



AD FS Configuration for SSO

May, 2019



Table of Contents

Introduction	2
Assumptions	2
Preparation	3
AD FS Installation	7
AD FS Configuration	10
Envi Testing	17

Introduction

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

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

Note: In the following table, you can find the abbreviations used in the document.

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

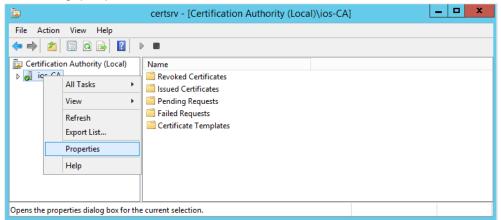
To configure **Active Directory Federation Services** (**AD FS**), follow the next preparatory steps:

- <u>Certification Authority</u>
- <u>Certificate Templates</u>
- Default Domain Policy
- <u>SSL Certificate</u>
- <u>Site Bindings</u>

Certification Authority

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

 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.

	ios-CA Prope	erties	? X		ios-CA Pr	operties		? X
Enrollment Agents	Auditing F	Recovery Agents	Security	Enrollment Agents	Auditing	Recovery	Agents	Security
General	Policy Module	Б	dt Module	General	Policy Mo	dule	Exit	Module
Extensions	Storage	Certificate	Managers	Extensions	Storage		Certificate M	lanagers
Select extension:				Select extension:				
CRL Distribution Poin	t (CDP)		~	Authority Information	Access (AIA)			~
Specify locations from (CRL). C:\Windows\system: http://cServerDNSN	32\CertSrv\CertEnroll ame>>CertEnroll/ <ca< td=""><td>\<caname><crl< td=""><td>NameSuffix><i< td=""><td>Specify locations from C:\Windows\system3 http://cServerDNSN</td><td>2\CertSrv\CertE</td><td>nroll\<serve< td=""><td>rDNSName SName>_<</td><td>>_<caname< td=""></caname<></td></serve<></td></i<></td></crl<></caname></td></ca<>	\ <caname><crl< td=""><td>NameSuffix><i< td=""><td>Specify locations from C:\Windows\system3 http://cServerDNSN</td><td>2\CertSrv\CertE</td><td>nroll\<serve< td=""><td>rDNSName SName>_<</td><td>>_<caname< td=""></caname<></td></serve<></td></i<></td></crl<></caname>	NameSuffix> <i< td=""><td>Specify locations from C:\Windows\system3 http://cServerDNSN</td><td>2\CertSrv\CertE</td><td>nroll\<serve< td=""><td>rDNSName SName>_<</td><td>>_<caname< td=""></caname<></td></serve<></td></i<>	Specify locations from C:\Windows\system3 http://cServerDNSN	2\CertSrv\CertE	nroll\ <serve< td=""><td>rDNSName SName>_<</td><td>>_<caname< td=""></caname<></td></serve<>	rDNSName SName>_<	>_ <caname< td=""></caname<>
when publishing m include in CRLs. C include in the CDF Publish Delta CRL include in the IDP	 Specifies where to p anually. Itients use this to find extension of issued 	Delta CRL locatio certificates	ns.	Include in the AIA (Include in the onlin Include in the onlin	e certificate stat	us protocol ((DCSP) exter	
ОК	Cancel	Apply	Help	ОК	Canc	el	Apply	Help

Certificate Templates

The next step is about certificate templates.

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

-	wor	k - [Console Root\(Certificate Templates
🚟 File Action View Favorites Window He	lp		
Console Root	Template Display Name	Schema Version	Version
Certificates (Local Computer)	CEP Encryption	1	4.1
Default Domain Policy [adfs.ios.test] Policy	R Code Signing	1	3.1
Certificate Templates (adfs.ios.test)	R Computer	1	5.1
	R Cross Certification Authority	2	105.0
	Directory Email Replication	2	115.0
	🗷 Domain Controller	1	4.1
	Representation Domain Controller Authentication	2	110.0
	I EFS Recovery Agent	1	6.1
	R Enrollment Agent	1	4.1
	R Enrollment Agent (Computer)	1	5.1
	🖳 🗷 Exchange Enrollment Agent (Offline requ	1	4.1
	🖳 Exchange Signature Only	1	6.1
	🖳 Exchange User	1	7.1
	IPSec	1	8.1
	IPSec (Offline request)	1	7.1
	Rerberos Authentication	2	110.0
	🖳 Key Recovery Agent	2	105.0
	OCSP Response Signing	3	101.0
	RAS and IAS Server	2	101.0
	Root Certification Authority	1	5.1
	Router (Offline request)	1	4.1
	R Smartcard Logon	1	6.1
	R Smartcard User	1	11.1
	Representation Authority	1	5.1
	R Trust List Signing	1	3.1
	🚇 User	1	3.1
	🚇 User Signature Only	1	4.1
	🚇 Web Server	1	4.1
	Workstation Authentication	2	101.0

- 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

Web Server Pro	operties	? X
General Request Handling Subject Nam	e Extensions S	ecurity
Group or user names:		
& Authenticated Users		
RETWORK SERVICE		
Domain Admins (IOS\Domain Admins) Domain Computers (IOS\Domain Com		
R Domain Controllers (IOS\Domain Cont		
Admins (IOS\Enterprise Admins (IOS\Enterprise Admins)	mins)	
& IIS_IUSRS (IOS\IIS_IUSRS)		
		-
	Add	Remove
Permissions for Domain Computers	Allow	Deny
Full Control		
Read	✓	
Write		
Enroll	\checkmark	
For special permissions or advanced setting	as. click	Advanced
Advanced.	,	Advanced
OK Cancel	Apply	Help

Default Domain Policy

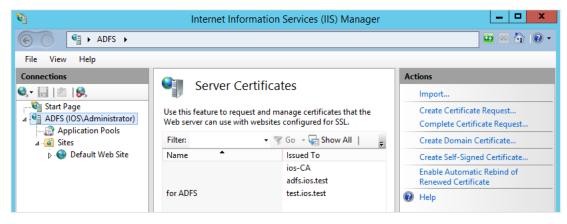
Under Computer Configuration, import the CA certificate to Trusted Root Certifications Authorities.

🚡 work - [Conso	le Root\Default Domain Policy [adfs.ios.test]
🚟 File Action View Favorites Window	Help
🗢 🔿 🙍 🗊 📋 🧟 😹 🚺 📷	
Certificates (Local Computer)	∧ Issued To ▲ Issued By
Default Domain Policy [adfs.ios.test] Policy	ios-CA ios-CA
Computer Configuration Policies	
Software Settings	
⊿ ☐ Windows Settings	
Name Resolution Policy	
Scripts (Startup/Shutdown)	
A here is a security Settings	
Account Policies	
Local Policies	
Event Log	
Restricted Groups	=
System Services	
▷ 📴 Registry ▷ 🔂 File System	
Wired Network (IEEE 802.)	
Windows Firewall with Ac	
📔 Network List Manager Po	
Wireless Network (IEEE 80)	
⊿ 🧰 Public Key Policies	
🚞 Encrypting File System	
Data Protection	
BitLocker Drive Encry	
BitLocker Drive Encry	
Cartificate	
Contracted Root Certifica	
Intermediate Certifica	
Trusted Publishers	
Untrusted Certificates	
🦳 Trusted People	~
< III >	<
Trusted Root Certification Authorities store contains	i 1 certificate.

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.

V j	Internet Information Services (IIS) Manager	_ 🗆 X
📀 💿 VADFS 🔸 Sit	es 🔸 Default Web Site 🔸	🔛 🖂 🟠 🕡 -
File View Help		
Connections Sant Page Sant Page A Application Pools A Sites Default Web Site Type Host Na		
http	80 • 443 • Edit Site Binding ? Type: IP address: Port: https V All Unassigned V 443 Host name: Require Server Name Indication SSL certificate: for ADFS V Select View OK Cancel	
Ready		• <u>1</u> .:

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:

 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 >.

è		Active Directory Federation Services Configuration Wizard	_ 🗆 X
(Connect to Activ	e Directory Domain Services	TARGET SERVER adfs.ios.test
	Welcome Connect to AD DS	Specify an account with Active Directory domain administrator permissions to perform federation service configuration.	orm the
	Specify Service Properties	IOS\Administrator (Current user) Change	
	Specify Service Account		
	Specify Database		
	Pre-requisite Checks		
	Results		
		< Previous Next > Configure	Cancel

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 >.

la 4	Active Directory Federation Servic	ces Configuration Wizard 📃 🗖 🗙
Specify Service P	roperties	TARGET SERVER adfs.ios.test
Welcome Connect to AD DS Specify Service Properties	SSL Certificate:	adfs.ios.test view
Specify Service Account Specify Database	Federation Service Name:	adfs.ios.test <i>Example: fs.contoso.com</i>
Review Options Pre-requisite Checks Installation	Federation Service Display Name:	ADFS Test Lab Users will see the display name at sign in. Example: Contoso Corporation
Results		
	<	Previous Next > Configure Cancel



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

Note: This account should require no special permissions.

b	Active Directory Federation	Services Configuration Wiz	ard 📃	D X
Specify Service A	ACCOUNT	the KDS Root Key has not been s	adfs	SERVER s.ios.test
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Create a Group Managed S Account Name:	t or group Managed Service Acco Service Account IOS\ er account or group Managed Ser IOS\adminaccount		.t
		< Previous Next >	Configure	ancel

- **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.

la /	Active Directory Federation Services	Configuration Wizard	_ D X
Image: Specify Configuration Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options	ation Database	irectory Federation Service configuration of Ig Windows Internal Database.	TARGET SERVER adfs.ios.test
Pre-requisite Checks Installation Results	Database Instance:	To use the default instance, leave this field	d blank.
	< Pr	evious Next > Configure	Cancel

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

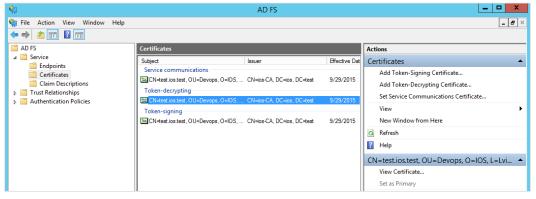
To ensure that you have properly installed **AD FS**, check the following settings in **AD FS Management**:

• 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**.

御			AD FS			_ D X
🙀 File Action View Window Help						_ 8
🗢 🔿 🔁 🖬 🛛 🖬						
📔 AD FS	Endpoints				Act	ions
⊿ 🧮 Service	Enabled	Proxy Enabled	URL Path	Type \land	En	dpoints ·
Endpoints	No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledes	WS-Trus	-	View
Certificates	No	No	/adrs/services/trust/2005/issuedtokensymmetrictripledes /adfs/services/trust/2005/issuedtokensymmetrictripledess	WS-Trus WS-Trus		View
Claim Descriptions	No	No	/adis/services/trust/2005/issuedtokensymmetrictriple	WS-Trus	L	New Window from Here
Trust Relationships	No	No	/adis/services/trust/2005/issuedtokenmixedsymmetrictripl	WS-Trus WS-Trus	a	Refresh
Authentication Policies	Yes	No	/adis/services/trust/2005/issuedtokenmixedsymmetricitipi /adis/services/trust/13/kerberosmixed	WS-Trus WS-Trus	-	
	No	No	/adfs/services/trust/13/certificate	WS-Trus	?	Help
	Yes	Yes	/adis/services/trust/13/certificatemixed	WS-Trus	12	dfs/services/trust/mex
	No	No	/adis/services/trust/13/certificatetransport	WS-Trus	1	
	No	No	/adis/services/trust/13/usemame	WS-Trus	L	Enable on Proxy
	No	No	/adis/services/trust/13/usemamebasictransport	WS-Trus		Disable
	Yes	Yes	/adfs/services/trust/13/usemamemixed	WS-Trus	?	Help
	No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trus ≡		
	No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sh	WS-Trus	L	
	Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic	WS-Trus	L	
	No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic	WS-Trus	L	
	Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2	WS-Trus	L	
	No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2	WS-Trus		
	No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trus	L	
	No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256sha	WS-Trus	L	
	No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trus		
	No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha	WS-Trus		
	No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trus		
	No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripled	WS-True Y		
	<		ш	>		

• 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: <u>http://ip-your-adfs-server/certsrv</u>.

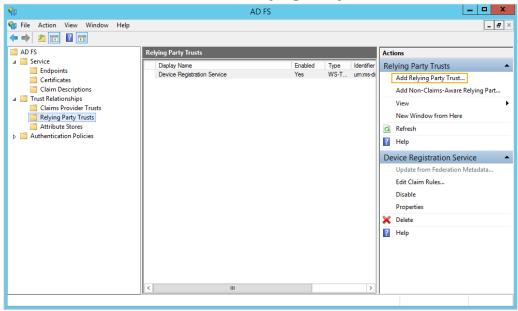
Once obtained, follow the next steps:

- 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.

\$	Add Relying Party Trust Wizard
Welcome	
Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard. </th

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

\$	Add Relying Party Trust Wizard
Select Data Source	
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	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: @ Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

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

\$	Add Relying Party Trust Wizard	×
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Envi	
Specify Display Name	Notes:	
Choose Profile		^
Configure Certificate		
Configure URL		
Configure Identifiers		
Configure Multi-factor Authentication Now?		~
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
Finish		
	< Previous Next > Can	el

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

\$	Add Relying Party Trust Wizard
Choose Profile	
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	This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust. AD FS profile This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol. AD FS 1.0 and 1.1 profile This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1. AD FS 1.0 and 1.1 profile This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1. AD FS 1.0 and 1.2 profile This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

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.

\$ #	Add Relying Party Trust Wizard	x
Configure Certificate		
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure URL Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse Issuer: CN=ios-ADFS-CA, DC=ios, DC=test Subject: CN=adfs ios.test, OU=Devops, O=IOS, L=Lviv, S=Lviv, C=UA Effective date: 9/28/2015 2:41:23 PM Expiration date: 9/27/2017 2:41:23 PM View Browse	
	< Previous Next > Cancel	

- 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 >**.

\$ #	Add Relying Party Trust Wizard
Configure URL	
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	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-Federation Passive 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 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://www.envi.net Example: https://www.contoso.com/adfs/ls/
	< Previous Next > Cancel

- 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.

\$	Add Relying Party Trust Wizard	x
Configure Identifiers		
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers t	for this relvina
Welcome	party trust.	
Select Data Source	Relying party trust identifier:	
Specify Display Name		Add
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust	
Configure Certificate	Relying party trust identifiers:	
Configure URL	https://www.envi.net	Remove
Configure Identifiers		
Configure Multifactor Authentication Now?		
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
Finish		
	< Previous Next >	Cancel

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** >.

\$	Add Relying Party Trust Wizard
Steps	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if
Welcome	there is a match for any of the specified requirements.
Select Data Source	
Specify Display Name	Multifactor Authentication Global Settings
Choose Profile	Requirements Users/Groups Not configured
Configure Certificate	Device Not configured
Configure URL	Location Not configured
Configure Identifiers	
Configure Multi-factor Authentication Now?	
 Choose Issuance Authorization Rules 	
 Ready to Add Trust Finish 	 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 <u>Configuring Authentication Policies</u>.
	< Previous Next > Cancel

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

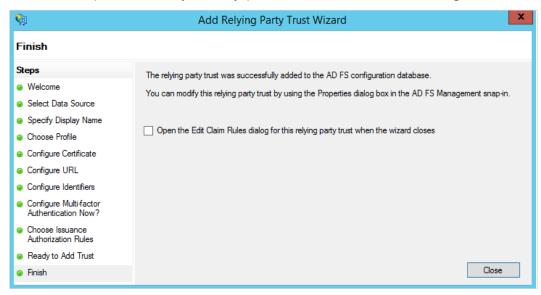


12. On the **Ready to Add Trust** page, only select **Next** >.

\$	Add Relying Party Trust Wizard	x
Ready to Add Trust		
Steps Velcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Identifiers Configure Multifactor 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 Note Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL: Image: Configuration of the configuration	
	< Previous Next > Cancel	

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 <u>AD FS Configuration</u> section).

USERNAME	username
PASSWORD	
ENDPOINT URL	https://www.envi.net/adfs/services/trust/13/usernamemixed
IDENTIFIER URL	https://www.envi.net
	AUTHENTICATE

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.

