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.

2. ShareFile redirects to https://NSGatewayFQDN/cginfra/https/Endpoint Management server: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 to complete the authentication. The user is then presented with their ShareFile folders at 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:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler Gateway</td>
<td>10.5</td>
</tr>
<tr>
<td>Endpoint Management Server</td>
<td>10.0</td>
</tr>
<tr>
<td>ShareFile Sync for Windows ShareFile</td>
<td>2.8</td>
</tr>
<tr>
<td>Plugin for Microsoft Outlook ShareFile</td>
<td>2.1.20</td>
</tr>
<tr>
<td>Sync for Mac OS</td>
<td>1.7</td>
</tr>
<tr>
<td>ShareFile app for iPad</td>
<td>2.1.2</td>
</tr>
<tr>
<td>ShareFile app for iPhone</td>
<td>2.1.1</td>
</tr>
<tr>
<td>ShareFile app for Android Tablet</td>
<td>2.3</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>ShareFile app for Android Phone</td>
<td>2.3</td>
</tr>
</tbody>
</table>
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.

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.
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

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.

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**.

**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**.

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

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".

![Endpoint Management server login interface](image1.png)

![XenMobile app controller interface](image2.png)
Modify the ShareFile.com single sign-on settings.

1. Log on to your account (https://subdomain.sharefile.com) as a ShareFile administrator.


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

   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:


   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).


   c. Add &nssso=true to the end of the URL. For example:

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
  - HTTP Redirect with no signature
- Enable Web Authentication
  - Yes
  - No
- SP-Initiated Auth Context
  - User Name and Password
  - Minimum
- 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.