Configure TitanFile SSO with ADFS

Last updated: 2021-07-15

Overview

TitanFile can be configured to integrate with Active Directory (AD) to provide single sign-on (SSO) capability to users with AD credentials in your organization. TitanFile's SSO is supported through the Security Assertion Markup Language (SAML). A SAML-based identity federation service needs to run within your network. When your users attempt to login their requests are redirected to your Active Directory. The same SAML-based identity federation service can be used to provide SSO to multiple applications. If you already use such a service with another application, you can use the same service for TitanFile.

Configuring the SAML-based identity federation service

You will need the following information when configuring your SAML-based identity federation service:

- Your TitanFile subdomain: subdomain.titanfile.com
- SAML assertion consumer service URL: <u>https://subdomain.titanfile.com/saml2/acs/</u>
- SAML single logout service URL: <u>https://subdomain.titanfile.com/saml2/ls/</u> (optional)
- Application name: TitanFile

Here are the detailed steps to do this.

1. In the ADFS Management Console, expand "Trust Relationships", go to "Relying Party Trusts" and select "Add Relying Party Trust..."

\$ 1	Add Relying Party Trust Wizard	x
Welcome		
Steps Welcome to the Add Relying Party Trust Wizard • Welcome This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. • Specify Display Name • Configure Multifactor Authentication Now? The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.		3
Authorization Rules Ready to Add Trust Finish		
	< Previous Start Cancel	

2. Press start and enter the TitanFile metadata URL:

https://subdomain.titanfile.com/saml2/metadata/

Select Data Source Steps • Welcome • Select Data Source • Configure Multi-factor Authorization Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish • Impot data about the relying party published online or on a local network. • Select In Authorization Rules • Ready to Add Trust • Finish • Impot data about the relying party from a file Use this option to impot the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Use this option to impot the necessary data and certificates from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: • Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.	\$	Add Relying Party Trust Wizard
Welcome Select an option that this wizard will use to obtain data about this reging party: Welcome Select Data Source Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): Choose Issuance Authentication Now? Choose Issuance Authonization Rules Ready to Add Trust Pederation metadata address (host name or URL): Intps://app.ttanfile.com/saml2/metadata/ Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location:	Select Data Source	
< Previous Next > Cancel	Welcome Select Data Source Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust	Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): https://app.titarfile.com/saml2/metadata/ Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Browse Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.

3. Specify a display name or keep the default.

\$	Add Relying Party Trust Wizard	×
Specify Display Nam	le	
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	app.titanfile.com	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?		^
 Choose Issuance Authorization Rules 		
Ready to Add Trust		_
Finish		
	< Previous Next > Cance	ł

4. Keep default multi-factor authentication settings.

\$	Add Relying Party Trust Wizard	×
0		
Steps Welcome Select Data Source	Configure multifactor authentication settings for this relying party trust. Multifactor authentication there is a match for any of the specified requirements.	is required if
Specify Display Name	Multifactor Authentication Global	Settings
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured	
Choose Issuance Authorization Rules	Device Not configured Location Not configured	
 Ready to Add Trust Finish 	I do not want to configure multi-factor authentication settings for this relying party trust at this ti Configure multi-factor authentication settings for this relying party trust.	me.
	You can also configure multi-factor authentication settings for this relying party trust by navig Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .	ating to the
	< Previous Next >	Cancel

5. Set desired authorization rules. Either permit all user to access this relying party or configure permissions for each user/role separately.



6. Review settings, go back to adjust if needed.

%	Add Relying Party Trust Wizard		
Ready to Add Trust			
Steps Welcome	 The relying party trust has been configured. Review the following settings, and then click. Next to add the 		
 Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note<		
	< Previous Next > Cancel		

7. All set and ready to configure the Claim Rules.

\$ 1	Add Relying Party Trust Wizard	x
Finish		
Steps	The relying party trust was successfully added to the AD FS configuration database.	
Welcome	You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in	
Select Data Source	To be can meanly and reging party adde by daining the more dealed block in the rise to management and pin	
Specify Display Name		
Configure Multi-factor Authentication Now?	Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
Finish		
	Close	

8. Here you add rules to map AD entities to TitanFile fields.

Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules The following transform rules specify the claims that will be sent to the relying party. Image: Claims Order Rule Name Issued Claims Image: Claim State of the relying party issued claim State o	🕅 Edit Claim Rules for app.titanfile.com	_		x
Order Rule Name Issued Claims Image: Control of the second seco	Issuance Transform Rules Issuance Authorization Rules Delegation Authoriz	ation R	lules	
Add Rule Edit Rule Remove Rule	The following transform rules specify the claims that will be sent to the relying	party.		
Add Rule Edit Rule	Order Rule Name Issued Claims]	
Add Rule Edit Rule				
Add Rule Remove Rule				
Add Rule Remove Rule				
Add Rule Remove Rule				
Add Rule Edit Rule				_
				7
]	
OK Cancel Apply	Add Rule Edit Rule Remove Rule			
OK Cancel Apply				
	OK Cancel		Appl	ly

9. Add a claim rule using the LDAP template.



10. Populate the rule as per the screenshot below.

Edit Rule - LDAP

 \times

 \sim

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

laim rule name:	
DAP	
Rule template: Send LDAP Attributes as Claims	

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses ~	Name ID 🗸 🗸 🗸
	Given-Name 🗸	FirstName 🗸
	Sumame ~	LastName 🗸
	~	~ ~

Information required by TitanFile

In order to establish a trust relationship between TitanFile and your identity federation service, TitanFile needs some information. All should be available in the configuration section of your federation service software:

- SAML entity ID
 - In ADFS Management Console, select "AD FS", choose "Edit Federation Service Properties...", and provide us with the value of "Federation Service Identifier" from the dialog box as in the screenshot below.

Federation Service Properties
General Organization Events Federation Service display name:
TtanFile
Example: Fabrikam Federation Service Federation Service name:
sso.titanfile.com
Example: fs.fabrikam.com Federation Service identifier:
http://sso.titanfile.com/adfs/services/trust
Example: http://fs.fabrikam.com/adfs/services/trust
Web SSO lifetime: 430 🗘 minutes
OK Cancel Apply

- SAML metadata XML file.
 - This can typically be downloaded from <u>https://localhost/federationmetadata/2007-06/federationmetadata.xml</u> where localhost is your ADFS server name. Please provide us with the XML file or the URL to download the XML file if it's publicly accessible.

Final remarks

After both ends have been configured correctly - the identity federation (ADFS) end and the TitanFile service end - then the single sign on can be tested. Attempting to test intermediate configuration is not possible due to the way the SAML 2.0 protocol works.