AD FS Configuration for SSO

February, 2020

Table of Contents

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

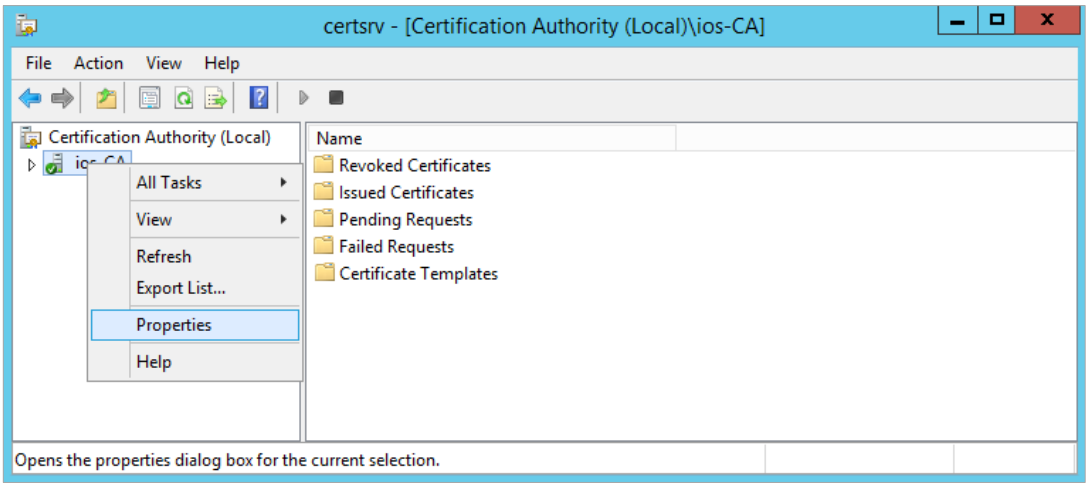
1. **SSL certificates.** Configuration of each AD FS server requires the next SSL certificates:

   - 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

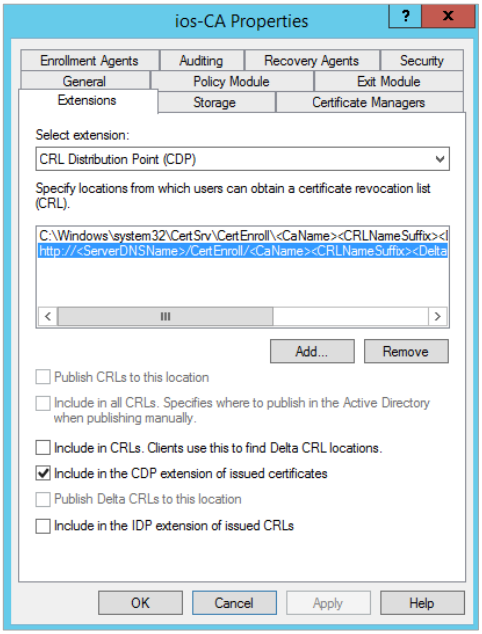
   These SSL certificates must contain the **Server Authentication Enhanced Key Usage** value and it is recommended to use publicly trusted certificates for both production and testing deployments.

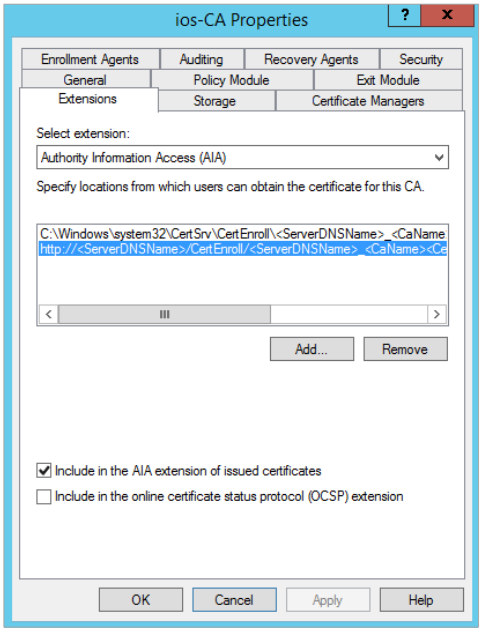
   However, if you want to use self-signed SSL certificates in your configuration, you should be aware of the following aspects:

   - 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)

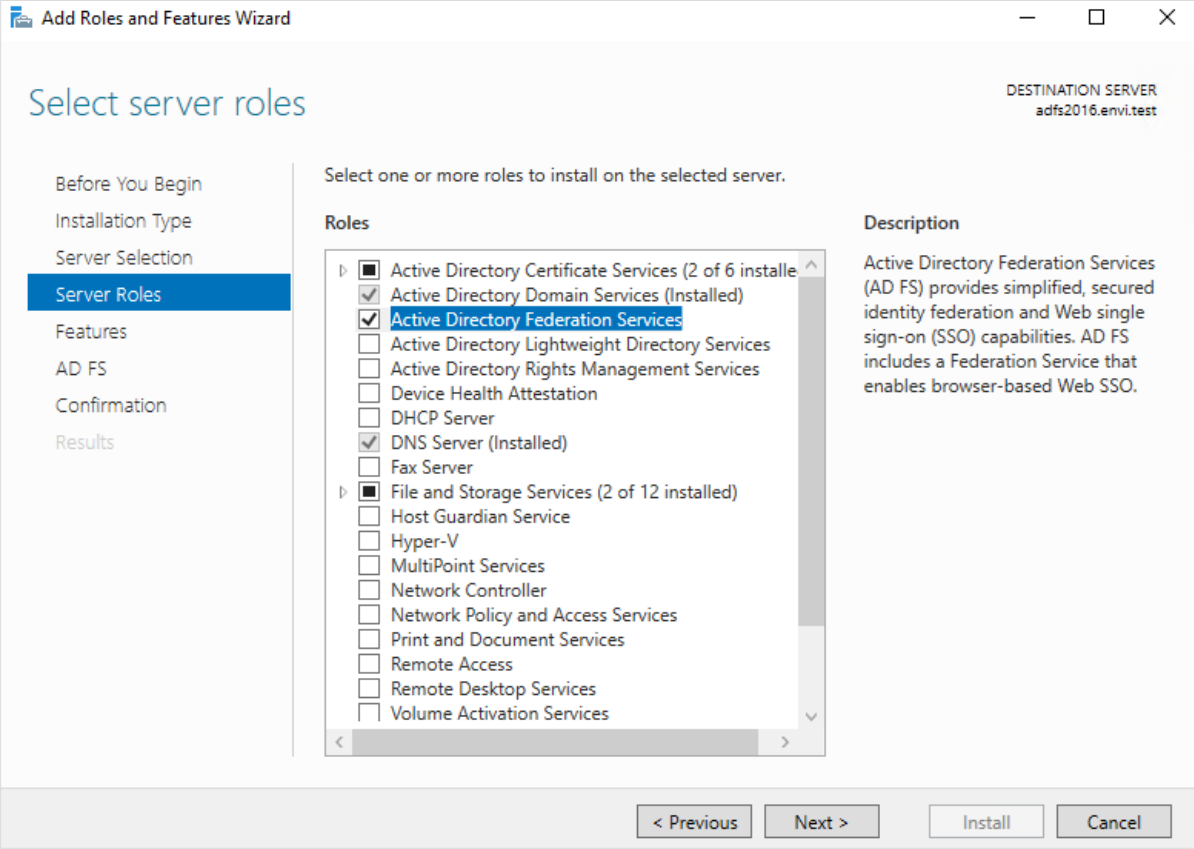
Prepare required SSL certificates (self-signed or publicly trusted) according to the above requirements (please follow the instructions in Appendix 2 for creating self-signed SSL certificates using preconfigured CA).

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.

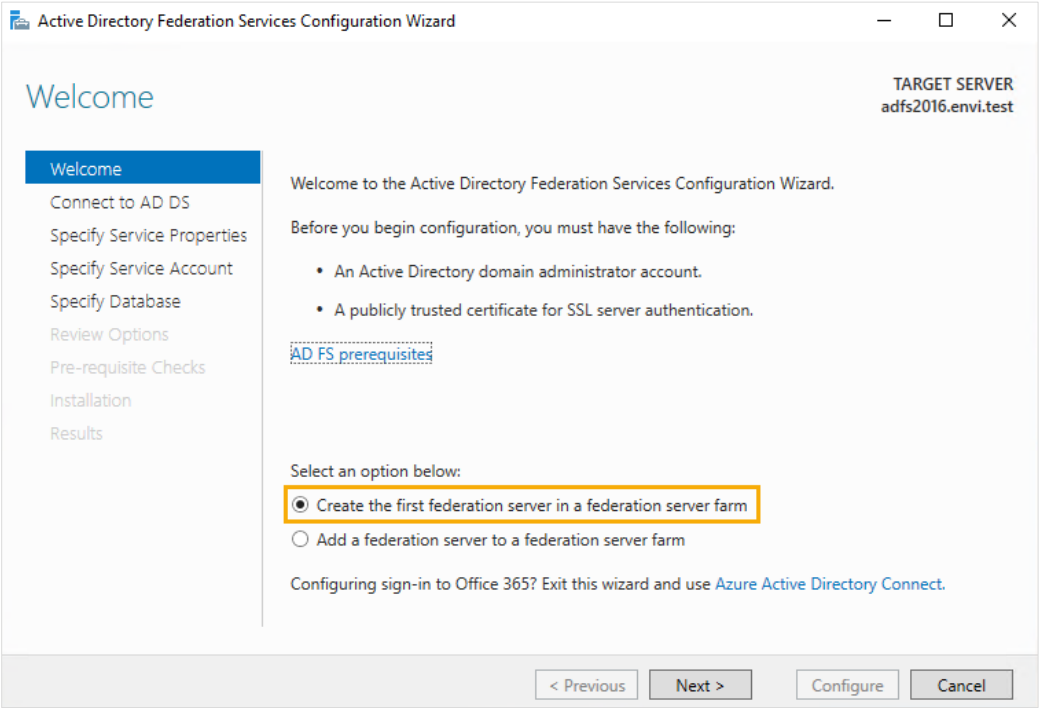
AD FS Installation

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



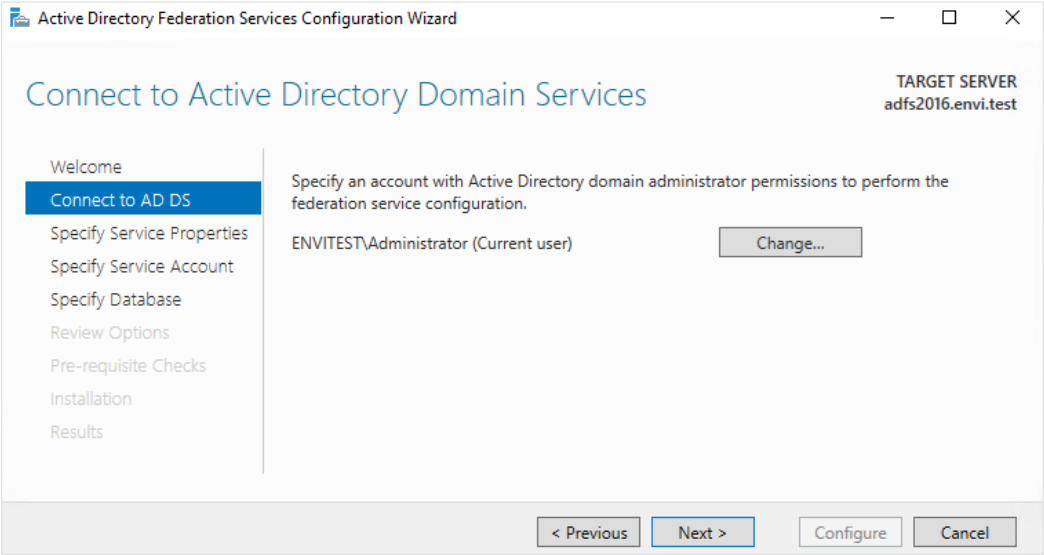
After successful AD FS 4.0 installation, configure the AD FS server and create **Relying Party Trust**:

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

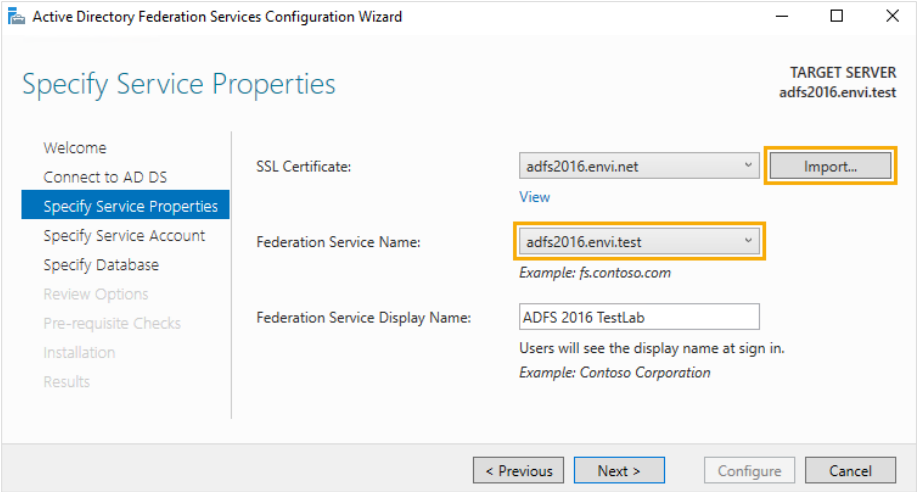


2. On the **Connection to AD FS** section, specify the AD account that has permissions to perform the federation service configuration.

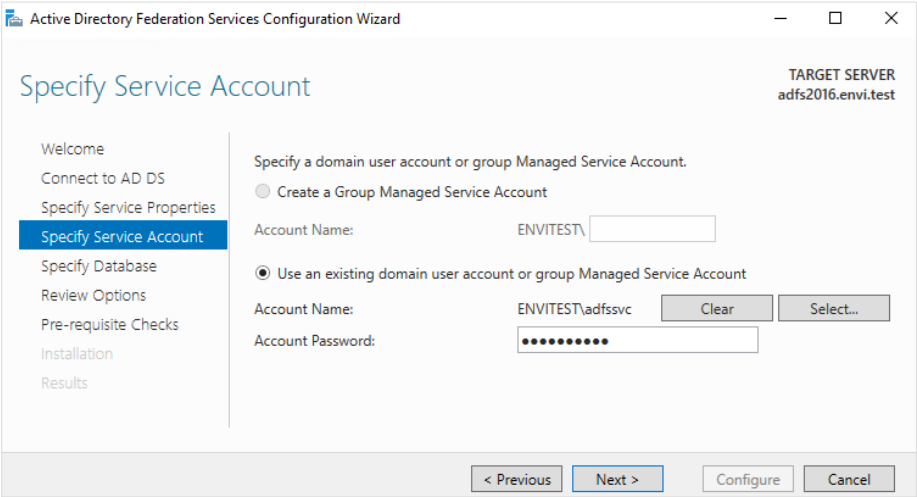
   Note: Requirements for this account are described in the Preparation section.



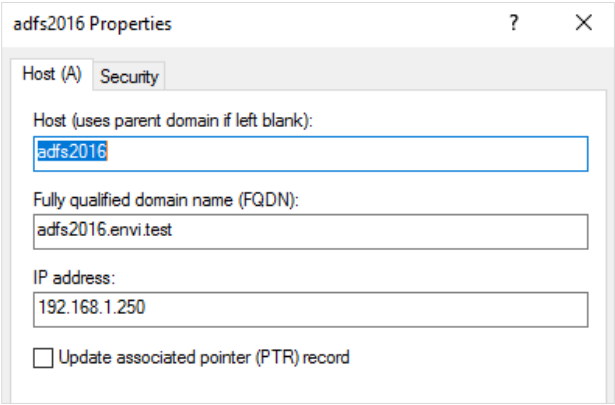
3. On the **Specify Service Properties** section, specify the properties you want. Import the SSL certificate for the service URL. Then, edit the default **Federation Service Name**, it will be your federation service address and serve as the root of your sign in URL.



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



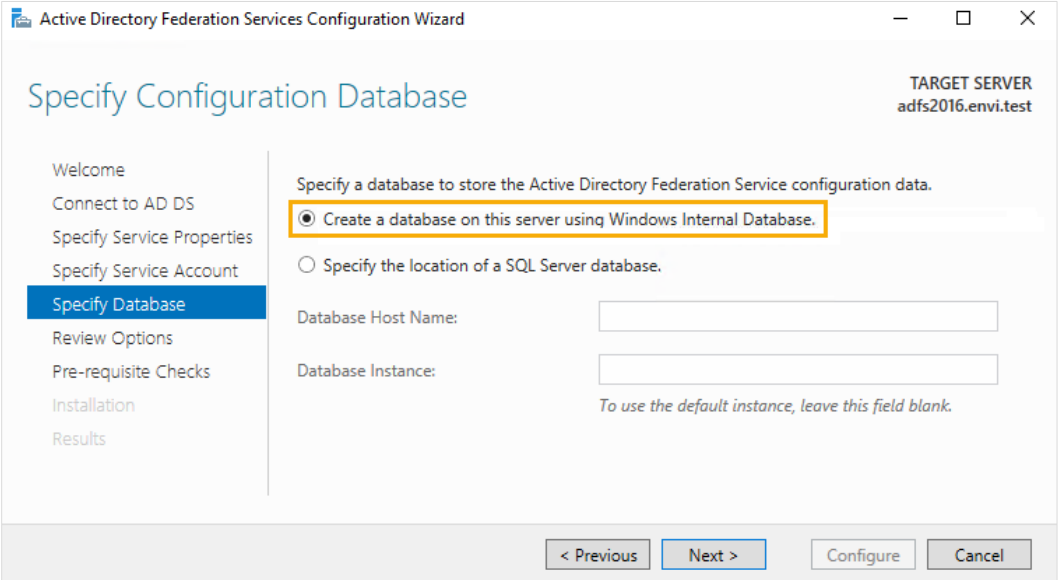
Note: Ensure that your DNS settings contain **A** record created to support the **Federation Service** name.



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**.

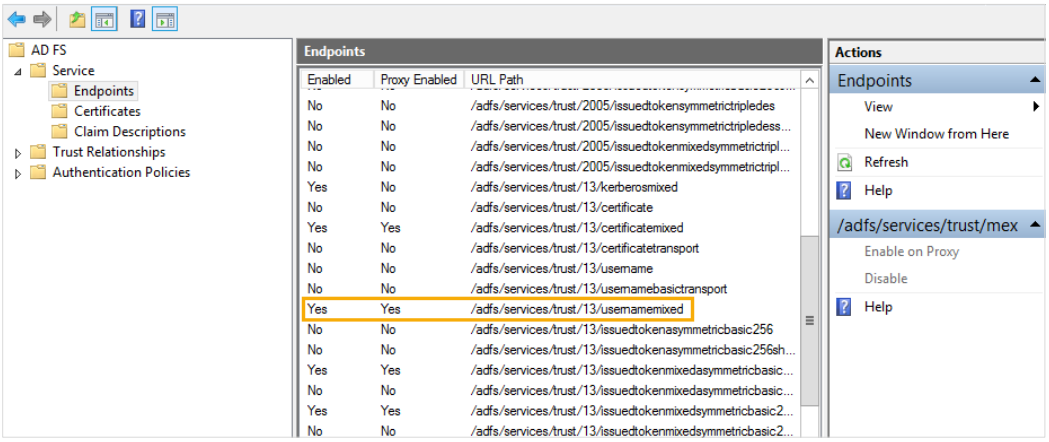


6. Proceed with **Pre-requisite Checks section**, and then complete the configuration.

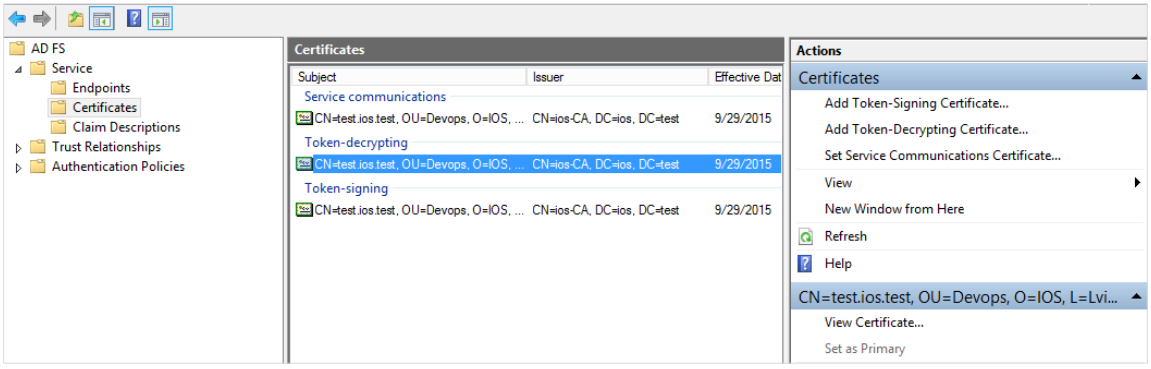
After installation, main AD FS tool is located on the following location: **Server Manager** > **Tools** > **AD FS Management**.

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.



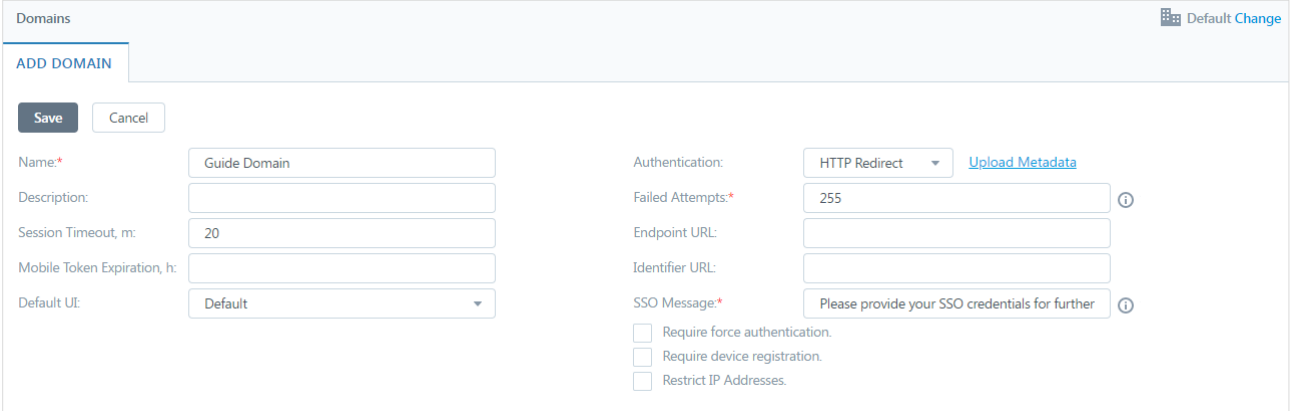
To change any of these certificates you can use your own publicly trusted certificates or generate the new ones.

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**.

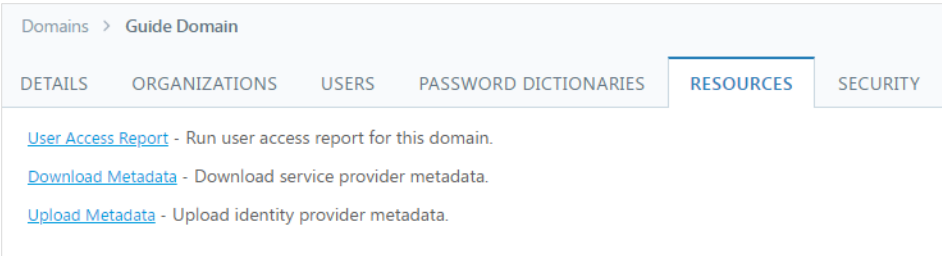
AD FS Configuration

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.

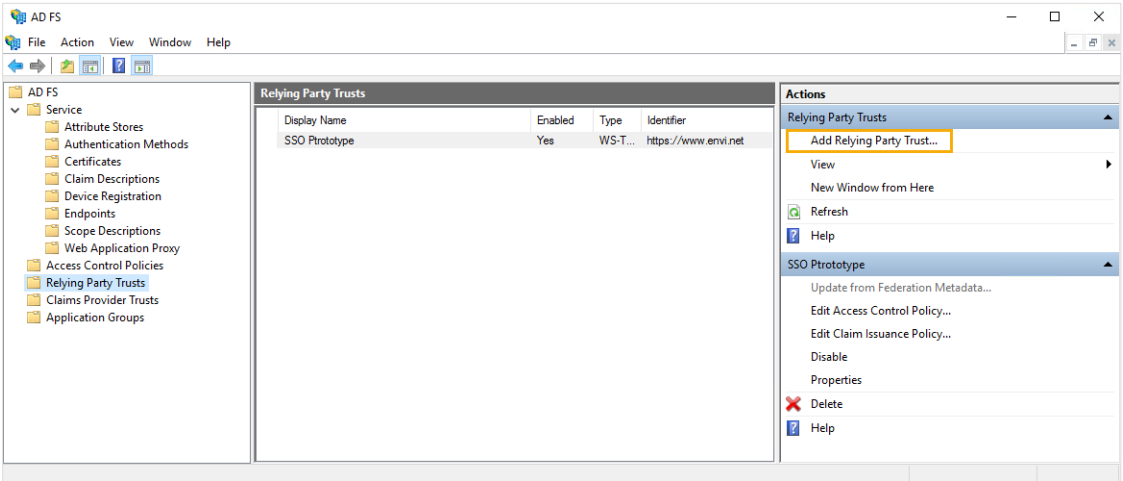


2. Navigate to the **Resources** tab, and then select **Download Metadata**. Save metadata file to the appropriate location, and then copy it to the server instance with ADFS.

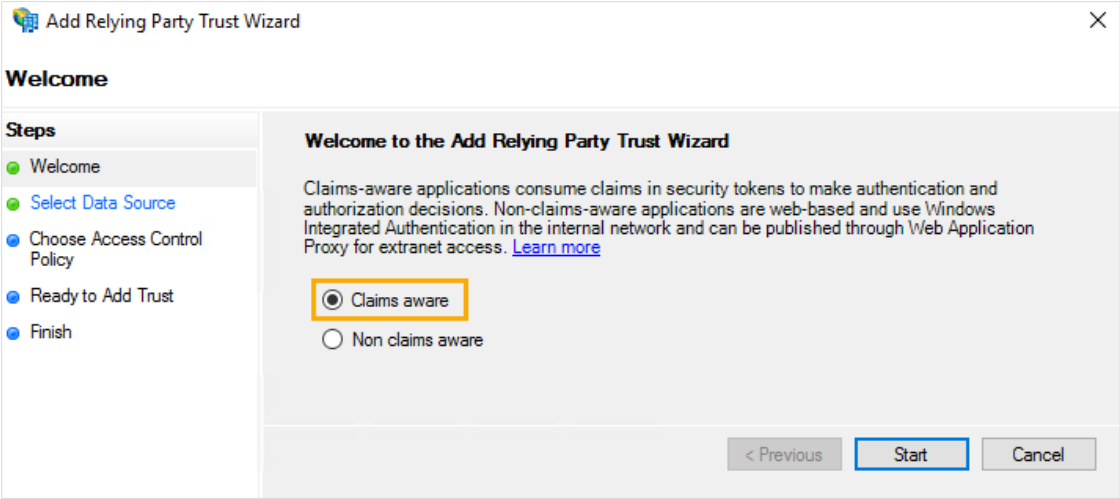


3. Open **AD FS Management**.

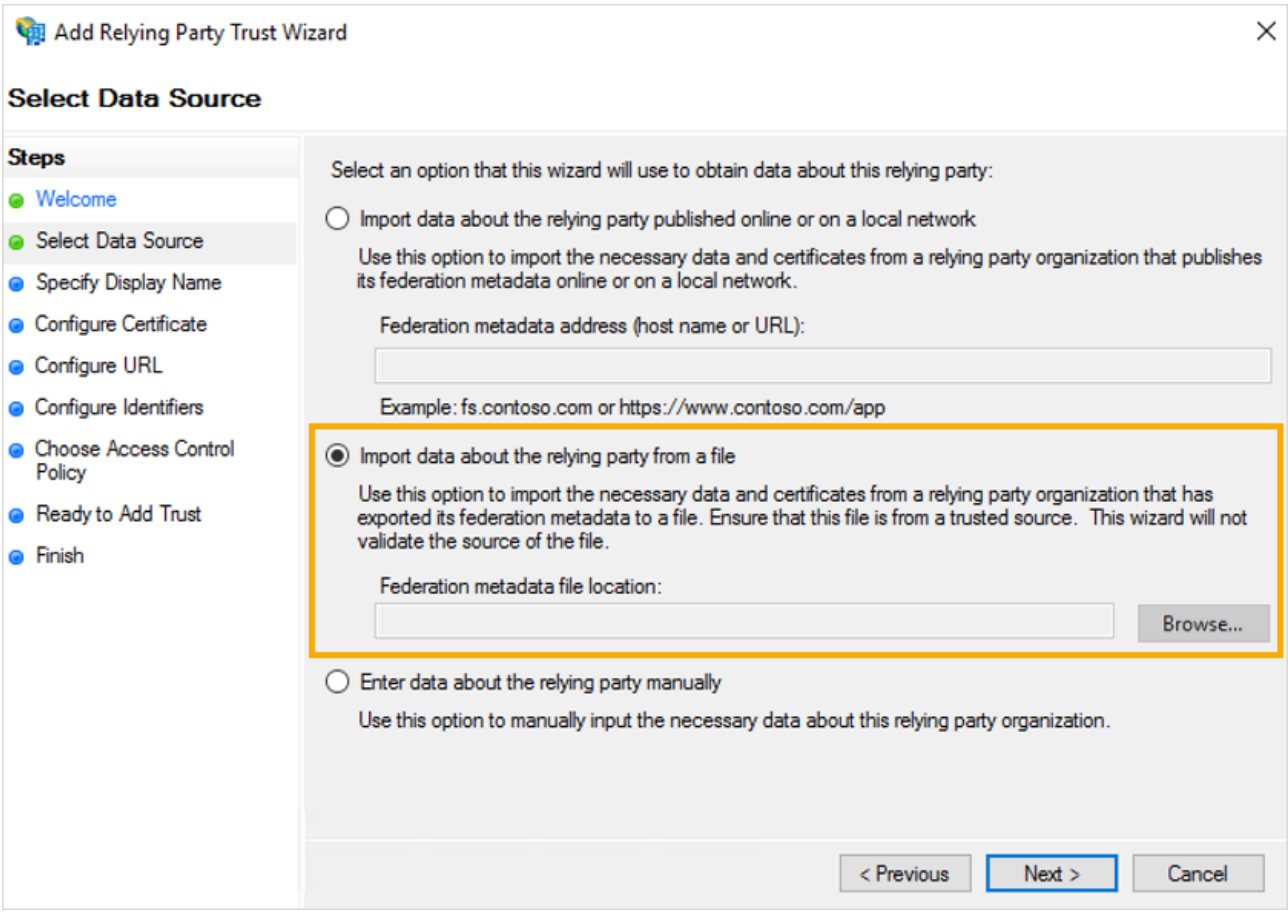
4. On the **Actions** section, select **Add Relying Party Trust**.



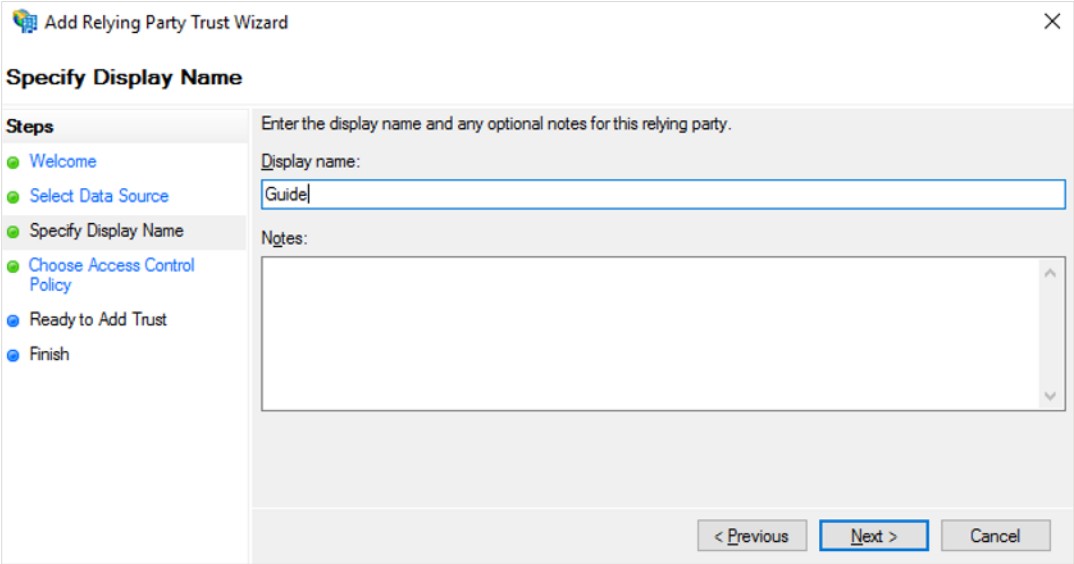
5. Follow the wizard's steps. Select **Claims aware**, and then click **Start**.



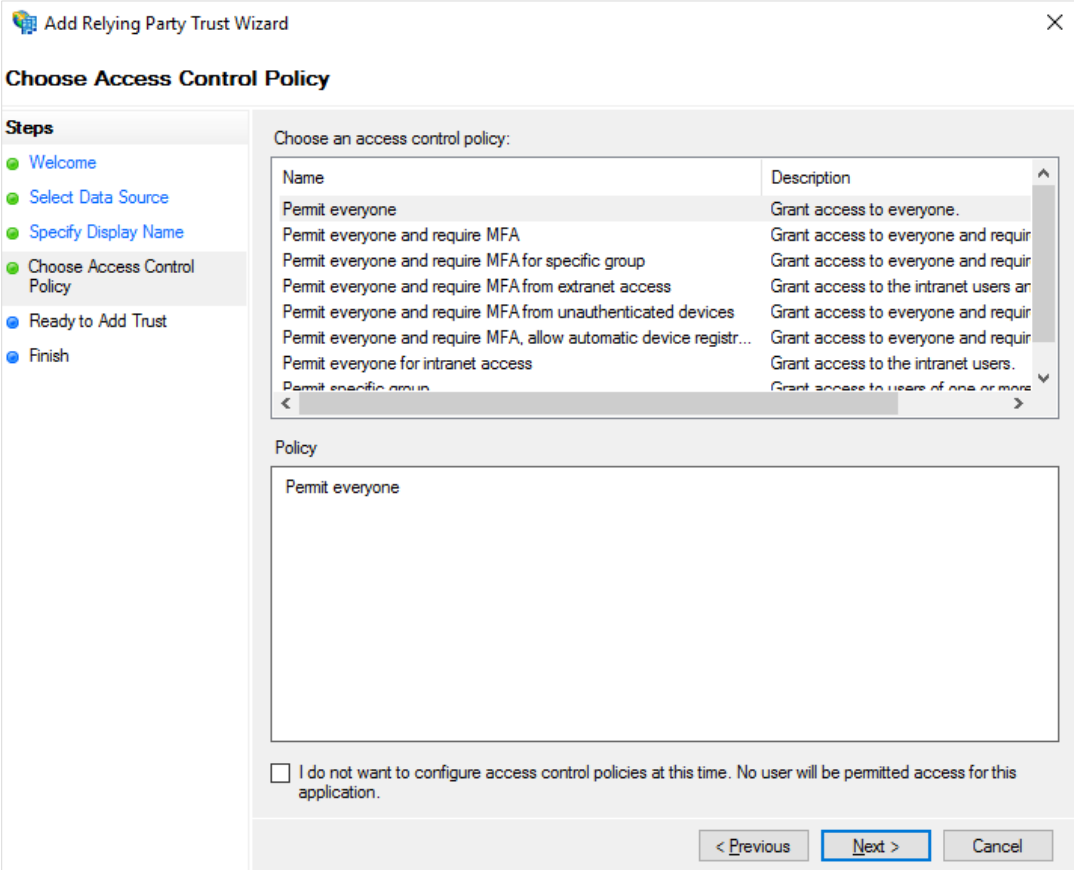
6. Select **Import data about the relying party from a file**, click the **Browse** button, and then select location of the metadata file from Envi. Click **Next**.



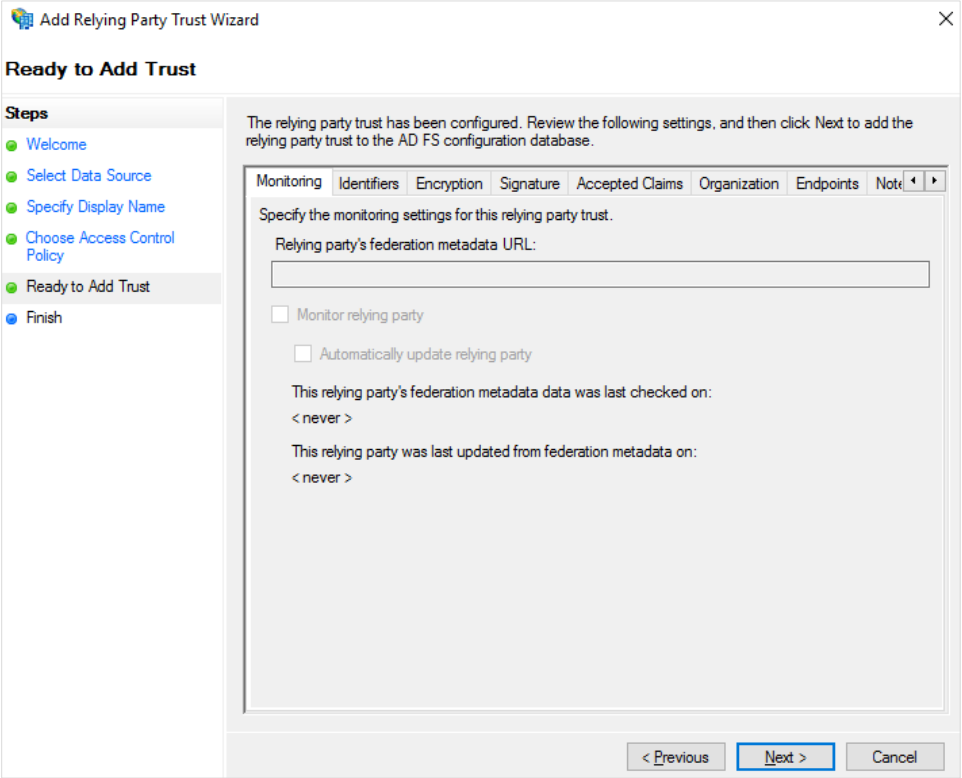
7. Enter Display name. Click **Next**.



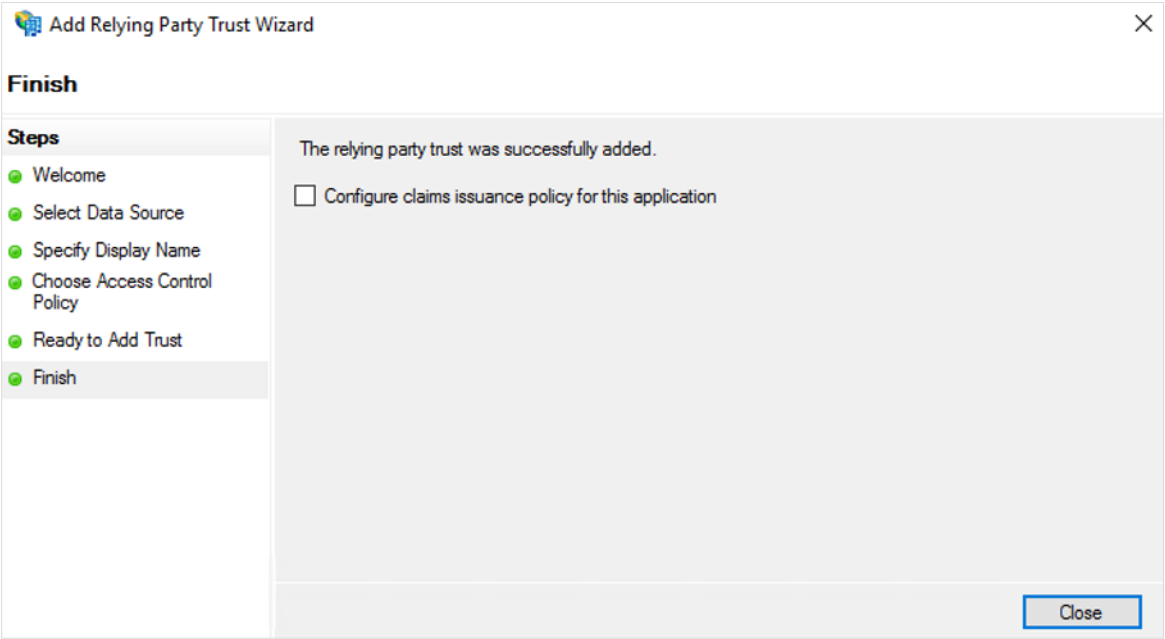
8. Select **Permit everyone**. Click **Next**.



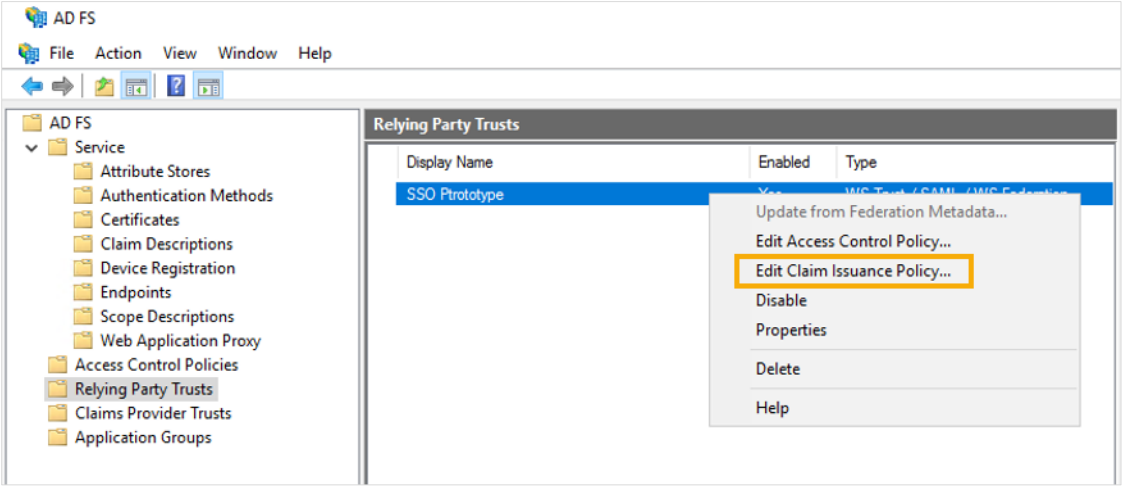
9. Click **Next**.



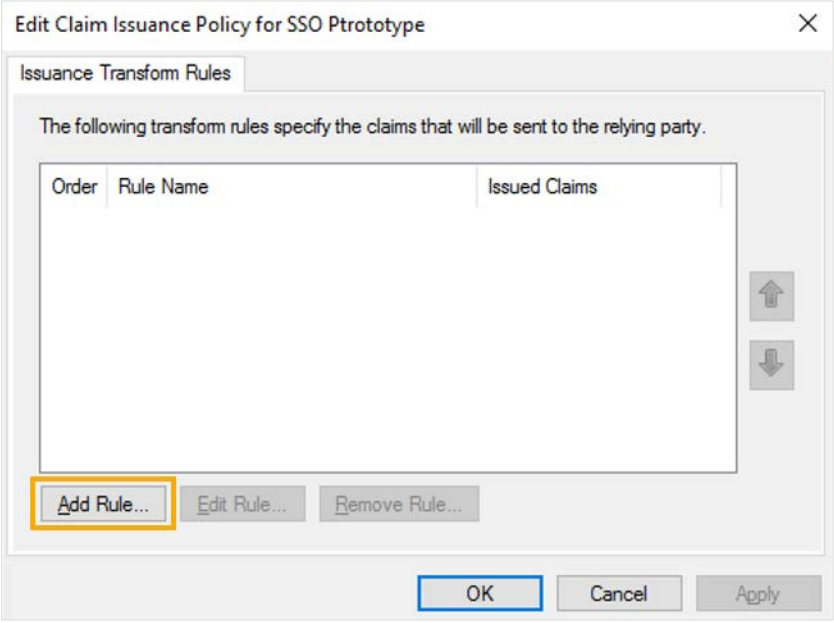
10. Clear the check box (it's not necessary, but with selected check box you can continue with additional configuration). Click **Close**.



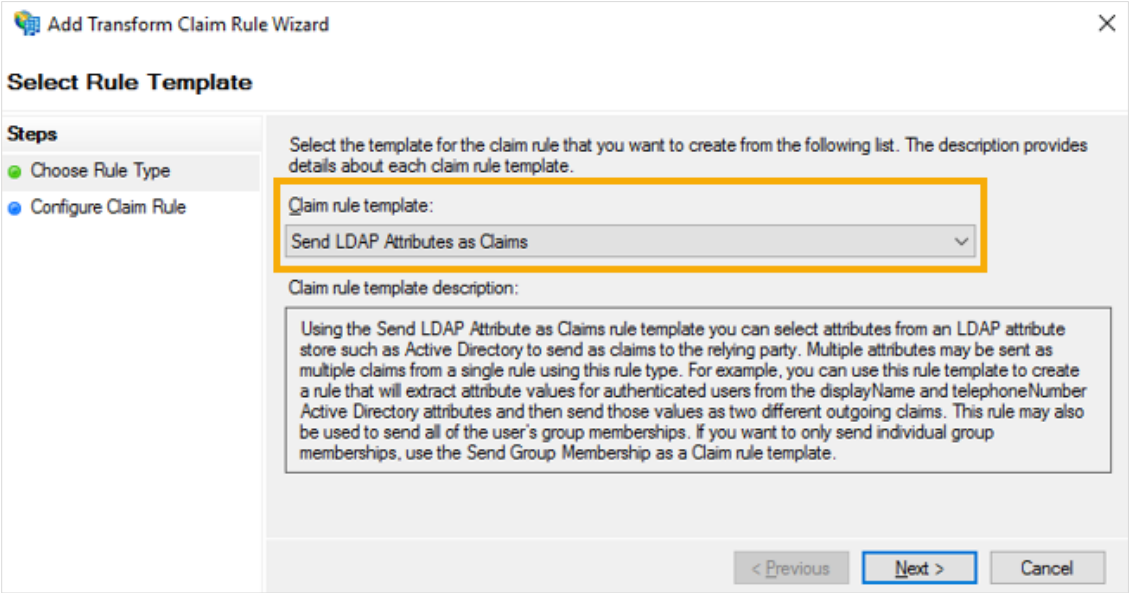
11. Select created Relying Party Trust record and right click it. From the context menu, select **Edit Claim Issuance Policy**.



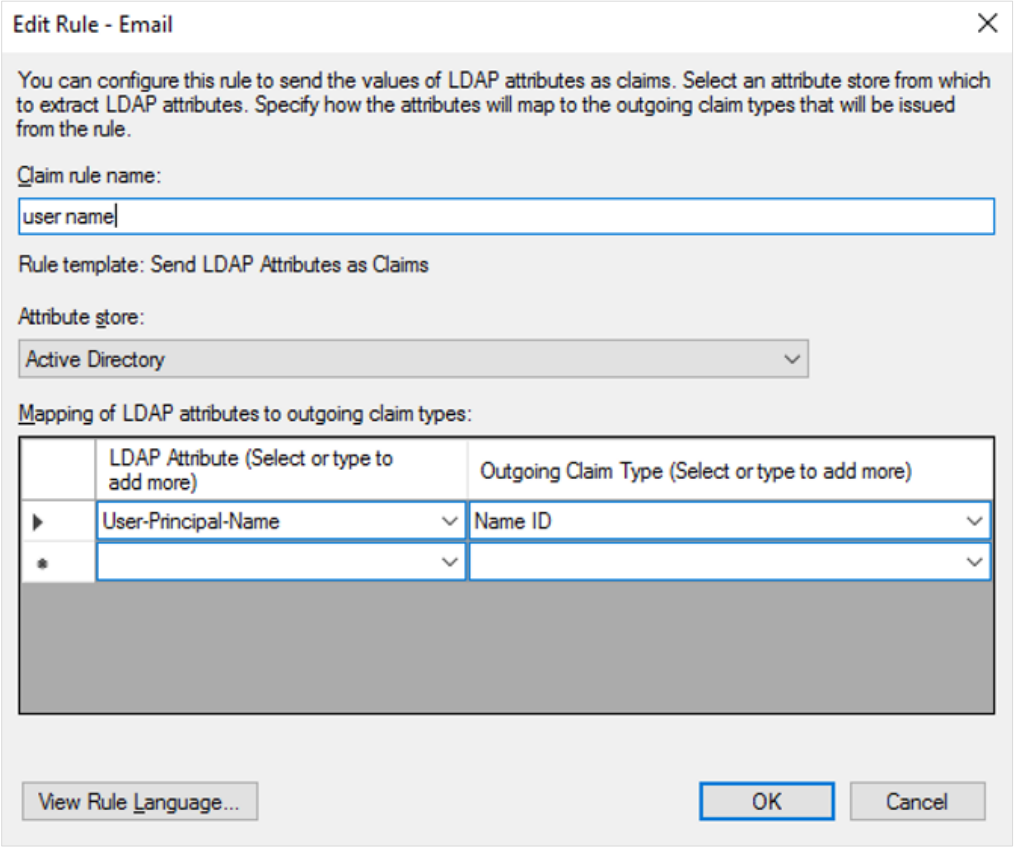
12. Click the **Add Rule** button.



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

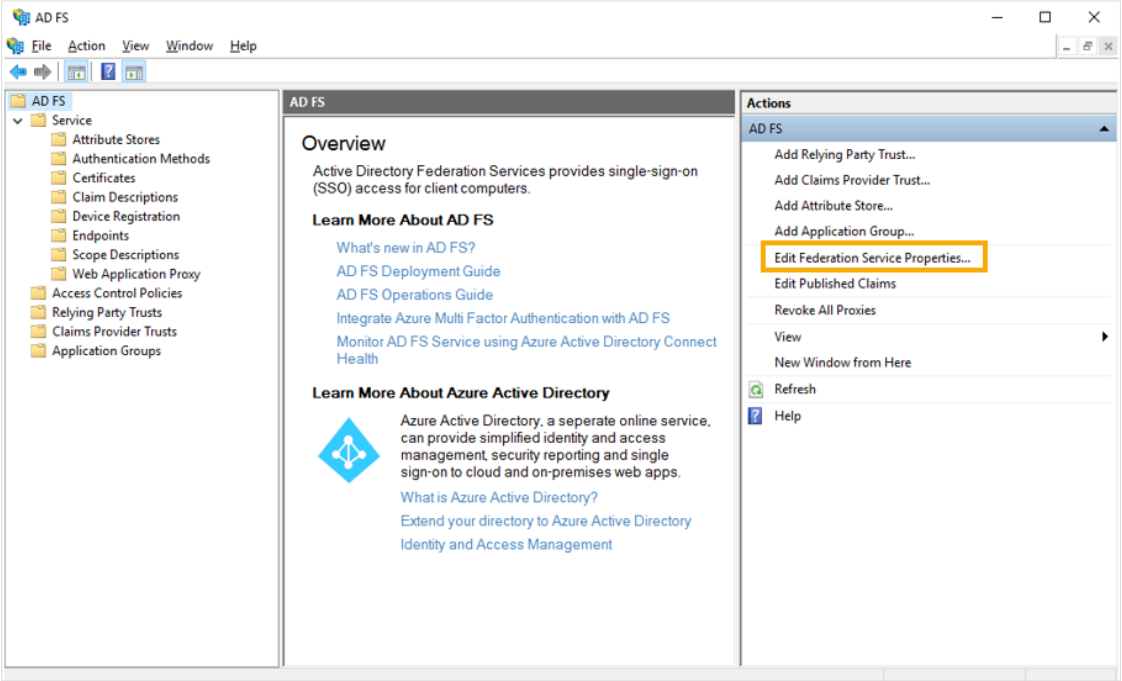


14. Specify rule name and select **Active Directory** as attribute store value. Click the first **LDAP Attribute** column on the **Mapping of LDAP attributes to outgoing claim types** section, and then select the **User-Principal-Name** value. Click the second **Outgoing Claim Type** column, and then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

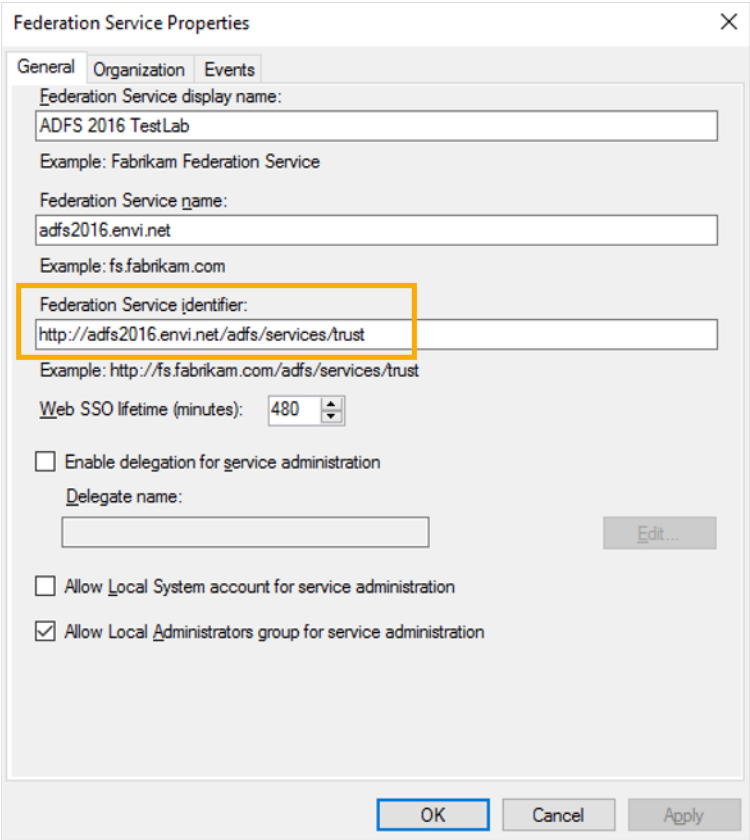


15. Click **OK** button, and then close window.

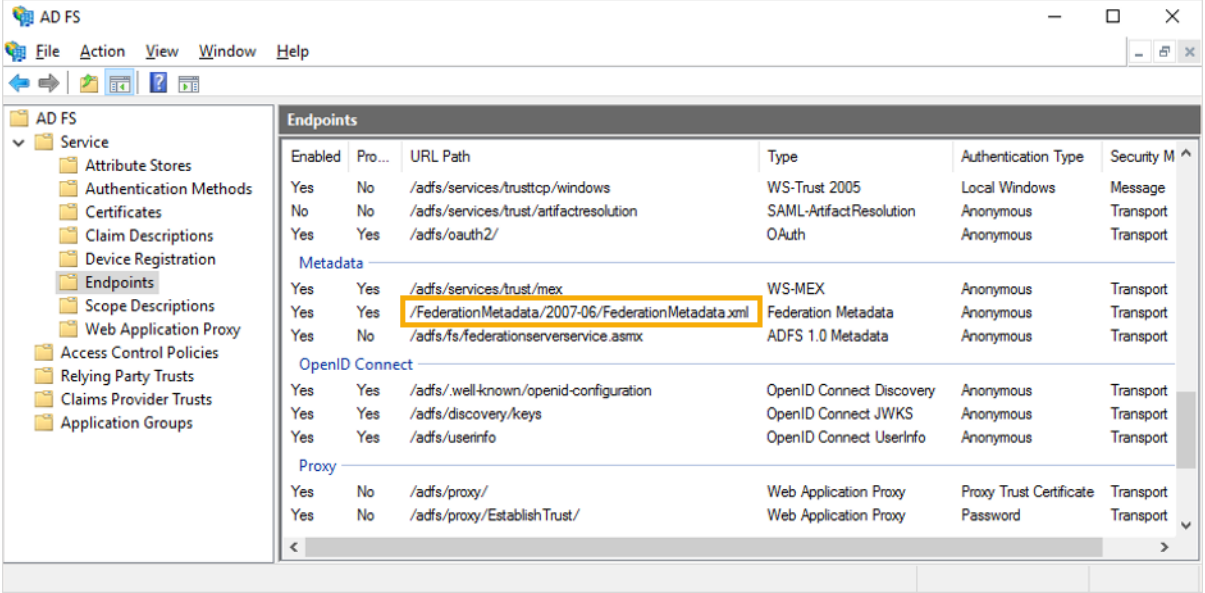
16. Select the main **AD FS** node, and then click **Edit Federation Service Properties**.



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.



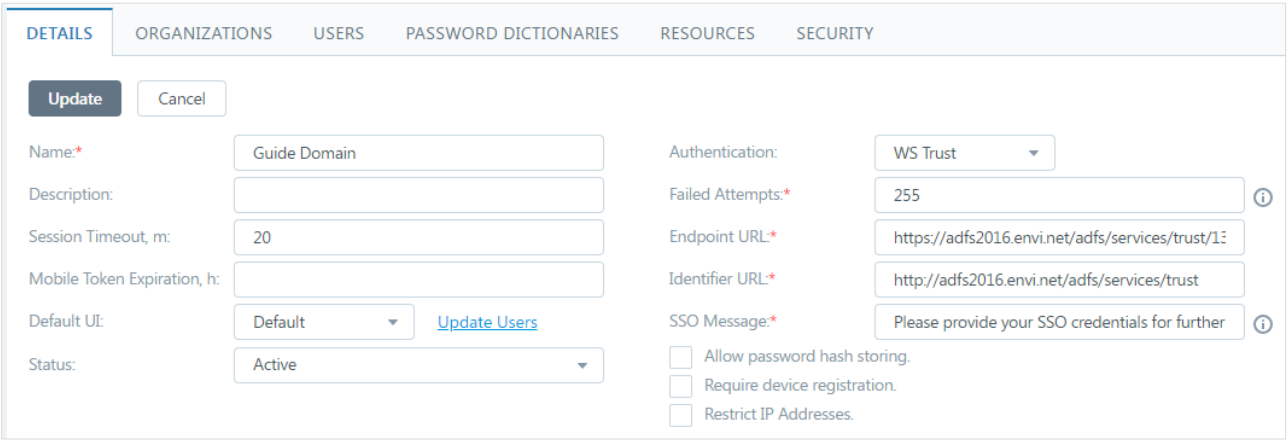
Configuration of AD FS is successfully completed. You can begin to configure your domain settings in Envi.

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

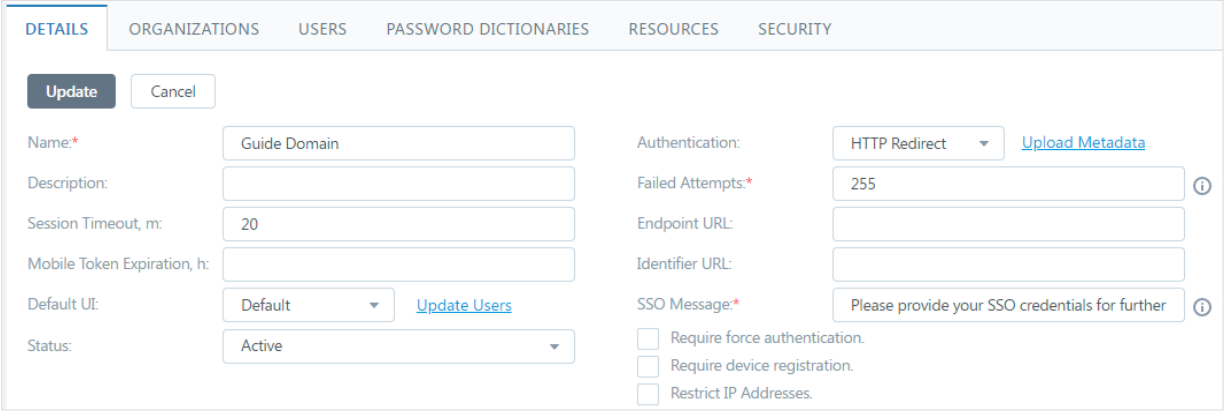


Configuration is completed. While creating a user, select the domain with WS Trust type of authentication. In the **SSO User Name** field, enter the username from the AD FS application.

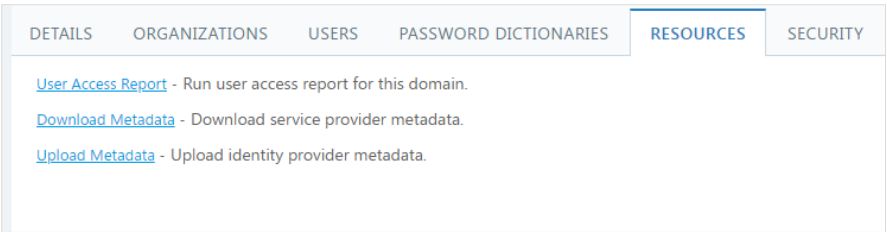
Now, user can sign in the Envi application using AD FS.

HTTP Redirect SSO configuration

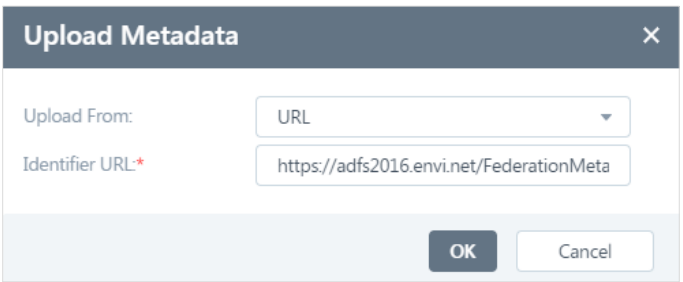
1. Change type of domain authentication to **HTTP Redirect**, leave the **Endpoint URL** and **Identifier URL** fields empty, and then **Save** the changes.



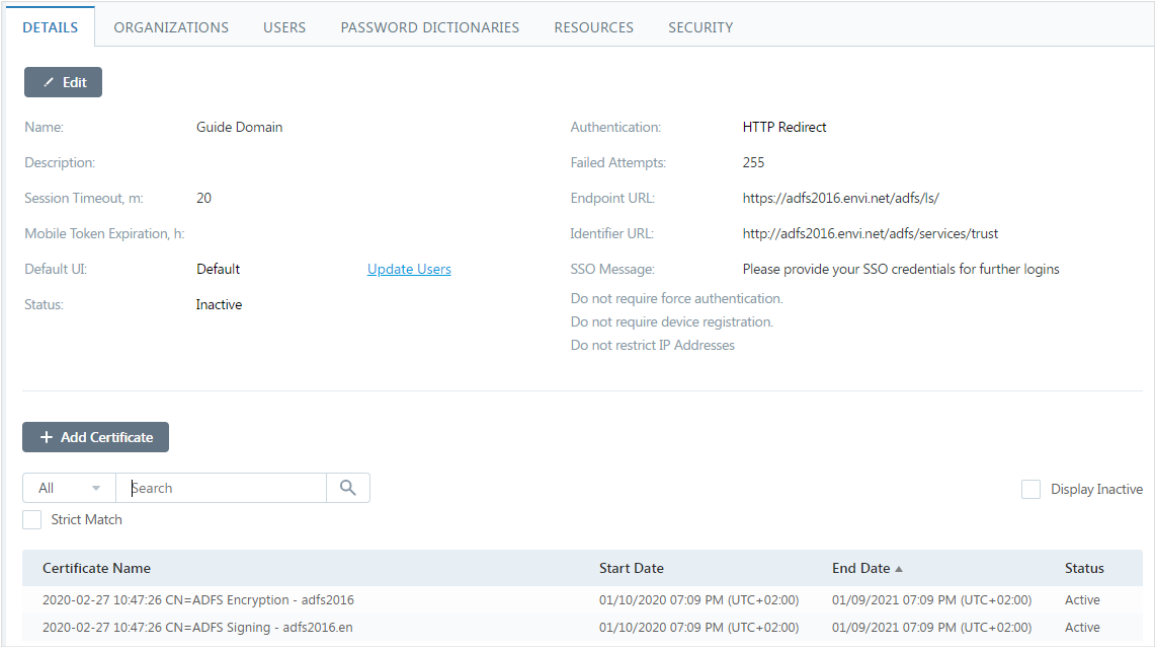
2. Navigate to the **Resources** tab, and then click **Upload Metadata**:



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**.



4. 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.



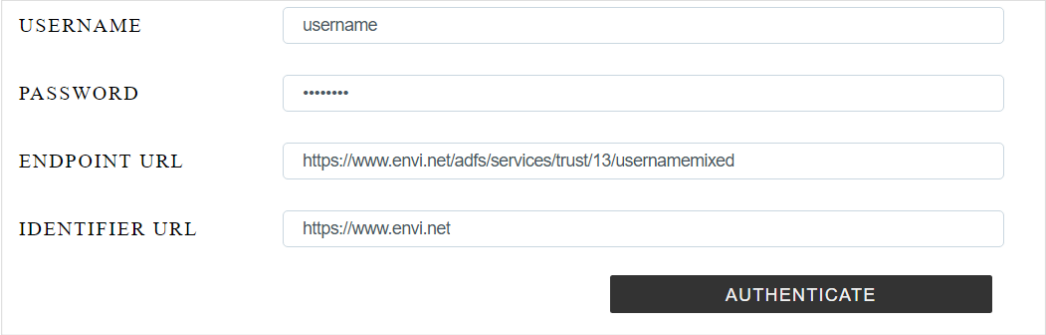
Configuration is completed. While creating a user, select the domain with **HTTP Redirect** type of authentication. In the **SSO User Name** field, enter the username from the AD FS application.

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 (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)



3. Click the **Authenticate** button.

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

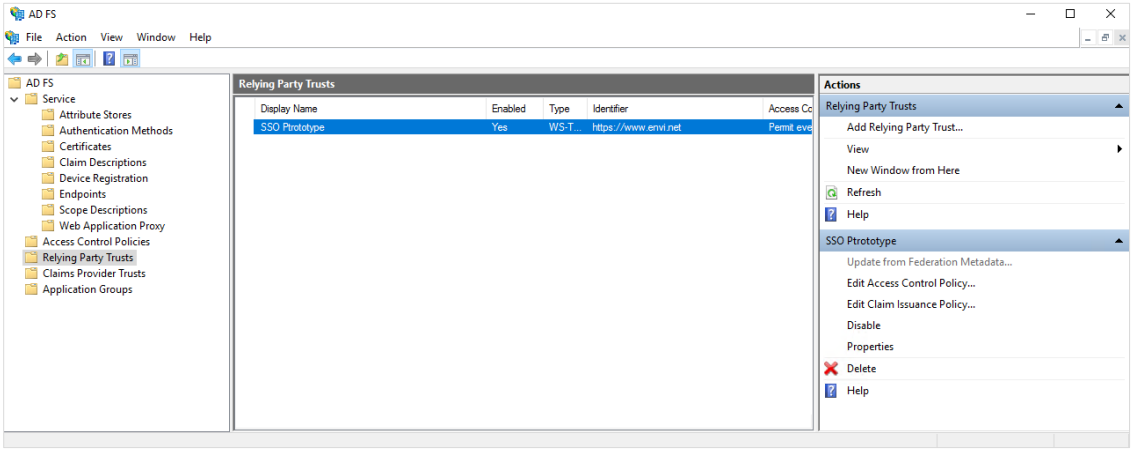
In case of error you will see the error description.

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:

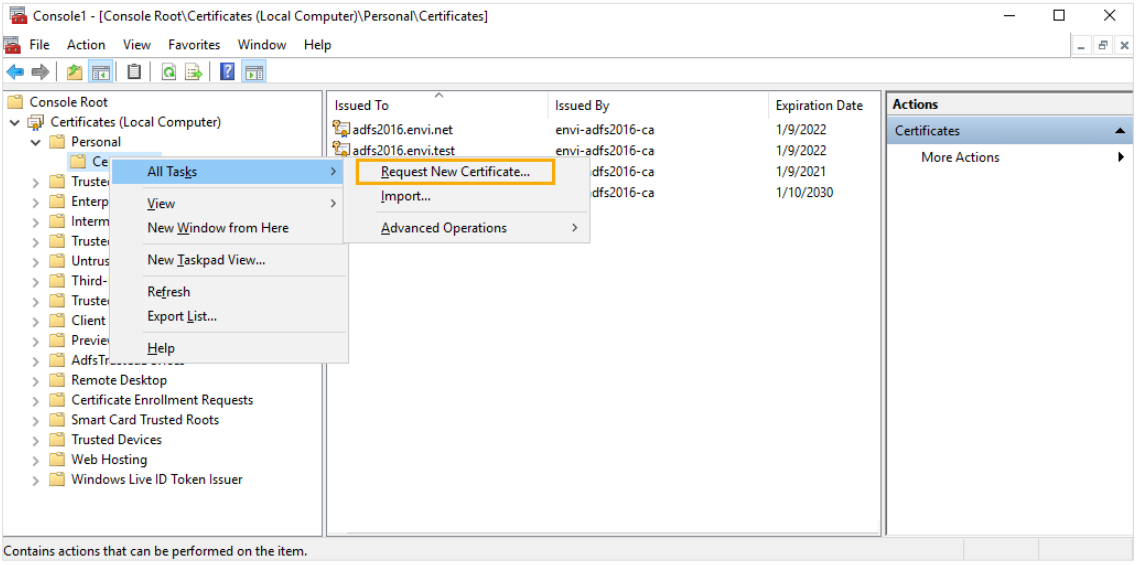
```
Get-AdfsRelyingPartyTrust -Identifier 'https://www.envi.net' | Set-
AdfsRelyingPartyTrust -SigningCertificateRevocationCheck None -
EncryptionCertificateRevocationCheck None
```

Appendix 2. SSL Certificates issuing

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

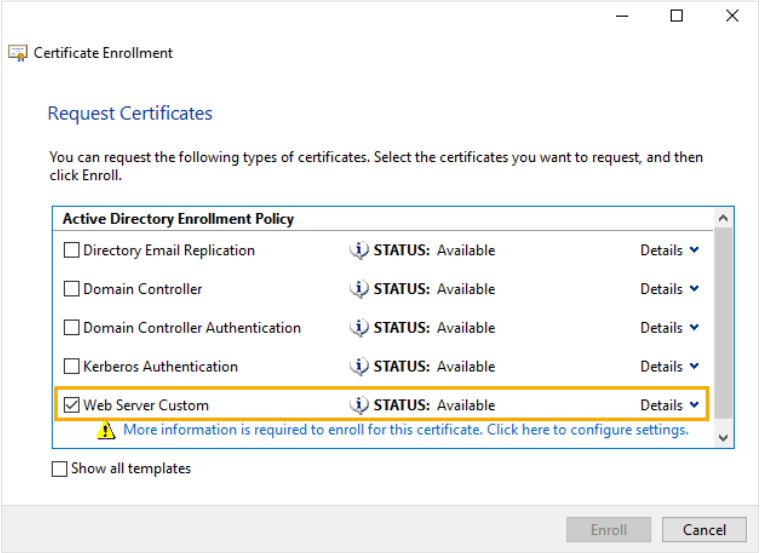
Note: You can also create SSL certificates for Token-decrypting and Token-Signing or use certificates that were automatically generated during ADFS configuration.

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.

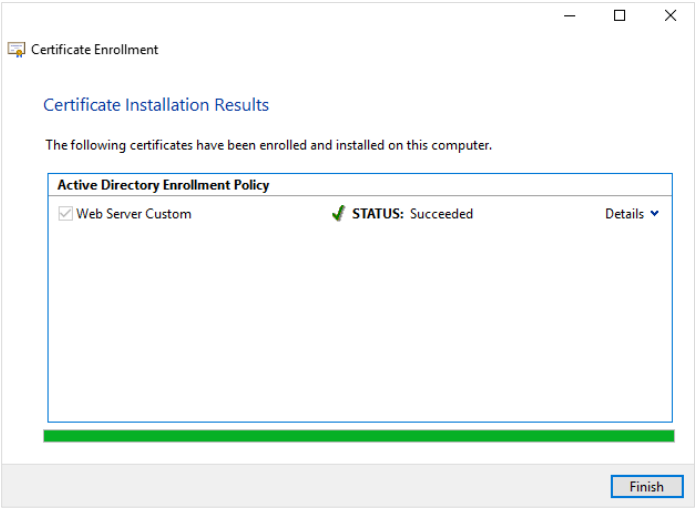


3. On the Certificate Enrollment window, select the Web Server template.

   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.