



Content Collaboration: Single Sign-On Configuration Guide

OneLogin

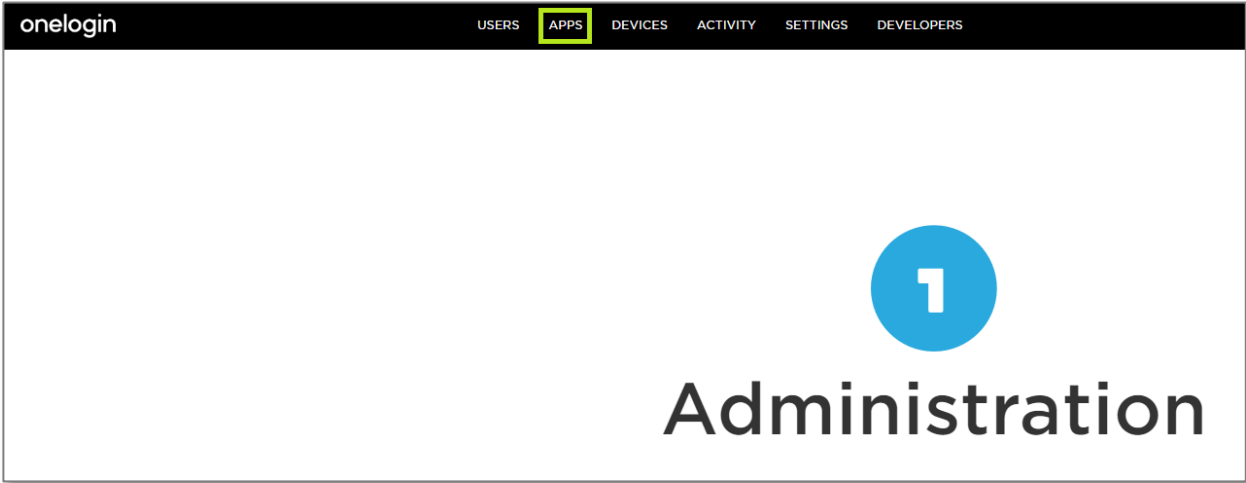
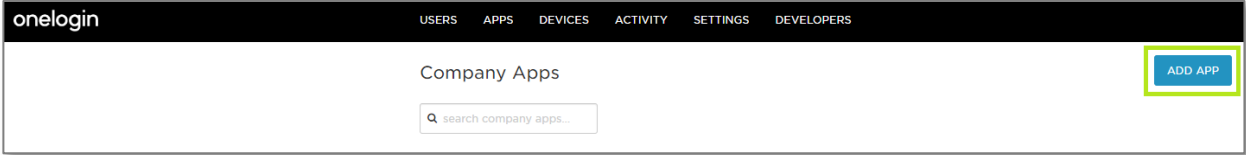
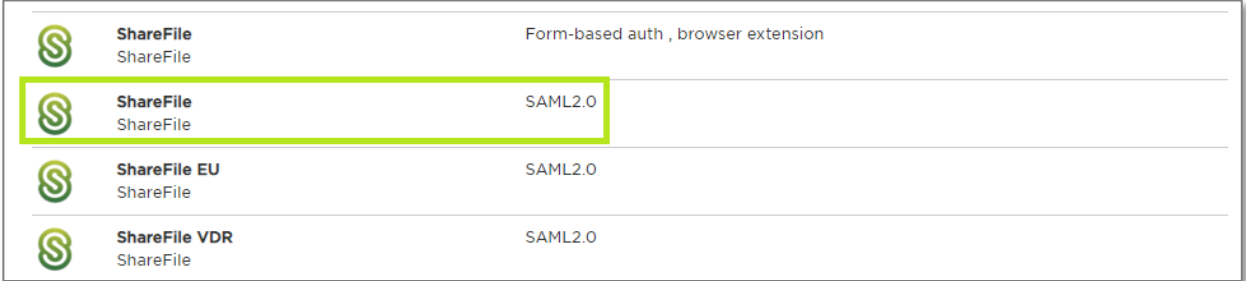


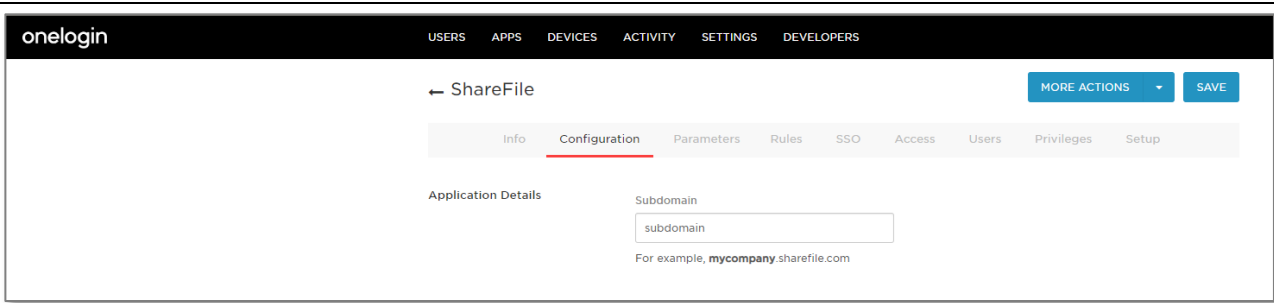
Last Revised: May 2019

LEGAL NOTICE

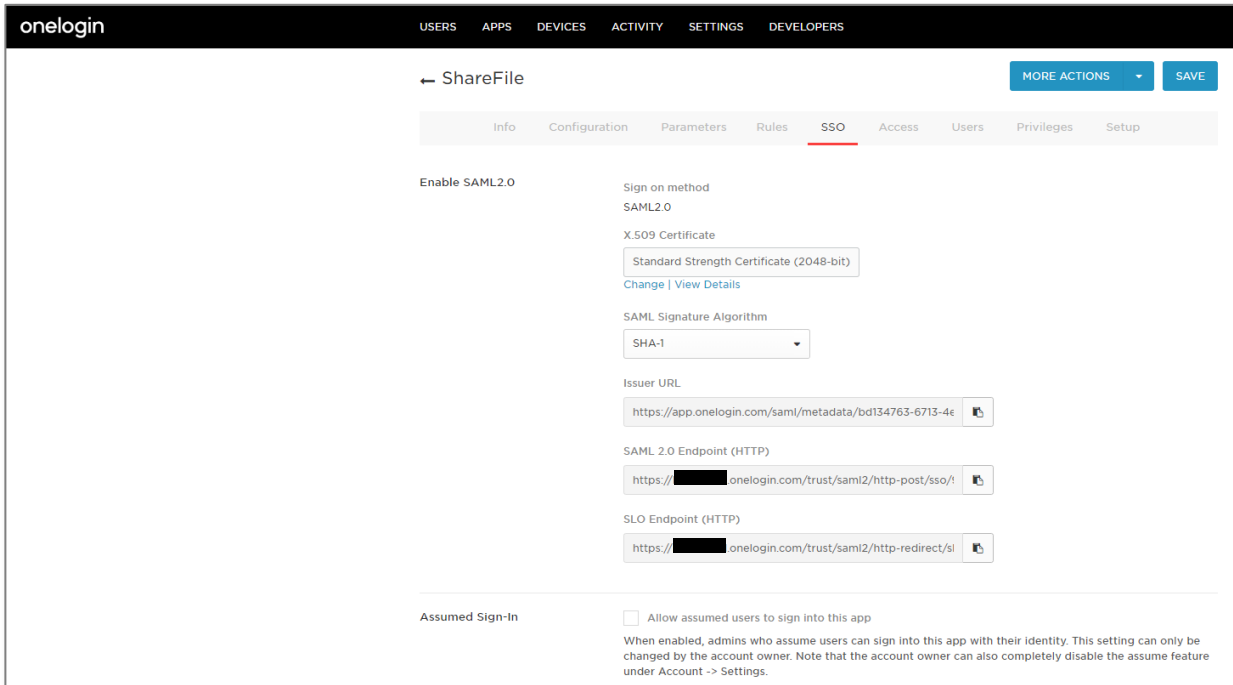
This document is furnished "AS IS" without warranty of any kind. This document is not supported under any Citrix standard support program. Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness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

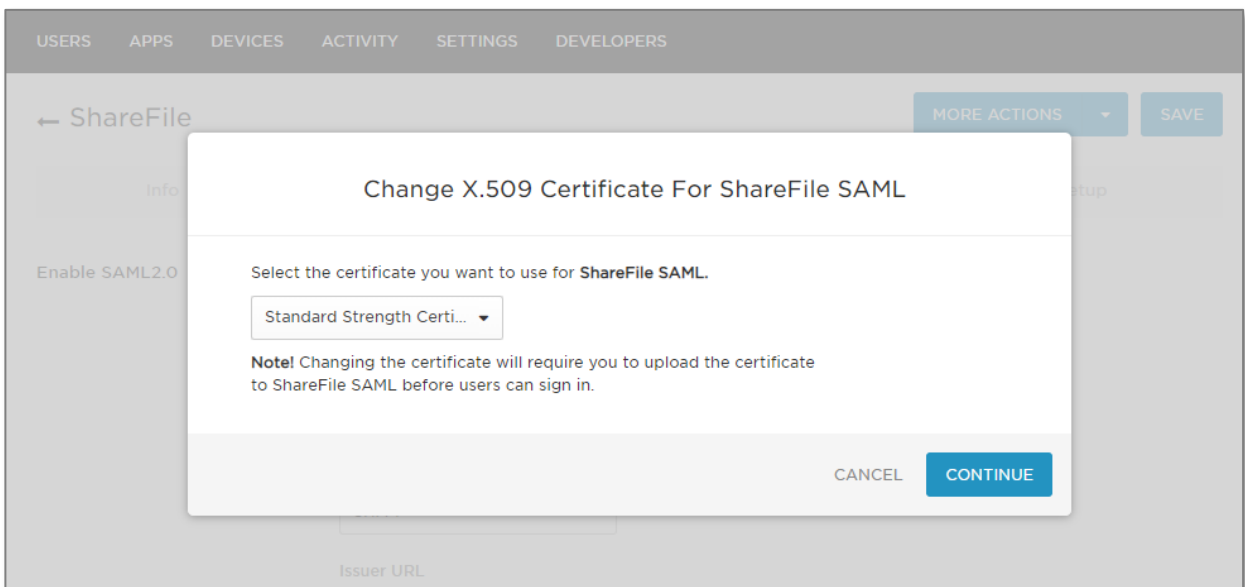
Steps	Description
1.	<p>Log in to the OneLogin Administrator site.</p> <p>For example, login to https://company.onelogin.com/admin</p>
2.	<p>Click on Apps.</p> 
3.	<p>Click on Add App.</p> 
4.	<p>Search or select File sharing > ShareFile SAML 2.0</p> 
5.	<p>On Configuration tab, enter ShareFile subdomain 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 items 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="
3  https://app.onelogin.com/saml/metadata/bd134763-6713-4e8f-90c6-e166ca2ec273">
4  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
5  "urn:oasis:names:tc:SAML:2.0:protocol">
6  <KeyDescriptor use="signing">
7  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
8  <ds:X509Data>
9  <ds:X509Certificate>MIID5TCCAs2gAwIBAgIUUV05SawyJOp1FX/xUvEkZRK9oM/cwDQYJKoZIhvcNAQEF
10 BQAwSDEtMBEGA1UECgwKaG1ldHRjbG91ZDEVMBMGA1UECwwMT251TG9naW4gSWRQ
11 MR0wGAYDVQDDBFBmVmb2dpbiBBY2NvdW50IDAEFw0xOTA0MDcxNzE5NDNaFw0y
12 NDA0MDcxNzE5NDNaMEgxEzARBGNVBAoMcmhpZXROy2xvdlWQxFTATBgNVBAsMDE9u
13 ZUxvZ21uIElkUDEaMBGGA1UEAwwRT251TG9naW4gQWNjb3VudCAwggEiMA0GCScqG
14 Sib3DQEBAQUAA4IBDwAwggEKAoIBAQCzYRtO2Zmc6ZcSZ21Wc9Basq3YRNIesZHg
15 WGe722KX00XToSEW/M/pvdcNKgV8oNYTmj0B5rFysVgNd08KFZBmHUJ+WWD1p3GF
16 9KCNwJwwEd3hkYQpHHErEQLCMY7UGwGtSFw2iHbL2BL2ScOVOzL5Y9sPrnYuMOHi
17 aITELz808I7iE3Bg1/z1GhSGMzxr3IUqE00kCVy2jaHVP7vwLDN1b5kq96MYjGM
18 u03n1Jhs4a5IIFyQUOB3MPm4QNbPkIT7f6Yb27jGrVAzraoa8FL7ZpLw6W08XNvA
19 zrgvB1bwcF7pF9qEgtGTwg491GehVfndNFM7kP43bnd2RoePTc1tAgMBAAGjgcYw
20 gcMwDAYDVROTAQH/BAIwADAdBgNVHQ4EFggQUJAchzi3Jc46v5+aT/9DMfAnWF6Ew
21 gYMGA1UdIw8MHqAFQCQHIc4tyXOOr+fmk//QzHwL1hehoUykSjBIMRMwEQYDVQQK
22 DApoaWV0dGNsb3VkmRUwEwYDVQQLDAXPbmVmb2dpbiBJZFAxGjAYBgNVBAMMEU9u
23 ZUxvZ21uIEIEFjY291bnQgghRXT1JrDik6mUVF/FS8SR1Er2gz9zAOBgNVHQ8BAf8E
24 BAMCB4AwDQYJKoZIhvcNAQEFBQADggEBAEg2E6oyTThFvF16j2CJpF62xSWFrqdN
25 M72STJ1K7Nu60Mcuxzgz2bGI8T+7o17qbMxpKC5jS2qIaoMysggS/RSNyfK6fUQss
26 nknkc1ohAcWhBC+fTmlJnYux2A9MZKBEVYOxCpTRZVNHfM776Vbz1D6dCtA5QEYm
27 rVDNOS9ob1UzaFZhKG7Gr4qmwWGkc/nV622eAtLRUeQoByeJravUEIgg9awCVA/+
28 Yq4bBN5MnHxxMYIMCzfdN4E+11SwiGczXmsGAKEnrgqxu5n0/a76VgHeYUDon20gU
29 c+Pn3XfIomvDzBjC7B/31vJlx8frNGquw9TBckSGnkqgSojv5yzz1w=</ds:X509Certificate>
30 </ds:X509Data>
31 </ds:KeyInfo>
32 </KeyDescriptor>
33 <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
34 https://subdomain.onelogin.com/trust/saml2/http-redirect/slo/924109"/>
35 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
36 <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
37 https://subdomain.onelogin.com/trust/saml2/http-redirect/sso/924109"/>
38 <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=
39 "https://subdomain.onelogin.com/trust/saml2/http-post/sso/924109"/>
40 <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location=
41 "https://subdomain.onelogin.com/trust/saml2/soap/sso/924109"/>
42 </IDPSSODescriptor>
43 </EntityDescriptor>

```

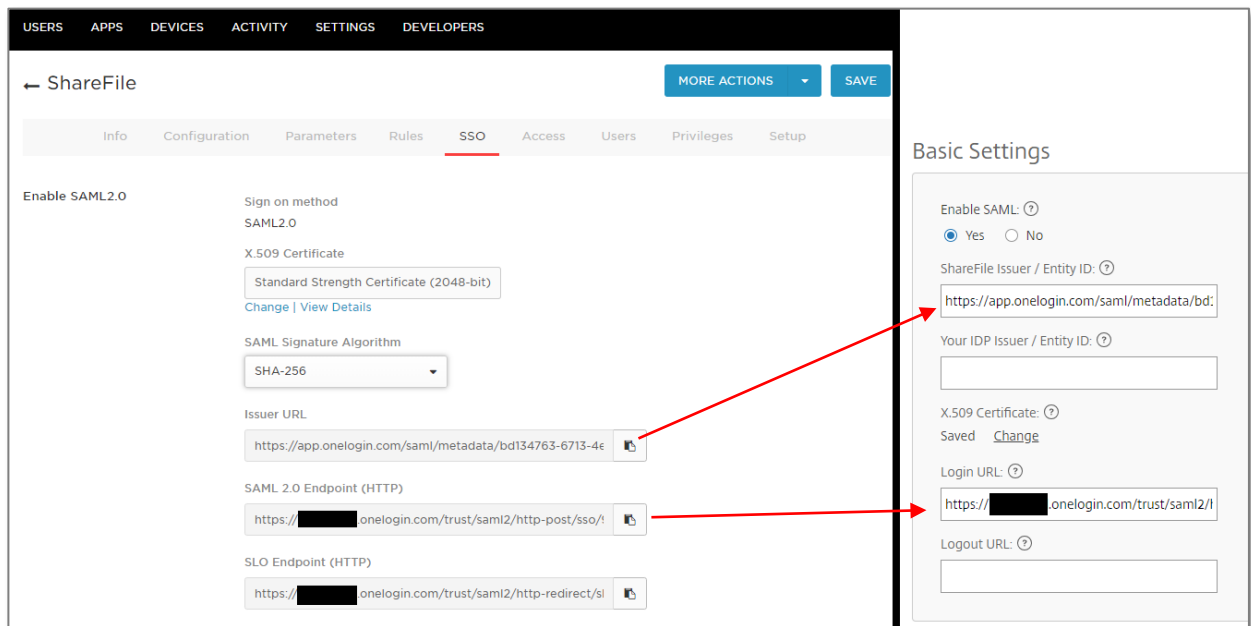
11. Go to your ShareFile account: <https://subdomain.sharefile.com> > Login with Administrator account > **Settings > Admin Settings > Security > Login & Security Policy** > scroll down on this page to **Single sign on / SAML 2.0 Configuration**.

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: (?)

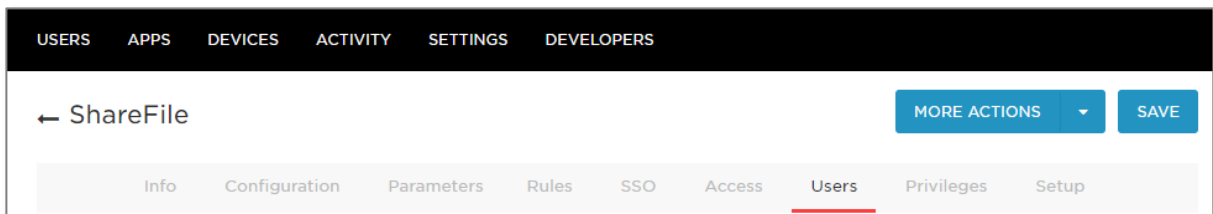
SP-Initiated SSO certificate: (?)

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

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 OneLogin for sign in:



onelogin

Username

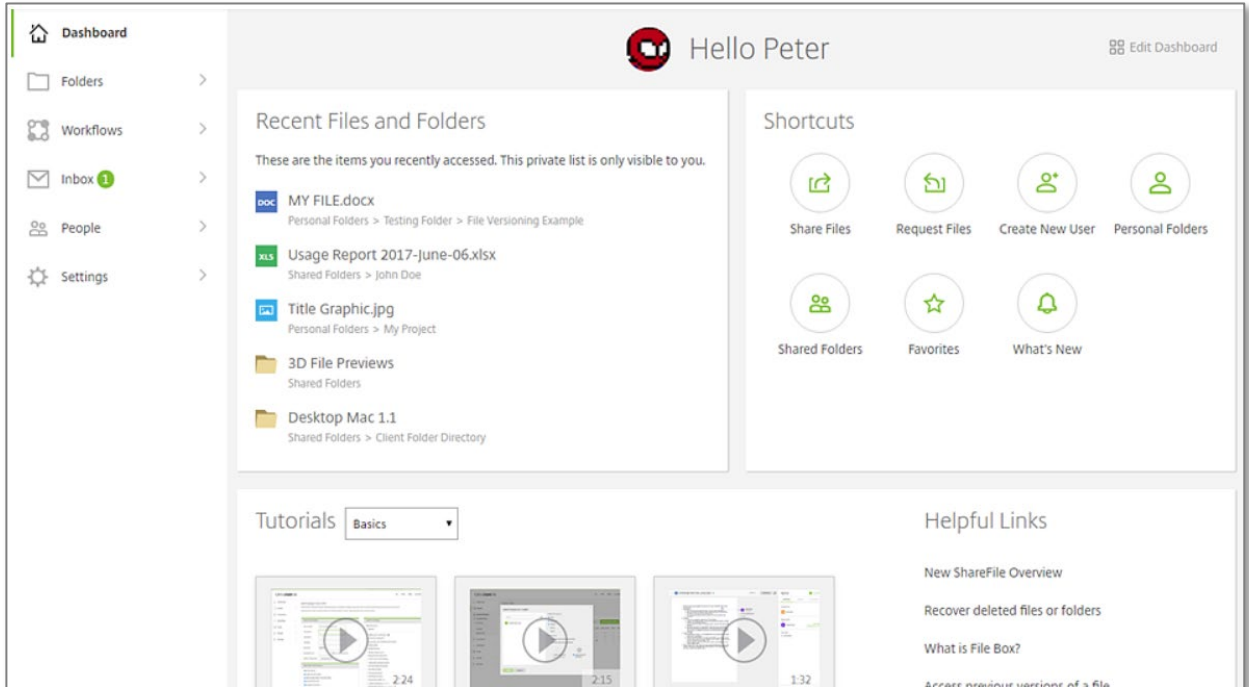
|

Continue

[Forgot Password](#)

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

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



16.

Done!