VMware Identity Manager Integration with Active Directory Federation Services

VMware Identity Manager

NOVEMBER 2016  V3
# Table of Contents

Introduction ....................................................................................................................................... 2  
Active Directory Federation Services ............................................................................................... 2  
Configuring AD FS Instance in VMware Identity Manager ............................................................... 2  
  Add and Configure AD FS in the Service .................................................................................... 3  
  Configuring Just-in-Time Provisioning for AD FS in the Service ................................................. 4  
    Review Attributes Used for SAML Assertion ......................................................................... 4  
    Add and Configure ADFS in VMware Identity Manager ................................................... 4  
  Add Authentication Methods to Policy Rules ........................................................................... 6  
Integrating VMware Identity Manager Service with AD FS 3.0 ........................................................ 7  
  Configure AD FS 3.0 ................................................................................................................ 7  
  Configure AD FS Relying Party Trust .................................................................................... 7  
  Create AD FS Relying Party Email Claim Rules .................................................................. 8  
    Add Custom Rule to Transform Email Addresses Format .............................................. 8  
    Create AD FS Relying Party Username Claim Rule ......................................................... 9  
    Add Custom Rule to Transform User Name Attribute Format ...................................... 9  
Integrating VMware Identity Manager Service with AD FS 2.0 ...................................................... 10  
  Installing AD FS ................................................................................................................ 10  
  Configure AD FS ................................................................................................................ 11  
Troubleshooting .............................................................................................................................. 14  
  How to log in ...................................................................................................................... 14  
  Error: Cannot update Identity Provider ............................................................................. 14  
  Error: Contact your administrator ..................................................................................... 14  
  Error: 404.idp.not.found ................................................................................................... 14  
Resources .................................................................................................................................. 15
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.

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

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-part 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. Go to the Identity & Access Management tab and select Setup > Network Ranges. 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 administration console.
2. In the Identity & Access Management tab, select Manage > Identity Providers.
3. Click Add Identity Provider and edit the form settings.

<table>
<thead>
<tr>
<th>FORM ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider Name</td>
<td>Enter a name for this identity provider instance.</td>
</tr>
</tbody>
</table>

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.
- b. Click Process IdP Metadata. The ID format mapping from the SAML response displays.

<table>
<thead>
<tr>
<th>Name ID Format</th>
<th>Name ID Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:oasis:names:tc:SAML:1.1:nameid-format:email</td>
<td>emails</td>
</tr>
<tr>
<td>urn:oasis:names:tc:SAML:2.0:nameid-format:pi</td>
<td>id</td>
</tr>
<tr>
<td>urn:oasis:names:tc:SAML:2.0:nameid-format:trans</td>
<td>userName</td>
</tr>
</tbody>
</table>

- 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.

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.

To authenticate using both Kerberos and password authentication methods, configure the SAML authentication context classes

To configure urn:federation:authentication:windows, in the SAML Context drop-down menu, scroll to the end of the list and select Add a new SAML Context.... Type urn:federation:authentication:windows in the text box.

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
VMware Identity Manager Integration with Active Directory Federation Services

configured, AD FS prompts for Kerberos authentication before prompting for the user name and password.

<table>
<thead>
<tr>
<th>Single Sign-Out Configuration</th>
<th>Optional. Enable single sign-out to log users out of their IdP session after they sign out from their apps portal.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Signing Certificate</td>
<td>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.</td>
</tr>
</tbody>
</table>

4. 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.

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 administration console.
2. In the Identity & Access Management tab, select Manage > Identity Providers.
3. Click Add Identity Provider and edit the form settings.
VMware Identity Manager Integration with Active Directory Federation Services

<table>
<thead>
<tr>
<th>FORM ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider Name</td>
<td>Enter a name for this identity provider instance.</td>
</tr>
</tbody>
</table>
| 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.  
   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 Provisioning     | Enable just-in-time 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 AD FS authentication method.  
   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**.  
   To configure **urn:federation:authentication:windows**, in the SAML Context drop-down menu, scroll to the end of the list and select Add a new SAML Context.... Type **urn:federation:authentication:windows** in the text box.  
   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. |
<table>
<thead>
<tr>
<th>Single Sign-Out Configuration</th>
<th>Optional. Enable single sign-out to log users out of their IdP session after they sign out from their apps portal.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Signing Certificate</td>
<td>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.</td>
</tr>
</tbody>
</table>

4. 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 as the 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 configure another 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 File 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 Email Claim Rules**

Once the relying party trust is created, you create the claim rules and update the relying party trust with minor changes not set up by the wizard. To configure what to pass to VMware Identity Manager in the SAML, you add 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,

5. Click **Finish**.
Create AD FS Relying Party Username Claim Rule

Configure a second claim rule to pass the user name to VMware Identity Manager in the SAML.

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.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 = 
```

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

**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.
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.

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

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


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, thexml 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.