Content Collaboration: Single Sign-On Configuration Guide

Netscaler ADC

Last Revised: May 2019

LEGAL NOTICE

Configure ShareFile Single Sign-On with NetScaler

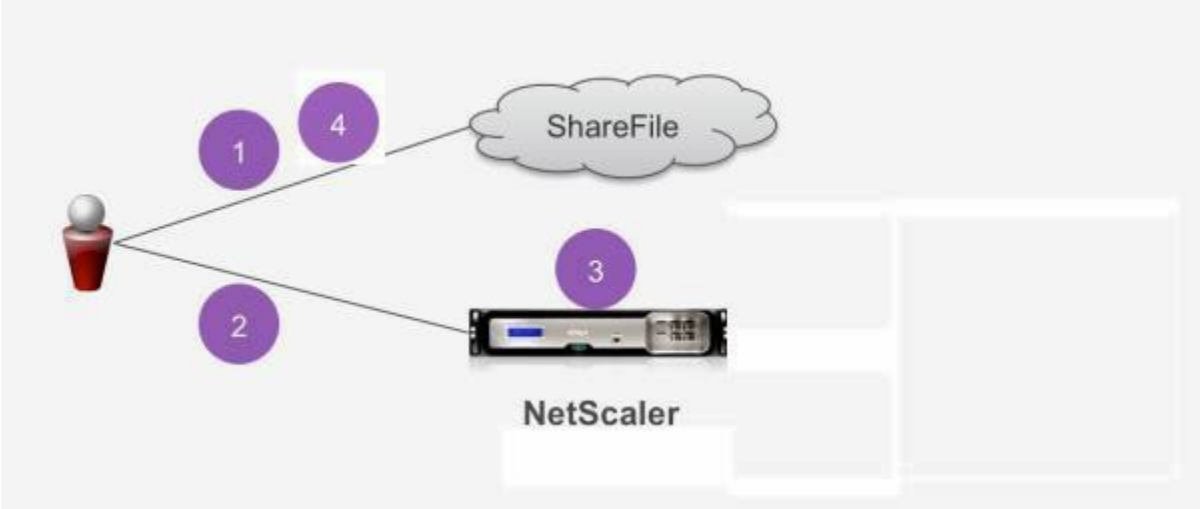
You can configure Citrix NetScaler ADC using the AAA feature to function as a SAML identity provider for ShareFile.

In this configuration, a user logging on to ShareFile using a web browser or other ShareFile clients is redirected to a virtual server on the NetScaler with a SAML IP Policy enabled for user authentication. After successful authentication via the NetScaler the user receives a SAML token that is valid for logon to their ShareFile account.

Contents

Authentication Overview

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



1. A user navigates to https://subdomain.sharefile.com/saml/login.
2. ShareFile redirects to https://NS_AAA_FQDN/vpn/tmindex.html.
3. NetScaler displays a log on form to the user, who supplies ShareFile log on information in the form of an email address. The authenticated user is logged on and the NetScaler silently returns a SAML assertion to the user.
4. 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.

Both web browsers and ShareFile clients can leverage NetScaler for user authentication using this deployment.

System requirements

The following NetScaler ADC and ShareFile client versions and above are required to support using NetScaler as a SAML identity provider:

Component	Version
NetScaler	11.1 50.x
ShareFile Sync for Windows	3.11
ShareFile Plugin for Microsoft Outlook	4.3
ShareFile Desktop App	1.11
ShareFile Drive Mapper	3.5
ShareFile app for iPhone/iPad	5.x
ShareFile app for Android	5.x
ShareFile app for Windows UWP	4.9

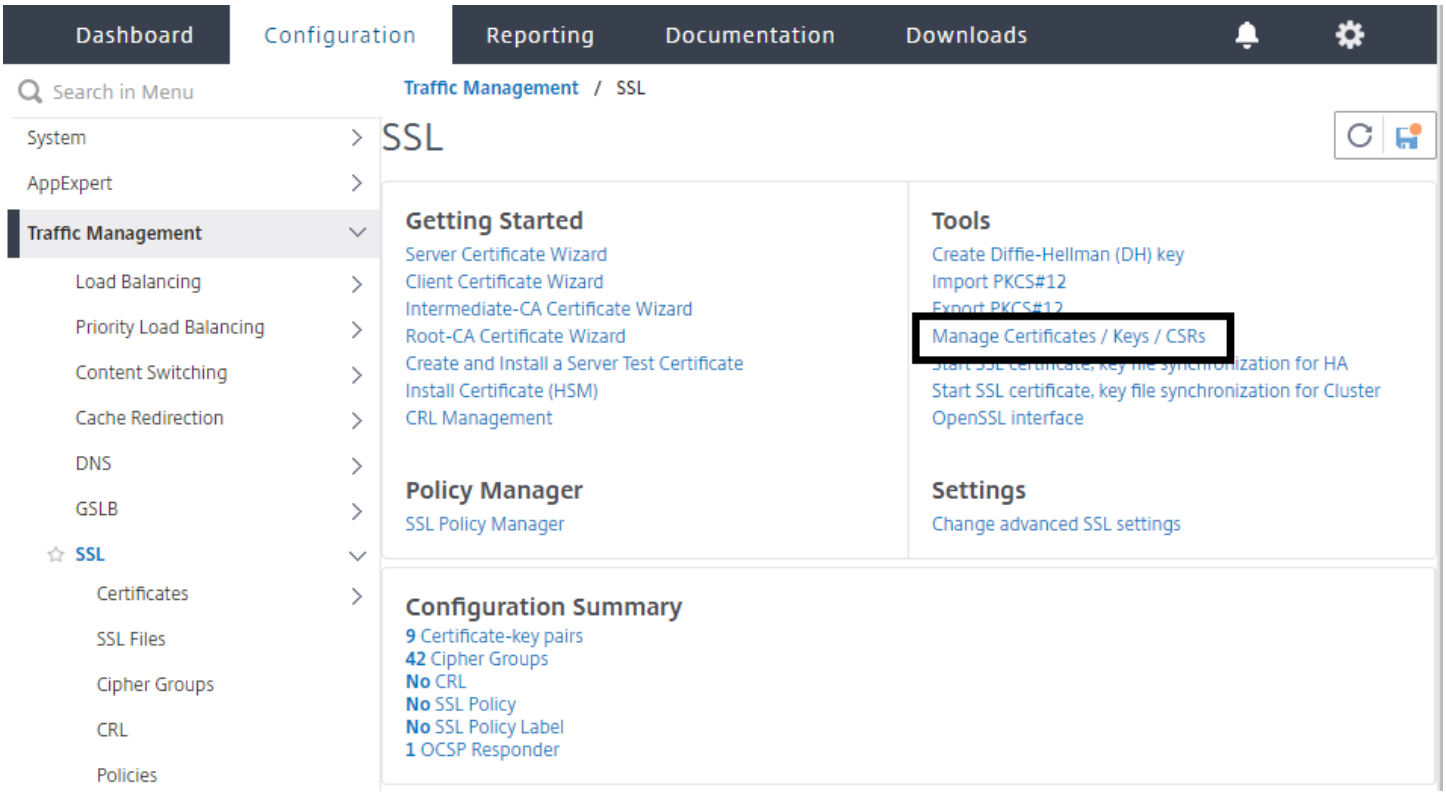
The configuration of ShareFile SSO is required as the first step in order for the ShareFile SP Certificate to be created so we can import it on the NetScaler and bind it to your AAA Virtual Server. It will be assumed for the purposes of this document that you have already created the appropriate external and/or internal DNS entries to route authentication requests an IP address that the NetScaler will listen on, and that an SSL certificate has already been created and installed on the NetScaler for the SSL/HTTPS communication.

Step 1: Configure ShareFile

- Login to your ShareFile account at https://subdomain.sharefile.com with a user account that has admin rights
- Select the **Settings > Admin Settings** links near the left side of the page
- Select **Security > Login & Security Policy**, scroll down and select the **Single Sign-On** Configuration option
- Under **Basic Settings**, check the **Enable SAML**.
- In the **ShareFile Issuer / Entity ID** field enter: https://*subdomain*.sharefile.com/saml/acs
- In the **Login URL** field enter the URL that users will be redirected to when using SAML. Example: https://aaavip.mycompany.com/saml/login
- In the **Logout URL** field enter the logout URL that will expire the users session upon selecting the logout option in the ShareFile Web UI. Example: https://aaavip.mycompany.com/cgi/tmlogout

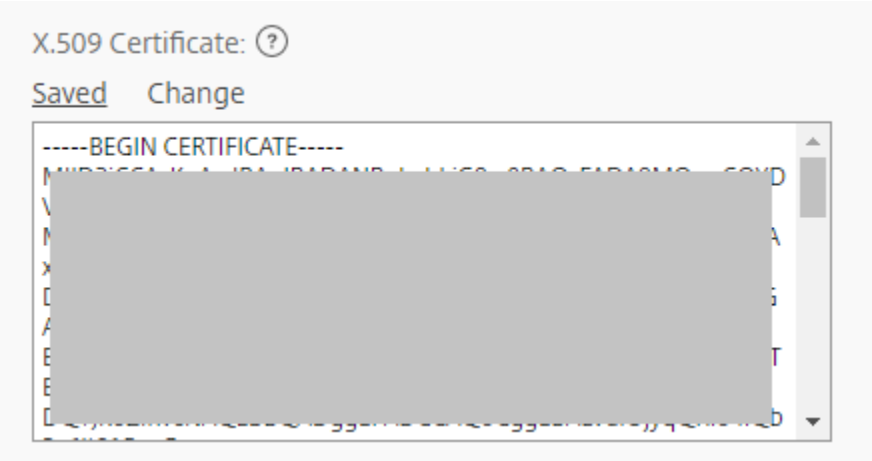
- For the X.509 Certificate, we will need to export the SSL certificate from your NetScaler appliance that is going to be answering for your AAA traffic. In the example above, this is referenced as being assigned the following FQDN: aaavip.mycompany.com. Follow the below steps in order to export this certificate.

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



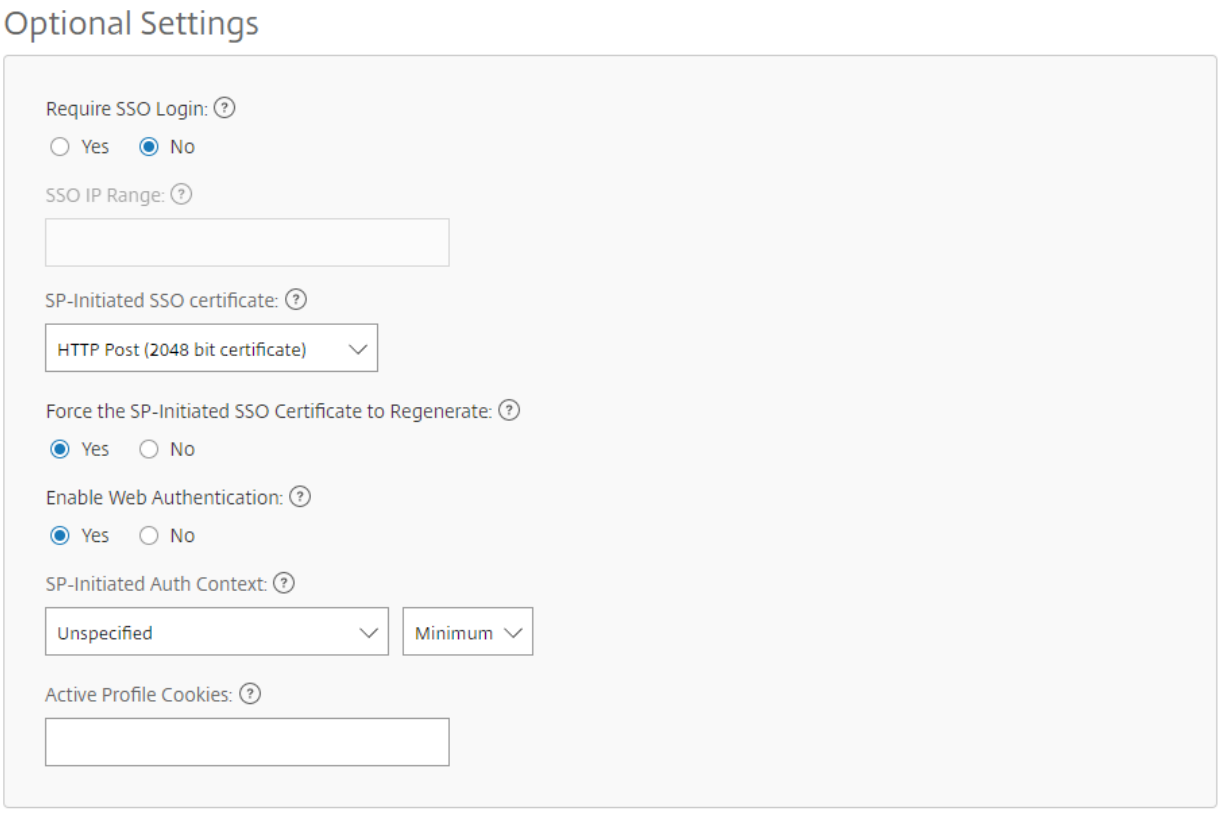
1. From the **Manage Certificates** window, browse to the certificate you will be using for your AAA Virtual Server. Select the certificate and choose the **Download** button. Save the certificate to a location of your choice.
2. From the downloaded location, **right click** on the certificate and open it with a text editor such as Notepad. (**Hint: Open Notepad and drag the file into the blank space**).
3. Copy the entire contents of the certificate to your clipboard.
4. Navigate back to your ShareFile account via the web browser.
5. For the **X.509 Certificate** select **Change**.

Paste the contents of the certificate you copied to your clipboard into the window.



Select **Save**.

- Under **Optional Settings**, switch **Require SSO Login** to yes if you wish all Employee ShareFile users to be required to use their AD credentials to logon to ShareFile. (**This will not affect Client users**)
- Next, select the dropdown list next to **SP-Initiated SSO Certificate**. From the list, select **HTTP Post (2048 bit certificate)**
  Check **Yes** to **Force the SP-Initiated SSO Certificate to Regenerate**
- Check **Yes** to **Enable Web Authentication**
- Under the **SP-Initiated Auth Context**, choose **Unspecified**



- Select the **Save** button at the bottom of the screen.

Step 2: Configure NetScaler

1. The following configuration is required on NetScaler for it to be supported as a SAML identity provider:
2. LDAP Authentication Policy and Server for domain authentication
3. SSL Certificate with External / Internal DNS configured accordingly to the FQDN being presented by the certificate (Wildcard certificates are supported)**
4. ShareFile SP Certificate
5. SAML IDP Policy and Profile
6. AAA Virtual Server

**For the purposes of this material, we will be covering the LDAP configuration, the ShareFile SP Certificate importation on the NetScaler, the SAML IDP settings, and the AAA Virtual Server configuration. The SSL Certificate and DNS configurations should be in place prior to setup.

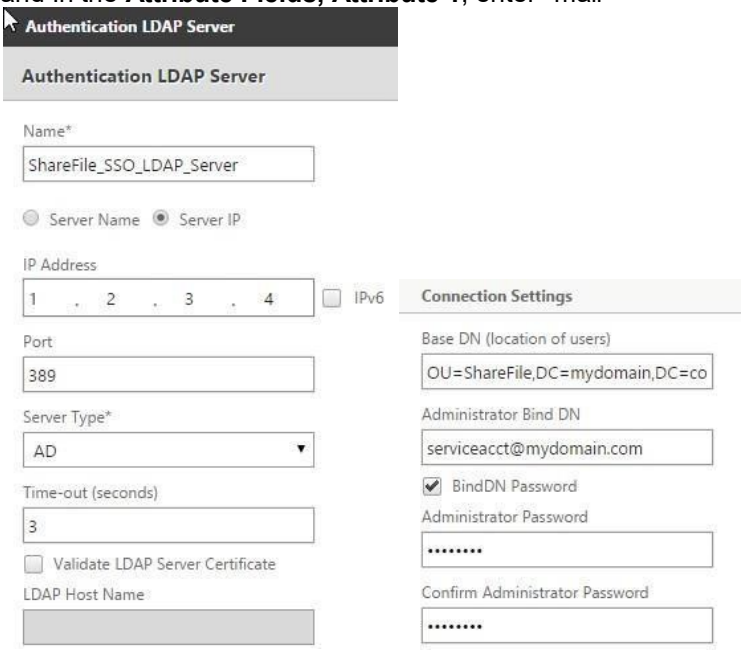
To configure domain authentication

In order for domain users to be able to logon to NetScaler using their corporate email address, you must configure an LDAP Authentication Server and Policy on the NetScaler and bind it to your AAA VIP. (Use of an existing LDAP configuration is also supported)

1. In the NetScaler configuration utility, select **Security > AAA – Application Traffic > Polices > Authentication > Advanced Policies > Policy > LDAP** in the left navigation pane.
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 **Action Type**, Select **LDAP**.

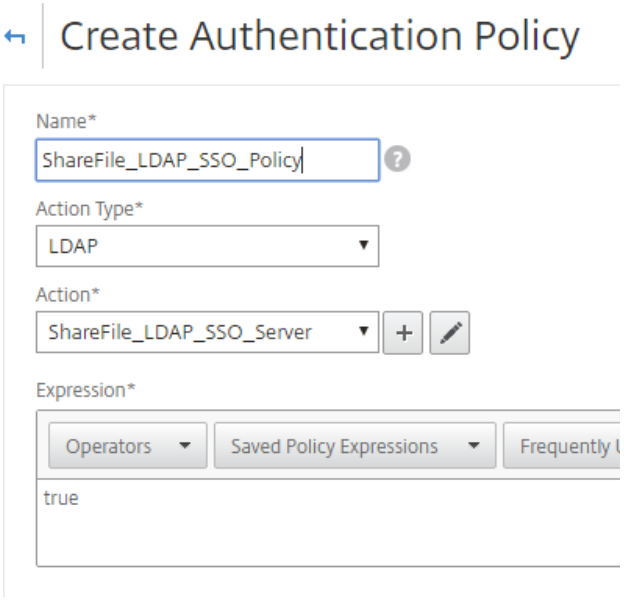
3. In the **Action** field, hit the '**+**' to add a new server. The **Create Authentication LDAP Server** window appears.

i. In the **Name** field, enter **ShareFile_LDAP_SSO_Server**.
ii. Select the bullet for **Server IP**. Enter the IP address of one of your AD domain controllers. (You can also point to a Virtual Server IP for the purpose of redundancy if you are load balancing DC's).
iii. Specify the port that the NetScaler NSIP will use to communicate with the domain controller. Use **389 for LDAP** or **636 for Secure LDAP**.
iv. Under **Connection Settings**, enter the **Base DN** where the user accounts reside in AD that you would like to allow authentication. Ex. OU=ShareFile,DC=domain,DC=com.
v. 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 such that there will be no issues with logins if the account that is configured has a password expiration.
vi. Check the box for **Bind DN Password** and supply the password **twice**.
vii. Under **Other Settings**: Enter 'sAMAccountName' (without quotes) as the **Server Logon Name Attribute**.
viii. Under the **Group Attribute** field, enter 'memberof'
ix. Under the **Sub Attribute** field, enter 'CN'
x. Click **More**
xi. Scroll down and In the **Attribute Fields, Attribute 1**, enter 'mail'



i. Hit the **Create** button to complete the LDAP server settings.

ii. For the **LDAP Policy Configuration**, select the newly created LDAP server from the **Server** dropdown, and in the Expression field type, 'true'



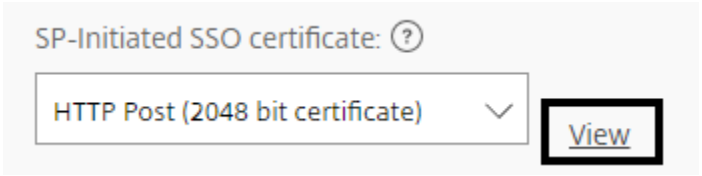
Hit the **Create** button to complete the LDAP Policy and Server configuration.

To import the ShareFile SP-Certificate onto the NetScaler

Login to your ShareFile account at https://subdomain.sharefile.com with a user account that has admin rights

Select the **Settings > Admin Settings** link near the left/center of the page. Select **Security > Logon & Security Policy**, then scroll down to **Single Sign-On Configuration**

Under **Optional Settings**, next to SP-Initiated SSO Certificate, HTTP Post (2048 Bit Certificate) click on **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**
- Navigate to the **NetScaler Configuration Utility**.
- Select **Traffic Management > SSL > Certificates > CA Certificates**
- Click on **Install**
- From the **Install Certificate Window**, provide a **Certificate-Key Pair Name**
- Under the **Certificate File Name** section, select the dropdown next to **Browse** and select **Local** and browse to the location you saved the ShareFile_SAML.cer file Once the file is

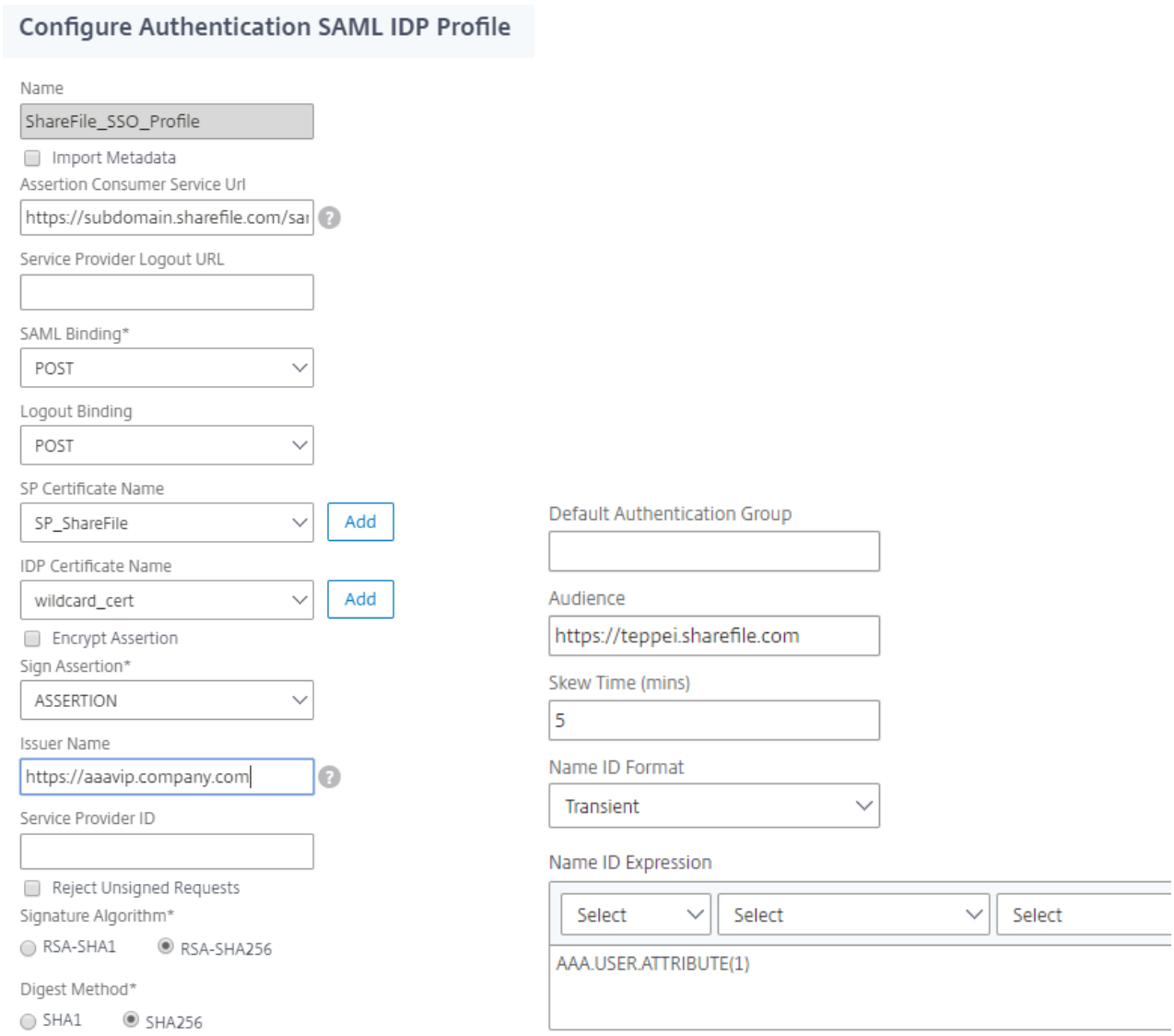
chosen, select **Install**

To Configure the SAML IDP Policy and Profile

In order for your users to receive the SAML Token to logon to ShareFile, you must configure a SAML IDP Policy and Profile, which will be bound to the AAA Virtual Server that the users are providing their credentials to.

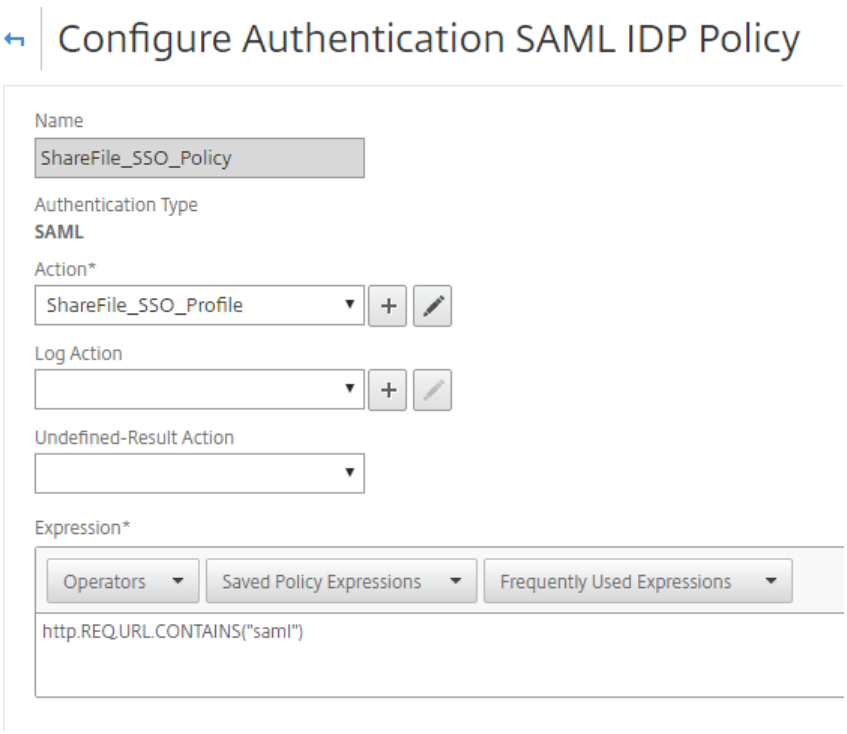
The following steps outline this process:

- Open the **NetScaler Configuration Utility** and navigate to **Security > AAA – Application Traffic > Policies > Authentication > Advanced Policies > SAML IDP**
- Under the **Policies Tab**, select the **Add** button.
- From the **Create Authentication SAML IDP Policy Window**, provide a name for your policy. Example – ShareFile_SSO_Policy
- To the right of the **Action** field, hit the **'+**' sign to Add a new Action/Profile
- Provide a name such as **ShareFile_SSO_Profile** and remove the checkbox for "Import Metadata." If running an older version of Netscaler this checkbox might not exist.
- In the **Assertion Consumer Service URL** field, enter **your ShareFile account URL followed by /saml/acs**: Ex. https://subdomain.sharefile.com/saml/acs
- In the **IDP Certificate Name** field, browse to the certificate installed on the NetScaler that is will be used to secure your AAA authentication Virtual Server.
- In the **SP Certificate Name** field, select the dropdown and browse to the ShareFile SP certificate you imported earlier and added as a CA Certificate on the NetScaler
- For **Sign Assertion**, leave **ASSERTION**.
- **Uncheck** Send Password
- In the **Issuer Name** field enter the URL for your AAA traffic *(Example– https://aaavip.mycompany.com)*
- Leave Service Provider ID blank
- **Uncheck** Reject Unsigned Requests
- **Signature Algorithm**, **RSA-SHA256**
- **Digest Method**, **SHA256**
- For **SAML Binding**, select **POST**
- Click **More**
- Under the **Audience** field provide the **URL for your ShareFile account** (Example – https://subdomain.sharefile.com)
- For **Skew Time**, enter **5**. *(This allows for a 5 minute time difference between the client, NetScaler and ShareFile.)*
- For **Name ID Format,** select **Transient**
- In the **Name ID Expression** field, type the following: aaa.user.attribute(1). If using Netscaler 11.x type http.req.user.attribute(1).



- Click **Create** to complete the SAML IDP profile configuration and return to the SAML IDP Policy creation window
- In the **Expression** field, add the following expression: HTTP.REQ.URL.CONTAINS(“saml”)

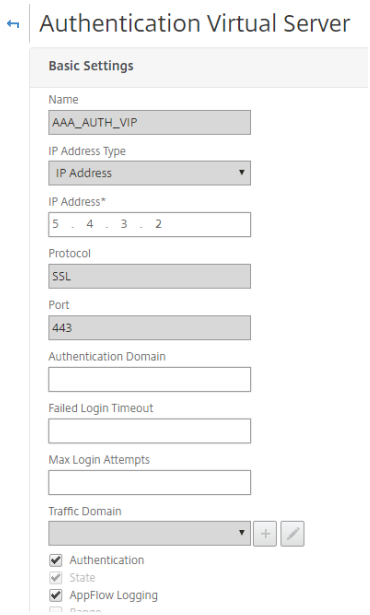
- Click **Create** to complete the SAML IDP Configuration


Configure Authentication SAML IDP Policy
Name
ShareFile_SSO_Policy
Authentication Type
SAML
Action*
ShareFile_SSO_Profile
Log Action
Undefined-Result Action
Expression*
Operators
Saved Policy Expressions
Frequently Used Expressions
http.REQ.URL.CONTAINS("saml")

To Configure your AAA Virtual Server

When an employee attempts to login to ShareFile, in order for them to utilize their corporate credentials, they will be redirected to a NetScaler AAA Virtual Server. This virtual server will be listening on port 443, which requires an SSL certificate, in addition to external and/or internal DNS resolution to the IP address being hosted on the NetScaler. The following steps require these pre-exist, assume that the DNS name resolution is already in place, and that the SSL certificate is already installed on your NetScaler appliance.

- In the **NetScaler Configuration Utility** navigate to **Security > AAA – Application Traffic > Virtual Servers** and select the **Add** button
- From the **Authentication Virtual Server** window, provide a Name and an IP address.
- Scroll down and make sure that the **Authentication** and **State** checkboxes are checked



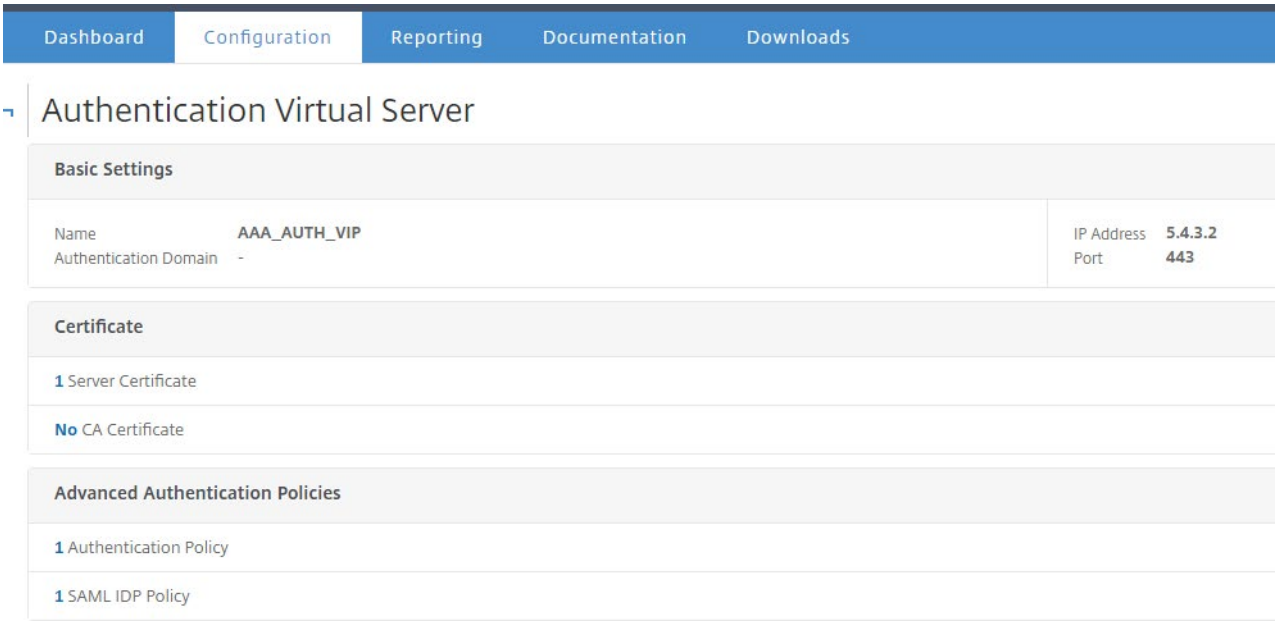
- Click **Continue**
- In the **Certificates** section click on **No Server Certificate**
- From the **Server Cert Key** window **click** Bind
- Under **SSL Certificates**, choose your **AAA SSL Certificate** and select **Insert**
- **(**Note – This is NOT the ShareFile SP certificate**)**
- Click **Bind**, then click **Continue**
- From the **Advanced Authentication Policies** option, click **No Authentication Policy**.
- From the **Policy Binding** page**, Select Policy,** select **ShareFile_LDAP_SSO_Policy** created earlier
- Click **Select,** then **Bind** (leaving defaults) to return to the Authentication Virtual Server screen
- Under **Advanced Authentication Policies** click **No SAML IDP Policy**
- Under **Policies**, select your **SHAREFILE_SSO_POLICY**. Click **Select**.

- From the Policy Binding page (leave defaults), Click **Bind**.

- Then **Close**

- Click **Continue** and **Done**

Image of AAA Virtual Server after proper configuration is completed:



Validate the configuration

Point your browser to https://subdomain.sharefile.com/saml/login.

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

Logon with your user credentials that are valid for the NetScaler environment you just configured.

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