## 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.	Log in to the Idaptive Portal URL.
	For example, login to: <u>https://customerid.my.centrify.com/manage</u> .
	idaptivで い と と と と と の た し と の し し し と の し し し し し し の し し し し し し し し し し し し し
2.	In the Dashboard navigation menu, click on Apps > Web Apps.
	Web Apps       Mobile Apps       Image: Deprive a structure of the structure of t
	Settings >

3.	Click on Add Web Apps.
	Web Apps
	Search SAML 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.
	Categories       All Apps       Strix ShareFile       Add         Featured       Analytics       SAML + Provisioning       Add         Collaboration       Communication       CRM       Customer Service       DevOps       Education       ERP       Finance       Government       Health Care       Close
5.	Confirm <b>Yes</b> to add the application.

	Add Web App	×	
	Citrix ShareFile		
	Description ShareFile allows businesses to securely anyone, anywhere. Send big files up to your PC, MAC, or mobile device.	send large files to 0 gigabytes from	
	Do you want to add this ap	plication?	
6.	Exit Add Web App, an	d begin to co	onfigure Citrix ShareFile app.
	Core Services	Citrix Share Type: Web - SAM Actions 👻	PFIIE SAML IL + Provisioning + Status: Ready to Deploy
	Users	Settings	Settings
	Roles	Trust	Learn more
	Policies	SAML Response	
	Reports	Permissions Policy	Customize Name and Description for each language (1)
	Requests	Account Mapping	Name *
	Apps	Linked Applications	Description
	Web Apps	Workflow	ShareFile allows businesses to securely send large files to anyone,
	Mobile Apps	Changelog	anywhere. Send big files up to 10 gigabytes from your PC, MAC, or mobile device.
	Downloads		Category *
	Settings		Content Collaboration
			Logo Browse Recommended image size is 180 x 180
			Advanced
			Application ID ①
			✓ Show in user app list ①
			Save
7.	Click on the <b>Trust</b> sect	ion. Under <b>l</b> e	dentity Provider Configuration > select Manua

Trust	Trust Learn more			
SAML Response	Identity Provider Confi	guration		
Policy	Configure your Your IDP Issue	r / Entity ID and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configu		
Account Mapping	O Metadata	Manual Configuration		
Linked Applications Provisioning	<ul> <li>Manual Configuration</li> </ul>	If your SAML Service Provider provides a SAML SSO configuration screen, copy the If SAML Service Provider requires you to send IdP Configuration values, copy them for the service provider requires you to send IdP Configuration values.	applicable IdP Conf from below and sen	
Workflow		✓ Your IDP Issuer / Entity ID (j)		
Changelog		https://aan0092.my.centrify.com/471dce39-3404-4c07-a35c-e3be312b62	Сору	
		✓ Signing Certificate ①		
		Idaptive SHA256 Tenant Signing Certificate (default)	·	
		Thumbprint: CAEB80BCADB2720200F55D5FD36700E0414172E5 Subject: CN=Centrify Customer ABB0471 Application Signing Certificate Algorithm: sha256RSA Expires: 12/31/2038 7:00:00 PM Download		
		Login URL (j)		
		https://abb0471.my.centrify.com/run?appkey=0e105117-8cdf-4d52-8	Сору	
		Logout URL (j)		
		https://abb0471.my.centrify.com/applogout/appkey/0e105117-8cdf-z	Сору	
		Single Sign On Error URL		
			9.02	

	📝 Idantive SHA256 Tenant Signing Certificate (default).cer - Notepad++ — — — — X
	File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? X
0	]
ī	🔚 Idaptive SHA256 Tenant Signing Certificate (default).cer 🗵
	1BEGIN CERTIFICATE
	2 MIIDkTCCAnmgAwIBAgIQZDGCDiCuT7t0jDsvUkdh5DANBgkqhkiG9w0BAQsFADAk 3 MSIwIAYDVOODDB1JZGFwdG12ZSBDdXN0b211ciBB0kIwNDcxMB4XDTE5MD0vMTE4
	4 MTc00FoXDTM5MDEwMTAwMDAwMFowRDFCMEAGA1UEAww5Q2VudHJpZnkgQ3VzdG9t
	5 ZXIgQUJCMDQ3MSBBcHBsaWNhdGlvbiBTaWduaW5nIENlcnRpZmljYXRlMIIBIjAN
	7 LT4DEFYAAvISdBwcWLnObHbm+soRD.TbVT.TXpmUeN22HDCvTT5o2+XFfKccKC5RY5
	8 +1whc31x1Wi8270gb1vgwEtAT4c7csLlQvBc1ETt0MEE3c/RvOfgnaW+Hysu37nC
	9 FDeValar-ogf (http://www.brdow/ibicher.com/force/factorer.com/force/
	11 4V008xEUTg0Dj+0JB25qTFFFEjoEQg0WTvKeBgeQVh0La0t60y21L50Fvw1DAQAB
	12 o45eMIGEMBHSCI#SAQQBpgTwAQXEBQwCHE4wHBcOCI#SAQQBpgTwAQHECQwHQD3C
	14 japléhokwivyltfgäla.bukarrinawögytyvkösaga/aagcagegelaeöciedaggbegiv
	15 AggEDgwLgKBw661 jYXRg634wDgYJKo31hvcRAgELBgADggEBABxx/kkLakf9FTA5
	16 X1YY+d3Ap4gic4Cig0VTo1fAaaTBJtyCGanMa0Cv7Ewtm3CEBu1V1rsAkT/jToRt 000/WESV11ed6VTepsteds1000000000000000000000000000000000000
	11 2jyhcLa8fisd/v0b0pd8nVAhc+dD7ya7Lnt4sj31VL0A330u8D9phyyAJDshD2TF
	<ol> <li>vvv0rJ2TvpfWtjm2pa40qEXuF2TvxBfjev3nkv4L8NpJPC0WLh1F#dEbqQRNEaQH</li> </ol>
	20 21 5
	22END CERTIFICATE
	23
	Normal text file   length : 1,322   lines : 24 Ln : 22 Col : 1 Sel : 0   0 Windows (CR LF) UTF-8 INS
	lick on the Truct section to the left newlection many Under Service Provider
9. 0	lick on the <b>Trust</b> section to the left havigation menu. Onder <b>Service Provider</b>
	<b>onfiguration</b> > select <b>Manual Configuration</b> . Enter the following settings only:
CI	haroEilo Issuer / Entity ID: https://subdomain.sharofilo.com/saml/info
31	naret ne 1550er / Linuy ID. <u>https://subdomain.snaretne.com/sami/into</u>
A	ssertion consumer Service (ACS) UKL: <a href="https://subdomain.snaretile.com/saml/acs">https://subdomain.snaretile.com/saml/acs</a>
	uthentication Context Class: PasswordProtectedTransport
C	lick <b>Save</b> when done.
C	lick <b>Save</b> when done.

	Trust					
Trust	Learn more					
SAML Response	select the configuration metho	od specified by service Provider, and then rollow the instructions.				
Permissions	O Metadata	Manual Configuration				
Policy Account Mapping	<ul> <li>Manual Configuration</li> </ul>	Fill out the form below with information given by your Service Provider. Be sure to save your work wi				
Linked Applications		ShareFile Issuer / Entity ID (i)				
Provisioning		https://subdomain.sharefile.com/saml/info				
Workflow		Assertion Consumer Service (ACS) URL (i)				
Changelog		https://subdomain.sharefile.com/saml/acs				
		Enter Recipient here				
		Sign Response or Assertion?       Response Assertion				
		NamelD Format (j)				
		emailAddress 👻				
		Single Logout URL (i)				
		Enter URL here				
		Encrypt SAML Response Assertion (i)				
		Choose File Encryption Certificate (Required)				
		Pelay State (i)				
		Authentication Context Class (i)				
		PasswordProtectedTransport				
10. Click on <b>Permi</b> s	Save Cancel	avigation menu. Choose <b>Add</b> to select users that				
have access to	single sign on to SI	hareFile.				
**You will need t	**You will need to make sure each selected user has an Email Address in Idaptive and their					
account in Share	-ile should have a mat	tching Email Address. The Web app switches to <b>Ready</b>				
Deploy to Deploy	Deploy to Deployed when users are assigned.					
Citrix ShareFile SAML						
	itatus: Ready to Deploy					
Type: Web - SAML + Provisioning - S Actions -						
Settings Permit	ssions					
Settings Permit SAML Response	ssions					

Actions -	L + Provisioning • Status: Deployed	
Settings Trust SAML Response Permissions Policy Account Mapping Linked Applications Provisioning Workflow Changelog	Account Mapping Lear more	Directory Service Field Use the following Directory Service field to supply the user name Directory Service field name * mail

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

## **Basic Settings**

- o 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.)

Enable SAML: ⑦ ④ Yes O No ShareFile Issuer / Entity ID: ⑦ https://subdomain sharefile.com/saml/info Your IDP Issuer / Entity ID: ⑦	Service Provider Confi Select the configuration metho Metadata Manual Configuration	guration         od specified by Service Provider, and then follow the instructions.         Manual Configuration         Fill out the form below with information given by your Service Provider. Be sure to sa         ShareFile Issuer / Entity ID (i)
https://aan0092.my.centrify.com/471dce39-34		https://subdomain.sharefile.com/saml/info
X.509 Certificate: ⑦ Saved <u>Change</u> Login URL: ⑦ https://abb0471.my.centrify.com/run?appkey= Logout URL: ⑦	Identity Provider Configura Configure your Your IDP Issuer / Ent Metadata Manual Configuration	ity ID and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Config         Manual Configuration         f your SAML Service Provider provides a SAML SSO configuration screen, copy the applicable IdP Config         SAML Service Provider requires you to send IdP Configuration values, copy them from below and ser         Your IDP Issuer / Entity ID ()         https://aan00992.my.centrify.com/471dce39-3404-4c07-a35c-e3be312b62         Copy
		.ogin URL ① https://abb0471.my.centrify.com/run?appkey=0e105117-8cdf-4d52-8 Copy

Require SSO Login: Optional
(After single sign on is successfully validated, checking <b>Yes</b> for this option <u>will</u>
require all non-admin Employees to log in using Idaptive. Admins can login
using Idantive or email address and their ShareFile password )
using happive of email datess and then share he password.
SSO IB Pango: Ontional
(Limit requiring non admin Employees to legin from a specific ID range
(Limit requiring non-admin Employees to login from a specific iP range.
Employees outside of this specified range <u>will not be required</u> 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
he available)
SD initiated Auth Contact: Salast Decaward Drotacted Transport
Sr-initiated Auth Context. Select Password Protected Transport.
Active Profile Cookies: Leave blank
<ul> <li>Click Save</li> </ul>

	Optional Settings
	Require SSO Login: ③
	SSO IP Range: ⑦
	SP-Initiated SSO certificate: ⑦
	Enable Web Authentication: ③
	● Yes ○ No SP-Initiated Auth Context: ⑦
	Password Protected Transport $\checkmark$ Minimum $\checkmark$
	Active Profile Cookies: ⑦
	Save Cancel
14.	est successful authentication by going to ShareFile URL: <u>ttps://subdomain.sharefile.com</u> and click <b>Sign in</b> under <b>Company Employee Sign</b>
	Citrix <b>Share</b> File
	Company Employee Sign In Sign In
	ShareFile is a safe, secure method for sharing files. To access, use your Active Directory credentials.
	Password
	Sign In     Sign In       Remember Me     Forgot Password?

