

Content Collaboration: Single Sign-On Configuration Guide

Centrify / Idaptive



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.

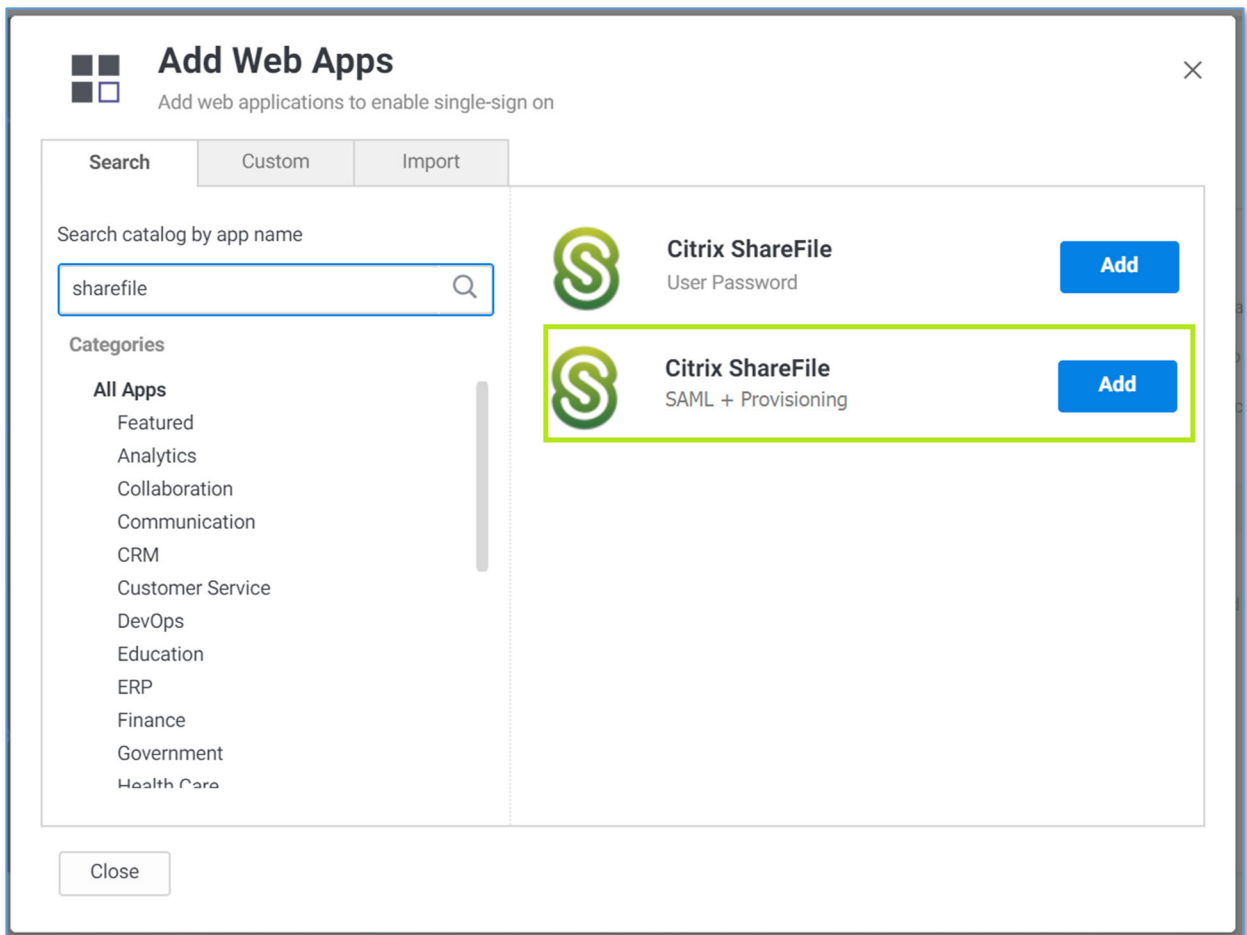
Steps	Description
1.	<p>Log in to the Idaptive Portal URL.</p> <p>For example, login to: https://customerid.my.centriify.com/manage.</p> 
2.	<p>In the Dashboard navigation menu, click on Apps > Web Apps.</p> 

3. Click on **Add Web Apps**.

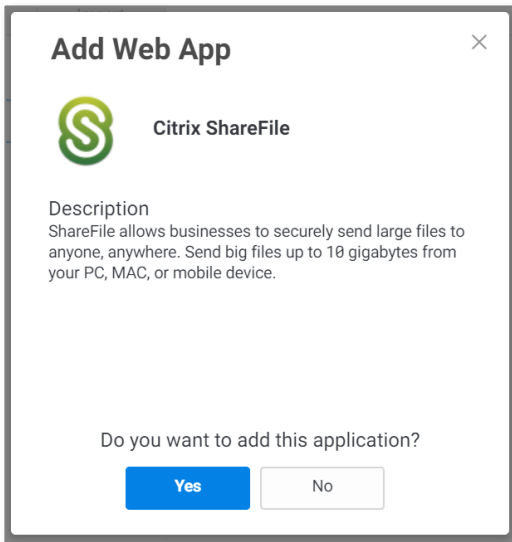


4. Search the catalog for "sharefile." Choose **Add** for **Citrix ShareFile**.

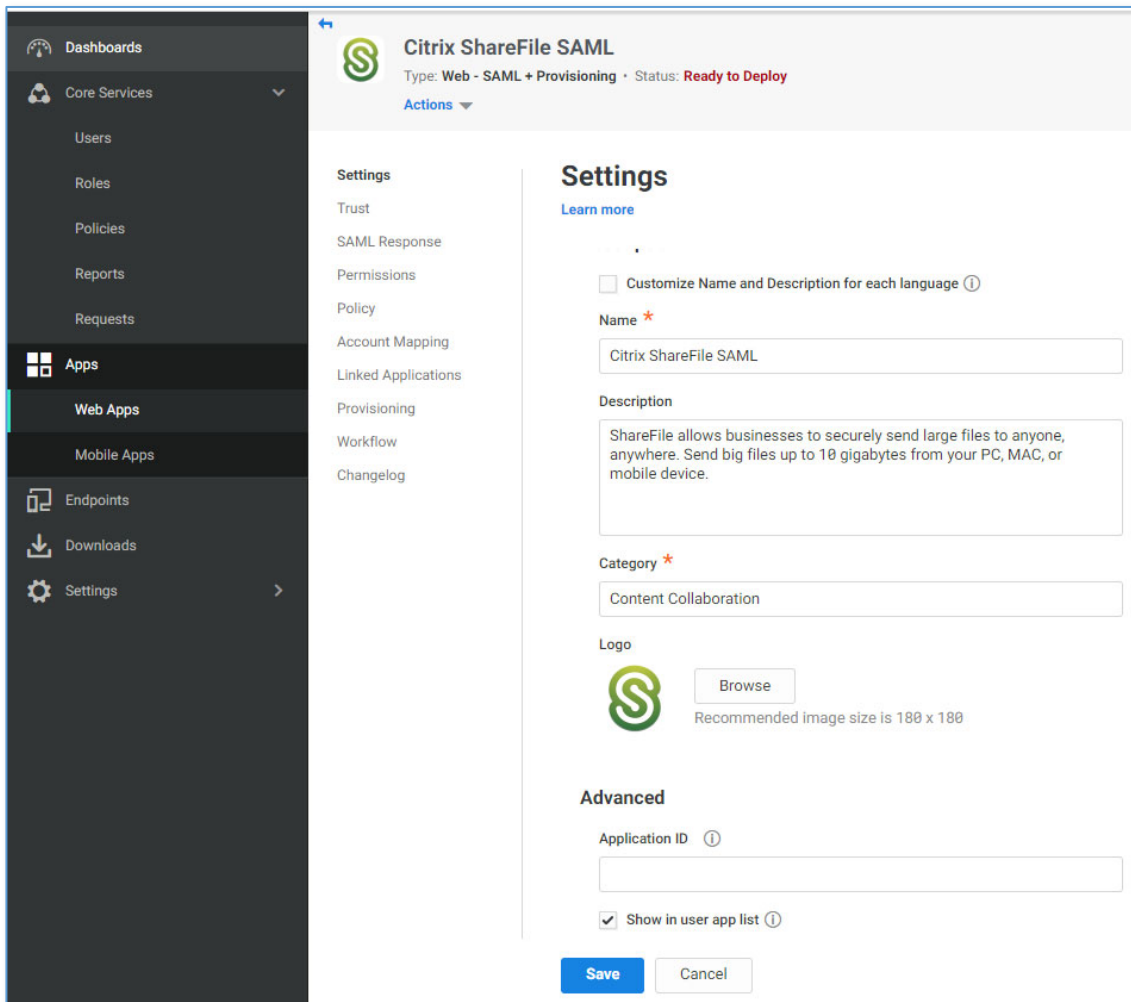
****Make sure the app is SAML + Provisioning. The User Password Web App is not compatible for SAML authentication. Contact Idaptive support team if the Web App is not available in the admin portal.**



5. Confirm **Yes** to add the application.



6. Exit **Add Web App**, and begin to configure **Citrix ShareFile** app.



7. Click on the **Trust** section. Under **Identity Provider Configuration** > select **Manual Configuration** > Expand **Signing Certificate** > click **Download**.

Citrix ShareFile SAML
 Type: Web - SAML + Provisioning · Status: Ready to Deploy
 Actions ▾

Settings

Trust [Learn more](#)

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

Workflow

Changelog

Trust

Identity Provider Configuration

Configure your Your IDP Issuer / Entity ID and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values. If SAML Service Provider requires you to send IdP Configuration values, copy them from below and send them to the SAML Service Provider.

Metadata
 Manual Configuration

Manual Configuration

If your SAML Service Provider provides a SAML SSO configuration screen, copy the applicable IdP Configuration values. If SAML Service Provider requires you to send IdP Configuration values, copy them from below and send them to the SAML Service Provider.

Your IDP Issuer / Entity ID ⓘ

Signing Certificate ⓘ
 Idaptive SHA256 Tenant Signing Certificate (default) ▾

Thumbprint: CAEB80BCADB2720200F55D5FD36700E0414172E5
Subject: CN=Centriify Customer ABB0471 Application Signing Certificate
Algorithm: sha256RSA
Expires: 12/31/2038 7:00:00 PM

Login URL ⓘ

Logout URL ⓘ

Single Sign On Error URL

- The default certificate file is a .cer file. Open the file with **Notepad** or any text editor and save for later steps.

```
-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIQZDGCdCuT7t0jDsvUkdh5DANBgkqhkiG9w0BAQsFADAK
MSIwIAYDVQQDDBlJZGFwZG12ZSBDb211ciBBQkIwNDcxMB4XDTE5MDQyMTE4
MTc0OFoXDTM5MDEwMTAwMDAwMFowRDFCMEAGA1UEAww5Q2VudHJpZnkgQ3VzdG9t
ZXIqQUJCMQ3MSBBcHBsaWNhdGlvbiBTAWduaW5nIEN1cnRpZmljYXR1MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAXaWtbVoadnw0owOwx5CmU4ABRmCU
LT4DEFYAAvISdRwcWLnOhHm+soRD.JhVT.JXpmUeN22HDCvTI5oZ+XfKccKC5RY5
+*whc32a2N1E27oghIvgeW1AY4c7ezL1Qvbc3E0t0MSE0y/8v0f9naW+89yru57eC
8DwYala++qgJmMuJ3980tThgsowg8pY0F0FWE1a2ga0M89W13a8KXVb1CJFaeCh
UJubEYU10eaF18p3ayy0y0pyL8MCR4W1uWf8gtfaa4KO+1dCDE4Mba4ogkF00Y9
4V00deE0Tg00j+0J811gtFFF9j+02g0WYv8abgngYh0Lad040y21L50Fw1DAGAB
+40W10M8M0C1eCAGQ8gg1wAGKEgW0M4w80c0C1eCAGQ8gg1wAGKEgW0M0JC
M0G1M0A18p8V0M800a8p8a8M0K8Wyt0F+2JF+v0w0003a8110A8p8V0M4E8Fg00
jxp14hQ8wFvY1tEgA1A7wA8F8w0gY0V0F0A0M/8A00A8p8w0C1eCAGQ8gg1w
AGKEgW0M0JC1Y88p824w0G7J8c218v+0MAG18QADggY8ABaa/akLakF9TAS
X1YY+088p4g1e4C1g0Vt01E8a8Y81tY00a8W0Cv78wa3C8Bu1V1raAAT/jY0K
00G/M85V11g8K3uagtW0+M88p8gW0T00/0gF0M8318K21W31aE8a8M0K18Lak1
2jy8cLakF1ad/v080p8W0M4w80c0C1eCAGQ8gg1wAGKEgW0M0JC1Y88p824w0G7
wv0eJ2T8pFW13a8p80G0K0F2T8a8F3a83a8418M8p8FC0M8118W08g0M0a8M
0F0a82480F8CRJFCT000070L8A43a8a80gY7909E8a8+T//0C8aF08b91ampJ8a
30ATEAA=
-----END CERTIFICATE-----
```

9. Click on the **Trust** section to the left navigation menu. Under **Service Provider Configuration** > select **Manual Configuration**. Enter the following settings only:

ShareFile Issuer / Entity ID: <https://subdomain.sharefile.com/saml/info>
Assertion Consumer Service (ACS) URL: <https://subdomain.sharefile.com/saml/acs>
Authentication Context Class: PasswordProtectedTransport

Click **Save** when done.

Citrix ShareFile SAML
Type: Web - SAML + Provisioning · Status: Ready to Deploy

Actions ▾

Settings

Trust [Learn more](#)

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

Workflow

Changelog

Select the configuration method specified by Service Provider, and then follow the instructions.

Metadata

Manual Configuration

Manual Configuration

Fill out the form below with information given by your Service Provider. Be sure to save your work when done.

ShareFile Issuer / Entity ID ⓘ

Assertion Consumer Service (ACS) URL ⓘ

Recipient * ⓘ Same as ACS URL

Sign Response or Assertion?
 Response Assertion

NameID Format ⓘ

Single Logout URL ⓘ

Encrypt SAML Response Assertion ⓘ

Relay State ⓘ

Authentication Context Class ⓘ

10. Click on **Permissions** in the left navigation menu. Choose **Add** to select users that have access to single sign on to ShareFile.

You will need to make sure each selected user has an Email Address in Idaptive and their account in ShareFile should have a matching Email Address. The Web app switches to **Ready to Deploy to **Deployed** when users are assigned.

Citrix ShareFile SAML
Type: Web - SAML + Provisioning · Status: Ready to Deploy

Actions ▾

Settings

Trust

SAML Response

Permissions [Learn more](#)

Policy

Account Mapping

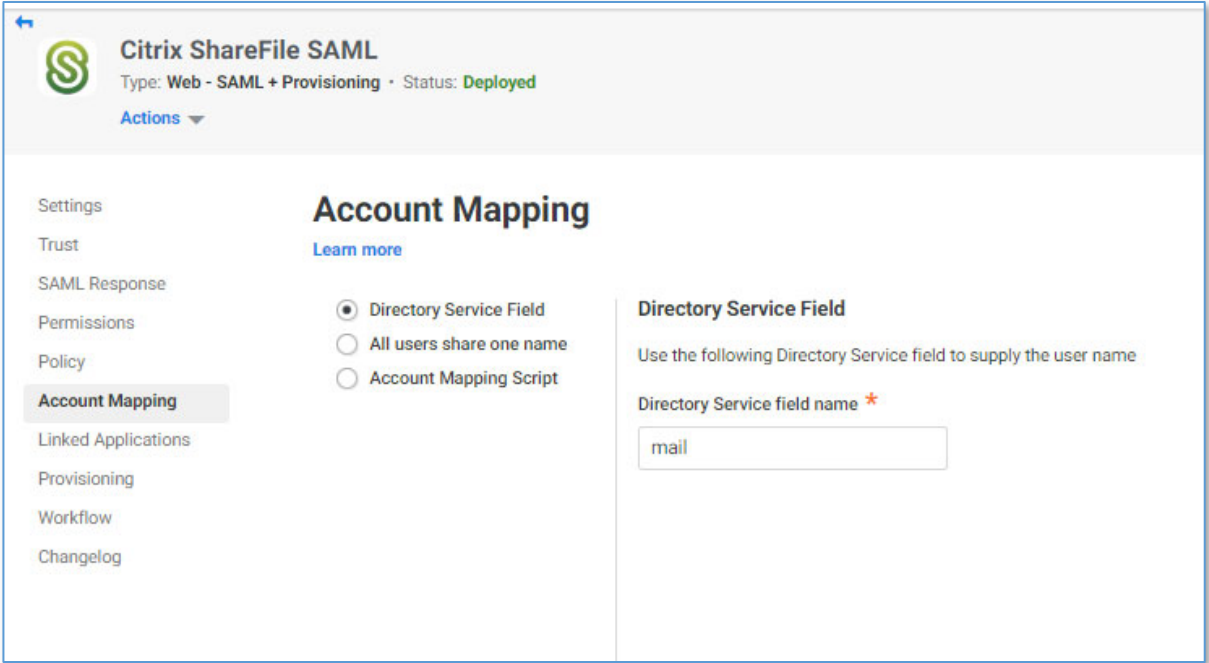
Linked Applications

Provisioning

Workflow

Changelog

Name	Grant	View	Run	Automatically Deploy	Starts	Expires	Inherited From
<input type="checkbox"/> sysadmin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			Sysadmin

	Click Save when done.
11.	<p>Click on Account Mapping in the left navigation menu. Ensure the Directory Service Field name is left as mail.</p>  <p>The screenshot shows the 'Citrix ShareFile SAML' configuration page. The left sidebar contains a navigation menu with items: Settings, Trust, SAML Response, Permissions, Policy, Account Mapping (highlighted), Linked Applications, Provisioning, Workflow, and Changelog. The main content area is titled 'Account Mapping' with a 'Learn more' link. Under 'Directory Service Field', three radio buttons are present: 'Directory Service Field' (selected), 'All users share one name', and 'Account Mapping Script'. To the right, under 'Directory Service Field', there is a text input field labeled 'Directory Service field name' with a red asterisk, containing the text 'mail'. The status bar at the top indicates 'Type: Web - SAML + Provisioning' and 'Status: Deployed'.</p> <p>Click Save when done.</p>
12.	<p>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.</p>

Use values from Admin Portal > Web App > Citrix ShareFile > Trust settings to configure **Single sign on / SAML 2.0 Configuration**:

Basic Settings

- **Enable SAML:** Select **Yes**
- **ShareFile Issuer / Entity ID:** Copy and paste from Service Provider Configuration
- **Your Issuer / Entity ID:** Copy and paste from Identity Provider Configuration
- **X.509 Certificate:** Click **Change**, then copy and paste the certificate downloaded in previous steps
- **Login URL:** Copy and paste from Identity Provider Configuration
- **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:

Your IDP Issuer / Entity ID:

X.509 Certificate: Saved [Change](#)

Login URL:

Logout URL:

Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

Metadata Manual Configuration

Manual Configuration

Fill out the form below with information given by your Service Provider. Be sure to save

ShareFile Issuer / Entity ID

Identity Provider Configuration

Configure your Your IDP Issuer / Entity ID and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values, copy them from below and send them to your Service Provider.

Metadata Manual Configuration

Manual Configuration

If your SAML Service Provider provides a SAML SSO configuration screen, copy the applicable IdP Configuration values, copy them from below and send them to your Service Provider. If SAML Service Provider requires you to send IdP Configuration values, copy them from below and send them to your Service Provider.

Your IDP Issuer / Entity ID [Copy](#)

> Signing Certificate

Login URL [Copy](#)

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 Idaptive. Admins can login using Idaptive 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 Idaptive 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

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

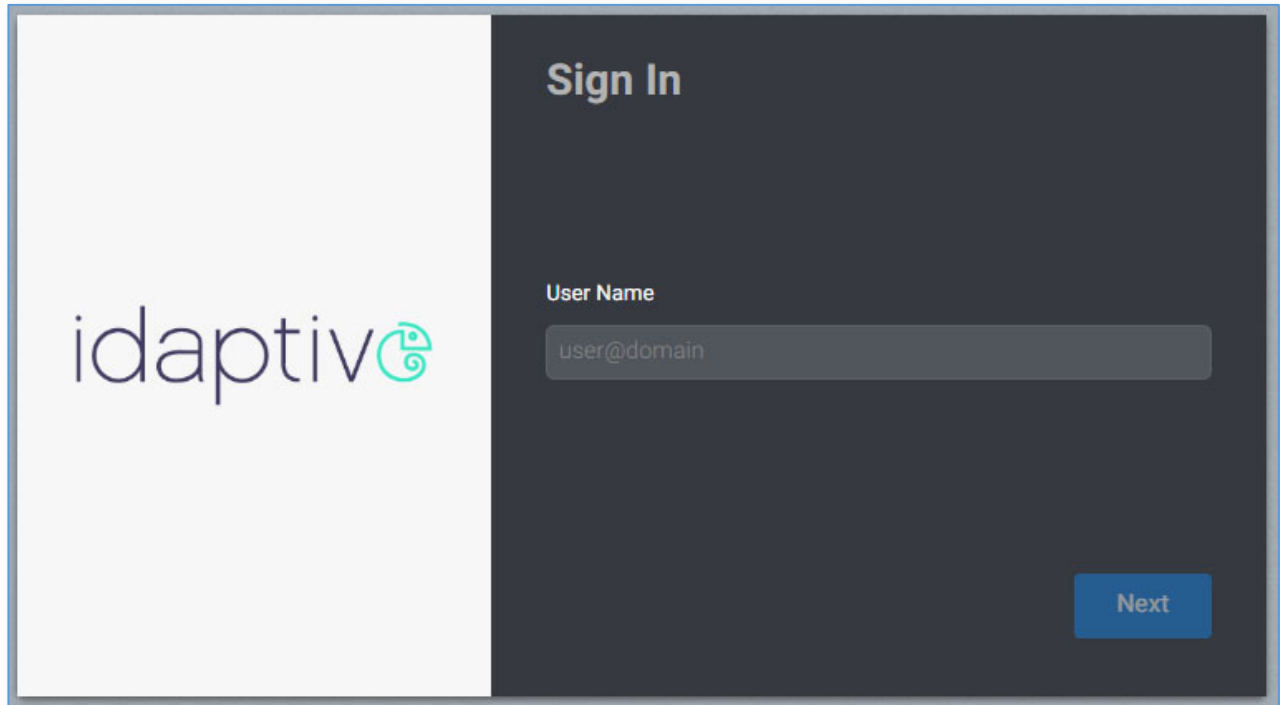
Password

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 Idaptive for sign in:



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

