ShareFile Dual IDP (ADFS & XenMobile)

Introduction:

This document was created to assist in the configuration of utilizing both XenMobile 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 XenMobile server. This will provide a single ShareFile account to:

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

Contents

ShareFile Dual IDP (ADFS & XenMobile)	1
Introduction:	1
Prerequisites:	2
Preparing the ADFS Token Signing Certificate:	2
Generate the SAML Certificate:	2
Upload Newly Created Token Signing Certificate to ADFS:	7
XenMobile Configuration	8
Backup XenMobile SAML Certificate (Recommended)	8
Install New SAML Certificate:	8
ShareFile Single-Sign-On Configuration Check:	10
Testing	11

Prerequisites:

- XenMobile 10/10.3 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 Sign-On.
- NetScaler 11.x for generation of the SAML certificate and key used on both XenMobile and ADFS.

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 a certificate was issued from the NetScaler 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.

System	>	SSL
AppExpert	>	
Traffic Management	~	Getting Started Server Certificate Wizard
Load Balancing	>	Intermediate-CA Certificate Wizard
Content Switching	>	Root-CA Certificate Wizard CRL Management
Cache Redirection	>	
DNS	>	SSL Keys Create RSA Key
GSLB	>	Create DSA Key
SSL	~	
Certificates	\sim	

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.
- **PEM Encoding Algorithm** Drop down to **DES**.
- Provide a **Passphrase** and **Confirm**.
- Click **Create** to create the Key.
 - SSL Root-CA Certificate Wizard

1	Create Key
۲	RSA O DSA
	Key Filename*
	Choose File saml_dualidp.key
	Key Size(bits)*
	2048
	Public Exponent Value*
	3
	Key Format*
	PEM 🔻
	PEM Encoding Algorithm
	DES
	PEM Passphrase*
	Confirm PEM Passphrase*
	••••••
Creat	Cancel

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.
- Provide the **Passphrase** for the Key.
- 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.

Renu	est File Name*
Ch	oose File saml dualidp.csr
Kov E	ilename*
Ch	oose File 🔻 saml dualido key
Kau F	
PEN	
	Passabrasa (Ear Encrypted Vay)
•••••	•••
Dines	t Method*
SHA	×256 •
Distir	nuished Name Fields
Cours	
UNI	TED STATES
State	or Province*
Your	State
Orga	nization Name*
Your	Organization
City	
Your	City
Email	Address
user	@company.com
Orgai	nization Unit
Your	Organization
Comr	non Name*
dual	idp.company.com
Attrik	oute Fields
Challe	enge Password
Comp	bany Name

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**.
- Provide the **PEM Passphrase** for the Key.
- The Key Filename should be pre-populated from the first step.
- Click **Create** to create the **Certificate**.

1	SSL RSA/DSA Keys			
Key Ty RSA	уре	Key Filename saml_dualidp.k		
2	SSL Certificate			
Reque saml	est File Name _ dualidp.csr	Country UNITED STATES		
3	Certificate			
Certif	icate File Name*			
Cho	oose File 🔻 saml_dualidp.cer			
Certif	icate Format*			
PEN	1 🗸			
Auditi Root-	ing Type CA			
Certif	icate Request File Name*			
Cho	oose File 🔻 saml_dualidp.csr	1		
Key Fo	ormat*			
PEN	1 •			
Validi	ty Period (Number of Days)			
365				
PEM Passphrase (For Encrypted Key)				
	lename*			
Key Fi				

- 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.

Confirm	×
Do you want to cancel the process? - Note: Earl submitted changes will not be rolled back.	ier

We now need to export the newly created certificate and key off the NetScaler for use on the XenMobile server as well as on ADFS. For XenMobile, 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 XenMobile. Follow the below steps to save the files to a location we can then use to upload them to your XenMobile 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 Certificates** 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).

4	Mana	ige Certificates		
<	> Cur	rent Directory: /nsconfig/ssl/		
	Downloa	d Upload View Delete Open Directory	Action	•
		Name	Туре	Date Modified
		i saml_dualidp.cer	File	Thu May 19 12:04:30 2016
		📄 saml_dualidp.csr	File	Thu May 19 11:42:54 2016
		📄 saml_dualidp.key	File	Thu May 19 11:29:34 2016
		saml_dualidp.cer saml_dualidp.csr saml_dualidp.key	File File File	Thu May 19 12:04:30 2016 Thu May 19 11:42:54 2016 Thu May 19 11:29:34 2016

- **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.**
- **Select** 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 Actions pane on the right, select Set As Primary. Click Yes at the confirmation prompt.



This completes the ADFS configuration section.

XenMobile Configuration

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

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

Backup XenMobile SAML Certificate (Recommended)

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

Туре	Private key
SAML	×

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

Install New SAML Certificate:

- Log onto the XenMobile 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.

Import You can import certificates or keyst	ores used by PKI components. You o	can import	several c	ertificates,	×
but you can only have one certificat					
Import	Certificate		*		
Use as	SAML		•		
Certificate import*	saml_dualidp.cer	Browse			
Private key file*	saml_dualidp.key	Browse			
Password*					
Description	Dual_IdP SAML Certificate		4		
			Cancel	Import	

- On the XenMobile 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 Provisioning **OFF** (especially if using the ShareFile User Management Tool UMT).
- Click Save to complete the ShareFile configuration on XenMobile.

ShareFile			
Configure settings to connect to the ShareFile account and administrator service accourt	It for user account management.		
Domain*	company.sharefile.com		
Assign to delivery groups	Type to search	Q	Search
	AllUsers		
	ShareFile		
	TitanUsers		
ShareFile Administrator Account Logon			
User name*	email@company.com		
		_	
Password*			
User account provisioning	OFF		
SAML certificate			
Name			
Advanced ShareFile Configuration			
Autorica Statellic configuration			

ShareFile Single-Sign-On Configuration Check:

Once both XenMobile 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 <u>https://adfs.company.com/adfs/ls/?wa=wsignout1.0</u> (this will need to be added as a logout point on ADFS if not done so already).
- Enable Web Authentication: CHECK
- **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).

Basic Settings	
Enable SAML:	 Ø
ShareFile Issuer / Entity ID: *	subdomain.sharefile.com
Your IDP Issuer / Entity ID:	
X.509 Certificate: *	Saved <u>Change</u>
Login URL: *	https://adfs.companycom/adfs/is
Logout URL:	https://adfs.company.com/adfs/ls/?wa=wsignout1.0
Optional Settings	
Require SSO Login:	
SSO IP Range:	0
SP-Initiated SSO certificate:	HTTP Redirect with no signature
Enable Web Authentication:	•
SP-Initiated Auth Context:	User Name and Password Minimum Ø
Active Profile Cookies:	0

Testing

Re-enroll your device to XenMobile (or just for BYO), download the app and see if MDX SSO is working.

Also perform testing using SP initiated authentication: <u>https://subdomain.sharefile.com/saml/login</u>.