Integrating VMware Workspace ONE with Active Directory Federation Services

MAY 2019
VMware Identity Manager
You can find the most up-to-date technical documentation on the VMware website at:
https://docs.vmware.com/
If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
Integrating VMware Workspace ONE with Active Directory Federation Services

*Integrating VMware Workspace ONE with Active Directory Federation Services* provides information about integrating Active Directory Federation Services with VMware Workspace™ ONE™. It describes specific use cases and provides instructions on how to configure Workspace ONE and Active Directory Federation Services to support those use cases.

**Intended Audience**

This information is intended for IT system administrators configuring Workspace ONE in an existing Active Directory Federation Services environment.

**Additional Information**

- VMware documentation:
  - VMware Workspace ONE
  - VMware Identity Manager
  - VMware Workspace ONE UEM

- Microsoft documentation:
  - Microsoft Active Directory Federation Services
Requirements

You must meet certain system requirements before beginning the Workspace ONE and Active Directory Federation Services integration.

Components

The following components are required.

- A Workspace ONE UEM tenant (administrator role required)
- A VMware Identity Manager tenant (administrator role required)
- AirWatch Cloud Connector (ACC)
- VMware Identity Manager connector

Note  If your existing deployment syncs users to VMware Identity Manager from Workspace ONE UEM, the VMware Identity Manager connector is not required. For new deployments, use the VMware Identity Manager connector to sync users from Active Directory to VMware Identity Manager.

- Microsoft Active Directory Federation Services (administrator role required)

Workspace ONE UEM and VMware Identity Manager Integration

Integrate your Workspace ONE UEM and VMware Identity Manager tenants and configure the mobile single sign-on (SSO) authentication methods that you intend to use for device trust.

Active Directory Integration

Before integrating Workspace ONE with Active Directory Federation Services, integrate your Active Directory and sync users. You must integrate Active Directory with:

- Workspace ONE UEM using AirWatch Cloud Connector (ACC)
VMware Identity Manager using VMware Identity Manager connector (for new deployments)

**Note** If your existing deployment syncs users to VMware Identity Manager from Workspace ONE UEM, you do not need to use the VMware Identity Manager connector to sync users.

Ensure that you sync the same users to all the environments.
Overview of Workspace ONE and Active Directory Federation Services Integration

Integrating Workspace ONE with Active Directory Federation Services allows organizations to manage access to enterprise applications and resources with conditional user and device access policies.

About VMware Workspace ONE

VMware Workspace™ ONE™ is a secure enterprise platform that delivers and manages applications on iOS, Android, Windows 10, and Mac OS devices. Identity, application, and enterprise mobility management are integrated into the Workspace ONE platform.

VMware Identity Manager™ and VMware Workspace ONE™ UEM (formerly named AirWatch) are part of the Workspace ONE platform. As the identity component of Workspace ONE, VMware Identity Manager provides enterprise identity integration and web and mobile single sign-on (SSO) services.

About the Integration Process

VMware Identity Manager has the capability to act as a standalone federation identity provider (IdP). It can also integrate with existing IdP and SSO solutions like Active Directory Federation Services as a federated IdP or service provider (SP). When configured in this way, Workspace ONE can provide augmented services such as a unified application catalog and conditional access policies based on device posture.

With the flexible identity policies of VMware Identity Manager and Active Directory Federation Services, either identity provider can authenticate login requests depending on the scenario. For example, you can configure VMware Identity Manager to authenticate users of mobile devices, while Active Directory Federation Services continues to authenticate desktop users. This flexibility gives you the benefits of Workspace ONE integration in key areas while maintaining your existing Active Directory Federation Services workflow in other scenarios.

This guide provides step-by-step instructions on how to configure and test use cases supported by the Workspace ONE integration with Active Directory Federation Services. To perform the integration, you integrate VMware Identity Manager, the identity component of Workspace ONE, with Active Directory Federation Services.
This chapter includes the following topics:

- About Active Directory Federation Services and Claims-Based Authentication
- Main Use Cases
- IdP-initiated and SP-Initiated Authentication Flows

About Active Directory Federation Services and Claims-Based Authentication

Microsoft Active Directory Federation Services (AD FS) enables federated identity and access management by securely sharing digital identity and entitlement rights across security and enterprise boundaries. Both AD FS and VMware Identity Manager use a claims-based authentication 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 security token.

A claim typically consists of an Active Directory user attribute, such as the user principal name (UPN) or email address. A security token bundles the set of claims about a particular user in the form of a Security Assertion Markup Language (SAML) assertion.

A claims-based workflow follows this sequence:

1. User requests access to an application or resource.
2. The application or resource service provider (also called the relying party) redirects the authentication request to the federated identity provider (also called the claims provider).
3. If needed, the user is prompted to enter authentication credentials into the claims provider's sign-in portal.
4. After authenticating the user's identity, the claims provider issues the security token and sends it back to the federated relying party.
5. Upon accepting the token as validation of the user's identity, the relying party grants the user access to the application or resource.

The following table shows the parallels between the terminology used by AD FS and VMware Identity Manager.

<table>
<thead>
<tr>
<th>AD FS Term</th>
<th>VMware Identity Manager Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Token</td>
<td>Assertion</td>
<td>Collection of SAML-formatted security information describing users, which is created and consumed during a federated access request.</td>
</tr>
<tr>
<td>Claims Provider or Issuer</td>
<td>Identity Provider (IdP)</td>
<td>Partner in a federation that creates security tokens for users.</td>
</tr>
<tr>
<td>AD FS Term</td>
<td>VMware Identity Manager Term</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</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>

**Main Use Cases**

By integrating AD FS with VMware Identity Manager, you can implement several beneficial use cases. The use cases include: Workspace ONE Login Using AD FS, Unified Application Catalog, and Mobile Device Trust.

The following sections describe the main use cases supported by AD FS integration, including the specific configuration procedures required to implement each use case. To realize the benefits of all three use cases, perform an end-to-end setup that includes all the integration procedures described in this guide.

**Use Case 1: Workspace ONE Login Using AD FS**

You can configure the Workspace ONE app and portal to use AD FS as a trusted identity provider. This configuration allows end users to log in to the Workspace ONE app and portal with their familiar Active Directory credentials. This use case also applies to VMware Horizon® customers who are using the Workspace ONE portal to run Horizon apps and desktops, but have not yet deployed Workspace ONE UEM to manage devices.

To implement this use case, perform the procedures described in Chapter 3 Integrating AD FS as a Federated Identity Provider for VMware Identity Manager.

**Use Case 2: Unified Application Catalog**

You can configure the Workspace ONE catalog to publish applications federated through AD FS. These applications appear alongside other resources configured through Workspace ONE, such as virtual Horizon and Citrix applications and desktops, and native Workspace ONE UEM applications. End users can go to a single portal to discover, run, or download their enterprise apps from any device with a consistent user experience.

To implement this use case, perform the procedures described in the following topics:

1. Creating a VMware Identity Manager Claims Provider Trust in AD FS
2. Configuring AD FS as a Service Provider for VMware Identity Manager
3. Test the VMware Identity Manager Authentication
4. Integrating AD FS-federated Applications With Workspace ONE
Use Case 3: Mobile Device Trust

Integrating AD FS with Workspace ONE lets administrators establish mobile device trust by evaluating device posture before permitting access from end users to sensitive applications. Device posture can refer to the security status of the mobile device, such as whether it is managed and compliant with your organization's IT requirements. Device posture policies are established in Workspace ONE UEM and evaluated whenever a user signs in to a protected application.

For example, a device trust flow using Office 365 follows this sequence:

1. Mobile user attempts to access the Office 365 tenant.
2. Office 365 redirects to AD FS as the federated identity provider.
3. AD FS processes the incoming request and routes the user to VMware Identity Manager as a trusted claims provider.
4. As the identity component of Workspace ONE, VMware Identity Manager challenges the user for authentication based on user access and device posture policies.
5. VMware Identity Manager performs authentication steps based on the device posture:
   a. If the device is managed and compliant with IT requirements, VMware Identity Manager authenticates the user.
   b. If the device is unmanaged but compliant with IT requirements, VMware Identity Manager enrolls the device and authenticates the user.
   c. If the device is not compliant with IT requirements, VMware Identity Manager blocks the user from accessing the Office 365 application.
6. Upon successful authentication with VMware Identity Manager, the user is redirected back to AD FS.
7. AD FS issues the SAML assertion for Office 365 and grants the user access to the application.

Figure 2-1. Device Trust Flow
To implement this use case, perform the procedures described in the following topics:

1. Creating a VMware Identity Manager Claims Provider Trust in AD FS
2. Configuring AD FS as a Service Provider for VMware Identity Manager
3. Test the VMware Identity Manager Authentication
4. Redirect Mobile Users to VMware Identity Manager for Authentication

**Note** Alternatively, you can configure Office 365 to authenticate directly with the VMware Identity Manager service, without using AD FS as an intermediary. For information on configuring this alternative use case, see VMware Identity Manager Integration with Office 365.

**End to End Setup Covering All Use Cases**

To set up the complete Workspace ONE and AD FS integration to cover all use cases, perform all the procedures described in the following topics:

1. Chapter 3 Integrating AD FS as a Federated Identity Provider for VMware Identity Manager
2. Chapter 4 Integrating VMware Identity Manager as a Federated Identity Provider for AD FS
3. Chapter 5 Configure the Claims Provider for the VMware Identity Manager Relying Party Trust

**IdP-initiated and SP-Initiated Authentication Flows**

In an AD FS-federated configuration, the authentication flow differs depending on where the user initiates the login request. This guide differentiates between IdP-initiated and SP-initiated login requests.

This guide uses the following terminology to refer to the origin of an authentication request:

- An **identity provider-initiated (IdP-initiated)** flow occurs when the user attempts to log in to an application from the Workspace ONE portal.
- A **service provider-initiated (SP-initiated)** flow occurs when the user attempts to log into an application directly from the application's sign-in portal (for example, portal.office.com for Office 365).

Your configuration can support both IdP-initiated and SP-initiated authentication flows. To support each type of authentication flow, you must configure certain settings, such as access policies in VMware Identity Manager.
Integrating AD FS as a Federated Identity Provider for VMware Identity Manager

With AD FS integrated as a trusted identity provider, end users can log in to the Workspace ONE portal with their Active Directory credentials. To complete the integration, configure AD FS as an identity provider for VMware Identity Manager, and VMware Identity Manager as a relying party for AD FS.

Integrating AD FS as a federated identity provider for VMware Identity Manager allows you to implement Workspace ONE Login Using AD FS (see Main Use Cases). This use case employs the following authentication flow.

1. End user seeks access to the Workspace ONE portal.
2. As the identity component of Workspace ONE, VMware Identity Manager redirects the authentication request to AD FS.
3. If needed, AD FS prompts the user to log in with Active Directory credentials.
4. AD FS authenticates the user, and issues a security token containing the LDAP email address attribute of the user.
5. VMware Identity Manager accepts the SAML-formatted token from AD FS as the trusted identity provider.
6. VMware Identity Manager grants the user access to the Workspace ONE portal.

Figure 3-1. AD FS Identity Provider Flow
This chapter includes the following topics:

- Obtain the VMware Identity Manager SP Metadata
- Configuring AD FS as a Trusted Identity Provider for VMware Identity Manager
- Configuring VMware Identity Manager as a Relying Party for AD FS
- Test the Workspace ONE Login with AD FS Authentication

**Obtain the VMware Identity Manager SP Metadata**

AD FS requires the VMware Identity Manager service provider (SP) metadata for federation. The SP metadata is an XML file that describes the capabilities and requirements of VMware Identity Manager as a trusted service provider.

**Procedure**

1. Log in to the VMware Identity Manager console.
2. Select the **Catalog > Web Apps** tab.
3. Click **Settings** and then select **SAML Metadata**.
4. Under the SAML Metadata section, next to **Service Provider (SP) metadata**, click the **Copy URL** link to copy the SP metadata URL to the clipboard. Paste and save the URL in a text file on your computer.
5. Close the Settings page.
Configuring AD FS as a Trusted Identity Provider for VMware Identity Manager

You can configure VMware Identity Manager to use AD FS as a trusted identity provider for authentication.

Add AD FS as an Identity Provider in the Service

To configure the AD FS integration, you must add AD FS as an identity provider instance in VMware Identity Manager.

Prerequisites

- Download the federation metadata file for the AD FS server by navigating to the URL: https://ADFSdomain/FederationMetadata/2007-06/FederationMetadata.xml where ADFSdomain is replaced with the fully qualified domain name for your AD FS server.

- In the VMware Identity Manager console, configure the access policies that you want to use for the AD FS identity provider instance. For information about configuring access policies, see the VMware Identity Manager Administration Guide.

Procedure

1. Log in to the VMware Identity Manager console with full administrator privileges.
2. Select the Identity & Access Management tab. Click Manage, and then click Identity Providers.
3. Click Add Identity Provider and select Create Third Party IDP.
4 Modify the configuration settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider Name</td>
<td>Enter a short descriptive name for the AD FS identity provider instance.</td>
</tr>
</tbody>
</table>
| SAML Metadata                  | a To establish trust with AD FS, add the federation metadata here. In the text box, copy and paste the contents of the AD FS federation metadata file that you obtained previously.  
                                          b Click **Process IdP Metadata**. The Name ID format mappings are automatically imported from the AD FS metadata.  
                                          c (Optional) Configure additional AD FS Name ID formats and map them to user values in the VMware Identity Manager service. |
| Just-in-Time User Provisioning | Do not enable. |
| Users                          | Select the VMware Identity Manager directories of the users that can authenticate using AD FS. |
| 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 AD FS for authentication. |
| Authentication Methods         | To add an authentication method that you want AD FS to use, click the green plus sign and enter the name of the method. Then select the SAML authentication context class that supports the method. Configure the following authentication methods.  
                                          - **Kerberos-based authentication**: For SAML Context, select `urn:federation:authentication:windows` |
| Single Sign-Out Configuration  | Do not enable. Single sign-out configuration is not required for the AD FS identity provider instance. |
| SAML Signing Certificate       | To display the VMware Identity Manager service provider metadata in a browser window, click **Service Provider (SP) Metadata**. Copy and save the URL. You need this URL later when you configure the Federation Service Properties in AD FS. |

5 Click **Add**.
What to do next

Add AD FS Authentication Methods to Access Policy Rules

Add AD FS Authentication Methods to Access Policy Rules

To complete the configuration of the AD FS identity provider instance, incorporate the AD FS authentication methods into your access policies.

The following procedure describes an example of incorporating AD FS authentication methods into a policy rule for Windows 10 devices. You can use this example as a guideline when configuring your own access policies.

For more information about configuring access policies and policy rules, see the VMware Identity Manager Administration Guide.

Prerequisites

Add AD FS as an Identity Provider in the Service

Procedure

1. Log in to the VMware Identity Manager console with full administrator privileges.

2. Select the Identity & Access Management tab. Click Manage, and then click Policies.

3. Select the access policy that you want to modify and click Edit.

   The Edit Policy wizard appears.

4. Click Next.
5 On the Configuration page, click **Add Policy Rule** and create a rule for Windows 10 devices.

   a Specify Kerberos-based authentication as the first authentication method and Forms-based authentication as the fallback method, according to the following example. Leave the **and user belongs to group(s):** option blank to apply the rule to all users.

   
   If a user's network range is: ALL RANGES
   and user accessing content from: Windows 10
   and user belongs to group(s):
   Then perform this action: Authenticate using
   then the user may authenticate using: Kerberos-based authentication
   If the preceding method fails or is not applicable, then: Forms-based authentication

   b Click **Save**.
   
   The new policy rule appears as **Kerberos-based authentication+1** in the rules list.

6 In the rules list, reorder the rules such that **Kerberos-based authentication+1** appears at the top of the list as the first rule to apply. To move the rule in the list, drag the handle at the left of the rule name.
7  Click Next. Review your changes and then click Save.

You are now finished with configuring AD FS as a trusted identity provider for VMware Identity Manager. Next, you must configure VMware Identity Manager as a trusted relying party for AD FS.

What to do next

Perform the procedures described in Configuring VMware Identity Manager as a Relying Party for AD FS.

Configuring VMware Identity Manager as a Relying Party for AD FS

A relying party trust defines how AD FS recognizes a relying party (or service provider) and issues claims to it. To create a relying party trust, you add VMware Identity Manager as a relying party for AD FS and then configure claim rules.

Add VMware Identity Manager as a Relying Party for AD FS

To add VMware Identity Manager to the AD FS federation, you configure VMware Identity Manager as a relying party (or service provider) for AD FS.

Prerequisites

Obtain the VMware Identity Manager SP Metadata

Procedure

1  On the AD FS server, run the AD FS Management console as an administrator.

2  (AD FS 3.0) In the left pane, expand the Trust Relationships folder.

3  In the left pane, click Relying Party Trusts to highlight it. Then right-click Relying Party Trusts and select Add Relying Party Trust from the menu.
4 Start the Add Relying Party Trust Wizard.
   - (AD FS 4.0) Select **Claims aware**, and then click **Start**.
   - (AD FS 3.0) Click **Start**.
5 On the Select Data Source page, select **Import data about the relying party published online or on a local network**. In the text box, paste the URL of the VMware Identity Manager service provider metadata file that you obtained earlier. Then click **Next**.

The URL resembles `https://{VIDMtenant}/SAAS/API/1.0/GET/metadata/sp.xml`, where `{VIDMtenant}` is replaced with the fully qualified domain name (FQDN) of the VMware Identity Manager service.

6 On the Specify Display Name page, in the **Display name** text box, enter a name for the VMware Identity Manager service. In the **Notes** text box, enter a description of this relying party trust. Then click **Next**.

In AD FS 3.0, the Multi-factor Authentication page appears. The Workspace ONE integration does not require multi-factor authentication. Click **Next**.

7 Configure the appropriate setting to allow all users access to Workspace ONE after VMware Identity Manager receives the valid claims.

- (AD FS 4.0) On the Choose Access Control Policy page, select **Permit everyone**. Then click **Next**.
- (AD FS 3.0) On the Choose Issuance Authorization Rules page, select **Permit all users to access this relying party**. Then click **Next**.

8 On the Ready to Add Trust page, review your changes and then click **Next**.

9 On the Finish page, select the option to edit the claim rules or issuance policy after you close the wizard.

- (AD FS 4.0) Select the **Configure claims issuance policy for this application** check box and then click **Close**.
- (AD FS 3.0) Select the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box and then click **Close**.

The Edit Claim Issuance Policy window (AD FS 4.0) or Edit Claim Rules window (AD FS 3.0) appears.
What to do next

Configure Claim Rules for the Relying Party Trust

Configure Claim Rules for the Relying Party Trust

As the claims issuer (or identity provider), AD FS sends security tokens containing authentication claims to VMware Identity Manager. Relying party claim rules define the content of these claims and transform them into a format that VMware Identity Manager can recognize and consume.

You must configure two claim rules for VMware Identity Manager as the relying party. The first rule directs AD FS to look up the LDAP email address attribute for the requesting user and to send this attribute as the claim. The second rule transforms this claim into the SAML-based email address attribute expected by VMware Identity Manager.

Prerequisites

Add VMware Identity Manager as a Relying Party for AD FS
**Procedure**

1. If needed, open the Edit Claim Issuance Policy window (AD FS 4.0) or Edit Claim Rules window (AD FS 3.0) on the AD FS server by performing the following steps.
   a. Run the AD FS Management console as an administrator.
   b. (AD FS 3.0) In the left pane, expand the **Trust Relationships** folder.
   c. In the left pane, select **Relying Party Trusts**.
   d. In the center pane, select the relying party trust that you created for VMware Identity Manager.
   e. In the right pane, click **Edit Claim Issuance Policy** (AD FS 4.0) or **Edit Claim Rules** (AD FS 3.0).

2. In the Edit Claim Issuance Policy window (AD FS 4.0) or Edit Claim Rules window (AD FS 3.0), select the **Issuance Transform Rules** tab.
3 Click **Add Rule**.

The Add Transform Claim Rule Wizard appears.

4 For **Claim rule template**, select **Send LDAP Attributes as Claims**. Then click **Next**.

The Configure Rule page appears.

5 Specify the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim rule name</td>
<td>Enter a descriptive name for the rule (for example, Get E-Mail Address Attribute).</td>
</tr>
<tr>
<td>Attribute store</td>
<td>Select Active Directory.</td>
</tr>
<tr>
<td>LDAP Attribute</td>
<td>Select E-Mail-Addresses.</td>
</tr>
<tr>
<td>Outgoing Claim Type</td>
<td>Select E-mail address.</td>
</tr>
</tbody>
</table>

6 Click **Finish**.
7 Verify that the email address attribute rule appears in the list of claim rules.

Next, you add a second rule that transforms the email address attribute in the outgoing claim to the SAML-based format expected by VMware Identity Manager.

8 Click Add Rule.

9 For Claim rule template, select Send Claims Using a Custom Rule. Then click Next.

10 Specify the following settings.

   - For Claim rule name, enter a descriptive name for the rule (for example, Transform E-Mail Address).
   - In the Custom rule text box, enter the following script, where {VIDMtenant} at the end of the script is replaced with the fully qualified domain name (FQDN) of the VMware Identity Manager service. This script uses the required syntax for custom rules.

   ```
   c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
   
   ```

11 Click Finish.
Verify that both new rules appear in the rules list, with the custom transformation rule appearing in the second position. Click **Apply**, and then click **OK**.

This procedure concludes the integration of AD FS as a federated identity provider for VMware Identity Manager.

**What to do next**

1. **Test the Workspace ONE Login with AD FS Authentication**

**Test the Workspace ONE Login with AD FS Authentication**

After integrating AD FS as a federated identity provider for VMware Identity Manager, test the configuration by logging in to the Workspace ONE portal.

**Prerequisites**

Perform all the procedures described in Chapter 3 Integrating AD FS as a Federated Identity Provider for VMware Identity Manager.
Procedure

1. In a web browser, navigate to your organization's Workspace ONE portal.

2. Enter the Active Directory credentials of a test user, and verify that the user can successfully access the Workspace ONE portal based on those credentials.

**Note**  If the test login fails, you can reaccess the VMware Identity Manager console by navigating to https://{VIDMtenant}/SAAS/login/0, where {VIDMtenant} is the fully qualified domain name of the VMware Identity Manager tenant.
Integrating VMware Identity Manager as a Federated Identity Provider for AD FS

To perform the integration, you first configure VMware Identity Manager as a federated identity provider (or claims provider) for AD FS. Then you configure AD FS as a service provider for VMware Identity Manager.

Integrating VMware Identity Manager as a federated identity provider allows you to implement the Mobile Device Trust and Unified Application Catalog use cases (see Main Use Cases).

This chapter includes the following topics:

- Creating a VMware Identity Manager Claims Provider Trust in AD FS
- Configuring AD FS as a Service Provider for VMware Identity Manager
- Test the VMware Identity Manager Authentication
- Integrating AD FS-federated Applications With Workspace ONE
- Redirect Mobile Users to VMware Identity Manager for Authentication

Creating a VMware Identity Manager Claims Provider Trust in AD FS

A claims provider trust defines how AD FS recognizes a claims provider (or identity provider) and accepts claims from it. To create a claims provider trust, you add VMware Identity Manager as a claims provider for AD FS and then configure claim rules.

Download the VMware Identity Manager IdP Metadata

AD FS requires the VMware Identity Manager identity provider (IdP) metadata for federation. The IdP metadata describes the capabilities and requirements of VMware Identity Manager as a trusted identity provider.

Procedure

1. Log in to the VMware Identity Manager console with full administrator privileges.
2. Select the Catalog > Web Apps tab.
3 Click **Settings** and then select **SAML Metadata**.

4 Under the SAML Metadata section, click the **Identity Provider (IdP) metadata** link to open a new window displaying the contents of the SAML metadata .xml file. Right-click in the window and select **Save as** to save the contents to a .xml file on your computer.

5 Close the Settings page.

**What to do next**

**Add VMware Identity Manager as a Claims Provider for AD FS**

**Add VMware Identity Manager as a Claims Provider for AD FS**

To create a federation between VMware Identity Manager and AD FS, you configure VMware Identity Manager as a claims provider (or identity provider) for AD FS.

**Prerequisites**

- Download the VMware Identity Manager IdP Metadata
- Verify the federation between AD FS and the application that you want to authenticate through the VMware Identity Manager service. Verify that AD FS successfully authenticates users logging into the application through a web browser.

**Note** Before proceeding,
Procedure

1. On the AD FS server, run the AD FS Management console as an administrator.
2. (AD FS 3.0) In the left pane, expand the Trust Relationships folder.
3. In the left pane, click Claims Provider Trusts to highlight it. Then right-click Claims Provider Trusts and select Add Claims Provider Trust from the menu.

The Add Claims Provider Trust Wizard appears.
4 Click **Start**.

5 On the Select Data Source page, import the IdP metadata file that you downloaded from VMware Identity Manager.
   a Select **Import data about the claims provider from a file**.

   ![Select Data Source](image)

   b Click **Browse**, and navigate to the VMware Identity Manager IdP metadata file. To import the metadata file, click **Open**.

   c Then click **Next**.

6 On the Specify Display Name page, in the **Display name** text box, enter a name for the VMware Identity Manager relying party. Use a name that is recognizable to users who might need to select VMware Identity Manager as the authentication option during the login process. Then click **Next**.

7 On the Ready to Add Trust page, review your changes and then click **Next**.

8 On the Finish page, select the **Open the Edit Claim Rules dialog for this claims provider trust when the wizard closes** check box. Then click **Close**.

   The Edit Claim Rules window appears.
Configure Claim Rules for the Claims Provider Trust

As a claims issuer, VMware Identity Manager sends security tokens containing authentication claims to AD FS. Claim rules define the content of these claims and transform them into a format that AD FS can recognize and consume.

VMware Identity Manager sends the Name ID user attribute as an authentication claim to AD FS. This attribute takes the form `domain\samAccountName` in the SAML assertion issued by VMware Identity Manager. However, AD FS expects instead a value of type `WindowsAccountName` formatted as `domain\user`. AD FS also expects to see Active Directory named as the issuer of this value.

The solution is to configure a claim rule that transforms the Name ID attribute into `WindowsAccountName` format and changes the named issuer from VMware Identity Manager to Active Directory. AD FS can then recognize and consume the incoming claim from VMware Identity Manager.

What to do next

Configure Claim Rules for the Claims Provider Trust
Prerequisites

Add VMware Identity Manager as a Claims Provider for AD FS

Procedure

1. If needed, open the Edit Claim Rules window on the AD FS server by performing the following steps.
   a. Run the AD FS Management console as an administrator.
   b. (AD FS 3.0) In the left pane, expand the Trust Relationships folder.
   c. In the left pane, select Claims Provider Trusts.
   d. In the center pane, select the claims provider trust that you created for VMware Identity Manager.
   e. In the right pane, click Edit Claim Rules.

2. In the Edit Claim Rules window, click Add Rule.
The Add Transform Claim Rule Wizard appears.

3 For **Claim rule template**, select **Send Claims Using a Custom Rule**. Then click **Next**.
The Configure Rule page appears. You can now create a rule that transforms the incoming Name ID attribute into the WindowsAccountName value formatted as domain\user. The rule also names Active Directory as the issuer of this value.

4 On the Configure Rule page, perform the following steps.

a For **Claim rule name**, enter a descriptive name for the rule.

b In the **Custom Rule** text box, enter the following rule.

```c:
[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] ==
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"]

=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer = "AD AUTHORITY", OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType);```
5  Click **Finish**.

6  In the Edit Claim Rules window, verify that the custom rule you created appears in the list.
7  Click **Apply**, and then click **OK**.

**What to do next**

Proceed to **Configuring AD FS as a Service Provider for VMware Identity Manager**.

**Configuring AD FS as a Service Provider for VMware Identity Manager**

After configuring VMware Identity Manager as the claims provider, complete the federation setup by configuring AD FS as the service provider. You must add AD FS as an application source in VMware Identity Manager and make the application source available to all users.

**Add AD FS as an Application Source in VMware Identity Manager**

To configure AD FS as a service provider for VMware Identity Manager, you add AD FS as an application source. The AD FS application source enables VMware Identity Manager to respond to authentication requests from the AD FS server.
Prerequisites

Download the federation metadata file for the AD FS server by navigating to the URL: https://{ADFSdomain}/FederationMetadata/2007-06/FederationMetadata.xml where {ADFSdomain} is replaced with the fully qualified domain name (FQDN) your AD FS server.

Procedure

1. Log in to the VMware Identity Manager console with full administrator privileges.
2. Select the Catalog > Web Apps tab.
3. Click Settings.
4. In the left pane, click Application Sources.
5. On the Application Sources page, click ADFS.
6. On the Definition page of the ADFS Application Source wizard, click Next.
7. On the Configuration page, perform the following steps.
   a. For Configuration, select URL/XML.
   b. In the URL/XML text box, copy and paste the contents of the federation metadata file that you downloaded previously from the AD FS server.
Click Next.

On the Access Policies page, select the access policy that you want to use for the AD FS application source.

For more information about access policies, see the VMware Identity Manager Administration Guide.

Click Next, review your selections, and click Save.

Saving the setup at this stage allows VMware Identity Manager to import configuration settings from the AD FS metadata.

On the Application Sources page, click ADFS again. Then click Next.

Some settings on the Configuration page now contain values imported from the AD FS metadata.
12 On the Configuration page, modify the following settings. Accept the default values for all other settings.
   a For **Username Format**, select **Unspecified**.
   b For **Username Value**, enter `${user.domain}\${user.userName}`. This value ensures that VMware Identity Manager sends the user name value in the WindowsAccountName domain\user format required by AD FS.

13 Expand the **Advanced Properties** section and configure the following settings.
   a Set **Include Assertion Signature** to **Yes**.
   b For **Signature Algorithm**, select **SHA256 with RSA**.

14 Click **Next**, and click **Next** again to advance to the Summary page. Then click **Save**.

**What to do next**

**Assign the AD FS Application Source to All Users**

**Assign the AD FS Application Source to All Users**

After you configure the AD FS application source, assign it to all users in VMware Identity Manager.

**Prerequisites**

**Add AD FS as an Application Source in VMware Identity Manager**

**Procedure**

1 Log in to the VMware Identity Manager console with full administrator privileges.
2 Select the **Users & Groups > Groups** tab.
3 Click **ALL USERS**.
4 Click the **Apps** tab.
5 If needed, click **Expand All**. Click the edit icon to the right of the **AD FS** application source.
6 For the Deployment type, select **Automatic**. Then click **Save**.

**What to do next**

**Test the VMware Identity Manager Authentication**

**Test the VMware Identity Manager Authentication**

After configuring VMware Identity Manager as the claims provider and AD FS as the service provider, you can test the SP-initiated authentication flow with an AD FS-federated application. A successful configuration allows you to use VMware Identity Manager to authenticate access to an AD FS-federated application.
Use the following procedure to test the SP-initiated authentication flow with an AD FS-federated application. For more information about authentication flows, see IdP-initiated and SP-Initiated Authentication Flows.

Prerequisites

Perform the procedures described in the following topics:

- Creating a VMware Identity Manager Claims Provider Trust in AD FS
- Configuring AD FS as a Service Provider for VMware Identity Manager

Procedure

1. Open a private browsing session (a good practice when testing federated authentication) on your computer browser.

2. Navigate to the login portal for an AD FS-federated application (for example, https://login.microsoftonline.com for Office 365).

   ![Login Portal](image)

3. Enter the user name of a user residing in the AD FS-federated domain.

   Verify that the application portal redirects you to the AD FS Home Realm Discovery page, which presents VMware Identity Manager as an authentication option.
Note The VMware Identity Manager authentication option uses the Display Name that you specified during the Claims Provider configuration. For more information, see Add VMware Identity Manager as a Claims Provider for AD FS.

4 Select the option to authenticate with VMware Identity Manager.

Verify that AD FS redirects you to the Workspace ONE login page.
5 Enter the credentials of a user entitled to this resource.

Verify that VMware Identity Manager successfully authenticates you into the application portal.

What to do next

Proceed to Integrating AD FS-federated Applications With Workspace ONE.
Integrating AD FS-federated Applications With Workspace ONE

After verifying the federation between AD FS and VMware Identity Manager, you can add AD FS-federated applications to the Workspace ONE catalog. End users can then use an IdP-initiated authentication flow to access AD FS-federated applications alongside other enterprise applications from the Workspace ONE portal.

For more information about authentication flows, see IdP-initiated and SP-Initiated Authentication Flows.

Enable the RelayState Parameter in AD FS

To complete the integration of AD FS-federated applications with Workspace ONE, you must enable the RelayState parameter in AD FS. This parameter passes an application’s relying party identifier from VMware Identity Manager to AD FS, so that AD FS can redirect users to the application portal.

Without the RelayState parameter enabled, users can click an AD FS-federated application in the Workspace ONE portal and authenticate into AD FS through VMware Identity Manager. However, they are not further redirected to the application portal.

With RelayState enabled, an IdP-initiated authentication flow follows this sequence:

1. End user requests access to an AD FS-federated application in the Workspace ONE portal.
2. VMware Identity Manager sends an IdP-initiated authentication response to AD FS. This SAML response contains a RelayState value set to the relying party identifier of the application.
3. AD FS accepts the authentication response and redirects the user to the application portal specified by the RelayState value.
4. User is granted access to the application.

For more information about IdP-initiated authentication flows, see IdP-initiated and SP-Initiated Authentication Flows. For more information about RelayState support in AD FS, see the following links:


Prerequisites

Test the VMware Identity Manager Authentication

Procedure

1. On the AD FS server, open the file: %systemroot%\AD FS\Microsoft.IdentityServer.Servicehost.exe.config
2 Insert `<useRelayStateForIdpInitiatedSignOn enabled="true" />` within the `<microsoft.identityServer.web>` section of the config file.

```xml
<microsoft.identityServer.web>
  <useRelayStateForIdpInitiatedSignOn enabled="true" />
  <acceptedFederationProtocols wfsFederation="true" saml="true" />
  <localAuthenticationTypes enabled="true" />
</microsoft.identityServer.web>
```

What to do next

**Obtain the Relying Party Identifier for an AD FS-federated Application**

**Obtain the Relying Party Identifier for an AD FS -federated Application**

The relying party identifier uniquely identifies an AD FS-federated application so that another claims provider can authenticate users seeking access to the application. You must obtain the relying party identifier for each AD FS-federated application that you want to add to the Workspace ONE catalog.

**Prerequisites**

**Enable the RelayState Parameter in AD FS**

**Procedure**

1. On the AD FS server, run the AD FS Management console as an administrator.
2. (AD FS 3.0) In the left pane, expand the Trust Relationships folder.
3. In the left pane, select Relying Party Trusts.
4. In the Relying Party Trusts list, locate the name of the AD FS-federated application that you want to add to the catalog. Note the relying party identifier that appears in the Identifier column for the application.
What to do next

Add an AD FS-federated Application to the Workspace ONE Catalog

Add an AD FS-federated Application to the Workspace ONE Catalog

Adding an AD FS-federated application to the catalog makes it possible for end users to access the application alongside other enterprise applications from the Workspace ONE portal. You must repeat this procedure for each application that you want to add to the catalog.

Prerequisites

- Enable the RelayState Parameter in AD FS
- Obtain the Relying Party Identifier for an AD FS-federated Application

Procedure

1. Log in to the VMware Identity Manager console with full administrator privileges.
2. Select the Catalog > Web Apps tab.
3. Click New.
4. On the New SaaS Application wizard's Definition page, enter the following information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the application.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description of the application.</td>
</tr>
<tr>
<td>Icon</td>
<td>(Optional) Upload an icon.</td>
</tr>
<tr>
<td>Category</td>
<td>(Optional) To add the application to a category, select it from the drop-down menu.</td>
</tr>
</tbody>
</table>
5 Click **Next**.

6 On the Configuration page, enter the following information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>Select ADFS Application Source.</td>
</tr>
<tr>
<td>Target URL</td>
<td>Enter the URL of the application in this format: ( \text{RPID} = { \text{AppIdentifier} } ), where ( { \text{AppIdentifier} } ) is replaced with the application's relying party identifier that you obtained previously from the AD FS Management console.</td>
</tr>
<tr>
<td>Open in VMware Browser</td>
<td>Set to <strong>No</strong>.</td>
</tr>
</tbody>
</table>

7 Click **Next**.

8 On the Access Policies page, select the access policy that you want to use for the application, and then click **Next**.

For more information about access policies, see the VMware Identity Manager Administration Guide.
9 Review your selections and click **Save**, or click **Save & Assign** to assign the application to users and groups.

If you do not assign the application to any users and groups now, you can do so later by selecting the application on the **Catalog > Web Apps** page and clicking **Assign**.

10 Verify that the application is added to the catalog.

11 Repeat this procedure for each application that you want to add to the Workspace ONE catalog.

**What to do next**

Using a test user account, navigate to your organization's Workspace ONE portal. From the application catalog, issue an IdP-initiated authentication request by opening the target AD FS-federated application. Verify that you are successfully redirected to the application's login portal.

For more information about IdP-initiated authentication flows, see [IdP-initiated and SP-Initiated Authentication Flows](#).

### Redirect Mobile Users to VMware Identity Manager for Authentication

In a successful configuration, users who visit the web portal of an AD FS-federated application can select their authentication method. You can automate this selection by configuring AD FS to authenticate desktop users and route mobile users to VMware Identity Manager for authentication.

Use the following procedure to implement Mobile Device Trust (see [Main Use Cases](#)). With this use case, you gain the unique mobile device management features provided by VMware Identity Manager with Workspace ONE UEM. Desktop users can continue to use the existing AD FS authentication workflow to which they are accustomed.

This use case applies to users who log in directly to an AD FS-federated application through the application portal (for example, portal.office.com for Office 365). When a user starts an SP-initiated flow in this way, AD FS routes the authentication request to the appropriate identity provider based on the user's device type.

- If the user logs in from a desktop computer, AD FS handles the authentication request as the identity provider. The login experience remains unchanged for desktop users, as they sign in to the application using their familiar AD FS credentials.

- If the user logs in from a mobile device, AD FS forwards the authentication request to VMware Identity Manager as the trusted identity provider (or claims provider). VMware Identity Manager validates the user's credentials, and Workspace ONE UEM manages the user's access to the application based on the device posture policies in effect.

For more information about SP-initiated authentication flows, see [IdP-initiated and SP-Initiated Authentication Flows](#).

**Prerequisites**

Perform the procedures described in [Integrating AD FS-federated Applications With Workspace ONE](#).
Procedure

1. Log in to the AD FS server with full administrator privileges.
2. Run PowerShell as an administrator.
3. Create a working folder by entering the following cmdlet.

   ```bash
   mkdir c:\myscripts
   ```

4. Export the default AD FS web theme.

   ```powershell
   Export-AdfsWebTheme -Name "Default" -DirectoryPath c:\myscripts
   ```

   ![](image1.png)

   The Export cmdlet creates an `onload.js` file in the `c:\myscripts\script` folder. To specify the authentication option based on the type of user device, you modify this JavaScript file.

5. Open `C:\myscripts\script\onload.js` in a text editor such as Notepad++, and add the following JavaScript code to the beginning of the file.

   ```javascript
   var myCheckHRD = document.getElementById('hrdArea');
   if (myCheckHRD) {
       // redirect mobile users to VMware Identity Manager for authentication
       if (navigator.userAgent.match(/Mac|iPad|iPhone|Android/i) != null) {
           HRD.selection('https://{VIDMtenant}/SAAS/API/1.0/GET/metadata/idp.xml');
   ```

   ![](image2.png)

   Replace the placeholder values in the code as follows.

<table>
<thead>
<tr>
<th>Placeholder Value</th>
<th>Replacement Value for AD FS 4.0</th>
<th>Replacement Value for AD FS 3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{VIDMtenant}</code></td>
<td>Fully qualified domain name (FQDN) of the VMware Identity Manager service</td>
<td>FQDN of the VMware Identity Manager service</td>
</tr>
<tr>
<td><code>{AD FS claims provider}</code></td>
<td>'AD Authority'</td>
<td>'http://{ADFSdomain}/adfs/services/trust' (where <code>{ADFSdomain}</code> is the FQDN of the AD FS server)</td>
</tr>
</tbody>
</table>
This code designates the VMware Identity Manager service as the authentication option for users logging in from a mobile device. It designates AD FS as the authentication option for users logging in from all other devices. It also instructs AD FS to route authentication requests automatically without prompting the user for action.

6 Put the updated onload.js file in the c:\myscripts\script folder, overwriting the old file.

Next, you customize the AD FS login page by creating a AD FS web theme that references the updated onload.js file.

7 In PowerShell, create a AD FS web theme.

```powershell
New-AdfsWebTheme -Name "VIDM" -SourceName "Default"
```

8 Import the updated onload.js file.

```powershell
Set-AdfsWebTheme -TargetName VIDM -AdditionalFileResource
  @{"Uri="/adfs/portal/script/onload.js";path="c:\myscripts\script\onload.js"}"
```

9 Activate the new web theme.

```powershell
Set-AdfsWebConfig -ActiveThemeName "VIDM"
```

10 To save your changes, restart the AD FS service.

```powershell
Restart-Service adfssrv
```

**Note** If you want to revert to the default AD FS web theme, enter this cmdlet:

```powershell
Set-AdfsWebConfig -ActiveThemeName "Default"
```
Configure the Claims Provider for the VMware Identity Manager Relying Party Trust

When setting up an end-to-end integration to cover all main use cases, you must specify Active Directory as the sole claims provider for the VMware Identity Manager relying party trust. This claims provider configuration is required to prevent an authentication loop from occurring between AD FS and VMware Identity Manager.

Use the following procedure to specify Active Directory as the sole claims provider for the VMware Identity Manager relying party trust. After you complete the configuration, authentication requests will follow this flow:

1. End user attempts to access the Workspace ONE portal.
2. VMware Identity Manager redirects the authentication request to AD FS as the federated identity provider.
3. AD FS refers to the VMware Identity Manager relying party trust.
4. Since Active Directory is the sole claims provider specified for the relying party trust, the flow concludes with AD FS as the final authentication authority.

For more information about setting up an end-to-end integration, see Main Use Cases.

Prerequisites

Perform all the procedures described in the following topics:

- Chapter 3 Integrating AD FS as a Federated Identity Provider for VMware Identity Manager
- Chapter 4 Integrating VMware Identity Manager as a Federated Identity Provider for AD FS

Procedure

1. On the AD FS server, open a PowerShell session with elevated administrator rights.
2. Run the following cmdlet.

   ```shell
   Set-ADFSRelyingPartyTrust -TargetName "[VMWARE IDENTITY MANAGER RELYING PARTY]" -ClaimsProviderName "Active Directory"
   ```

   Replace `{VMWARE IDENTITY MANAGER RELYING PARTY}` with the name of the relying party trust that you configured for VMware Identity Manager. Use the name as it appears in the AD FS Management console.
Configure VMware Identity Manager as the Default Claims Provider for an AD FS-federated Application

This optional topic explains how to configure VMware Identity Manager as the default claims provider for an AD FS-federated application.

**Note** Do not perform the following procedure if you want to implement the Mobile Device Management use case. Instead, perform the procedure described in Redirect Mobile Users to VMware Identity Manager for Authentication.

**Prerequisites**

Perform the procedures described in the following topics.

- Creating a VMware Identity Manager Claims Provider Trust in AD FS
- Configuring AD FS as a Service Provider for VMware Identity Manager
- Test the VMware Identity Manager Authentication

**Procedure**

1. On the AD FS server, open a PowerShell session with elevated administrator rights.
2. Run the following cmdlet.

   ```powershell
   Set-ADFSRelyingPartyTrust -TargetName "{RP_app}" -ClaimsProviderName "{VMWARE IDENTITY MANAGER CLAIMS PROVIDER}"  
   ```

   Replace the placeholders in the cmdlet as follows.

   - Replace `{RP_app}` with the name of the relying party trust corresponding to the target application.
   - Replace `{VMWARE IDENTITY MANAGER CLAIMS PROVIDER}` with the name of the claims provider trust that you configured for VMware Identity Manager.

   Use the names of the relying party trust and claims provider trust as they appear in the AD FS Management console.

Since VMware Identity Manager is the sole claims provider specified in the cmdlet, all authentication requests for the designated relying party trust are redirected to VMware Identity Manager. This configuration eliminates the user’s choice to authenticate with the AD FS authentication policies.
What to do next

For information about more customization options on the AD FS sign-in page, see the following link:
Troubleshooting

To troubleshoot issues you might encounter with the VMware Identity Manager and AD FS integration, look up symptoms and error messages.

For more help with investigating and troubleshooting login issues, see the following resources.

- The VMware Identity Manager documentation.
- The VMware Identity Manager Audit Events report. This report lists the events related to user logins, including the authentication methods used to log in. To run this report, log in to the VMware Identity Manager console with full administrator privileges. Then navigate to Dashboard > Reports > Audit Events, and click Show.

This chapter includes the following topics:

- Unable to log in to VMware Identity Manager
- Error: "Contact your administrator"
- Error: "Cannot update Identity Provider"
- Error: "404.idp.not.found"
- Unable to authenticate into Workspace ONE portal using AD FS
- Unable to authenticate into AD FS-federated applications

Unable to log in to VMware Identity Manager

Problem

You cannot log in to VMware Identity Manager from the login page.

Cause

VMware Identity Manager is not configured correctly.

Solution

- To log in as the local administrator, use the following login URL:

  https://{VIDMtenant}/SAAS/login/0, where {VIDMtenant} is replaced with the fully qualified domain name of the VMware Identity Manager tenant.
Error: "Contact your administrator"

Problem
User is unable to log in and receives the error **Contact your administrator**.

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

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

Solution
- Download the VMware Identity Manager signing certificate XML file, and copy and paste the content directly into the appropriate AD FS certificate page.

Error: "Cannot update Identity Provider"

Problem
In the VMware Identity Manager console, after editing the AD FS identity provider to add or update an authentication method, you receive the error **Cannot update Identity Provider**.

Cause
When adding or updating a SAML context rule, the SAML context name must be unique in your VMware Identity Manager tenant. Authentication methods for the AD FS identity provider are not deleted when you click **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 repetitive authentication methods, use a consistent naming convention to remember the last authentication method that you created. For example, use a date in the authentication method name: **Password092116**.

Error: "404.idp.not.found"

Problem
When attempting a login to the Workspace ONE portal using AD FS as the identity provider, the user encounters the error **404.idp.not.found**.
Cause
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 or an authentication method of a disabled identity provider. The error also occurs when the AirWatch Cloud Connection password authentication method is selected but not enabled in VMware Identity Manager and the AirWatch pages.

Solution
♦ In the access policy rule, select an authentication method that is active and current.

Unable to authenticate into Workspace ONE portal using AD FS

Problem
When logging in, users cannot advance past the Workspace ONE sign-in page.

Cause
The VMware Identity Manager relying party trust does not have Active Directory designated as its sole claims provider. The missing claims provider designation results in an authentication loop between AD FS and VMware Identity Manager.

Solution
♦ Perform the procedures described in Chapter 5 Configure the Claims Provider for the VMware Identity Manager Relying Party Trust.

Unable to authenticate into AD FS-federated applications

Problem
You cannot authenticate into AD FS-federated applications using VMware Identity Manager as the identity provider.

Cause
Possibly one of the following:
- The federation between VMware Identity Manager and AD FS is configured incorrectly.
- The value or format provided in the claim issued by VMware Identity Manager does not match the value or format expected by AD FS.
- The RelayState parameter is not enabled, or the relying party identifier is not configured for the application.
Solution

1. Attempt an IdP-initiated login into AD FS by navigating to:
   https://{ADFSdomain}/ADFS/ls/idpinitiatedsignon.aspx, where {ADFSdomain} is replaced with the fully qualified domain name of the AD FS server.
   - A successful IdP-initiated login indicates that trust and authentication endpoints have been configured correctly in both AD FS and VMware Identity Manager. Proceed to step 2.
   - If the IdP-initiated login fails, check and redo all the configuration procedures described in Chapter 4 Integrating VMware Identity Manager as a Federated Identity Provider for AD FS.

2. Check the AD FS Event Viewer log for authentication errors.
   Most errors indicate a mismatch between the value or format provided by VMware Identity Manager and what is expected by the AD FS server. Check and redo the procedure described in Configure Claim Rules for the Claims Provider Trust.