VMware Identity Manager Integration with Active Directory Federation Services

VMware Identity Manager

MAY 2018 V4

Table of Contents

Introduction

Active Directory Federation Services (AD FS) is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries.

You can configure the VMware Identity Manager service to use Active Directory Federation Service (AD FS) as the third-party identity provider instance for authentication.

Active Directory Federation Services

AD FS uses a claims-based access control authorization model to maintain application security and implement federated identity.

Claims-based authentication is the process of authenticating users based on a set of claims about their identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate users by other means and is trusted by the entity doing the claims-based authentication.

The following table shows the parallels between VMware Identity Manager and Microsoft technologies.

ADFS	SAML	DESCRIPTION
Security Token	Assertion	Collection of XML-formatted security information describing users, which is created and consumed during a federated access request.
Claim Provider	Identity Provider (IdP)	Partner in a federation that creates security tokens for users
Relying Party	Service Provider (SP)	Partner in a federation that consumes security tokens for providing access to applications
Claims	Assertion Attributes	Data about users that is sent inside security tokens

Configuring AD FS Instance in VMware Identity Manager

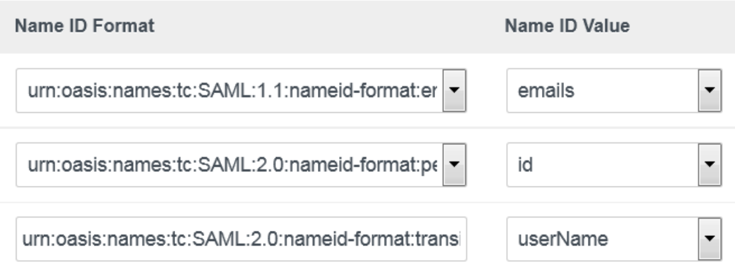
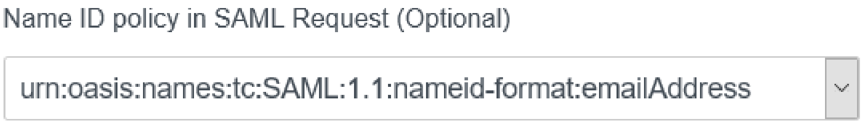
You can configure the service to use AD FS as the third-party identity provider instance for authentication. Complete the following tasks prior to using the administration console to add the identity provider instance.

Prerequisites

- Obtain the AD FS metadata information to add when you configure the identity provider in the VMware Identity Manager administration console. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata. The URL to this metadata is https://adfs.yourdomain.com/FederationMetadata/2007-06/FederationMetadata.xml.
- In the administration console, configure the network ranges that you want to direct to this identity provider instance for authentication. Network Ranges are configured in the Policies section. Go to the Identity & Access Management tab and select **Manage Policies**. For more information about adding network ranges, see the VMware Identity Manager Administration Guide.

Add and Configure AD FS in the Service

1. Log in to the VMware Identity Manager console.
2. In the Identity & Access Management tab, select **Manage > Identity Providers**.
3. Click **Add Identity Provider** and select Create Third Party IDP.
4. Edit the form settings.

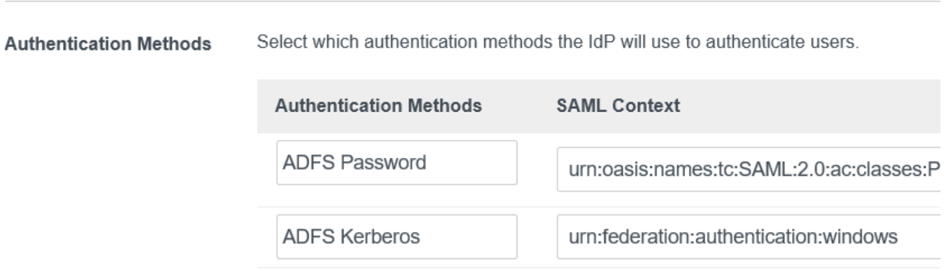
FORM ITEM	DESCRIPTION
Identity Provider Name	Enter a name for this identity provider instance.
SAML Metadata	a. Add the AD FS metadata here. Enter the URL or the xml content of the Federation metadata from the AD FS server to establish trust with the identity provider. b. Click **Process IdP Metadata**. The ID format mapping from the SAML response displays.  Name ID Format — Name ID Value urn:oasis:names:tc:SAML:1.1:nameid-format:er — emails urn:oasis:names:tc:SAML:2.0:nameid-format:pe — id urn:oasis:names:tc:SAML:2.0:nameid-format:trans — userName c. Make sure that the user values in the service are mapped for the ID formats displayed. You can add custom third-party name ID formats and map them to the user values in the service. d. (Optional) Select the NameIDPolicy response identifier string format. The format is usually **unspecified** or **emailAddress**. You create a relying party custom claim rule in AD FS to transform the string. Make sure that the NameIDPolicy format matches the claim rule configured in AD FS.  Name ID policy in SAML Request (Optional) urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Just-in-Time User Provisioning	Do not enable.
Users	Select the VMware Identity Manager directories of the users that can authenticate using this identity provider.
Network	The existing network ranges configured in the service are listed. Select the network ranges for the users, based on their IP addresses, that you want to direct to this identity provider instance for authentication.

Authentication Methods

Add the authentication methods that your AD FS installation supports.

Select the SAML authentication context class that supports the authentication method.

When Kerberos authentication is used, configure to authenticate using both Kerberos and password authentication methods. Configure the SAML authentication context classes **urn:oasis:names:tc:SAML:2.0:ac:classes:Password** and **urn:federation:authentication:windows**.



Authentication Methods — Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	SAML Context
ADFS Password	urn:oasis:names:tc:SAML:2.0:ac:classes:P
ADFS Kerberos	urn:federation:authentication:windows

You create rules in access policies to manage authentication. Create a rule to use AD FS Kerberos authentication first and fall back to AD FS password authentication, if necessary.

When the SAML context urn:oasis:names:tc:SAML:2.0:ac:classes:Password is configured, AD FS prompts for the user name and password at every sign-in request.

When the SAML context urn:federation:authentication:windows is configured, AD FS prompts for Kerberos authentication before prompting for the user name and password.

Single Sign-Out Configuration

Optional. Enable single sign-out to log users out of their IdP session after they sign out from their apps portal.

SAML Signing Certificate

Click **Service Provider (SP) Metadata** to see URL to VMware Identity Manager SAML service provider metadata URL . Copy and save the URL. This URL is configured when you edit the Federation Service Properties in AD FS to map to the VMware Identity Manager service.

5. Click **Add**.

What to do next

In the Identity and Access Management tab Manage > Policies page, configure the VMware Identity Manager default access policy rule to include the authentication methods you configured for the AD FS identity provider. If you configured Kerberos authentication, make sure that Kerberos authentication is the first authentication method listed in the policy rule.

Configuring Just-in-Time Provisioning for AD FS in the Service

Just-in-time user provisioning lets you create users in the VMware Identity Manager service dynamically when a user signs in, using SAML assertions sent by a third-party identity provider.

Prerequisites

- When you are configuring AD FS for just-in-time user provisioning with the VMware Identity Manager service, review the user attribute settings on the service.
- Create Local Groups in the service

See the Just-in-Time Provisioning chapter in the VMware Identity Manager Administration Guide.

Review Attributes Used for SAML Assertion

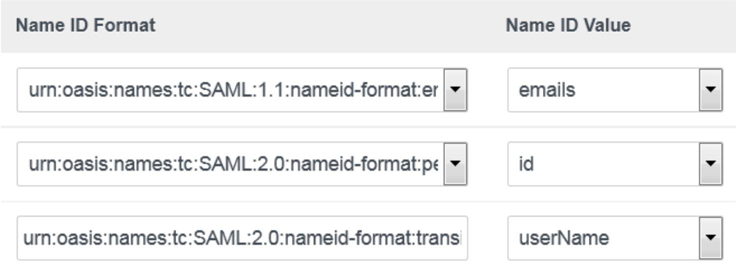
When users are provisioned through just-in-time provisioning, the SAML assertion is used to create the user. Only those attributes in the SAML assertion that match the attributes listed in the VMware Identity Manager User Attributes page are used.

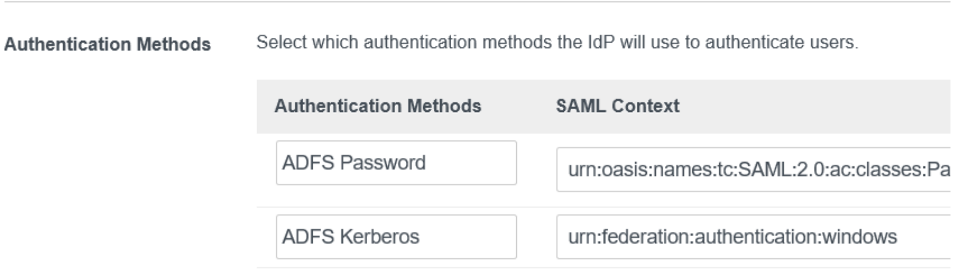
- The SAML assertion must include the **userName** attribute.
- The SAML assertion must include all the user attributes that are marked as required in the VMware Identity Manager service.

  To view or edit the user attributes in the administration console, in the **Identity & Access Management** tab, click **Setup** and then click **User Attributes**.
- If you configure multiple domain for the just-in-time directory, the SAML assertion must include the **domain** attribute. The value of the attribute must match one of the domains configured for the directory. If the value does not match or a domain is not specified, login fails.

Add and Configure ADFS in VMware Identity Manager

1. Log in to the VMware Identity Manager console.
2. In the Identity & Access Management tab, select **Manage > Identity Providers**.
3. Click **Add Identity Provider** and select Create Third Party IDP.
4. Edit the form settings.

FORM ITEM	DESCRIPTION
Identity Provider Name	Enter a name for this identity provider instance.
SAML Metadata	a. Enter the URL or the xml content of the Federation metadata from the AD FS server to establish trust with the identity provider. Configure the SAML assertion mapping. b. Click **Process IdP Metadata**. The ID format mapping from the SAML response displays.  Name ID Format — Name ID Value urn:oasis:names:tc:SAML:1.1:nameid-format:er — emails urn:oasis:names:tc:SAML:2.0:nameid-format:pe — id urn:oasis:names:tc:SAML:2.0:nameid-format:trans — userName c. Add the following Name ID Format attribute, **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified.** The Name ID Value should be **userName**. Make sure that the user values in the service are mapped for the ID formats displayed.
Just-in-Time User	Enable just-in-time provisioning.

Provisioning	Enter the JIT directory name you created in the service and the JIT user domains.
Users	Select the VMware Identity Manager directories of the users that can authenticate using this identity provider.
Network	The existing network ranges configured in the service are listed. Select the network ranges for the users, based on their IP addresses, that you want to direct to this identity provider instance for authentication.
Authentication Methods	Add the authentication methods that your AD FS installation supports. Select the SAML authentication context class that supports the authentication method. When Kerberos authentication is use, configure to authenticate using both Kerberos and password authentication methods. Configure the SAML authentication context classes **urn:oasis:names:tc:SAML:2.0:ac:classes:Password** and **urn:federation:authentication:windows**.  Authentication Methods Select which authentication methods the IdP will use to authenticate users. Authentication Methods — SAML Context ADFS Password — urn:oasis:names:tc:SAML:2.0:ac:classes:Pa ADFS Kerberos — urn:federation:authentication:windows You create rules in access policies to manage authentication. When the SAML context urn:oasis:names:tc:SAML:2.0:ac:classes:Password is configured, AD FS prompts for the user name and password at every sign-in request. When the SAML context urn:federation:authentication:windows is configured, AD FS prompts for Kerberos authentication before prompting for the user name and password.
Single Sign-Out Configuration	Optional. Enable single sign-out to log users out of their IdP session after they sign out from their apps portal.
SAML Signing Certificate	Click **Service Provider (SP) Metadata** to see the metadata xml file. for the VMware Identity Manager SAML service provider. Copy and save the URL. This URL is configured when you edit the Federation Service Properties in AD FS to map to the VMware Identity Manager service.

5. Click **Add**.

What to do next

In the Identity and Access Management tab Manage > Policies page, configure the VMware Identity Manager default access policy rule to include authentication methods you configured for the AD FS identity provider. If you configured Kerberos authentication, make sure that Kerberos authentication is the first authentication method listed in the policy rule.

Add Authentication Methods to Policy Rules

The authentication methods you added when you configured the AD FS identity provider instance must be added to the default policy rules.

1. In the administration console Identity & Access Management tab, select **Manage > Policies**.
2. Click the default access policy set to open the policy page to edit.
3. In the **Policy Rules** section, select the rule to edit or add a new rule.
4. Complete the form. To configure the authentication order, in the **then the user must authenticate using the following method** drop down menu, select the AD FS authentication method to apply first. If you configured both Kerberos and password authentication, select the Kerberos authentication method as the first method to use.
5. If you configured other authentication method, continue to select them in the order they should be applied.
6. Click **Save** and click **Save** again on the Policy page.

Integrating VMware Identity Manager Service with AD FS 3.0

Configure the AD FS third-party identity provider instance by applying the SAML information from the VMware Identity Manager service.

You must be an administrator on your Active Directory server.

Note: This guide does not go into detail about how to properly set up AD FS in the best possible scenario. The directions in this guide assume that AD FS is already correctly configured. This guide can be used to quickly get an AD FS instance up and running for testing purposes only.

Configure AD FS 3.0

After AD FS is installed, you configure the AD FS server and create the identity provider Security Token Service. The AD FS Configuration Wizard walks you through the steps to configure AD FS.

1. Log in to the AD FS server and open the management console.
2. Navigate to the Federation Service Properties page and in the General tab, confirm that the DNS entries and certificate names match. Note the Federation Service Identifier value. This is used in the VMware Identity Manager configuration.
3. Browse to the certificates page and export the Token-Signing certificate. Make sure that **No, do not export the private key** is selected. Select to export the file as **DER encoded binary x.509 (.cer)**. This certificate must be in the PEM format for VMware Identity Manager. Convert the certificate to PEM format using client tools.

Configure AD FS Relying Party Trust

After the configuration is complete, you add a relying party trust to the AD FS configuration database. The relying party trust defines how the Federation Service recognizes the relying party and issues claims to it.

1. Open the AD FS Management console and select to **Relying Party Trusts**.
2. Select **Add a Relying Party Trust**. In the Add Wizard page, click **Start** to begin.
3. Use the **Import File** option to import the VMware Identity Provider service provider metadata XML file that you copied and saved previously. See the *Obtain the VMware Identity Manager Service Provider Metadata Fil*e section in this guide.
4. Enter a name for the VMware Identity Manager service and in the **Notes** text box, type a description of this relying party trust.
5. Select **AD FS 3.0 Profile**.

   IMPORTANT

   - Do not select a token encryption certificate. The profile uses the certificate that is defined on the VMware Identity Manager service.
   - Do not enable any settings on the Configure URL.
6. Enter the service site name to which you connected as the **Relying party trust identifier**. For example https://myco.vmwareidentitymgr.com.
7. If you are using multi-factor authentication, select the settings for this relying party trust and follow the additional steps in the wizard. **Note**: Using multi-factor authentication is beyond the scope of this guide.

8. Configure the Claim Issuance Authorization Rules. Select **Permit all users to access this relying party**.
9. In the Finish page, clear the **Open the Claims when this finishes** check box.

   When you close this page, the Edit Claim Rules dialog box appears.

Create AD FS Relying Party Claim Rules

Once the relying party trust is created, you create the claim rules configure what to pass to VMware Identity Manager in the SAML.

Only one custom rule is configured. Below are examples of how to configure either an email claim rule or a user name claim rule

Create AD FS Relying Party Email Claim Rules

1. If the Rules Editor appears, **click Add Rule**. Otherwise, in the Relying Party Trusts list, right-click the relying party you just created and click **Edit Claims Rules**.
2. In the Issuance Transform Rules tab, click **Add Rule** and select **Send LDAP Attributes as Claims** as the template. Click **Next**.

   This template is used to create a rule that selects attributes from an LDAP attribute store to send as claims to the relying party.
3. In the Configure Rule page, enter the claim rule name as **Get Attributes**. This rule pulls user attributes from the LDAP.
   a. For Attribute store, select **Active Directory**.
   b. In the Mapping of LDAP attributes to outgoing claim types section, select the LDAP attribute **E-Mail Addresses** and the Outgoing Claim Type, **E-Mail Address**.
4. Click **Finish**. Click **OK** to save the new rule.

Add Custom Rule to Transform Email Addresses Format

Create a custom rule to transforms the email address attribute that is retrieved from LDAP in the Get Attributes rule into the desired SAML format. The custom rule uses the AD FS claim rule language.

1. In the Edit Claim Rules page, click **Add Rule** and select **Send Claims Using a Custom Rule** as the template. Click **Next**.
2. Enter the **claim rule name**. For example, GetAttributes Email Transform .
3. Click **View Rule Language**, to edit the existing rule.
4. Replace the existing rule that displays with the rule listed below. Change the **spnamequalifier** field to match your VMware Identity Manager installation.

```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/for
mat"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spn
amequalifier"] = "yourcompany.vmwareidentity.com");
```

5. Click **Finish**.

Create AD FS Relying Party Username Claim Rule

To pass the user name to VMware Identity Manager in the SAML, configure this claim rule and add the custom rule.

1. Right-click the relying party you created and click **Edit Claims Rules**.
2. In the Issuance Transform Rules tab, click **Add Rule** and select **Send LDAP Attributes as Claims** as the template. Click **Next**.

   This template is used to create a rule that selects attributes from an LDAP attribute store to send as claims to the relying party.
3. Add the rule you created, for example Get Attributes. This rule pulls user attributes from the LDAP.
   a. For Attribute store, select **Active Directory**.
   b. In the Mapping of LDAP attributes to outgoing claim types section, select the LDAP attributes **SAM Account Name** and the Outgoing Claim Type **E-Mail Address**.
4. Click **Finish**.
5. In the **Edit Rule – Default Claims** page, before you click **OK**, you can click View Rule Language to see the parameters for the rule you just created.

   An example follows.

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountn
ame", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory",
types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
query = ";sAMAccountName;{0}", param = c.Value);
```

Add Custom Rule to Transform User Name Attribute Format

Create a custom rule to transforms the SAM Account Name attribute that is retrieved from LDAP in the Get Attributes rule into the desired SAML format. The custom rule uses the AD FS claim rule language.

1. Click **Add Rule** and select **Send Claims Using a Custom Rule** as the template. Click **Next**.
2. Enter the **Claim rule name**. For example, enter **Get Attributes SAMAccountName Transform**.
3. Replace the existing rule that displays with the rule listed below. Change the **spnamequalifier** field to match your VMware Identity Manager installation.

```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperti
es/format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperti
es/spnamequalifier"] = "yourcompany.vmwareidentity.com");
```

4. Click **Finish** to save the rule.

Integrating VMware Identity Manager Service with AD FS 2.0

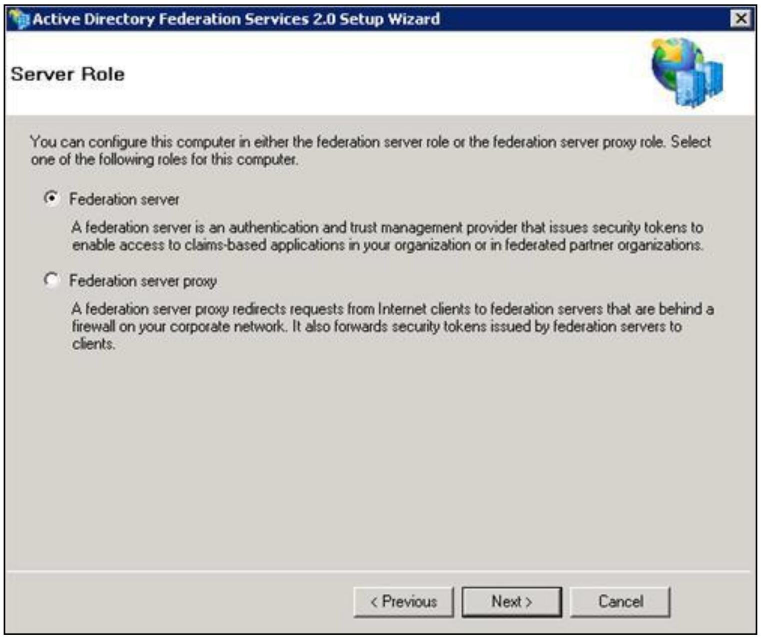
Configure the third-party identity provider instance by applying the SAML information from the VMware Identity Manager service.

You must be an administrator on your Active Directory server.

Installing AD FS

Note: This guide does not go into detail about how to properly set up AD FS in the best possible scenario. The directions in this guide assume that AD FS is already correctly configured. This guide can be used to quickly get an AD FS instance up and running for testing purposes only.

1. Download the AD FS 2.0 executable file to your computer.
2. Open the AdfsSetup.exe file to start the AD FS installation wizard.
3. On the Server Role dialog box, select Federation Server and click **Next**.



You can configure this computer in either the federation server role or the federation server proxy role. Select one of the following roles for this computer.

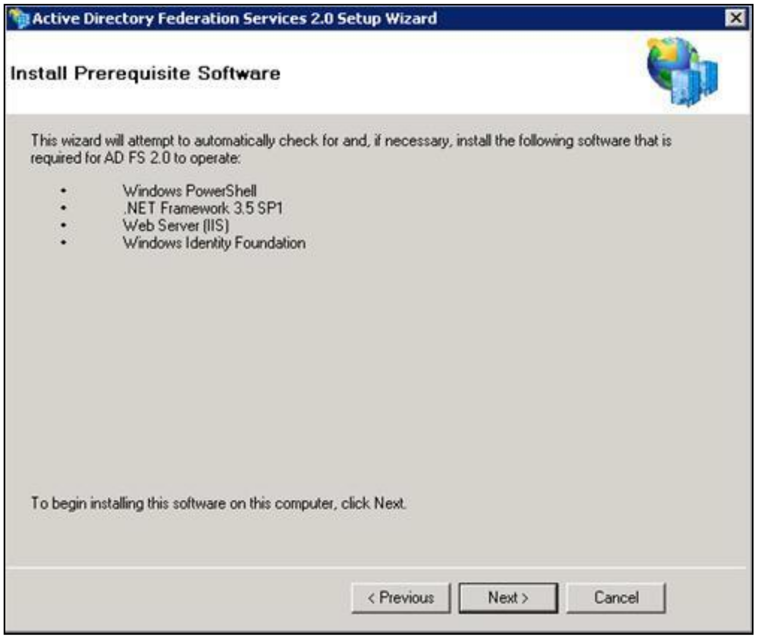
● Federation server

A federation server is an authentication and trust management provider that issues security tokens to enable access to claims-based applications in your organization or in federated partner organizations.

○ Federation server proxy

A federation server proxy redirects requests from Internet clients to federation servers that are behind a firewall on your corporate network. It also forwards security tokens issued by federation servers to clients.

4. On the Install Prerequisite Software dialog box, click **Next** to install the required prerequisites.



Active Directory Federation Services 2.0 Setup Wizard

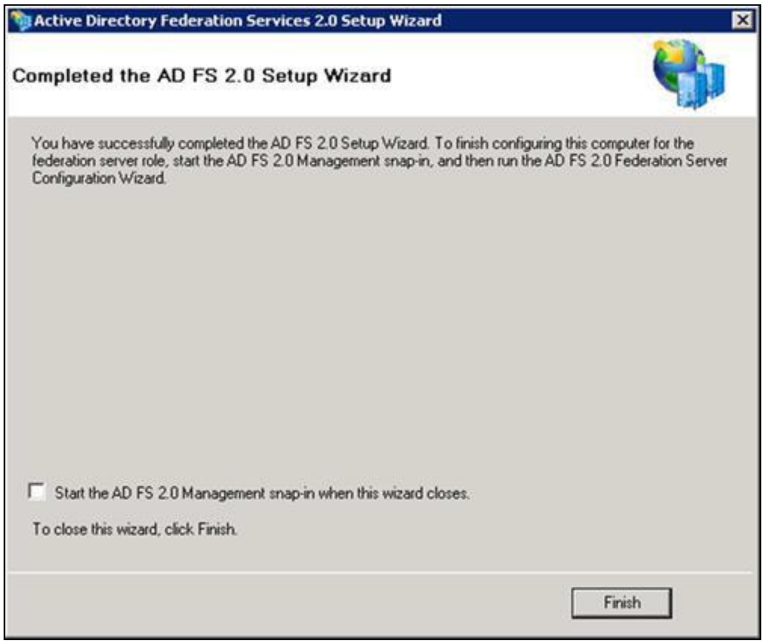
Install Prerequisite Software

This wizard will attempt to automatically check for and, if necessary, install the following software that is required for AD FS 2.0 to operate:

- Windows PowerShell
- .NET Framework 3.5 SP1
- Web Server (IIS)
- Windows Identity Foundation

To begin installing this software on this computer, click Next.

5. On the completed the AD FS2.0 Setup Wizard dialog box, check **Start the AD FS 20 Management snap-in when this wizard closes** and click **Finish**.



Active Directory Federation Services 2.0 Setup Wizard

Completed the AD FS 2.0 Setup Wizard

You have successfully completed the AD FS 2.0 Setup Wizard. To finish configuring this computer for the federation server role, start the AD FS 2.0 Management snap-in, and then run the AD FS 2.0 Federation Server Configuration Wizard.

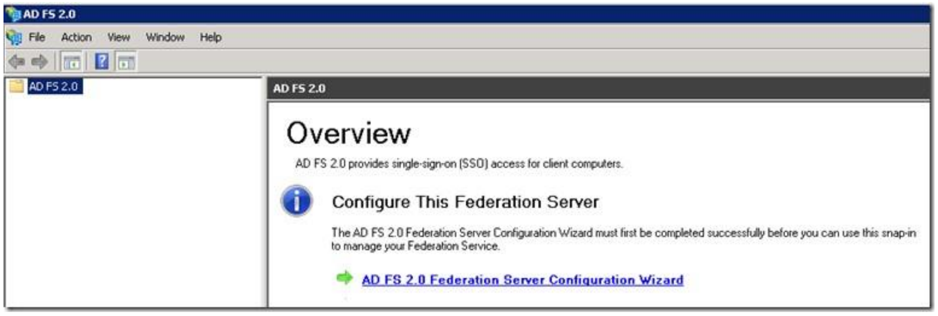
□ Start the AD FS 2.0 Management snap-in when this wizard closes.

To close this wizard, click Finish.

Configure AD FS

When the installation is complete, the AD FS 2.0 management page should open. If it does not open, go to Start > Administrative Tools > AD FS 2.0 Management.

1. In the Overview page, click AD FS 2.0 Federation Server Configuration Wizard.



Overview

AD FS 2.0 provides single-sign-on (SSO) access for client computers.

Configure This Federation Server

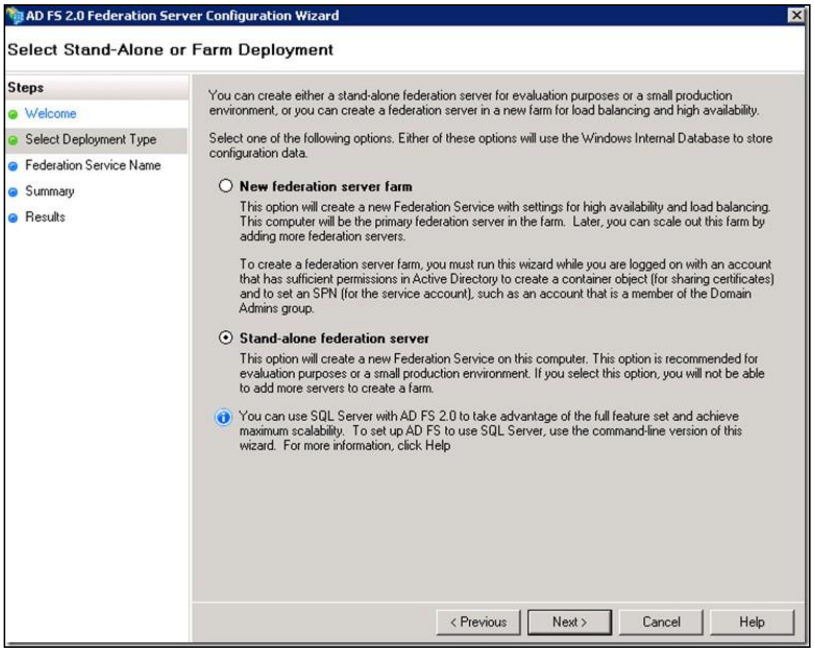
The AD FS 2.0 Federation Server Configuration Wizard must first be completed successfully before you can use this snap-in to manage your Federation Service.

AD FS 2.0 Federation Server Configuration Wizard

2. To configure a new AD FS server, select **Create a New Federal Service** and click **Next**.

3. In the Select Stand-Alone or Farm Deployment dialog box, select Stand-alone federation server.

This option is for testing and evaluation purposes. This option does not provide for high availability and load balancing.



Select Stand-Alone or Farm Deployment

You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability.

Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.

○ New federation server farm

This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers.

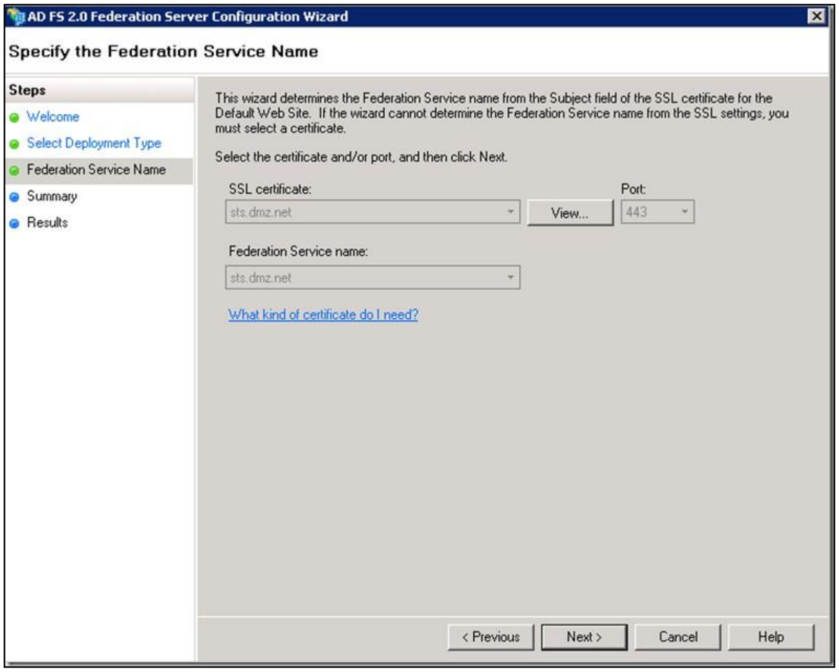
To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group.

● Stand-alone federation server

This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.

You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help

4. Specify the Federation Service name. The configuration wizard retrieves the SSL certificate bound to the Default Web Site in IIS and uses the subject name specified there. If you use a wildcard certificate, you must enter the Federation Service name.



Specify the Federation Service Name

This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate.

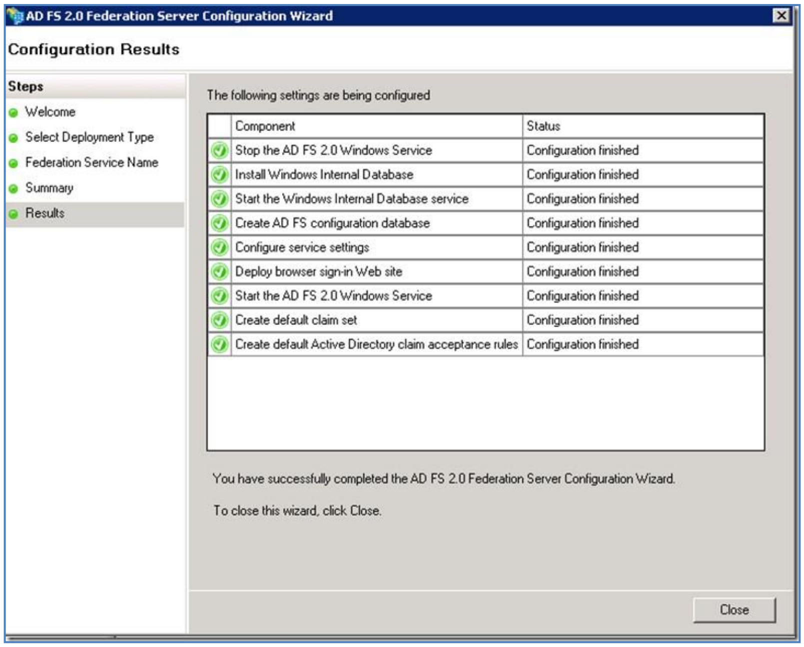
Select the certificate and/or port, and then click Next.

SSL certificate: sts.dmz.net

Port: 443

Federation Service name: sts.dmz.net

5. Continue through the configuration wizard and click **Close** when complete.



Configuration Results

The following settings are being configured

	Component	Status
✓	Stop the AD FS 2.0 Windows Service	Configuration finished
✓	Install Windows Internal Database	Configuration finished
✓	Start the Windows Internal Database service	Configuration finished
✓	Create AD FS configuration database	Configuration finished
✓	Configure service settings	Configuration finished
✓	Deploy browser sign-in Web site	Configuration finished
✓	Start the AD FS 2.0 Windows Service	Configuration finished
✓	Create default claim set	Configuration finished
✓	Create default Active Directory claim acceptance rules	Configuration finished

You have successfully completed the AD FS 2.0 Federation Server Configuration Wizard.

To close this wizard, click Close.

Now you can use the AD FS to build trust relationships with claims-aware applications and with federated partners.

What to do next

- In the AD FS management console, configure the Relying Party Trust
- Configure the Relying Party Claims Rules

See Configure AD FS Relying Party Trust section.

Troubleshooting

How to log in

Problem

When VMware Identity Manager is not configured correctly, you might not be able to log in from the log in page.

Solution

To log in as the local admin user, add ?login after the login URL. Enter as

`https://<tenant>.vmwareidentity.com/SAAS/auth/login?login`

Error: Cannot update Identity Provider

Problem

After editing the Identity Provider to add or update an authentication method, you see the error Cannot update Identity Provider. When adding or updating a SAML context rule, the SAML context name has to be unique in your VMware Identity Manager tenant. Authentication methods in the IdP are not deleted when you click on Save.

Solution

Provide a new authentication method name. This name must be unique in your tenant.

Note: Authentication methods you add here can be deleted only through the REST API. To avoid issues with too many unorganized auth methods, use a consistent naming convention to remember the last authentication method you created. For example, use a date in the auth method name, **Password092116.**

Error: Contact your administrator

Problem

When AD FS is configured with the VMware Identity Manager signing certificate URL, the xml file is downloaded for every user log in request. If the XML download fails once, this blocks further log in attempts and breaks the IDP integration. .

Cause

When integrating with AD FS, the VMware Identity Manager signing certificate URL was specified as a URL or as XML information.

Solution

Download the XML file and copy and paste the content into the appropriate AD FS certificate page.

Error: 404.idp.not.found

Problem

When testing, the name of the authentication method is not removed from an access policy rule when changing the rule's configuration. This error occurs when the policy selects an old authentication method, an auth method of a disabled IdP, or the AirWatch Cloud Connection password authentication method is selected but not enabled in VMware Identity Manager, AirWatch pages..

Solution

In the access policy rule, select an authentication method which is active and current.

Resources

- VMware Identity Manager documentation
- VMware Identity Manager audit events reports. This report lists the events related to user logins, including which authentication method was used to log in. You can run this report from the VMware Identity Manager admin console Dashboard. In the User section, click **See Full Report**.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com