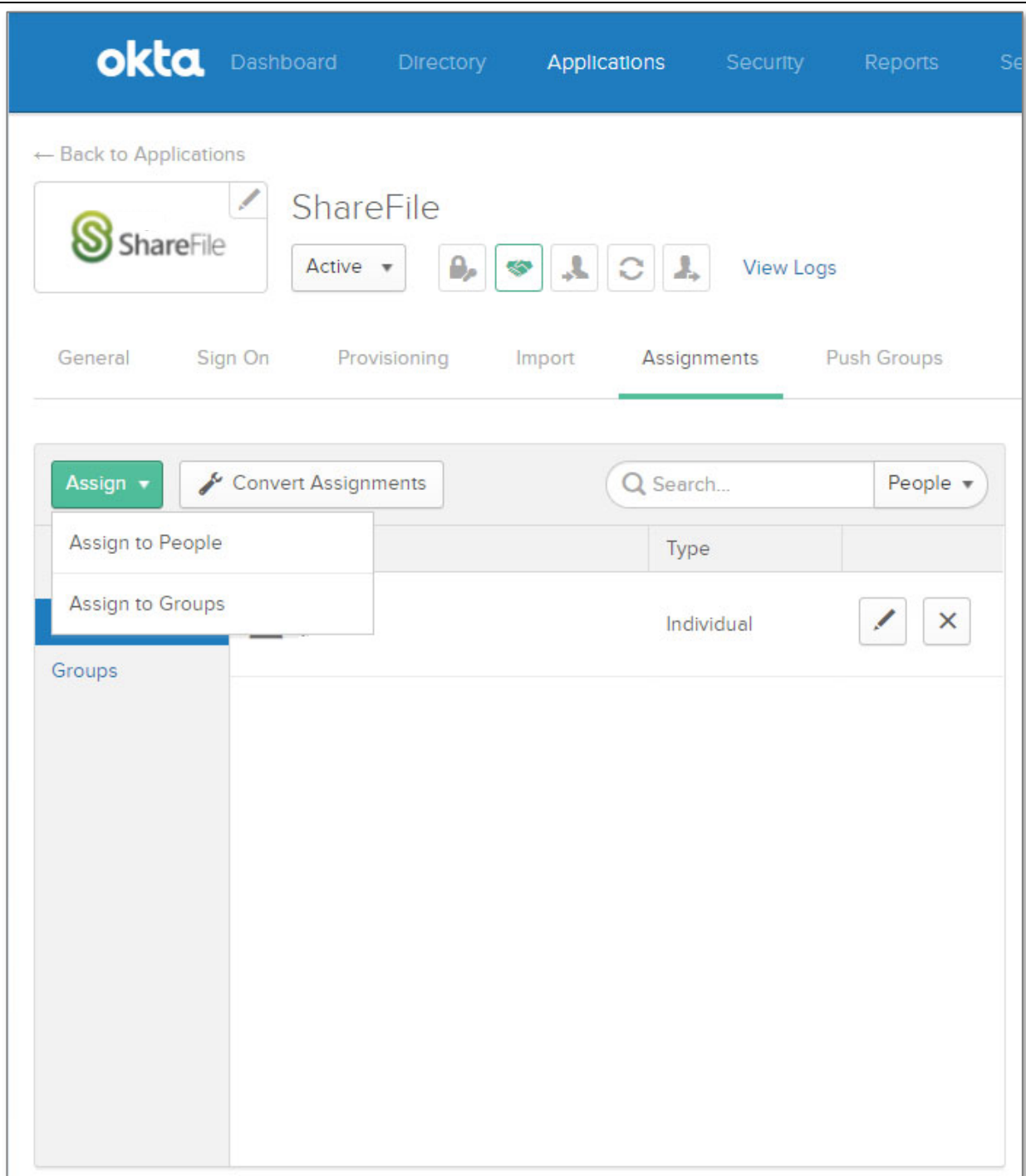
Cancel

10. In Okta, select the **General** tab for the ShareFile app, then click **Edit**.

Confirm the base URL of your **ShareFile Issuer/Entity ID** is value you made a copy of in **ShareFile Single Sign on** settings into the **Base URL** field. For example:

<https://subdomain.sharefile.com>

11. In Okta, select the **Assignments** tab in the ShareFile application, click on the **Assign** and **Assign to People** or **Assign to Groups** to authorize these users to sign via Okta into ShareFile.



12. Test successful authentication by going to your ShareFile URL:
<https://subdomain.sharefile.com>

***Testing single-sign-on logins in private/incognito browser mode is best.*

Click **Sign in** under **Company Employee Sign In**

Citrix ShareFile

Company Employee Sign In

ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials.

Sign In

Sign In

Email


Password



Sign In

Remember Me [Forgot Password?](#)

****Make sure the user logging in with single sign-on has an Active Directory or Identity Provider email address that matches their email address in their ShareFile account.**

Sign in will redirect you Okta for sign in:

Connecting to  ShareFile

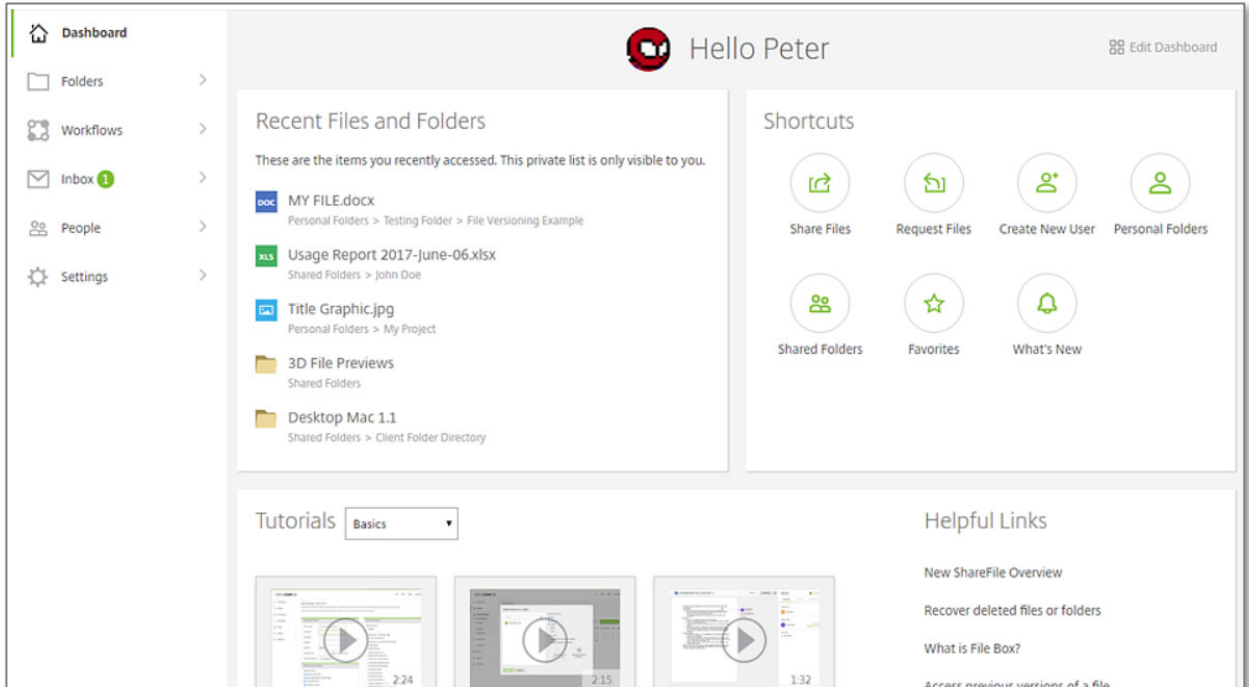


Sign In

Remember me

Sign In

Need help signing in?

Successful logins will authenticate users into their ShareFile account **Dashboard**.



13.

Done!