



AMP FOR ENDPOINTS SSO FOR ACTIVE DIRECTORY

Overview

The AMP for Endpoints Single Sign-On (SSO) feature streamlines the user login process while enhancing security. This user guide will help you configure your AMP for Endpoints Console to use SSO with Active Directory.

Set Up Active Directory 2012 ADFS

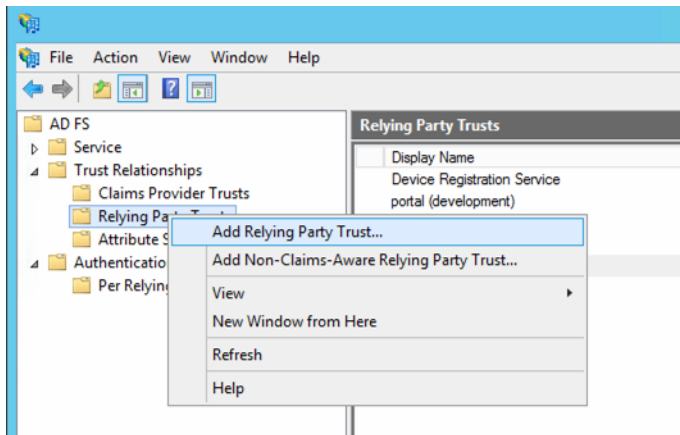
This guide assumes you have already completed your Active Directory Federation Service (ADFS) connection with the AMP for Endpoints Console. There are additional steps required to complete the setup.

For additional information on setting up and using ADFS see the [AD FS Content Map Technet Article](#).

Add a Relying Party Trust

Once you have set up the ADFS connection, the connection between ADFS and the AMP for Endpoints console is defined using a **Relying Party Trust (RPT)**.

1. Select the **Relying Party Trusts** folder from ADFS Management and add a new Relying Party Trust from the **Actions** sidebar.



2. Click Start on the wizard to begin the setup.

3. Choose **Import data about the relying party published online** and enter the entity ID URL. In the example shown, this is: `https://auth.amp.cisco.com/auth/metadata/service_provider`.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The window is divided into two main sections. On the left is a 'Steps' pane with a list of steps: 'Welcome', 'Select Data Source' (highlighted with a green dot), 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area on the right is titled 'Select Data Source' and contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' (selected with a black dot). Below this is the instruction: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' followed by a text field labeled 'Federation metadata address (host name or URL):' containing the URL 'https://auth.amp.cisco.com/auth/metadata/service_provider'. Below the text field is an example: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Below this is the instruction: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' followed by a text field labeled 'Federation metadata file location:' and a 'Browse...' button. 3. 'Enter data about the relying party manually'. Below this is the instruction: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right of the main area are three buttons: '< Previous', 'Next >', and 'Cancel'.

4. Click **Next** and verify the Display name (ensuring it is one that you will recognize in the future), along with any notes you may want to make.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (current step), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text box containing 'auth.amp.cisco.com'. Below the text box is a 'Notes:' label followed by a large text area. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

5. On the next screen, you can configure multi-factor authentication but it is not required at this stage. Click **Next**.

6. On the **Choose Issuance Authorization Rules** screen, select **Permit all users to access the relying party**. Click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Choose Issuance Authorization Rules'. On the left, a 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules (highlighted), Ready to Add Trust, and Finish. The main area contains text explaining that issuance authorization rules determine whether a user is permitted to receive claims. It offers two options: 'Permit all users to access this relying party' (selected with a radio button) and 'Deny all users access to this relying party'. Below these options, a note states: 'You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.' At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'.

7. Configuration of the relying party trust is now complete. On the **Advanced** tab select SHA-256 for the **Secure hash algorithm**.

The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Ready to Add Trust' step. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Ready to Add Trust'. The 'Steps' pane on the left is the same as in the previous screenshot, with 'Ready to Add Trust' highlighted. The main area contains text: 'The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.' Below this text is a tabbed interface with tabs for Encryption, Signature, Accepted Claims, Organization, Endpoints, Notes, and Advanced (selected). The 'Advanced' tab displays the text 'Specify the secure hash algorithm to use for this relying party trust.' and a dropdown menu labeled 'Secure hash algorithm:' with 'SHA-256' selected. At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'.

8. On the Monitoring tab make sure the metadata URL is correct..

The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Monitoring' tab selected. The 'Ready to Add Trust' section on the left lists the steps: Welcome, Select Data Source, Specify Display Name, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area displays the following information:

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note < >

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

☒ Monitor relying party

☒ Automatically update relying party

This relying party's federation metadata data was last checked on:
6/5/2017

This relying party was last updated from federation metadata on:
6/5/2017

< Previous Next > Cancel

9. On the Encryption tab verify the certificate information.

The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Encryption' tab selected. The 'Ready to Add Trust' section on the left lists the steps: Welcome, Select Data Source, Specify Display Name, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area displays the following information:

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Note < >

Specify the encryption certificate for this relying party trust.

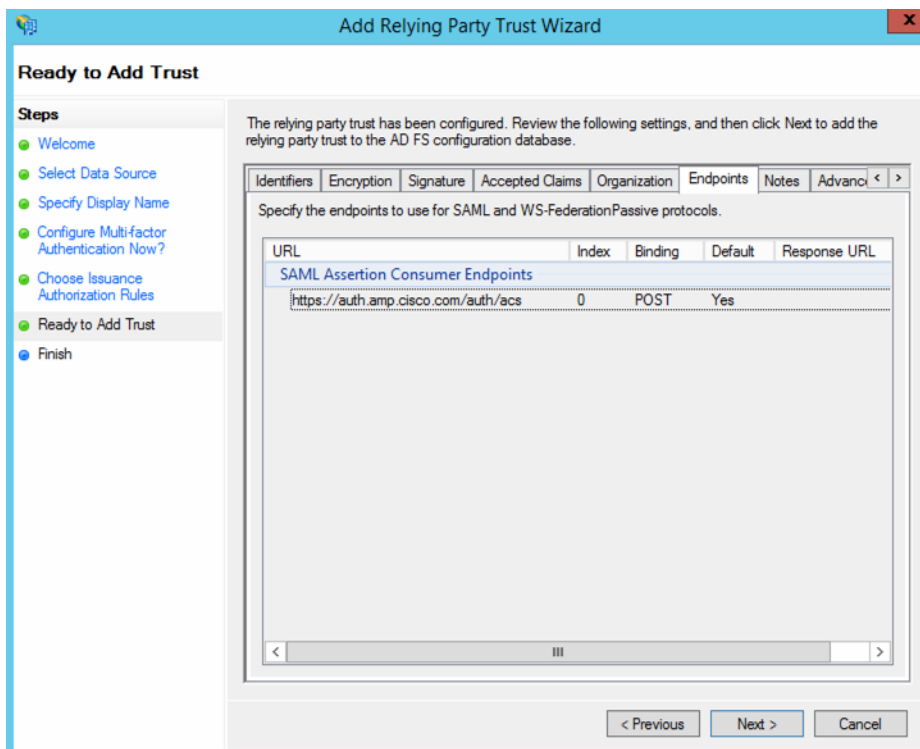
Encryption certificate:

Issuer: CN=HydrantID SSL ICA G2, O=HydrantID (Avalanche Cloud Corporation), C=US
Subject: CN=sso.amp.cisco.com, O="Cisco Systems, Inc.", L=San Jose, S=CA, C=US
Effective date: 11/22/2016 8:16:27 AM
Expiration date: 11/22/2018 8:16:22 AM

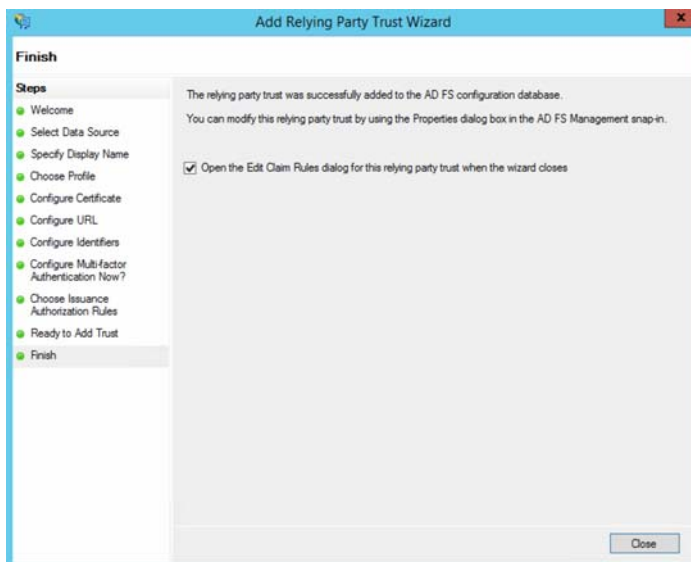
View...

< Previous Next > Cancel

10. Check the Endpoints tab. Once you are satisfied that the settings are correct, click **Next**.

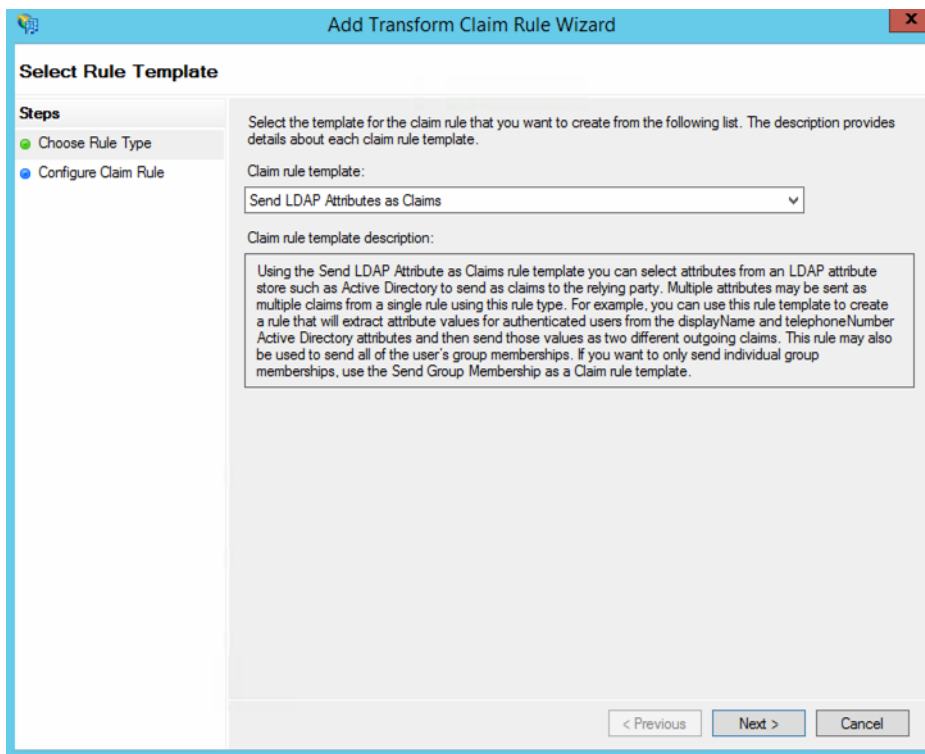


11. On the final screen, click the **Open the Edit Claim Rules** check box then click **Close**.



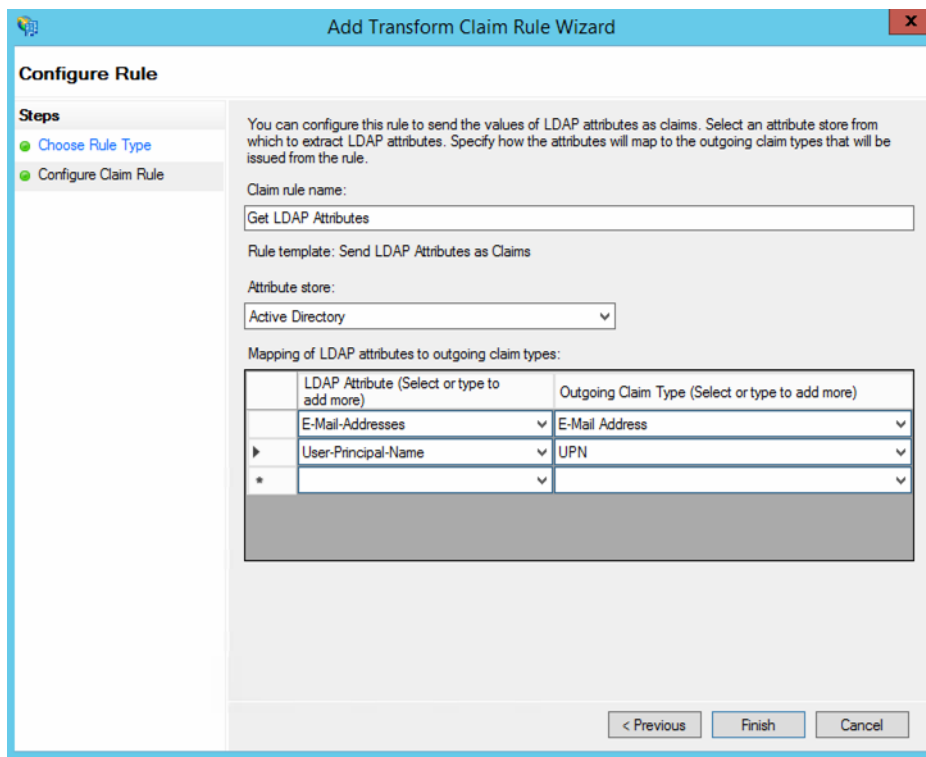
Create a Claim Rule

1. In the **Edit Claim Rules** dialog, click on **Add Rule**. This will open the **Choose Rule Template** screen. In the **Claim rule template** drop-down, click **Send LDAP Attributes as Claims**. Click next to go to the **Configure Claim Rule** screen.



2. On the **Configure Claim Rule** screen, select **Active Directory** as your attribute store. Then do the following:
 - a. In the first row of the **LDAP Attribute** column, select **E-Mail Addresses**.
 - b. In the first row of the **Outgoing Claim Type** column, select **E-Mail Address**.
 - c. In the second row, of the **LDAP Attribute** column, select **User-Principal Name**.
 - d. In the second row of the **Outgoing Claim Type** column, select **UPN**.

3. Click **Finish** to save the new rule.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Get LDAP Attributes

Rule template: Send LDAP Attributes as Claims

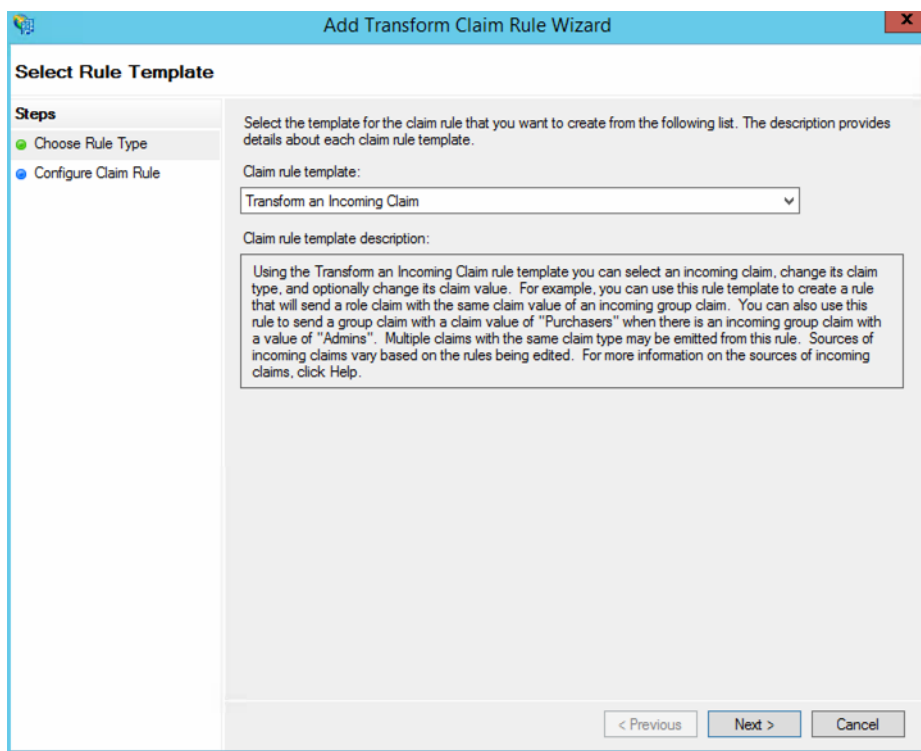
Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	E-Mail Address
▶	User-Principal-Name	UPN
*		

< Previous Finish Cancel

4. In the **Edit Claim Rules** dialog, click on **Add Rule**. Under the **Claim rule template**, select **Transform an Incoming Claim**.



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:
Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

< Previous Next > Cancel

5. On the next screen, Configure Rule:

- a. For **Incoming claim type**, select **E-mail Address**.
- b. For **Outgoing claim type**, select **Name ID**.
- c. For **Outgoing name ID format**, select **Email**.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The 'Steps' pane on the left shows 'Choose Rule Type' and 'Configure Claim Rule'. The main area contains instructions and configuration options. The 'Claim rule name' is 'Map Email address to NameID'. The 'Rule template' is 'Transform an Incoming Claim'. The 'Incoming claim type' is 'E-Mail Address', 'Incoming name ID format' is 'Unspecified', 'Outgoing claim type' is 'Name ID', and 'Outgoing name ID format' is 'Email'. Three radio buttons are present: 'Pass through all claim values' (selected), 'Replace an incoming claim value with a different outgoing claim value', and 'Replace incoming e-mail suffix claims with a new e-mail suffix'. The 'Finish' button is highlighted.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Map Email address to NameID

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

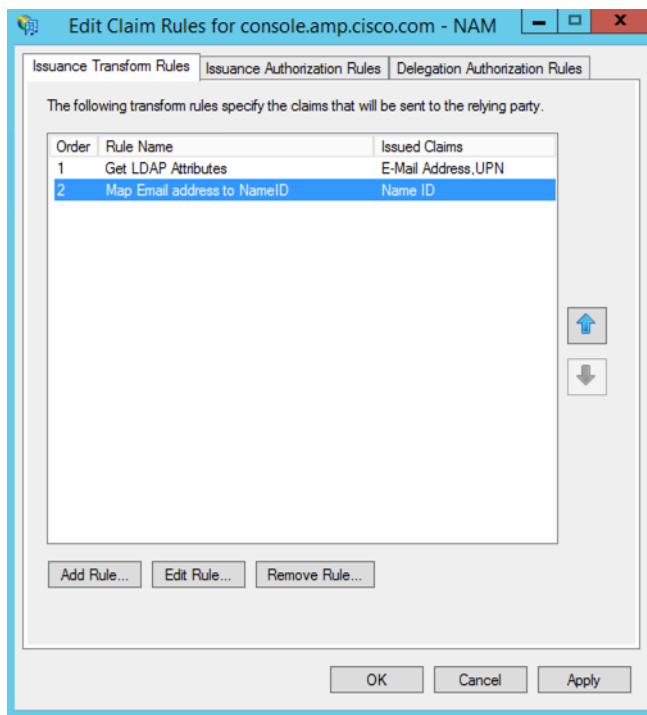
☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix: Example: fabrikam.com

< Previous Finish Cancel

- 6. Leave Pass through all claim values checked, as it is by default. Click Finish.**

7. The **Edit Claim Rules** dialog should appear as follows. Click **OK** to finish creating the rules.



Adjusting the Trust Settings

You still need to adjust a few settings on your Relying Party Trust. To access these settings, select **Relying Party Trust** and select **Properties** from the **Actions** sidebar. In the **Advanced** tab, make sure **SHA-256** is specified as the **secure hash algorithm**.