



AD FS

Configuration for SSO

May, 2019



Table of Contents

Introduction.....	3
Assumptions.....	3
Preparation.....	4
AD FS Installation.....	9
Certificates Management	12
AD FS Configuration.....	12
Envi Testing.....	19

Introduction

The purpose of this document is to describe 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
IIS	Internet Information Services
WIF	Windows Identity Foundation

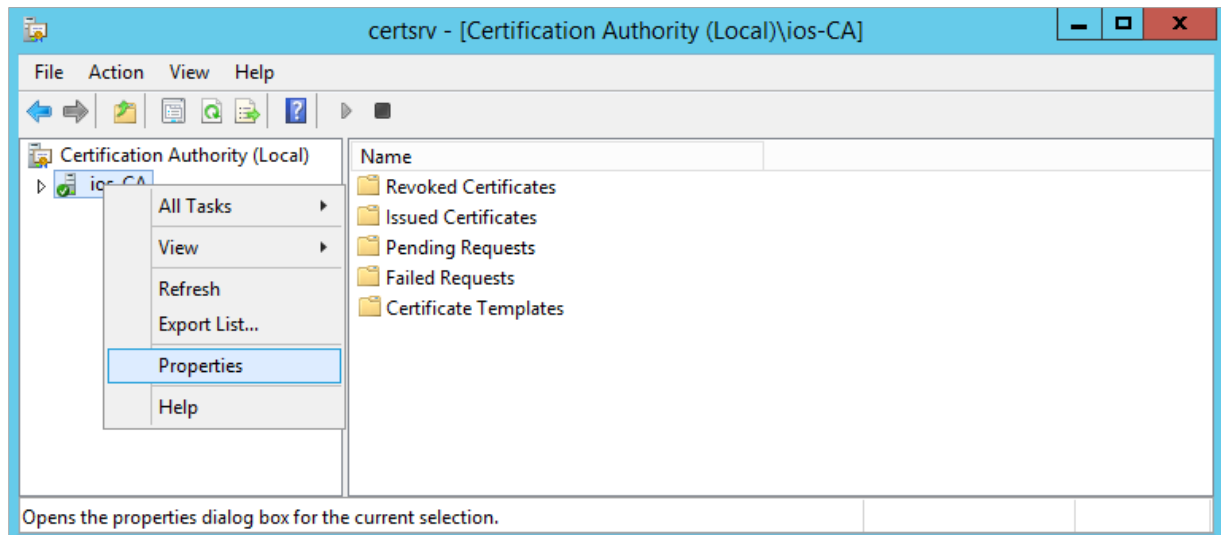
Assumptions

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

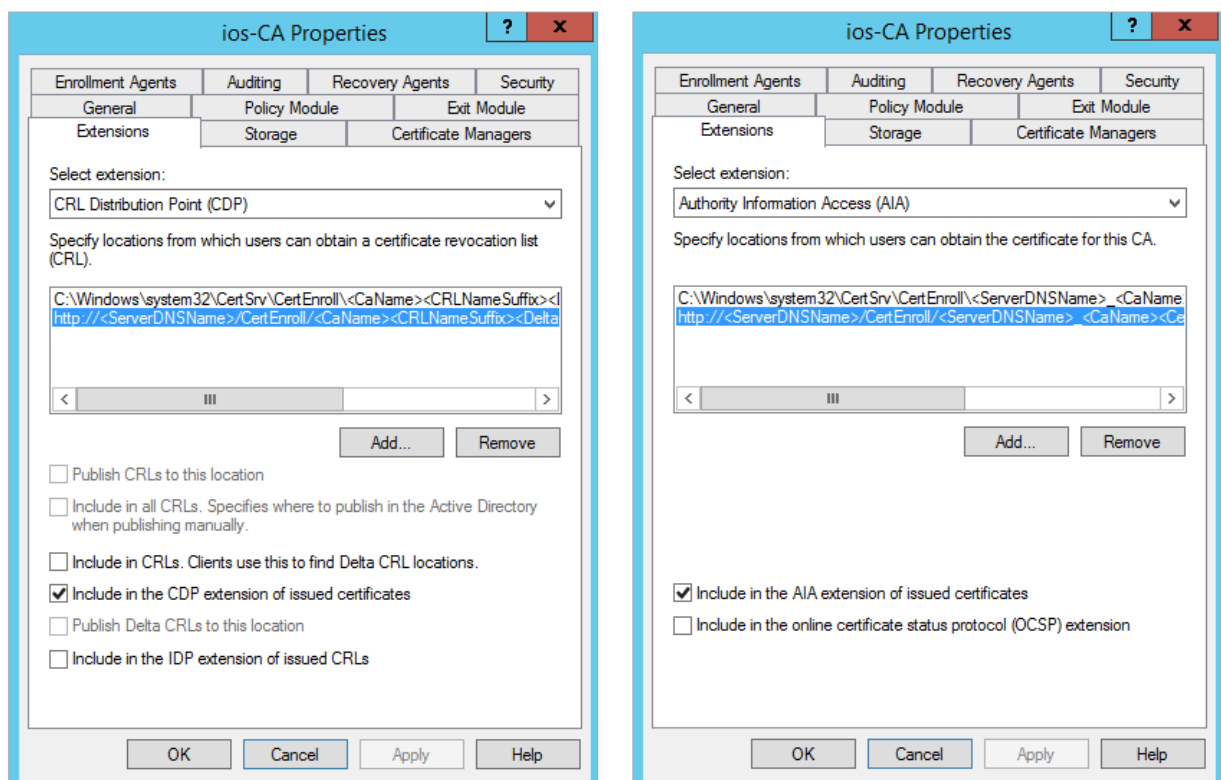
- The prototype is going to work with AD FS 3.0
- Base OS is Windows 2012 R2
- AD is preinstalled in the system
- AD CS is preinstalled in the system
- Envi is going to be delivered as zip archive package

Preparation

1. Certification Authority. Edit Certification Authority properties under Server Manager > Tools > Certification Authority.

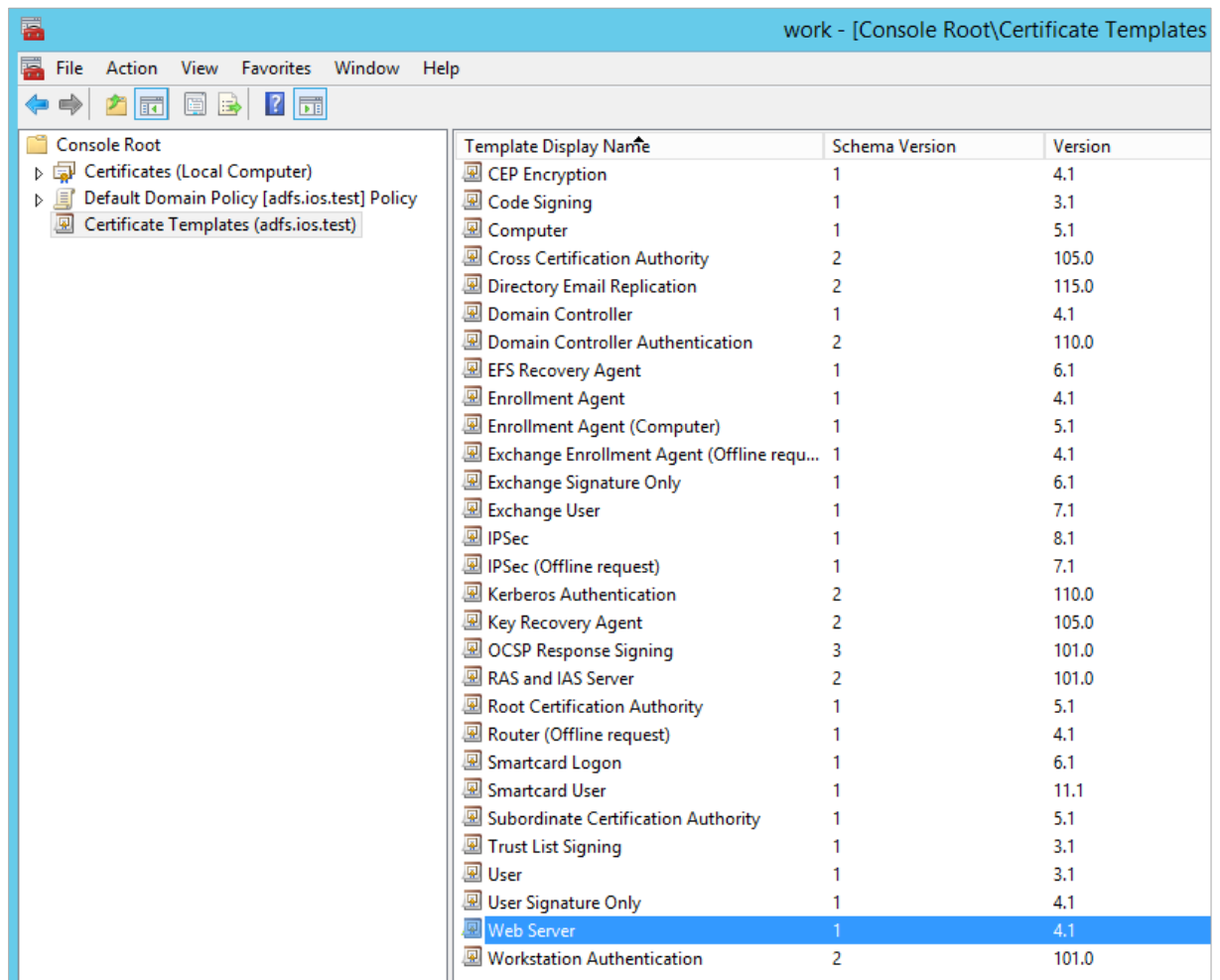


On the CA Properties Extensions tab, you need to remove **ldap** and **file** locations on both CRL Distribution Point and Authority Information Access extensions.

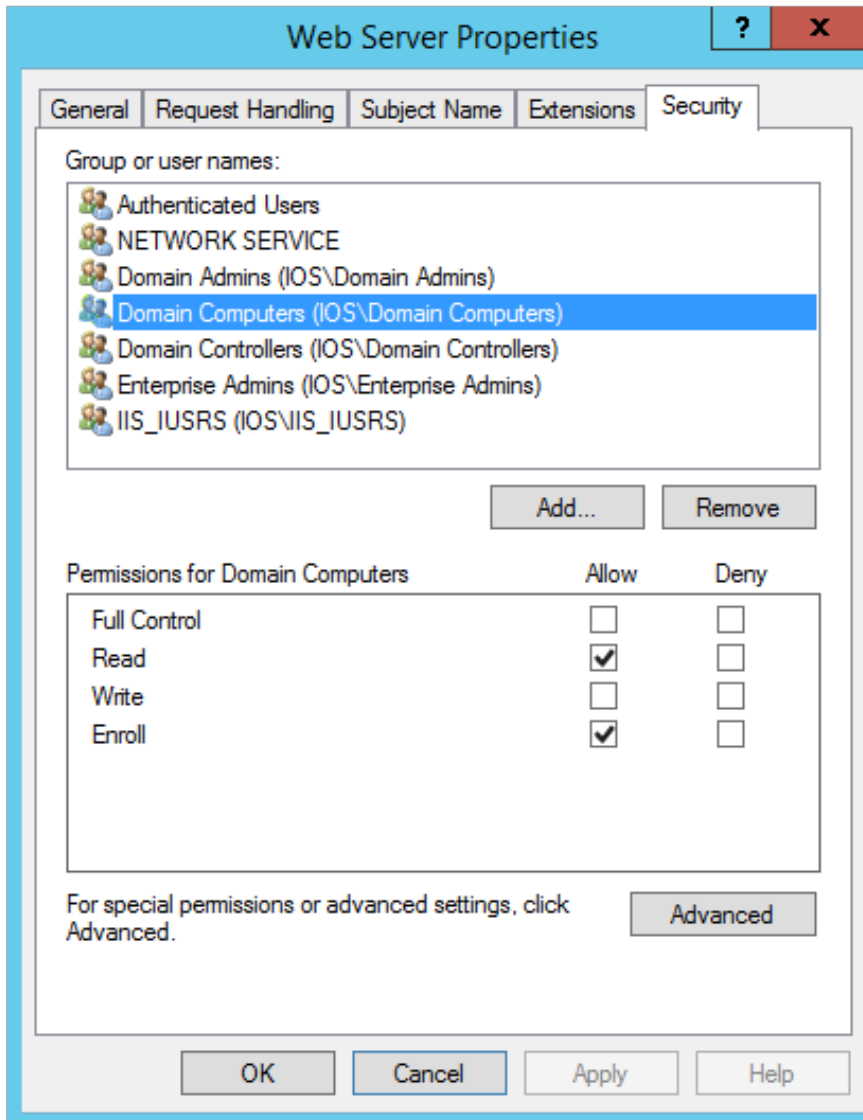


Also, you need to select the **Include in the CDP extension of issued certificates** and **Include in the AIA extension of issued certificates** check boxes.

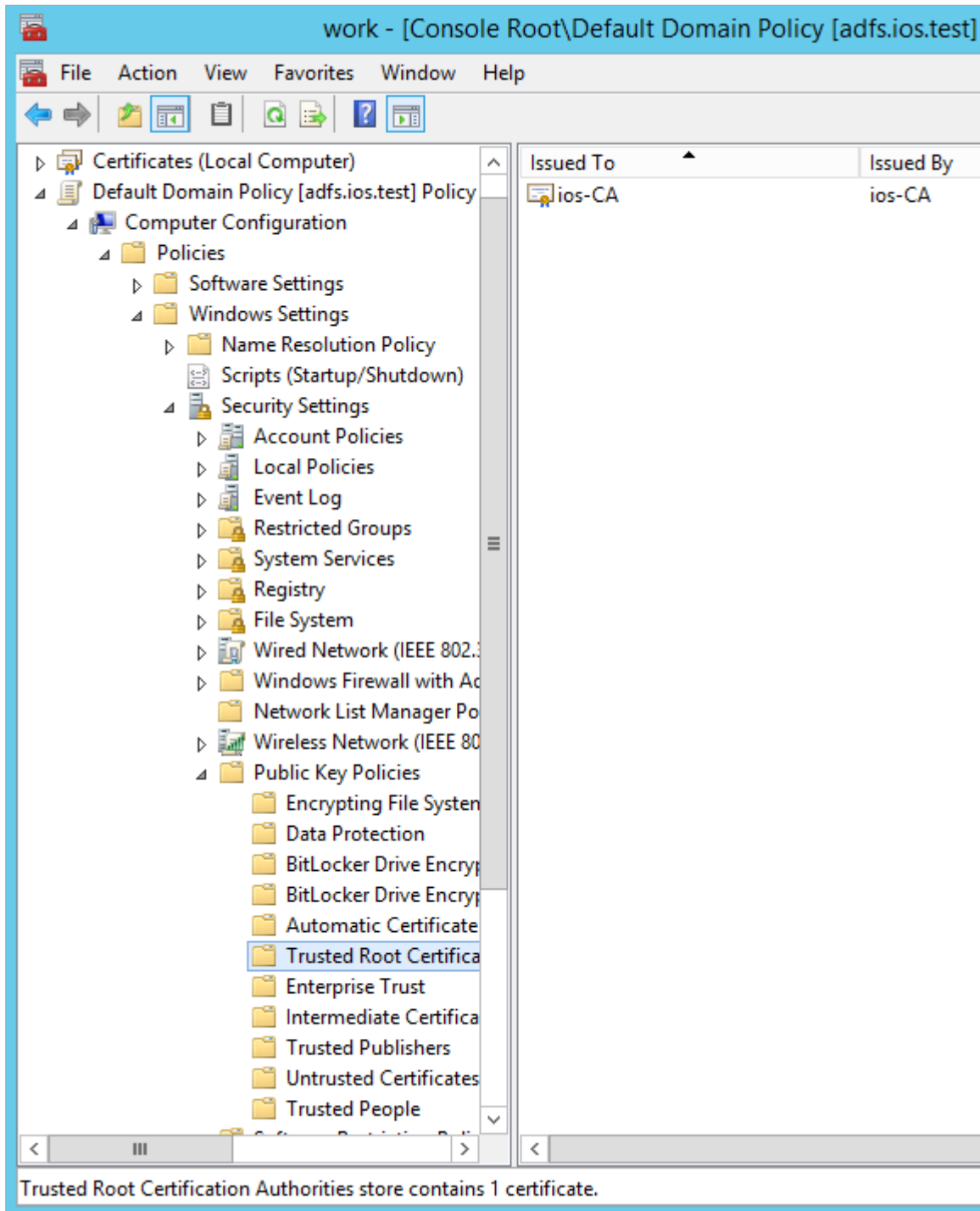
2. **Certificate Templates.** Using mmc console, edit properties of **Web Server** Certificate Template.



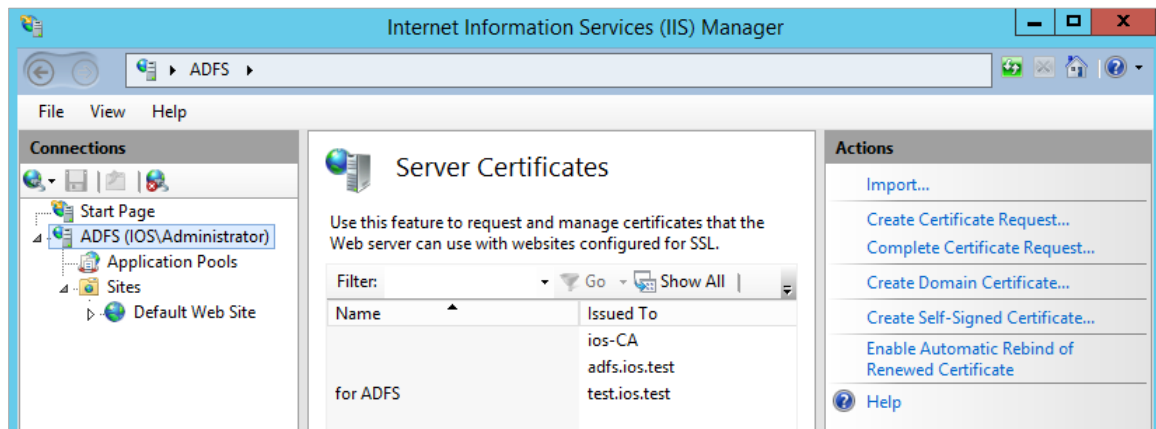
On the **Security** tab, add **Domain computers**, **Domain Controllers**, **IIS_IUSRS**, and **NETWORK SERVICE** with **Read** and **Enroll** permissions.



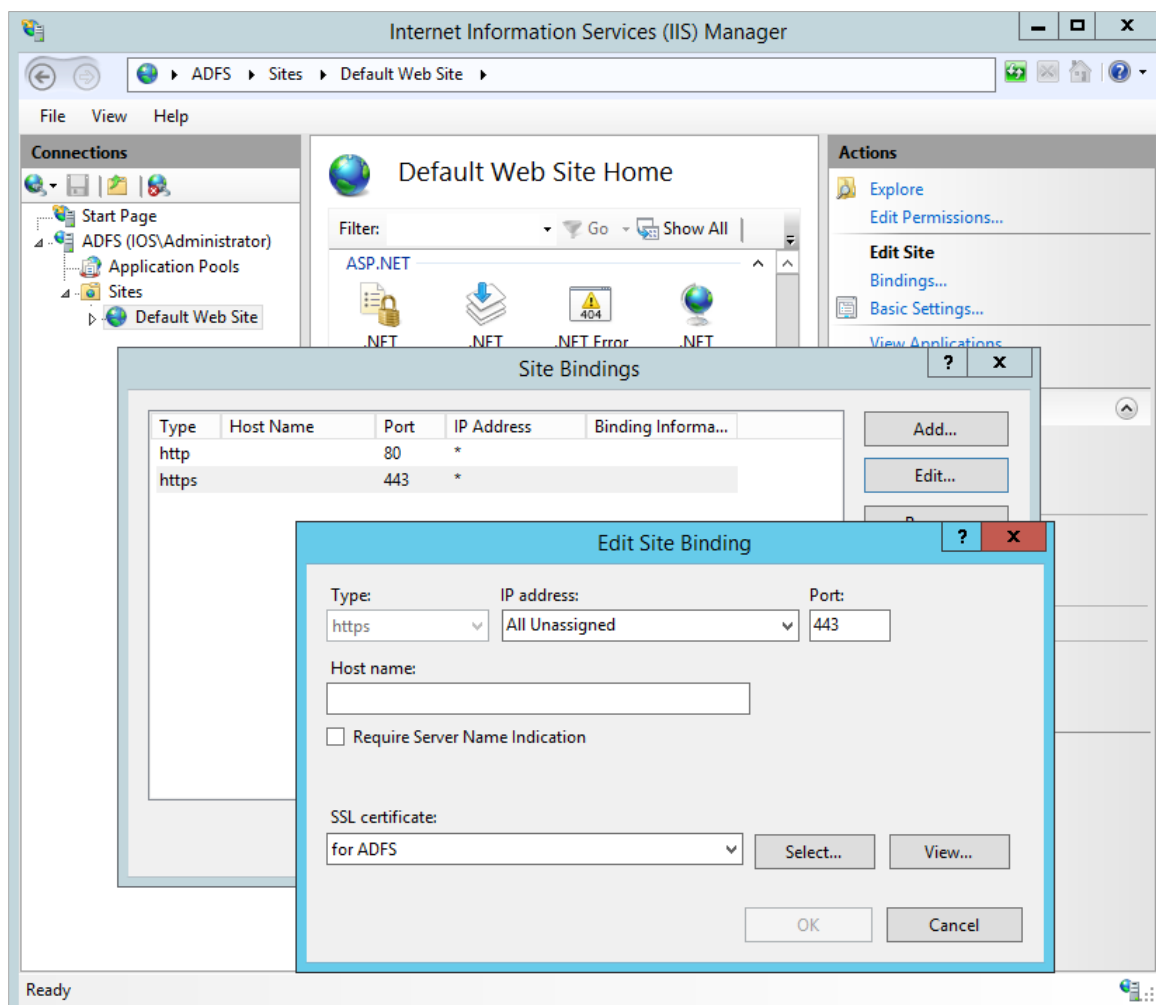
- 3. Default domain Policy. Import CA certificate to Trusted Root Certifications Authorities under Computer Configuration.



4. **SSL Certificate.** On IIS Manager, select **Create Domain Certificate** (CN must be the same as domain name) or use commercial certificate.



5. **Site bindings.** Add https binding to **Default Web Site** using self-created or commercial certificate.

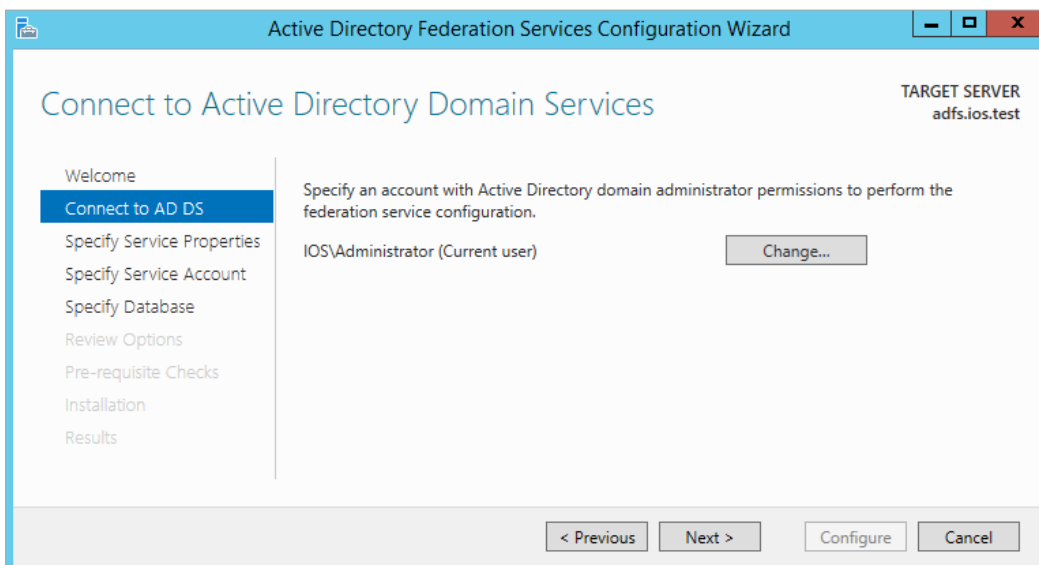


AD FS Installation

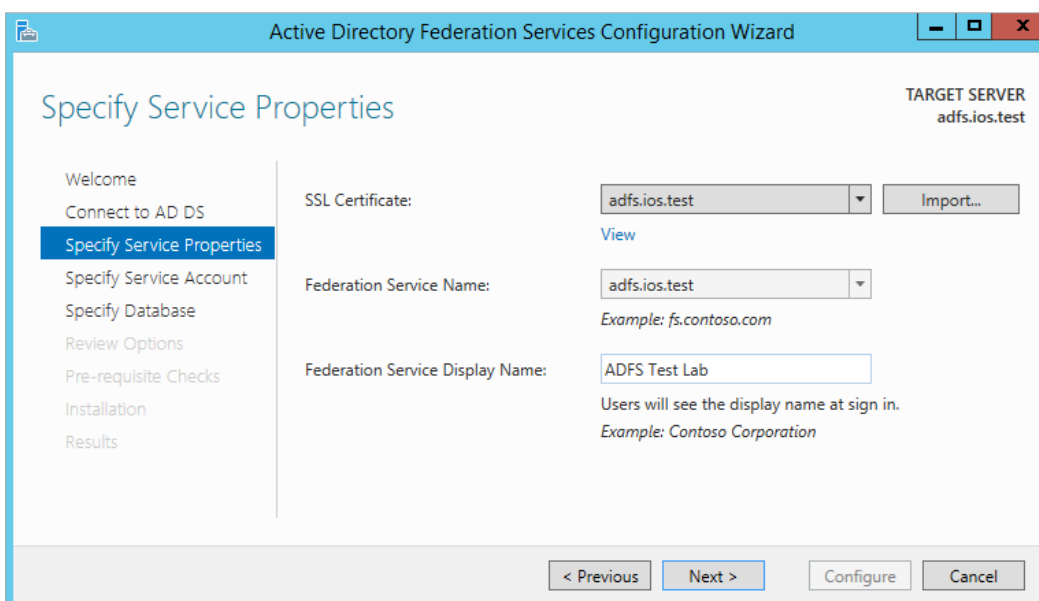
AD FS installs as a Windows Server 2012 R2 server role and does not require any additional download. After AD FS 3.0 installation configure the AD FS server and create the identity provider Security Token Service.

In the first panel of the AD FS Configuration Wizard specify the AD account that has permissions to perform the federation service configuration.

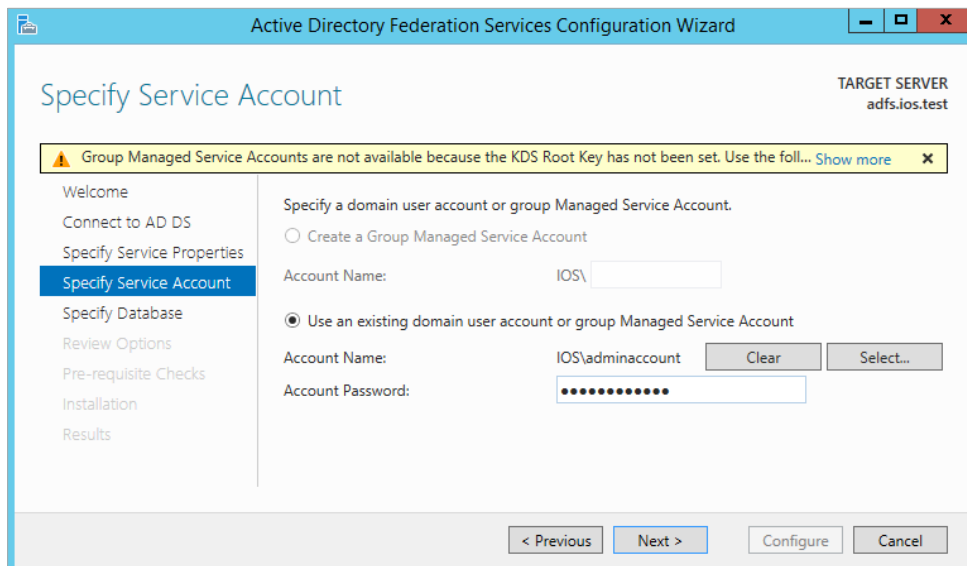
Note: This account must be a domain administrator.



In the next panel, specify the service properties. Import a wildcard SSL certificate for the service URL. Then, edit the default Federation Service Name of **adfs.ios.test**. This will be your federation service address and will serve as the root of your sign in URL.

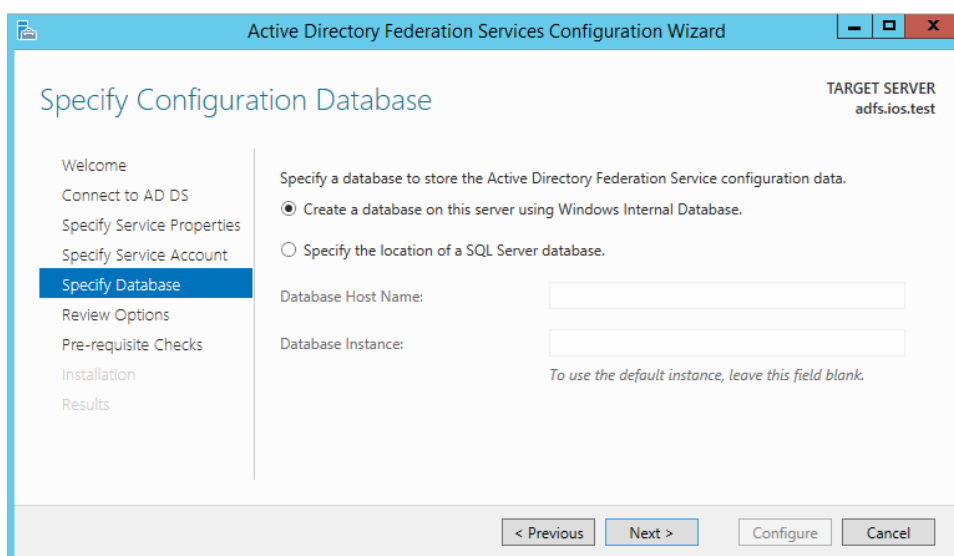


Specify a service account for the AD FS service. This should be a domain user account and requires no special permissions.



Note: One of the steps that is missing in almost every walk through of this process is the requirement to have a DNS **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 3.0 requires two databases to store configuration and artifact information and can use either the Windows Internal Database (WID) or SQL Server 2012. Both options do offer scalability although there are limitations to the use of the WID, such as the total number of federation servers allowed in the farm (5) or the lack of HA solution such as clustering or mirroring.

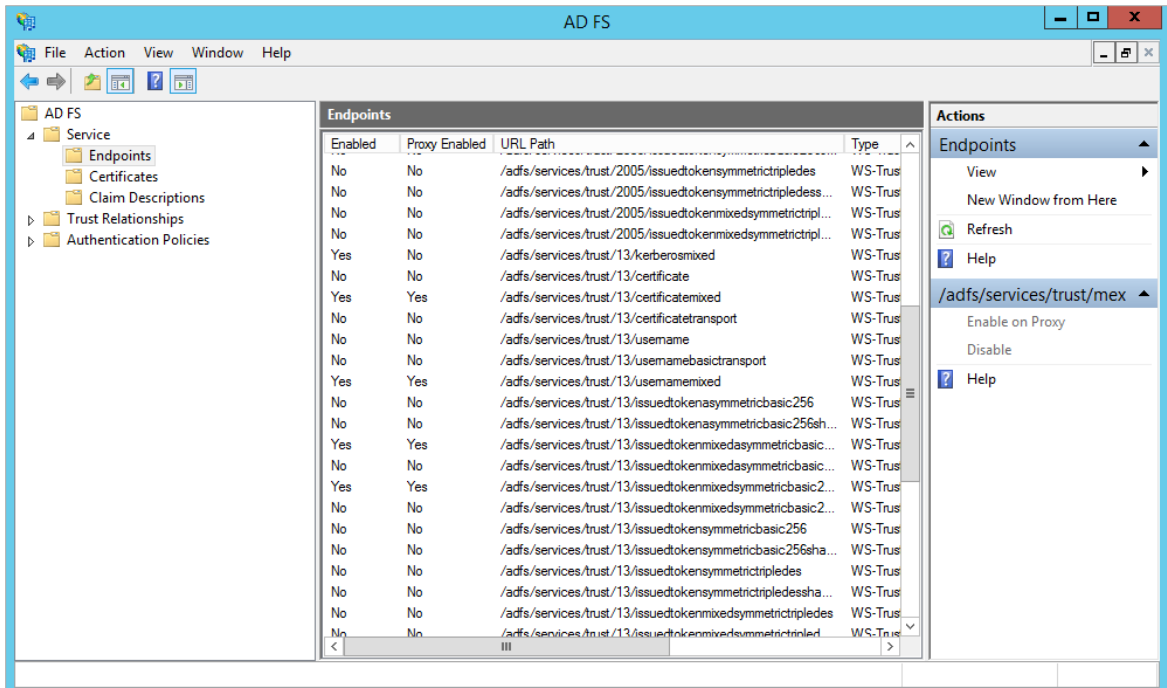


Main AD FS tool after installation is **Server Manager > Tools > AD FS Management**.

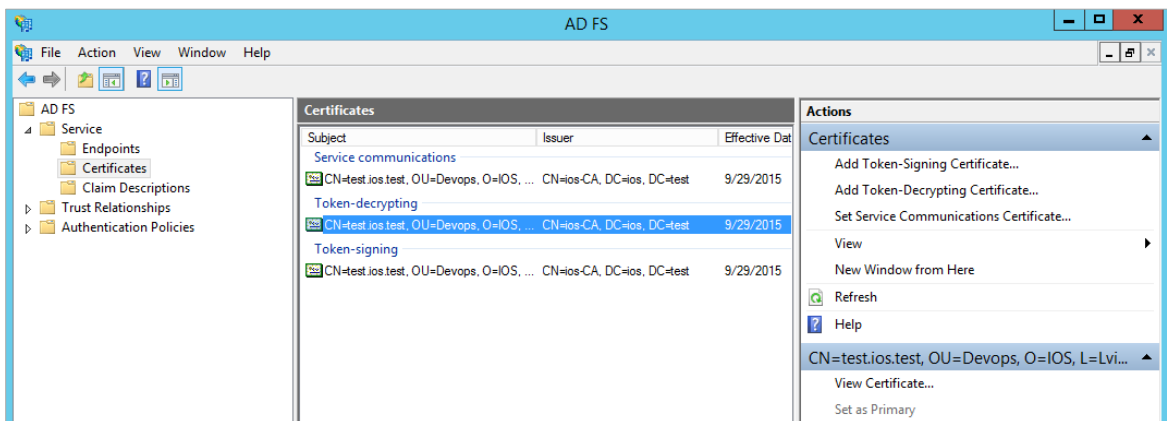
AD FS Configuration for SSO

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

- **Endpoints.** Verify that `/adfs/services/trust/13/usernamemixed` endpoint's **Enabled** and **Proxy Enabled** are Yes.



- **Certificates.** Make sure that all three subjects have certificates.



Certificates Management

From AD FS Management console you need navigate to the **Service > Certificates** folder. Then, navigate valid certificate (Token-decrypting or Token-signing), right click on it and you will have possibility to set it as a **Primary**.

If you will need to generate new certificates (**Decrypting/Signing/Service**), you may do this from:

<http://ip-your-adfs-server/certsrv>

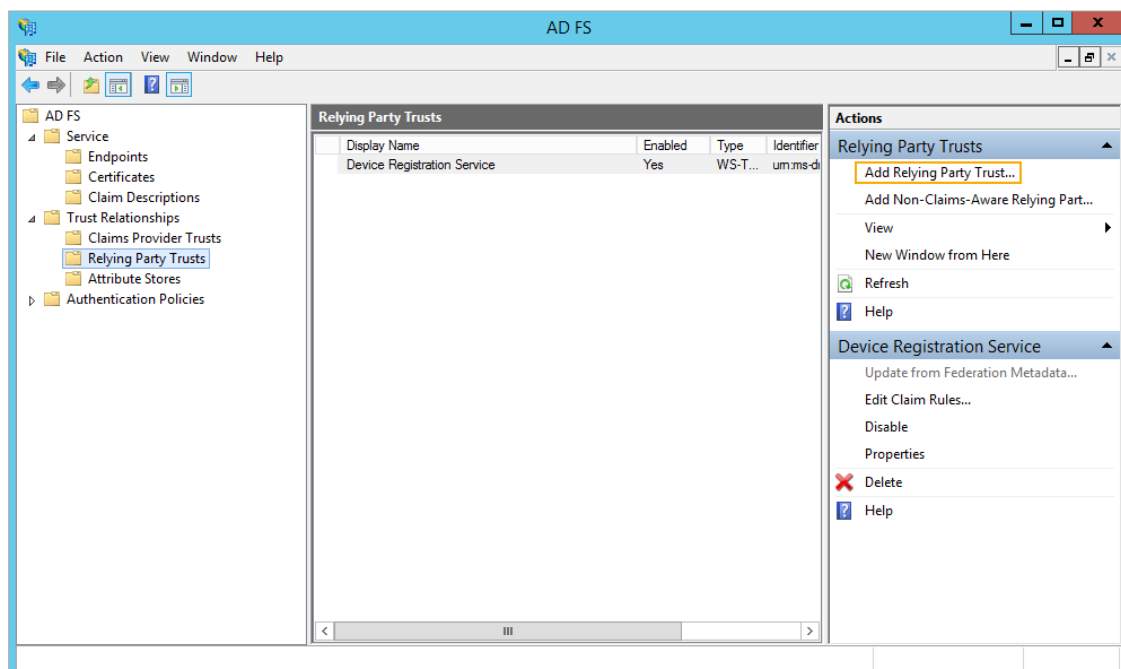
You may assign new certificates from **AD FS 3.0 Management** console, from the **Certificates** action pane.

After you assign new certificates, you need to restart **AD FS 3.0 Windows Service**.

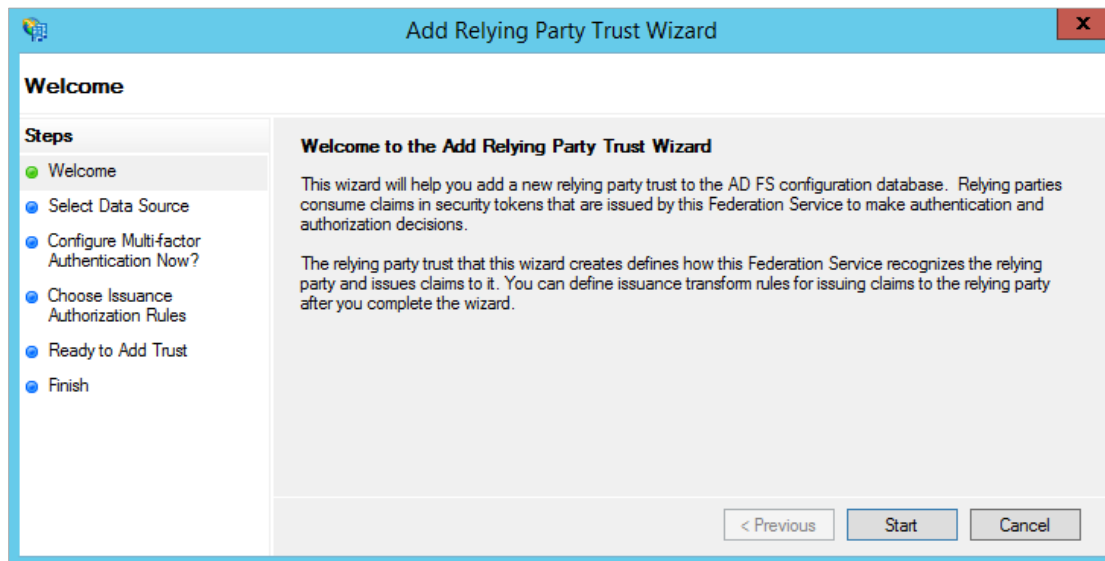
AD FS Configuration

AD FS should be configured to provide access to endpoints for Envi:

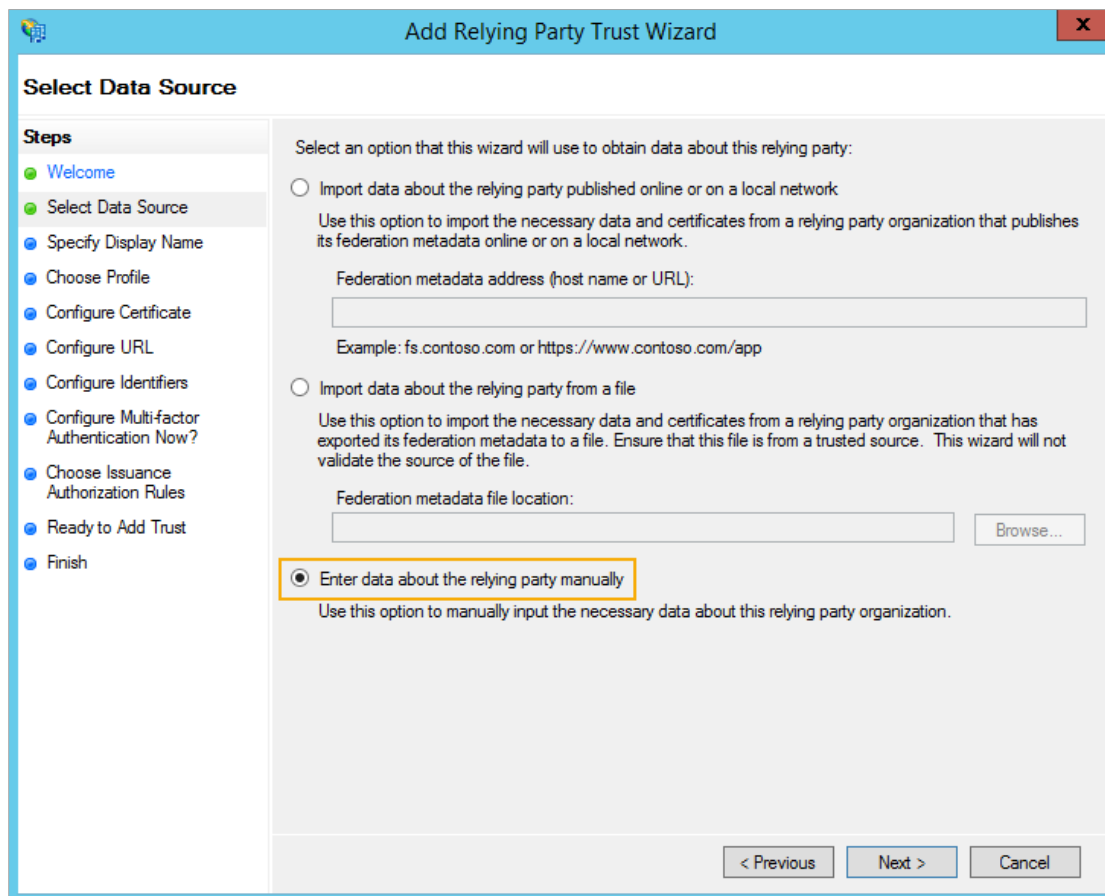
1. Open AD FS Management.
2. Select **Add Relying Party Trust** from the **Actions** section.



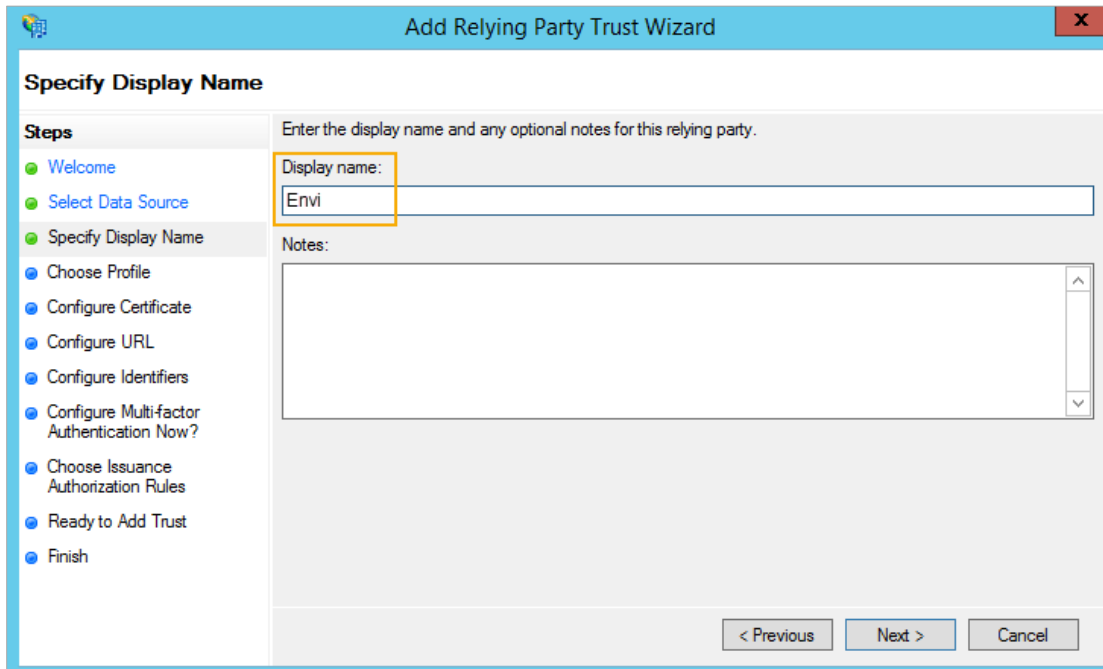
3. Follow wizard's steps. Click **Start**.



4. Select Enter data about the relying party manually. Click **Next >**.

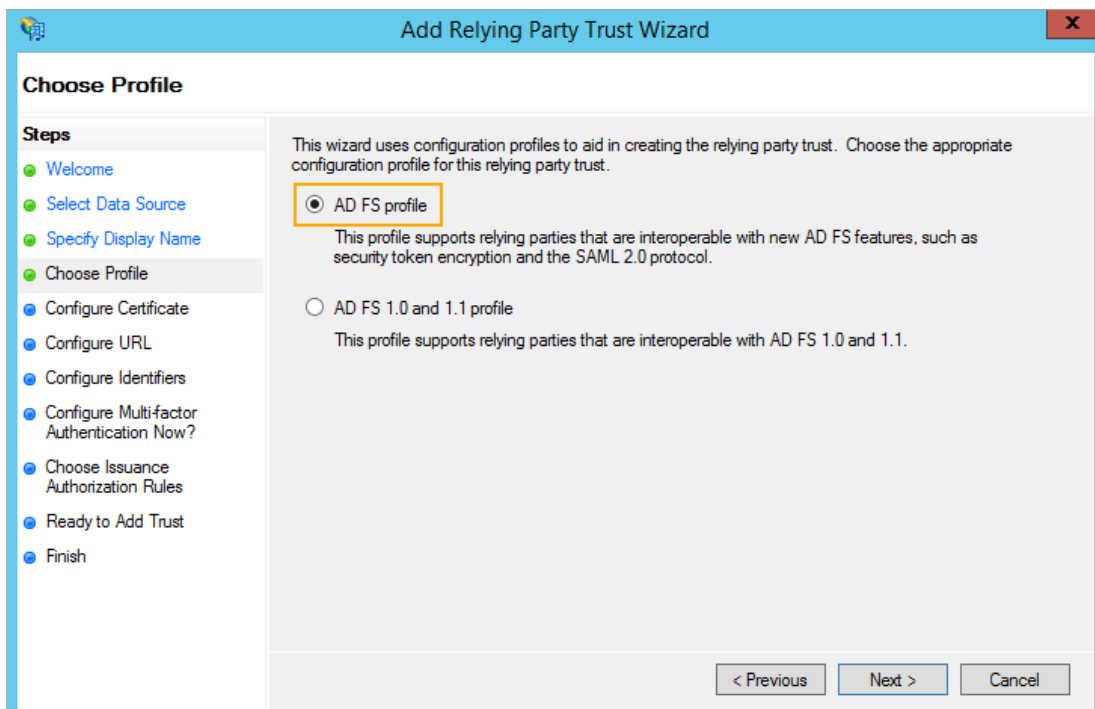


5. Type Display name. Click Next >.



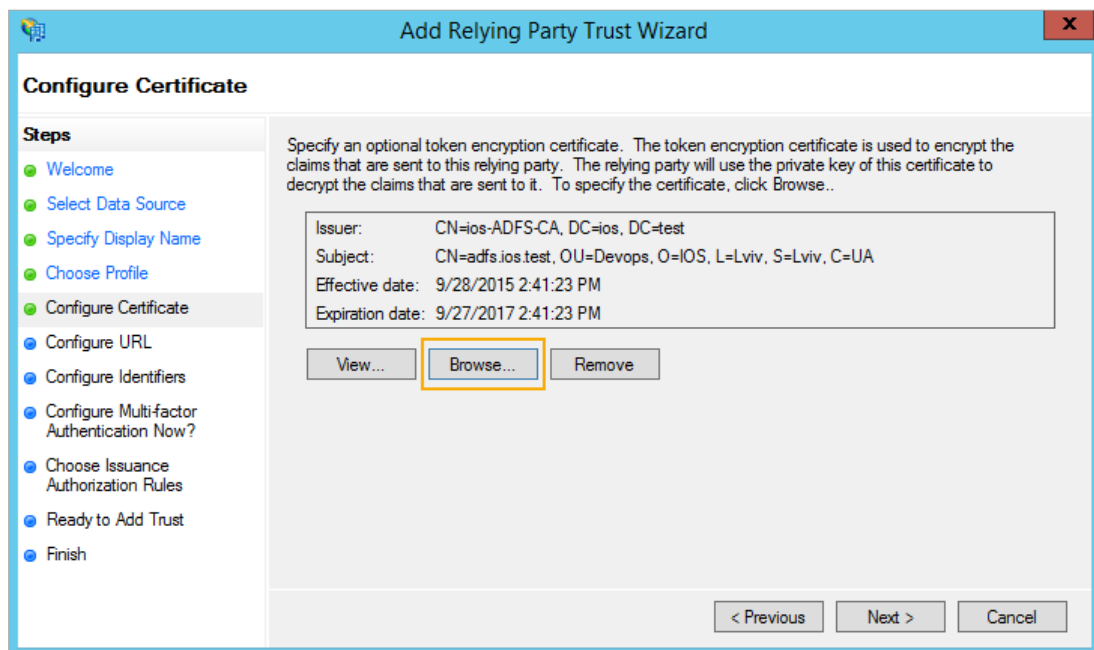
The screenshot shows the 'Specify Display Name' step of the 'Add Relying Party Trust Wizard'. The window title is 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction: 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' text box containing the text 'Envi', which is highlighted with a yellow box. Below the text box is a 'Notes:' text area. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

6. Select AD FS profile. Click Next >.

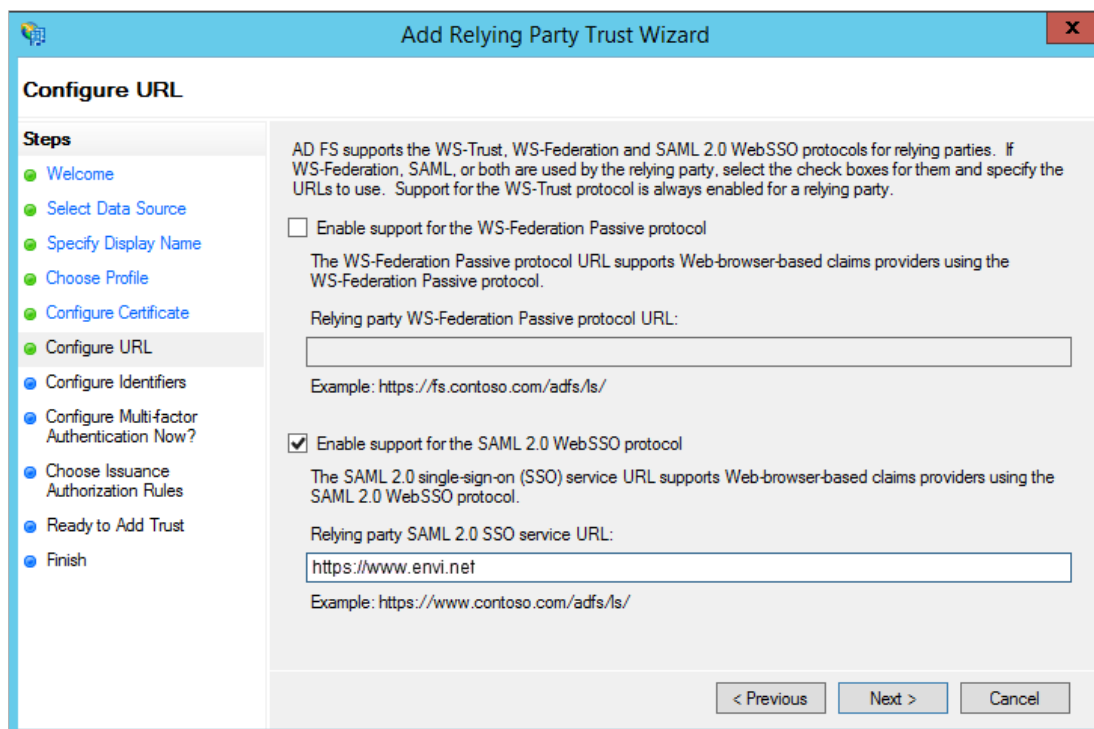


The screenshot shows the 'Choose Profile' step of the 'Add Relying Party Trust Wizard'. The window title is 'Add Relying Party Trust Wizard'. The main heading is 'Choose Profile'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile (highlighted), Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction: 'This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.' Below this, there are two radio button options. The first option is 'AD FS profile', which is selected and highlighted with a yellow box. Below it is the text: 'This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.' The second option is 'AD FS 1.0 and 1.1 profile', which is not selected. Below it is the text: 'This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

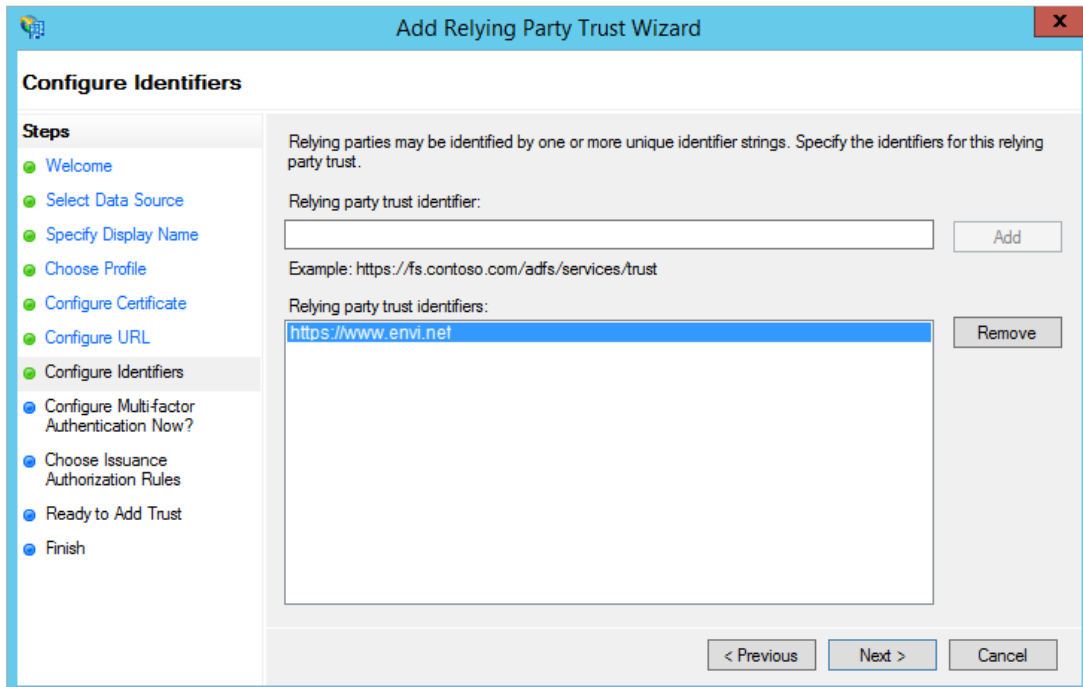
7. Select certificate with the **Browse** button. It could be your main certificate that you use during AD FS installation. Click **Next >**.



8. Select **Enable support for the SAML 2.0 WebSSO protocol**, and then type Envi application URL (it must be https). Click **Next >**.



- Fill **Relying party trust identifier**. It could be any URL address (easy to reuse your application one). Click **Add** then **Next >**.



Add Relying Party Trust Wizard

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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

Relying party trust identifier:

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

Relying party trust identifiers:

<code>https://www.envi.net</code>	<input type="button" value="Remove"/>
-----------------------------------	---------------------------------------

< Previous Next > Cancel

- Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time**. Click **Next >**.

Configuring Authentication Policies.' Navigation buttons '< Previous', 'Next >', and 'Cancel' are at the bottom." data-bbox="148 535 816 918"/>

Add Relying Party Trust Wizard

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

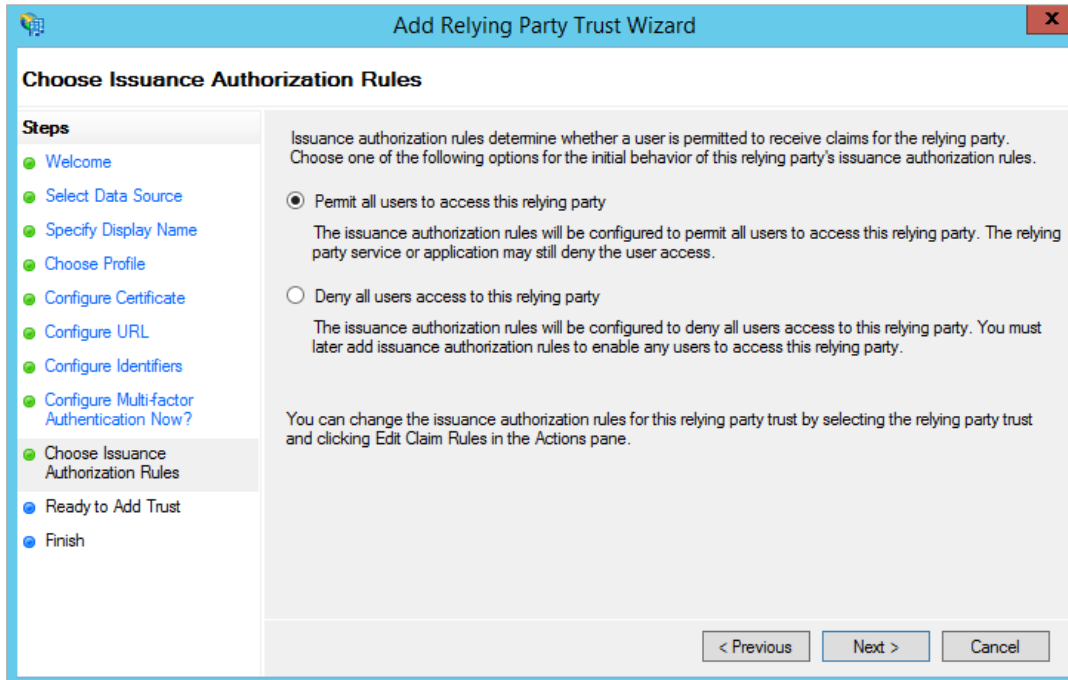
I do not want to configure multi-factor authentication settings for this relying party trust at this time.

 Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous Next > Cancel

11. Select Permit all users to access this relying party. Click Next >.



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules**
- Ready to Add Trust
- Finish

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

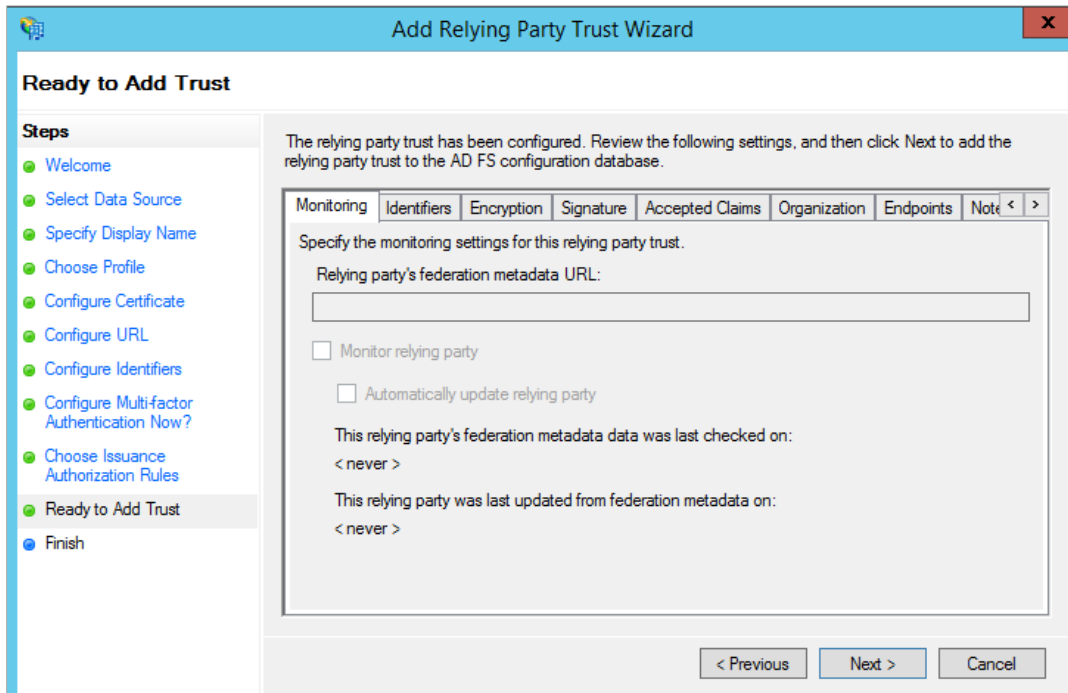
Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

< Previous Next > Cancel

12. Click Next >.



Add Relying Party Trust Wizard

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust**
- Finish

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.

Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Not < >

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

Monitor relying party

Automatically update relying party

This relying party's federation metadata data was last checked on:

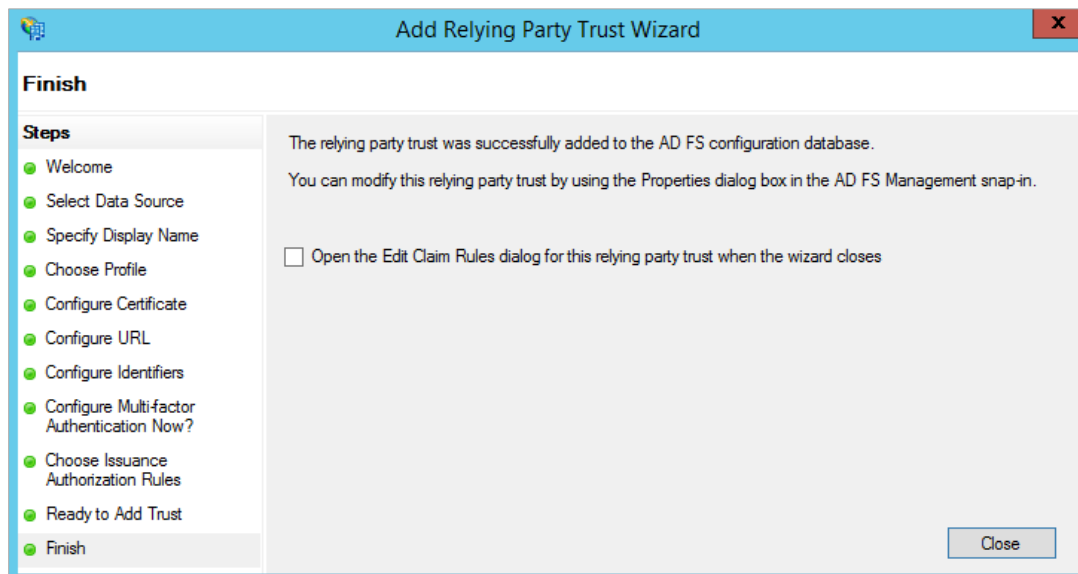
< never >

This relying party was last updated from federation metadata on:

< never >

< Previous Next > Cancel

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



Envi Testing

To test Envi, perform the following steps:

1. Open Envi application URL.
(for example, <https://sso-demo.envi.com>)
2. Fill in all the required fields:
 - **Username** – existing user in your system (under AD)
 - **Password** – password for existing 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** – the 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"/>
---	---