

INTRADYN

Email Archiving & eDiscovery

Configuring Single Sign-On Log In with SAML 2.0 for the Intradyn Email Archiver

V.1.2

All Microsoft references, screenshots, and logos are used with permission from Microsoft.

© 2019 Intradyn Inc, Inc.

All rights reserved. No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Intradyn Inc., nor may it be resold or distributed by any entity other than Intradyn, Inc., without prior written authorization of Intradyn, Inc. Intradyn, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Intradyn, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

Introduction

The Intradyn Email Archiver supports single sign-on (SSO) log in through SAML 2.0.

A SAML 2.0 identity provider (IDP) that is commonly used is a self-hosted Active Directory Federation Services (AD FS) server. AD FS is a service provided by Microsoft that allows the Windows Server to provide a web login using existing Active Directory credentials.



You must have the AD FS server already set up for your company before beginning this guide. If you need assistance, please refer to these resources from Microsoft:

[AD FS Help](#)

[AD FS Troubleshooting](#)

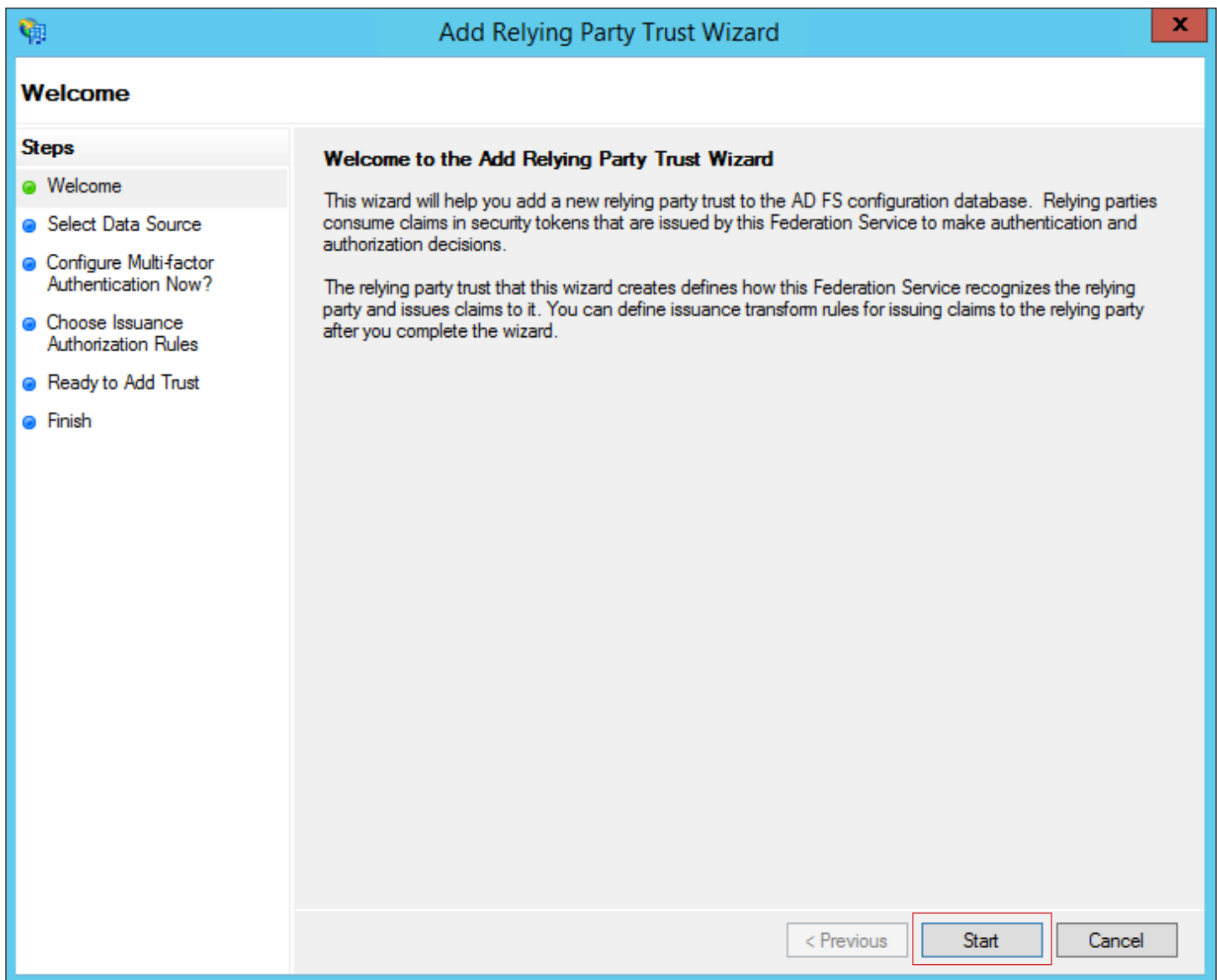
Requirements

- Intradyn Email Archiver
- An Active Directory where all users have an email address
- A server running Microsoft Server 2016, 2012, or 2008
- SSL certificate to sign the AD FS login page and the fingerprint for that certificate
- For use with host mapping in the Intradyn Email Archiver, you will need an installed certificate for the hosted SSL

Part One- Create a Relying Party Trust

The connection between AD FS and Intradyn is defined by using a Relying Party Trust (RPT).

1. In the Server Manager, click on **"Tools"**, then select **"AD FS Management"**.
2. Under the **"Actions"** sidebar on the right, click on **"Relying Party Trusts"**, then add a new **"Standard Relying Party Trust"**. This will open the **"Add Relying Party Trust Wizard"**.
3. On the **"Welcome"** page, click on **"Start"** to begin the wizard.



4. On the “**Select Data Source**” screen, select “**Enter Data About the Party Manually**”, then click “**Next**”.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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

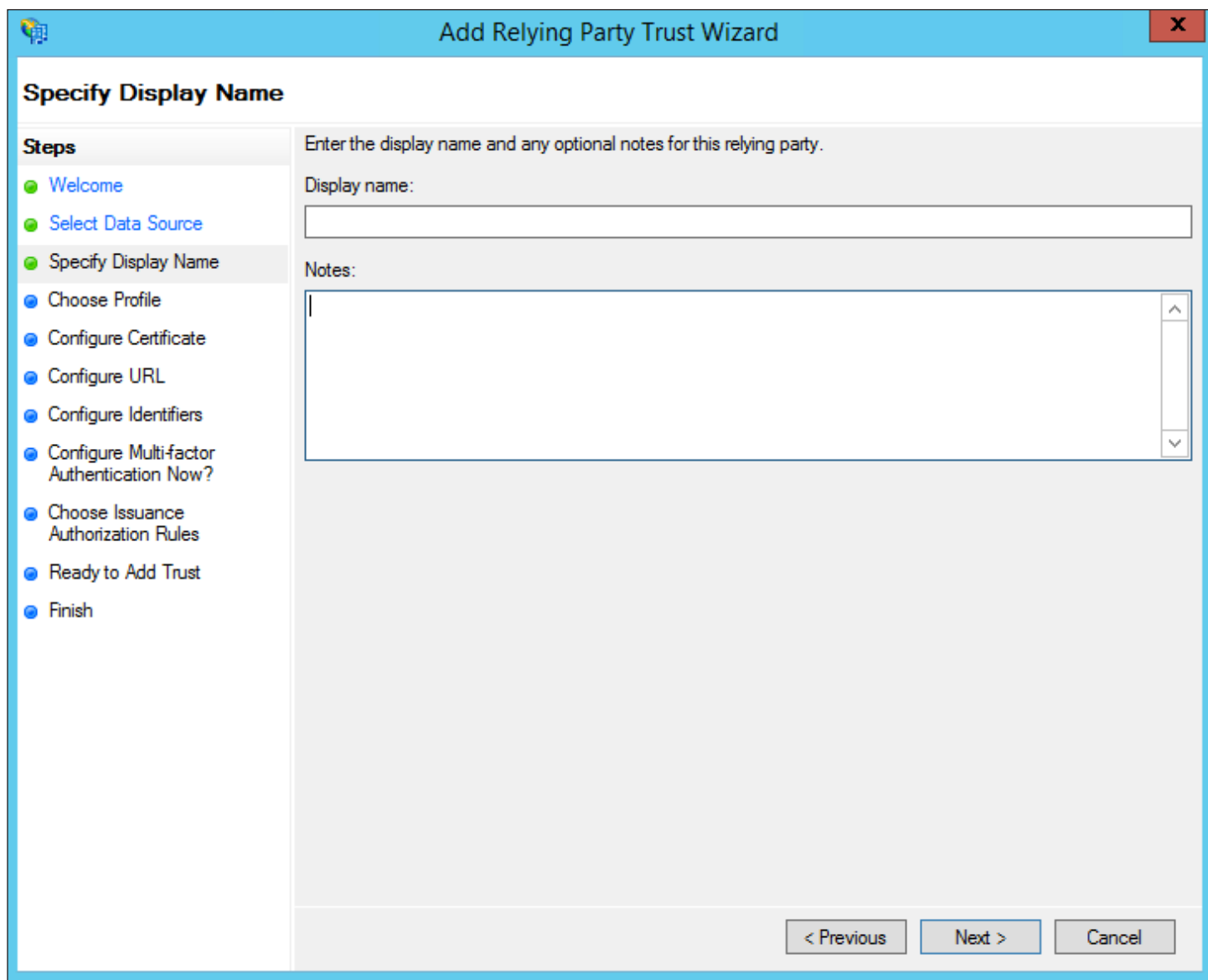
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

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.

5. On the “**Specify Display Name**” screen, enter a name in the “**Display Name**” field, then add any notes needed to the “**Notes**” field. Click “Next”.



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with a close button (X) in the top right corner. The main window has a light blue header with the title 'Add Relying Party Trust Wizard'. Below the header, the window is divided into two main sections. On the left is a 'Steps' sidebar with a list of steps: 'Welcome', 'Select Data Source', 'Specify Display Name' (which is highlighted with a green circle), 'Choose Profile', 'Configure Certificate', 'Configure URL', 'Configure Identifiers', 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area on the right is titled 'Specify Display Name' and contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this instruction are two input fields: 'Display name:' with a text box, and 'Notes:' with a larger text area. At the bottom right of the main area are three buttons: '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Specify Display Name

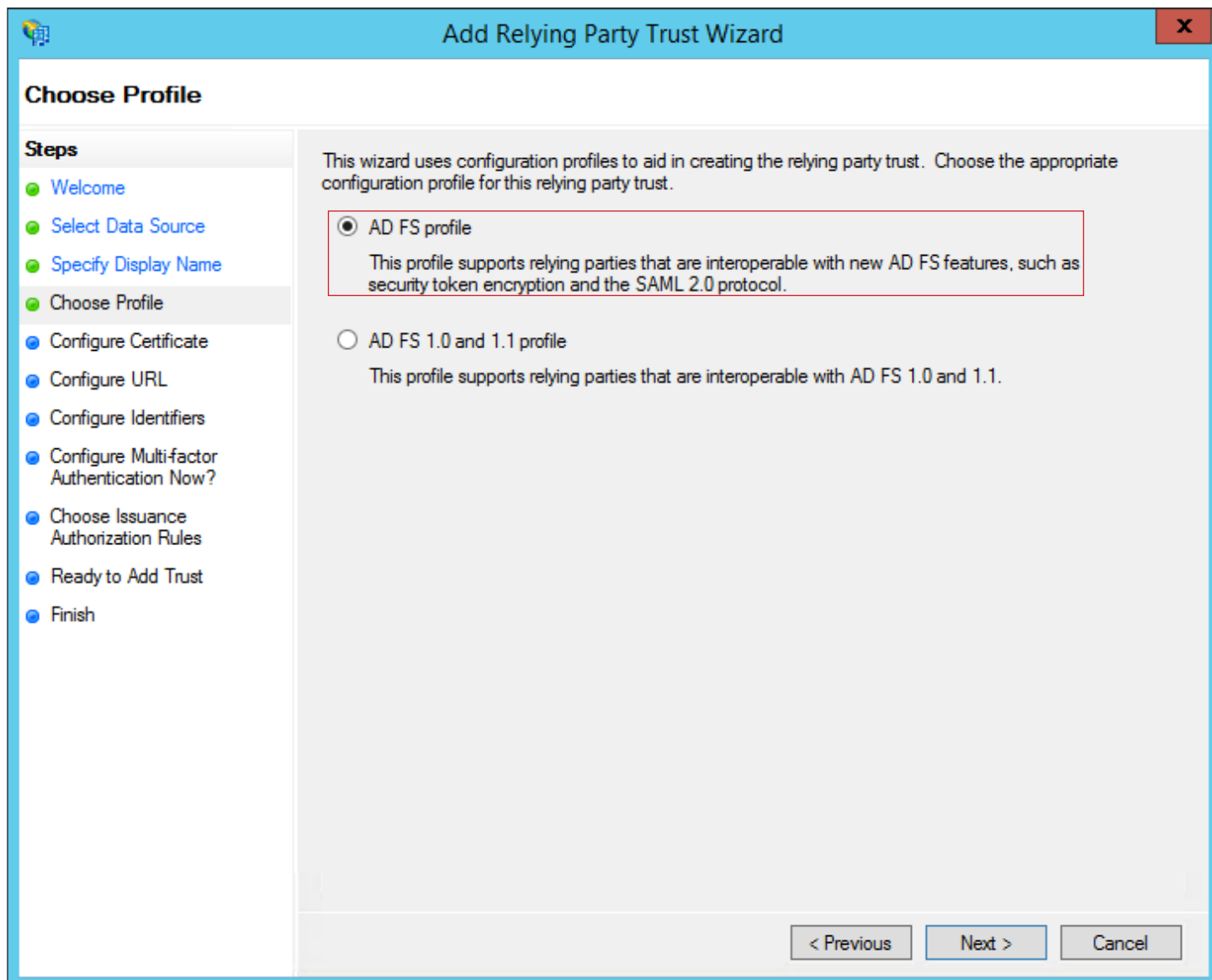
Enter the display name and any optional notes for this relying party.

Display name:

Notes:

< Previous Next > Cancel

6. On the “**Choose Profile**” screen, select “**AD FS profile**”, then click “**Next**”.



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with a close button (X) on the right. The main content area is white. On the left, there is a 'Steps' sidebar with a list of steps: Welcome, Select Data Source, Specify Display Name, Choose Profile (highlighted), Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area has a heading 'Choose Profile' and a description: 'This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.' Below this, there are two radio button options. The first option, 'AD FS profile', is selected and highlighted with a red border. Its description is: 'This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.' The second option is 'AD FS 1.0 and 1.1 profile', with the description: 'This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Choose Profile

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile**
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

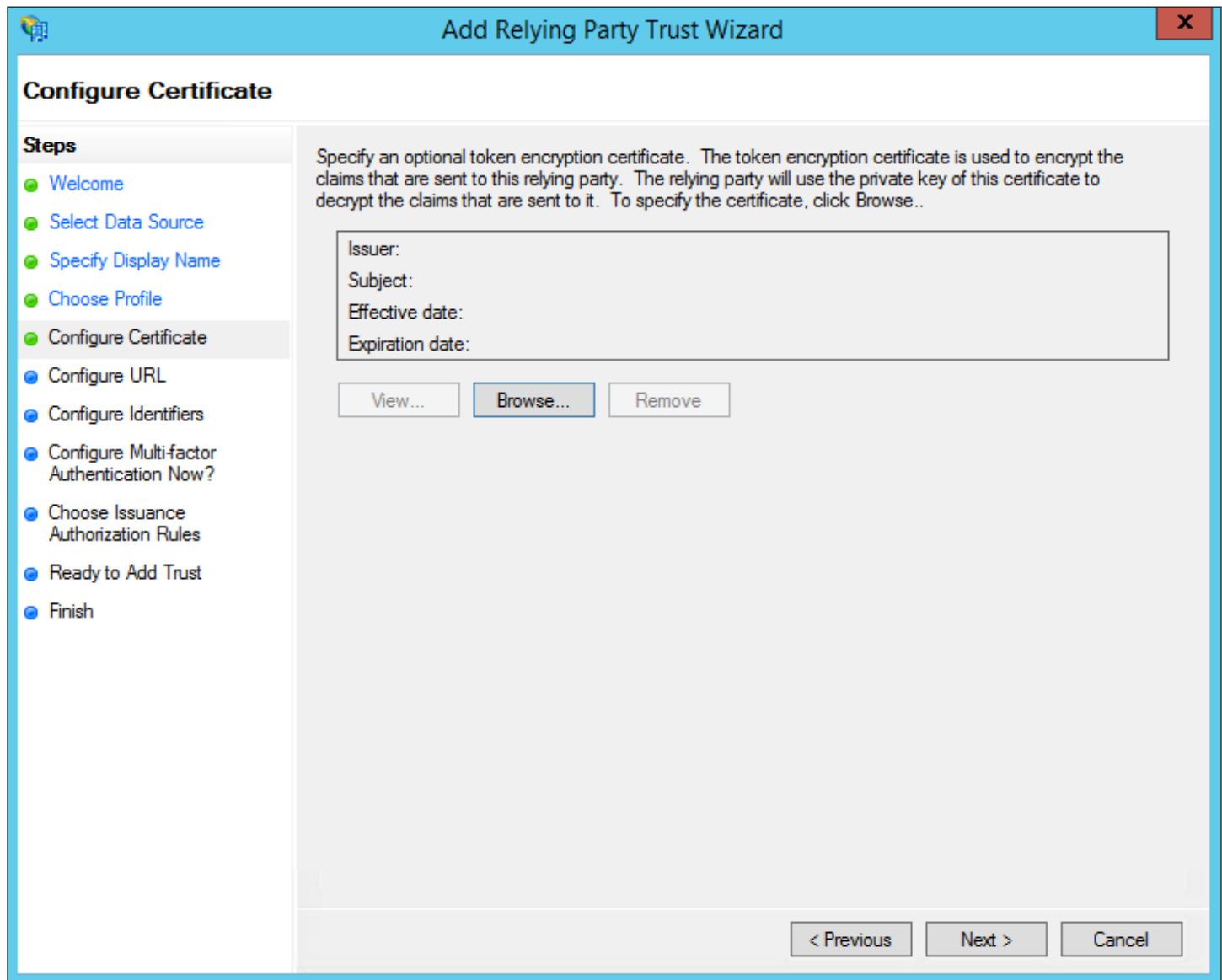
This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

☒ **AD FS profile**
This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

☐ **AD FS 1.0 and 1.1 profile**
This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

< Previous Next > Cancel

7. On the “**Configure Certificate**” screen, leave the certificate settings at their defaults and click “**Next**”.



The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Configure Certificate' step selected. The window has a blue title bar and a sidebar on the left listing the steps of the wizard. The main area contains instructions and a form for configuring the certificate.

Add Relying Party Trust Wizard

Configure Certificate

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate**
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

View... Browse... Remove

< Previous Next > Cancel

- On the “**Configure URL**” page, click the “**Enable support for the SAML 2.0 WebSSO protocol**” check box. Under “**Relying party SAML 2.0 SSO service URL**”, type the SAML service endpoint URL for this relying party trust.

The service URL will be:

`https://subdomain.yourcompany.com/access/saml`

You will replace *subdomain* with your Intradyn subdomain and *yourcompany* with your company name as registered with Intradyn. Note that there’s no trailing slash at the end of the URL.

Then click “**Next**”.

The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Configure URL' step selected. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL (selected), Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains instructions for AD FS protocols. The 'Enable support for the SAML 2.0 WebSSO protocol' checkbox is checked and highlighted with a red border. Below it, the 'Relying party SAML 2.0 SSO service URL' field is empty, with an example URL provided. The 'Enable support for the WS-Federation Passive protocol' checkbox is unchecked. At the bottom, there are buttons for '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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.

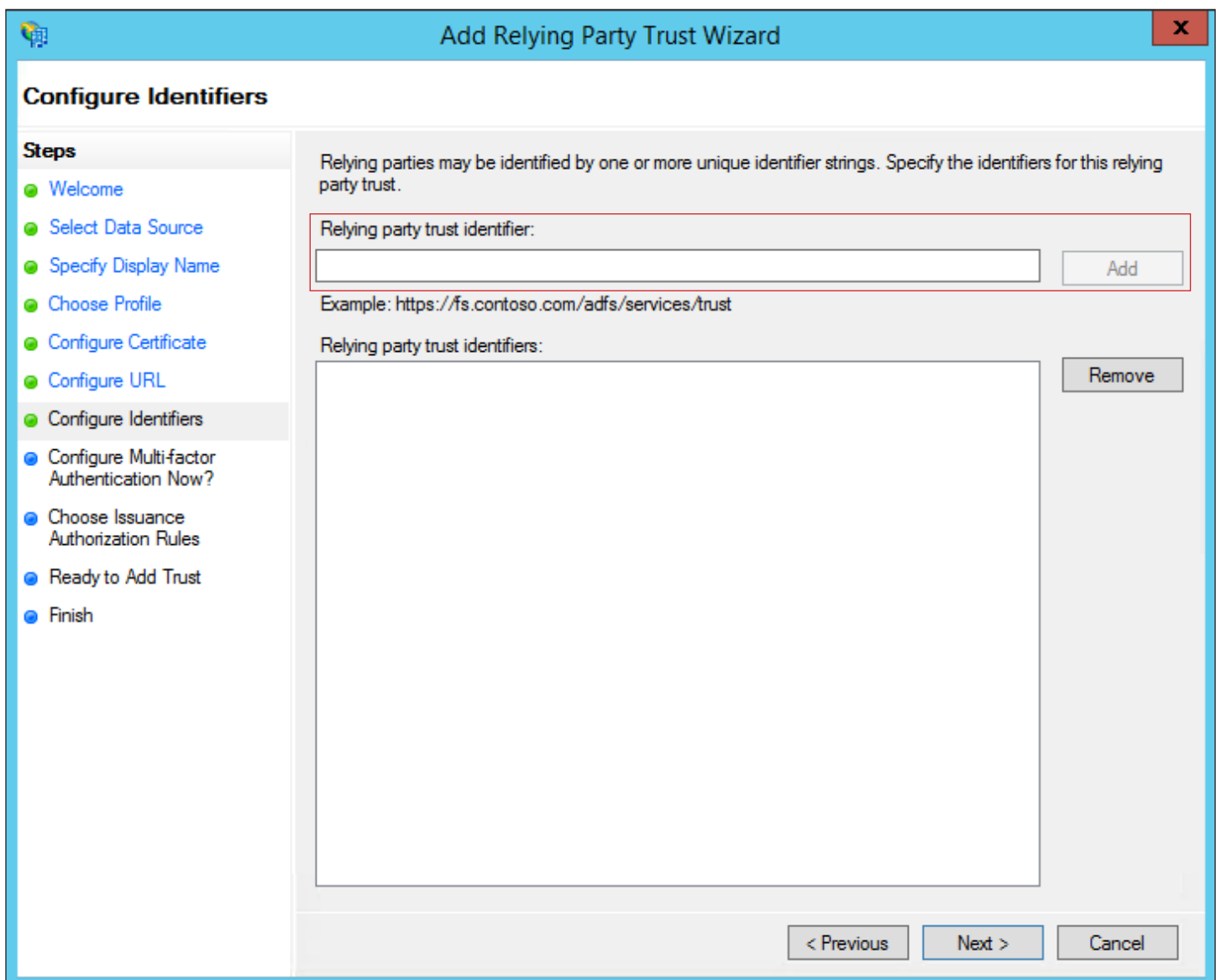
Relying party SAML 2.0 SSO service URL:

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

< Previous Next > Cancel

9. On the “**Configure Identifiers**” screen, specify a “**Relying party trust identifier**” using “*subdomain.yourcompany.com*”, replacing *subdomain* with your Intradyn subdomain and *yourcompany* with your company name as registered with Intradyn, in the empty field and click on “**Add**”.

If you enter “*subdomain.yourcompany.com*”, and receive a “request failure” error, you may need to enter your subdomain as “**https://subdomain.yourcompany.com**”.



Add Relying Party Trust Wizard

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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

Relying party trust identifier:

Add

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

Relying party trust identifiers:

Remove

< Previous Next > Cancel

10. On the “**Configure Multi-factor Authentication Now?**” screen, you may configure multi-factor authentication, however that is beyond the scope of this manual. Click “**Next**” to continue.
11. On the “**Choose Issuance Authorization Rules**” screen, select “**Permit all users to access this relying party**”.

Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules**
- Ready to Add Trust
- Finish

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

☒ **Permit all users to access this relying party**

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

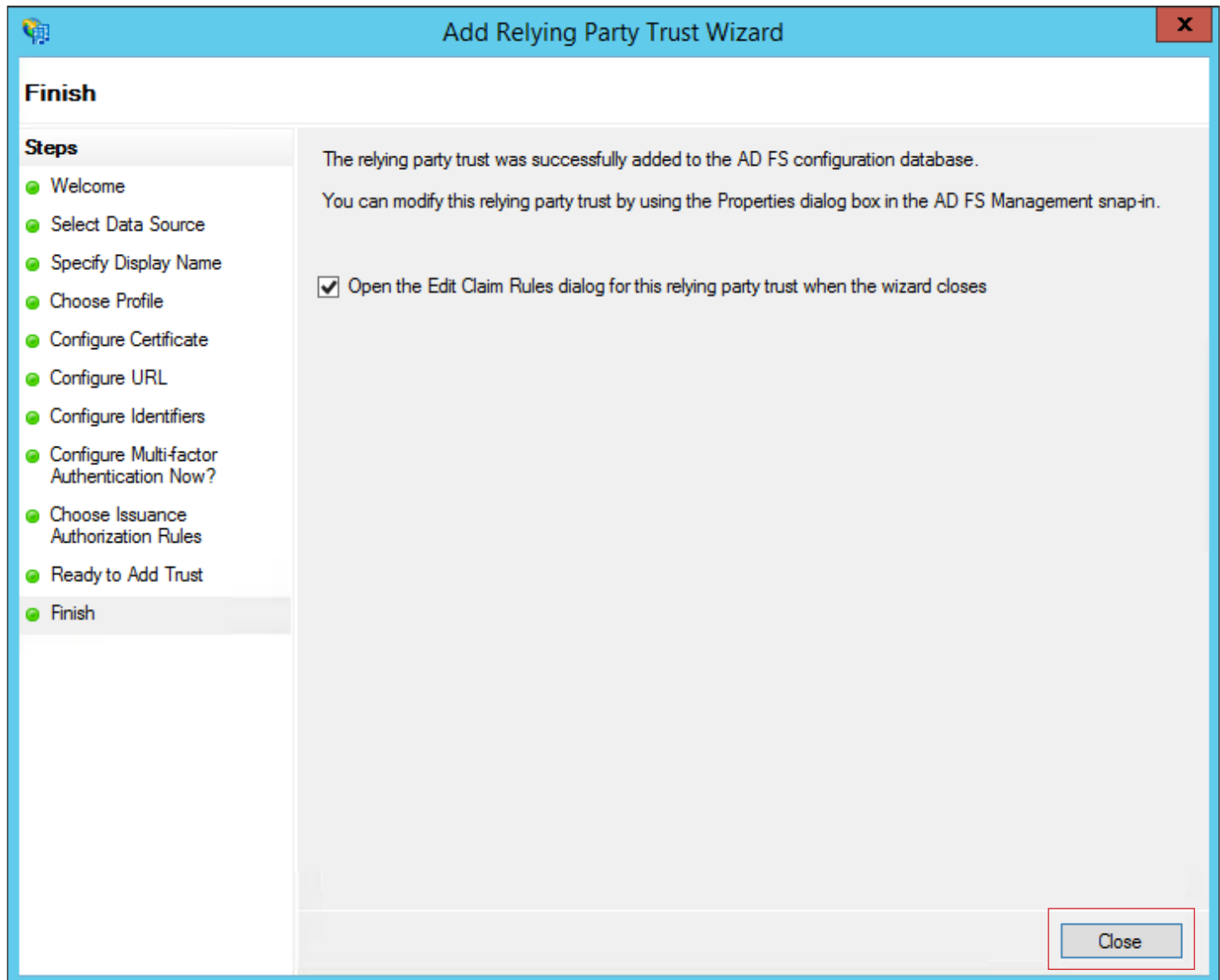
☐ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

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.

< Previous Next > Cancel

12. On the “**Ready to Add Trust**” screen, review your settings for accuracy, then click “**Next**” to save your relying party settings.
13. On the “**Finish**” page, click “**Close**”. This will exit the wizard and open the “**Claims Rules Editor**”.



PART 2- Creating and Configuring Claims Rules

Once the RPT has been created, you can create claim rules and update the RPT with changes that you are not set by the wizard.

1. Click on **“Add Rule...”**, then on the next screen select **“Send LDAP Attributes as Claims”** from the dropdown menu. Then click **“Next”**.

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:

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.

< Previous Next > Cancel

2. On the next screen, type in a name for your claim rule, select **“Active Directory”** from the **“Attribute store”** dropdown menu. Then do the following:
 - A. In the **“LDAP Attribute”** column, select **“E-Mail Addresses”**.
 - B. In the **“Outgoing Claim Type”** column, select **“E-mail Address”**.
 - C. Click **“OK”** to save the rule.

Edit Rule - LDAP EMAIL

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:

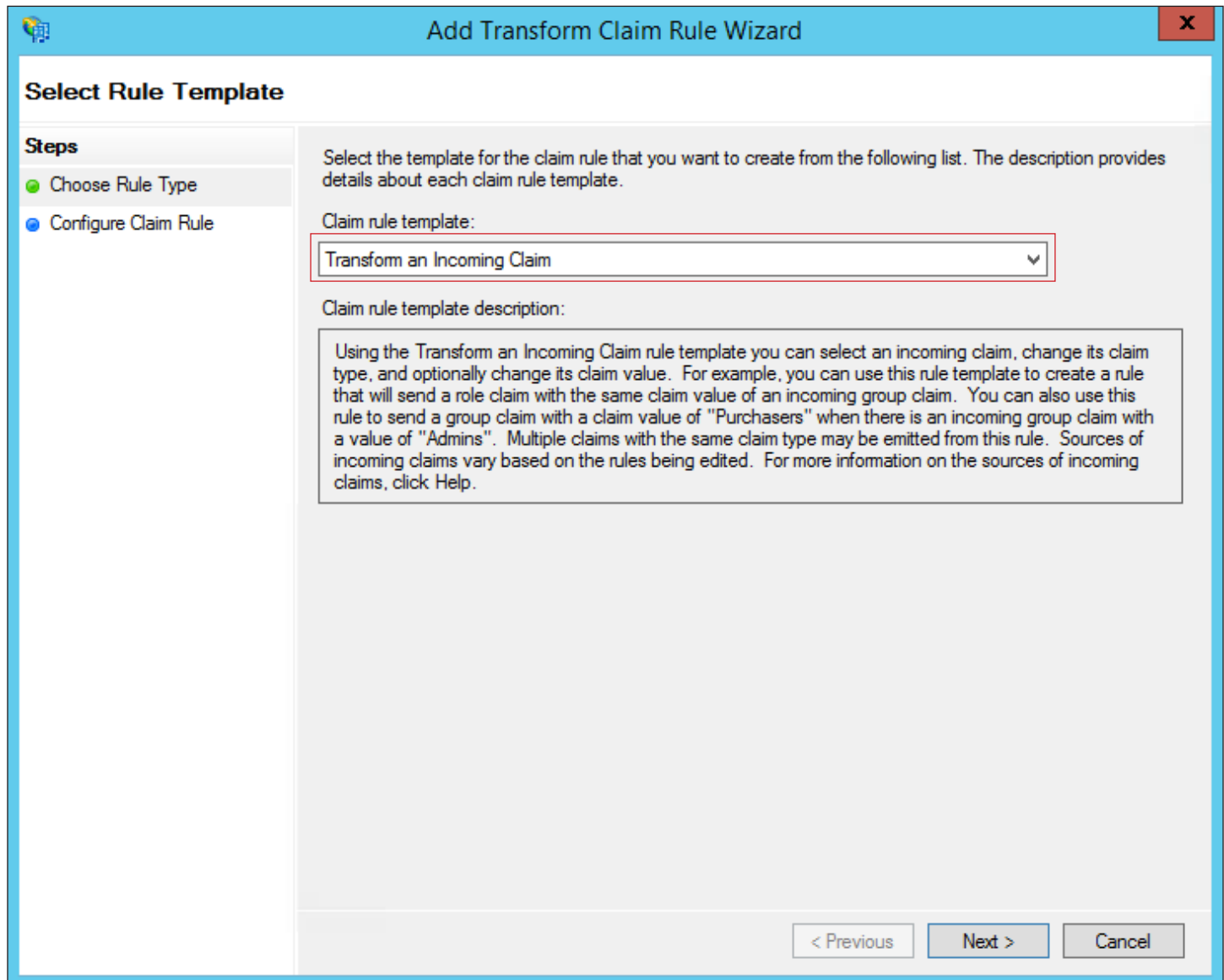
Rule template: Send LDAP Attributes as Claims

Attribute store:

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)
▶	<input type="text" value="E-Mail-Addresses"/>	<input type="text" value="E-Mail Address"/>
*	<input type="text"/>	<input type="text"/>

3. Create an additional rule by clicking **"Add Rule..."**, this time select **"Transform an Incoming Claim"** from the template dropdown.



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 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. For more information on the sources of incoming claims, click Help.

< Previous Next > Cancel

4. On the next screen, type in a name for your claim rule, then do the following:
 - 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"**.
 - D. Leave the rule to the default of **"Pass through all claim values"**.
 - E. Click **"OK"** to create the claim rule, and then **"OK"** again to finish creating rules.

Edit Rule - Email Transform

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:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ 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

PART 3- Adjusting the Trust Settings

There are additional settings you need to adjust to complete your set-up.

1. Right click on the RPT you created and select **"Properties"**.
2. Click on the **"Advanced"** tab, confirm that **"SHA-256"** is specified as the secure hash algorithm.

The screenshot shows a dialog box titled "No Host-Map Spoke Properties" with a red 'X' button in the top right corner. The dialog has a tabbed interface with the following tabs: Monitoring, Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, Proxy Endpoints, Notes, and Advanced. The "Advanced" tab is selected and highlighted with a red box. Inside the dialog, there is a text label "Specify the secure hash algorithm to use for this relying party trust." followed by a dropdown menu labeled "Secure hash algorithm:" which currently displays "SHA-256" and has a red box around it. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

3. In the **“Endpoints”** tab, click on **“Add SAML”** to add a new endpoint.
4. For the **“Endpoint type”**, select **“SAML Logout”**.
5. For the **“Binding”**, choose **“POST”**
6. For the Trusted URL, create a URL using:
 - A. The web address of your AD FS server
 - B. The AD FS SAML endpoint you noted earlier
 - C. The string ‘?wa=wsignout1.0’

The URL should look similar to:

“https://sso.yourdomain.tld/adfs/ls/?wa=wsignout1.0”

Click **“OK”** to close this window, then click **“Apply”**, and **“OK”** on the **“Login Properties”** window.

Note: If your AD FS has security settings that require all Federation Services Properties to be filled out and published in the metadata, you must check the **“Publish organization information in federation metadata”** box.

The screenshot shows the 'Login Properties' dialog box with the 'Edit Endpoint' tab selected. The 'Endpoint type' dropdown is set to 'SAML Logout'. The 'Binding' dropdown is set to 'POST'. There is an unchecked checkbox for 'Set the trusted URL as default'. The 'Index' is set to 0. The 'Trusted URL' field contains the text 'https://sso.domain.tld/adfs/ls/?wa=wsignout1.0'. Below this field is an example: 'Example: https://sts.contoso.com/adfs/ls'. The 'Response URL' field is empty, with an example below it: 'Example: https://sts.contoso.com/logout'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

