envi

AD FS Configuration for SSO

May, 2019

Table of Contents

Introduction

The document provides an overview of **Active Directory Federation Services** (**AD FS**) for **Envi**.

Note: In the following table, you can find 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 a zip archive package.

Preparation

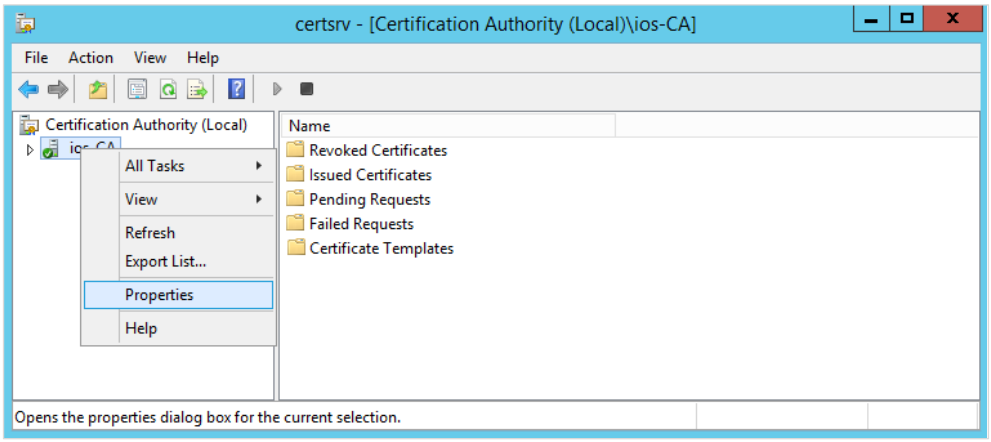
To configure **Active Directory Federation Services** (**AD FS**), follow the next preparatory steps:

- Certification Authority
- Certificate Templates
- Default Domain Policy
- SSL Certificate
- Site Bindings

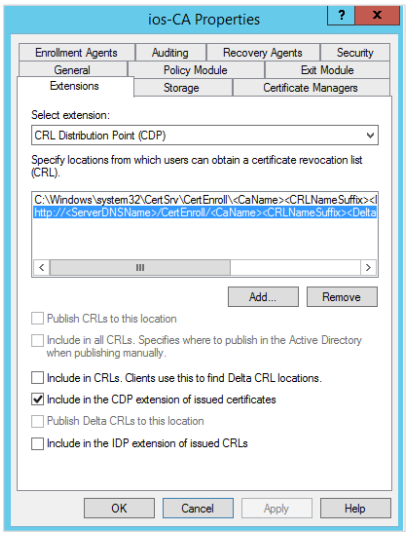
Certification Authority

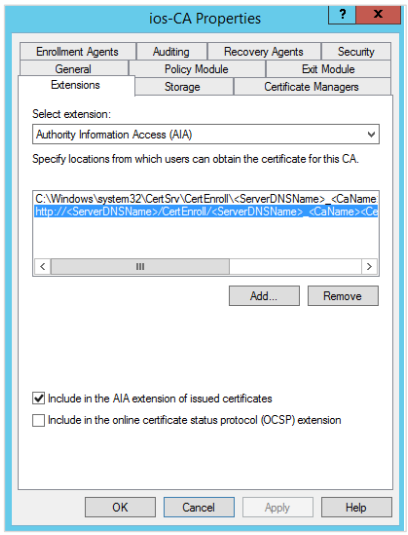
Let's start with the first option from the list—**Certification Authority**.

1. Under **Server Manager** > **Tools** > **Certification Authority**, edit **Certification Authority** properties.



2. On the **CA Properties Extensions** tab, follow the next steps for both the **CRL Distribution Point** and **Authority Information Access** extensions:
   a. Remove **ldap** and **file locations**.
   b. Select the **Include in the CDP extension of issued certificates** and **Include in the AIA extension of issued certificates** checkboxes accordingly.

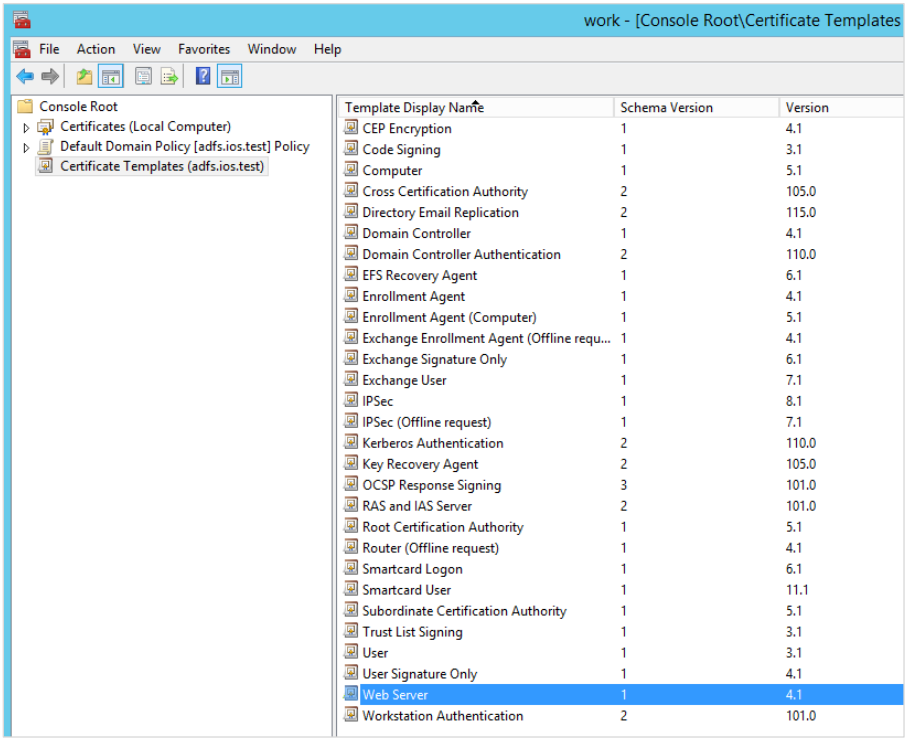




Certificate Templates

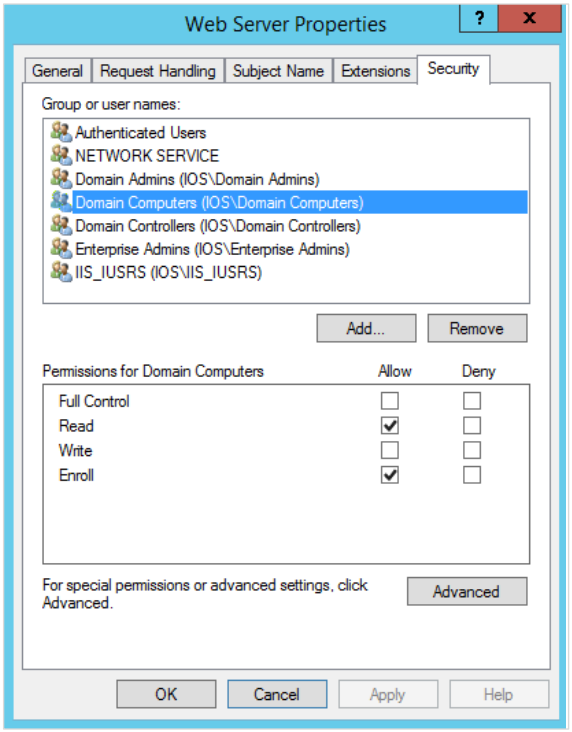
The next step is about certificate templates.

1. Edit properties of **Web Server** Certificate Template using **mmc console**.



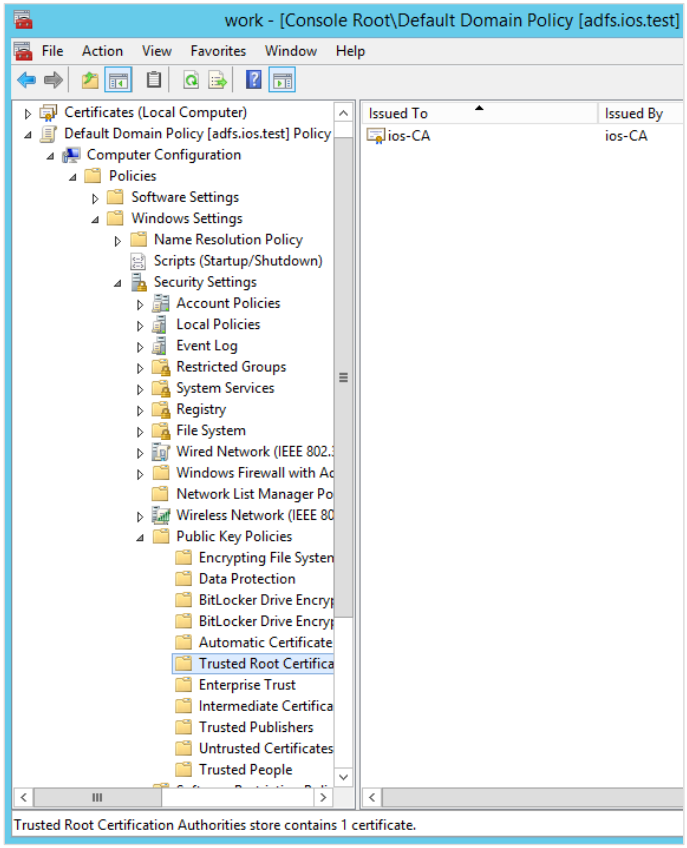
2. On the **Security** tab, add the following group and user names with the **Read** and **Enroll** permissions for each:

   - **NETWORK SERVICE**
   - **Domain Computers**
   - **Domain Controllers**
   - **IIS_IUSRS**



Default Domain Policy

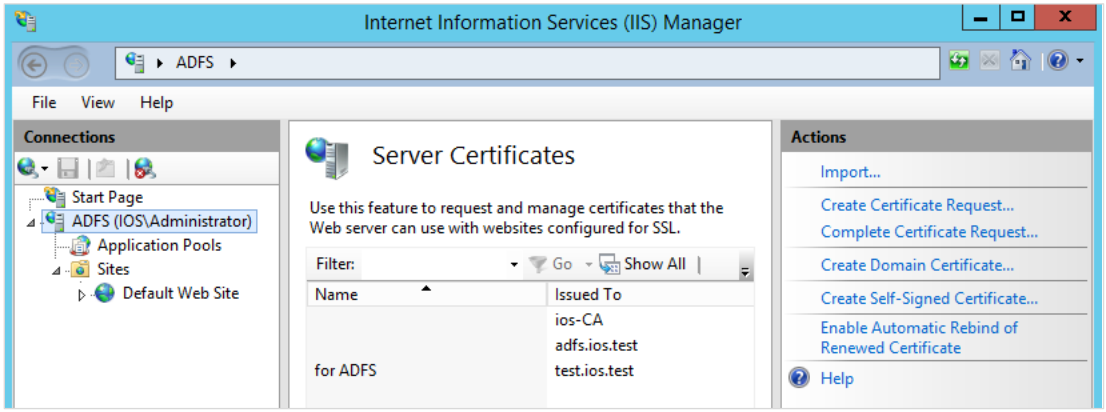
Under **Computer Configuration**, import the **CA certificate** to **Trusted Root Certifications Authorities**.



SSL Certificate

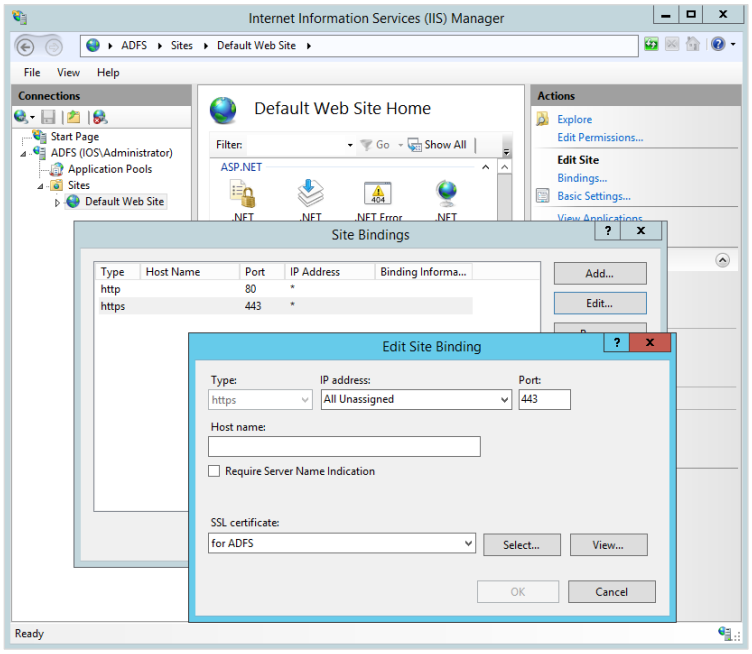
On **IIS Manager**, select **Create Domain Certificate** or use a commercial certificate.

Note: The **CN** must be the same as the domain name.



Site Bindings

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

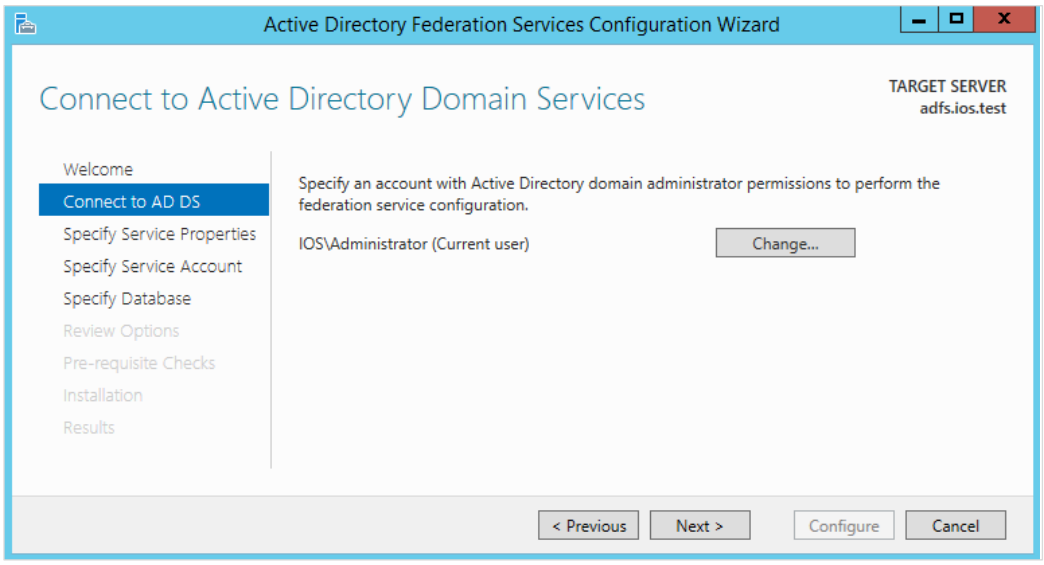


AD FS Installation

AD FS installs as a **Windows Server 2012 R2** server role and requires no additional download. After the **AD FS 3.0** installation, configure the **AD FS** server and create the identity provider Security Token Service. To do this, follow the next steps:

1. In the **AD FS Configuration Wizard**, on the **Connect to Active Directory Domain Services** page, specify the **AD** account with permissions to perform the federation service configuration and then select **Next >**.

   Note: This account must be a domain administrator.



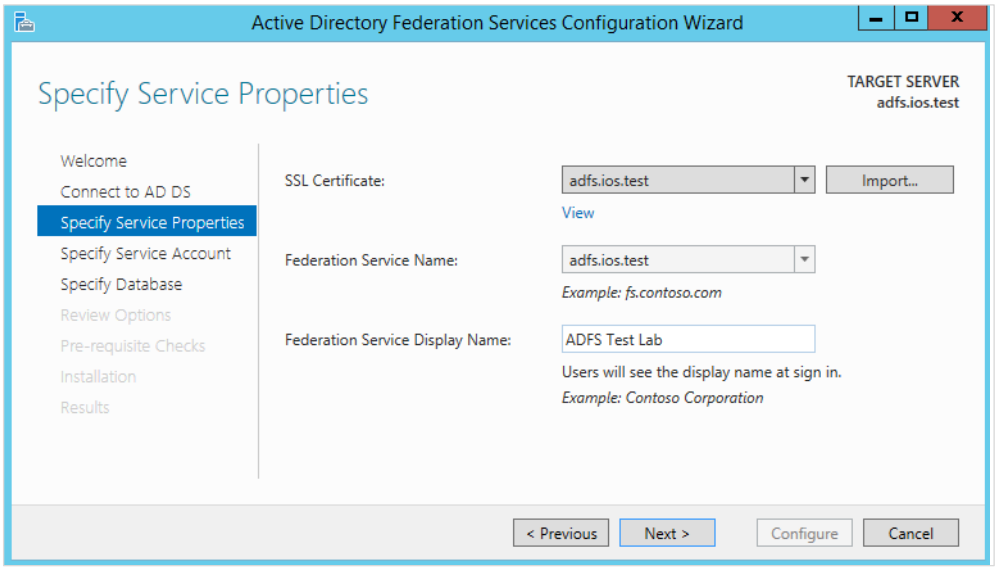
2. On the **Specify Service Properties** page, follow the next steps:

   c. **Import** a wildcard **SSL Certificate** for the service URL.

   d. Edit the default **Federation Service Name** (for example, adfs.ios.test).

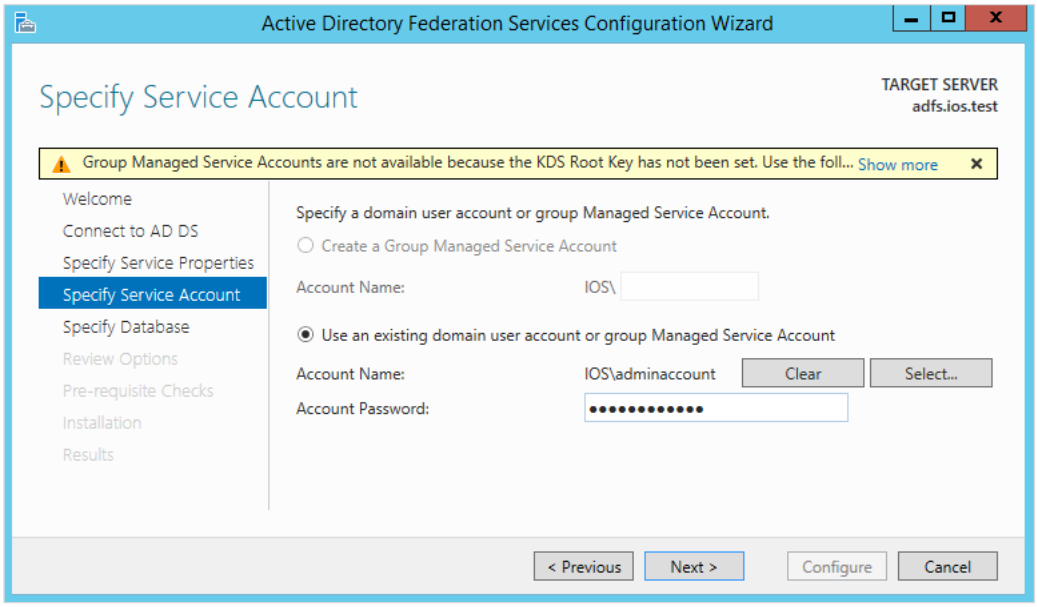
      Note: The name you provide will serve as your federation service address and act as the root of your sign-in URL.

   e. Select **Next >**.



3. On the **Specify Service Account** page, specify a domain user service account and then select **Next >**.

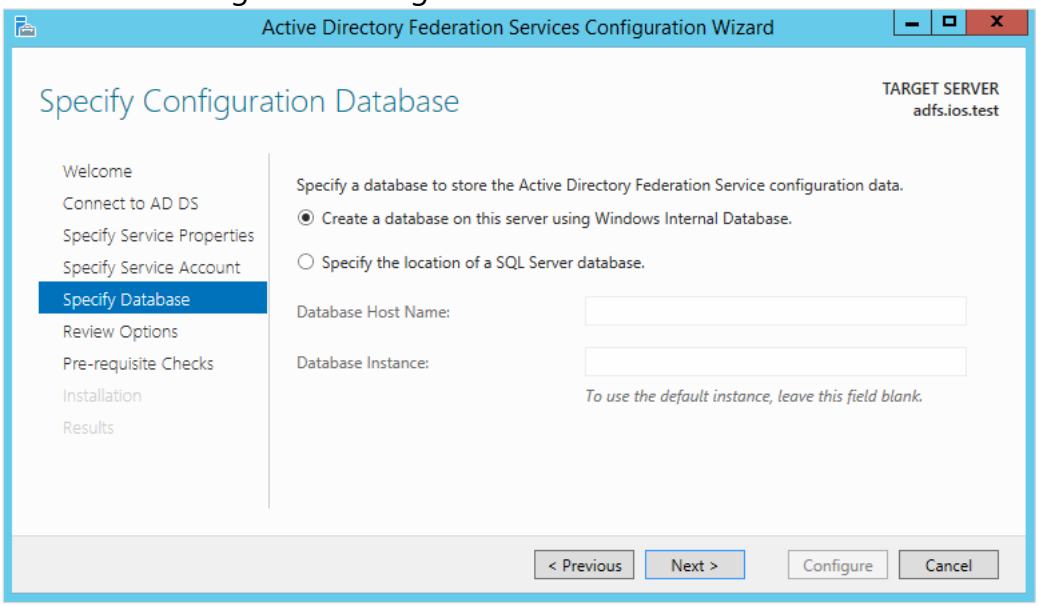
Note: This account should require no special permissions.



Note: One of the steps often missing in many walkthroughs of this process is the necessity of creating a **DNS A** record to support the **Federation Service** name. Without this **DNS** entry, applications that support **Single Sign-On** (**SSO**) won't be able to resolve the URL and connect to the **AD FS** service.

Note: **AD FS 3.0** requires two databases to store configuration and artifact information. It supports the **Windows Internal Database** (**WID**) or **SQL Server 2012**.

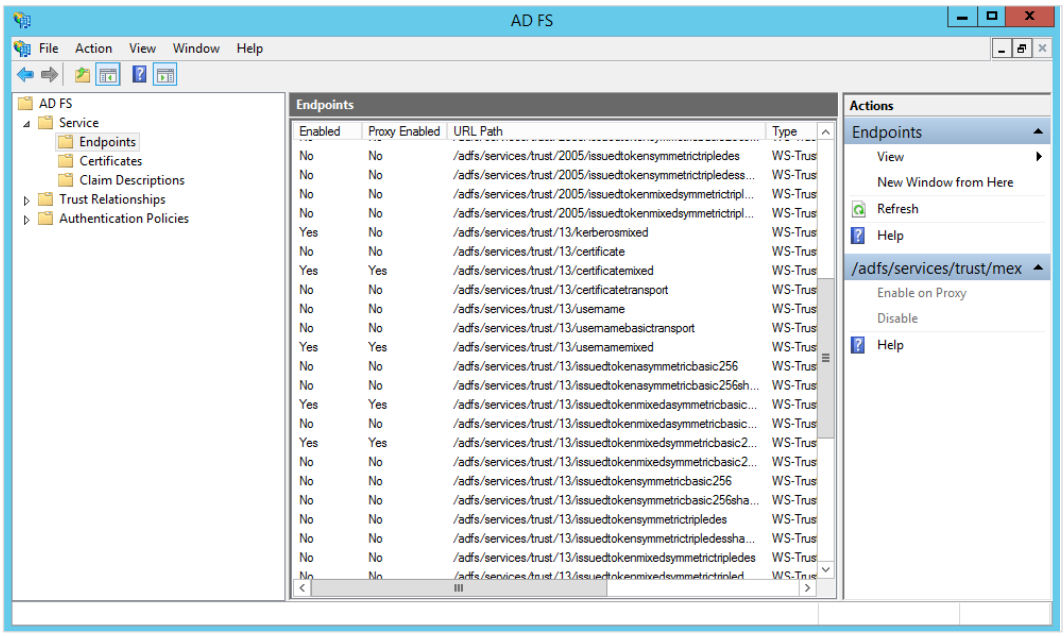
Both options offer scalability, although **WID** has limitations, such as the total number of federation servers allowed in the farm (5) or the absence of HA solutions, such as clustering or mirroring.



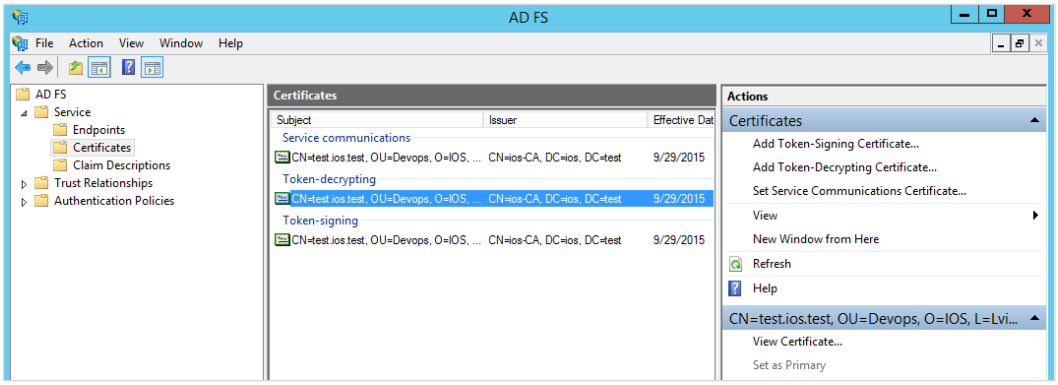
Note: The main **AD FS** tool after the installation is **Server Manager** > **Tools** > **AD FS Management**.

To ensure that you have properly installed **AD FS**, check the following settings in **AD FS Management**:

- **Endpoints**: review the configuration of the **/adfs/services/trust/13/usernamemixed** endpoint to ensure that both the **Enabled** and **Proxy Enabled** settings are set to **Yes**.



- **Certificates**: confirm that all three subjects have certificates.



Certificates Management

To manage certificates, follow the next steps:

1. Open the **AD FS Management** console and then go to the **Service** > **Certificates** folder.
2. Select a valid certificate (Token-decrypting or Token-signing).
3. Right-click the selected certificate and then set it to **Primary**.

Note: If you need new certificates (Decrypting/Signing/Service), use the following template: **http://ip-your-adfs-server/certsrv**.

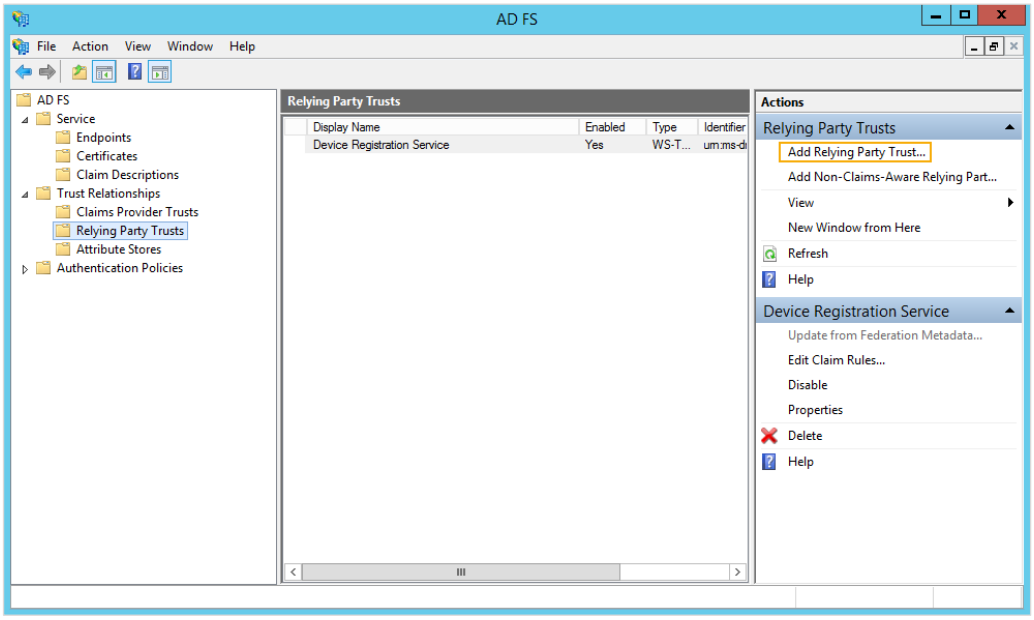
Once obtained, follow the next steps:

1. Assign certificates using the **AD FS 3.0 Management** console in the **Certificates** action pane.
2. Restart the **AD FS 3.0 Windows Service**.

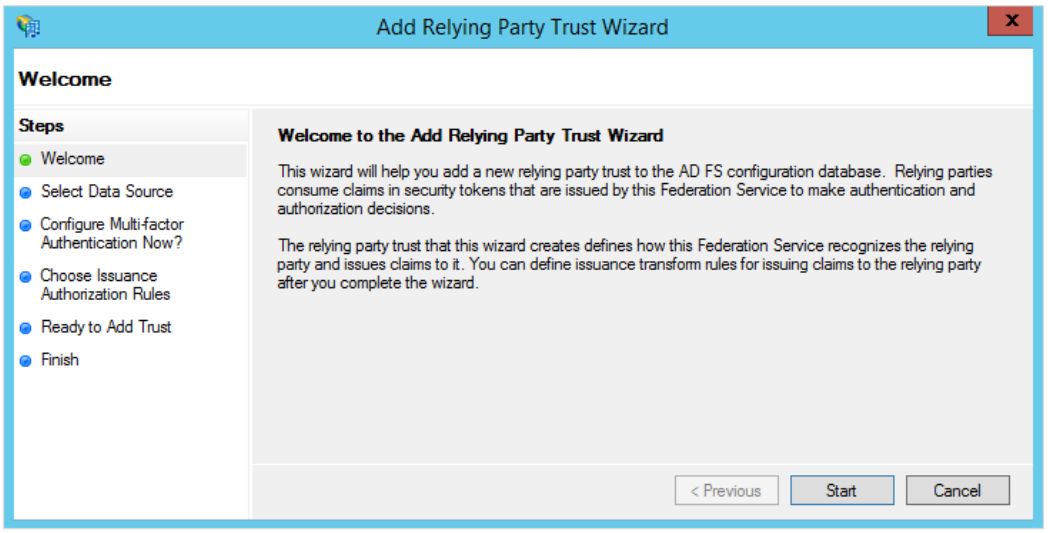
AD FS Configuration

Before providing access to endpoints for **Envi**, it's crucial to configure **AD FS** appropriately. To start the configuration, follow the next steps:

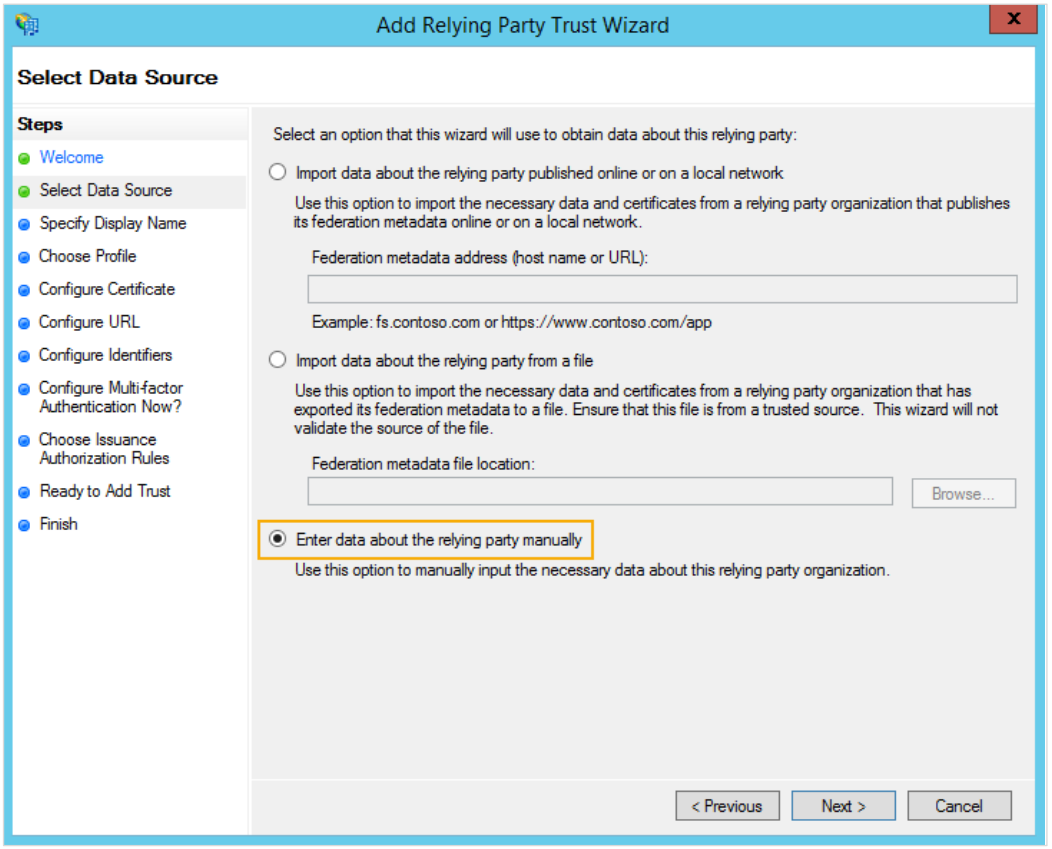
1. Open the **AD FS Management** console.
2. In the **Actions** section, select **Add Relying Party Trust**.



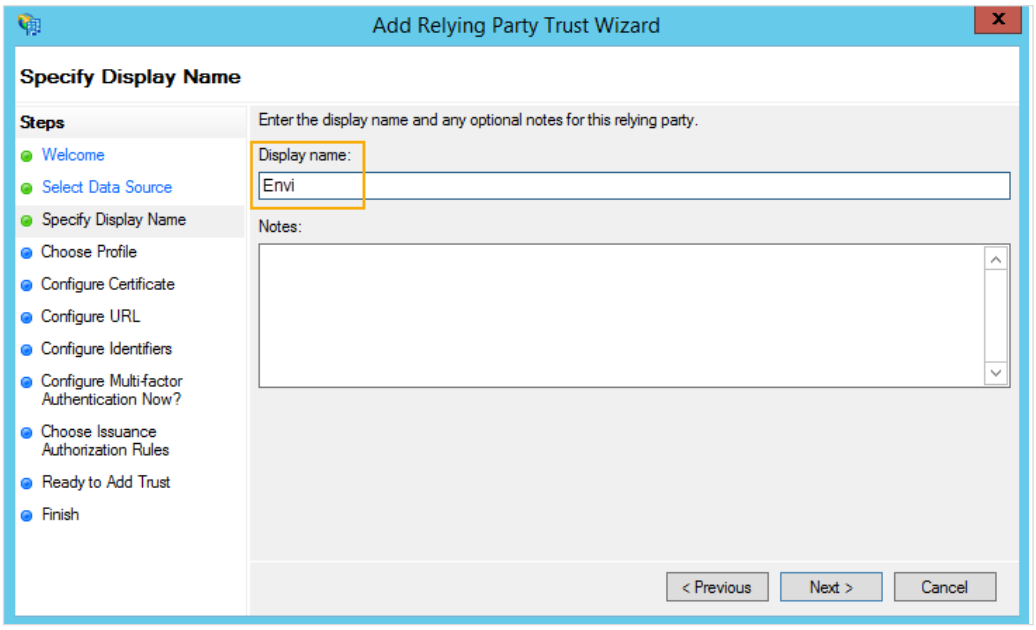
3. In **Add Relying Party Trust Wizard**, on the **Welcome** page, select **Start**.



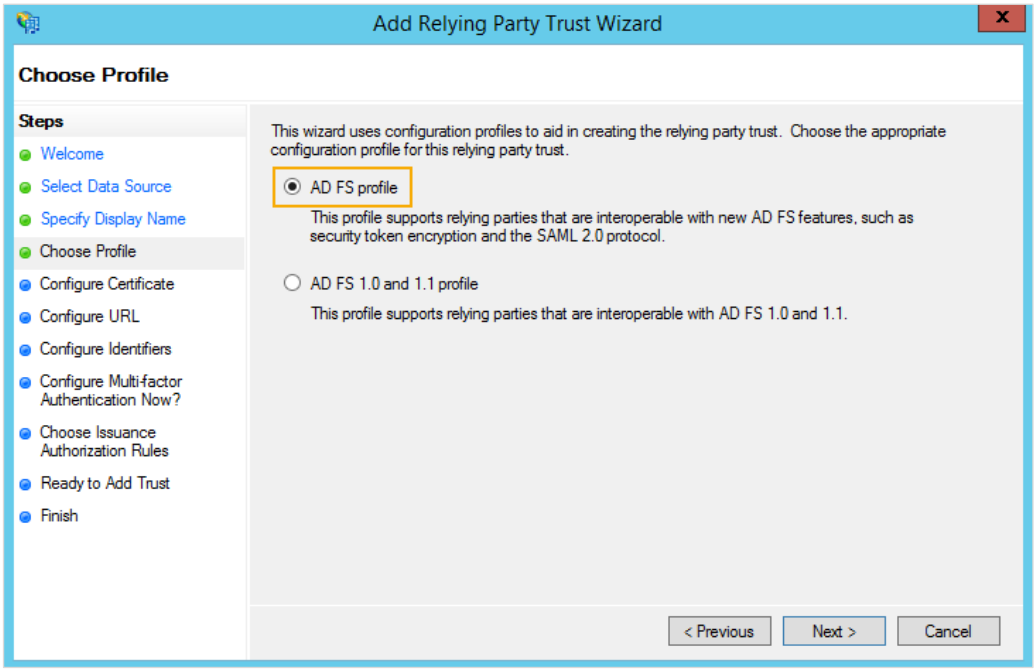
4. On the **Select Data Source** page, select the **Enter data about the relying party manually** checkbox and then select **Next >**.



5. On the **Specify Display Name** page, enter **Display name** and then select **Next >**.

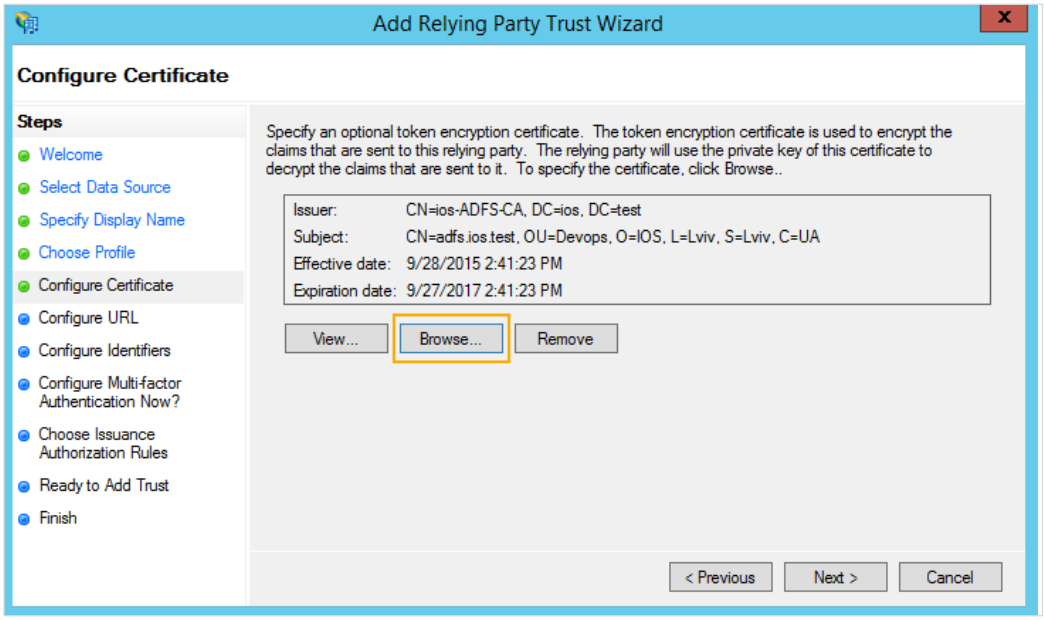


6. On the **Choose Profile** page, select the **AD FS profile** checkbox and then select **Next >**.



7. On the **Configure Certificate** page, select the **Browse** button to upload a certificate and then select **Next >**.

   Note: You can add the main certificate you used during the **AD FS** installation.

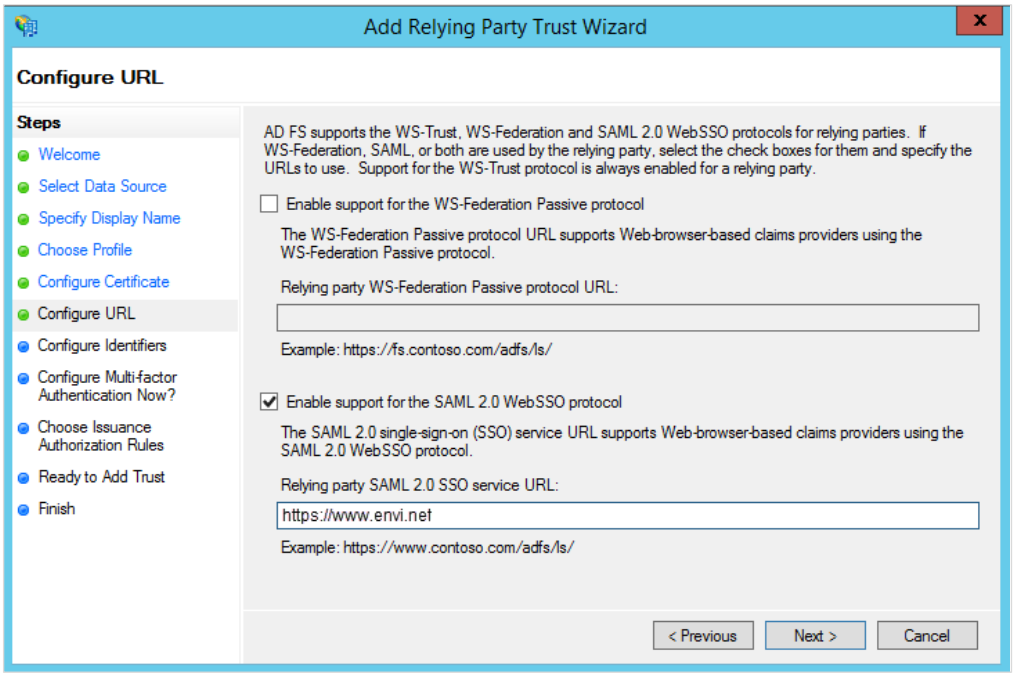


8. On the **Configure URL** page, follow the next steps:

   a. Select the **Enable support for the SAML 2.0 WebSSO protocol** checkbox.
   b. In the **Relying party SAML 2.0 SSO service URL** box, enter the URL of the **Envi** application.

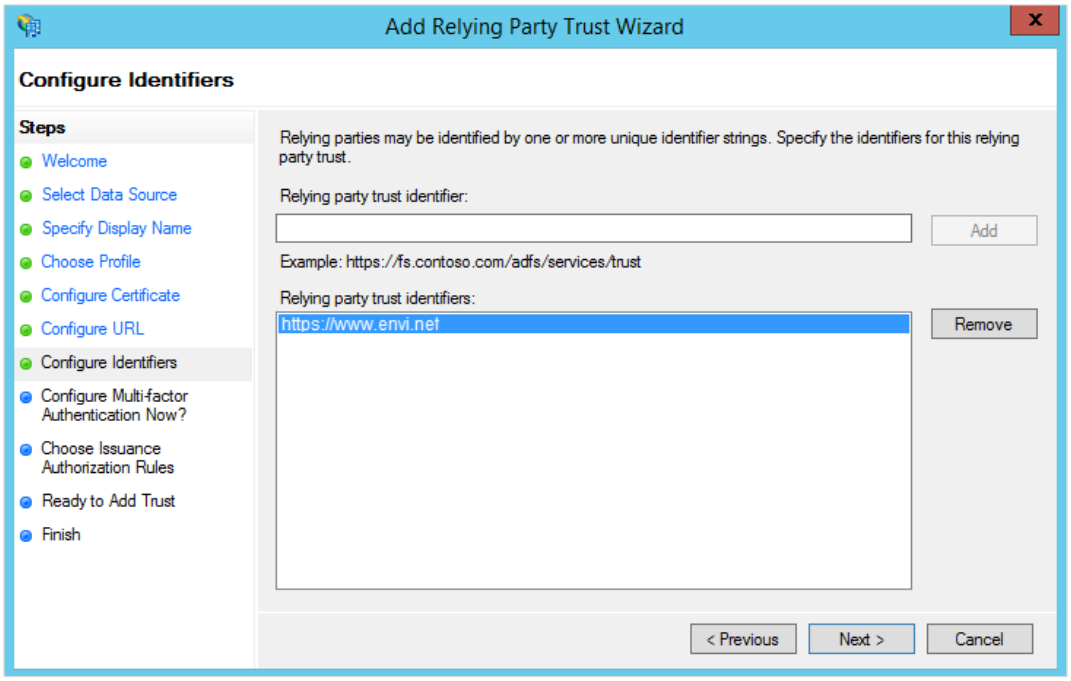
      Note: The URL must start with **https**.

   c. Select **Next >**.

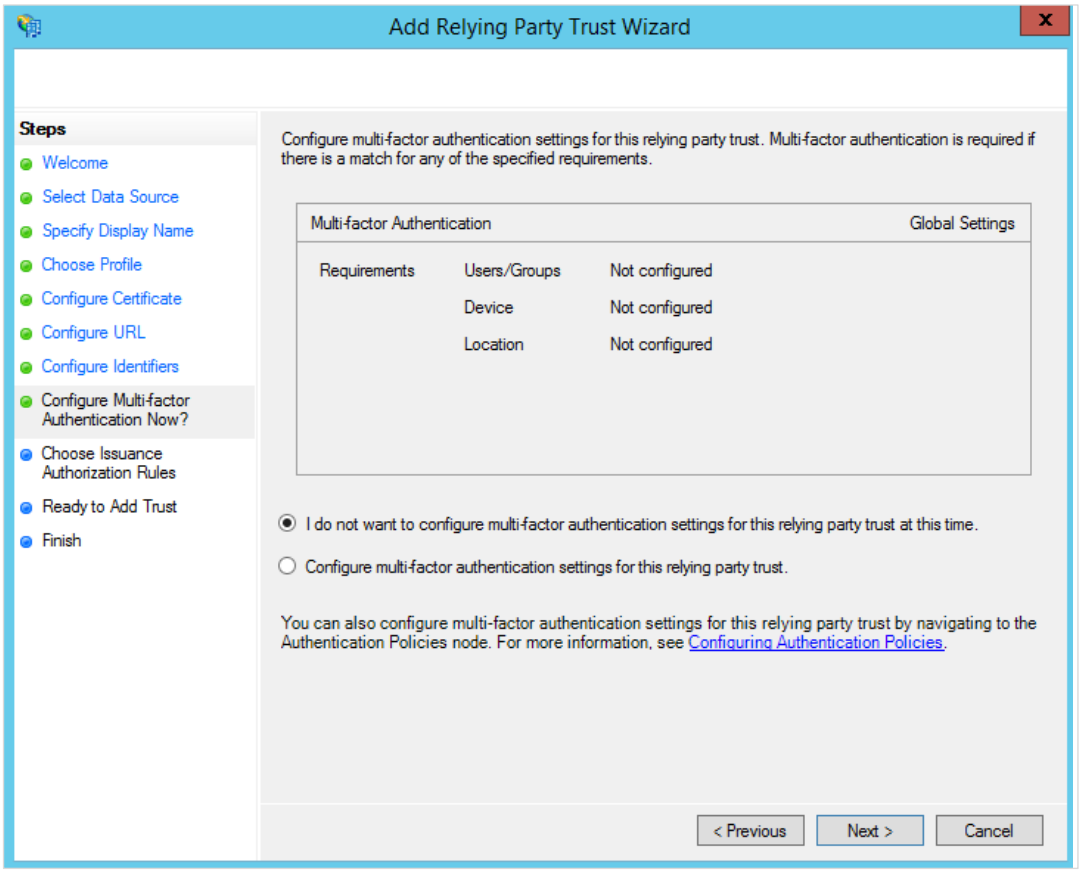


9. On the **Configure Identifiers** page, in the **Relying party trust identifier** box, select **Add** a URL address, and then select **Next >**.

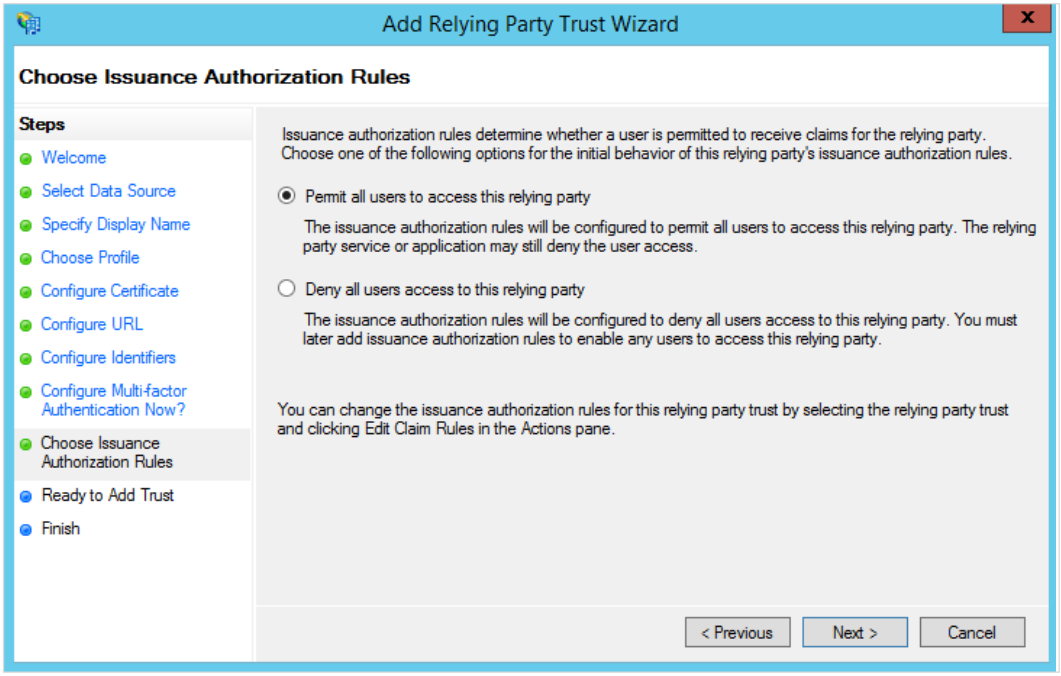
Note: You can use any URL address, including the option to reuse your application's URL.



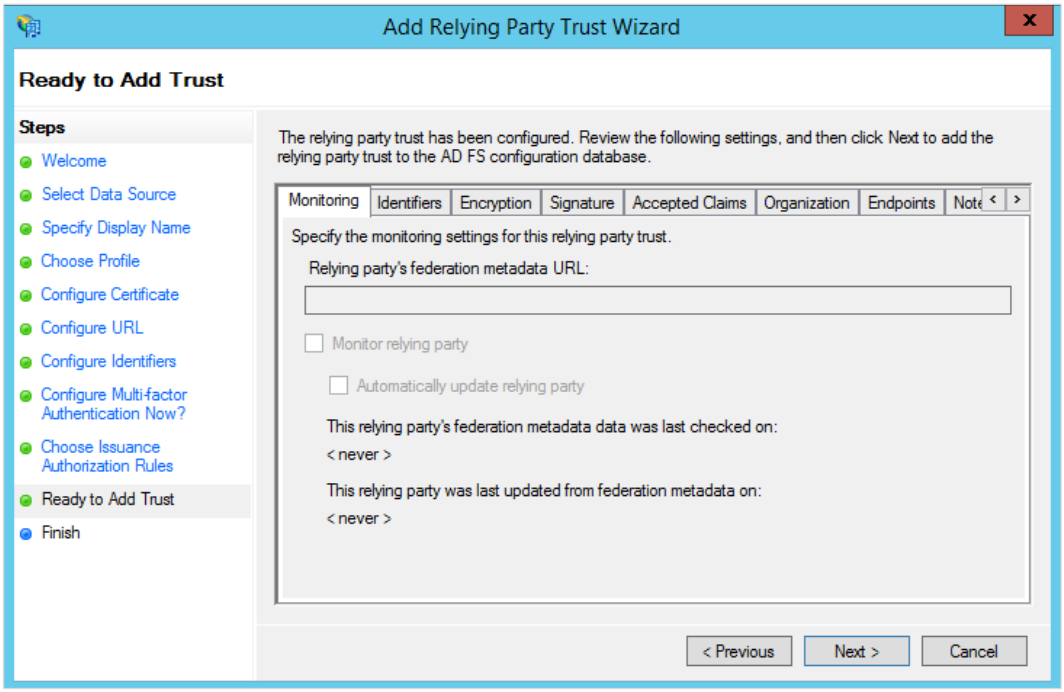
10. On the **Configure Multi-factor Authentication** page, select the **I do not want to configure multi-factor authentication settings for this relying party trust at this time** checkbox and then select **Next >**.



11. On the **Choose Issuance Authorization Rules** page, select the **Permit all users to access this relying party** checkbox and then select **Next >**.

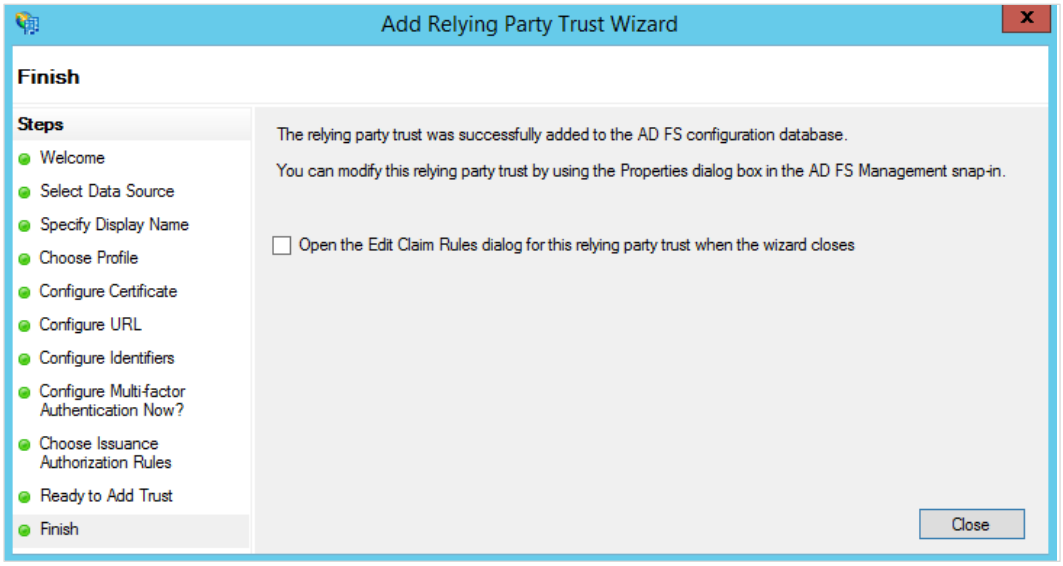


12. On the **Ready to Add Trust** page, only select **Next >**.



13. On the **Finish** page, clear the **Open the Edit Claim Rules for this relying party trust when the wizard closes** checkbox and then select **Close**.

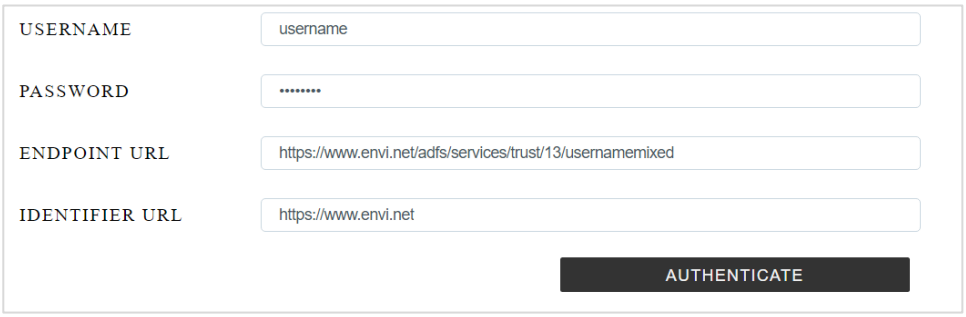
Note: It is optional, and you may proceed with additional configuration if needed.



Envi Testing

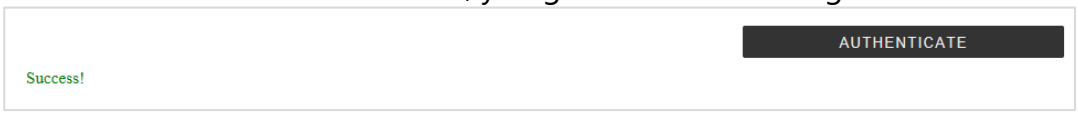
To test **Envi**, follow the next steps:

1. Open the **Envi** application URL (for example, https://sso-demo.envi.com).
2. Enter the required boxes with the following information:
   - **Username**—the username of an existing user in your system (under AD).
   - **Password**—the password for the existing user in your system.
   - **AD FS Endpoint URL**—create it by adding https://your.adfs.ip.address/ + adfs/services/trust/13/usernamemixed (you can use a domain name instead of the IP address).
   - **AD FS Identifier URL**—use the identifier entered during the creation of **Relying Party Trust** for **Envi** (for more information, go to the **AD FS Configuration** section).



3. Select the **Authenticate** button.

Note: If the authentication is successful, you get a success message.



Note: If an error occurs, you receive the error message.