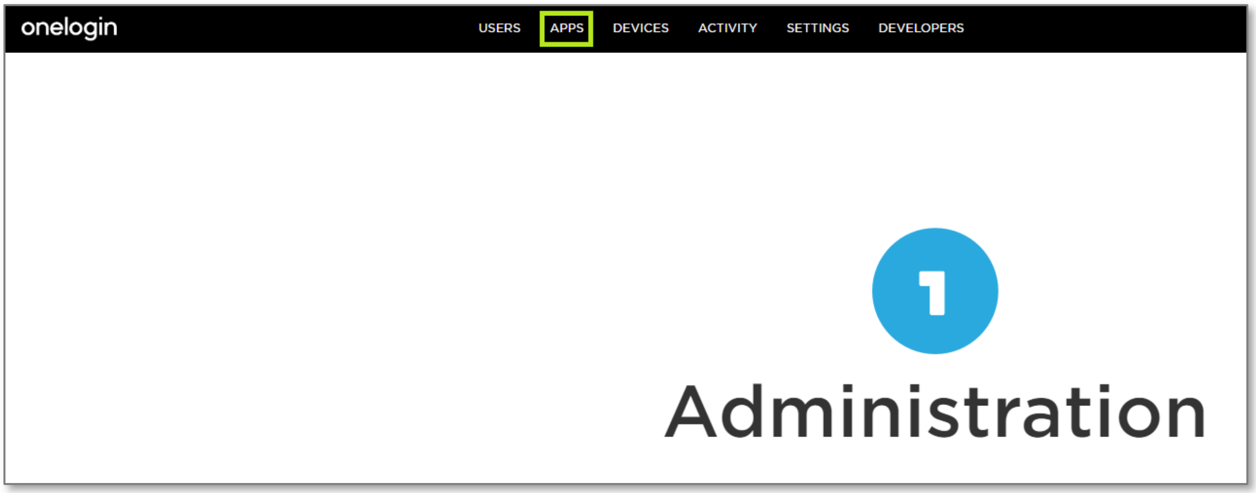
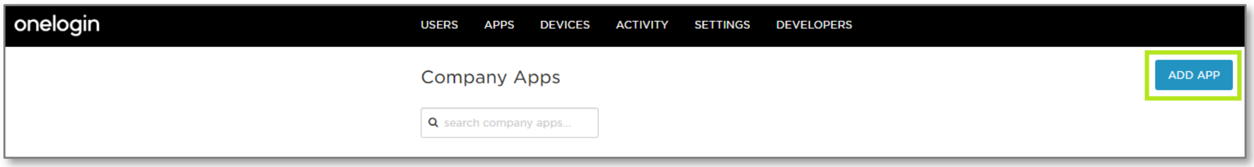
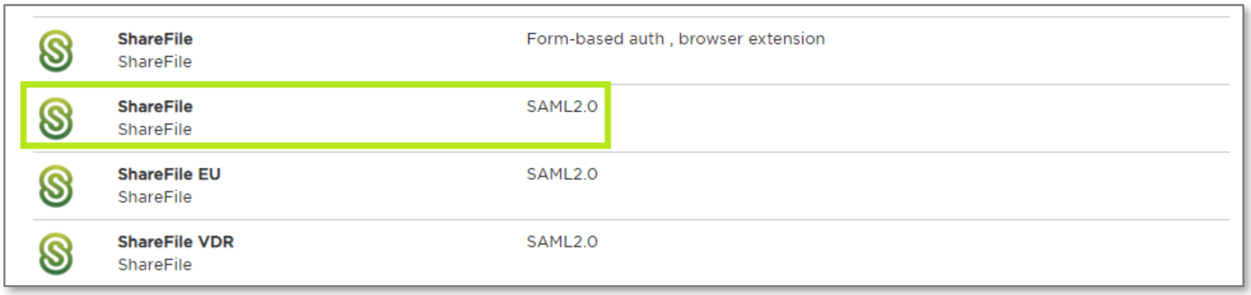
Content Collaboration: Single Sign-On Configuration Guide

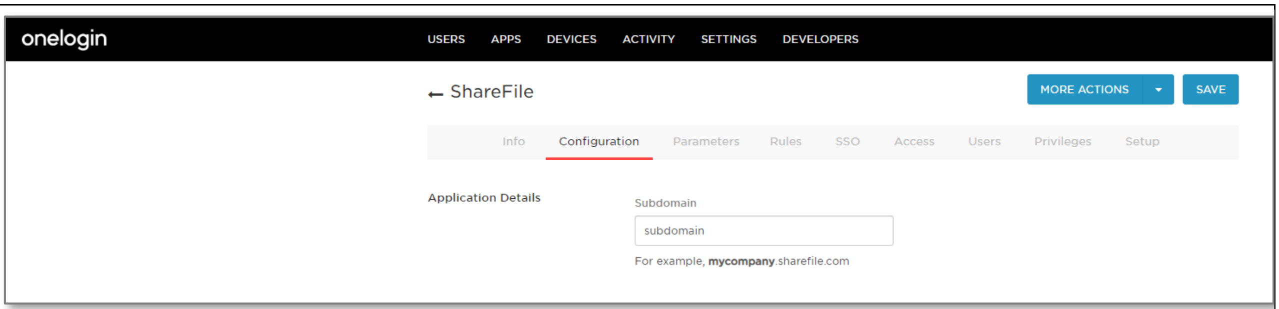
OneLogin

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.

Steps	Description
1.	Log in to the OneLogin Administrator site. For example, login to https://company.onelogin.com/admin
2.	Click on **Apps.**  onelogin USERS APPS DEVICES ACTIVITY SETTINGS DEVELOPERS 1 Administration
3.	Click on **Add App**.  onelogin USERS APPS DEVICES ACTIVITY SETTINGS DEVELOPERS Company Apps search company apps... ADD APP
4.	Search or select **File sharing** > **ShareFile SAML 2.0**  **ShareFile** ShareFile — Form-based auth , browser extension **ShareFile** ShareFile — SAML2.0 **ShareFile EU** ShareFile — SAML2.0 **ShareFile VDR** ShareFile — SAML2.0
5.	On **Configuration** tab, enter ShareFile subdomain in Application Details.



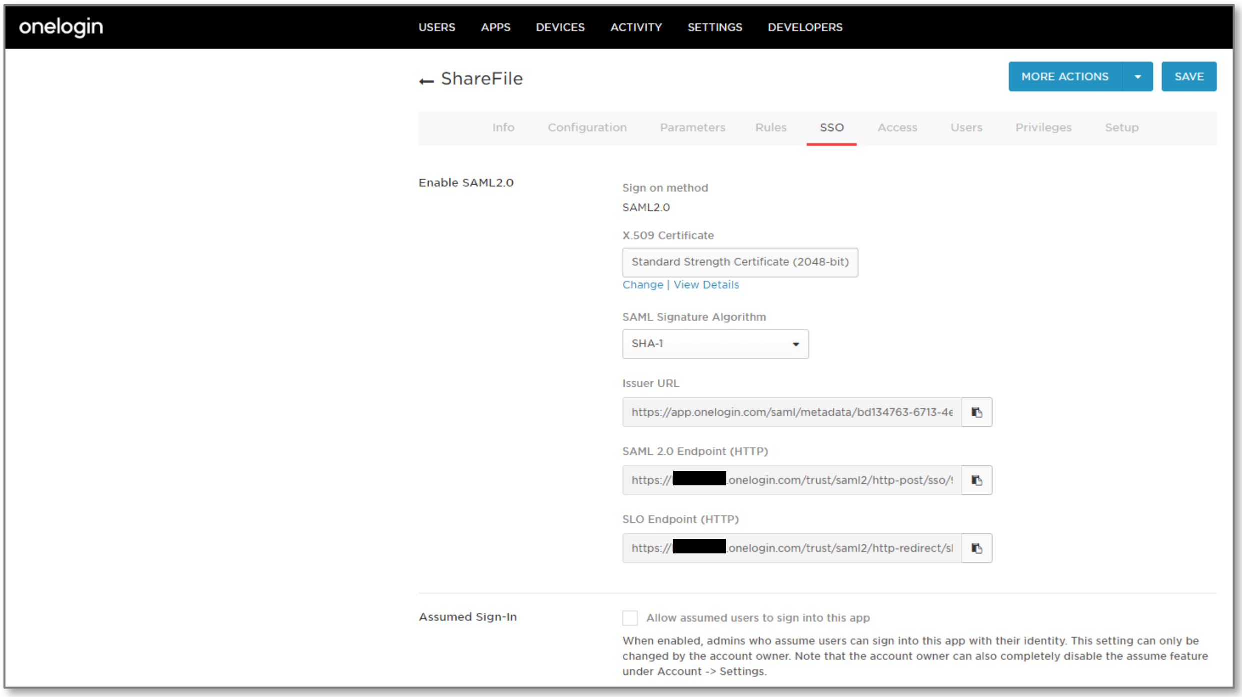
← ShareFile

Application Details

Subdomain: subdomain

For example, **mycompany**.sharefile.com

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



← ShareFile

Enable SAML2.0

Sign on method: SAML2.0

X.509 Certificate: Standard Strength Certificate (2048-bit)

SAML Signature Algorithm: SHA-1

Issuer URL: https://app.onelogin.com/saml/metadata/bd134763-6713-4e

SAML 2.0 Endpoint (HTTP): https://[redacted]onelogin.com/trust/saml2/http-post/sso/

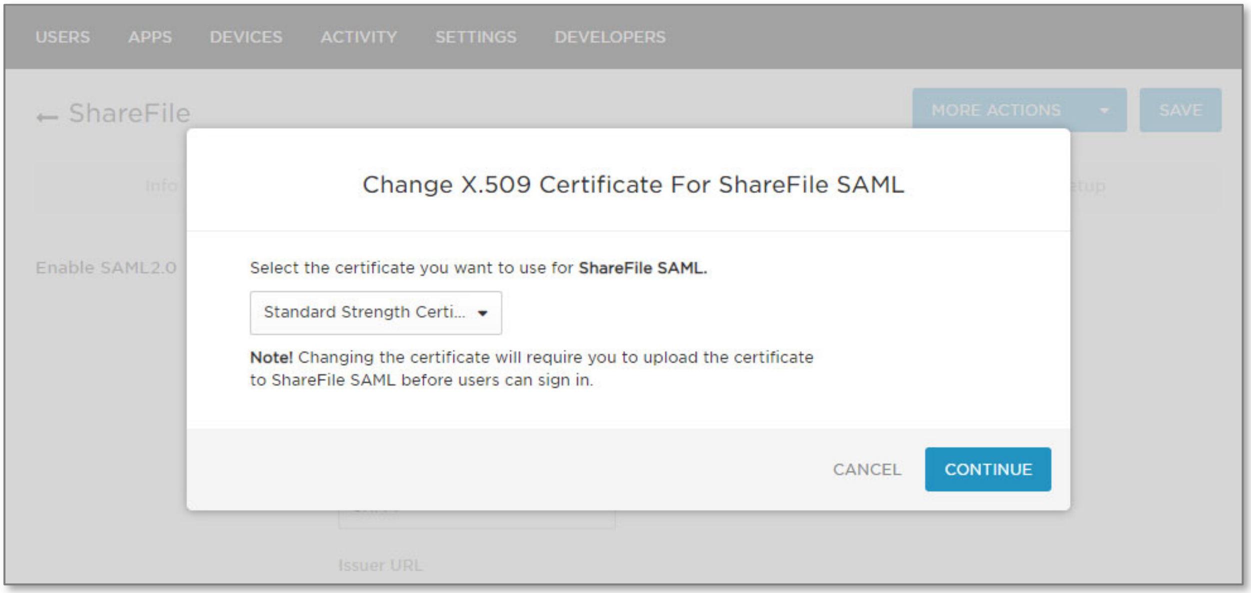
SLO Endpoint (HTTP): https://[redacted]onelogin.com/trust/saml2/http-redirect/sl

Assumed Sign-In

□ Allow assumed users to sign into this app

When enabled, admins who assume users can sign into this app with their identity. This setting can only be changed by the account owner. Note that the account owner can also completely disable the assume feature under Account -> Settings.

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



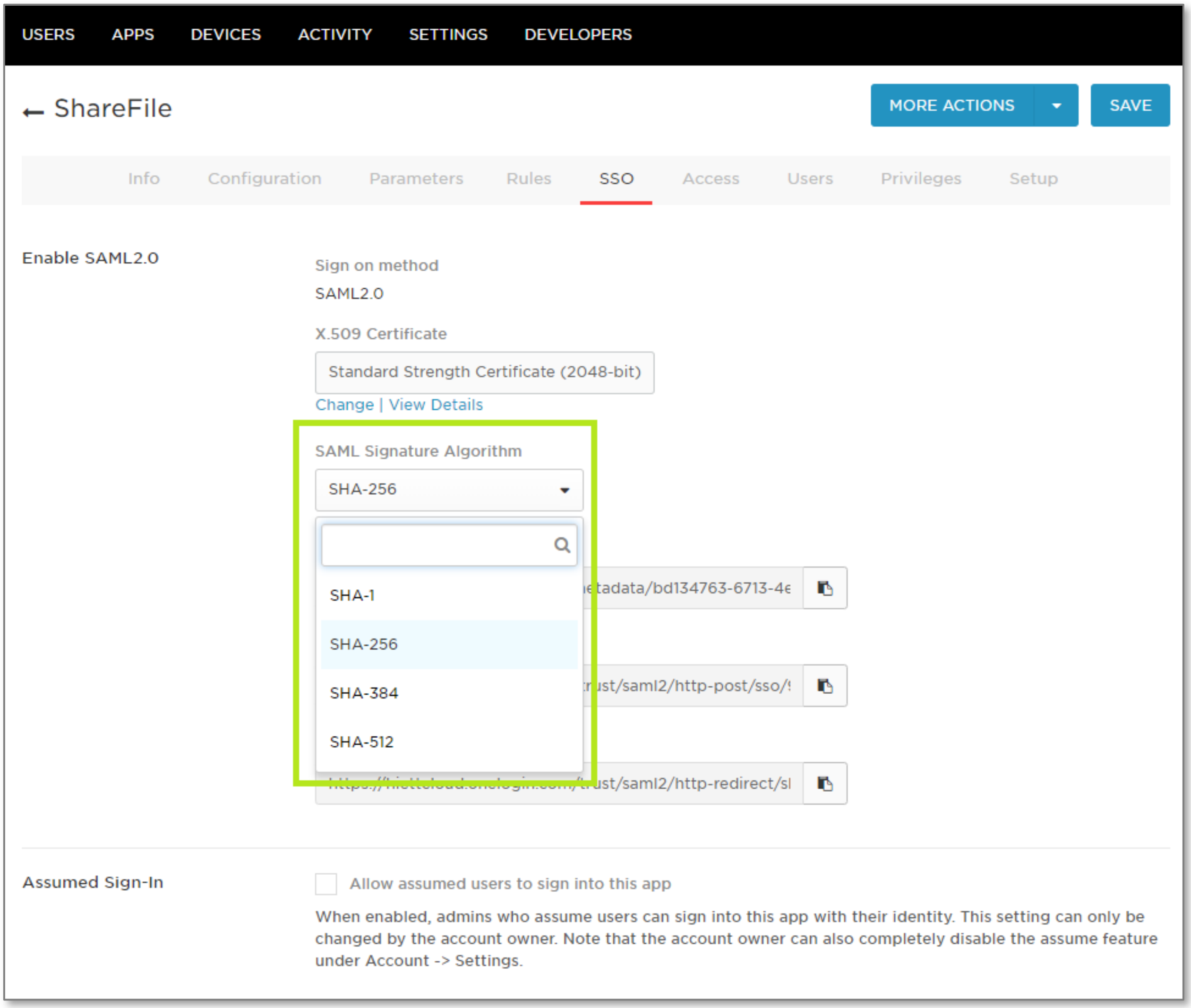
Change X.509 Certificate For ShareFile SAML

Select the certificate you want to use for **ShareFile SAML.**

Standard Strength Certi...

Note! Changing the certificate will require you to upload the certificate to ShareFile SAML before users can sign in.

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



Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)
Change | View Details

SAML Signature Algorithm
SHA-256

etadata/bd134763-6713-4e

rust/saml2/http-post/sso/

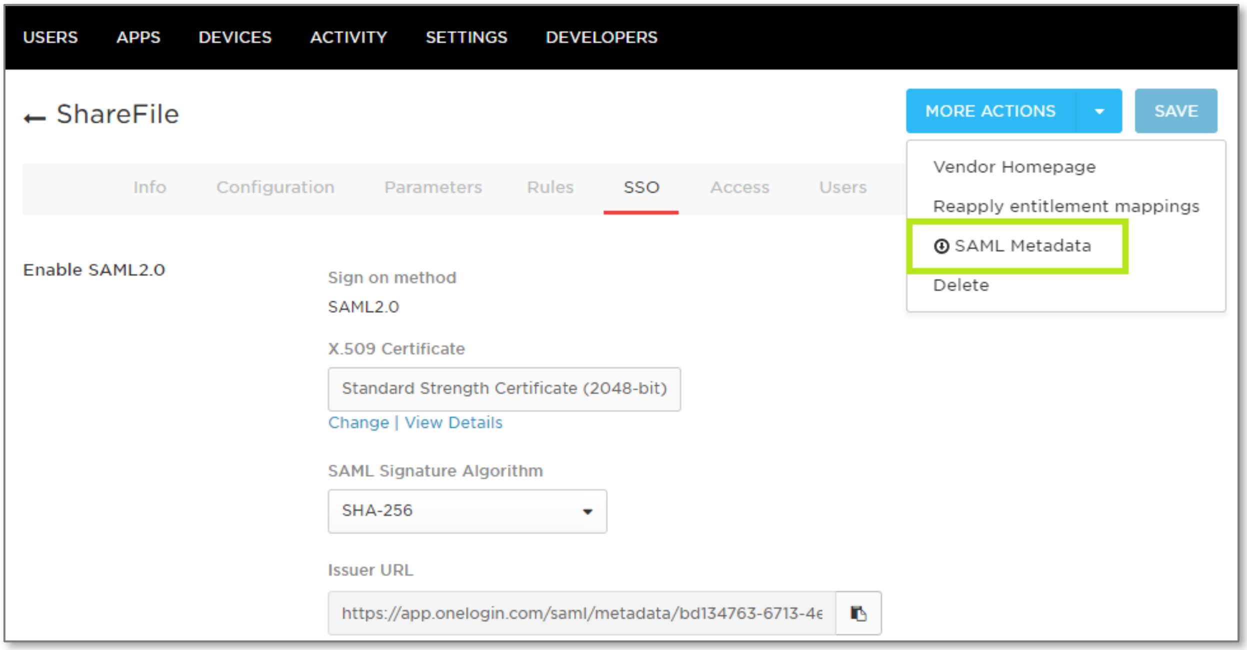
https://hiettcloud.onelogin.com/trust/saml2/http-redirect/sl

Assumed Sign-In

□ Allow assumed users to sign into this app

When enabled, admins who assume users can sign into this app with their identity. This setting can only be changed by the account owner. Note that the account owner can also completely disable the assume feature under Account -> Settings.

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



Enable SAML2.0

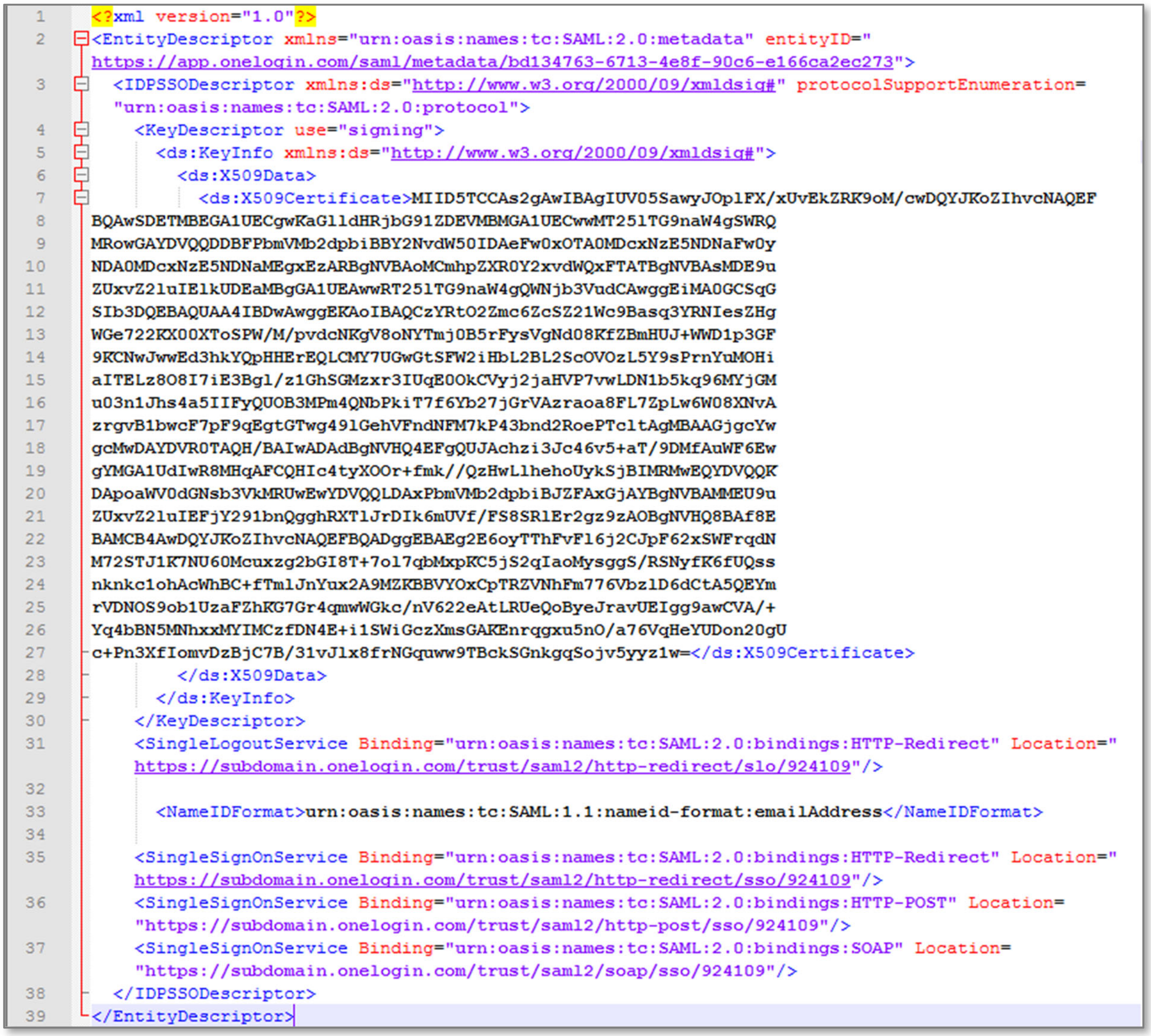
Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)
Change | View Details

SAML Signature Algorithm
SHA-256

Issuer URL
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:



```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
https://app.onelogin.com/saml/metadata/bd134763-6713-4e8f-90c6-e166ca2ec273">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
  "urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIID5TCCAs2gAwIBAgIUV05SawyJOplFX/xUvEkZRK9oM/cwDQYJKoZIhvcNAQEF
BQAwSDETMBEGA1UECgwKaGlldHRjbG91ZDEVMBMGA1UECwwMT25lTG9naW4gSWRQ
MRowGAYDVQQDDBFPbmVMb2dpbiBBY2NvdW50IDAeFw0xOTA0MDcxNzE5NDNaFw0y
NDA0MDcxNzE5NDNaMEgxEzARBgNVBAoMCmhpZXR0Y2xvdWQxFTATBgNVBAsMDE9u
ZUxvZ2luIElkUDEaMBgGA1UEAwwRT25lTG9naW4gQWNjb3VudCAwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzYRtO2Zmc6ZcSZ21Wc9Basq3YRNIesZHg
WGe722KX00XToSPW/M/pvdcNKgV8oNYTmj0B5rFysVgNd08KfZBmHUJ+WWD1p3GF
9KCNwJwwEd3hkYQpHHErEQLCMY7UGwGtSFW2iHbL2BL2ScOVOzL5Y9sPrnYuMOHi
aITELz8O8I7iE3Bgl/z1GhSGMzxr3IUqE0OkCVyj2jaHVP7vwLDN1b5kq96MYjGM
u03n1Jhs4a5IIFyQUOB3MPm4QNbPkiT7f6Yb27jGrVAzraoa8FL7ZpLw6W08XNvA
zrgvB1bwcF7pF9qEgtGTwg49lGehVFndNFM7kP43bnd2RoePTcltAgMBAAGjgcYw
gcMwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQUJAchzi3Jc46v5+aT/9DMfAuWF6Ew
gYMGA1UdIwR8MHqAFCQHIc4tyXOOr+fmk//QzHwLlhehoUykSjBIMRMwEQYDVQQK
DApoaWV0dGNsb3VkMRUwEwYDVQQLDAxPbmVMb2dpbiBJZFAxGjAYBgNVBAMMEU9u
ZUxvZ2luIEFjY291bnQgghRXTlJrDIk6mUVf/FS8SRlEr2gz9zAOBgNVHQ8BAf8E
BAMCB4AwDQYJKoZIhvcNAQEFBQADggEBAEg2E6oyTThFvFl6j2CJpF62xSWFrqdN
M72STJ1K7NU60Mcuxzg2bGI8T+7ol7qbMxpKC5jS2qIaoMysggS/RSNyfK6fUQss
nknkc1ohAcWhBC+fTmlJnYux2A9MZKBBVYOxCpTRZVNhFm776Vbz1D6dCtA5QEYm
rVDNOS9ob1UzaFZhKG7Gr4qmwWGkc/nV622eAtLRUeQoByeJravUEIgg9awCVA/+
Yq4bBN5MNhxxMYIMCzfDN4E+i1SWiGczXmsGAKEnrqgxu5nO/a76VqHeYUDon20gU
c+Pn3XfIomvDzBjC7B/31vJlx8frNGquww9TBckSGnkgqSojv5yyz1w=</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://subdomain.onelogin.com/trust/saml2/http-redirect/slo/924109"/>

      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>

    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://subdomain.onelogin.com/trust/saml2/http-redirect/sso/924109"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=
    "https://subdomain.onelogin.com/trust/saml2/http-post/sso/924109"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location=
    "https://subdomain.onelogin.com/trust/saml2/soap/sso/924109"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

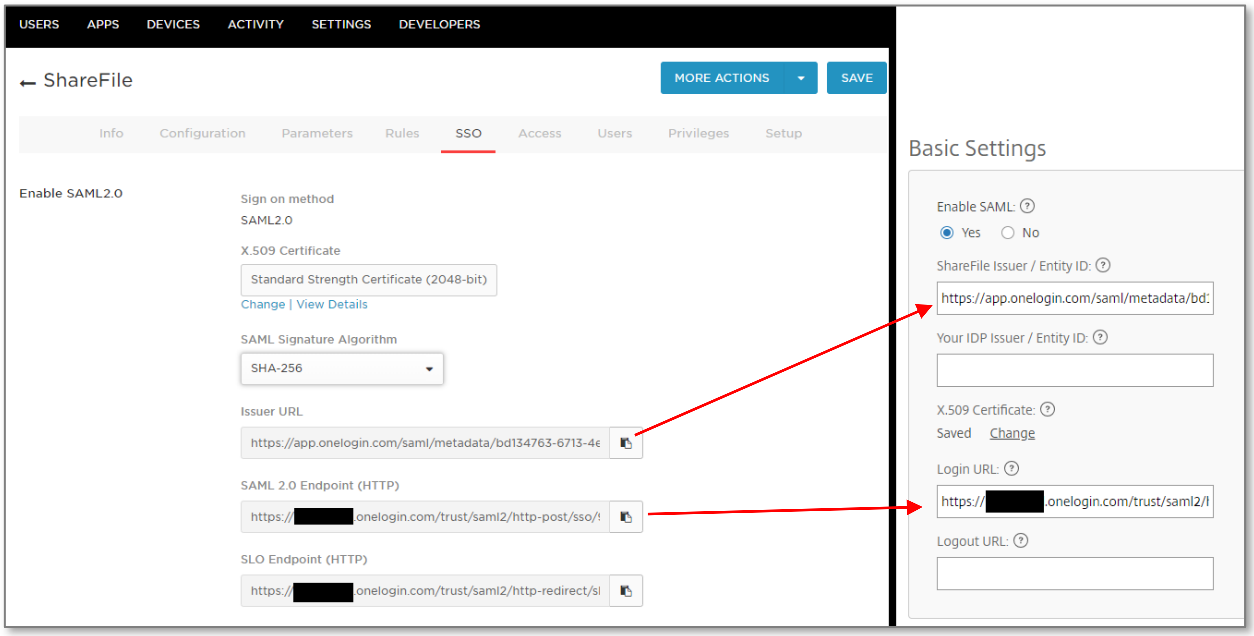
11. Go to your ShareFile account: https://subdomain.sharefile.com > Login with Administrator account > **Settings** > **Admin Settings** > **Security** > **Login & Security Policy** > scroll down on this page to **Single sign on / SAML 2.0 Configuration.**

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.)



Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)

SAML Signature Algorithm
SHA-256

Issuer URL
https://app.onelogin.com/saml/metadata/bd134763-6713-4e

SAML 2.0 Endpoint (HTTP)
https://[redacted].onelogin.com/trust/saml2/http-post/sso/

SLO Endpoint (HTTP)
https://[redacted].onelogin.com/trust/saml2/http-redirect/sl

Basic Settings

Enable SAML: ⓘ
● Yes ○ No

ShareFile Issuer / Entity ID: ⓘ
https://app.onelogin.com/saml/metadata/bd:

Your IDP Issuer / Entity ID: ⓘ

X.509 Certificate: ⓘ
Saved Change

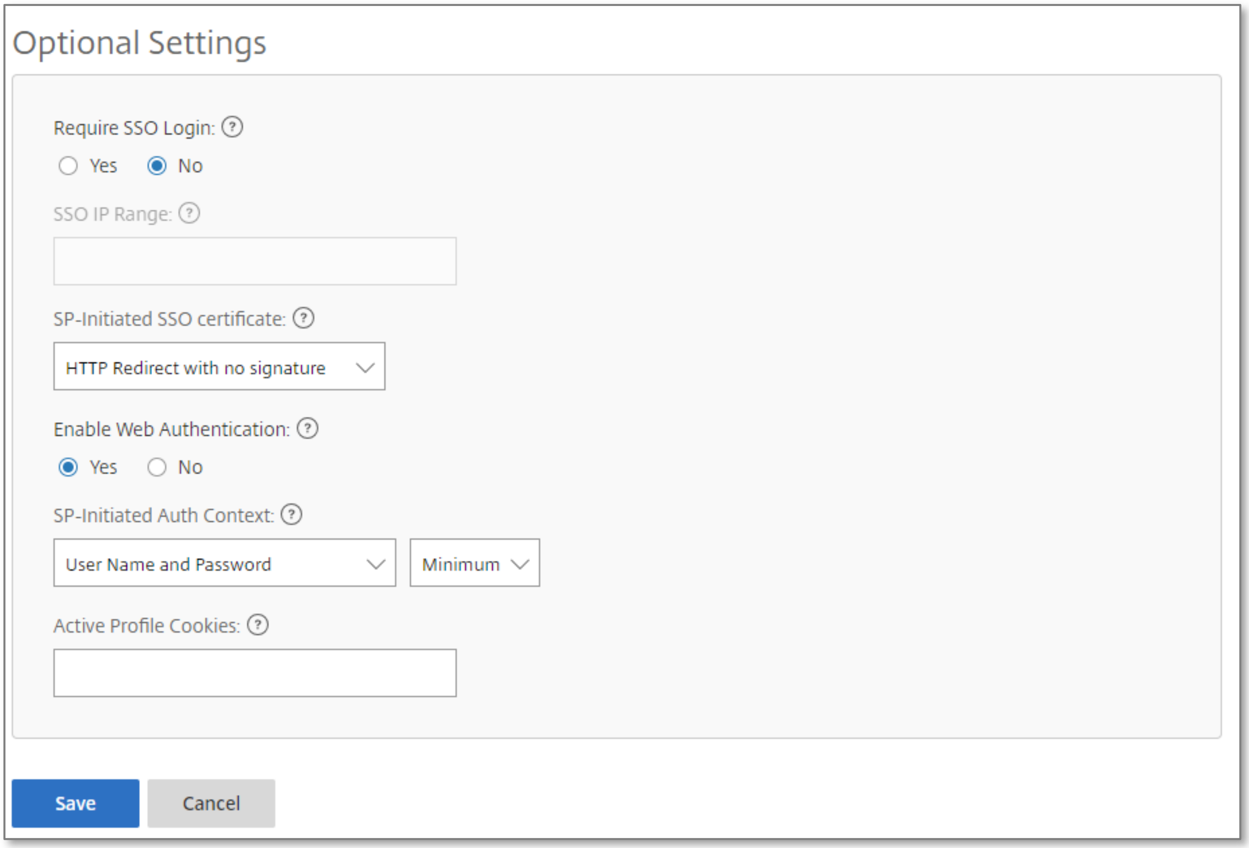
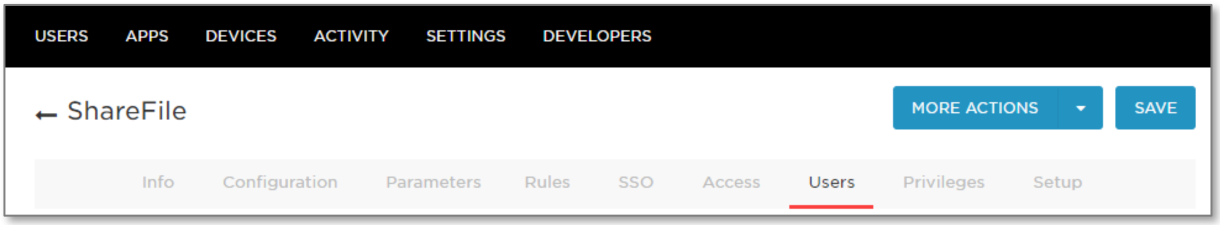
Login URL: ⓘ
https://[redacted].onelogin.com/trust/saml2/h

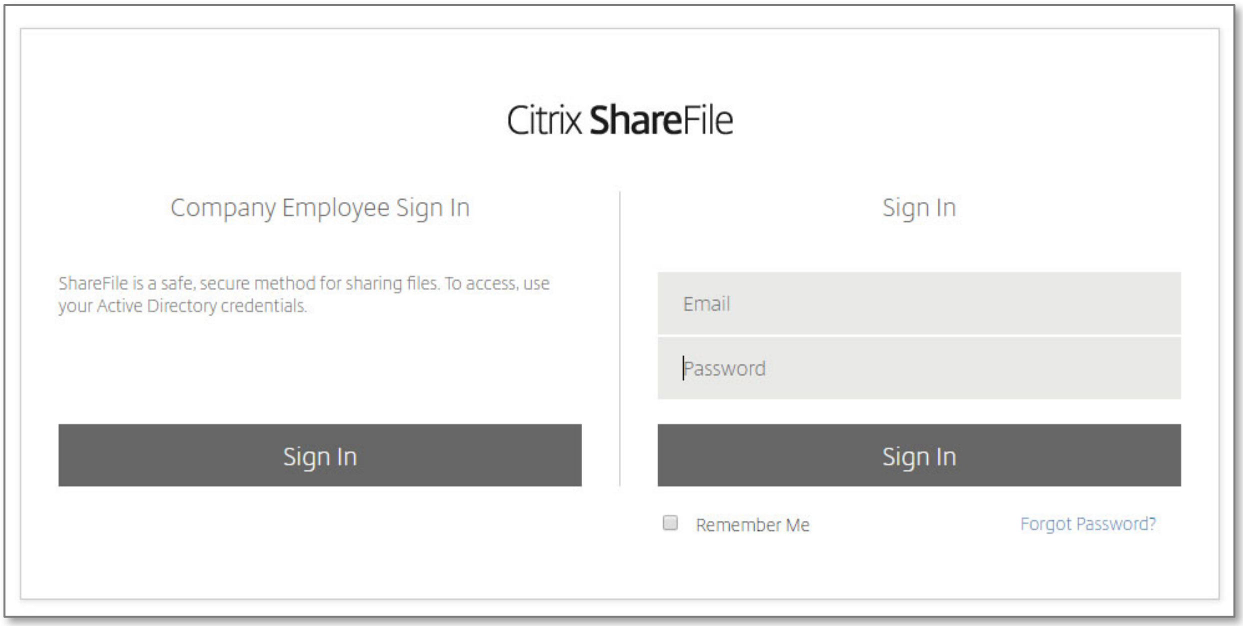
Logout URL: ⓘ

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

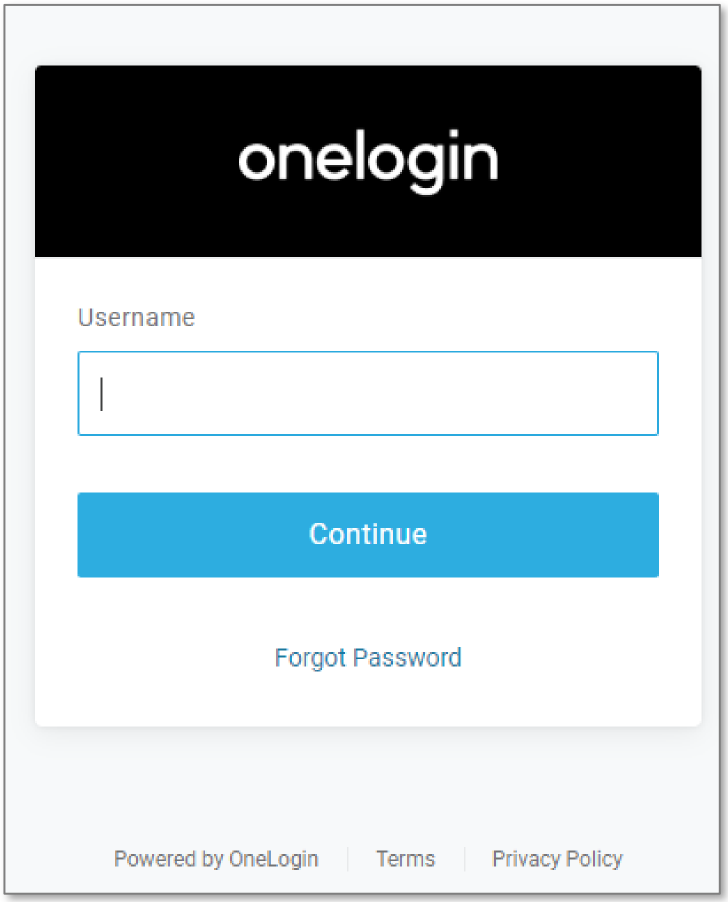
	will need to be available. **No** is not recommended). ○ **SP-initiated Auth Context**: Select **User Name and Password**. ○ **Active Profile Cookies**: Leave blank ○ Click **Save**  Optional Settings Require SSO Login: ○ Yes ● No SSO IP Range: SP-Initiated SSO certificate: HTTP Redirect with no signature Enable Web Authentication: ● Yes ○ No SP-Initiated Auth Context: User Name and Password, Minimum Active Profile Cookies:
14.	Make sure **Users** are authorized to use this app.  USERS APPS DEVICES ACTIVITY SETTINGS DEVELOPERS ← ShareFile MORE ACTIONS SAVE Info Configuration Parameters Rules SSO Access Users Privileges Setup
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**



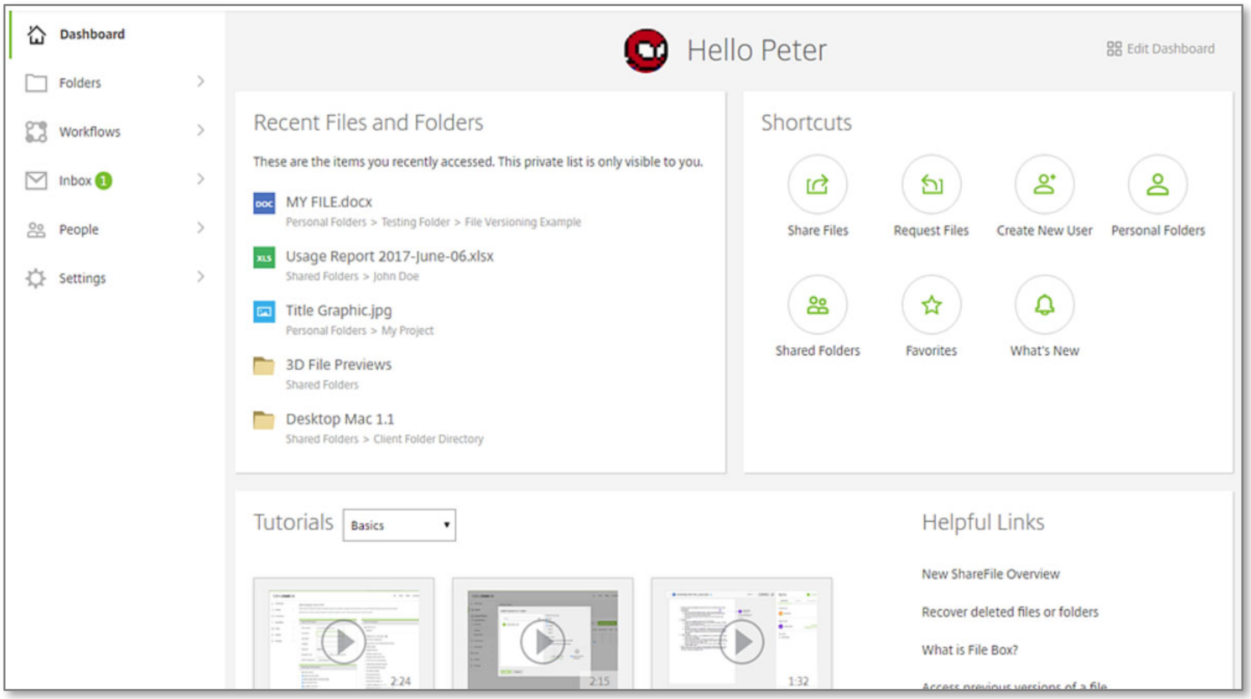
ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials.

****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:



<table>
<tr>
<td></td>
<td>
Successful logins will authenticate users into their ShareFile account **Dashboard**.



Recent Files and Folders

These are the items you recently accessed. This private list is only visible to you.

MY FILE.docx
Personal Folders > Testing Folder > File Versioning Example

Usage Report 2017-June-06.xlsx
Shared Folders > John Doe

Title Graphic.jpg
Personal Folders > My Project

3D File Previews
Shared Folders

Desktop Mac 1.1
Shared Folders > Client Folder Directory

Helpful Links

New ShareFile Overview

Recover deleted files or folders

What is File Box?

Access previous versions of a file
</td>
</tr>
<tr>
<td>16.</td>
<td>Done!</td>
</tr>
</table>