Configure Tenable Vulnerability Management with ADFS SAML

For FedRAMP and Non-FedRAMP Customers

Last Revised: November 07, 2023

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Prerequisites

In this walkthrough, we use the DNS FQDN of adfs.example.com as the ADFS instance we are configuring. Consider that your DNS FQDN may vary when observing the steps in this guide.

This document assumes that you have previously setup and configured an ADFS instance on a set of no less than two AD Domain controllers running on Windows Server 2022:

- ADFS Main AD DC
- ADFS Web Application Proxy (WAP)

Microsoft Documentation can assist you with setting up the ADFS instances on an existing Microsoft Active Directory Domain Controller.

This document also assumes that your ADFS Main AD DC runs Active Directory Domain Services (dcpromo), includes a Certificate Authority setup, and is properly configured.

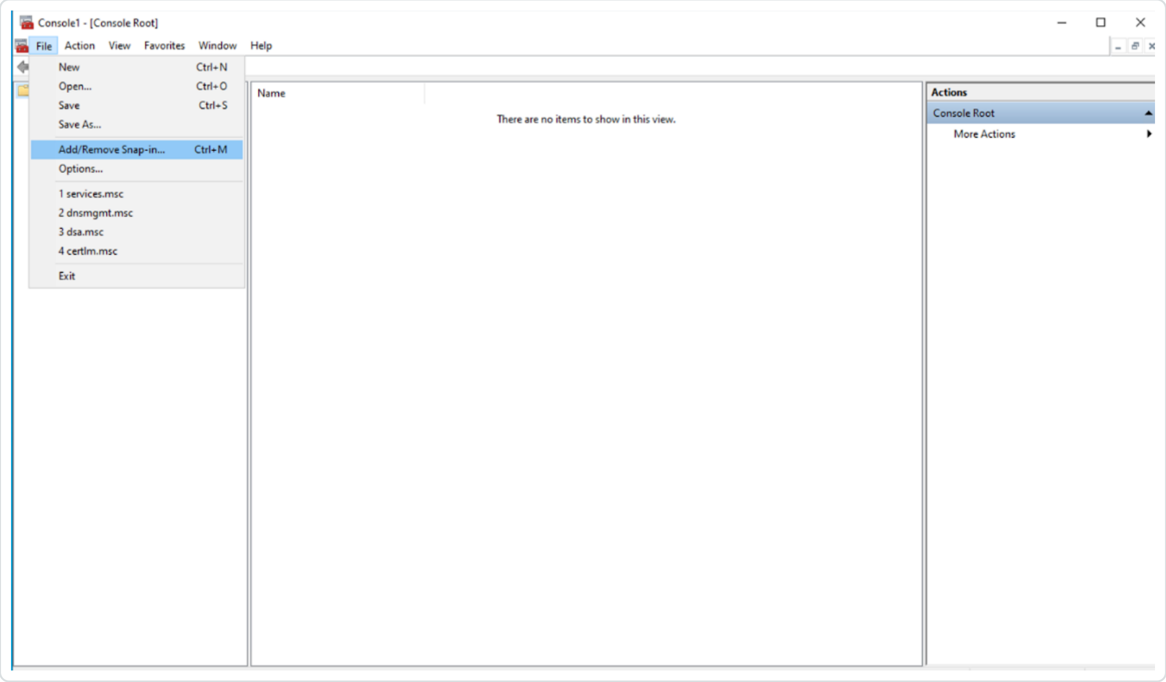
> **Note:** This document assumes you update your certificates for your Active Directory Certificate Authority and your ADFS instance on a yearly basis, so that your certificate lifespan is set to one year. Your actual configuration options may vary. Please keep this in mind to avoid issues with expiring certificates when configuring your instance.

Configure MMC to Manage ADFS

To configure the Microsoft Management Console (MMC) to manage ADFS:

1. Open the MMC.exe console.

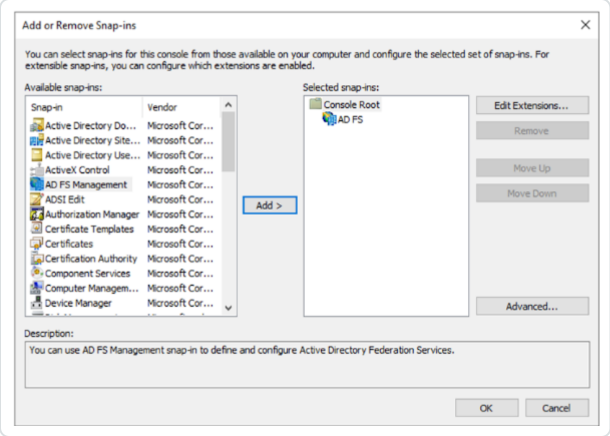
2. Click **File** > **Add/Remove Snap-in**.



There are no items to show in this view.

The **Add or Remove Snap-ins** window appears.

3. In the **Available Snap-ins** section, select the **ADFS Management** option and click **Add**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
AD FS Management	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...

Selected snap-ins:

- Console Root
  - AD FS

Description:

You can use AD FS Management snap-in to define and configure Active Directory Federation Services.

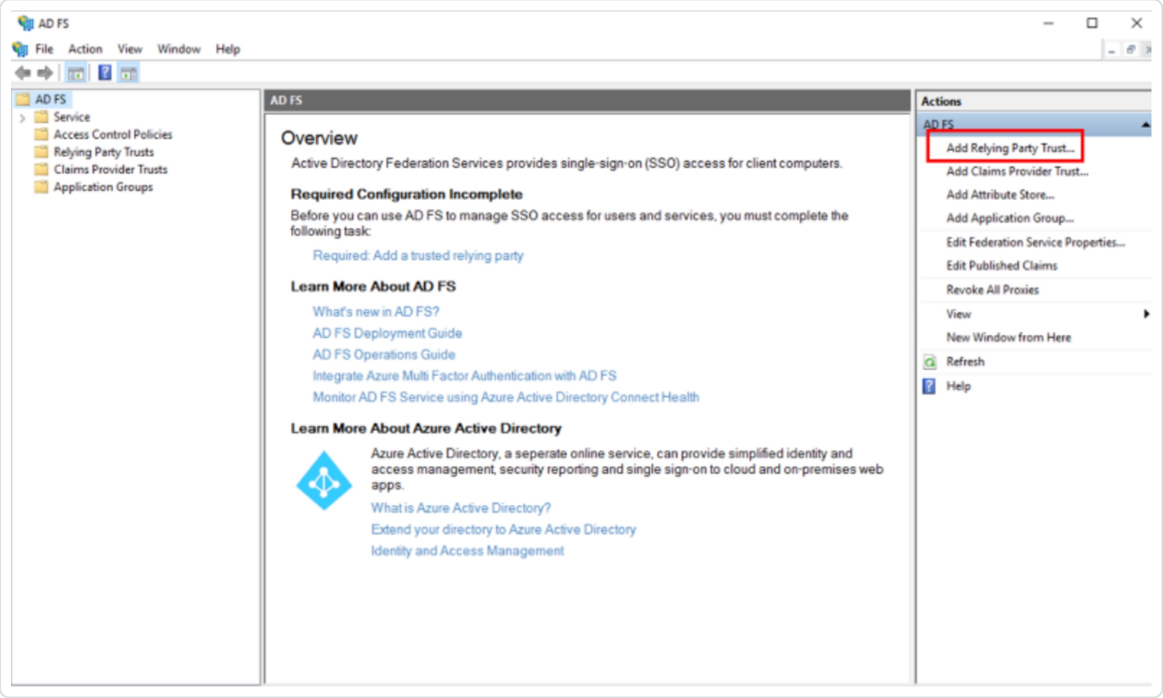
The console adds the snap-in to the **Selected Snap-in**s section.

4. Click **OK**.

Configure an ADFS Relying Party Trust

To configure an ADFS Relying Party Trust:

1. Open the MMC.exe console.
2. On the right side of the console, in the **Actions** section, click **Add Relying Party Trust**.

   Overview

   Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

   Required Configuration Incomplete

   Before you can use AD FS to manage SSO access for users and services, you must complete the following task:

   Required: Add a trusted relying party

   Learn More About AD FS

   What's new in AD FS?
   AD FS Deployment Guide
   AD FS Operations Guide
   Integrate Azure Multi Factor Authentication with AD FS
   Monitor AD FS Service using Azure Active Directory Connect Health

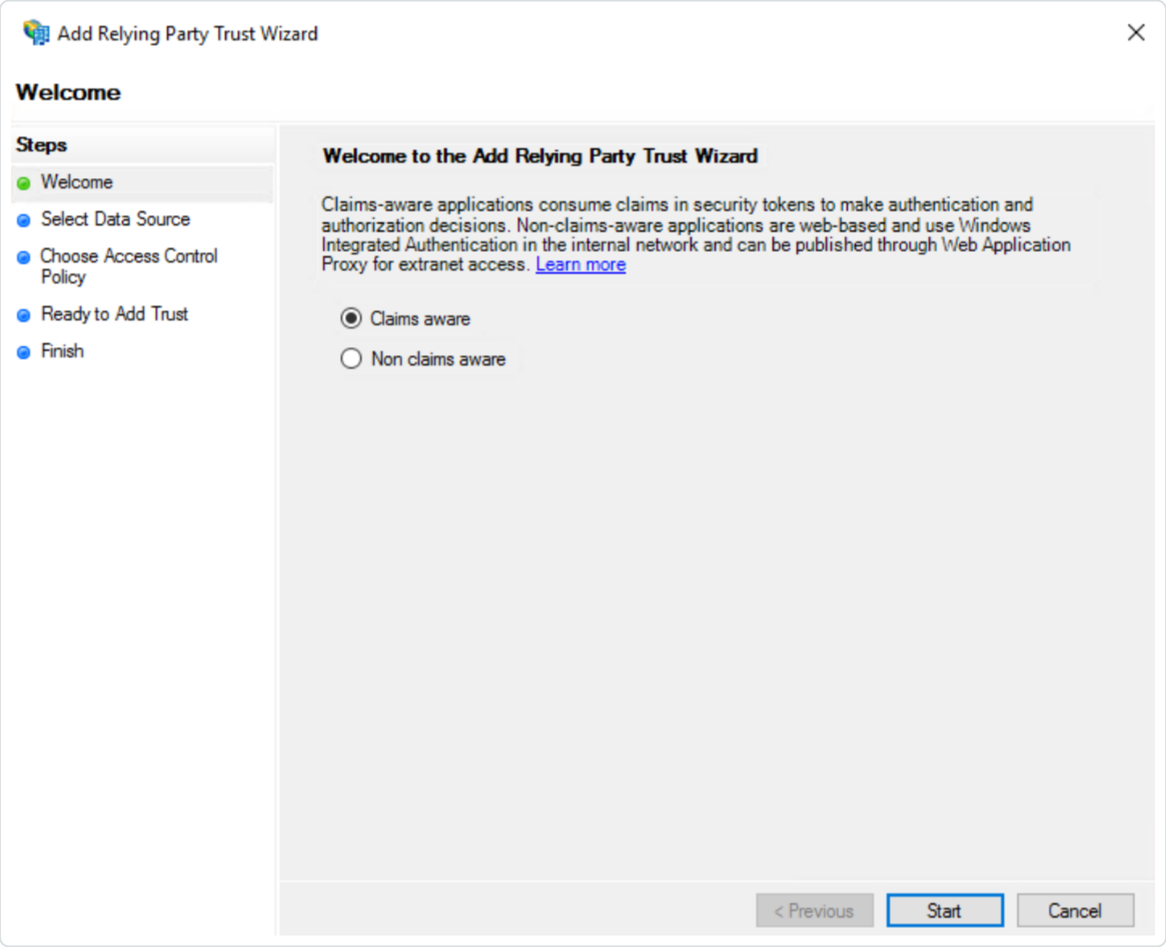
   Learn More About Azure Active Directory

   Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.

   What is Azure Active Directory?
   Extend your directory to Azure Active Directory
   Identity and Access Management

   The **Add Relying Party Trust** wizard appears.

3. In the wizard, select the **Claims aware** radio button.



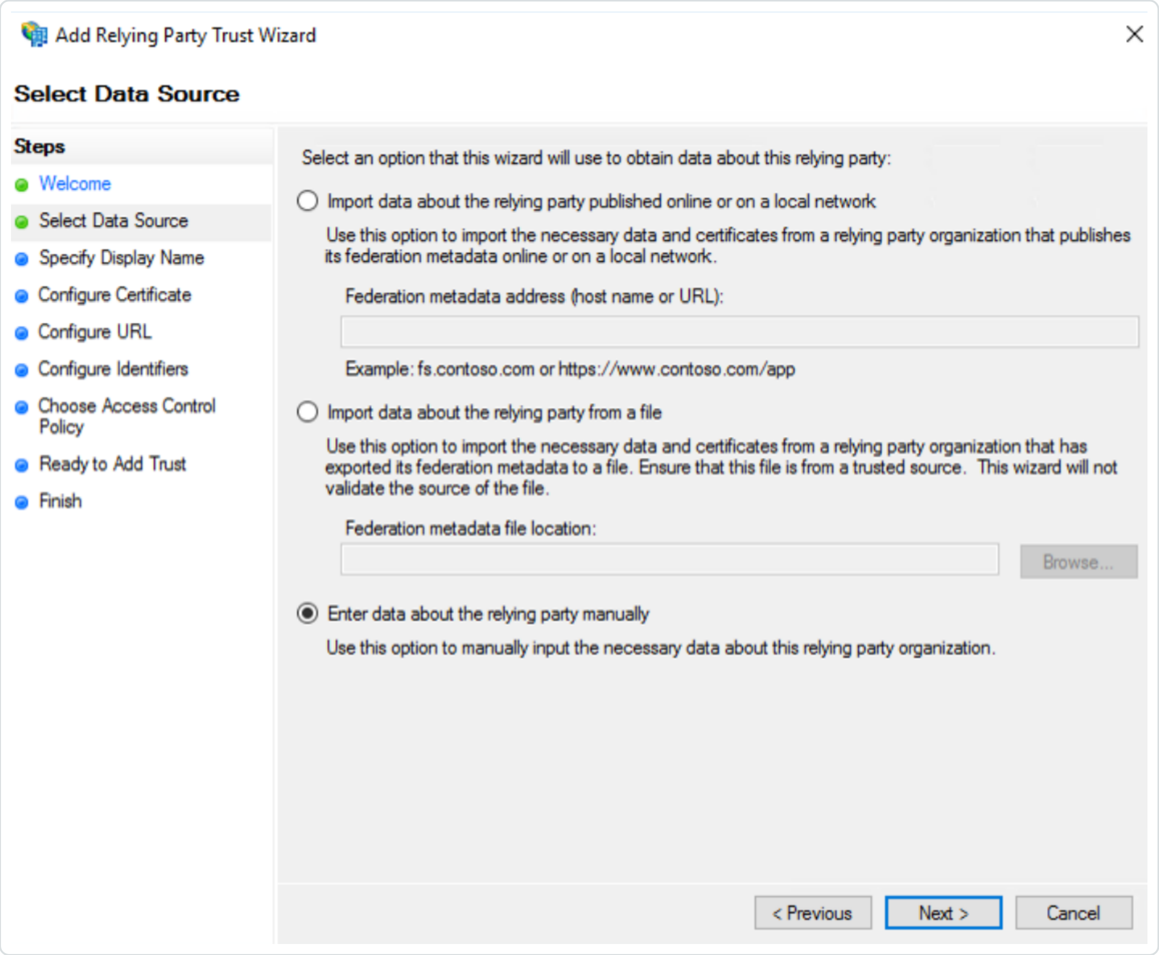
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

4. Click **Start**.
5. On the **Select Data Source** page, select the **Enter data about the relying party manually** radio button.



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

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.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

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.

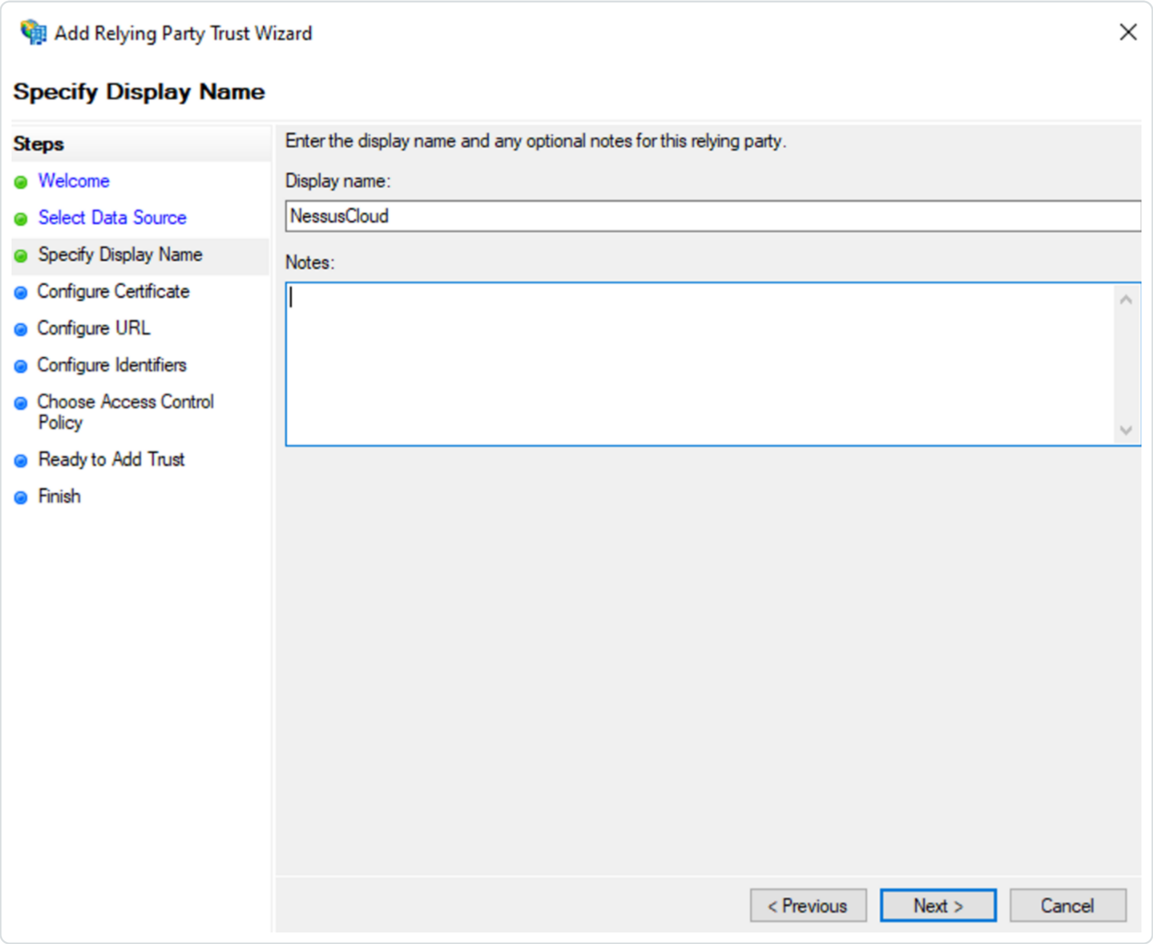
Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

6. Click **Next**.

7. On the **Specify Display Name** page, type a **Display Name** and any **Notes** you want to include.



Enter the display name and any optional notes for this relying party.

Display name: NessusCloud

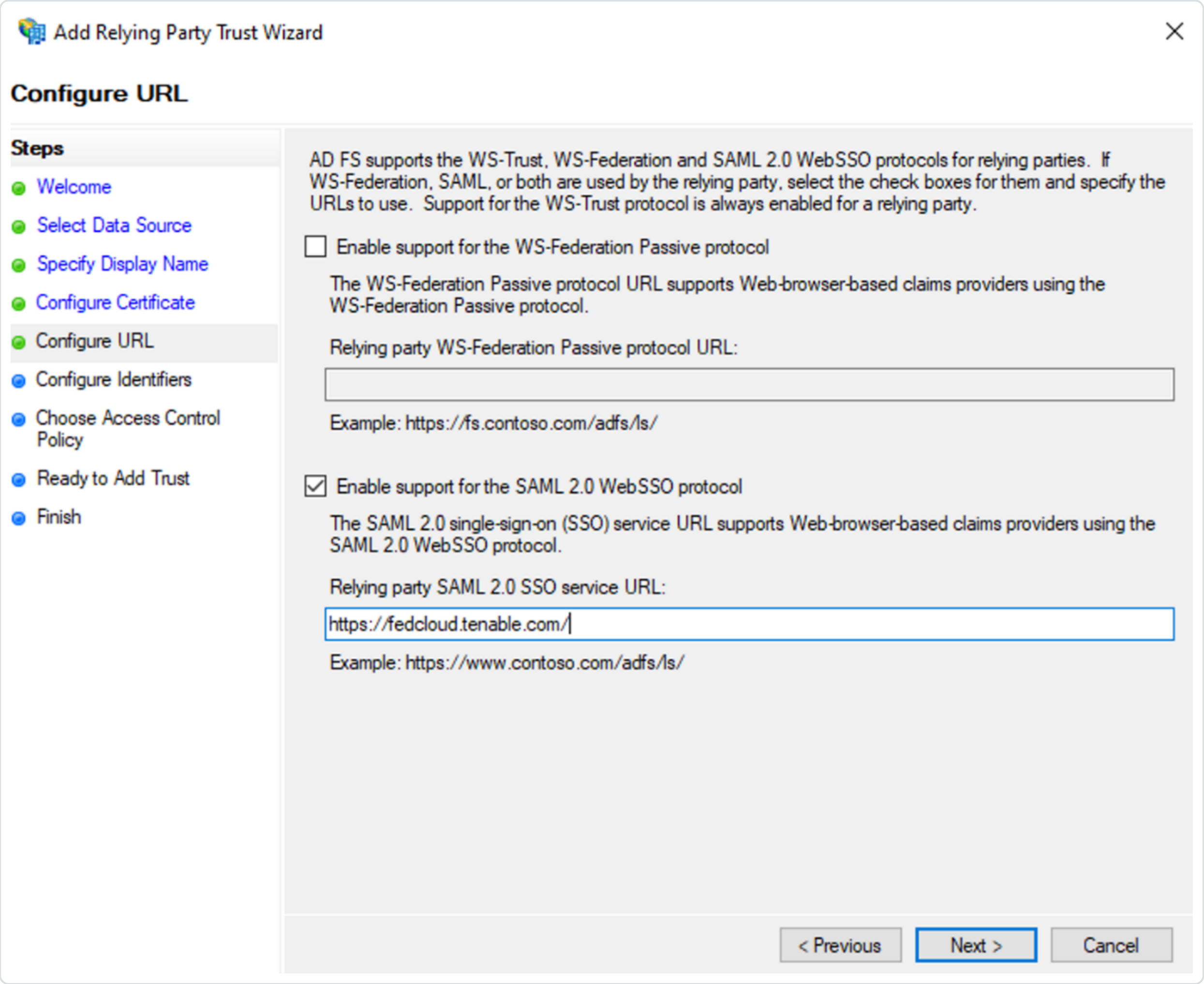
Notes:

8. Click **Next**.

9. Because the configuration is already encrypted, on the **Configure Certificate** page, do not make any changes.

10. Click **Next**.

11. On the **Configure URL** page, type the appropriate service URL. In this example, we use *https://fedcloud.tenable.com*.



Add Relying Party Trust Wizard

Configure URL

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

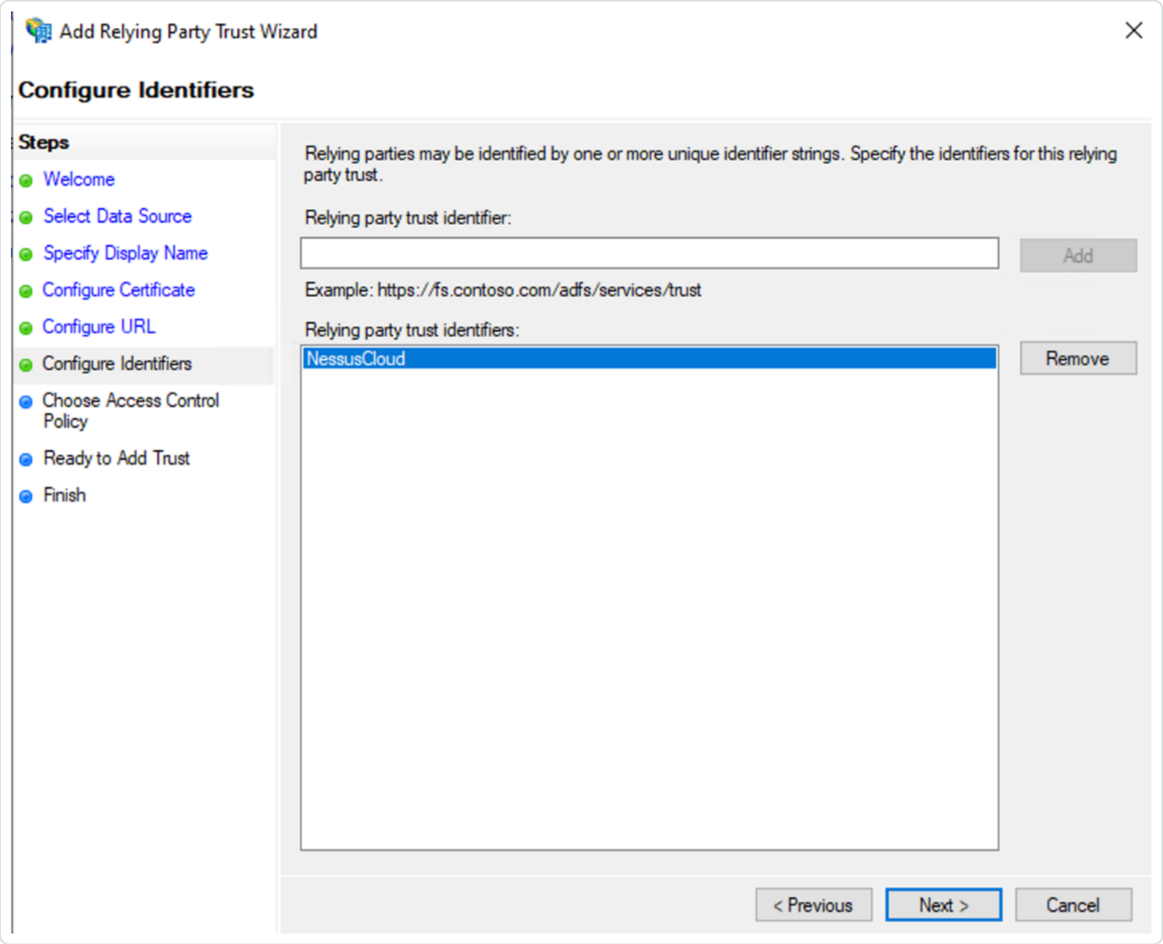
https://fedcloud.tenable.com/

Example: https://www.contoso.com/adfs/ls/

> **Note:** For FedRAMP deployments, your Tenable sales representative provides this URL. For non-FedRAMP deployments, you must first configure SAML in Tenable Vulnerability Management to determine the appropriate URL.

12. Click **Next**.

13. On the **Configure Identifiers** page, in the **Relying party trust identifier** text box, type the SP Entity ID to which you connected as the Relying Party Trust identifier.



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

NessusCloud

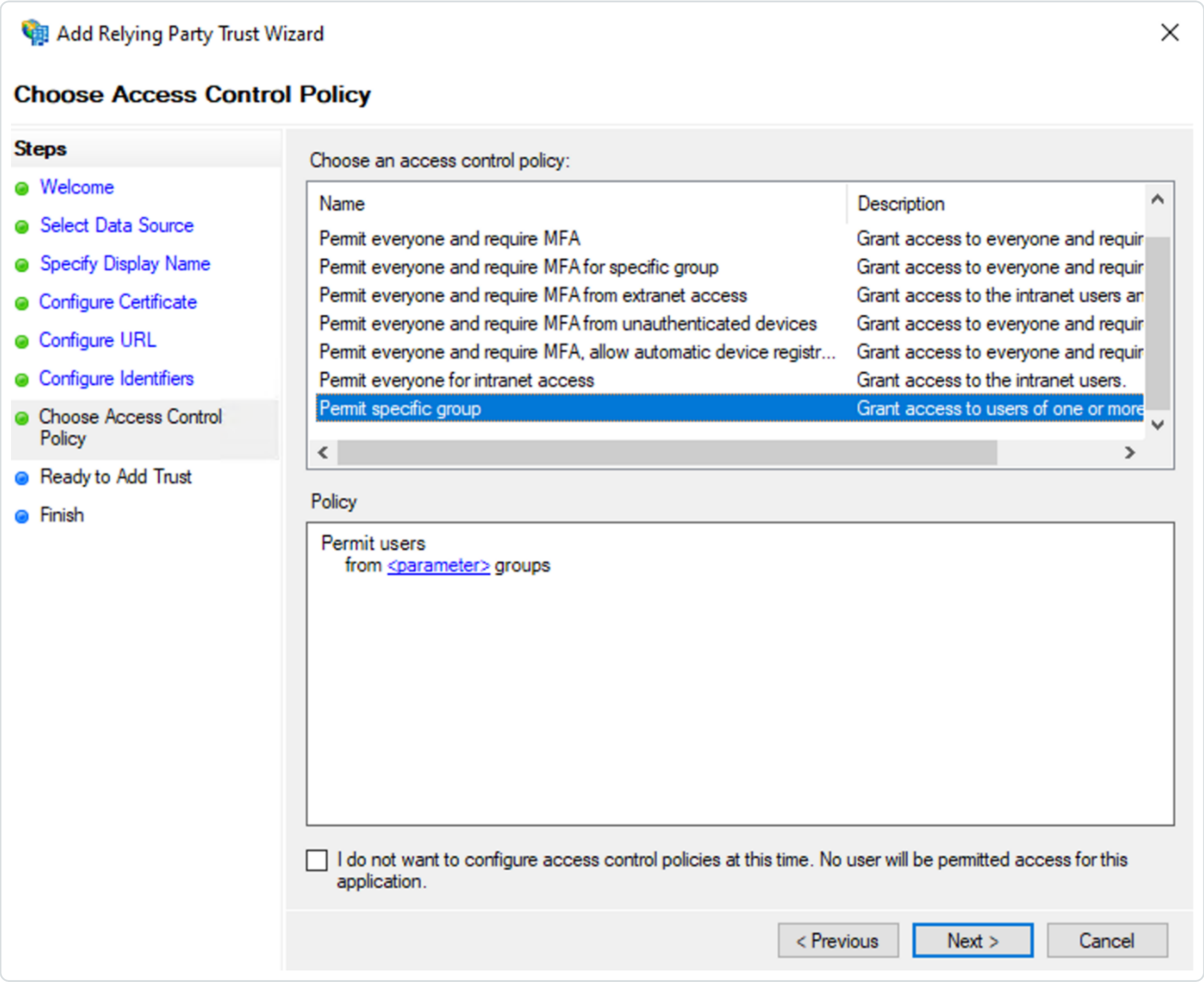
14. Click **Add**.

    The wizard adds the identifier to the **Relying party trust identifiers** section.

15. Click **Next**.

16. On the **Choose Access Control Policy** page, select the appropriate access control policy for your environment.

    > **Note:** In some cases, you may select **Permit Everyone** and let the application determine access. In other cases, you may select **Permit a specific group** to access the relying party. In this example, we choose the latter.



Choose Access Control Policy

Choose an access control policy:

Name	Description
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

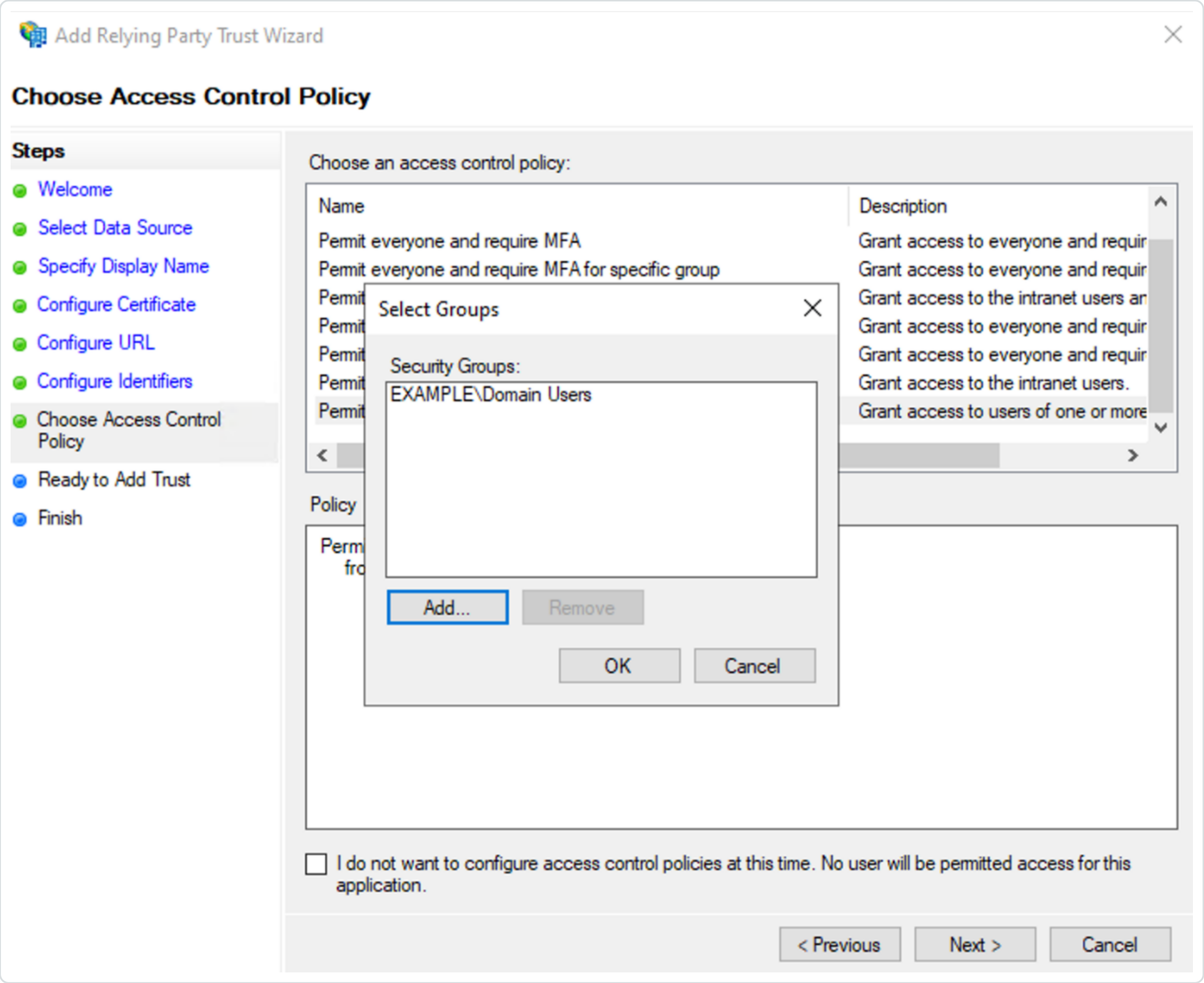
Permit users
from <parameter> groups

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

17. In the **Policy** section, click the **<parameter>** hyperlink.

    The **Select Groups** window appears.

18. In the **Select Groups** window, add the specific AD group to which you want to grant access.



Choose an access control policy:

Name	Description
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit	Grant access to the intranet users ar
Permit	Grant access to everyone and requir
Permit	Grant access to everyone and requir
Permit	Grant access to the intranet users.
Permit	Grant access to users of one or more

Select Groups

Security Groups:

EXAMPLE\Domain Users

Perm
fro

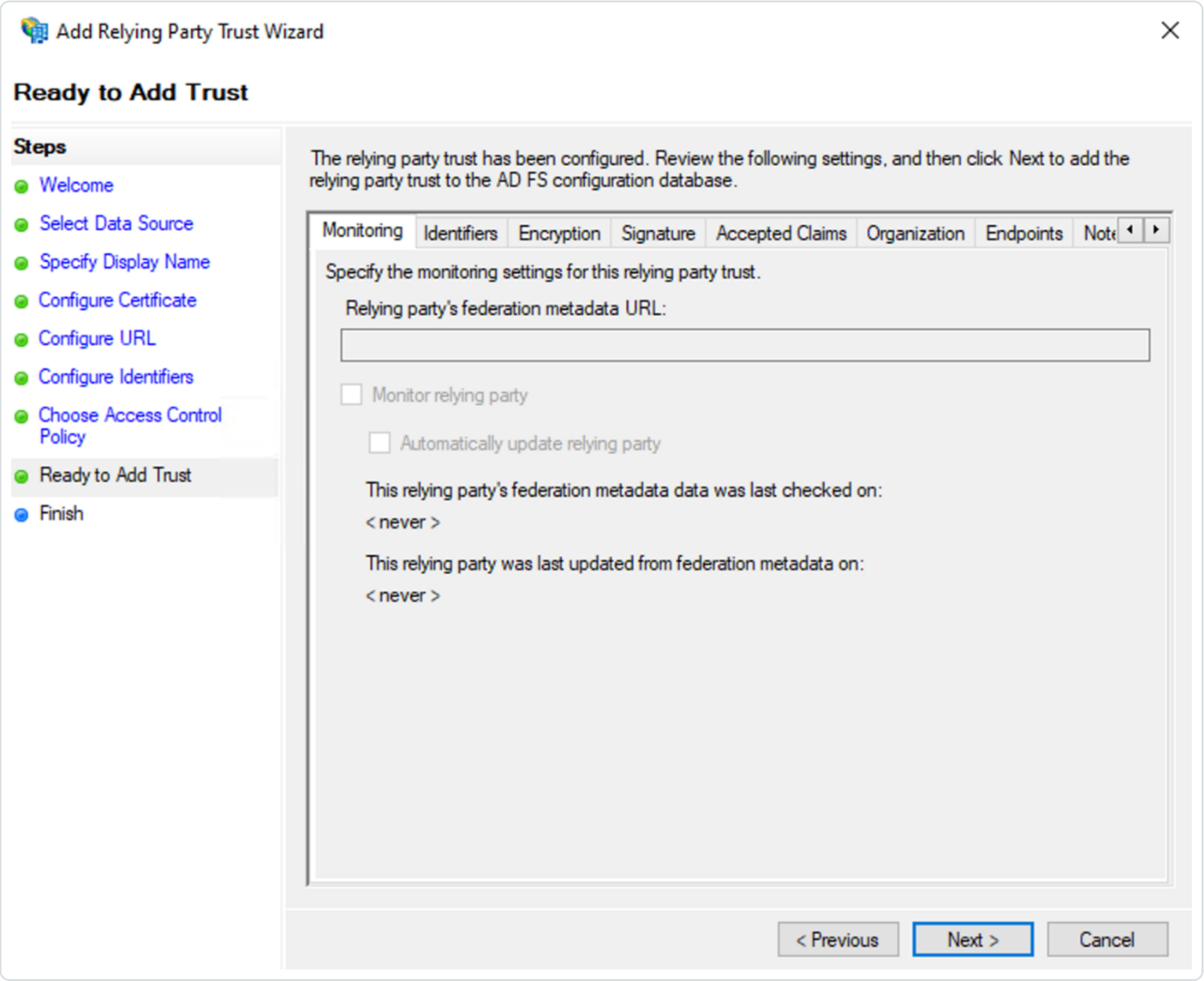
☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

19. Click **OK**.

    The wizard adds the selected group where the **<parameter>** hyperlink previously was.

20. Click **Next**.

21. On the **Ready to Add Trust** page, review your configuration.



Ready to Add Trust

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.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

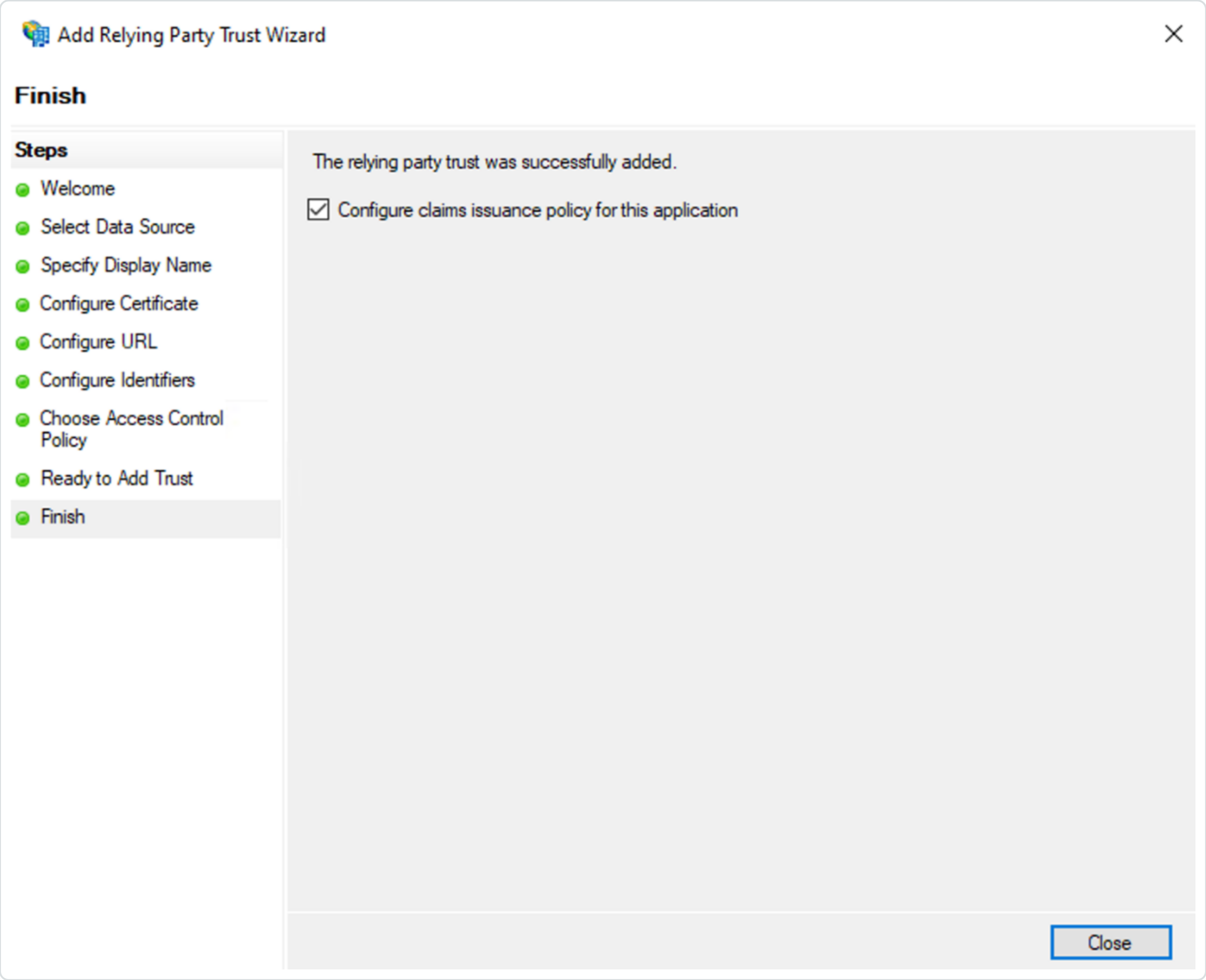
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

22. Click **Next**.
23. On the **Finish** page, select the **Configure claims insurance policy for this application** check box.



The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

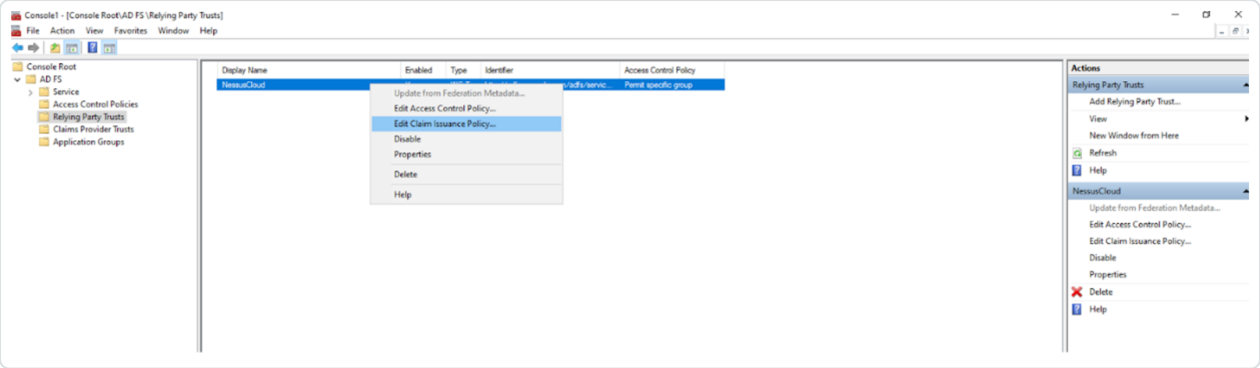
24. Click **Close**.

Configure ADFS Relying Party Claim Rules

Once you configure the ADFS Relying Party Trust, you must then configure the ADFS Relying Party Claim rules to allow proper communication.

To configure ADFS Relying Party Claim rules:

1. Open the MMC.exe console.
2. In the **Relying Party Trusts** folder, right-click the trust and select **Edit Claim Issuance Policy**.

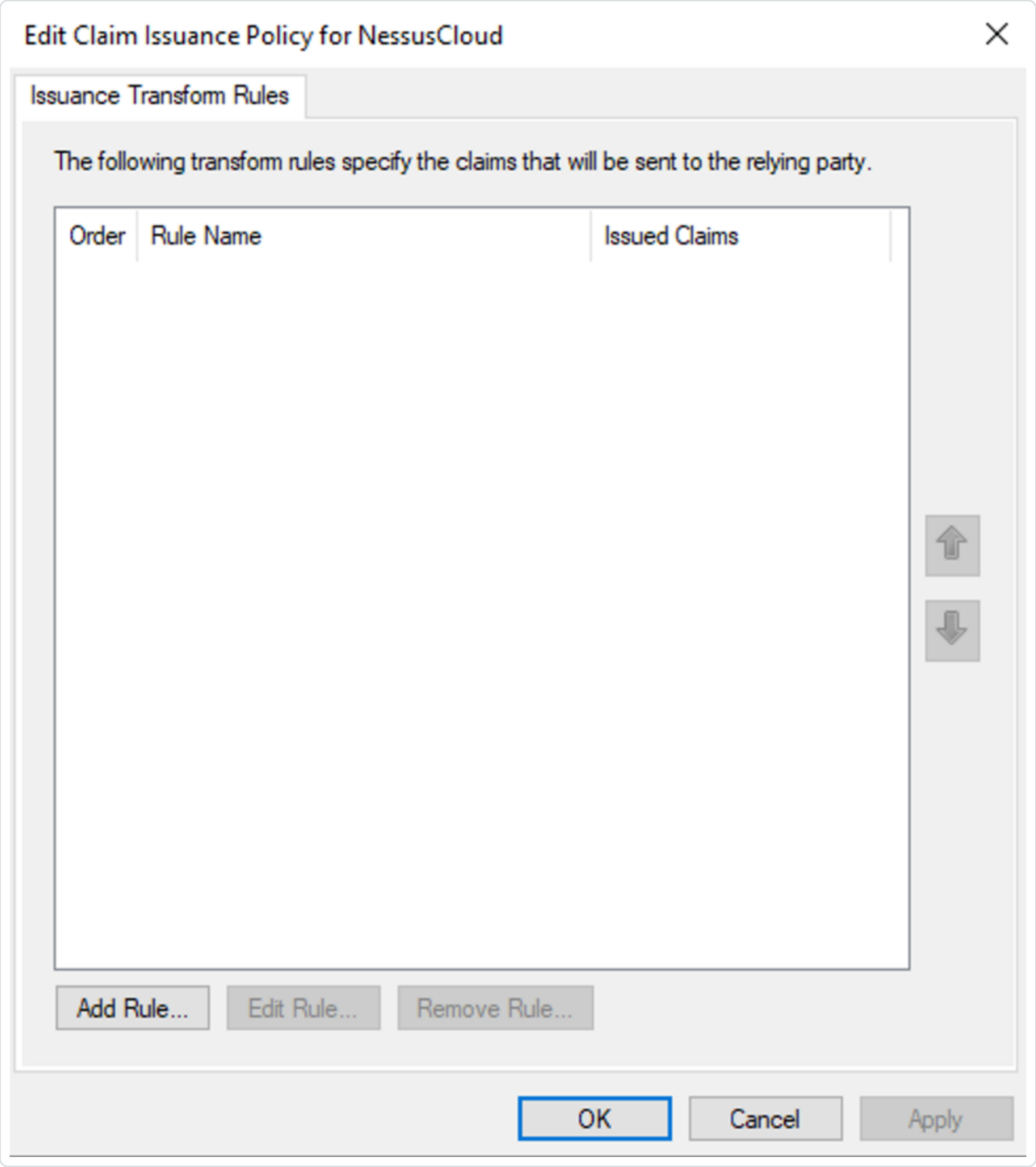


   The **Edit Claims Issuance Policy** window appears.

3. Configure two rules:

- Rule one:

  a. Click **Add Rule**.



Edit Claim Issuance Policy for NessusCloud

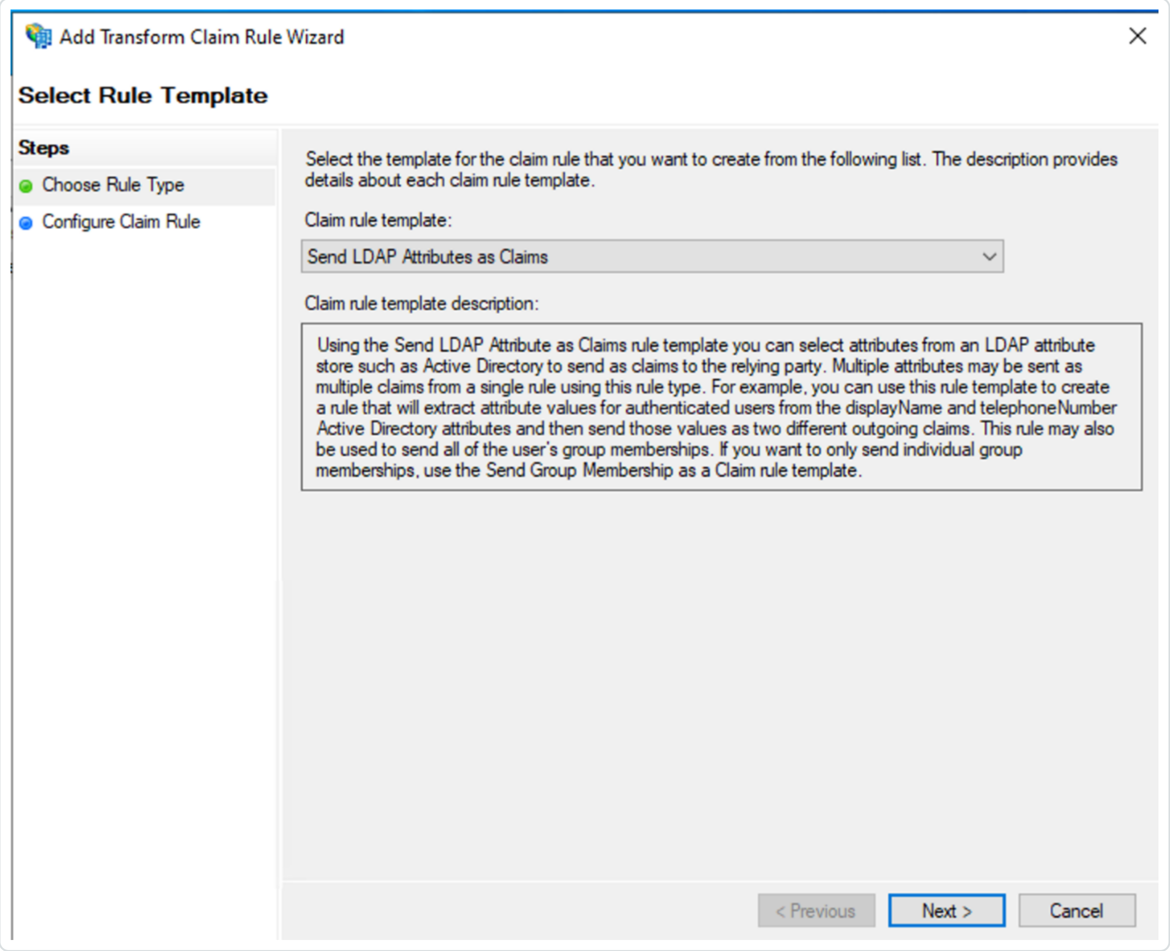
Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

The **Transform Claim Rule** wizard appears.

b. On the **Select Rule Template** page, in the **Claim rule template** drop-down, select **Send LDAP Attributes as Claims**.



Select Rule Template

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:

Send LDAP Attributes as Claims

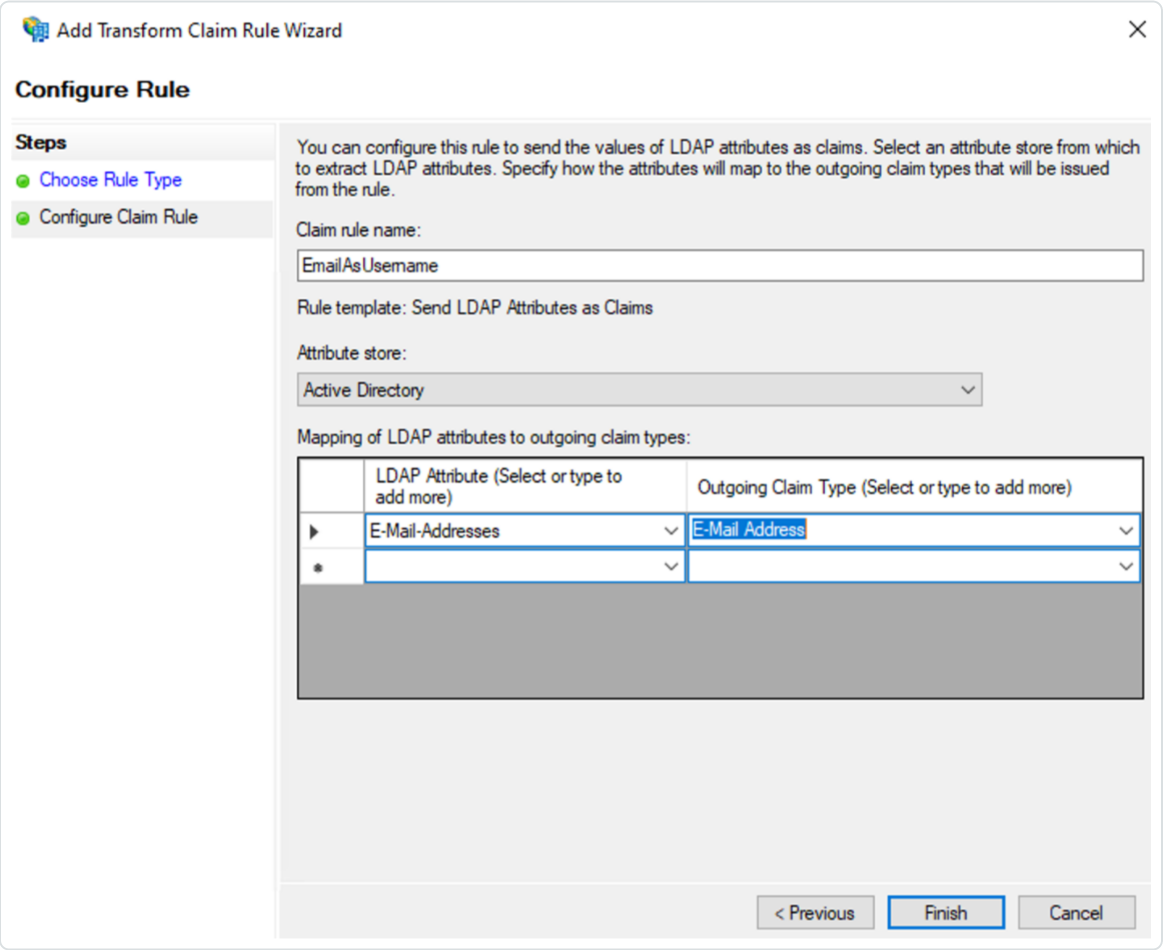
Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

c. Click **Next**.

d. On the **Configure Rule** page, configure the following settings:

- **Claim rule name**
- **Attribute store** — Select **Active Directory**
- **Mapping of LDAP attributes to outgoing claim types**



Configure 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:

EmailAsUsername

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

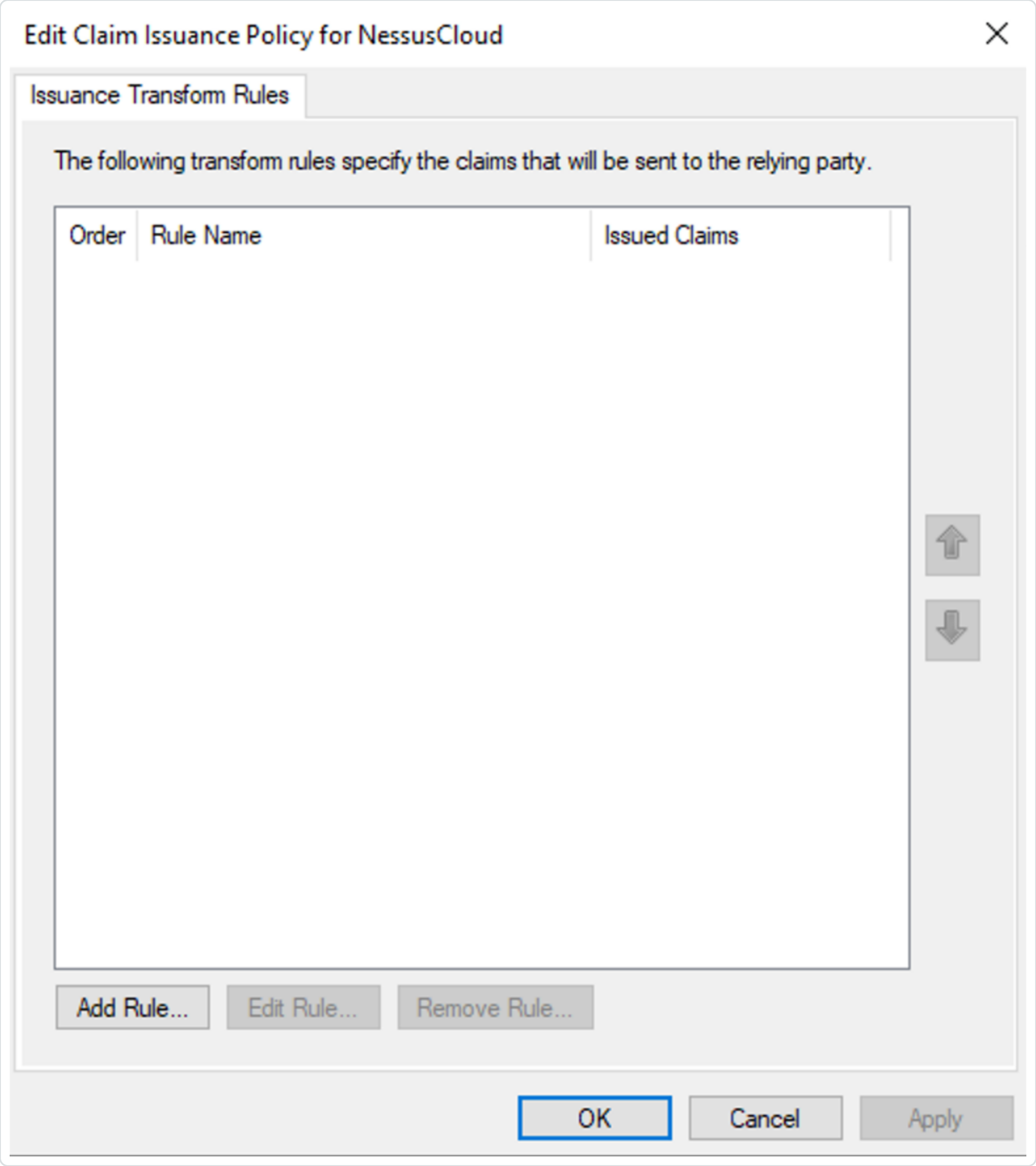
Mapping of LDAP attributes to outgoing claim types:

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

e. Click **Finish**.

Rule two:

a. Click **Add Rule**.



Edit Claim Issuance Policy for NessusCloud

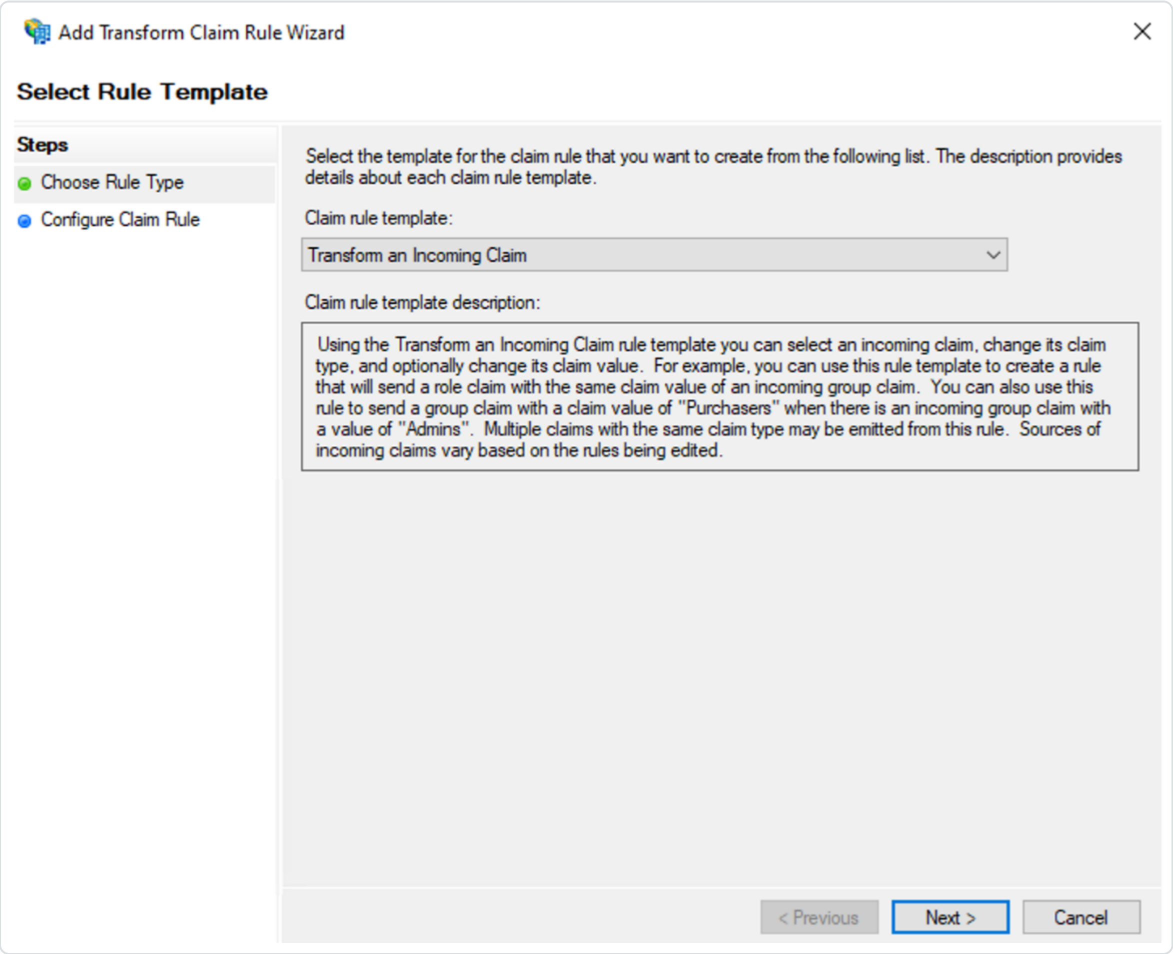
Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

The **Transform Claim Rule** wizard appears.

b. On the **Select Rule Template** page, in the **Claim rule template** drop-down, select **Transform an Incoming Claim**.



Select Rule Template

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

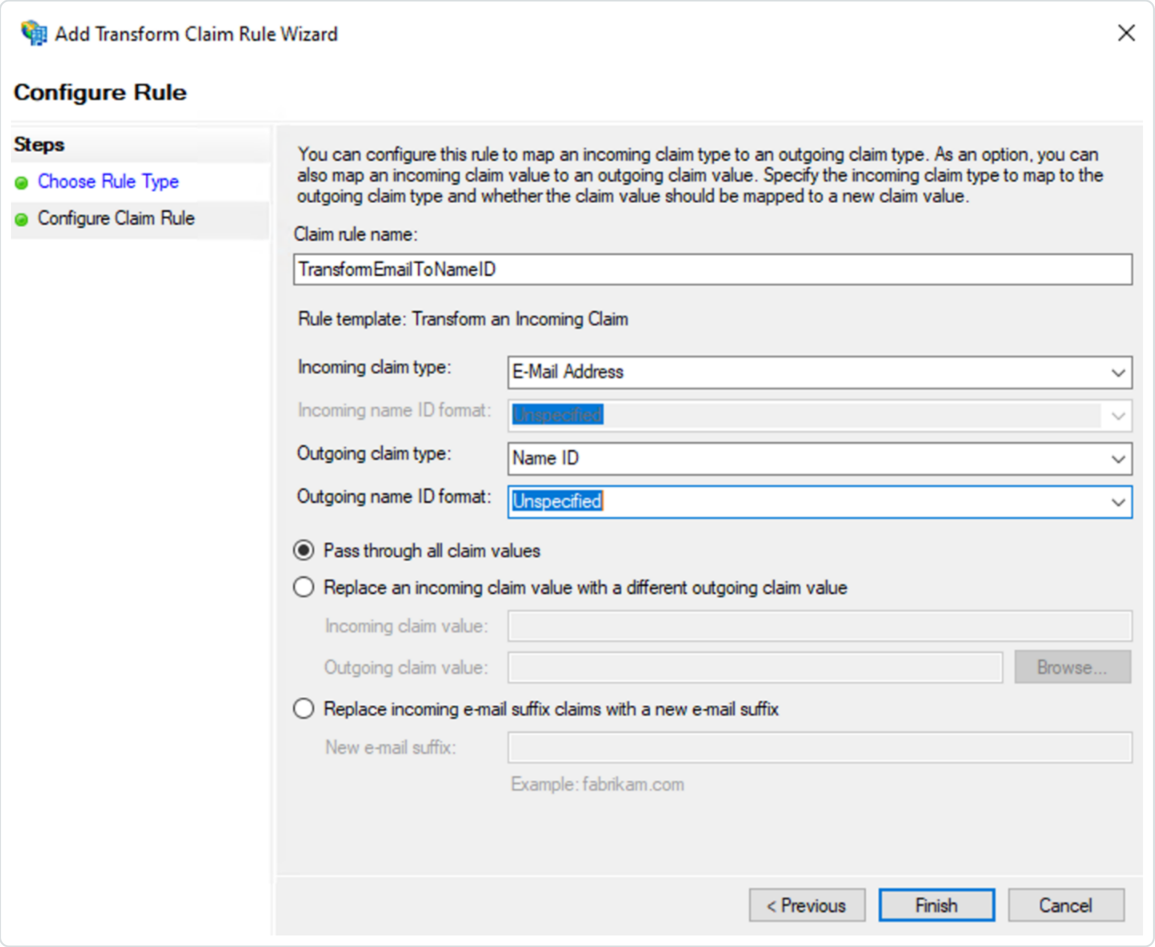
Claim rule template description:

Using the Transform an Incoming Claim rule 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.

c. Click **Next**.

d. On the **Configure Rule** page, configure the following settings:

- **Claim rule name**
- **Outgoing claim type** — select **E-mail Address**
- **Outgoing name ID format** — select **Unspecified**
- **Pass through all claim values** radio button — select radio button



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:

TransformEmailToNameID

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: Unspecified

● Pass through all claim values

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

Incoming claim value:

Outgoing claim value:

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

New e-mail suffix:

Example: fabrikam.com

   e. Click **Finish**.

You return to the **Edit Claims Issuance Policy** window.

4. Click **OK**.

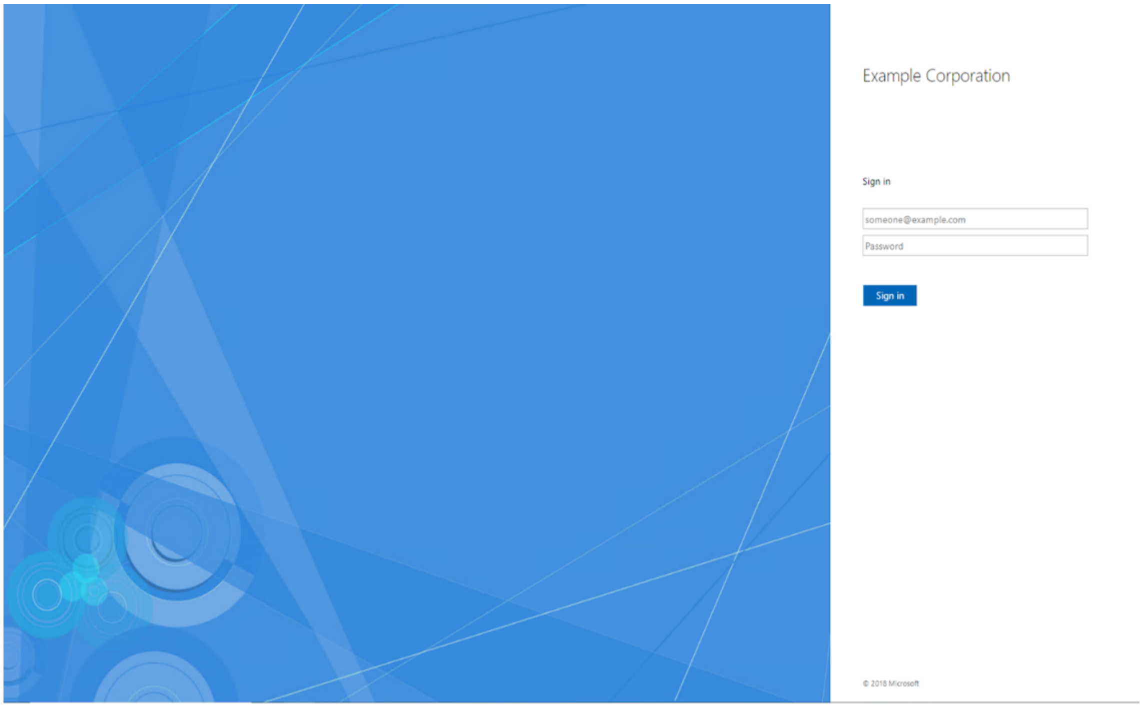
Download your SAML Metadata File

To download your SAML Metadata.xml file:

1. In your browser, navigate to your ADFS portal.

   > **Note:** Your login URL varies based on the DNS FQDN you configured. For example, in this case, the ADFS SSO Portal login would be: *https://adfs.example.com/adfs/ls/idpinitiatedsignon*.

2. Type your login credentials and click **Sign In**.

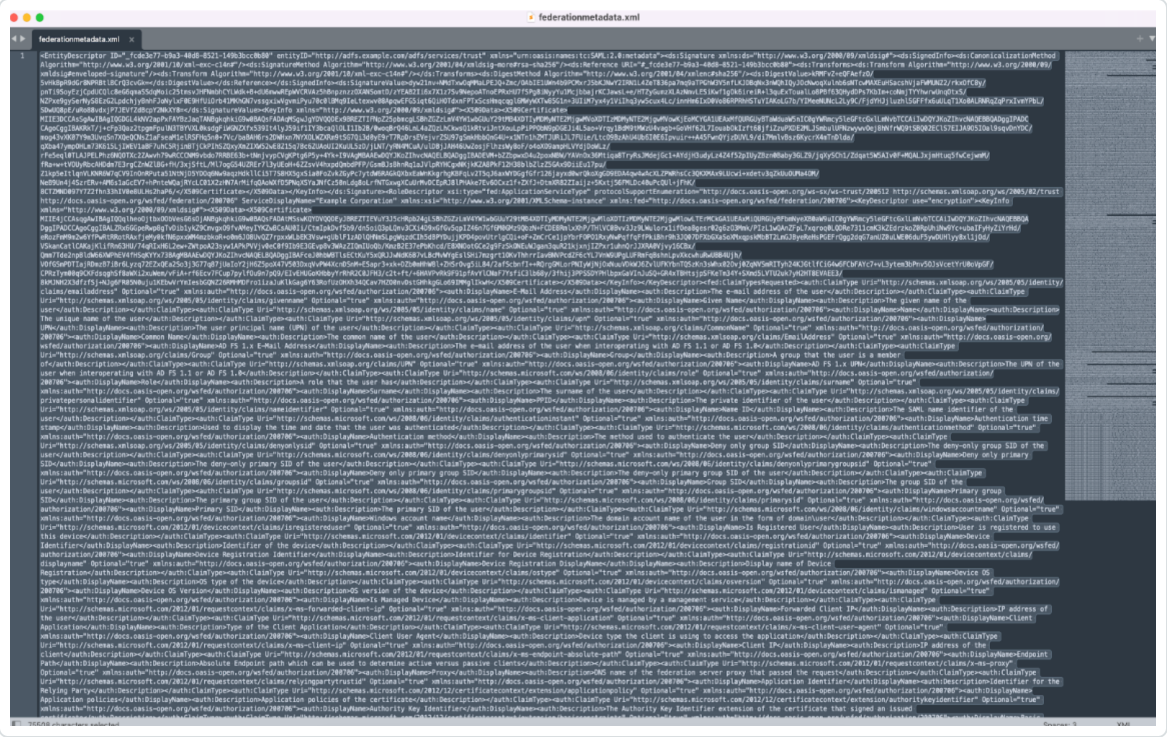
   

   You log in to the ADFS portal.

3. In your browser, paste your specific IDP address to download the metadata.xml file. In this example, our URL is *https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml*.

   The ADFS portal downloads the metadata.xml file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

4. Open the metadata.xml file to ensure it resembles the following screenshot:



```
<EntityDescriptor ID="_fcde3e77-b9a3-40d8-8521-149b3bcc0b80" entityID="http://adfs.example.com/adfs/services/trust" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><ds:Reference URI="#_fcde3e77-b9a3-40d8-8521-149b3bcc0b80"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"/><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>kRMFvZ+eQFAefzO/
5vHkBpR9dGr8NPRBtlBCrQ3cvGk=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>dyw21nv+NMdTxwOqMMaLPEJQ+Zmc/OAbIE1UWn4b9PCMxrJ5bKJNwY2IRN1L4ZeT836pa7mq9aTPGhW3V5nfLKJOBqNx3nWQhIQyJOcNwoqXulnb6sMTcwMAXEuH5acshVjaFWMUNZ2/rkxOfC8y/
pnTi95oyEzjCpdUCQlc8eG6qaa5SdqMoic25tmsvJHFNmbhCYLWdk+B+dU6mwwREpWYCRVAz5hBnpznzzOXANSomtD/zYEAB2Ii6x7X1z7Sv9NepoATnoEPRxHU7f5Pg8iNyyYu1McjbbajrKCJawsL+e/HTZyGumzXLAzNmvLE5iKwf1gOk6ireiR+l3quExTouaILo8PBf63QHydDPs7KbIm+coNmjTYYhwrwUnqOtx5/
NZPxe9gySerNy58EzG2LpdchjyBnhFJoNylxF0E9HfUiOrb41MKhGN7vssgxiwVgvmiPyu70c0lBMq9IeLtexwv0BApqwEFG5iqt6QiHOTdxnFPTxScsHmqcqgl6MWyWXTw85G1n+3UIiM7yx4y1ViIhq3yw5cux4Lc/innHm6IxD0Vo86RPRhHSTuYIAKoLG7b/YIMeeNUNcL2Ly9C/FjdYHJjluzhl5GFFfx6uULqT1Xo0ALRNRqZqPrxIvmYPbL/
SDwUQ8pE/uRo88vdxjP7JEVfZdBcpY2NkXY8=</ds:SignatureValue><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certificate>
MIIE3DCCAsSgAwIBAgIQGDGL4kNV2apPxFAYBzJaqTANBgkqhkiG9w0BAQsFADAqMSgwJgYDVQQDEx9BREZTIFNpZ25pbmcgLSBhZGZzLmV4YW1wbGUuY29tMB4XDTIyMDMyNTE2MjgwMVoXDTIzMDMyNTE2MjgwMVowKjEoMCYGA1UEAxMfQURGUyBTaWduaW5nIC0gYWRmcy5leGFtcGxlLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADC
CAgoCggIBAKRkT/j+cFp3Qaz2tpgmFpulN3TBYVXL0ksdgFiWGNZXfx539It4lyJ59if1IY3bcaQlOLI1Ib2B/0woqBrQ46LmL4aZQzLhCkwsQ1kRtviJntXouLpPiPPObN9pDGEJi4L5ao+Vrqy1BdM9tMWzU4vagb+GoVHf62L7IouabOkIzft68jfiZzuPXDE2MLJSmbulUFNzwywvOej8hNfrWQ9tSBQ02EC157EIJA905IOal9sqvOnYDC/
mog43vXK87Y9m3UvqSn7XQeQCNsZ1aFseaM1elRSFHq5n0+7Vc/baBAH6rs2DWHxn7NYXOLWZXRm9tSG7Qi3d0yE9rT7RpDrsEVejvrZSU97gSmkHbbQnG4U+x1NTn1hZMTJURiJL7FUie/Ltc09BzAhU4Ub6I0E6Ipvuir++A45FwnQYjzDUVL9/di7MmlvBsz6KycrX4mTnDlda/
qXba47ympOHLm73K615LjIWEV1a8F7uhC5RjinBTjCkPIhSZQxyXmZIXW52wE8215q7Bc6ZUAoUI2KuUL5zD/jLNT/yRN4MCuA/ulDBjJAH46UwZosjFlhzsWy8oF/o4oXO9ampHLVYdjDoWLz/
rFe5eql0TLAJPELPhz6NQOTXc2ZAwvh79wRCCCNM9vbdo7RRBE63b+tNnjvypCVgKPtg6P5y+4Yk+I9VAgMBAAEwDQYJKoZIhvcNAQELBQADggIBADEVM+bZZbpwxD4u2poxNBW/YAVnOx36MtiqaBTryRsJMdejGc1+AYdjH3udyLz4Z4f52pIUyZBzn00aby3GLZ9/jqXySCh1/Zdqat5W5AIv0F+MQALJxjmHtuq5fwCejwmM/
fRa+w+tVDUyRbcAHDdm7E3rgCZnWZlBG+fH/3xjSftL/Ml7ogG54UZREr7l3yUEoH+6ZZsvV4hxpdQmbdPFP/GsmBJsBhnRq1aJVlpRYHCgxNKjkKZA8PkF12H38blbZlzZ5GAx9DiiEu17pu/
Z1kp5eItlqnVLKNR6W7qCV9InOnRPuta51NtNjD5YDOq6Nw9aqzHdkllCi5T7S8HX5gxSia0FoZvkZGyPc7ytdW6RAGkQXbxEaWnKkgrhgKBFqLv2T5qJ6axWYDGgfGfr126jayxd0wrQkoXgGD9EDA4qw4wAcXLZPWRhsCc3QKXMAx9LUcwi+xdetv3qZkUuOUMa4OM/
NeB9Un4j4SzrERv+AM6s1aGcEV7+hPnteWQajRYcLC01X2zHN7ArMifqQAoNXfD5PNqX5YaJNfCz50nLdg8oLrfNTGxwgXCuUrMvDCEpRJ8lPHAke7Ev6OCxz1f+ZXfJ+DtmXRB2ZIaijz+5Kxtj56FMLDc40uPcQUl+jFhK/
BCTZMND097Y7Z2fhn33hIV8eBULHs2haP6/</X509Certificate></X509Data></KeyInfo></ds:Signature><RoleDescriptor xsi:type="fed:ApplicationServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512 http://schemas.xmlsoap.org/ws/2005/02/trust
http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="Example Corporation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"><KeyDescriptor use="encryption"><KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certificate>
MIIE4jCCAsqgAwIBAgIQQqlheoOjtbxDObVesG6sOjANBgkqhkiG9w0BAQsFADAtMSswKQYDVQQDEyJBREZTIEVuY3J5cHRpb24gLSBhZGZzLmV4YW1wbGUuY29tMB4XDTIyMDMyNTE2MjgwMloXDTIzMDMyNTE2MjgwMlowLTErMCkGA1UEAxMiQURGUyBFbmNyeXB0aW9uIC0gYWRmcy5leGFtcGxlLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQA
DggIPADCCAgoCggIBALZRx6GGpeRwp8gTvDib1ykZ9CmvgxO9fvAMeyIYKZwBCsAU0Ii/CtmIpkDvf5b9/dn5oiO3pLQnv3CXi4O9xGfGv5qpIZ46n7Gf6M0GMz9QbzN+FCDEBRmlxXhP/THlVC0Bvv3Jz9LWulorx1ifOea8gesr02g6zO3Mmk/PIzL1wQAnZFpL7xqroq0LQDRe7311cmK3kZEdrzkoZ0RpUhiNw9Yc+ubaIFyHyZiYrHd/
eRozFmM9m2w6YfPwRtRRotRAxfjeMy0kfN6pxxWM4mzbkoR+o0m6JO8UvQZ7rpxxWLbEK3Vsw+gUblF1zADlQHNmSLpgWqzdCIh5dBPYDujjKPD4povUtrlgCQi+oF+ZmCrCeljpYbrFOPO1RxyNwPqffqFfPkiBhr9h3JQ07DFXbGXaSoXMxqpskMbBT2LmGJByeReHsPGEFrQgg2dqG7anUZ0uLWE06duF5ywDUHlyy0xl1jOd/
VSkanCatlCAKajKlifRn63HU/74qRIxH6L2ew+ZWtpoA23syw1APkPVVjv0eC0f9Ib9E3GEvp8v3WAzZIQmIUoQb/KmzB2E37ePbKhcd/E8XNOotGCe2g9FzSkONEuWJgan3quR21kjxnjIZPxr1uhnQrJJXRA0Vjvy16CBx/
Qmm7Tde2npBldW66XWPhEV4fHSqKYYx73BAgMBAAEwDQYJKoZIhvcNAQELBQADggIBAFceJ0hbW8TlsECtKuY5xQRJJwNdK6B7vLBcMvWYgEslSHi7mzgrt10KvThhrrIavBNVPcdZF6cYL7VnW9UPgLUFRmFqBshnLpvXkcwhuRwUBB4Ujh/
V0fGSmPDTIajRDmz87iBr6Lyzq72EZxQEa2So3j3G77q87jUaIoY2jH6Z5poX47V503DxqVvPW4XcnDSnM+ESapr3+xk+DZb0mHhW8l+ZHSrOvg5iL84/2afScbnfI++RQrgGMLorPNIyWjNjOxNuuVDkWJ6ZvlUFKYbnTQSzKn3sWhx02Ovj0ZqNVSmRITyh24KJGtlfCiG4w6FCbFAYc7+vL3ytem3bPnv5OJsVcetYrU0oVpGF/
CPRzTym00q9CKFdsqghSf8aWXi2xuWem/vFiA+rf6Ecv7FCup7pylfOu9n7pQ9/ElvEHUGoKHbbyYrRhR2C0JFH3/c2t+ft/+6HAVPvRk9F91pfAvYlCNaF7YsfiC3lb68y/3fhij3PPSSDYPHlbpxGaVInJuSQ+GR4xTBHtsjpSFKeTm34Y+SXmd5LVTU2uk7yH2MT8EVAEE3/
8kMJNH2X3dfzfSj+NJg6FR85N0uju1KEbwVrYmIesbGQNZ26RMMMDFro1izaJuKlkGag6Y63RofUzOMXh34QCav7MZO0nvDstGMhkgGLo69IMMglIkwH=</X509Certificate></X509Data></KeyInfo></KeyDescriptor><fed:ClaimTypesRequested><auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/emailaddress" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>E-Mail Address</auth:DisplayName><auth:Description>The e-mail address of the user</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Given Name</auth:DisplayName><auth:Description>The given name of the
user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Name</auth:DisplayName><auth:Description>
The unique name of the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>
UPN</auth:DisplayName><auth:Description>The user principal name (UPN) of the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/claims/CommonName" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/
200706"><auth:DisplayName>Common Name</auth:DisplayName><auth:Description>The common name of the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/claims/EmailAddress" Optional="true" xmlns:auth="http://docs.oasis-open.org/
wsfed/authorization/200706"><auth:DisplayName>AD FS 1.x E-Mail Address</auth:DisplayName><auth:Description>The e-mail address of the user when interoperating with AD FS 1.1 or AD FS 1.0</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.xmlsoap.org/claims/Group" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Group</auth:DisplayName><auth:Description>A group that the user is a member
of</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/claims/UPN" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>AD FS 1.x UPN</auth:DisplayName><auth:Description>The UPN of the
user when interoperating with AD FS 1.1 or AD FS 1.0</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/
200706"><auth:DisplayName>Role</auth:DisplayName><auth:Description>A role that the user has</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname" Optional="true"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Surname</auth:DisplayName><auth:Description>The surname of the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
privatepersonalidentifier" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>PPID</auth:DisplayName><auth:Description>The private identifier of the user</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Name ID</auth:DisplayName><auth:Description>The SAML name identifier of the
user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Authentication time
stamp</auth:DisplayName><auth:Description>Used to display the time and date that the user was authenticated</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod" Optional="true"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Authentication method</auth:DisplayName><auth:Description>The method used to authenticate the user</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Deny only group SID</auth:DisplayName><auth:Description>The deny-only group SID of the
user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarysid" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Deny only primary
SID</auth:DisplayName><auth:Description>The deny-only primary SID of the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarygroupsid" Optional="true"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Deny only primary group SID</auth:DisplayName><auth:Description>The deny-only primary group SID of the user</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Group SID</auth:DisplayName><auth:Description>The group SID of the
user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Primary group
SID</auth:DisplayName><auth:Description>The primary group SID of the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/
authorization/200706"><auth:DisplayName>Primary SID</auth:DisplayName><auth:Description>The primary SID of the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname" Optional="true"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Windows account name</auth:DisplayName><auth:Description>The domain account name of the user in the form of domain\user</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.microsoft.com/2012/01/devicecontext/claims/isregistereduser" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Is Registered User</auth:DisplayName><auth:Description>User is registered to use
this device</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/devicecontext/claims/identifier" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Device
Identifier</auth:DisplayName><auth:Description>Identifier of the device</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/devicecontext/claims/registrationid" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/
authorization/200706"><auth:DisplayName>Device Registration Identifier</auth:DisplayName><auth:Description>Identifier for Device Registration</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/devicecontext/claims/
displayname" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Device Registration DisplayName</auth:DisplayName><auth:Description>Display name of Device
Registration</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/devicecontext/claims/ostype" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Device OS
type</auth:DisplayName><auth:Description>OS type of the device</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/devicecontext/claims/osversion" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/
200706"><auth:DisplayName>Device OS Version</auth:DisplayName><auth:Description>OS version of the device</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/devicecontext/claims/ismanaged" Optional="true"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Is Managed Device</auth:DisplayName><auth:Description>Device is managed by a management service</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Forwarded Client IP</auth:DisplayName><auth:Description>IP address of
the user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-application" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Client
Application</auth:DisplayName><auth:Description>Type of the Client Application</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-user-agent" Optional="true"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Client User Agent</auth:DisplayName><auth:Description>Device type the client is using to access the application</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Client IP</auth:DisplayName><auth:Description>IP address of the
client</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-endpoint-absolute-path" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Endpoint
Path</auth:DisplayName><auth:Description>Absolute Endpoint path which can be used to determine active versus passive clients</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy"
Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Proxy</auth:DisplayName><auth:Description>DNS name of the federation server proxy that passed the request</auth:Description></auth:ClaimType><auth:ClaimType
Uri="http://schemas.microsoft.com/2012/01/requestcontext/claims/relyingpartytrustid" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Application Identifier</auth:DisplayName><auth:Description>Identifier for the
Relying Party</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/12/certificatecontext/extension/applicationpolicy" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>
Application policies</auth:DisplayName><auth:Description>Application policies of the certificate</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.microsoft.com/2012/12/certificatecontext/extension/authoritykeyidentifier" Optional="true"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>Authority Key Identifier</auth:DisplayName><auth:Description>The Authority Key Identifier extension of the certificate that signed an issued
```

Appendix A: Configuring SAML in Tenable Vulnerability Management

To configure Tenable Vulnerability Management SAML in a FedRAMP environment:

1. Provide a copy of your metadata.xml file to your Tenable sales representative.

   The Tenable sales representative provisions your container appropriately. Once provisioned, your representative provides you with the completed URL for your Relying Party Trust.

2. Use this URL when configuring a Relying Party Trust. For more information, see Configure an ADFS Relying Party Trust.

To configure Tenable Vulnerability Management SAML in a non-FedRAMP environment:

Follow the SAML Configuration instructions in the *Tenable Vulnerability Management User Guide*.