Axure Cloud for Business / Axure Cloud for On-Premises

Axure Cloud for Business with Microsoft ADFS

Overview

This document will walk you through setting up Single Sign-On (SSO) for Axure Cloud for Business or Axure Cloud for Business On-Premises.

> **Note:** This document assumes you have some prior knowledge of server configurations and ADFS.

Prerequisites

- Functioning Active Directory domain controller, DNS, DHCP, ASE, database, and Certificate Authority servers.
- Administrative access to both Axure Cloud for Business (Super Admin or Technical Admin roles) and ADFS.
- If using Axure Cloud for Business (hosted on Axure servers), your ADFS server must have proper firewall ports open to be able to communicate with Axure Cloud for Business.
- If using Axure Cloud for Business On-Premises, your server must:
  - Installed
  - Configured to work with SSL.
- The ADFS server must already be joined to the same domain as the Active Directory (AD).
- Domain account attributes must be configured before you start

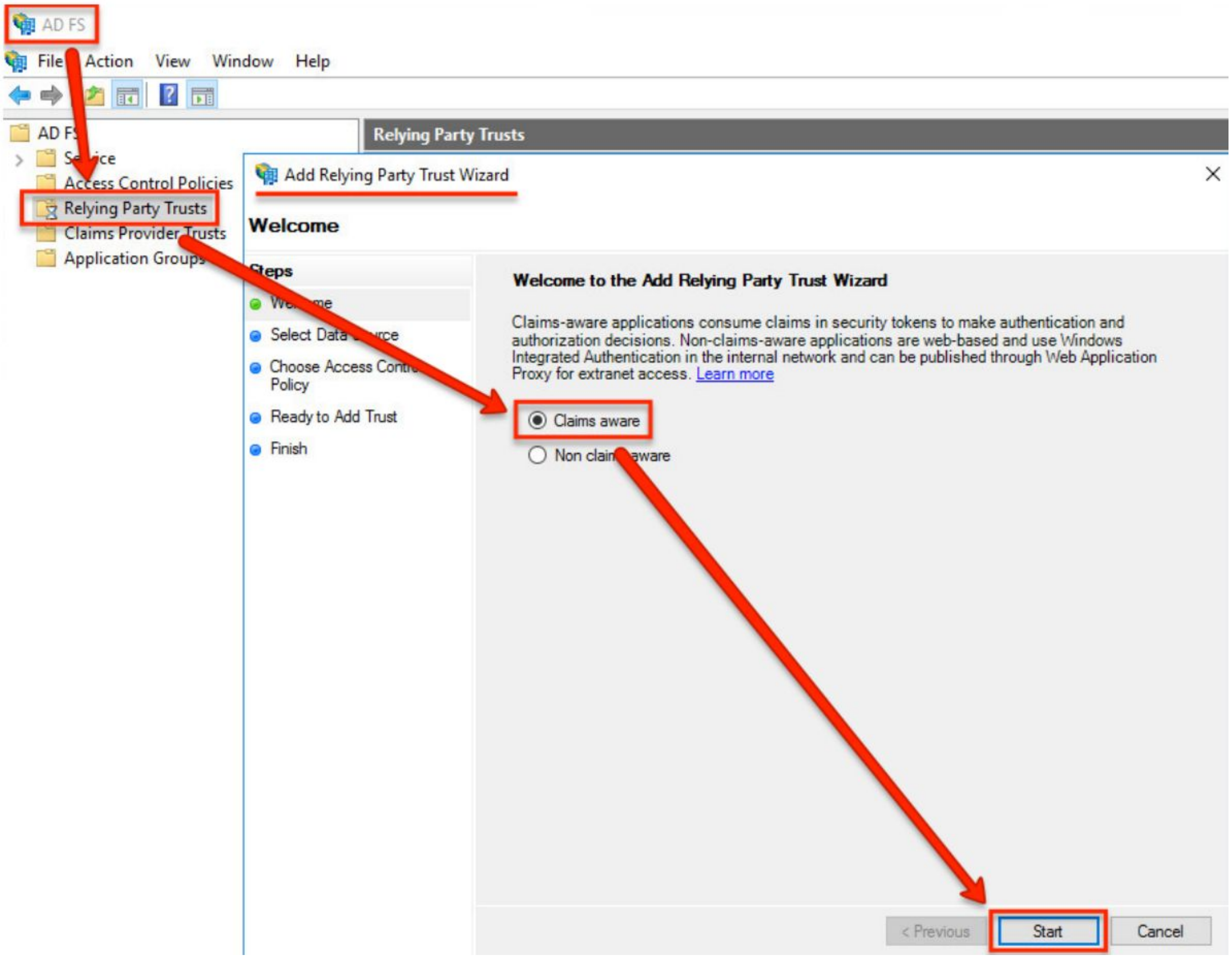
Configuring ADFS for Axure Cloud for Business

For Axure Cloud for Business or Axure Cloud for Business On-Premises to work with ADFS, the ADFS server must be configured first.

Add Relying Party Trust for Axure Cloud for Business

1. Open the **Server Manager Dashboard** and go to **Tools > AD FS Management.**
2. In the **AD FS** window, right-click **Relying Party Trust** in the left column and select **Add Relying Party Trust**

3. In the wizard that appears, make sure **Claims aware** is selected on the “Welcome” screen and click the **Start** button .



Welcome to the Add Relying Party Trust Wizard

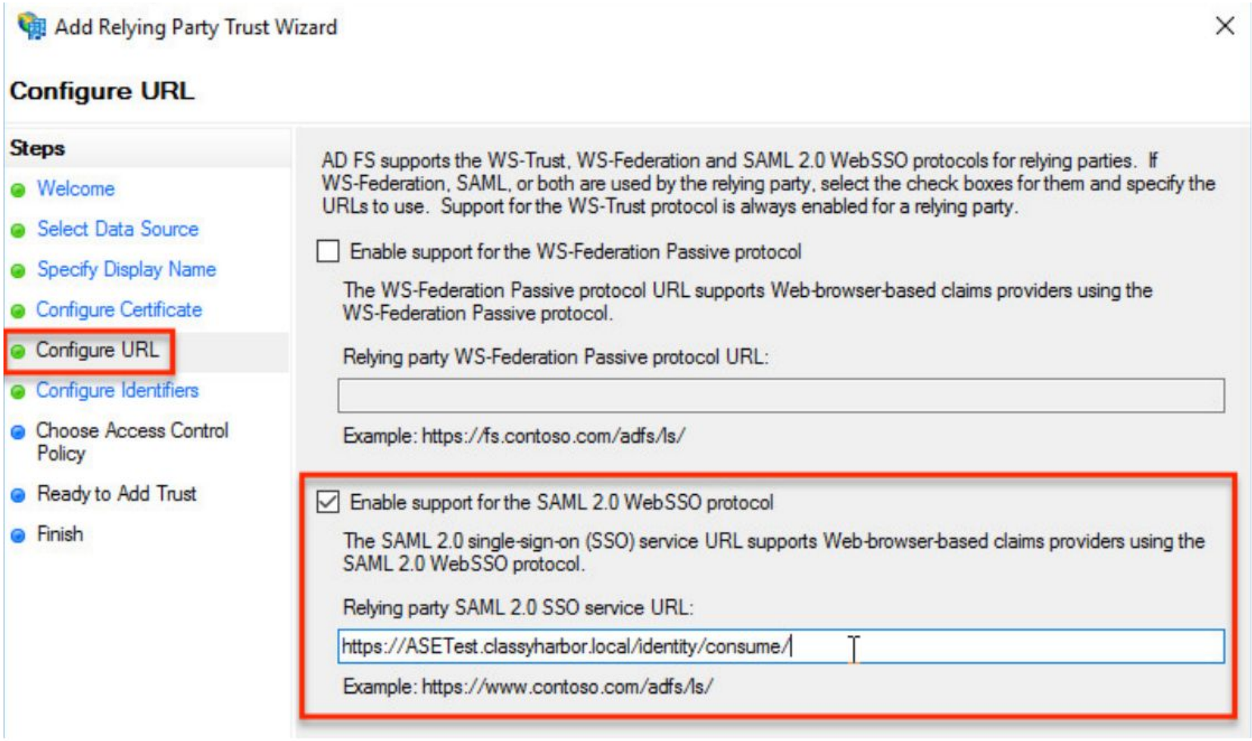
Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

4. On the **Select Data Source** screen, select **Enter data about the relying party manually**.
5. On the **Specify Display Name** screen, enter a descriptive display name for the relying party. Click **Next**, then **Next** again on the Configure Certificate screen.
6. On the **Configure URL** screen, check the box for **Enable support for the SAML 2.0 WebSSO protocol**.
7. Enter your service URL in the text field. The service URL is case sensitive and must be in the following formats:
    a. If you have a private instance of Axure Cloud for Business hosted on Axure servers:
    `https://[domain].axure.cloud/identity/consume`
        i. **[domain]** should be replaced with your private instance’s domain.
    b. If you have an on-premises installation of Axure Cloud for Business:
    `https://[hostname].[domain]/identity/consume`
        i. **[hostname]** should be replaced by the hostname of the Axure Cloud for Business On-Premises server

ii. **[domain]** should be replaced with the local domain the Axure Cloud for Business On-Premises server is installed on.



Add Relying Party Trust Wizard

Configure URL

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

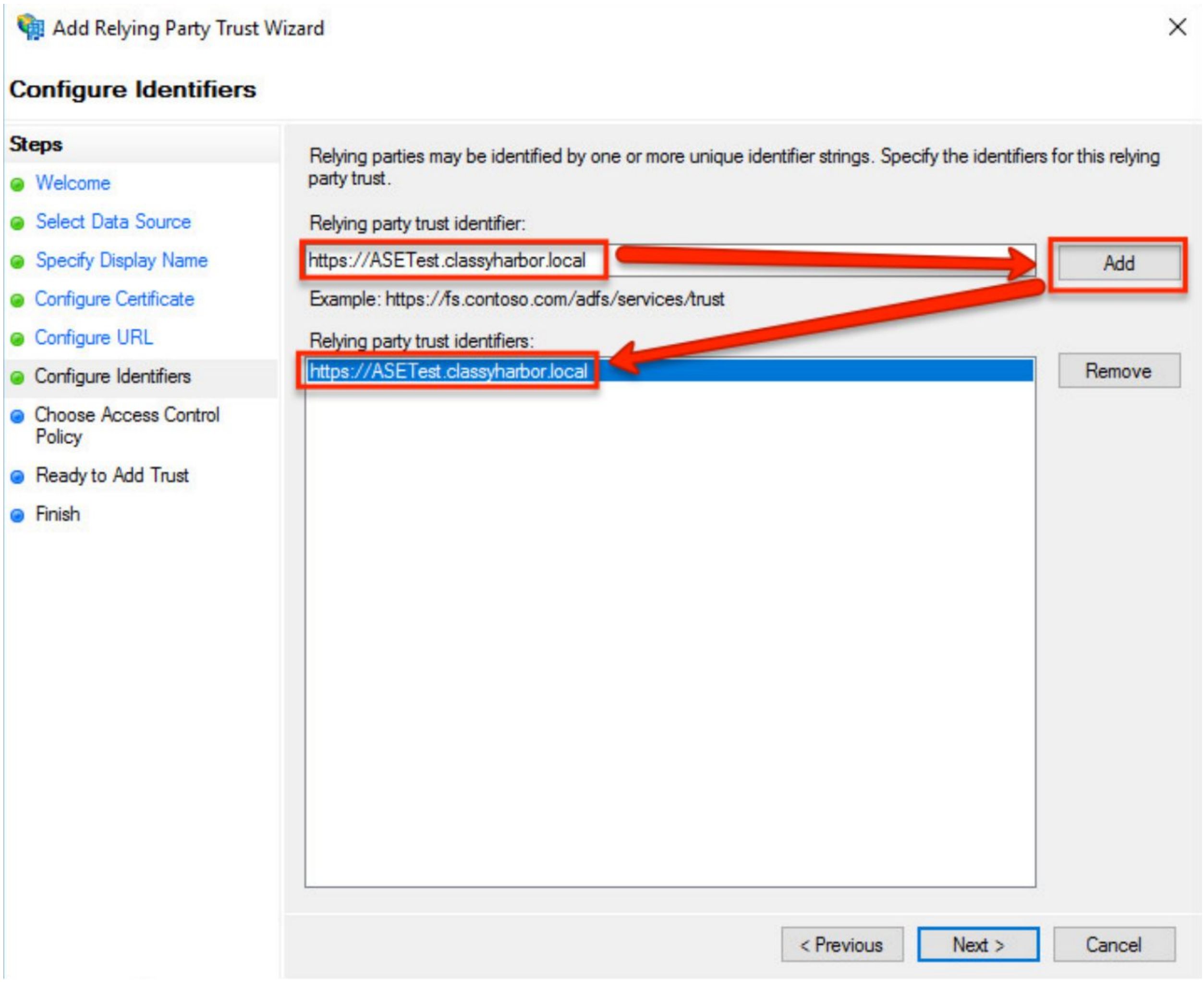
Relying party SAML 2.0 SSO service URL:

https://ASETest.classyharbor.local/identity/consume/

Example: https://www.contoso.com/adfs/ls/

8. On the **Configure Identifiers** screen, enter your Axure Cloud for Business server's URL in FQDN format:
   a. `https://[domain].axure.cloud`

9. Click **Add** to add it to the list of relying party trust identifiers.



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier: https://ASETest.classyharbor.local

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers: https://ASETest.classyharbor.local

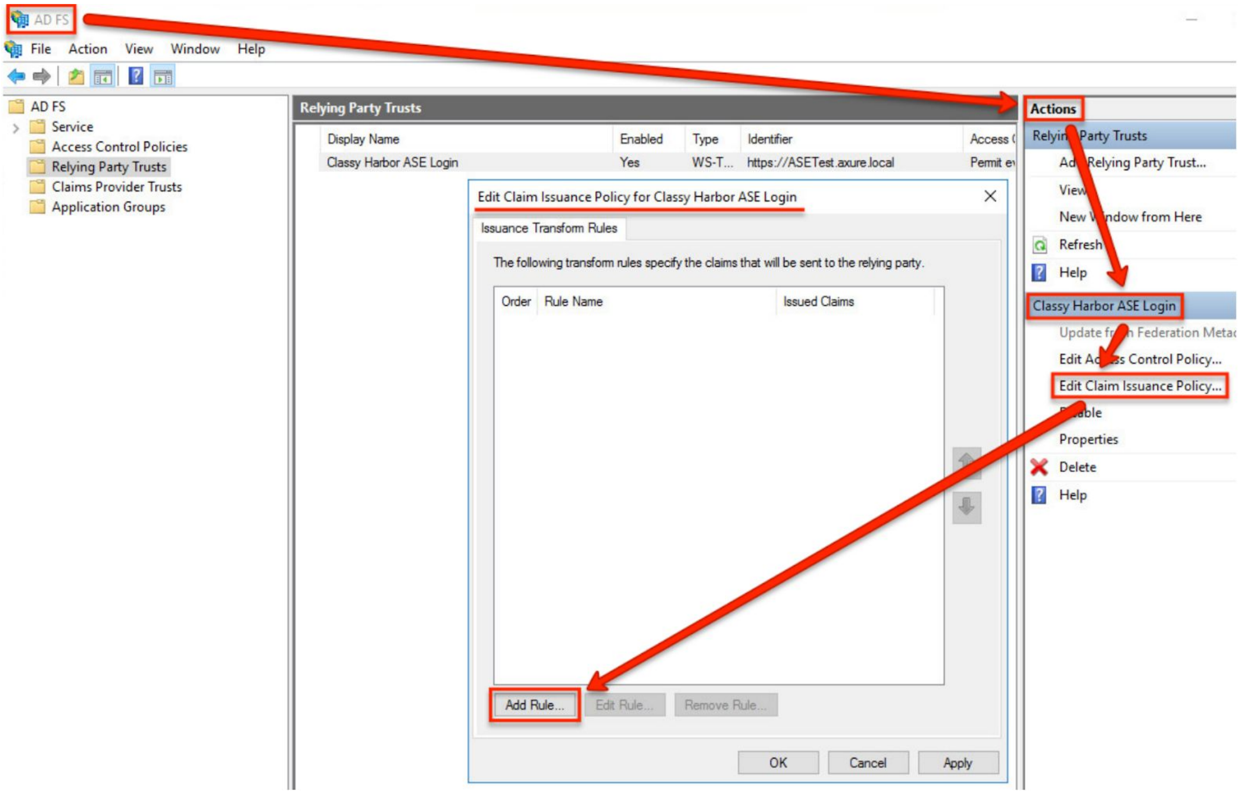
10. On the **Choose Access Control Policy** screen**,** select **Permit Everyone** for now. You can configure permissions after set up.
11. On the **Ready to Add Trust** screen, click **Next.**
12. On the **Finish** screen, make sure the box for **Configure claims issuance policy for this application** is checked and click **Close** .

Map Email to Domain Account

Once Axure Cloud for Business is added as a Relying Party Trust, emails will need to mapped to domain accounts.

1. Back in the **AD FS** window, go to the **Actions** panel on the right and click **Edit Claim Issuance Policy** under the name of the relying party trust you created in the previous section.

2. In the window that appears, click the **Add Rule** button.



Display Name	Enabled	Type	Identifier	Access (
Classy Harbor ASE Login	Yes	WS-T...	https://ASETest.axure.local	Permit ev

The following transform rules specify the claims that will be sent to the relying party.

3. On the **Choose Rule Type** screen, select **Send LDAP Attributes as Claims** in the **Claim rule template** dropdown.
4. On the **Configure Claim Rule** screen, enter a name for the rule and select **Active Directory** in the **Attribute store** dropdown.
5. At the bottom of the screen map your LDAP attributes to the outgoing claim types by adding a new row and select **E-Mail-Addresses** in the left dropdown and **Name ID** on the right.

> **Note:** If the dropdowns in the table are empty, your domain account attributes haven't been configured. Configure them now, and return to this step to continue.

6. Click **Finish** to close the wizard, then click **Apply** in the **Edit Claim Issuance Policy** window to complete the mapping.

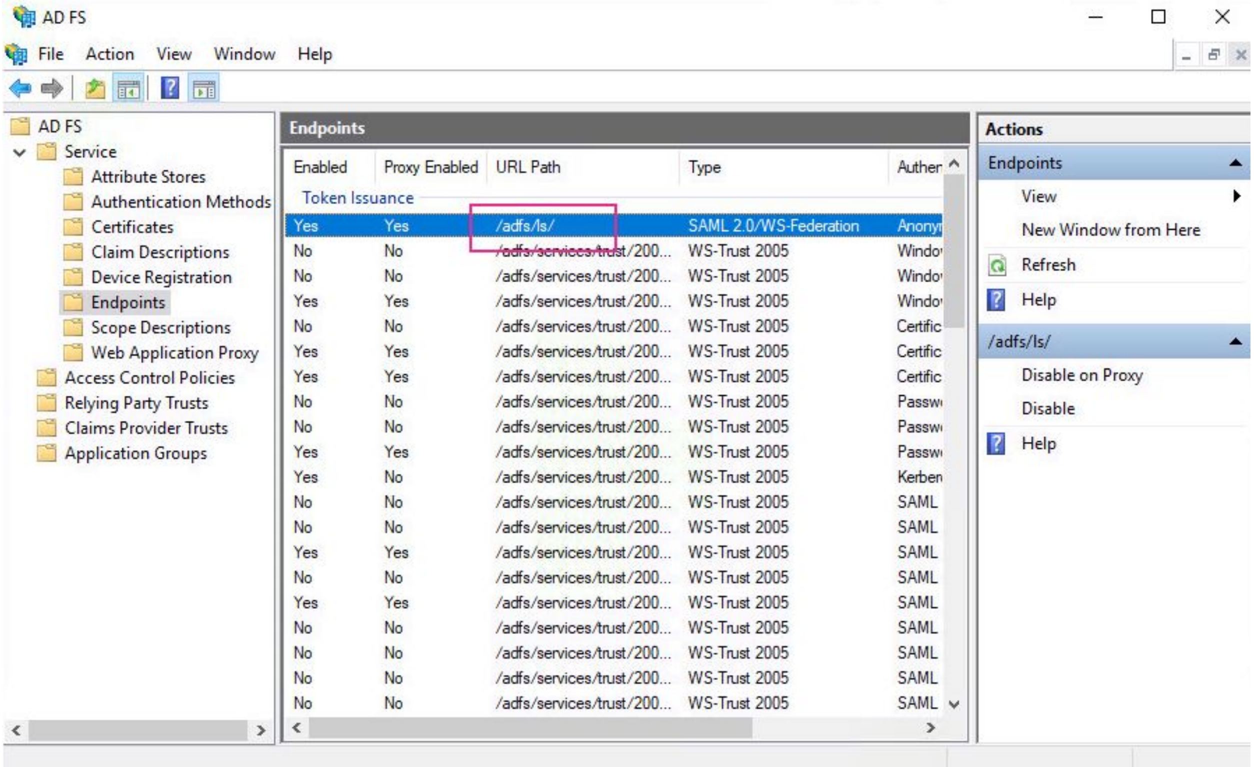
Collect Single Sign-On Service URL

The Single Sign-On Service URL will be entered in Axure Cloud for Business. This will be the ADFS server's FQDN, followed by the **SAML 2.0/WS-Federation** endpoint.

To find the **SAML 2.0/WS-Federation** endpoint, follow these steps:

1. Open the **ADFS Management window.**
2. Select the **Endpoints** folder to display a list of the ADFS endpoints.

3. Look for the **SAML 2.0/WS-Federation** type endpoint.



Enabled	Proxy Enabled	URL Path	Type	Auther
Token Issuance				
Yes	Yes	/adfs/ls/	SAML 2.0/WS-Federation	Anonyr
No	No	/adfs/services/trust/200...	WS-Trust 2005	Windo
No	No	/adfs/services/trust/200...	WS-Trust 2005	Windo
Yes	Yes	/adfs/services/trust/200...	WS-Trust 2005	Windo
No	No	/adfs/services/trust/200...	WS-Trust 2005	Certific
Yes	Yes	/adfs/services/trust/200...	WS-Trust 2005	Certific
Yes	Yes	/adfs/services/trust/200...	WS-Trust 2005	Certific
No	No	/adfs/services/trust/200...	WS-Trust 2005	Passw
No	No	/adfs/services/trust/200...	WS-Trust 2005	Passw
Yes	Yes	/adfs/services/trust/200...	WS-Trust 2005	Passw
Yes	No	/adfs/services/trust/200...	WS-Trust 2005	Kerber
No	No	/adfs/services/trust/200...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/200...	WS-Trust 2005	SAML
Yes	Yes	/adfs/services/trust/200...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/200...	WS-Trust 2005	SAML
Yes	Yes	/adfs/services/trust/200...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/200...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/200...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/200...	WS-Trust 2005	SAML
No	No	/adfs/services/trust/200...	WS-Trust 2005	SAML

4. Append the endpoint to your ADFS servers FQDN. For example: `https://[hostname].[domain]/adfs/ls`

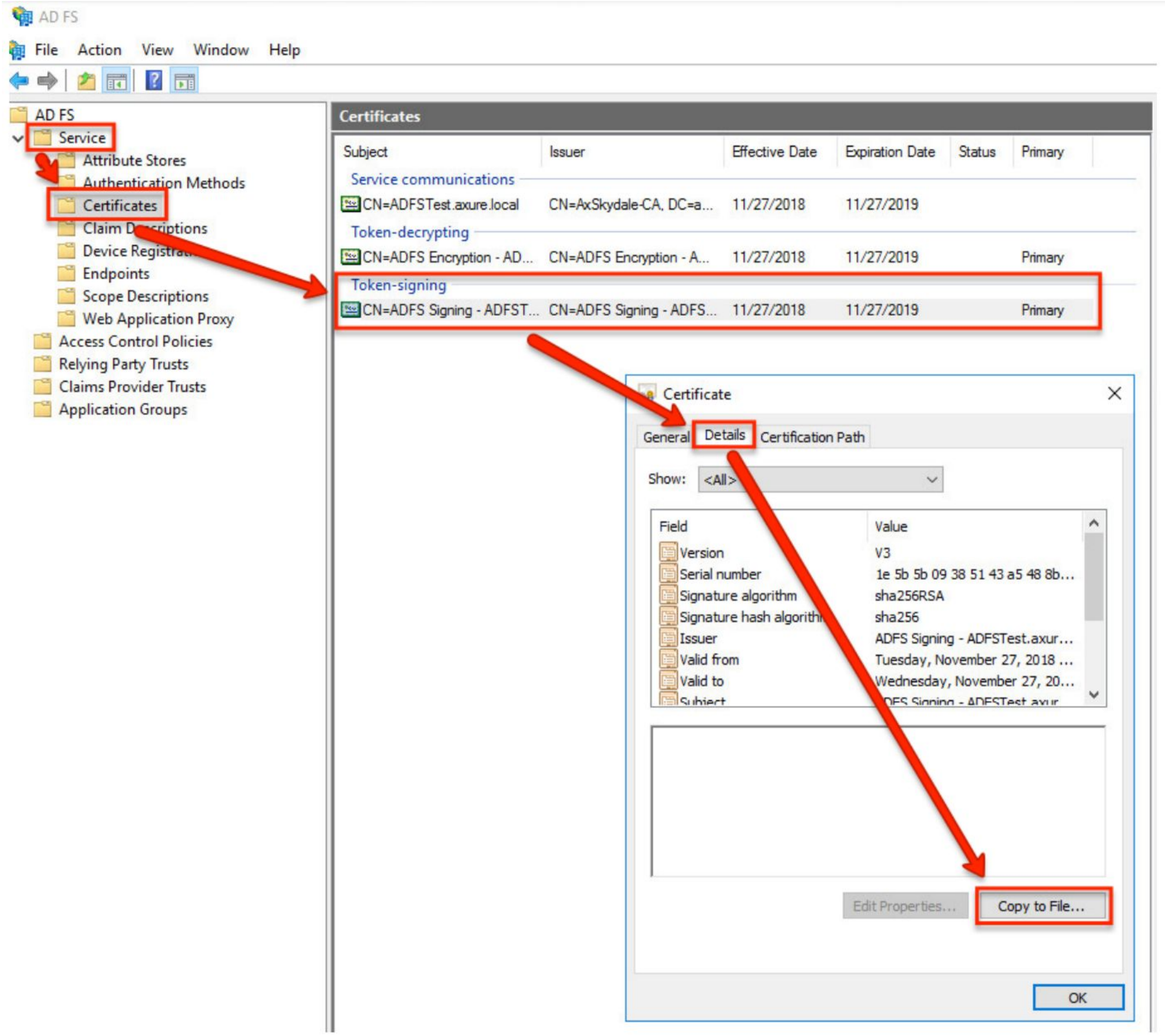
> **Note:** You'll need this URL in the Enabling Single Sign-On in Axure Cloud for Business section of this guide, so make sure to note down this URL.

Export ADFS Security Certificate

In this topic, a security certificate will be exported which is required in the next section of this guide.

1. Back in the **AD FS** window, expand the **Service** item in the left column and select **Certificates**.
2. Double-click the certificate listed under **Token-signing** in the center of the window.

3. In the window that appears, select the **Details** tab and click **Copy to File**.

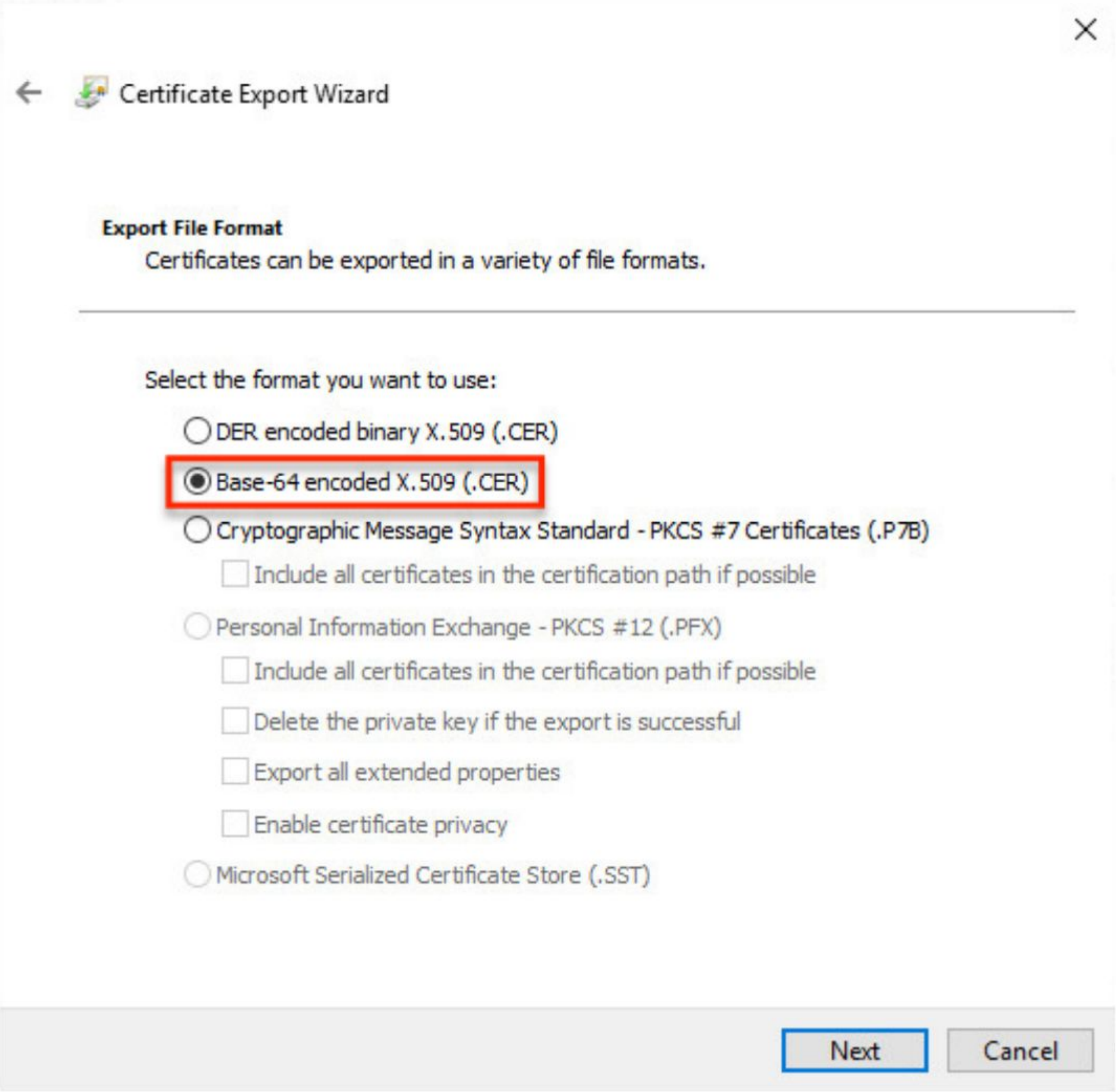


Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=ADFSTest.axure.local	CN=AxSkydale-CA, DC=a...	11/27/2018	11/27/2019		
Token-decrypting					
CN=ADFS Encryption - AD...	CN=ADFS Encryption - A...	11/27/2018	11/27/2019		Primary
Token-signing					
CN=ADFS Signing - ADFST...	CN=ADFS Signing - ADFS...	11/27/2018	11/27/2019		Primary

Field	Value
Version	V3
Serial number	1e 5b 5b 09 38 51 43 a5 48 8b...
Signature algorithm	sha256RSA
Signature hash algorith	sha256
Issuer	ADFS Signing - ADFSTest.axur...
Valid from	Tuesday, November 27, 2018 ...
Valid to	Wednesday, November 27, 20...
Subject	ADFS Signing - ADFSTest.axur

4. In the wizard that appears, click **Next**.

5. Select **Base-64 encoded X.509 (.CER)** then **Next.**



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

6. On the following screen, enter a descriptive name for the exported .CER file and select a save location.

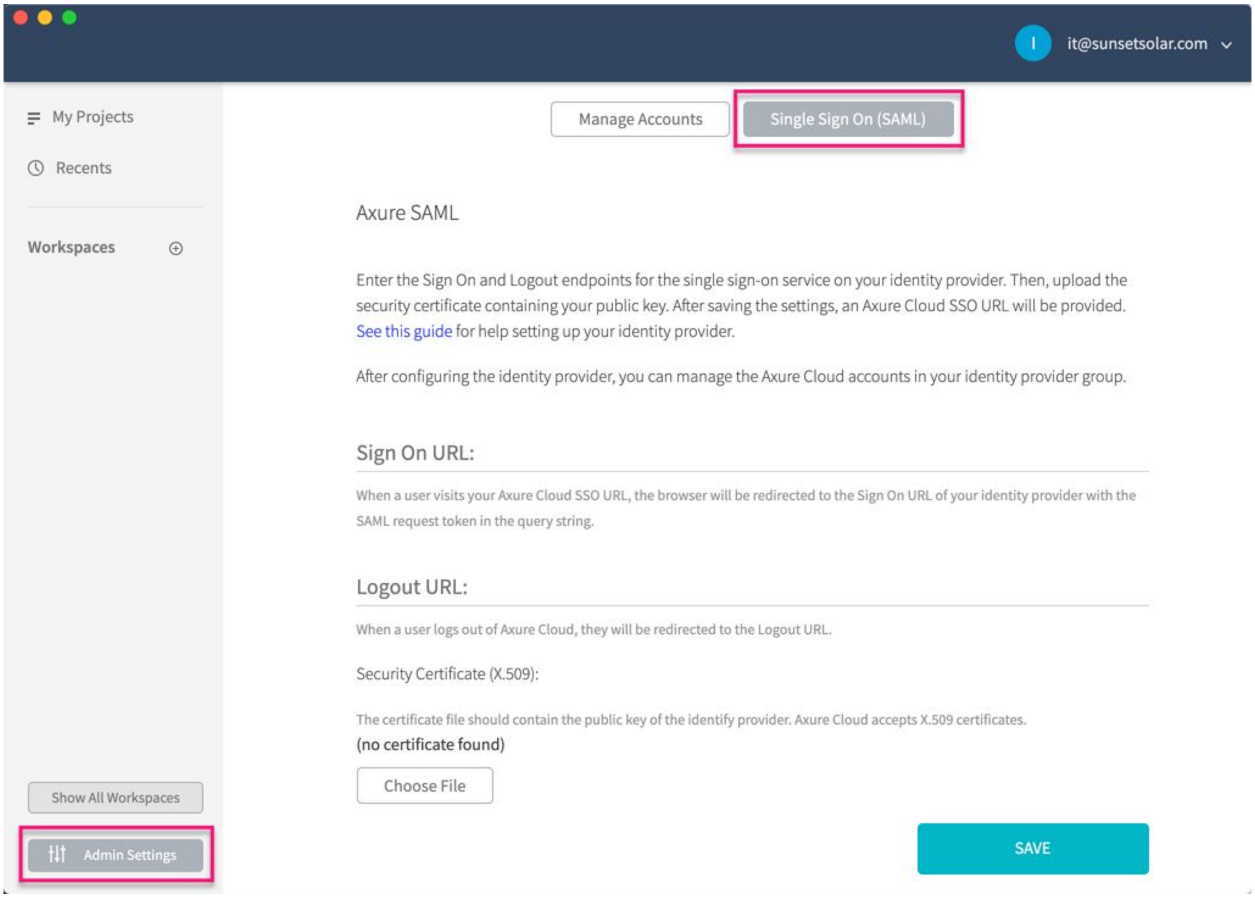
> **Note:** You'll need to access the file from Axure Cloud for Business in the next section of this guide, so make sure you have access to this file in the next section.

7. Click **Finish** to export the certificate file.

Enabling Single Sign-On in Axure Cloud for Business

After configuring ADFS, Axure Cloud for Business will need to be configured to work with ADFS using resources from the previous section.

1. Sign in to the Axure Cloud for Business web interface as a **Super Admin** or **Technical Admin.**
2. Click the **Admin Settings** button at the bottom left of the interface.
3. Click **Single Sign On (SAML)** at the top of the page.



Axure SAML

Enter the Sign On and Logout endpoints for the single sign-on service on your identity provider. Then, upload the security certificate containing your public key. After saving the settings, an Axure Cloud SSO URL will be provided. See this guide for help setting up your identity provider.

After configuring the identity provider, you can manage the Axure Cloud accounts in your identity provider group.

Sign On URL:

When a user visits your Axure Cloud SSO URL, the browser will be redirected to the Sign On URL of your identity provider with the SAML request token in the query string.

Logout URL:

When a user logs out of Axure Cloud, they will be redirected to the Logout URL.

Security Certificate (X.509):

The certificate file should contain the public key of the identify provider. Axure Cloud accepts X.509 certificates.

(no certificate found)

4. In the **Sign On URL** field, enter the URL from the [Collect Single Sign-On Service URL]() help topic.
5. In the **Logout URL** field, set this to any URL you like. This is the URL your users will be redirected to after signing out.
6. In the **Security Certificate (X.509)** field, click **Choose File** and upload the security certificate created in the “Export ADFS Security Certificate” topic.
7. Click **Save.**

Adding SSO to User Accounts

As a last step, users will need to have SSO enabled for their accounts. Instructions for adding SSO to accounts can be found here: https://docs.axure.com/axure-cloud/business/accounts-and-permissions/#adding-and-removing-saml-from-user-accounts