Content Collaboration: Single Sign-On Configuration Guide

Dual IDP (ADFS & CEM)

Last Revised: May 2019

LEGAL NOTICE

Introduction:

This document was created to assist in the configuration of utilizing both Endpoint Management and ADFS as the Identity Provider (IDP) for a single ShareFile account. The resulting configuration allows the Token Signing certificate on the ADFS server to be the same as the SAML certificate on the Citrix Endpoint Management server. This will provide a single ShareFile account to:

- Use Endpoint Management as the IDP for MDX wrapped apps. Providing a true SSO experience from a mobile device via ShareFile MDX applications.
- Use ADFS as the SAML IDP for SSO to Webapps (WebUI/Sync/OLP/DesktopApp/DriveMapper/PublicStore Apps).

Contents

Prerequisites:

- Citrix Endpoint Management 10.x server with fully functioning SSO for MDX configured to the ShareFile account.

- ADFS installed and configured within the infrastructure.
- Access to an administrator account within ShareFile with the ability to configure Single SignOn.

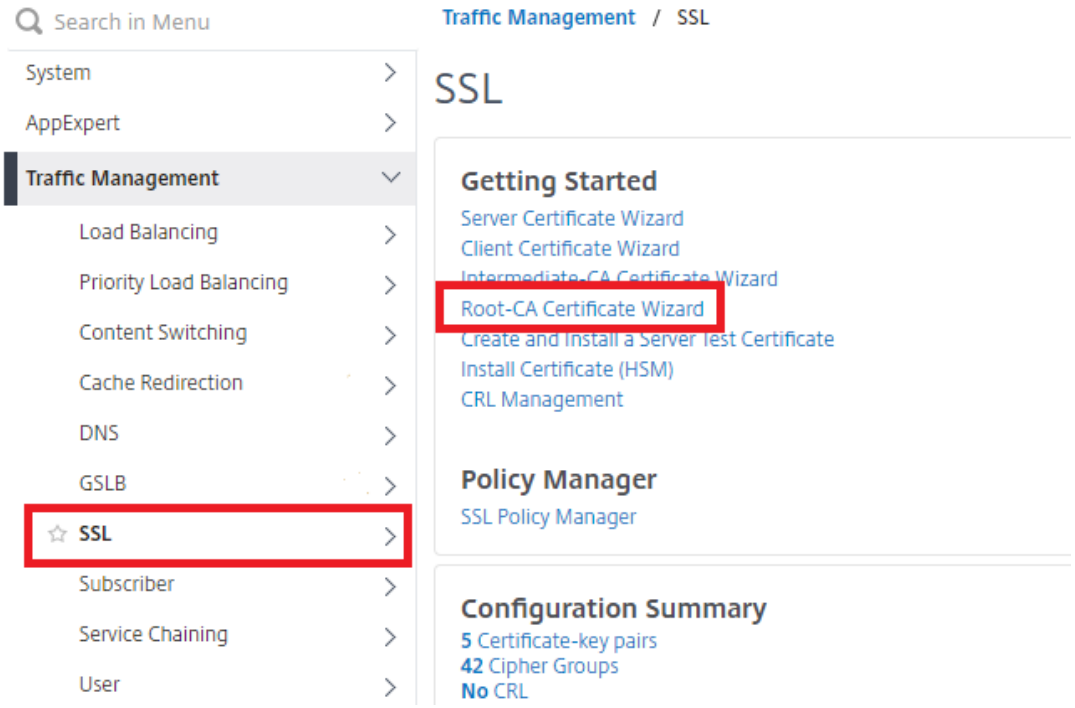
Preparing the ADFS Token Signing Certificate:

When configuring ADFS for SSO to ShareFile. It is required to upload the ADFS Token Signing certificate to the ShareFile Control Plane without the private key. ADFS generates a self-signed certificate to be used for Token Signing & Token Decrypting with a 1-year expiration. However, the self-signed certificate does contain a private key.

At the one-year mark, the self-signed certificate is renewed via Automatic Certificate Rollover 15 days prior to expiration and becomes the primary certificate. This causes all existing SSO trust relationships to fail. For this configuration the SAML certification from the Endpoint Management console is exported with an expiration of 3 years. The certificate validity period is customizable and will mitigate the need to renew the token signing certificate at the 1-year mark.

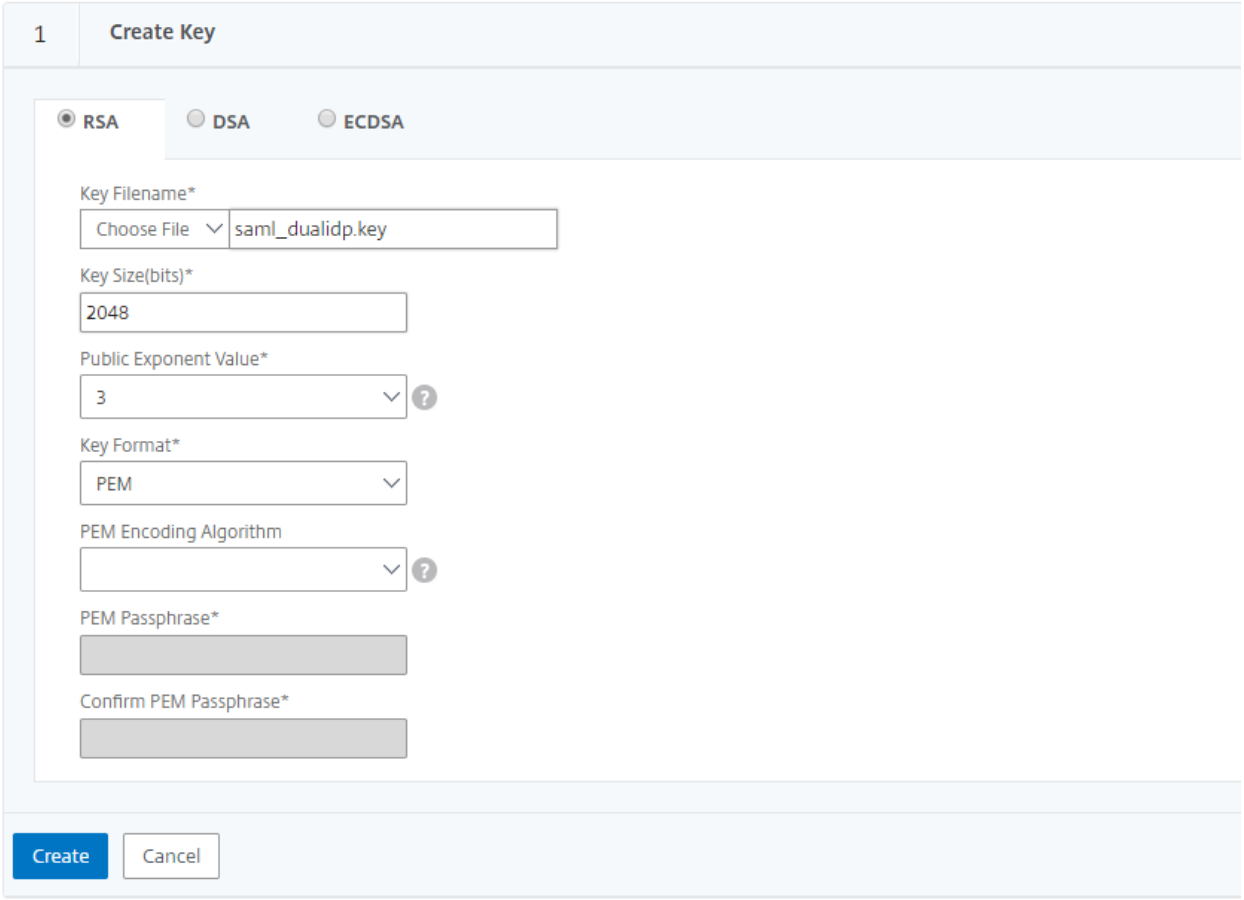
Generate the SAML Certificate:

- Logon to NetScaler GUI.
- Navigate to Traffic Management > SSL.
- Under Getting Started Section, Select Root-CA Certificate Wizard.



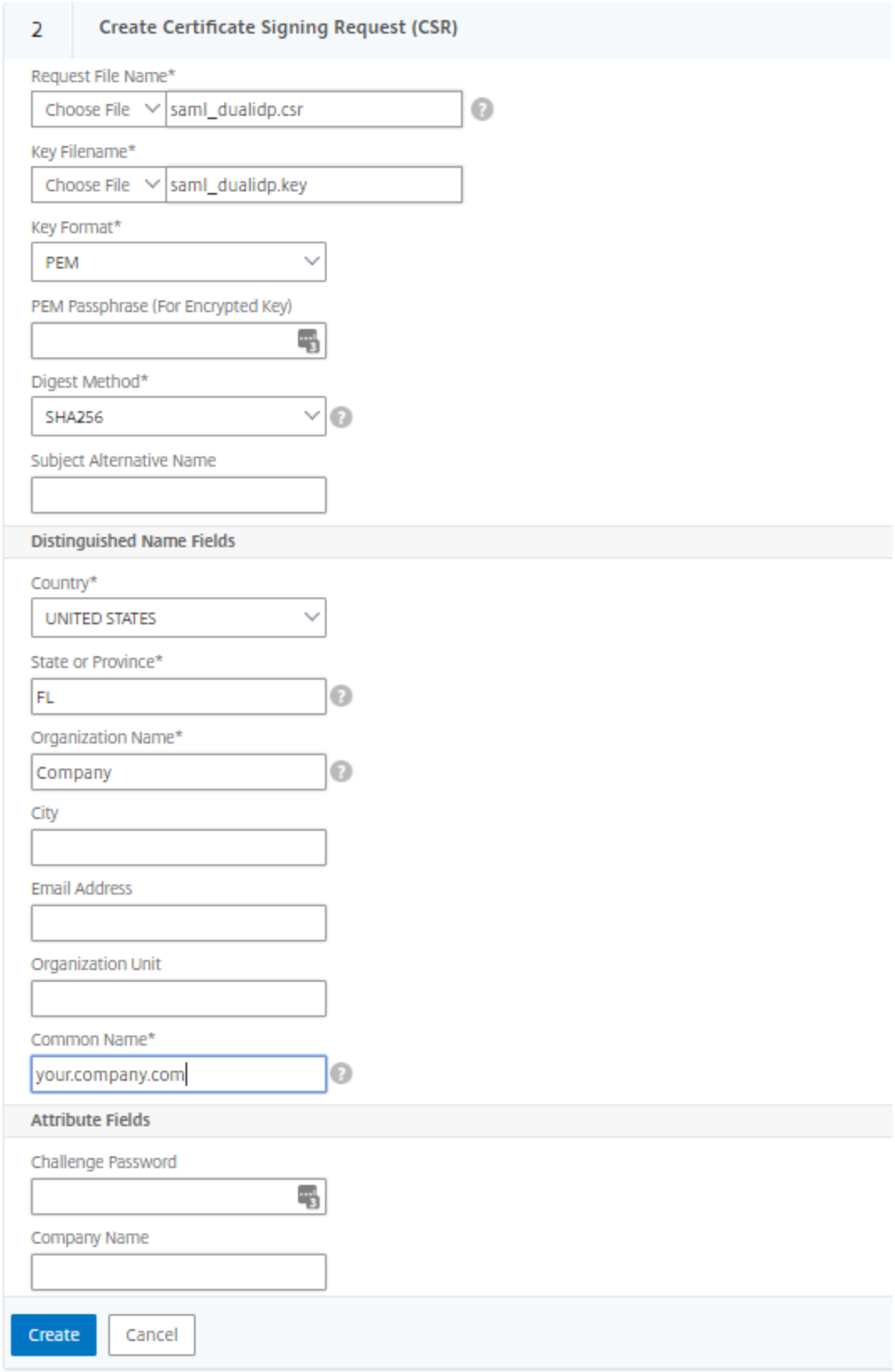
We are now prompted to create the Private Key.

- In the **Key Filename** field provide a name for your key (ex- saml_dualidp.key).
- **Key Size**, 2048.
- **Public Exponent Value**, 3.
- Click **Create** to create the Key.



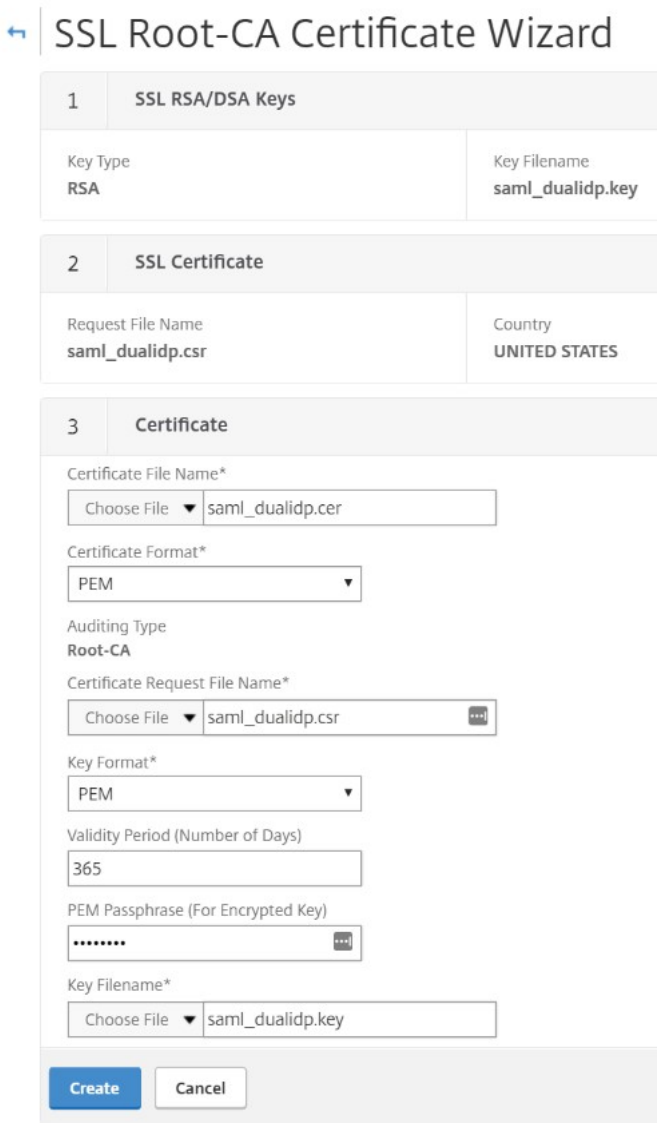
Next step is to create the CSR.

- In the **Request File Name** field, enter a name for the CSR (ex- saml_dualidp.csr).
- The **Key Filename** and **PEM** format should be pre-populated.
- Set **Digest Method** to **SHA256**.
- In the **Distinguished Name Fields**, provide information about your organization.
- In the **Attribute Fields**, we do not need a Challenge Password, however the **Company Name** can be added.
- Click **Create** to complete the CSR Request.

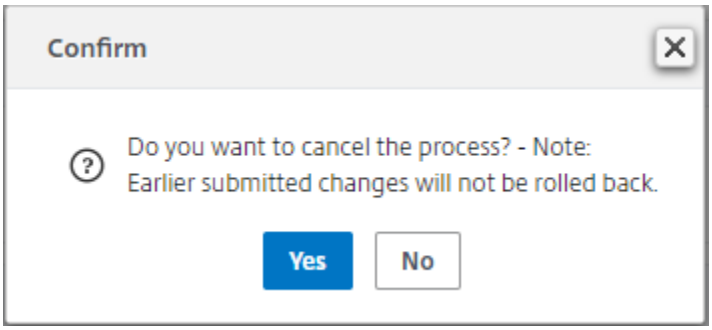


Final step is to Create the SAML Certificate.

- In the **Certificate File Name** field, enter the name of your certificate (Ex- saml_dualidp.cer).
- The **Certificate Format** should be pre-populated with **PEM**.
- The **Certificate Request File Name** should reflect the **CSR** you created in the previous step.
- The **Key Format** should default to **PEM**.
- Specify the **Validity Period** (in days) you wish the certificate to be valid for. In this example we are creating a 3 year certificate, so enter **1095**.
- The **Key Filename** should be pre-populated from the first step.
- Click **Create** to create the **Certificate**.

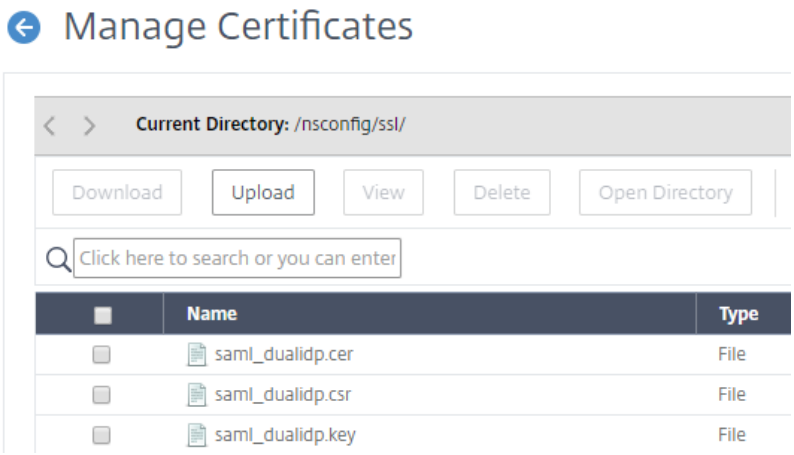


- After creating the certificate, we can now **EXIT** the Wizard as we do not need to install the certificate on the NetScaler.
- Click **Cancel** and Click **YES** to Confirm you would like to return back to the main SSL GUI Screen.



We now need to export the newly created certificate and key off the NetScaler for use on the Endpoint Management server as well as on ADFS. For Endpoint Management, we just need the saml_dualidp.cer file and saml_dualidp.key file we created in the previous steps, as the cert and key are already properly formatted for Endpoint Management. Follow the below steps to save the files to a location we can then use to upload them to your Endpoint Management server when replacing its built-in SAML certificate.

- From the NS GUI, under **Traffic Management > SSL**, under the section marked **Tools**, click on the option to **Manage Certificates / Keys / CSRs.**
- From the **Manage Certificate**s page, click on **Date Modified**, which should bring the newest files to the top. You should see the 3 newly created files from the previous steps. (If you do not see them, you may need to show more than 25 items per page)



- **Select** the saml_dualidp.cer file and choose the option to **Download**. Save to a location of your choice.
- Follow the same step above for the saml_dualidp.key.
- Click **Back** to return to the previous NS GUI Page.

Next we need to export the certificate and key in a file format that the ADFS server will understand.

- Under the same **Tools** section as earlier, select the option to **Export PKCS#12.**
- In the **Choose File** field, enter saml_dualidp.pfx.
- In the **Certificate File Name** field, select **Choose File**, **Date Modified**, and **select** the saml_dualidp.cer file. Click **Open.**
- In the **Key Filename** field, select **Choose File**, **Date Modified**, and **select** the saml_dualidp.key file. Click **Open.**
- Provide an **Export Password.**
- Provide the **PEM Passphrase.**
- Click **OK** to finish the export.

We now need to copy the .pfx file off the NetScaler and onto a network location.

- From the **Tools** menu once again, select the option to **Manage Certificates / Keys / CSRs.**
- S**elect** the newly created saml_dualidp.pfx file, and choose **Download.**
- **Save** the file somewhere locally accessible.
- **Close** the windows on NetScaler as we are now finished with the SAML certificate creation process.

Upload Newly Created Token Signing Certificate to ADFS:

The first step is to Disable Certificate Rollover on the ADFS server.

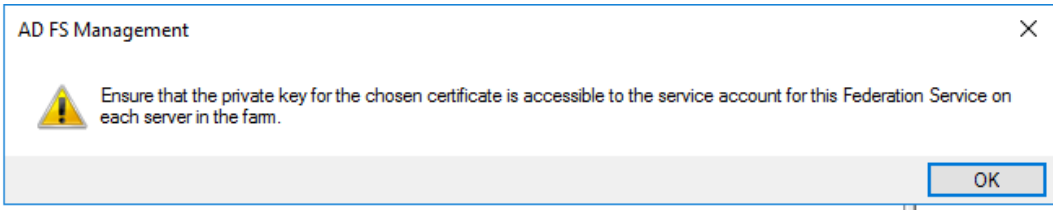
- **Create** a remote connection to your ADFS server.
- By default, ADFS enables AutoCertificateRollover in order to renew the self-signed certificate at the 1year mark. This feature will need to be disabled in order to upload the newly created Token Signing Certificate.
- **Run Powershell** as **Administrator** on the ADFS server.
- **Type**: **Get-ADFSProperties.**
- To disable AutoCertificateRollover: **Set-ADFSProperties -AutoCertificateRollover $false**

Secondly, we need to import the previously exported saml_dualidp.pfx file onto the ADFS server so we can use it as the Token Signing Certificate.

- On the ADFS server, **Right-Click, Start > Click Run > Type mmc**, and hit **enter** to open a Snapin.
- **Click File > Add/Remove Snap-in.**
- From the Available snap-ins section, Select **Certificates**, click **Add.**
- Select **Computer Account**, click **Next**. Select **Local Computer** and then **Finish**, click **OK.**
- Under Console Root, **Expand Certificates > Personal > Certificates.**
- **Right Click** the **Certificates** folder and select **All Tasks > Import.**
- From the Welcome screen hit **Next.**
- **Browse** to the saml_dualidp.pfx file you saved earlier, click **Open.**
- Select **Next**, type the password for the private key, select **Next** once again.
- Select **Place all certificates in the following store, Personal** and hit **Next.**
- Select **Finish** to complete the import, **close** the MMC Snap-in.

We now need to change the Token Signing Certificate in ADFS…

- On the ADFS server, from the Server Manager Dashboard, select **Tools**, **ADFS Management.**
- On the left hand side of the ADFS Management Console, expand **Service > Certificates.**
- Under the **Actions** menu, select **Add Token-Signing Certificate**, and **select** the newly imported Token-Signing Certificate.
- The newly added Token-Signing Certificate will be added as a secondary certificate. We will need to make it the primary.
- **Expand Service** and then select **Certificates**.
- **Click** the **Secondary** Token-Signing certificate.
- In the **Action**s pane on the right, select **Set As Primary.** Click **Yes** at the confirmation prompt.



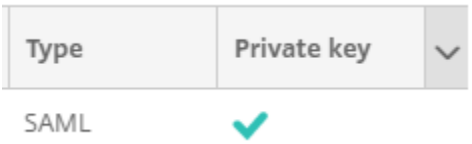
Endpoint Management Configuration

In order to use the same certificate on Endpoint Management, we only need to perform two steps.

1. Export the old SAML certificate for backup purposes
2. Import the new SAML certificate.

Backup Endpoint Management SAML Certificate (Recommended)

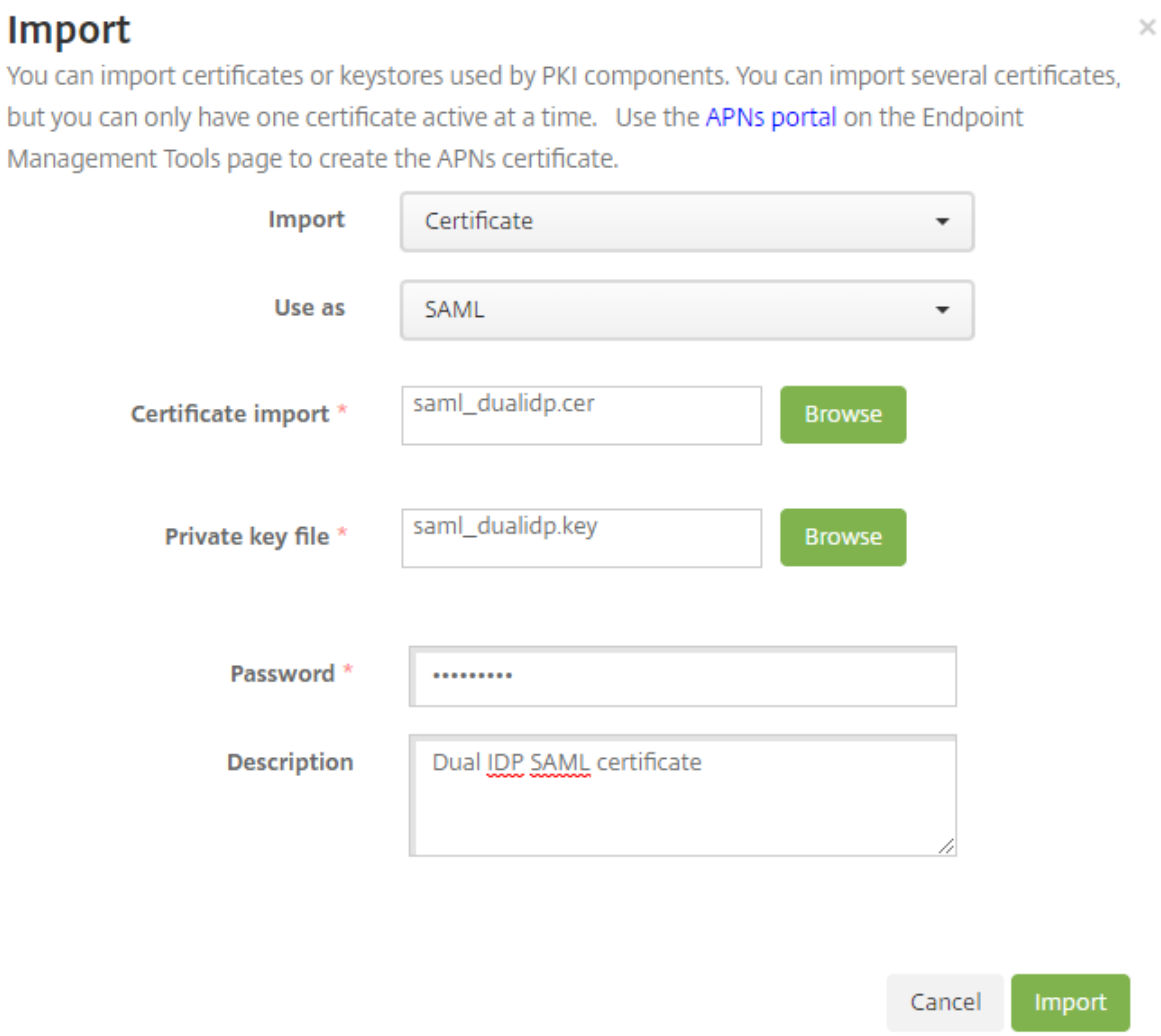
- Log onto the Endpoint Management Server, click on the **Gear** icon towards the top right, then under **Settings** select **Certificates.**
- **Highlight** the SAML cert, then click on **Export.**



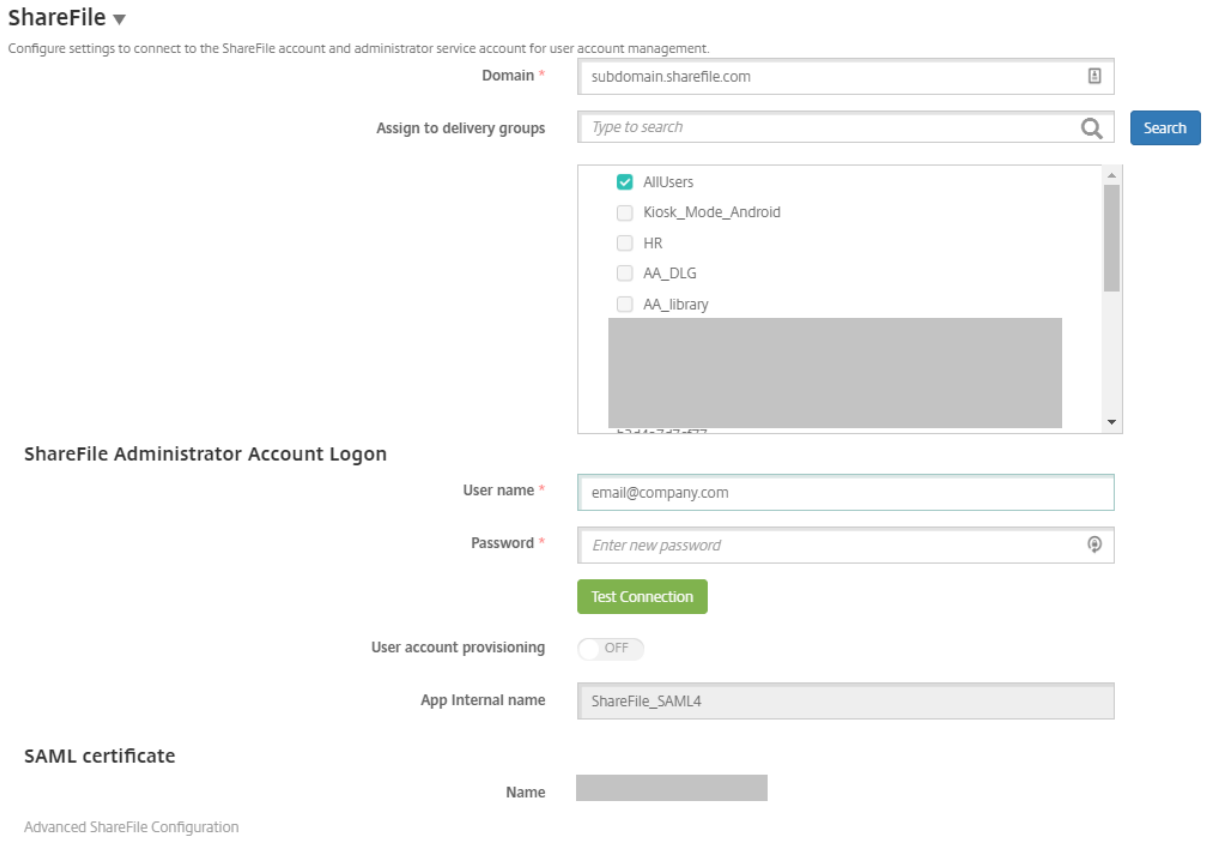
- Choose to export the private key also, then click **OK.**
- Store certificate and in safe location.

Install New SAML Certificate:

- Log onto the Endpoint Management Server, click the Gear icon, then under **Settings** click **Certificates.**
- Click **Import**, then select following options:
  - **Import: Certificate**
  - **Use as: SAML**
  - **Certificate import:** Browse your workstation/network for the previously exported saml_dualidp.cer file.
  - **Private key file**: Browse your workstation for the previously exported saml_dualidp.key file.
  - **Password:** enter the password for the private key.
  - **Description:** place enough detail for others to know it's function.
- Click on **Import** to complete.



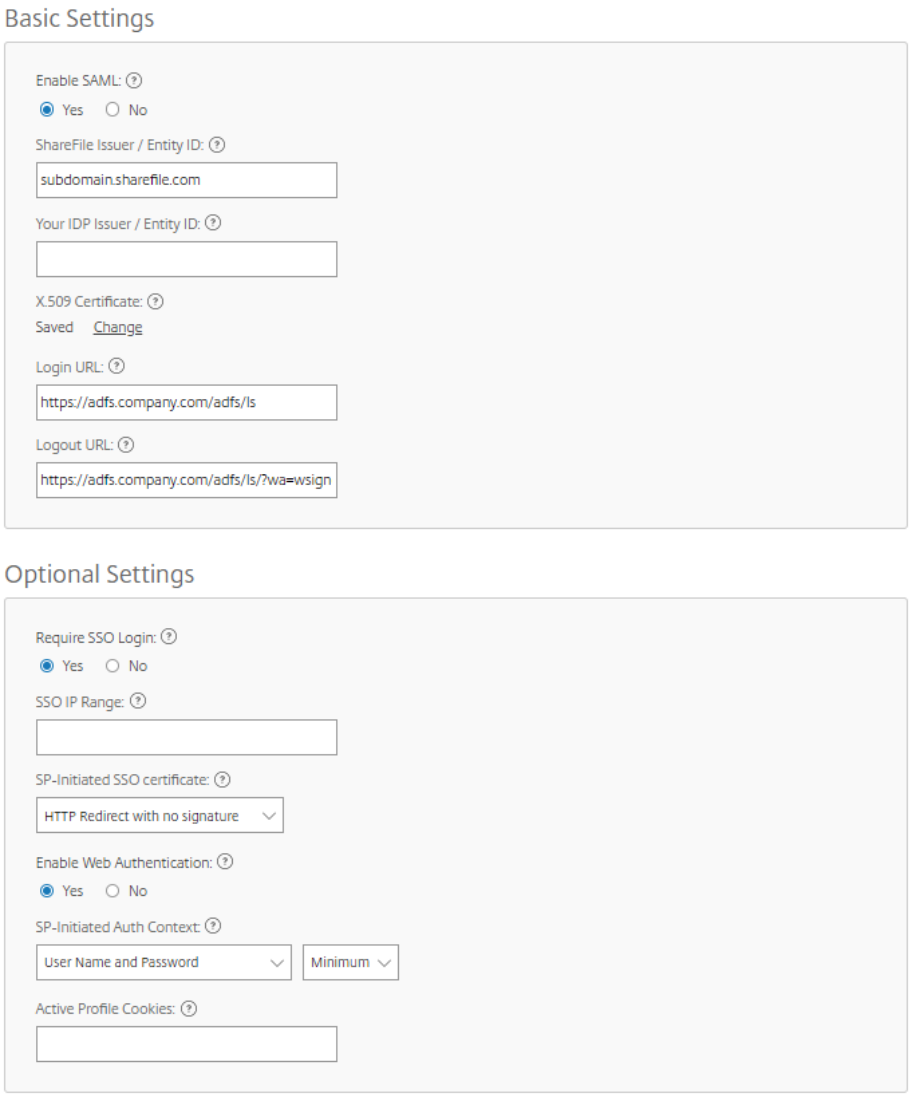
- On the Endpoint Management server, click **Configure**, then **ShareFile.**
- If you have a previous ShareFile configuration, just click the **Save** button on the bottom right of the screen.
  Note: This step will update the ShareFile account with the X.509 certificate that has just been created in the previous steps. It will also override the ShareFile SSO
    - *Configuration settings, which we will need to change in the steps outlined in the next section.*
- If ShareFile has not yet been configured, in the **Domain** field, enter your ShareFile account:
    - (ex - company.sharefile.com)
    - Select a **Delivery Group** that has access to the ShareFile MDX Application.
    - Provide your ShareFile administrator **User Name**: (ex- email@company.com) *This is a local ShareFile administrative user account.*
- Enter the ShareFile password *(not your AD password).*
- Leave *User account provisioning* **OFF** (especially if using the ShareFile User Management Tool – UMT).
- Click **Save** to complete the ShareFile configuration on Endpoint Management.



ShareFile Single-Sign-On Configuration Check:

Once both Endpoint Management and ADFS have been configured for ShareFile, follow the steps below to validate the SSO settings.

- Log into your ShareFile account via the WebUI, click on **Admin** then **Configure Single-Signon page**
- **ShareFile Issuer/Entity ID:** this needs to be identical to the Identifier Name within the ADFS configuration (ex- **subdomain.sharefile.com**).
- **Login URL**: Login URL to ADFS, eg **https://adfs.company.com/adfs/ls.**
- **Logout URL:** Logout URL to ADFS, eg **https://adfs.company.com/adfs/ls/?wa=wsignout1.0** ***(****this will need to be added as a logout point on ADFS if not done so already).*
- **Enable Web Authentication: Yes**
- **SP-Initiated Auth Context:** Select the option **User Name and Password** for Forms Authentication, or **Integrated Authentication** *(according to what your AD FS server is configured with).*



Testing

Re-enroll your device to Endpoint Management (or just for BYO), download the app and see if MDX SSO is working. Also perform testing using SP initiated authentication: https://subdomain.sharefile.com/saml/login.