

Content Collaboration: Single Sign-On Configuration Guide

OneLogin

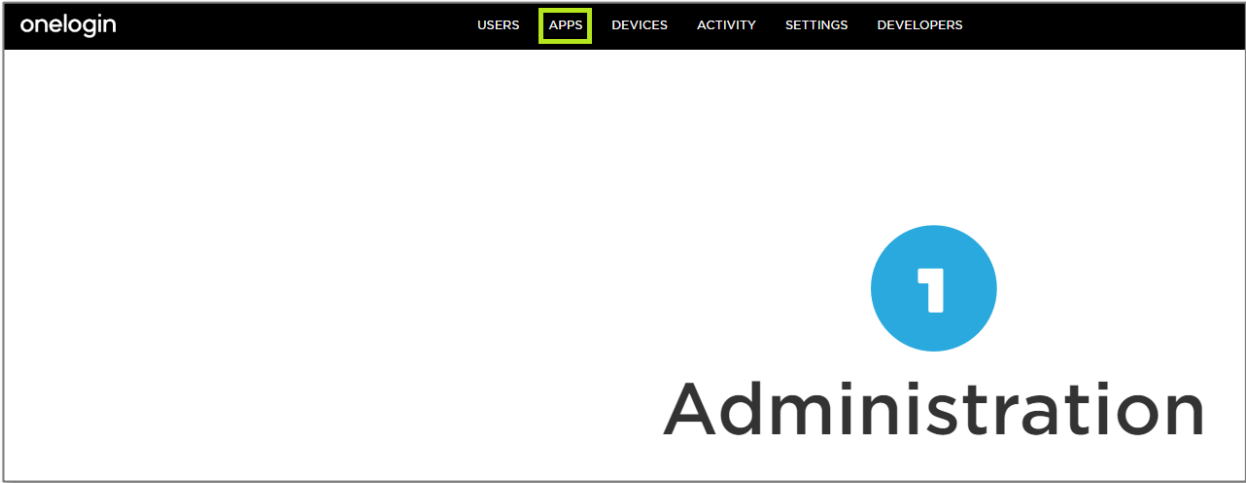
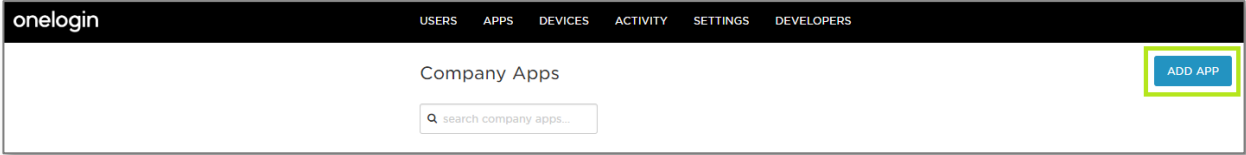
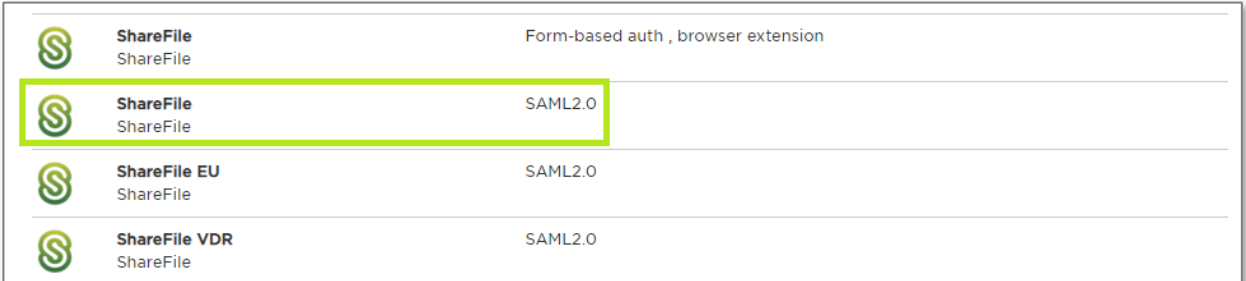














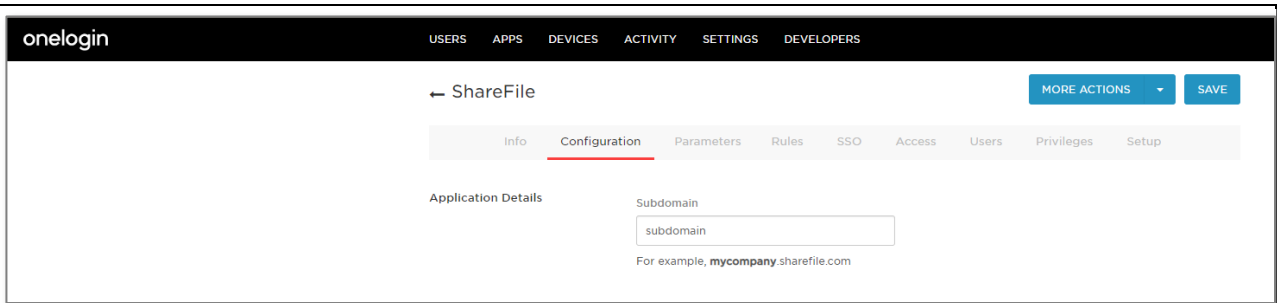
Last Revised: May 2019

LEGAL NOTICE

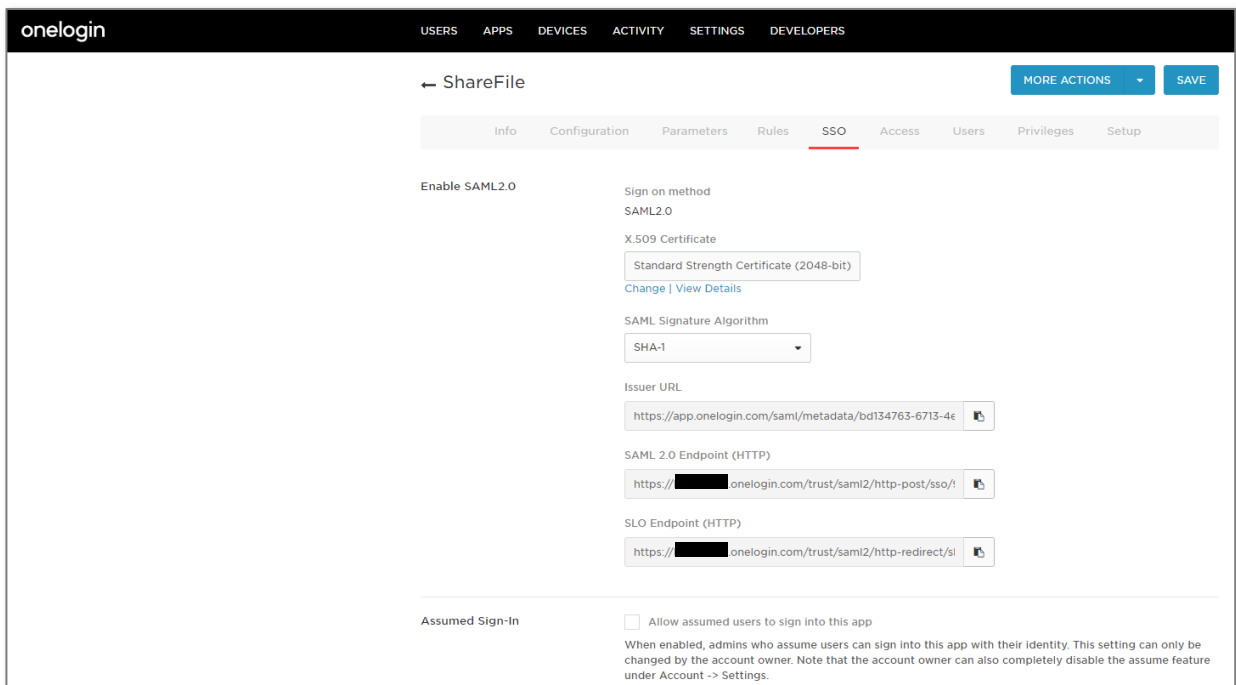
This document is furnished "AS IS" without warranty of any kind. This document is not supported under any Citrix standard support program. Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness 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.

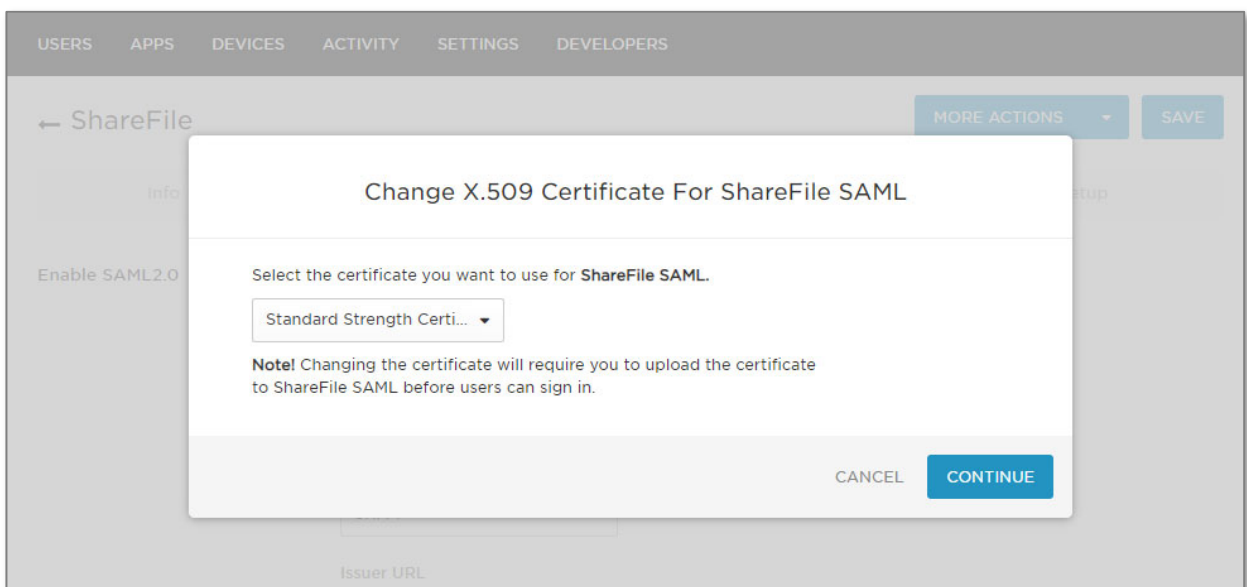
Steps	Description												
1.	<p>Log in to the OneLogin Administrator site.</p> <p>For example, login to https://company.onelogin.com/admin</p>												
2.	<p>Click on Apps.</p> 												
3.	<p>Click on Add App.</p> 												
4.	<p>Search or select File sharing > ShareFile SAML 2.0</p>  <table border="1"> <tbody> <tr> <td></td> <td>ShareFile ShareFile</td> <td>Form-based auth , browser extension</td> </tr> <tr> <td></td> <td>ShareFile ShareFile</td> <td>SAML2.0</td> </tr> <tr> <td></td> <td>ShareFile EU ShareFile</td> <td>SAML2.0</td> </tr> <tr> <td></td> <td>ShareFile VDR ShareFile</td> <td>SAML2.0</td> </tr> </tbody> </table>		ShareFile ShareFile	Form-based auth , browser extension		ShareFile ShareFile	SAML2.0		ShareFile EU ShareFile	SAML2.0		ShareFile VDR ShareFile	SAML2.0
	ShareFile ShareFile	Form-based auth , browser extension											
	ShareFile ShareFile	SAML2.0											
	ShareFile EU ShareFile	SAML2.0											
	ShareFile VDR ShareFile	SAML2.0											
5.	<p>On Configuration tab, enter ShareFile subdomain in Application Details.</p>												



6. Click on SSO tab to enable SAML2.0.



7. On X.509 Certificate, click Change. Select the Standard Strength Certificate (2048-bit).



8. On **SAML Signature Algorithm**, select **SHA-256**.

The screenshot shows the 'ShareFile' configuration page in the 'SSO' tab. The 'SAML Signature Algorithm' dropdown menu is open, displaying options: SHA-1, SHA-256 (highlighted), SHA-384, and SHA-512. Other visible settings include 'Enable SAML2.0', 'Sign on method: SAML2.0', 'X.509 Certificate: Standard Strength Certificate (2048-bit)', and 'Assumed Sign-In'.

9. Click **More Actions**, in the drop down menu choose, download **SAML Metadata**.

The screenshot shows the 'ShareFile' configuration page with the 'More Actions' dropdown menu open. The menu options are: Vendor Homepage, Reapply entitlement mappings, SAML Metadata (highlighted), and Delete. The 'SAML Signature Algorithm' is set to SHA-256, and the 'Issuer URL' is https://app.onelogin.com/saml/metadata/bd134763-6713-4e.

10. Open the **onelogin_metadata.xml** file with Notepad or a text editor. Be ready to copy the text from the X509Certificate section:

```

1  <?xml version="1.0"?>
2  <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
   https://app.onelogin.com/saml/metadata/bd134763-6713-4e8f-90c6-e166ca2ec273">
3  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
   "urn:oasis:names:tc:SAML:2.0:protocol">
4  <KeyDescriptor use="signing">
5  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
6  <ds:X509Data>
7  <ds:X509Certificate>MIID5TCCAs2gAwIBAgIUUV05SawyJOp1FX/xUvEkZRK9oM/cwDQYJKoZIhvcNAQEF
8  BQAwSDEtMBEgA1UECgwKaG1ldHRjbG91ZDEVMBMGA1UECwwMT251TG9naW4gSWRQ
9  MR0GAYDVBQDDBFBmVmb2dpbiBBY2NvdW50IDAeFw0xOTA0MDcxNzE5NDNaFw0y
10 NDA0MDcxNzE5NDNaMEgxEzARBGNVBAoMcmhpZXR0Y2xvdWQxFTATBgNVBAsMDE9u
11 ZUxvZ21uIElkUDEaMBGGA1UEAwRT251TG9naW4gQWNjb3VudCAwggEiMA0GCScqG
12 Sib3DQEBBAQUAA4IBDwAwggEKAoIBAQCzYRtO2Zmc6ZcSZ21Wc9Basq3YRNIesZHg
13 WGe722KX00XToSEW/M/pvdcNKgV8oNYTmj0B5rFysVgNd08KFZBmHUJ+WWD1p3GF
14 9KCNwJwwEd3hkYQpHHERBQLCMY7UGwGtSFw2iHbL2BL2ScOVozL5Y9sPrnYuMOHi
15 aITELz808I7iE3Bg1/z1GhSGMzxr3IUqE00kCVy2jaHVP7vwLDN1b5kq96MYjGM
16 u03n1Jhs4a5IIFyQUOB3MPm4QNbPkIT7f6Yb27jGrVAzraoa8FL7ZpLw6W08XNvA
17 zrgvB1bwcF7pF9qEgtGTwg491GehVfndNFM7kP43bnd2RoePTc1tAgMBAAGjgcYw
18 gcMwDAYDVDR0TAQH/BAIwADAdBgNVHQ4EFgQUJAchzi3Jc46v5+aT/9DMfAnWF6Ew
19 gYMGAL1UdIwR8MHqAFcQHIC4tyXOOr+fmk//QzHwLlhehoUykSjBIMRMwEQYDVQK
20 DApoaWV0dGNsb3VkmRUwEwYDVQQLDAXPbmVmb2dpbiBJZFAxGjAYBgNVBAMMEU9u
21 ZUxvZ21uIEIEFjY291bnQgghRXt1JrDik6mUVf/FS8SR1Er2gz9zAOBgNVHQ8BAf8E
22 BAMCB4AwDQYJKoZIhvcNAQEFBQADggEBAEg2E6oyTThFvF16j2CJpF62xSWFrqdN
23 M72STJ1K7IwR60McuXzgz2bGI8T+7o17qbMxpKC5jS2qIaoMysggS/RSNyfK6fUQss
24 nknkc1ohAcWhBC+fTmlJnYux2A9MZKBBVYOxCpTRZVNHfM776Vbz1D6dCtA5QEYm
25 rVDNOS9ob1UzaFZhKG7Gr4qmwWGkc/nV622eAtLRUeQoByeJravUEIgg9awCVA/+
26 Yq4bBN5MhxxMYIMCzfdN4E+i1SwiGczXmsGAKEnrqgXu5n0/a76VqHeYUDon20gU
27 c+Pn3XFfomvDzBjC7B/31vJlx8frNGquw9TBckSGnkqgSojv5yyz1w=</ds:X509Certificate>
28 </ds:X509Data>
29 </ds:KeyInfo>
30 </KeyDescriptor>
31 <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
   https://subdomain.onelogin.com/trust/saml2/http-redirect/slo/924109"/>
32
33 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
34
35 <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
   https://subdomain.onelogin.com/trust/saml2/http-redirect/sso/924109"/>
36 <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=
   "https://subdomain.onelogin.com/trust/saml2/http-post/sso/924109"/>
37 <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location=
   "https://subdomain.onelogin.com/trust/saml2/soap/sso/924109"/>
38 </IDPSSODescriptor>
39 </EntityDescriptor>

```

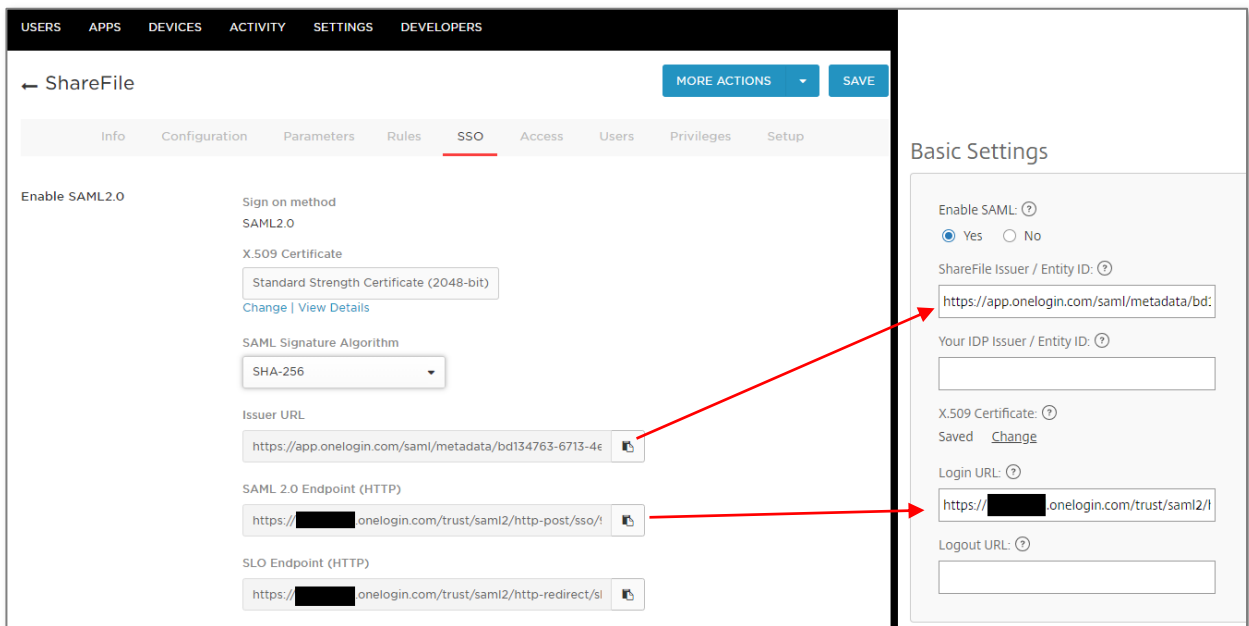
11. Go to your ShareFile account: <https://subdomain.sharefile.com> > Login with Administrator account > **Settings > Admin Settings > Security > Login & Security Policy** > scroll down on this page to **Single sign on / SAML 2.0 Configuration**.

12. Configure **Single sign on / SAML 2.0 Configuration** with the below:

Basic Settings

- **Enable SAML:** Select **Yes**
- **ShareFile Issuer / Entity ID:** Copy to clipboard the **Issuer URL** from One Login and paste
- **Your Issuer / Entity ID:** Leave blank

- **X.509 Certificate:** Click **Change**, then copy and paste the certificate from the **onelogin_metadata.xml** file from the step above
- **Login URL:** Copy to clipboard the **SAML 2.0 Endpoint (HTTP)** from OneLogin and paste
- **Logout URL:** Leave blank
(When users log out of ShareFile, they will be redirected to ShareFile login page <https://subdomain.sharefile.com>.)



13.

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 OneLogin. Admins can login using OneLogin or email address and their ShareFile password.)
- **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 OneLogin 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 single sign on logins via a web browser. This means Windows authentication

will need to be available. **No** is not recommended).

- **SP-initiated Auth Context:** Select **User Name and Password**.
- **Active Profile Cookies:** Leave blank
- Click **Save**

Optional Settings

Require SSO Login: (?)
 Yes No

SSO IP Range: (?)

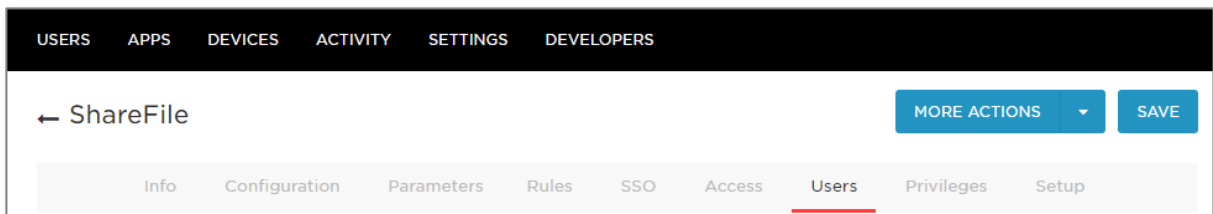
SP-Initiated SSO certificate: (?)

Enable Web Authentication: (?)
 Yes No

SP-Initiated Auth Context: (?)

Active Profile Cookies: (?)

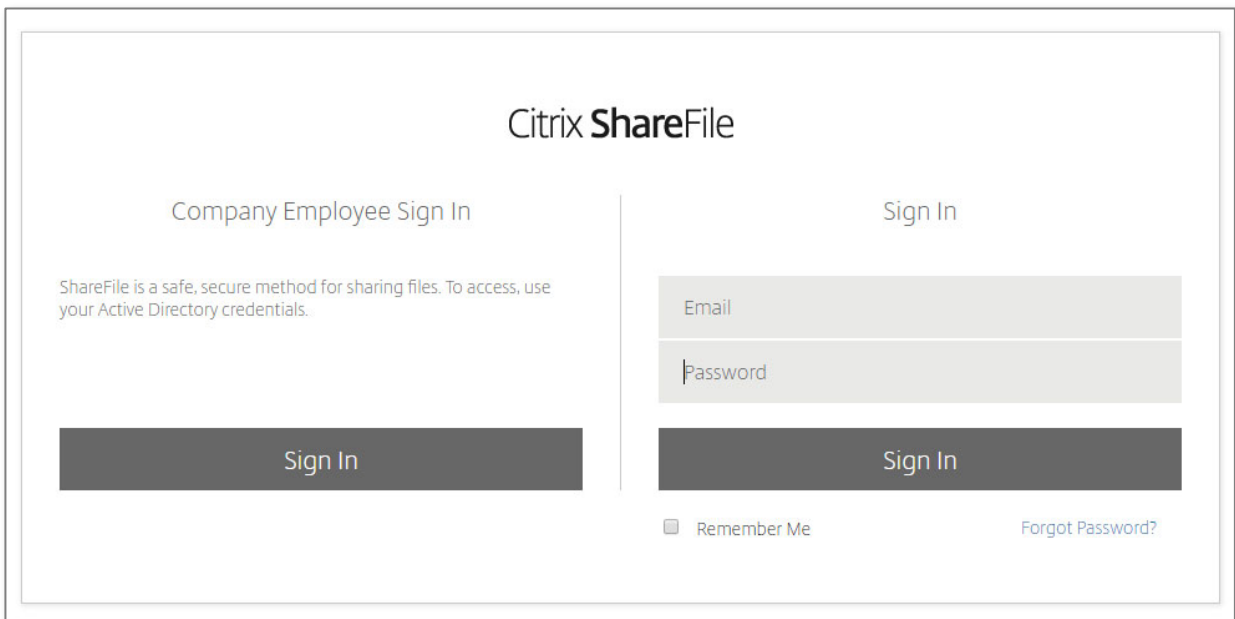
14. Make sure **Users** are authorized to use this app.



15. 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

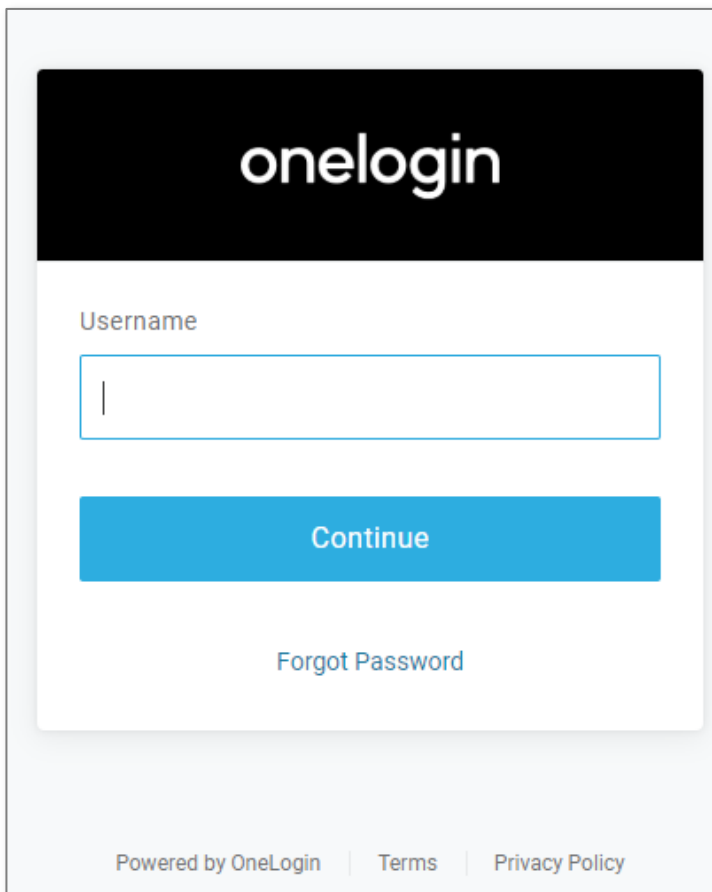
Sign In

Remember Me [Forgot Password?](#)

The image shows the Citrix ShareFile login interface. It is divided into two main sections. The left section is titled 'Company Employee Sign In' and contains a descriptive paragraph about the security of the service and a 'Sign In' button. The right section is titled 'Sign In' and contains input fields for 'Email' and 'Password', followed by a 'Sign In' button. Below the 'Sign In' button on the right are two links: 'Remember Me' with a checkbox and '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 OneLogin for sign in:



onelogin

Username

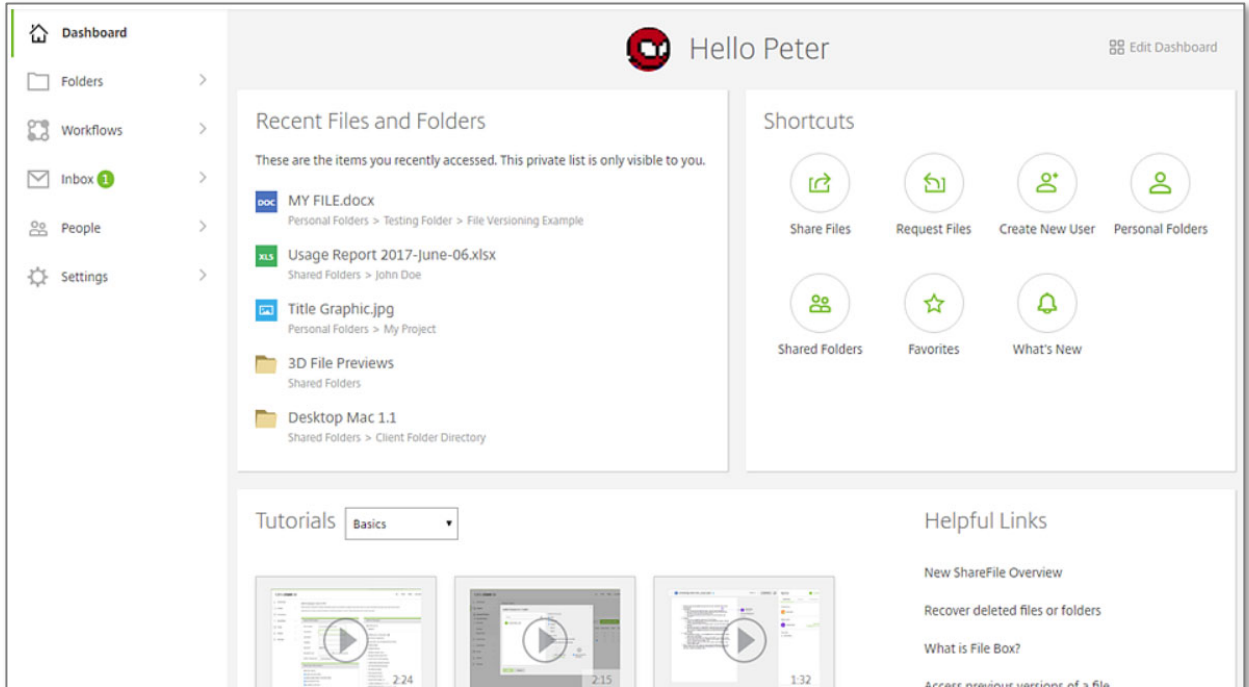
Continue

[Forgot Password](#)

Powered by OneLogin | [Terms](#) | [Privacy Policy](#)

The image shows the OneLogin sign-in page. It features a black header with the 'onelogin' logo in white. Below the header is a white form area with a 'Username' label and a text input field. A blue 'Continue' button is positioned below the input field. At the bottom of the form area is a blue link for 'Forgot Password'. The footer of the page contains the text 'Powered by OneLogin' followed by links for 'Terms' and 'Privacy Policy'.

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



16.

Done!