



AD FS Configuration for SSO

February, 2020

Table of Contents

Introduction	3
Assumptions.....	3
Preparation.....	4
AD FS Installation.....	6
AD FS Configuration.....	11
Envi Domain Configuration	19
WS-Trust SSO configuration	19
HTTP Redirect SSO configuration.....	20
Envi Testing.....	22
Appendix 1. Disabling the revocation checks for encryption and signing certificates.....	23
Appendix 2. SSL Certificates issuing	24

Introduction

The purpose of this document is to describe configuration of Active Directory Federation Services for Envi. The following table shows the abbreviations used in the document.

Abbreviation	Definition
AD	Active Directory
AD FS	Active Directory Federation Services
AD CS	Active Directory Certificate Services
CA	Certification Authority
CRL	Certificate Revocation List
IIS	Internet Information Services

Assumptions

The deployment process is based on a set of assumptions about installed software and system requirements:

- Envi SSO prototype is going to work with AD FS 4.0
- Base OS is Windows Server 2016
- AD is installed and configured
- Computer is joined to the domain
- AD CS is installed and configured (recommended)

Preparation

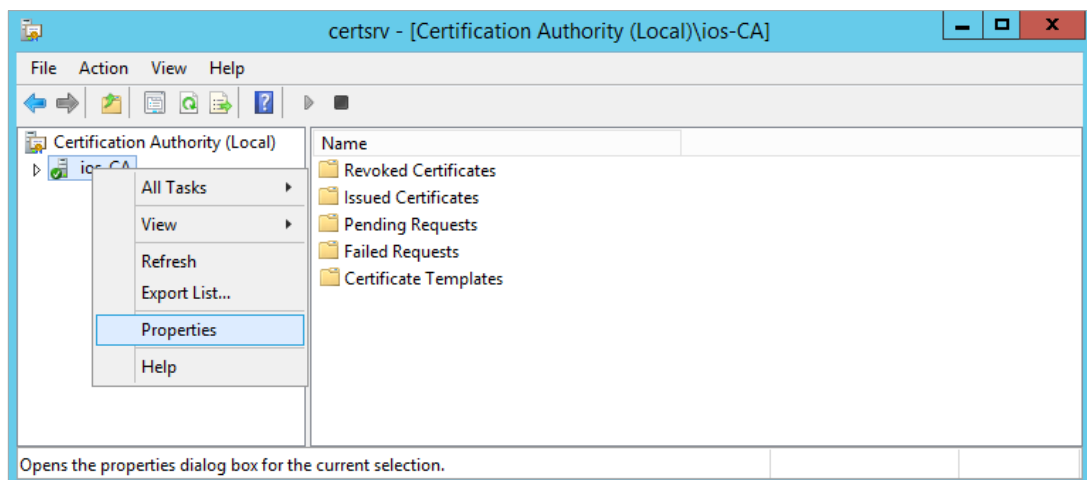
1. **SSL certificates.** Configuration of each AD FS server requires the next SSL certificates:

- Service Communication Certificate, which is used to serve HTTPS requests to the federation service
- Token Signing certificate, which is used to sign issued tokens to relying parties
- Token Encrypting/Decrypting certificate, which is used by claims providers who encrypt tokens issued to AD FS

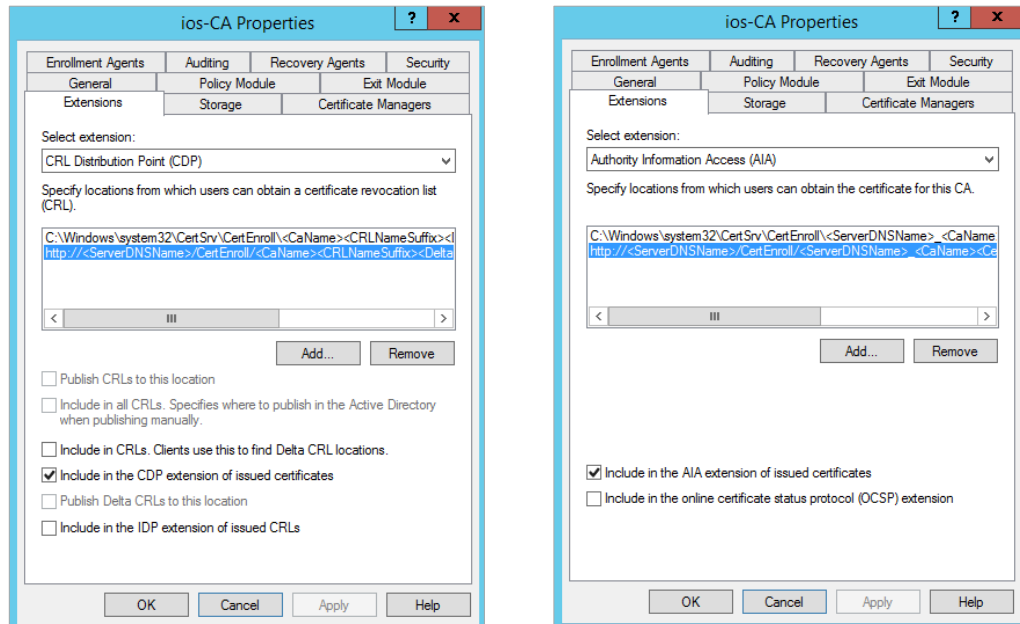
These SSL certificates must contain the **Server Authentication Enhanced Key Usage** value and it is recommended to use publicly trusted certificates for both production and testing deployments.

However, if you want to use self-signed SSL certificates in your configuration, you should be aware of the following aspects:

- If you have preinstalled AD CS and utilize your own CA, you should configure your CA to publish Certificate Revocation Lists (CRLs). To do this, edit the **Certification Authority Properties** under **Server Manager > Tools > Certification Authority**.



On the **CA Properties Extensions** tab, you need to select the **Include in the CDP extension of issued certificates** and **Include in the AIA extension of issued certificates** check boxes.



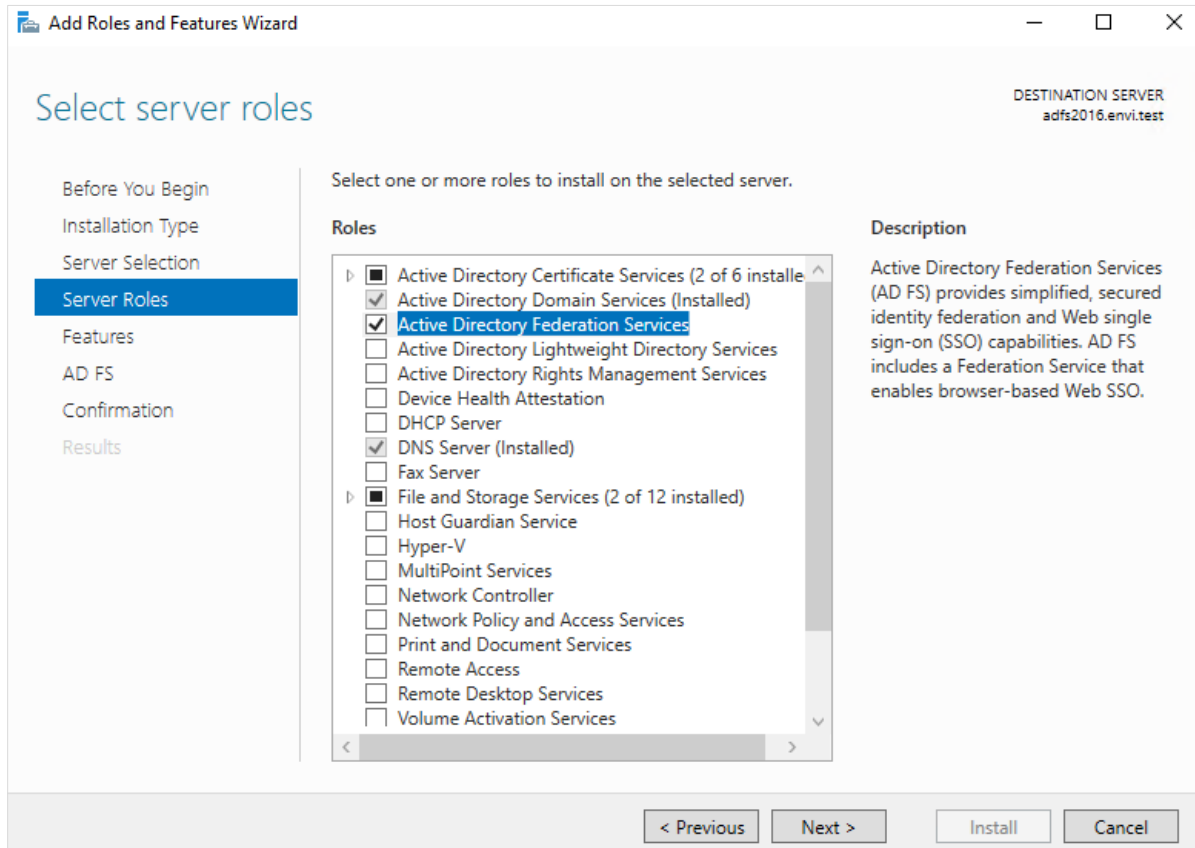
- If you are going to use self-signed SSL certificates created using OpenSSL or any other tool, you will need to disable the revocation check for encryption and signing certificates (please see [Appendix 1](#))

Prepare required SSL certificates (self-signed or publicly trusted) according to the above requirements (please follow the instructions in [Appendix 2](#) for creating self-signed SSL certificates using preconfigured CA).

2. **Permissions requirements.** The account that performs the installation and the initial configuration of AD FS must have local administrator permissions on the AD FS server.
3. **Service account requirements.** The domain user account that will be used for AD FS service running should be created. It can be a regular domain user account with no special permissions.

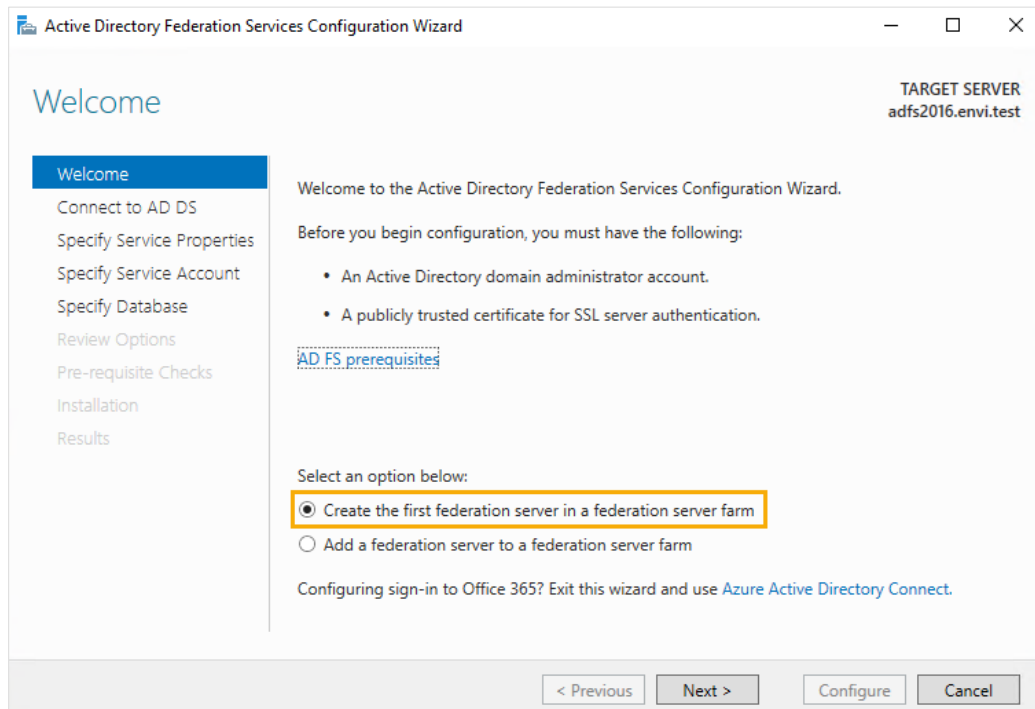
AD FS Installation

AD FS is installed as a Windows Server 2016 server role and does not require any additional downloads.



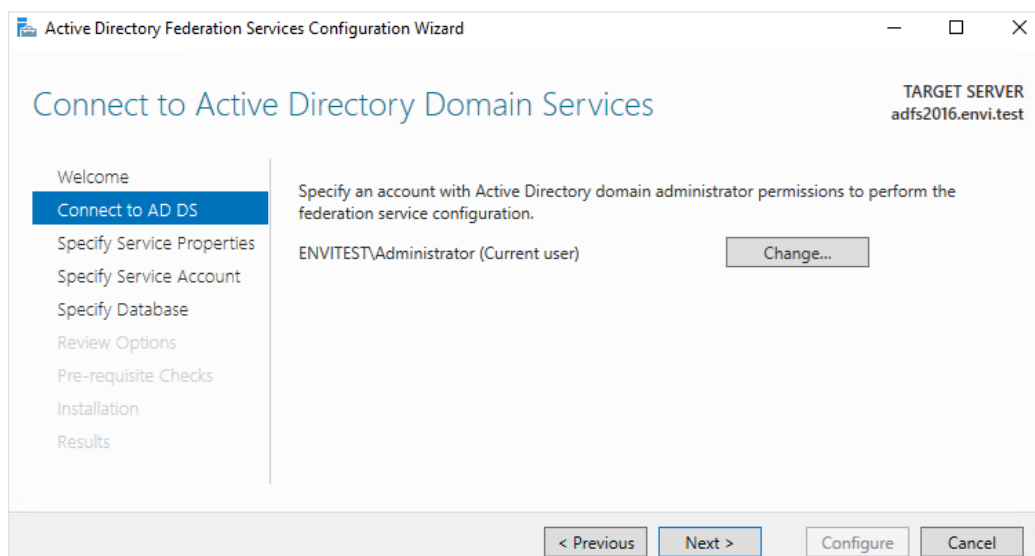
After successful AD FS 4.0 installation, configure the AD FS server and create Relying Party Trust:

1. On the first **Welcome** section of the AD FS Configuration Wizard, select **Create the first federation server in a federation server farm**.



2. On the **Connection to AD FS** section, specify the AD account that has permissions to perform the federation service configuration.

Note: Requirements for this account are described in the [Preparation](#) section.



- On the **Specify Service Properties** section, specify the properties you want. Import the SSL certificate for the service URL. Then, edit the default **Federation Service Name**, it will be your federation service address and serve as the root of your sign in URL.

Active Directory Federation Services Configuration Wizard

Specify Service Properties

TARGET SERVER
adfs2016.envi.test

Welcome

Connect to AD DS

Specify Service Properties

Specify Service Account

Specify Database

Review Options

Pre-requisite Checks

Installation

Results

SSL Certificate: adfs2016.envi.net

View

Federation Service Name: adfs2016.envi.test

Example: fs.contoso.com

Federation Service Display Name: ADFS 2016 TestLab

Users will see the display name at sign in.
Example: Contoso Corporation

< Previous Next > Configure Cancel

4. On the **Specify Service Account** section, specify service account for the AD FS service (please check requirements in the [Preparation](#) section).

Active Directory Federation Services Configuration Wizard

Specify Service Account

TARGET SERVER
adfs2016.envi.test

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a domain user account or group Managed Service Account.

☐ Create a Group Managed Service Account

Account Name: ENVITEST\

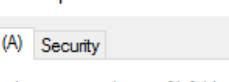
☒ Use an existing domain user account or group Managed Service Account

Account Name: ENVITEST\adfsvc Clear Select...

Account Password:

< Previous Next > Configure Cancel

Note: Ensure that your DNS settings contain **A** record created to support the **Federation Service** name.



adfs2016 Properties

Host (A) Security

Host (uses parent domain if left blank):

adfs2016

Fully qualified domain name (FQDN):

adfs2016.envi.test

IP address:

192.168.1.250

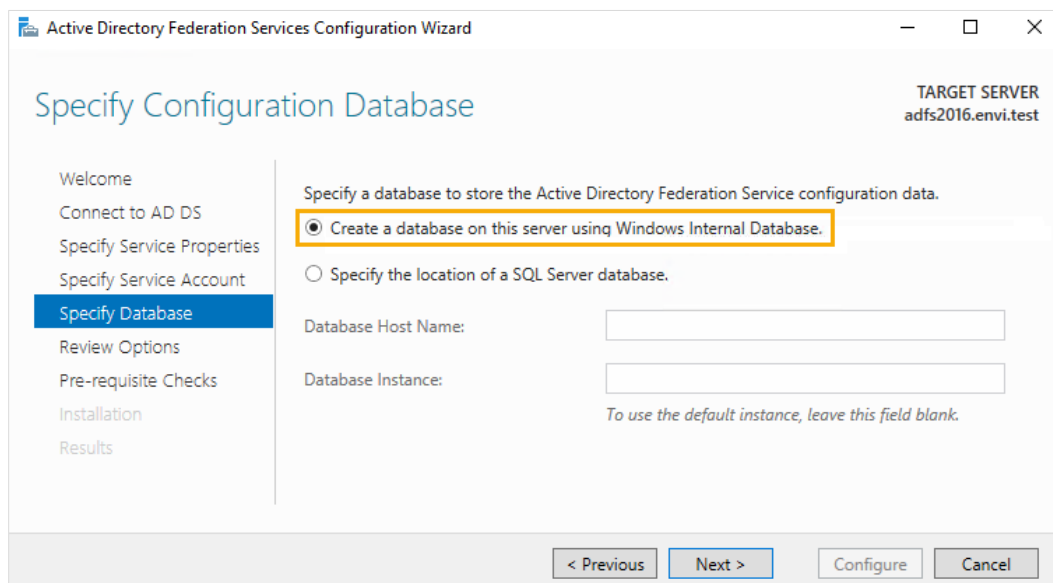
☐ Update associated pointer (PTR) record

AD FS Configuration for SSO

Without that **DNS** entry, application which support SSO will not be able to resolve the URL and connect to the AD FS service.

AD FS requires database to store configuration and artifact information and can use either the Windows Internal Database (WID) or MS SQL Server.

5. On the **Specify Database** section, select **Create a database on this server using Windows Internal Database**.

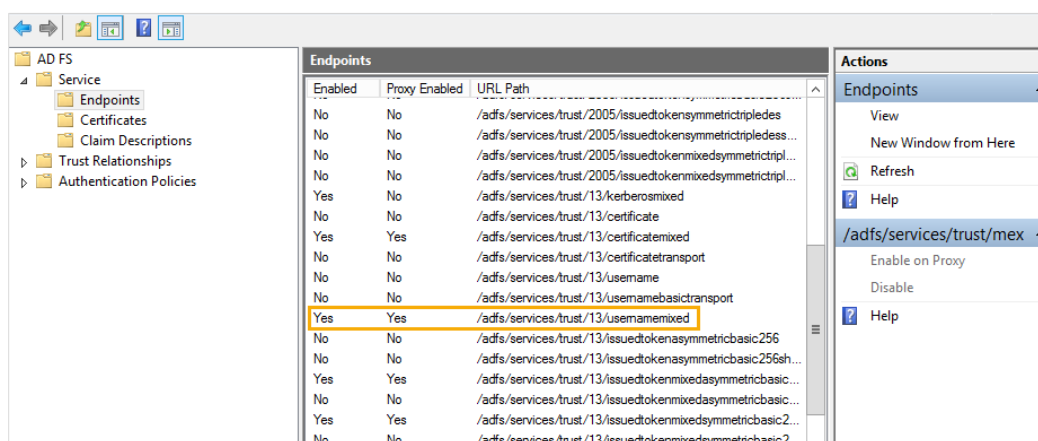


6. Proceed with **Pre-requisite Checks** section, and then complete the configuration.

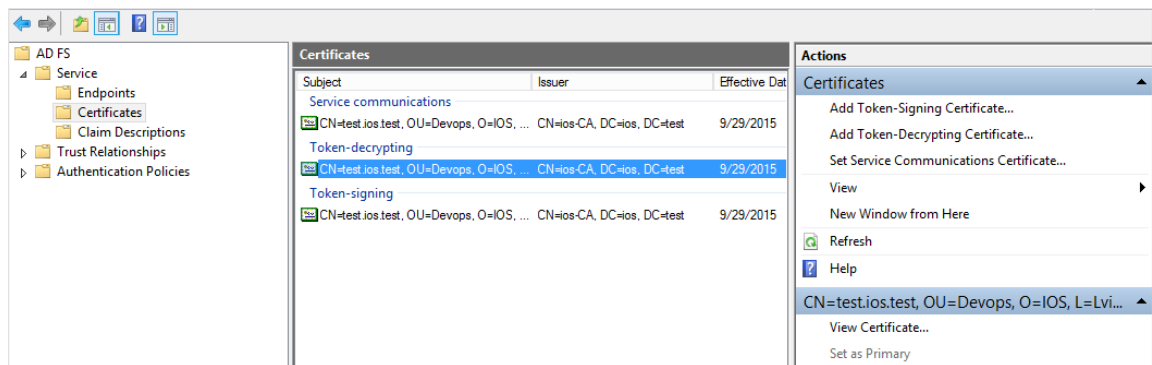
After installation, main AD FS tool is located on the following location: **Server Manager > Tools > AD FS Management**.

To make sure you have properly installed AD FS, check the following settings on AD FS Management:

- **Endpoints**. Verify that `/adfs/services/trust/13/usernamemixed` endpoint is **Enabled** and **Proxy Enabled** contains the **Yes** value.



- **Certificates.** Make sure that all three subjects have the certificates. Certificate for **Service communications** was specified during ADFS configuration, while **Token-signing** and **Token-decrypting** were generated automatically during the configuration.



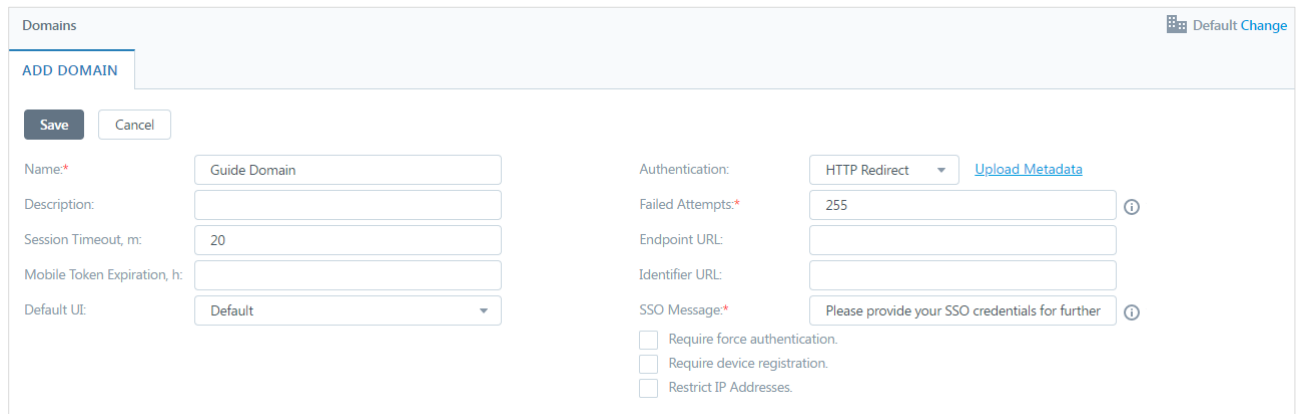
To change any of these certificates you can use your own publicly trusted certificates or generate the new ones.

After generating or purchasing the new certificates, you can assign them from **AD FS Management** console, from the **Certificates** action pane. After you assign the new certificates, you need to restart **AD FS Windows Service**.

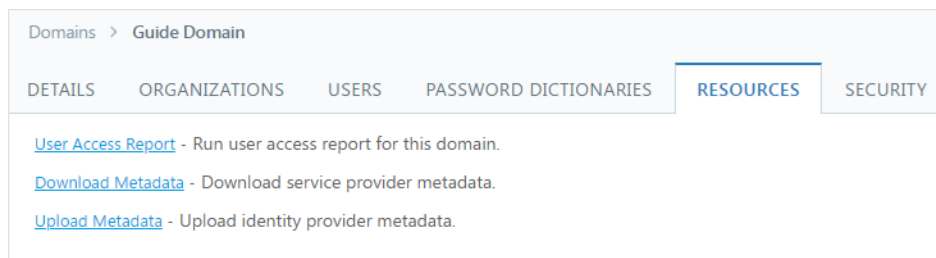
AD FS Configuration

To configure ADFS access for Envi, perform the following configuration steps:

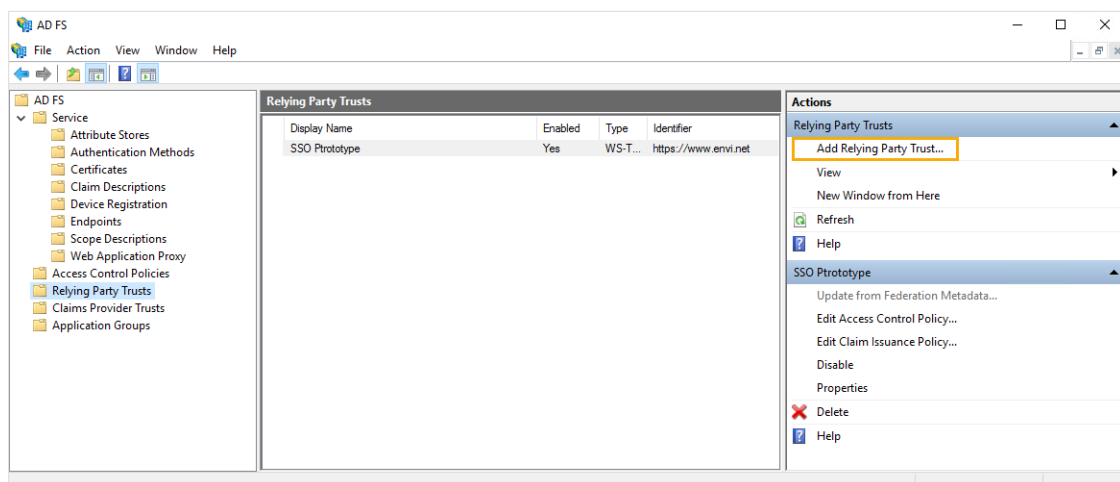
1. Sign in the Envi application, navigate to your domain details and click **Edit**. Change domain authentication type to **HTTP Redirect** or **WS-Trust**. Save changes.



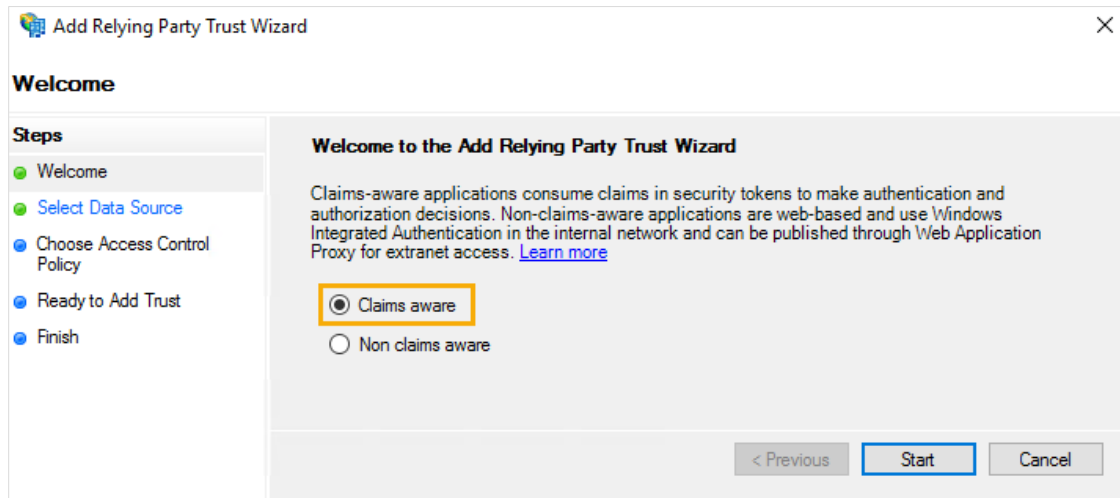
2. Navigate to the **Resources** tab, and then select **Download Metadata**. Save metadata file to the appropriate location, and then copy it to the server instance with ADFS.



3. Open AD FS Management.
4. On the **Actions** section, select **Add Relying Party Trust**.

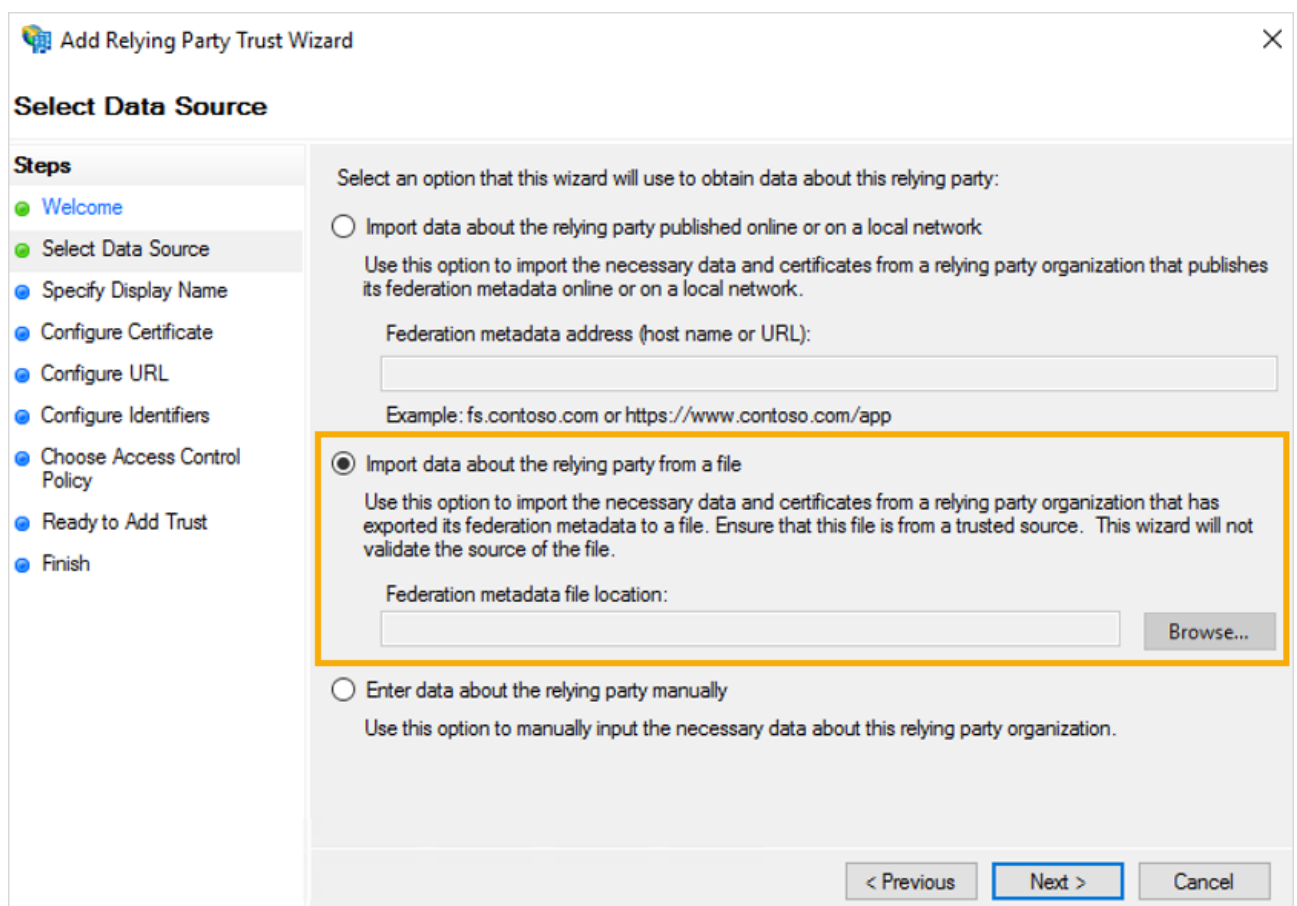


5. Follow the wizard's steps. Select **Claims aware**, and then click **Start**.



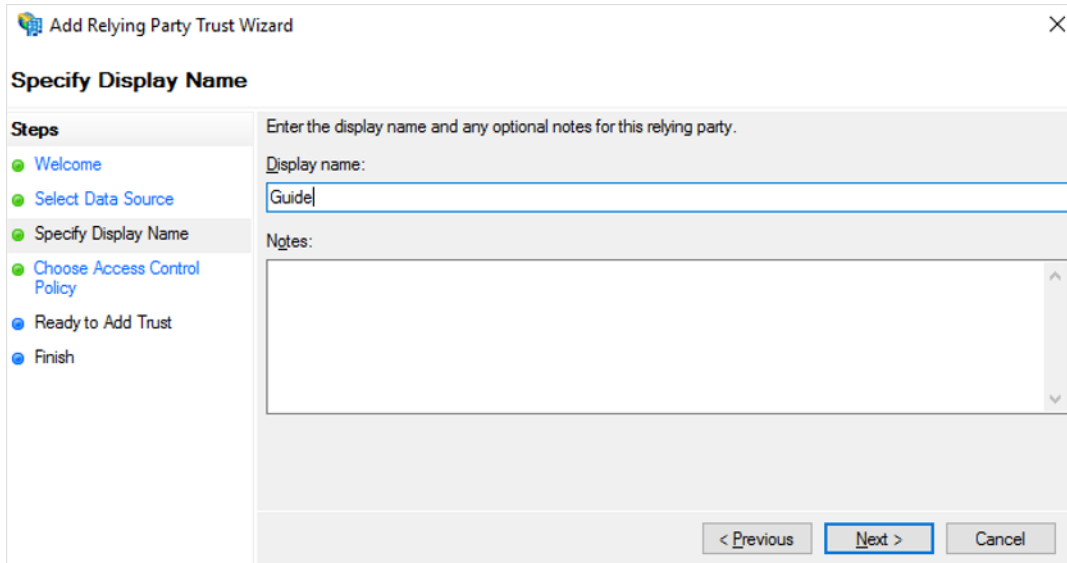
The screenshot shows the 'Add Relying Party Trust Wizard' window. The 'Steps' pane on the left lists: Welcome, Select Data Source, Choose Access Control Policy, Ready to Add Trust, and Finish. The main pane is titled 'Welcome to the Add Relying Party Trust Wizard' and contains explanatory text about claims-aware applications. Two radio buttons are present: 'Claims aware' (selected and highlighted with an orange box) and 'Non claims aware'. At the bottom right are buttons for '< Previous', 'Start' (highlighted with a blue border), and 'Cancel'.

6. Select **Import data about the relying party from a file**, click the **Browse** button, and then select location of the metadata file from Envi. Click **Next**.



The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Select Data Source' step. The 'Steps' pane on the left lists: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main pane asks to 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 'Import data about the relying party published online or on a local network', 'Import data about the relying party from a file' (selected and highlighted with an orange box), and 'Enter data about the relying party manually'. The 'Import from file' option includes a text box for 'Federation metadata file location:' and a 'Browse...' button. At the bottom right are buttons for '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

7. Enter Display name. Click **Next**.



Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

Steps

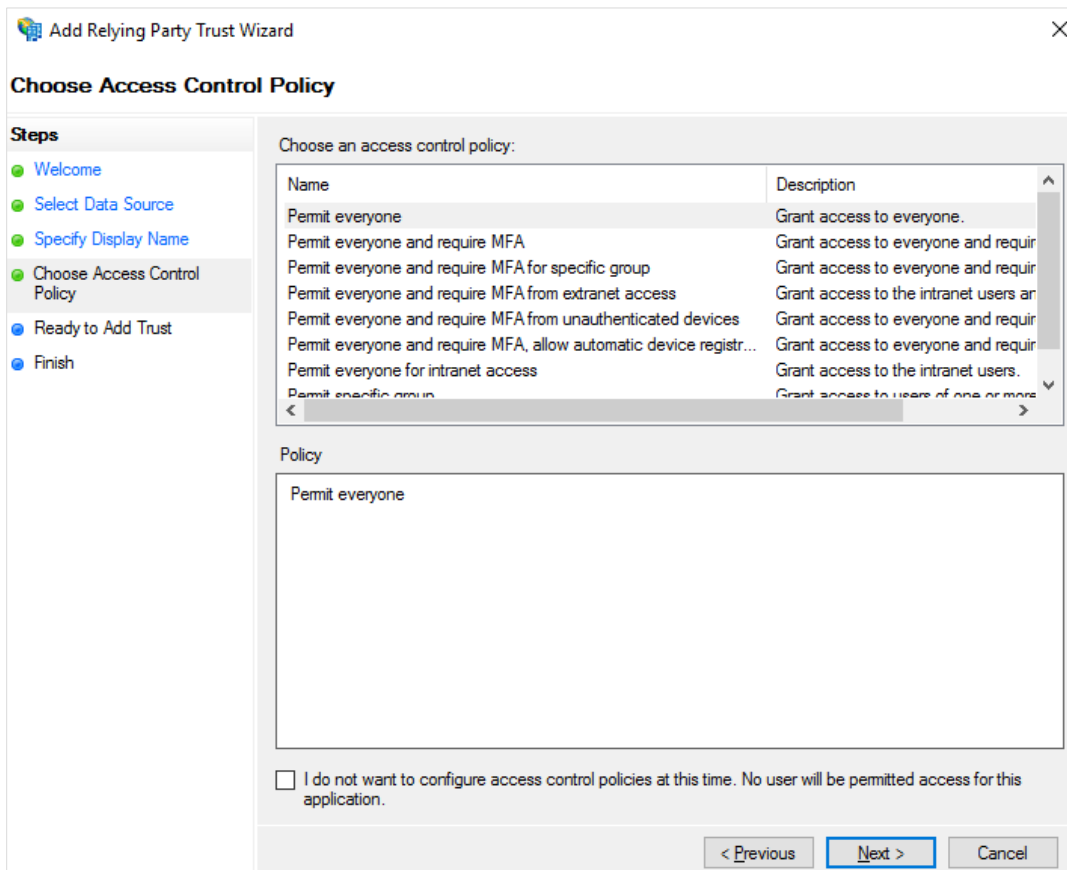
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Display name:

Notes:

< Previous **Next >** Cancel

8. Select **Permit everyone**. Click **Next**.



Add Relying Party Trust Wizard

Choose Access Control Policy

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for a specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more groups.

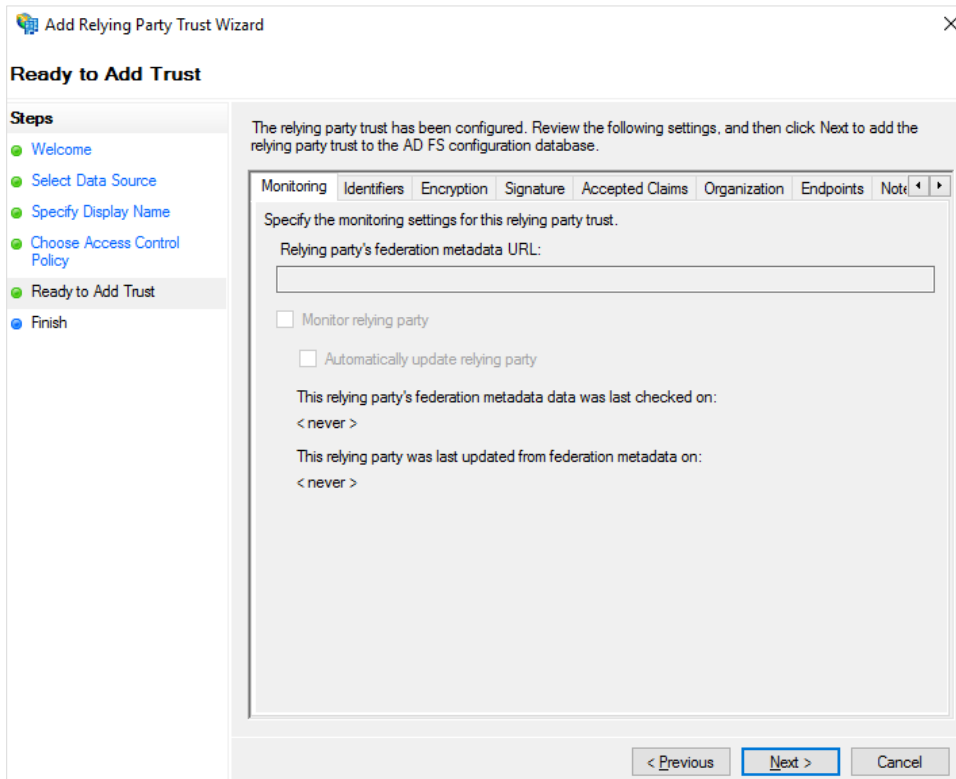
Policy:

Permit everyone

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

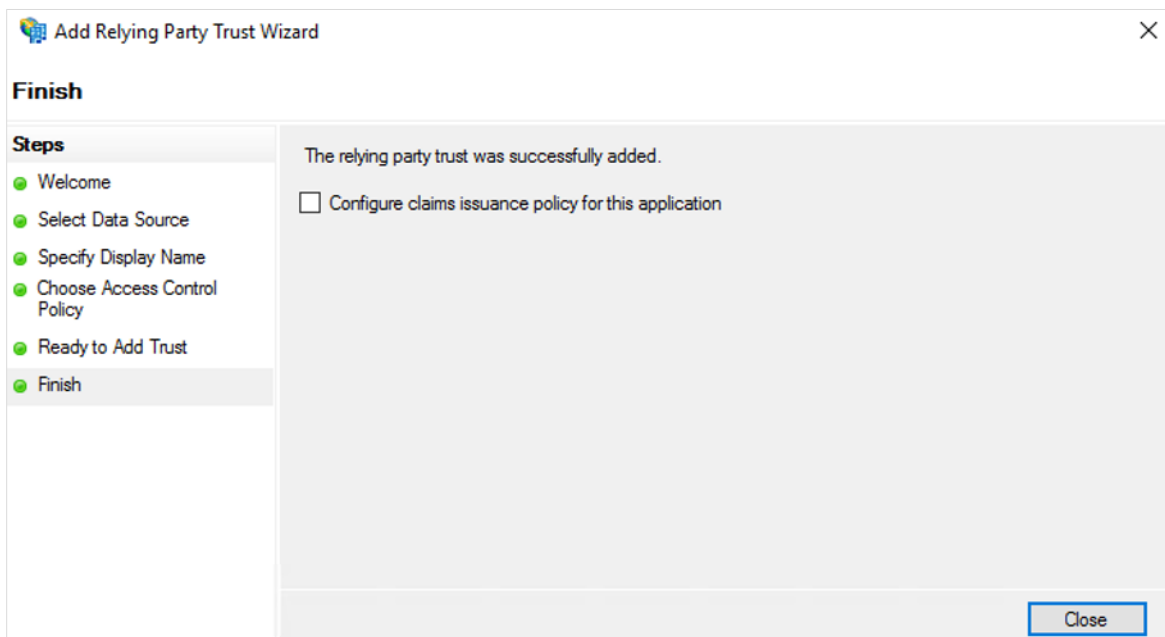
< Previous **Next >** Cancel

9. Click **Next**.



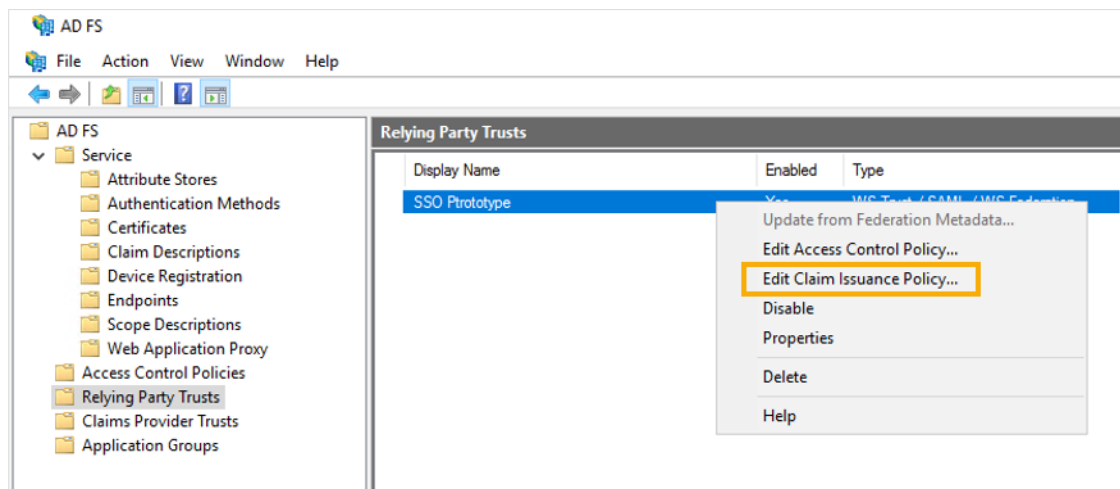
The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Ready to Add Trust' step. The left pane lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Access Control Policy, Ready to Add Trust, and Finish. The main pane displays a message: 'The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.' Below this is a tabbed interface with tabs for Monitoring, Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Notes. The 'Monitoring' tab is selected, showing options to specify monitoring settings. A text box for 'Relying party's federation metadata URL:' is present. Below it are two unchecked checkboxes: 'Monitor relying party' and 'Automatically update relying party'. Further down, two labels indicate the last checked and updated times, both set to '< never >'. At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'.

10. Clear the check box (it's not necessary, but with selected check box you can continue with additional configuration). Click **Close**.

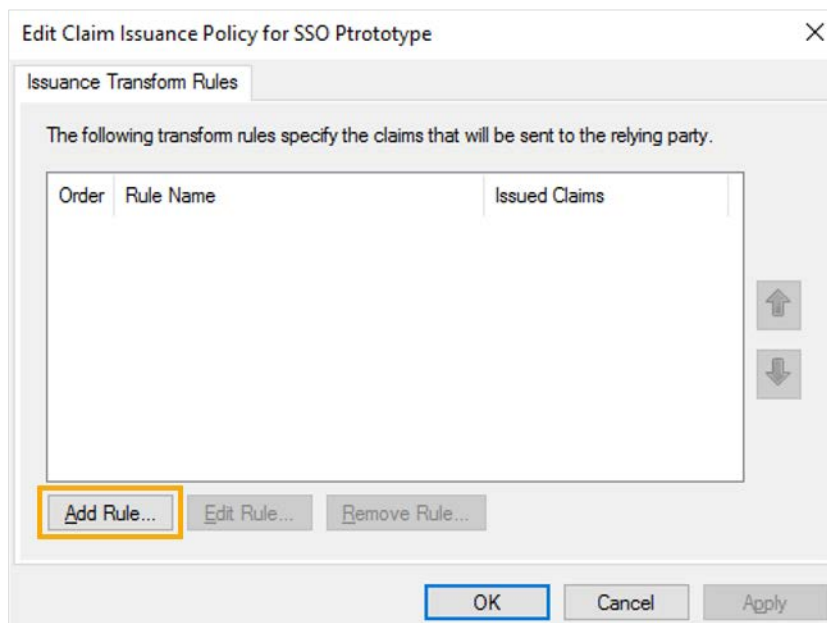


The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Finish' step. The left pane lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Access Control Policy, Ready to Add Trust, and Finish. The main pane displays a message: 'The relying party trust was successfully added.' Below this is an unchecked checkbox labeled 'Configure claims issuance policy for this application'. At the bottom right is a 'Close' button.

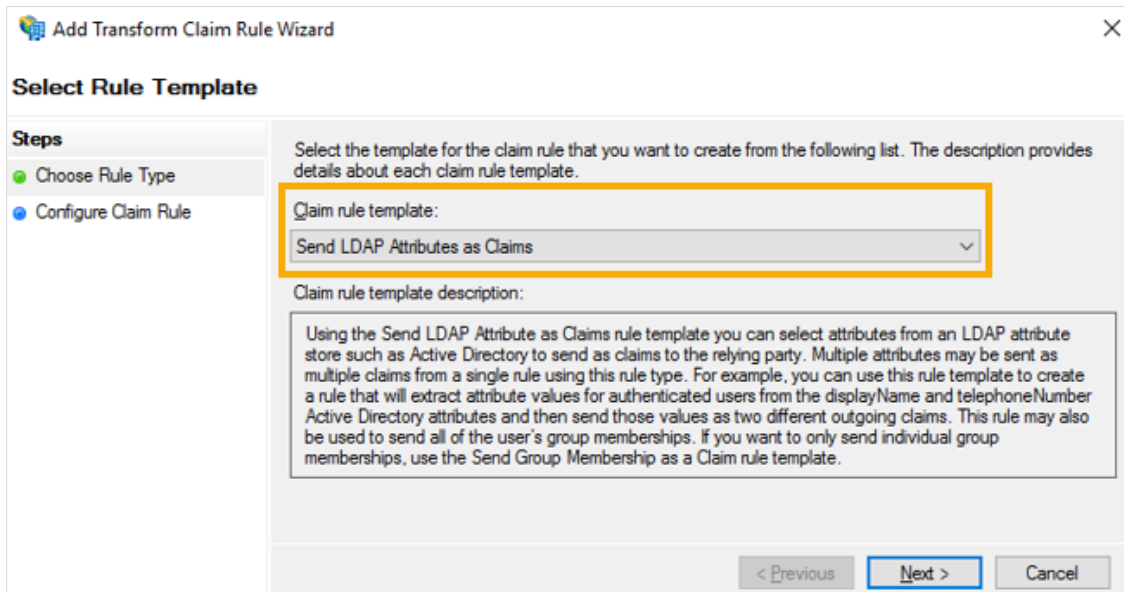
11. Select created Relying Party Trust record and right click it. From the context menu, select **Edit Claim Issuance Policy**.



12. Click the **Add Rule** button.



13. On the **Choose Rule Type** step, select **Send LDAP Attributes as Claims**, and then click **Next**.



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

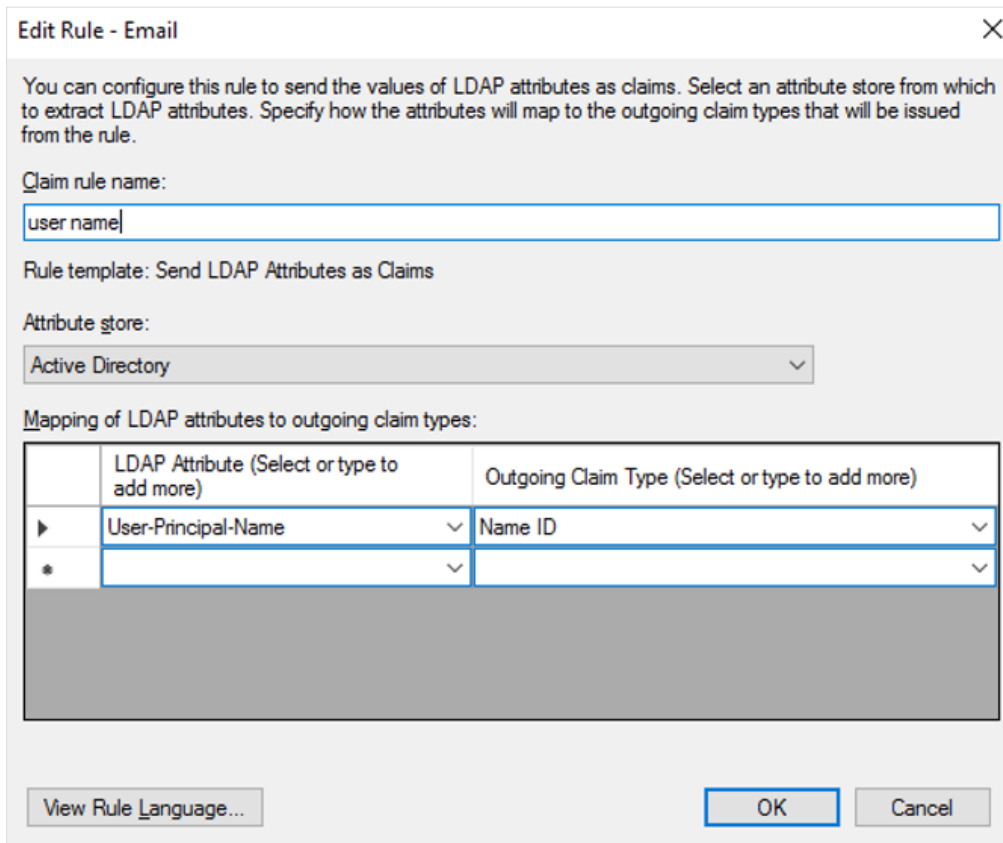
Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous Next > Cancel

14. Specify rule name and select **Active Directory** as attribute store value. Click the first **LDAP Attribute** column on the **Mapping of LDAP attributes to outgoing claim types** section, and then select the **User-Principal-Name** value. Click the second **Outgoing Claim Type** column, and then specify the **Name ID** value.



Edit Rule - Email

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.

Claim rule name:

user name

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

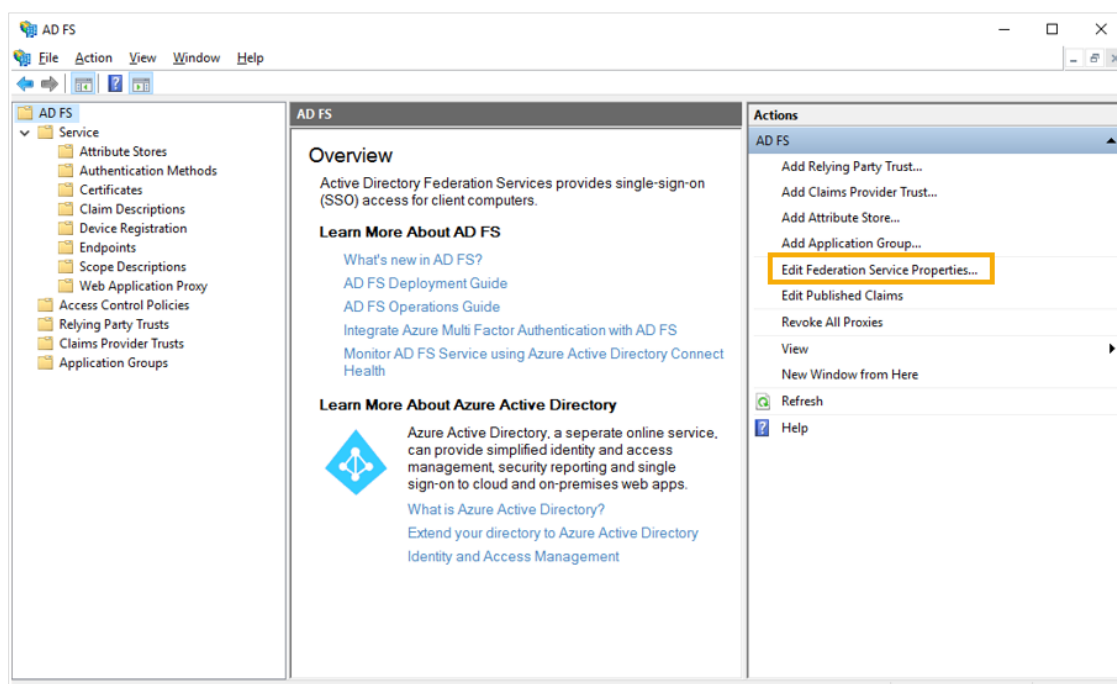
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

View Rule Language... OK Cancel

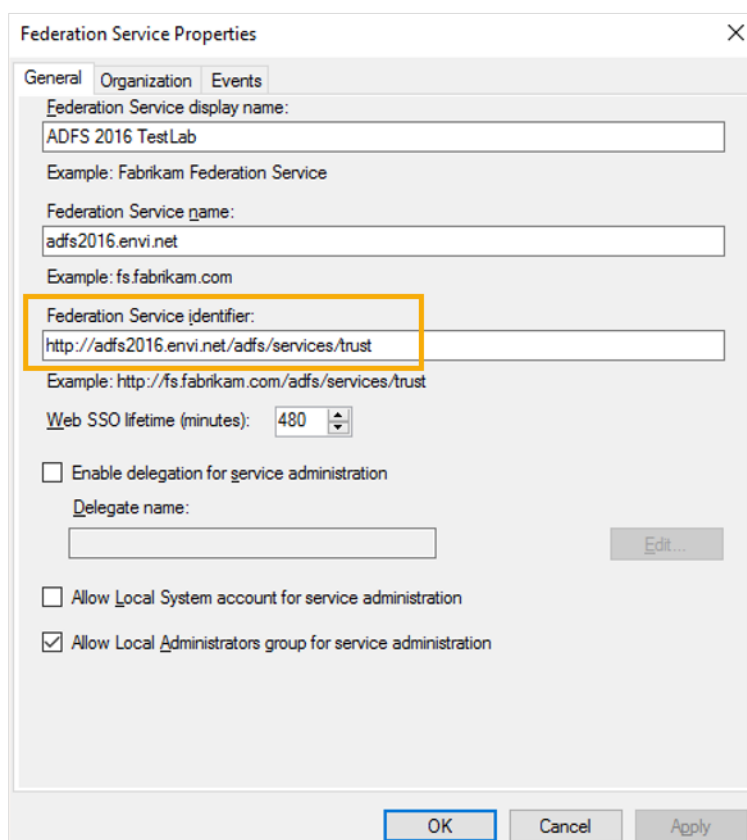
AD FS Configuration for SSO

15. Click **OK** button, and then close window.

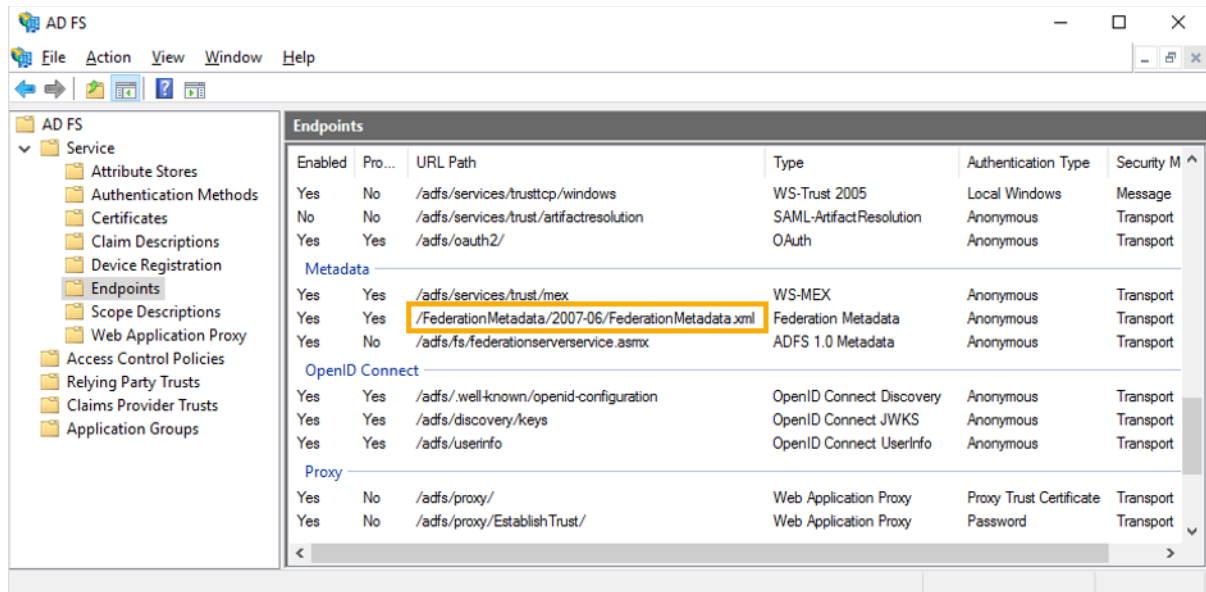
16. Select the main **AD FS** node, and then click **Edit Federation Service Properties**.



17. Go to the **General** tab and copy the **Federation Service Identifier** value—you will need it for further configuration of authentication in Envi.



18. Open **AD FS > Service > Endpoints**, navigate to the **Metadata** section, and then copy URL of the **Federation Metadata** type—you will need it for further configuration of authentication in Envi.



Enabled	Pro...	URL Path	Type	Authentication Type	Security M
Yes	No	/ads/services/trusttcp/windows	WS-Trust 2005	Local Windows	Message
No	No	/ads/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous	Transport
Yes	Yes	/ads/oauth2/	OAuth	Anonymous	Transport
Metadata					
Yes	Yes	/ads/services/trust/mex	WS-MEX	Anonymous	Transport
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Anonymous	Transport
Yes	No	/ads/fs/federationsservice.asmx	ADFS 1.0 Metadata	Anonymous	Transport
OpenID Connect					
Yes	Yes	/ads/.well-known/openid-configuration	OpenID Connect Discovery	Anonymous	Transport
Yes	Yes	/ads/discovery/keys	OpenID Connect JWKS	Anonymous	Transport
Yes	Yes	/ads/userinfo	OpenID Connect UserInfo	Anonymous	Transport
Proxy					
Yes	No	/ads/proxy/	Web Application Proxy	Proxy Trust Certificate	Transport
Yes	No	/ads/proxy/EstablishTrust/	Web Application Proxy	Password	Transport

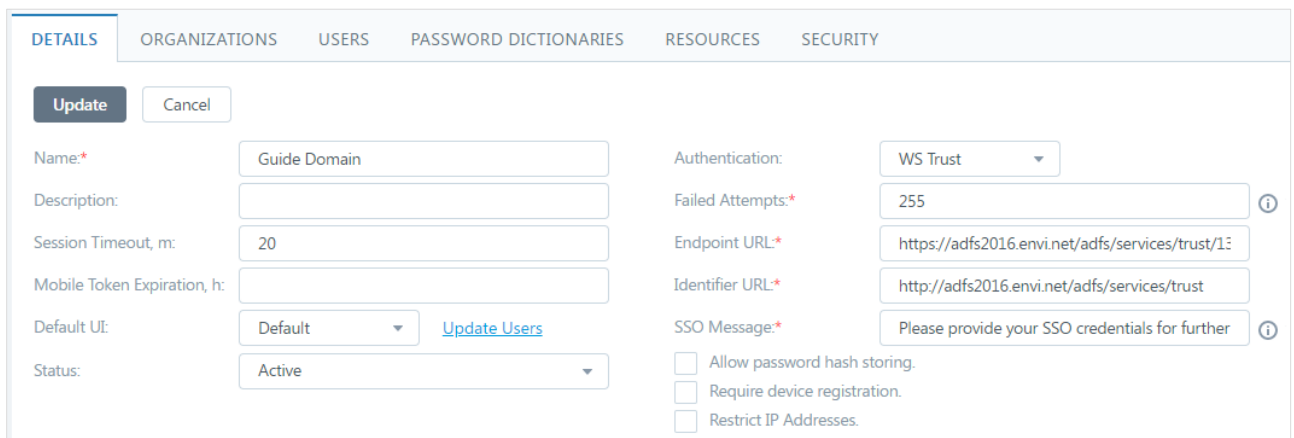
Configuration of AD FS is successfully completed. You can begin to configure your domain settings in Envi.

Envi Domain Configuration

Sign in Envi application, navigate to your domain details, and then click **Edit**.

WS-Trust SSO configuration

1. Change type of domain authentication to **WS Trust**.
2. Enter the following values and save the changes:
 - **Endpoint URL** field—value that consists of IDP Server Base URL + adfs/services/trust/13/usernamemixed
 - **Identifier URL** field—[Federation Service Identifier](#) value



The screenshot shows the 'DETAILS' tab of the Envi Domain Configuration interface. It includes tabs for ORGANIZATIONS, USERS, PASSWORD DICTIONARIES, RESOURCES, and SECURITY. The 'Update' button is highlighted. The configuration fields are as follows:

Field	Value
Name*	Guide Domain
Description:	
Session Timeout, m:	20
Mobile Token Expiration, h:	
Default UI:	Default (with 'Update Users' link)
Status:	Active
Authentication:	WS Trust
Failed Attempts*	255
Endpoint URL*	https://adfs2016.envi.net/adfs/services/trust/13/usernamemixed
Identifier URL*	http://adfs2016.envi.net/adfs/services/trust
SSO Message*	Please provide your SSO credentials for further

Additional options at the bottom:

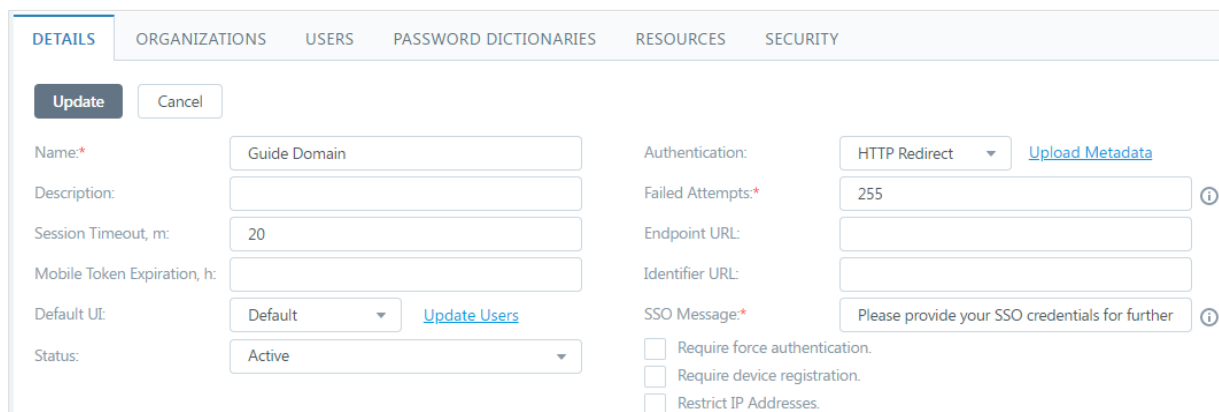
- ☐ Allow password hash storing.
- ☐ Require device registration.
- ☐ Restrict IP Addresses.

Configuration is completed. While creating a user, select the domain with WS Trust type of authentication. In the **SSO User Name** field, enter the username from the AD FS application.

Now, user can sign in the Envi application using AD FS.

HTTP Redirect SSO configuration

1. Change type of domain authentication to **HTTP Redirect**, leave the **Endpoint URL** and **Identifier URL** fields empty, and then **Save** the changes.



DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES RESOURCES SECURITY

Update **Cancel**

Name*: Guide Domain

Description:

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect [Upload Metadata](#)

Failed Attempts*: 255 ⓘ

Endpoint URL:

Identifier URL:

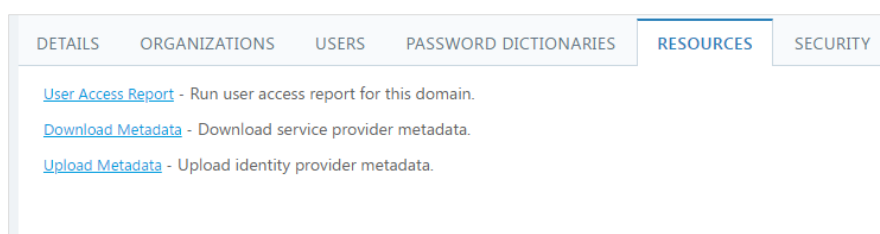
SSO Message*: Please provide your SSO credentials for further ⓘ

☐ Require force authentication.

☐ Require device registration.

☐ Restrict IP Addresses.

2. Navigate to the **Resources** tab, and then click **Upload Metadata**:



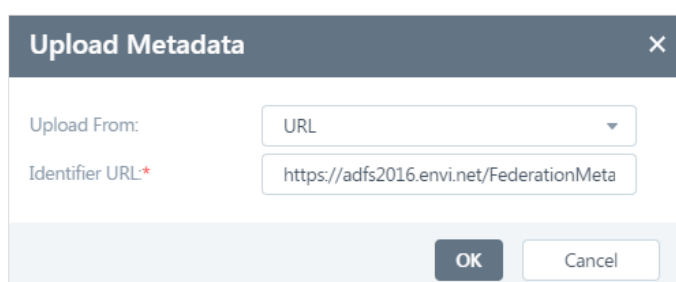
DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES **RESOURCES** SECURITY

[User Access Report](#) - Run user access report for this domain.

[Download Metadata](#) - Download service provider metadata.

[Upload Metadata](#) - Upload identity provider metadata.

3. On the **Upload Metadata** pop-up, select **URL** from the **Upload From** drop-down. Specify URL to the IDP metadata location. It consists of the **IDP Server Base URL** + **Federation Metadata URL** (e.g. <https://adfs2016.envi.net/FederationMetadata/2007-06/FederationMetadata.xml>). Click **OK**.



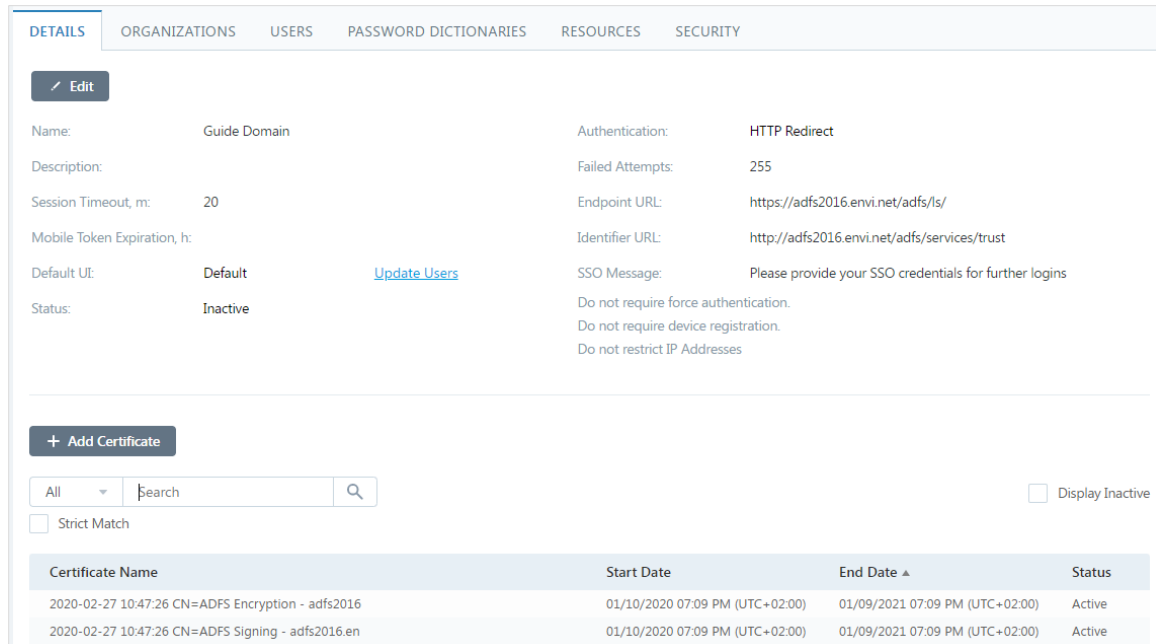
Upload Metadata ✕

Upload From: URL

Identifier URL*: <https://adfs2016.envi.net/FederationMeta>

OK **Cancel**

- Go back to the **Details** tab and make sure that the **Endpoint URL** and **Identifier URL** fields are populated with correct values. Also, the **Certificates** section is populated with at least one certificate.



DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES RESOURCES SECURITY

[Edit](#)

Name: Guide Domain Authentication: HTTP Redirect

Description: Failed Attempts: 255

Session Timeout, m: 20 Endpoint URL: https://adfs2016.envi.net/adfs/ls/

Mobile Token Expiration, h: Identifier URL: http://adfs2016.envi.net/adfs/services/trust

Default UI: Default [Update Users](#) SSO Message: Please provide your SSO credentials for further logins

Status: Inactive Do not require force authentication.
Do not require device registration.
Do not restrict IP Addresses

[+ Add Certificate](#)

All ☐ Display Inactive

☐ Strict Match

Certificate Name	Start Date	End Date ▲	Status
2020-02-27 10:47:26 CN=ADFS Encryption - adfs2016	01/10/2020 07:09 PM (UTC+02:00)	01/09/2021 07:09 PM (UTC+02:00)	Active
2020-02-27 10:47:26 CN=ADFS Signing - adfs2016.en	01/10/2020 07:09 PM (UTC+02:00)	01/09/2021 07:09 PM (UTC+02:00)	Active

Configuration is completed. While creating a user, select the domain with **HTTP Redirect** type of authentication. In the **SSO User Name** field, enter the username from the AD FS application.

Now, user can sign in the Envi application using AD FS.

Envi Testing

To test connection with Envi, perform the following steps:

1. Open Envi application URL.
(for example, <https://sso-demo.envi.net/>)
2. Fill in all the required fields:
 - **Username** – existing AD user in your system
 - **Password** – password for the user in your system
 - **AD FS Endpoint URL**—It could be created by adding [https://your.adfs.ip.address/ + adfs/services/trust/13/usernamemixed](https://your.adfs.ip.address/adfs/services/trust/13/usernamemixed) (you can use domain name instead of IP address)
 - **AD FS Identifier URL**—Identifier that you entered during creation Relying Party Trust for Envi (see [AD FS Configuration](#) section)

USERNAME	<input type="text" value="username"/>
PASSWORD	<input type="password" value="*****"/>
ENDPOINT URL	<input type="text" value="https://www.envi.net/adfs/services/trust/13/usernamemixed"/>
IDENTIFIER URL	<input type="text" value="https://www.envi.net"/>
<input type="button" value="AUTHENTICATE"/>	

3. Click the **Authenticate** button.

In case of successful authentication, you will see the following screen.

Success!	<input type="button" value="AUTHENTICATE"/>
----------	---

In case of error you will see the error description.

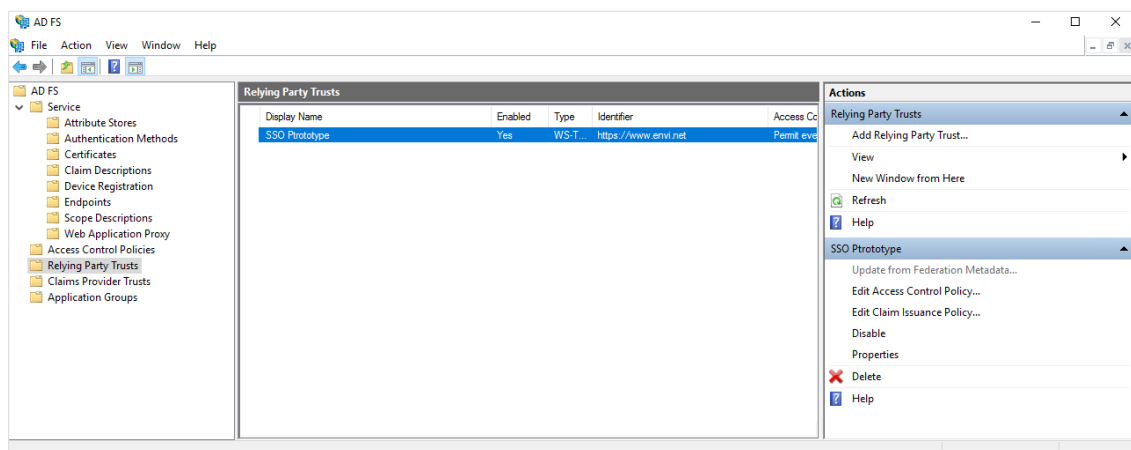
ID3082: The request scope is not valid or is unsupported.	<input type="button" value="AUTHENTICATE"/>
---	---

Appendix 1. Disabling the revocation checks for encryption and signing certificates

Note. This configuration could be used only in test environments or if there is any issue with the checking of CRLs.

For disabling the revocation checks, perform the following steps:

1. Note the Identifier URL of your Relying Party Trust (<https://www.envi.net> on the added screenshot)



2. Start the PowerShell session and type the following command:

```
Get-AdfsRelyingPartyTrust -Identifier 'https://www.envi.net' | Select-Object
SigningCertificateRevocationCheck, EncryptionCertificateRevocationCheck
```

```
PS C:\Users\Administrator> Get-AdfsRelyingPartyTrust -Identifier 'https://www.envi.net' | Select-Object SigningCertificateRevocationCheck, EncryptionCertificateRevocationCheck
SigningCertificateRevocationCheck EncryptionCertificateRevocationCheck
-----
CheckChainExcludeRoot           CheckChainExcludeRoot
```

In the output you will find your Relying Party Trusts and their Revocation Check setting. The default setting is **CheckChainExcludeRoot** for signing and encryption. This setting is recommended for security reasons.

3. In order to disable Revocation Check, use the following command:

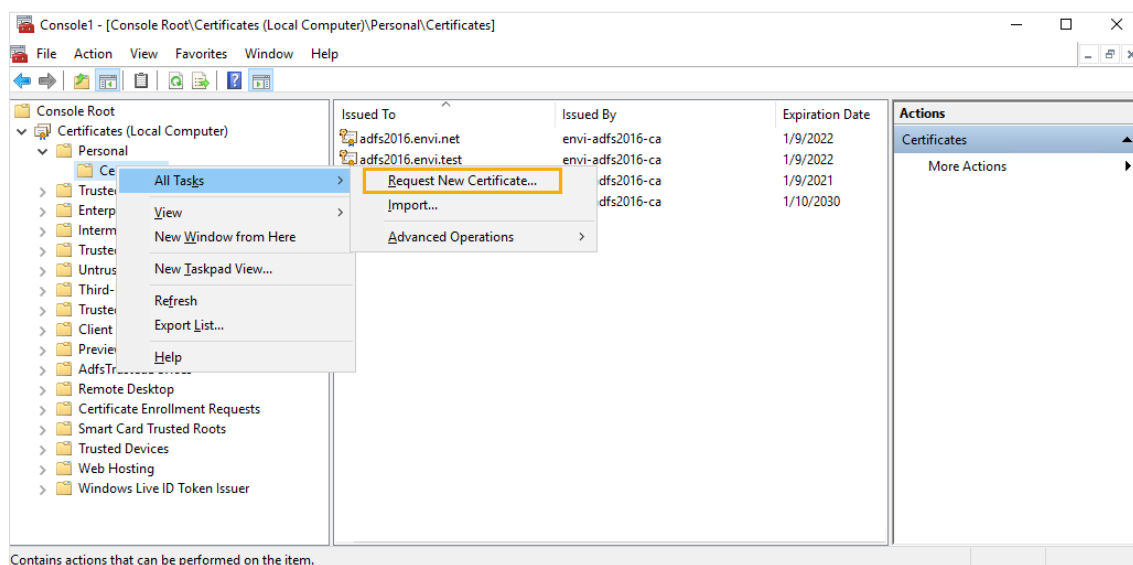
```
Get-AdfsRelyingPartyTrust -Identifier 'https://www.envi.net' | Set-
AdfsRelyingPartyTrust -SigningCertificateRevocationCheck None -
EncryptionCertificateRevocationCheck None
```

Appendix 2. SSL Certificates issuing

To create certificate for ADFS Service Communications follow the following steps:

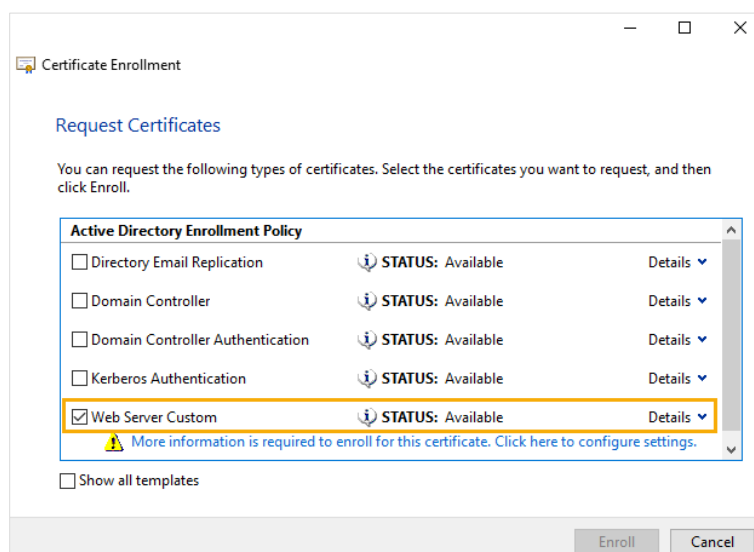
Note: You can also create SSL certificates for Token-decrypting and Token-Signing or use certificates that were automatically generated during ADFS configuration.

1. Launch **mmc** console, add the **Certificates** snap-in, and then select **Computer Account** > **Local computer**.
2. Navigate to **Personal** > **Certificates**, right-click **Certificates**, and then select **All Tasks** > **Request New Certificate**.

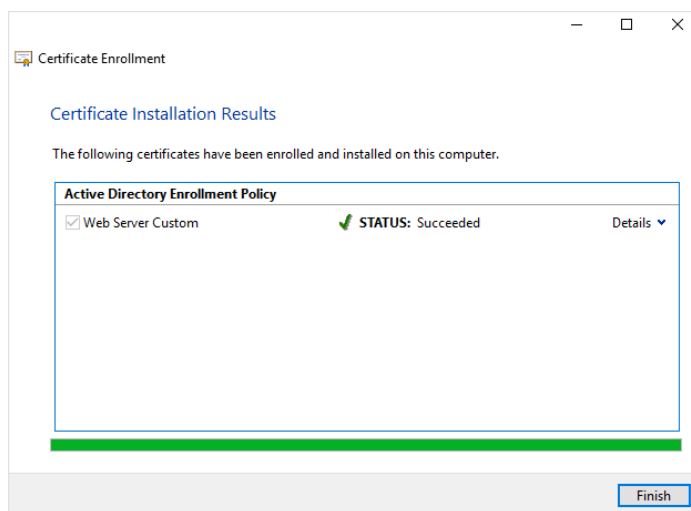


3. On the **Certificate Enrollment** window, select the **Web Server** template.

Note: You can use your custom template for issuing the certificates with the **Server Authentication** extended key usage.



4. Click **More information is required to enroll for this certificate. Click here to configure settings**, fill in all required fields, and then select **Enroll**:
 - Common name
 - Subject alternative name
 - Friendly name
 - Description
5. Check the status of enrollment on the **Certificate Installation Results** window and find your certificate in the **Certificates** console.



The certificate has been enrolled and installed on your computer successfully.