Single Sign On for ShareFile with NetScaler Unified Gateway

Deployment Guide

This deployment guide focuses on defining the process for enabling Single Sign On into Citrix ShareFile with Citrix NetScaler Unified Gateway.
# Table of Contents

- Introduction 3
- Configuration details 4
- NetScaler features to be enabled 4
- Solution description 5
- Step 1: Configure ShareFile 5
- Step 2: Configure NetScaler 7
  - To configure domain authentication 8
  - To import the ShareFile SP-Certificate onto the NetScaler 10
  - To configure the SAML IDP Policy and Profile 11
  - To configure your Unified Gateway Virtual Server 13
- Validate the configuration 15
- Conclusion 15
Citrix NetScaler Unified Gateway provides users with secure remote access to business applications deployed in the data center or a cloud across a range of devices including laptops, desktops, thin clients, tablets and smart phones. It provides a consolidated infrastructure, simplifies IT and reduces TCO of the data center infrastructure.

ShareFile is a cloud-based file sharing service that enables users to exchange documents easily and securely. ShareFile users can send large documents by email, securely handle document transfers to third parties, and access a collaboration space from desktops or mobile devices. ShareFile provides users with a variety of ways to work, including a web-based interface, mobile clients, desktop tools, and integration with Microsoft Outlook.

Introduction

This guide focuses on defining the guidelines for enabling Citrix ShareFile single sign on with Citrix NetScaler.

ShareFile is offered under several business plans. ShareFile Enterprise provides enterprise-class service and includes StorageZones Controller and the User Management Tool.
Configuration Details
The table below lists the minimum required software versions for this integration to work successfully. The integration process should also work with higher versions of the same.

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Required Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler</td>
<td>11.1, Enterprise/Platinum License</td>
</tr>
<tr>
<td>ShareFile Sync for Windows</td>
<td>3.2</td>
</tr>
<tr>
<td>ShareFile Plugin for Microsoft Outlook</td>
<td>3.3.3</td>
</tr>
<tr>
<td>ShareFile app for iPad</td>
<td>3.2.8</td>
</tr>
<tr>
<td>ShareFile app for iPhone</td>
<td>3.2.8</td>
</tr>
<tr>
<td>ShareFile app for Android Tablet</td>
<td>3.6.4</td>
</tr>
<tr>
<td>ShareFile app for Android Phone</td>
<td>3.6.4</td>
</tr>
</tbody>
</table>

NetScaler features to be enabled
The essential NetScaler features that need to be enabled are explained below. Please ensure these features are enabled in the NetScaler system.

- Load balancing
- SSLVPN

Here is a quick explanation of how these features work.

Load balancing
NetScaler load balancing evenly distributes requests to backend servers. Multiple algorithms (for example, LEASTCONNECTION and ROUNDROBIN) are supported to provide efficient load balancing logic for every application server.

SSLVPN
The SSLVPN feature is required for the use of Unified Gateway. It adds support for the creation of SSL-based VPN virtual servers for secure enterprise application access.
Solution description
The process for enabling SSO into ShareFile with NetScaler consists of two parts – configuration of the ShareFile portal and configuration of the NetScaler appliance. To begin with, you should complete the required configuration on the ShareFile portal in order for the ShareFile SP Certificate to be created. This should then be imported on the NetScaler and bound to the UG Virtual Server that will host the SAML IDP (Identity Provider) policy.

The following instructions assume that you have already created the appropriate external and/or internal DNS entries to route authentication requests to a NetScaler-monitored IP address, and that an SSL certificate has already been created and installed on the appliance for the SSL/HTTPS communication.

Step 1: Configure ShareFile
(Here, please replace the <subdomain> placeholder with your own ShareFile domain name.)
• In a web browser, log in to your ShareFile account at https://<subdomain>.sharefile.com with a user account that has admin rights
• Select the Admin link near the top of the page
• On the left side of the browser window, select the Configure Single Sign-On option
• Under Basic Settings, check the Enable SAML checkbox.
• In the ShareFile Issuer / Entity ID field enter: https://<subdomain>.sharefile.com/saml/info
• In the “Your IDP Issuer / Entity ID” field enter the FQDN (Fully Qualified Domain Name) of your UG Virtual server: example: https://ugvip.mycompany.com
• In the Login URL field enter the URL that users will be redirected to when using SAML. This is typically https://ugvip.mycompany.com/saml/login
• In the Logout URL field enter the logout URL that will end the user’s session when the logout option is selected in the ShareFile Web UI. An example for NetScaler would be https://ugvip.mycompany.com/cgi/tmilogout (where ugvip.mycompany.com is the public FQDN for your NetScaler UG vserver)
For the X.509 Certificate entry shown in the screenshot above, you need to export the SSL certificate from the NetScaler appliance that will receive and respond to your UG traffic. In the example above, this appliance is specified by the ugvip.mycompany.com FQDN. Use the following procedure to export this certificate:

1. Login to your NetScaler appliance via the Configuration Utility.
2. Select Traffic Management > SSL
3. On the right, under Tools, select Manage Certificates / Keys / CSR’s

From the Manage Certificates window, browse to the certificate you will be using for your UG Virtual Server. Select the certificate and choose the Download button. Save the certificate to a location of your choice.

5. From the downloaded location, right-click on the certificate and open it with a text editor such as Notepad. (**Hint: Open Notepad and drag the file into the blank space**).

6. Copy the entire contents of the certificate to your clipboard.

7. In your web browser, on the Single sign-on / SAML 2.0 Configuration page select the Change option for X.509 Certificate.

8. Paste the contents of the certificate you copied to your clipboard into the window. (screenshot on the next page)
10. Select **Save**.
11. Under Optional Settings, check the box to Require SSO Login if you want all Employee ShareFile users to be required to use their Active Directory (AD) credentials to log on to ShareFile. (This will not affect Client users)
12. From the drop-down list next to SP-Initiated SSO Certificate, select HTTP Post (2048 bit certificate)
13. Select the check box to Enable Web Authentication
14. Under the SP-Initiated Auth Context, choose Unspecified
15. Select the Save button at the bottom of the screen.

**Step 2: Configure NetScaler**

The following configuration is required on the NetScaler appliance for it to function as a SAML identity provider:

- LDAP authentication policy and server for domain authentication
- SSL certificate with external and internal DNS configured for the FQDN presented by the certificate (Wildcard certificates are supported)
- ShareFile Service Provider (SP) Certificate
- SAML IDP policy and profile
- UG virtual server

This guide only covers the LDAP configuration, the ShareFile SP certificate importation on the NetScaler, the SAML IDP settings, and the UG virtual server configuration. The SSL certificate and DNS configurations should be in place prior to setup.
To configure domain authentication

For domain users to be able to log on to the NetScaler appliance by using their corporate email addresses, you must configure an LDAP authentication server and policy on the appliance and bind it to your UG VIP address. (Use of an existing LDAP configuration is also supported)

1. In the NetScaler configuration utility, in the navigation pane, select NetScaler Gateway > – Policies > Authentication > LDAP.
2. To create a new LDAP policy: On the Policies tab click Add, and then enter ShareFile_LDAP_SSO_Policy as the name. In the Server field, click the '+' icon to add a new server. The Authentication LDAP Server window appears.
3. In the Name field, enter ShareFile_SSO_LDAP_Server.
4. Select the bullet for Server IP. Enter the IP address of one of your Active Directory domain controllers. (You can also point to a virtual server IP for the purpose of redundancy if you are load balancing domain controllers)
5. Specify the port that the NetScaler will use to communicate with the domain controller. Use 389 for LDAP or 636 for Secure LDAP (LDAPS).
6. Under Connection Settings, enter the base domain name for the domain in which the user accounts reside within the Active Directory (AD) for which you want to allow authentication. The example below uses OU=ShareFile,DC=domain,DC=com.
7. In the Administrator Bind DN field, add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. A service account is advisable, so that there will be no issues with logins if the account that is configured has a password expiration.
8. Check the box for Bind DN Password and enter the password twice.
9. Under Other Settings: Enter mail as the Server Logon Name Attribute.
10. In the SSO Name Attribute field, enter UserPrincipalName.
### Connection Settings

- **Base DN (location of users)**
  
  OU=ShareFile,DC=mydomain,DC=com

- **Administrator Bind DN**
  
  serviceacct@mydomain.com

- **BindDN Password**
  
  Password field

- **Administrator Password**
  
  Password field

- **Confirm Administrator Password**
  
  Password field

### Other Settings

- **Server Logon Name Attribute**
  
  mail

- **Search Filter**
  
  Add filter

- **Group Attribute**
  
  `memberOf`

- **Sub Attribute Name**
  
  CN

- **SSO Name Attribute**
  
  UserPrincipalName

- **Security Type**
  
  - [ ] PLAINTEXT
  - [ ] TLS
  - [ ] SSL

- **Authentication**
  
  - [ ] User Required

- **Referrals**
  
  - [ ]

11. Click the Create button to complete the LDAP server settings.
12. For the LDAP Policy Configuration, select the newly created LDAP server from the Server dropdown list, and in the Expression field type, `ns_true`. This is the base expression that allows all traffic, but the end user can create very complex policies as well if necessary and utilize help from the frequently used expressions dropdown to build them.

![Create Authentication LDAP Policy](image)

13. Hit the Create button to complete the LDAP Policy and Server configuration.

To import the ShareFile SP-Certificate onto the NetScaler

Log in to your ShareFile account (which must have admin rights) at https://<subdomain>.sharefile.com. Select the Admin link near the top of the page. On the left side of the browser window, select the Configure Single Sign-On option. Under Optional Settings, next to SP-Initiated SSO Certificate, HTTP Post (2048 Bit Certificate) click View.

- Copy the entire certificate hash to your clipboard, and paste it into a text reader such as Notepad.
- Observe the formatting and remove any extra spaces or carriage returns at the end of the file, then save the text file as ShareFile_SAML.cer.
- Return to the web browser and click Cancel to ensure no changes are made to the ShareFile SSO settings.
- Navigate to the NetScaler Configuration Utility.
• Navigate to Traffic Management > SSL > Certificates
• Click Install
• In the Install Certificate window, enter a certificate-key pair name.
• For the Certificate File Name field, from the Browse drop-list, select Local and browse to the location at which you saved the ShareFile_SAML.cer file.

Select the file and click Install.

**To Configure the SAML IDP Policy and Profile**

For your users to receive the SAML token for logging on to ShareFile, you must configure a SAML IDP policy and profile, and bind them to the UG virtual server to which the users send their credentials.
Use the following procedure:

1. Open the NetScaler Configuration Utility and navigate to NetScaler Gateway > Policies > Authentication > SAML IDP
2. On the Policies Tab, select the Add button.
3. In the Create Authentication SAML IDP Policy Window, provide a name for your policy. (for example, ShareFile_SSO_Policy)
4. To the right of the Action field, click the ‘+’ icon to add a new action.
5. Provide a name (for example, ShareFile_SSO_Profile)
6. In the Assertion Consumer Service URL field, enter your ShareFile account URL followed by /saml/acs. (for example, https://subdomain.sharefile.com/saml/acs)
7. In the SP Certificate Name field, select the dropdown and browse to the ShareFile SP certificate you imported earlier and added as a certificate on the NetScaler appliance.
8. In the IDP Certificate Name field, browse to the certificate installed on the NetScaler that is will be used to secure your UG authentication Virtual Server.
9. In the Issuer Name field enter the URL for your UG traffic (for example – https://ugvip.mycompany.com)
10. In the Audience field, enter the URL for your ShareFile account (for example – https://<subdomain>.sharefile.com)
11. Click Create to complete the SAML IDP profile configuration and return to the SAML IDP Policy creation window
12. In the Expression field, add the following expression: HTTP.REQ.URL.CONTAINS("saml")
13. Click Create to complete the SAML IDP Configuration

To Configure your Unified Gateway (UG) Virtual Server

1. Select the Unified Gateway option in the Integrate with Citrix Products section on the navigation panel to initiate the Unified Gateway Configuration Wizard.
2. First, provide an appropriate name, IP address and port for the UG virtual server.
3. In the next step, provide a server certificate (if it is already present on the NetScaler) or install a new certificate that will be used as the server certificate for the UG virtual server.
4. Next, define the authentication mechanism to be used for the UG Virtual Server.
   **Note:** In the Wizard, only the most common authentication mechanisms are configured. Select Active Directory/LDAP and add the LDAP server configured earlier.
5. Set the Portal Theme to Default (or a theme of your choice) and click on Continue.
6. In the Applications section, select the pencil shaped icon on the top right, then the plus-shaped icon to add a new application. Select Web Application, then provide the ACS (Assertion Consumer Service) URL provided in the NetScaler SAML IDP policy earlier with an appropriate name.
7. Click on Done once the application has been added.
8. To add the SAML IDP policy to the Unified Gateway, navigate to the VPN Virtual Server listing (NetScaler Gateway>Virtual Servers) to find the virtual server created using the wizard (named UG_VPN_<UG vserver name>). Choose the option for editing the virtual server, then add the SAML IDP policy created earlier in the Advanced Authentication section.
After completing the UG configuration above, this is how the Dashboard screen of the UG vserver will look:

### Dashboard

- **Total AAA Sessions**:
  - Time: 04:00:00 to 04:00:30
  - Sessions:
    - Active AAA Sessions: 0
    - Active ICA Sessions: 0

- **Packet CPU Usage**: 1%
- **Memory Usage**: 20%

### Authentication Virtual Server

**Basic Settings**

- **Name**: AAA_Vserver
- **IP Address**: 192.168.1.149
- **Port**: 443

**Certificates**

- 1 Server Certificate
- No CA Certificate

**Advanced Authentication Policies**

- No Authentication Policy

**Basic Authentication Policies**

- Primary Authentication
  - 1 LDAP Policy
  - 1 SAML IDP Policy
Validate the configuration

Point your browser to https://<subdomain>.sharefile.com/saml/login. You should be redirected to the NetScaler UG logon form.

Log in with user credentials that are valid for the NetScaler environment you just configured. Your ShareFile folders at <subdomain>.sharefile.com should appear.

Conclusion

NetScaler Unified Gateway enables a secure and seamless experience with ShareFile by enabling single sign on into ShareFile accounts, thus avoiding the need for users to remember multiple passwords and user IDs, while reducing the administrative overhead involved in maintaining these deployments.