How to install and configure AD FS 3.0 with Single Sign-On

Overview

This topic provides information on how to install and configure AD FS 3.0 with inSync Master.

Install Active Directory Federation Services

You must install the Active Directory Federation Services (AD FS) 3.0 software on a computer that you are preparing for the federation server role or the federation server proxy role. For more information on how you can install the AD FS software and its prerequisites, see the Microsoft documentation.

Before you begin

- Register your Windows Server 2012 server as a member server of existing domain.
- Log on to server as Domain Administrator.

Procedure

To install AD FS 3.0

1. Start Server Manager.
2. On the Menu bar, click Manage > Add Roles and Features. Add Roles and Features wizard is launched.
3. On the Before you begin page, click Next.
4. On the Select installation type page, click Role-based or feature-based installation, and then click Next.
5. On the Select destination server page, click Select a server from the server pool, and then click Next.
6. On the Select server roles page, select Active Directory Federation Services, and then click Next.
7. On the Select features page, click **Next**.

8. On the Active Directory Federation Services (AD FS) page, click **Next**.

9. On the Confirm installation settings page, verify the information, and click **Install**.
10. On the Installation progress page, you can view the installation progress. Verify the installed component, and click Close.

Configure the federation server

To configure the federation server

1. On the Server Manager Dashboard page, click the Notifications flag, and then click Configure the federation service on the server. The Active Directory Federation Service Configuration Wizard is launched.
2. On the Welcome page, select **Create the first federation server in a federation server farm**, and click **Next**.

3. On the Connect to Active Directory Domain Services page, specify an **account with domain administrator rights** for the Active Directory domain that this computer is joined to, and then click **Next**.
4. On the Specify Service Properties page, enter the following details, and click Next
   ◦ Browse to the location of your SSL certificate and import it.
   ◦ Type a Federation Service Name. This value is the same value that you provided when you enrolled an SSL certificate in Active Directory Certificate Services (AD CS).
   ◦ Type a Federation Service Display Name.
5. On the Specify Service Account page, select **Use an existing domain user account**, and click Next.

6. On the Specify Configuration Database page, select **Create a database on this server using Windows Internal Database**, and then click Next.
7. On the **Review Options** page, verify your configuration selections, and then click **Next**.
8. On the Pre-requisite Checks page, verify that all prerequisite checks were successfully completed, and then click Configure.

9. On the Results page, review the results, check whether the configuration has completed successfully.

**Configure AD FS to integrate with inSync Master**

After you have installed AD FS 3.0, perform the following actions:

1. Create trust between inSync Master and AD FS by configuring AD FS with a relying party rule, which is inSync Master.
2. Configure inSync Master to trust AD FS 3.0. The trust allows AD FS 3.0 to send claims to inSync Master.
3. Set up a web application and site to consume these claims.

**Create a relying party**

After you have set up the Federation Server, the next step is to create a relying party.

**To create a relying party**

1. On the Start menu, click Administrative Tools > AD FS 3.0 Management. The AD FS 3.0 window appears.
2. Expand the Trust Relationships node.
3. Right-click on the Relying Party Trusts folder. A list with additional options appears.
4. In the right pane, click Add Relying Party Trust. The Add Relying Party Trust Wizard appears.
5. Click **Start**. The **Select Data Source** page appears.

6. Click **Enter data about the relying party manually**, and then click **Next**. The **Specify Display Name** page appears.
7. Provide the appropriate information for each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Type a display name for the relying party.</td>
</tr>
<tr>
<td></td>
<td>For example, <strong>Druva inSync</strong>.</td>
</tr>
<tr>
<td>Notes</td>
<td>Type a description for the relying party.</td>
</tr>
</tbody>
</table>
8. Click **Next**. The **Choose Profile** page appears.

9. Select **AD FS profile** and click **Next**. The **Configure Certificate** page appears.
10. *(Optional)* If you want to encrypt the SAML token, browse and select the certificate, and then click **Next**. However, AD FS establishes a secure SSL connection to Druva inSync, which ensures the token is encrypted. Click **Next**.
11. The **Configure URL** page appears.
Select the **Enable support for the SAML 2.0 WebSSO 2.0 protocol** check box.

12. Click **Next**. The **Configure Identifiers** page appears.

13. In the **Relying party trust identifier** box, type:

```
https://<IP/FQDN of Master or Edge Server>/wrsaml/consume
```

For inSync On-Premises, you must add "https://" as a prefix to the Relying Party trust identifier.

The web application passes this realm to the AD FS when users log into the web restore URL.
14. Click Next. The Configure Multifactor Authentication Now? page appears. Select I do not want to configure MFA settings for this relying party trust at this time and click Next.

Note: If you want to configure Multifactor Authentication, you can do it at a later stage.
15. Click Next. The **Choose Issuance Authorization Rules** page appears.

16. Click **Permit all users to access this relying party** and then click Next. The **Ready to Add Trust** page appears.
For Single-Sign-On, ensure you enter the following details for Relying Party Trust:

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Type, http://&lt;IP/FQDN of Master or Edge Server&gt;</td>
</tr>
<tr>
<td>Endpoints</td>
<td>Type, http://&lt;IP/FQDN of Master or Edge Server&gt;/wrsaml/consume</td>
</tr>
</tbody>
</table>
| Accepted Claims  | • AD_Rule  
|                  | • SAML_Token  
|                  | • email-Transform  |
17. Review the other properties and if required update the settings that you have configured, and click Next. The Finish page appears.

18. Ensure that the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box is by default selected.

19. Click Close.

Create a new claim

To create a new claim


2. In the Claim rule template list, select **Send LDAP Attributes as Claims**, and then click Next.

3. The Add Transform Claim Rule Wizard window appears.
4. Provide the appropriate information for each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim rule name</td>
<td>Type a name for the claim rule.</td>
</tr>
<tr>
<td>Attribute store</td>
<td>In the list, select Active Directory</td>
</tr>
<tr>
<td>Mapping of LDAP attributes to outgoing claim types</td>
<td></td>
</tr>
<tr>
<td>LDAP Attribute</td>
<td>Map it to Outgoing claim type.</td>
</tr>
<tr>
<td>E-mail Addresses</td>
<td>Map it to E-mail Address.</td>
</tr>
<tr>
<td>E-mail Addresses</td>
<td>Map it to Name ID.</td>
</tr>
<tr>
<td>User-Principal-Name</td>
<td>Map it to Name.</td>
</tr>
</tbody>
</table>

5. Click Finish.
To create a new claim for Transform_rules


2. In the Claim rule template list, select Transform an Incoming Claim, and then click Next. The Edit Rule – Email-Transform window appears.
3. Provide the appropriate information for each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim rule name</td>
<td>Type a name for the claim rule.</td>
</tr>
<tr>
<td>Incoming claim type</td>
<td>Map it to E-mail Address.</td>
</tr>
<tr>
<td>Outgoing claim type</td>
<td>Map it to Name ID.</td>
</tr>
<tr>
<td>Outgoing name ID format</td>
<td>Map it to Email.</td>
</tr>
</tbody>
</table>

4. Click Finish.

Create a custom rule

To create a custom rule

2. In the Claim rule template list, select Send Claims Using a Custom Rule, and then click Next. The Edit Rule – Authentication window appears.

3. Provide the appropriate information for each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim rule name</td>
<td>Type a name for the custom rule.</td>
</tr>
<tr>
<td>Custom rule</td>
<td>Type,</td>
</tr>
<tr>
<td></td>
<td>=&gt; issue(Type = &quot;insync_auth_token&quot;, Value = &quot;value of SSO Token generated from inSync Console&quot;);</td>
</tr>
</tbody>
</table>
4. Click **OK**.

### Configure Single sign-on

#### Prerequisite to configure Single sign-on

Before you configure the single sign-on settings with inSync Master, download the metadata.xml file from:

https://<adfs fqdn>/federationmetadata/2007-06/federationmetadata.xml

#### Configure the single sign-on settings

To configure the single sign-on settings
1. On the inSync Master Management Console menu bar, click
   ![Settings]
   > Settings.
2. Click the Single Sign-on tab and then click Edit.
3. Provide the following appropriate information.

<table>
<thead>
<tr>
<th>SAML Attribute</th>
<th>Description and value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID Provider Login URL</td>
<td>Type,</td>
</tr>
<tr>
<td></td>
<td>https://&lt;ADFS FQDN&gt;/adfs/lr</td>
</tr>
<tr>
<td>ACS</td>
<td>Type,</td>
</tr>
<tr>
<td></td>
<td>&lt;inSync Master or Edge IP/FQDN&gt;</td>
</tr>
<tr>
<td>ID Provider Metadata XML</td>
<td>Copy and paste the contents of the federationmetadata.xml file.</td>
</tr>
<tr>
<td>AuthnRequests Signed</td>
<td>Select this checkbox, if you want signed SAML Authentication Requests.</td>
</tr>
<tr>
<td></td>
<td>By default, SAML Authentication Requests are not signed.</td>
</tr>
</tbody>
</table>
4. Click Save.

Note: The last step to setup SSO with AD FS requires changes in the configuration files. To verify and complete the configuration contact [Druva Support](https://docs.druva.com/010_002_inSync_On-premise/inSync_On-Premise_5.8/060_Reports_Troubleshoot/120_FAQs/How_to_install_and_configure_AD_FS_3.0_with_Single_Sign-On).