



# Content Collaboration: Single Sign-On Configuration Guide

## Citrix Endpoint Management



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.

## Configure ShareFile Single Sign-On with Endpoint Management 10

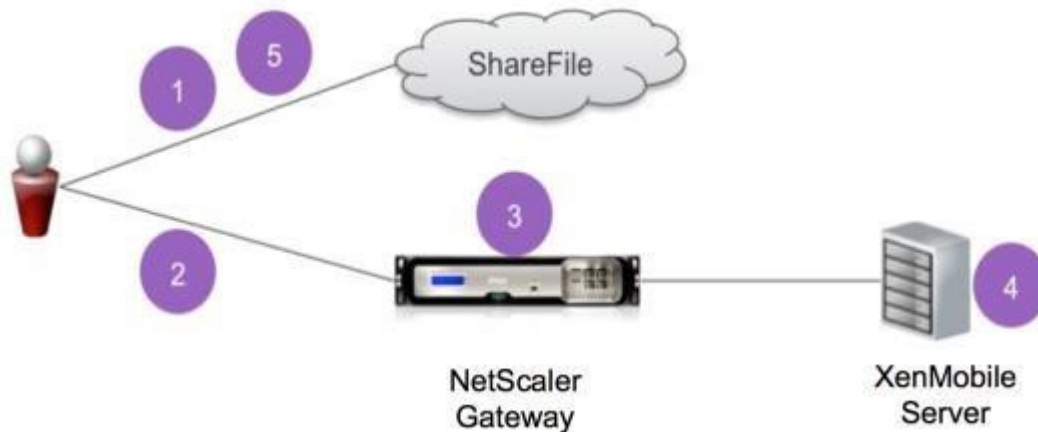
You can configure Citrix Endpoint Management server and NetScaler Gateway to function as a SAML identity provider for ShareFile. In this configuration, a user logging on to ShareFile using a web browser or other ShareFile clients is redirected to the Endpoint Management environment for user authentication. After successful authentication by Endpoint Management, the user receives a SAML token that is valid for logon to their ShareFile account.

### Contents

Configure ShareFile Single Sign-On with Endpoint Management 10 .....	3
Authentication Flow .....	4
System requirements .....	4
Prerequisites .....	6
Configure SAML SSO for ShareFile MDX Apps.....	6
Configure NetScaler Gateway.....	7
Disable Home Page Redirection .....	7
Create a ShareFile session policy and request profile .....	8
Configure policies on the NetScaler Gateway virtual server .....	11
Configure SAML for non-MDX ShareFile Apps.....	13
Modify the ShareFile.com single sign-on settings.....	14
Validate your configuration.....	15

## Authentication Flow

The following diagram represents the flow of events for user authentication when Endpoint Management is used as a SAML identity provider.



1. A user navigates to <https://subdomain.sharefile.com/saml/login>.
2. ShareFile redirects to [https://NSGatewayFQDN/cginfra/https/Endpoint Management server:8443/samlsp/webssp.do...](https://NSGatewayFQDN/cginfra/https/Endpoint%20Management%20server:8443/samlsp/webssp.do...)
3. NetScaler Gateway displays a log on form to the user, who supplies ShareFile log on information.
4. The authenticated user is logged on to the Endpoint Management server through single sign-on. Endpoint Management server silently returns a SAML assertion to the user.
5. The SAML assertion is passed to [subdomain.sharefile.com](https://subdomain.sharefile.com) to complete the authentication. The user is then presented with their ShareFile folders at [subdomain.sharefile.com](https://subdomain.sharefile.com).

All ShareFile clients can leverage Endpoint Management for user authentication using this deployment.

## System requirements

The following NetScaler, Endpoint Management Server and ShareFile client versions are required to support using Endpoint Management as a SAML identity provider:

Component	Minimum Version
NetScaler Gateway	10.5
Endpoint Management Server	10.0
ShareFile Sync for Windows ShareFile	2.8
Plugin for Microsoft Outlook ShareFile	2.1.20
Sync for Mac OS	1.7
ShareFile app for iPad	2.1.2
ShareFile app for iPhone	2.1.1

ShareFile app for Android Tablet	2.3
ShareFile app for Android Phone	2.3

## Prerequisites

- A working configuration of NetScaler Gateway and Endpoint Management server, which are configured.

## Configure SAML SSO for ShareFile MDX Apps

You can use the Endpoint Management Server along with SecureHub to single sign-on to ShareFile MDX wrapped applications.

In this scenario, Worx Home obtains a SAML token for the ShareFile login using Endpoint Management server as an IDP.

1. Log onto the Endpoint Management Server using the URL **https://<Endpoint Management Server>:4443**

2. Go to **Configure > ShareFile**.

3. Enter your ShareFile subdomain and choose the delivery groups that you wish to assign to the ShareFile MDX application. Only users in the delivery groups selected here will be able to use the Endpoint Management Server to SSO. In the **ShareFile Administrator Account Logon**, enter the ShareFile administrator account and save the settings. The Endpoint Management server will talk to ShareFile and save the SAML SSO settings in the ShareFile control plane.

### ShareFile ▼

Configure settings to connect to the ShareFile account and administrator service account for user account management.

Domain \*

Assign to delivery groups

- AllUsers
- [blurred]
- [blurred]
- [blurred]
- [blurred]
- [blurred]
- [blurred]
- [blurred]
- [blurred]
- [blurred]

### ShareFile Administrator Account Logon

User name \*

Password \*

At this point SAML configuration for MDX apps is configured. If you only wish to allow access to ShareFile using the MDX wrapped applications, you can ignore the Part 2 and 3. However if you wish to configure access for non-MDX ShareFile clients such as the web-site, Outlook Plug-In or the sync clients, please continue to Part 2.

**NOTE: Configuring ShareFile MDX SSO also enables the user provisioning in Endpoint Management server. Any users that are a part of the selected roles and do not have an account in ShareFile, will automatically be provisioned by Endpoint Management server based on how they first access ShareFile. To learn more about how Endpoint Management server provisions ShareFile users, please read the [ARTICLE posted here](#).**

## Configure NetScaler Gateway

The following configuration is required on NetScaler to support using Endpoint Management as a SAML identity provider:

1. Disable home page redirection
2. Create a ShareFile session policy and profile
3. Configure policies on the NetScaler Gateway virtual server.

## Disable Home Page Redirection

You must disable the default behavior for requests that come through the /cginfra path, so that the original requested internal URL is served to the user instead of the configured home page.

1. Edit the settings for the NetScaler Gateway virtual server that is used for Endpoint Management logins. Go to **Other Settings** and clear the checkbox labeled “**Redirect to Home Page**”:

### NetScaler 12.1

The screenshot shows the 'Other Settings' configuration window for a NetScaler virtual server. The 'Redirect to Home page' checkbox is unchecked. The 'ShareFile' field is populated with 'xms.citrix.lab:8443' and the 'AppController' field is populated with 'https://xms.citrix.lab:8443'. The 'Listen Policy Expression' field is empty, and the 'Listen Priority' field is also empty. The 'ICMP Virtual Server Response\*' and 'RHI State\*' dropdown menus are set to 'Passive'. An 'OK' button is visible at the bottom left of the window.

2. For **ShareFile** setting, add the internal server name and port of your Endpoint Management server. For example: **xms.citrix.lab:8443**.
3. For the AppController, enter the address of your Endpoint Management Server as shown above.

This configuration authorizes requests to the specified URL through the /cginfra path.

## Create a ShareFile session policy and request profile

1. In the Citrix Gateway configuration utility, select **Citrix Gateway > Policies > Session** in the left navigation pane.
2. To create a new session policy: On the **Policies** tab, click **Add...** and then enter **ShareFile\_Policy** as the name.
3. To create a new action, click **Add...**. The Create NetScaler Gateway Session Profile screen opens.
4. In **Name**, enter **ShareFile\_Profile** as the session profile name.
5. On the **Client Experience** tab:
  - For **Home Page**, enter **none**.
  - For **Session Time-out**, enter **1**.
  - Enable **Single Sign-on to Web Applications**.
  - For **Clientless Access** set to **On**.
  - **Clientless Access Persistent Cookie** set to **Allow**.
  - For **Credential Index**, select **PRIMARY**.

### Configure Citrix Gateway Session Profile

Network Configuration   **Client Experience**   Security   Published

Accounting Policy

Display Home Page

Home Page  
  Override Global

URL for Web-Based Email  
  Override Global

Split Tunnel\*  
  Override Global

Session Time-out (mins)  
  Override Global

Client Idle Time-out (mins)  
  Override Global

Clientless Access\*  
  Override Global

Clientless Access URL Encoding\*  
  Override Global

Clientless Access Persistent Cookie\*  
  Override Global

### Configure Citrix Gateway Session Profile

java  Override Global

Windows Plugin Upgrade  
  Override Global

Linux Plugin Upgrade  
  Override Global

MAC Plugin Upgrade  
  Override Global

AlwaysON Profile Name  
    Override Global

Single Sign-on to Web Applications  Override Global

Credential Index\*  
  Override Global

KCD Account  
    Override Global

Single Sign-on with Windows\*  
  Override Global

Client Cleanup Prompt\*  
  Override Global

**Advanced Settings**

6. On the **Security** tab set **Default Authorization Action** to **Allow**.



### Configure Citrix Gateway Session Profile

Name

Unchecked Override Global check box indicates that the value is inherited from Global Citrix Gateway Parameters.

Network Configuration
Client Experience
Security

Override Global

Default Authorization Action\*  
  Override Global

Secure Browse\*  
  Override Global

Smartgroup  
  Override Global

[Advanced Settings](#)

7. On the **Published Applications** tab:

- For **ICA Proxy**, select **ON**.
- In **Web Interface Address**, enter your **Endpoint Management server URL** as shown.
- In **Single Sign-on Domain**, enter your **Active Directory domain name**.

### Create Citrix Gateway Session Profile

Name\*  
 ?

Unchecked Override Global check box indicates that the value is inherited from Global Citrix Gateway Parameters.

Network Configuration
Client Experience
Security
Published Applications
Remote Desktop
PCoIP

Override Global

ICA Proxy\*  
  Override Global ?

Web Interface Address  
  Override Global ?

Web Interface Address Type\*

Web Interface Portal Mode\*  
  Override Global ?

Single Sign-on Domain  
  Override Global ?

Citrix Receiver Home Page  
  Override Global

Account Services Address  
  Override Global

Create
Close

**NOTE to IT Admins:** When configuring the NetScaler Gateway Session Profile above, the domain suffix entered into

the **Single Sign-On Domain** field must match the **Endpoint Management domain alias** defined in LDAP.

8. Click **Create** to finish defining the session profile.
9. For the **ShareFile\_Policy** expression, switch to **Classic Policy** and click **Expression Editor**.
10. Specify the expression as shown in the screen shot, using a **Value** of **NSC\_FSRD** and a **Header Name** of **COOKIE**.

VPN Virtual Server Session Policy Binding / Policy Binding / Session Policies / Create Citrix Gateway Session Policy / Add Expression

### Add Expression ✕

Select Expression Type:

Flow Type

Protocol

Qualifier

Operator

Value\*

Header Name\*

Length

Offset

11. Click **Done**, click **Create**, and then click **Close**.

### Create Citrix Gateway Session Policy ✕

Name\*

Profile\*

Advanced Policy  Classic Policy

Expression\* [OPSWAT EPA Editor](#) [Expression Editor](#)

REQ:HTTP:HEADER COOKIE CONTAINS NSC\_FSRD

## Configure policies on the NetScaler Gateway virtual server

1. In the NetScaler Gateway configuration utility, select **NetScaler Gateway > Virtual Servers** in the left navigation pane.
2. In the Details pane, click your NetScaler Gateway virtual server and then click **Edit**.
3. Go to the **Configured policies > Session policies** and click **Add binding**
4. Select the **ShareFile\_Policy**

5. Edit the auto-generated Priority number for the inserted policy so that it has the lowest number (highest priority) compared to any other policies listed. For example:

VPN Virtual Server Session Policy Binding

### VPN Virtual Server Session Policy Binding

▼

<input type="checkbox"/>	Priority	Policy Name	Expression
<input type="checkbox"/>	10	ShareFile_Policy	REQ.HTTPHEADER Cookie CONTAINS NSC_FSRD
<input type="checkbox"/>	100	PL_OS_NETSCALER_GATEWAY_VIP	REQ.HTTPHEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTPHEADER X-Citrix-Gate
<input type="checkbox"/>	100	PL_AG_PLG_NETSCALER_GATEWAY_VIP	REQ.HTTPHEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTPHEADER Referer I

6. Click Done and then save the running NetScaler configuration.

## Configure SAML for non-MDX ShareFile Apps

As a result of configuring Endpoint Management server with ShareFile account details, your ShareFile single sign-on settings are populated with a SAML login URL which points to an internal Endpoint Management server address. In order to allow non-MDX ShareFile Apps to use Endpoint Management server as a SAML IDP, you must edit that URL and also enable web authentication, as follows.

### 3.1 Locate the internal app name for ShareFile

Find the internal app name for your ShareFile configuration using the following steps.

1. Log onto the Endpoint Management server admin tool using the URL **https://<Endpoint Management server>:4443/OCA/admin/** and choose the **Configuration** view:

**NOTE: The OCA is case sensitive and needs to be in uppercase.**



2. Select the **Applications > Applications** node and note the **Application Name** for the app whose **Display Name** is "ShareFile".



Application Name	Display Name	Description
activedirectory	activedirectory	
AmericanExpress	AmericanExpress	Online access to world-class card, financial, insu...
Fidelity	Fidelity	Your Personal Investing Resource
LinkedIn	LinkedIn	Business-oriented social networking site
<b>ShareFile_SAML</b>	<b>ShareFile</b>	<b>Online storage for business</b>
MobileApp11	ShareFile_220	ShareFile 2.2.0
MobileApp13	ShareFile_iPhone_303	ShareFile 3.0.3
MobileApp14	ShareFile_iPhone_304	ShareFile 3.0.4

## Modify the ShareFile.com single sign-on settings.

1. Log on to your account (<https://subdomain.sharefile.com>) as a **ShareFile administrator**.
2. In the ShareFile web interface, navigate to **Admin Settings > Security > Login & Security Policy**, and scroll down to the Single Sign-On settings.
3. Edit the Login URL. Here is a sample Login URL that is populated as a result of the Endpoint Management server configuration:

[https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile\\_SAML\\_SP&req type=1](https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&req type=1)

### Basic Settings

Enable SAML: [?](#)  
 Yes  No

ShareFile Issuer / Entity ID: [?](#)

Your IDP Issuer / Entity ID: [?](#)

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

Login URL: [?](#)

Logout URL: [?](#)

- a. Insert the external FQDN of the NetScaler Gateway virtual server plus `/cginfra/https/` before the Endpoint Management server FQDN and `:8443` after the FQDN. For example:
  - [https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile\\_SAML\\_SP&reqtype=1](https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1)
- b. Change the parameter `&app=ShareFile_SAML_SP` to use the internal name of the ShareFile application that you determined in section 2.1. The internal name is **ShareFile\_SAML** by default, but with each change to your configuration the internal name changes to append a number (ShareFile\_SAML2, ShareFile\_SAML3, and so on).
  - [https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile\\_SAML&reqtype=1](https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1)
- c. Add `&nssso=true` to the end of the URL. For example:
  - [https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile\\_SAML&reqtype=1&nssso=true](https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true)

**Important Note:** Each time you edit or recreate the ShareFile app, the internal application name is updated with a number appended to the name. At this time, you must also update the Login URL in the ShareFile website to reflect the updated application name. The example below shows how the Login URL need to change when the internal application name changes from “ShareFile\_SAML” to “ShareFile\_SAML2”

4. Under **Optional Settings**, click the **Enable Web Authentication** check box.

## 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: [?](#)

5. Click **Save**.

## Validate your configuration

1. Point your browser to **<https://subdomain.sharefile.com/saml/login>**.

- You should be redirected to the NetScaler Gateway logon form.

2. Log in with user credentials that are valid for the NetScaler Gateway and Endpoint Management server environment you configured.

- Your ShareFile folders at subdomain.sharefile.com should appear.