

ADFS Single Sign-On with Therefore™ Online

www.therefore.net
© 2020 Therefore Corporation

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Windows® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Any other 3rd Party products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While care has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document.

VERSION: 2020 - 01

Table of Contents

1. Introduction	5
2. Setting up ADFS on the Customer's Side	6
2.1 Installing a suitable ADFS	6
2.2 Adding a Relying Party Trust	7
2.3 Add Relying Party Trust Wizard	9
2.4 Selecting Data Source	9
2.5 Specifying Display Name	11
2.6 Choosing Access Control Policies	12
2.7 Finalizing the Addition of the Relying Party Trust	13
2.8 Configuring Claims Insurance Policy	14
2.9 Editing Claim Insurance Policy	15
2.10 Adding a Rule	16
2.11 Choosing a Rule Type	17
2.11.1 Pass Through of Filter an Incoming Claim	17
2.11.2 Send LDAP Attributes as Claims	19
2.12 Setting all the Claim Rules	21
2.13 Setting up ADFS configuration on Therefore Server side	21
2.14 Connecting to Therefore™	24
3. Configuring Users for ADFS	27
3.1 Manual Configuration	27
3.1.1 Selecting SAML User	27
3.1.2 Entering Usernames	28
3.1.3 Selecting Users or Groups	29
3.2 Automatic Configuration	29
3.2.1 Selecting Replication	30
3.2.2 Connecting to Therefore™ XML Web Service	31
3.2.3 Setting Therefore™ Replication Service to Automatic	33
3.2.4 Setting Security Permissions	34
3.2.5 Setting an Account	35
3.2.6 Providing a Username and Password for Connection	36

3.2.7	User/Group Synchronization	37
3.2.8	Selecting Users or Groups	38
3.2.9	Entering Group Names	39
3.2.10	Synchronizing Users /Groups from the List	40

1. Introduction

This document will demonstrate how to set up ADFS on the customer side as well as configure their users for ADFS both manually and automatically.



Note: Each subtitle under the chapters of this document are steps in the ADFS configuration process and should be followed in sequential order.

2. Setting up ADFS on the Customer's Side

You will learn:

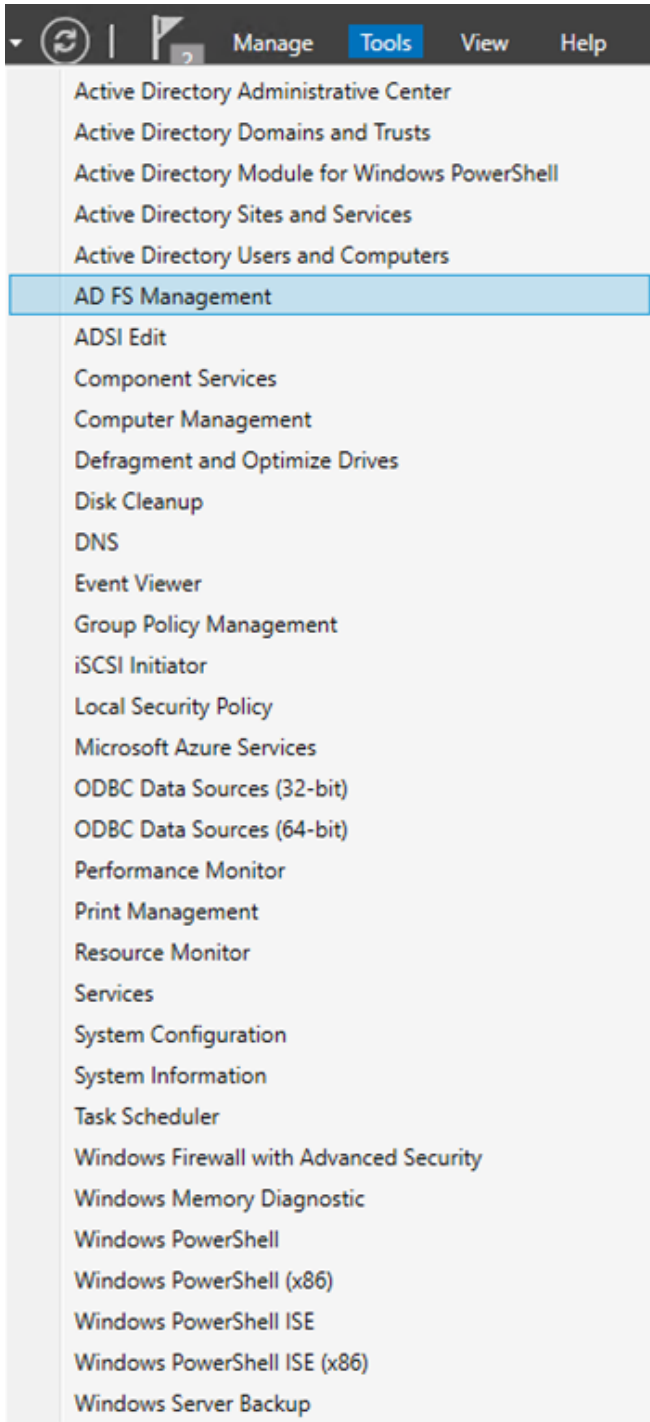
1. How to set up ADFS on the customer's side.
2. How to set up permitted users manually.
3. How to extract permitted users automatically from the customer's active directory.

2.1 Installing a suitable ADFS

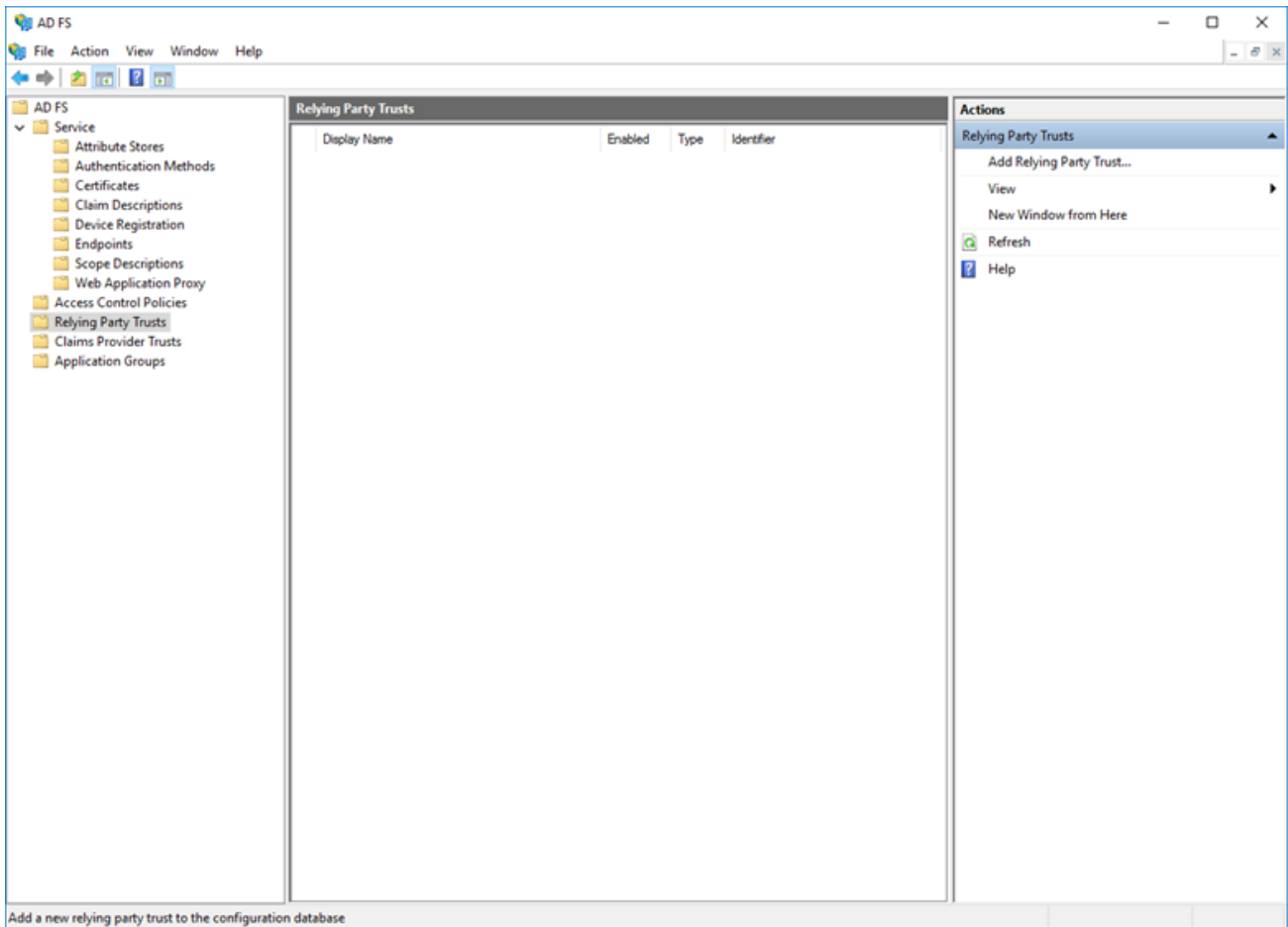
ADFS will first need to be installed and configured on the customer's server; once this has been established, a certificate should be obtained. For instructions on installing the most suitable ADFS, please find the relevant details on the following Microsoft link: <https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services>

2.2 Adding a Relying Party Trust

Open the 'Server Manager' program, and on the ribbon menu, select **Tools > AD FS Management** - this will open the **AD FS** dialog.

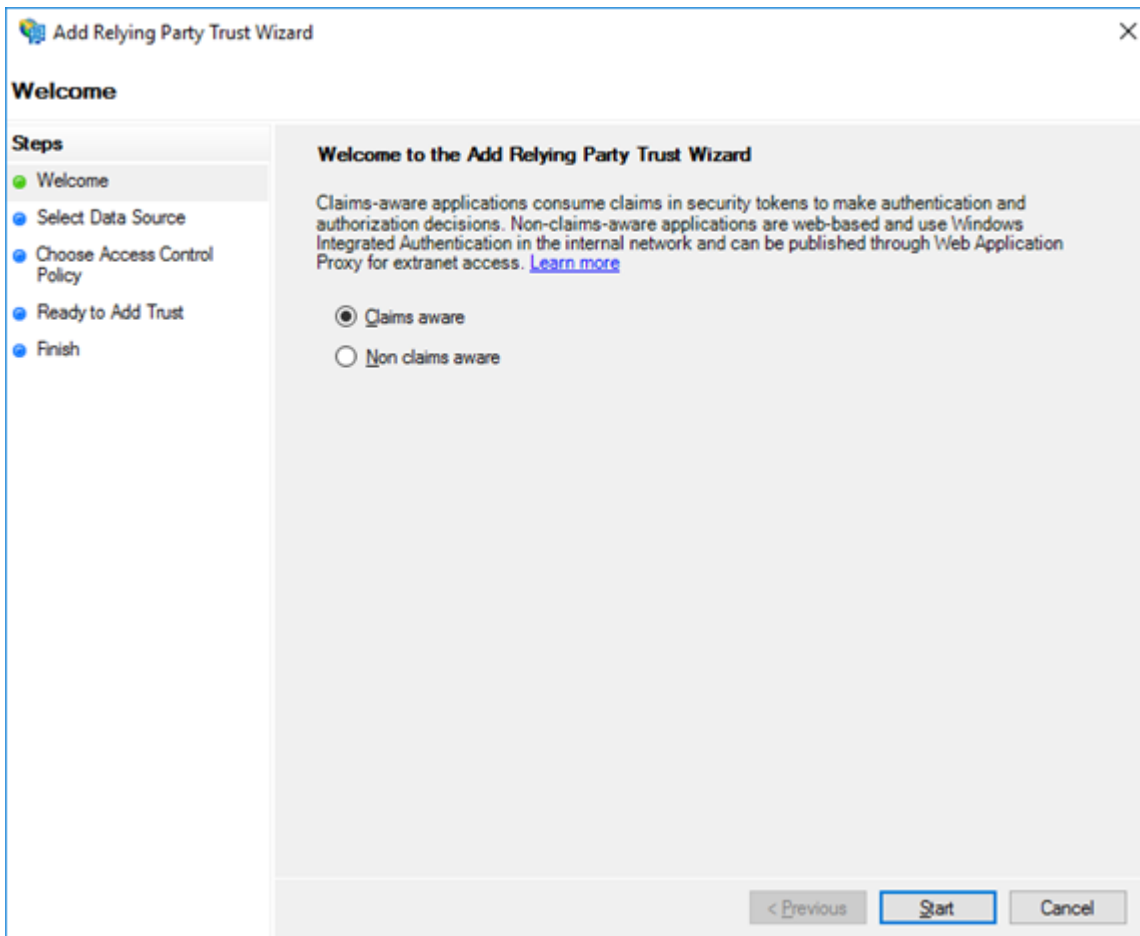


Once the AD FS dialog has opened, select **'Relying Party Trusts'** (in the left-hand file column) in order to allow this to work with Therefore™. In the right-hand **'Actions'** column, select **'Add Relying Party Trust'**.



2.3 Add Relying Party Trust Wizard

In the 'Add Relying Party Trust Wizard', select 'Claims Aware' and then 'Start'.



2.4 Selecting Data Source

In the next set of options, select 'Import data about the relying party published online or on a network', and enter the required URL (based on the user's region). Click 'Next' once this step has been completed.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome (completed), Select Data Source (current), Specify Display Name, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options:

- Import data about the relying party published online or on a local network** (selected):
 - 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.

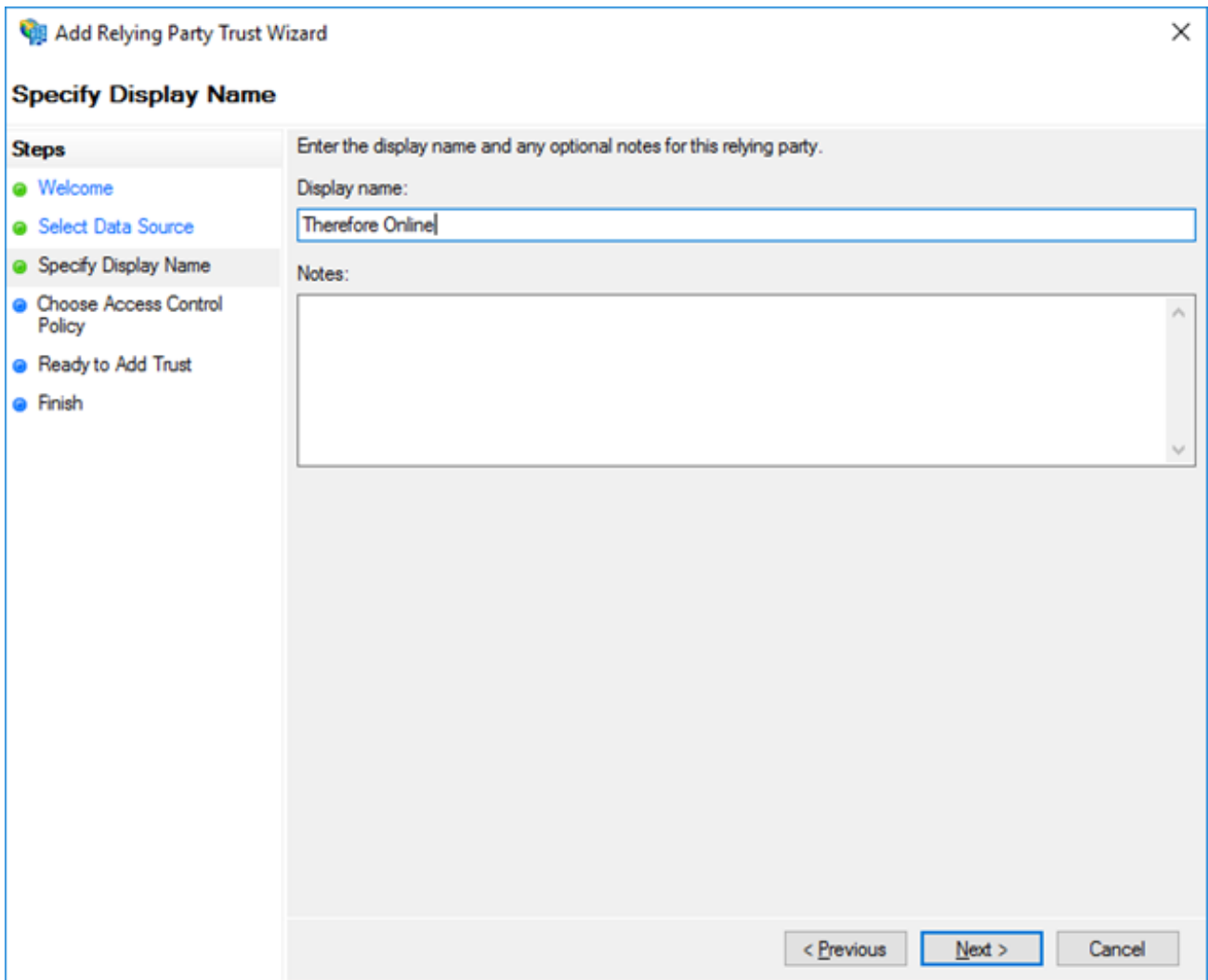
At the bottom right, there are three buttons: '< Previous' (disabled), 'Next >' (active), and 'Cancel' (disabled).



Note: The Regional ADFS information URL that is entered in the 'Federation metadata address' field needs to be requested from Therefore Support. Please open a support request (include the Customer ID and tenant name for the customer that you are setting up ADFS for). In the request just write that you need the Regional ADFS information URL for setting up ADFS for Customer XYZ. You must have this URL before you can continue with the next step.

2.5 Specifying Display Name

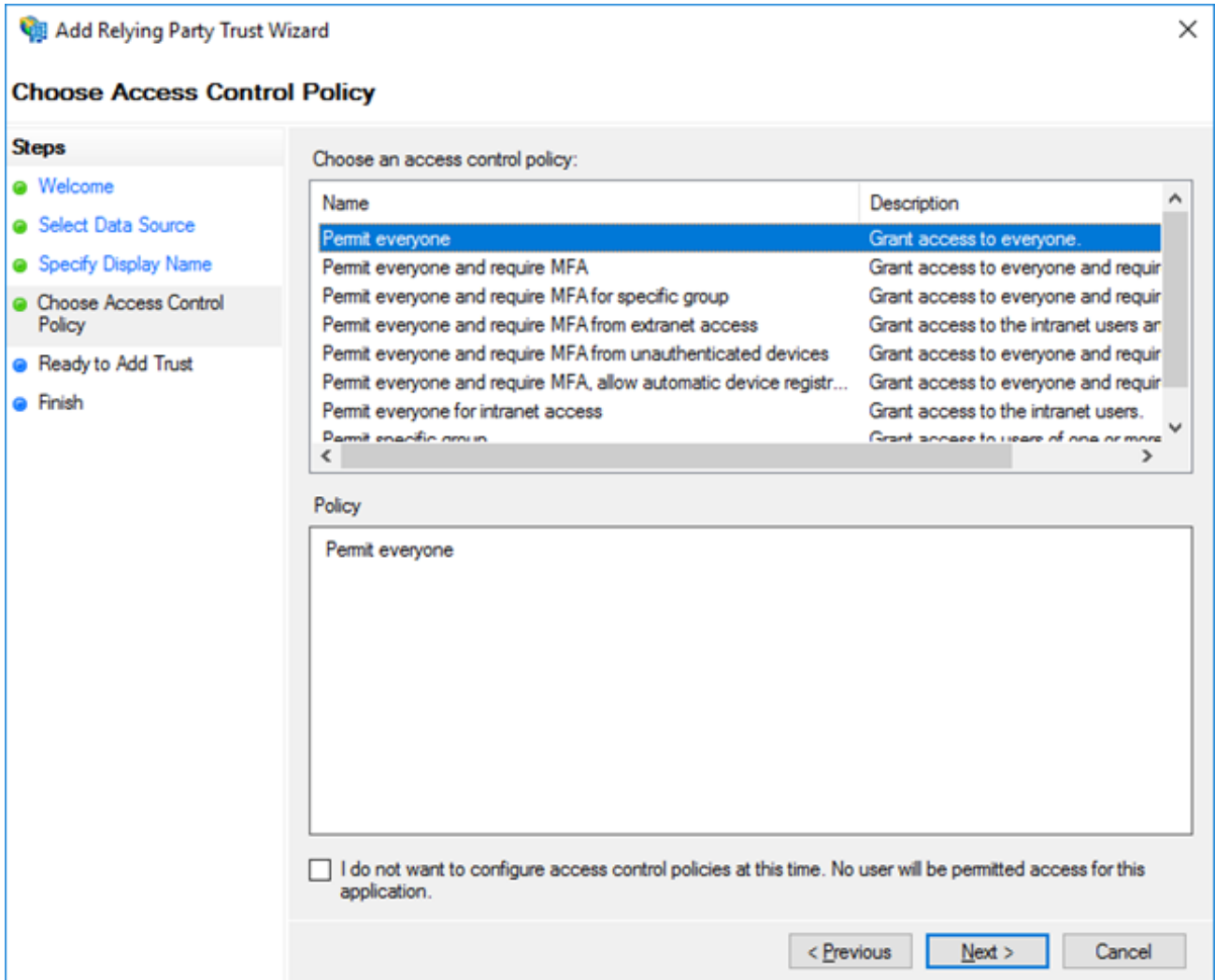
Enter the display name for the 'Relying Party Trust' in the 'Display name' field.



The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists: Welcome (green dot), Select Data Source (green dot), Specify Display Name (green dot and highlighted), Choose Access Control Policy (blue dot), Ready to Add Trust (blue dot), and Finish (blue dot). 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 input field containing 'Therefore Online'. Below the input field is a 'Notes:' label followed by a large, empty text area with a vertical scrollbar on the right. At the bottom right, there are three buttons: '< Previous' (disabled), 'Next >' (active/highlighted), and 'Cancel' (disabled).

2.6 Choosing Access Control Policies

It is then possible to select the access control policies, from the available list (e.g. Permit everyone, Permit everyone and require MFA, etc.) and click **'Next'** when completed.

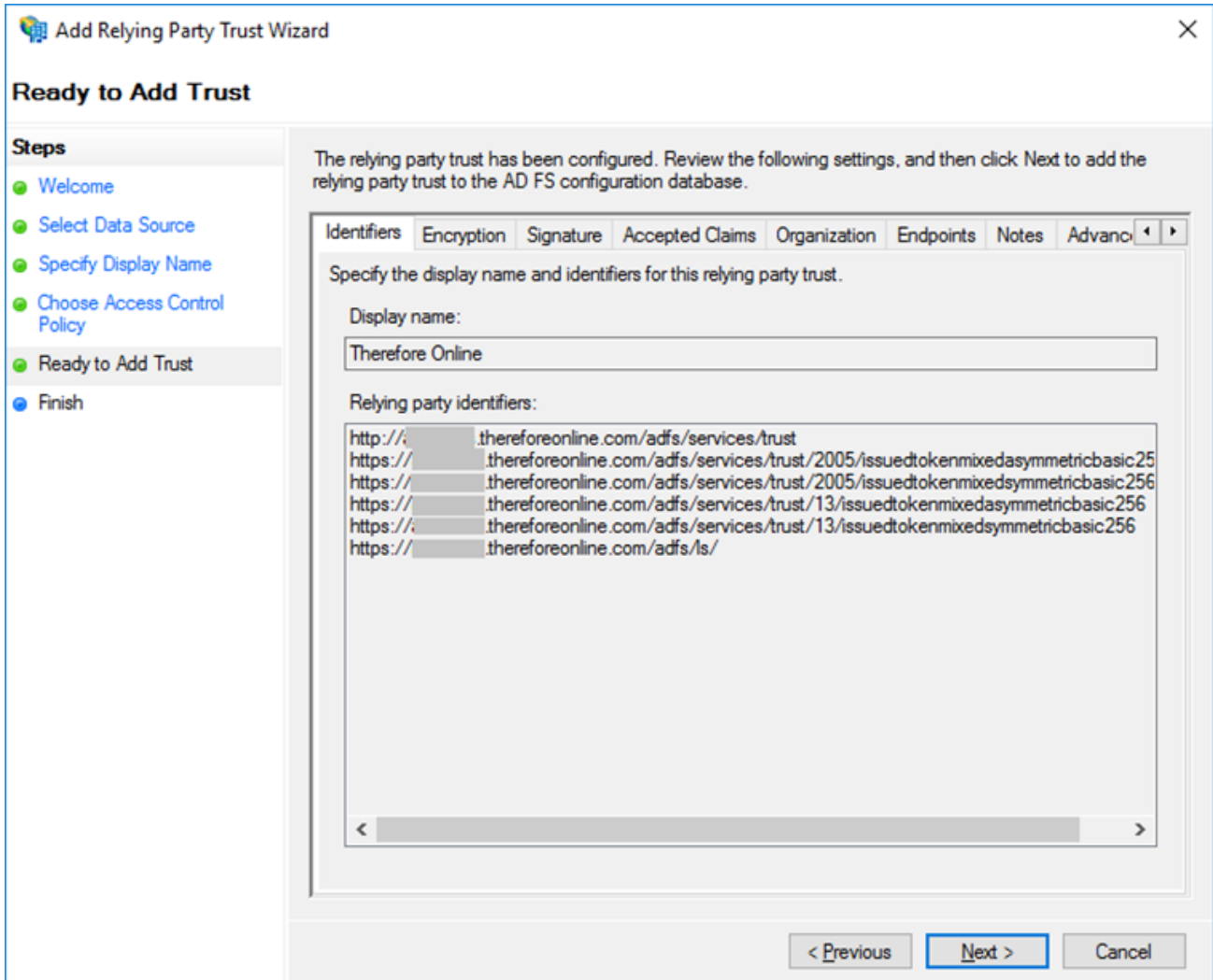


The customer should select the best-fit policy for their respective system. A list of available access control policies can be found in the following link:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/access-control-policies-in-ad-fs>

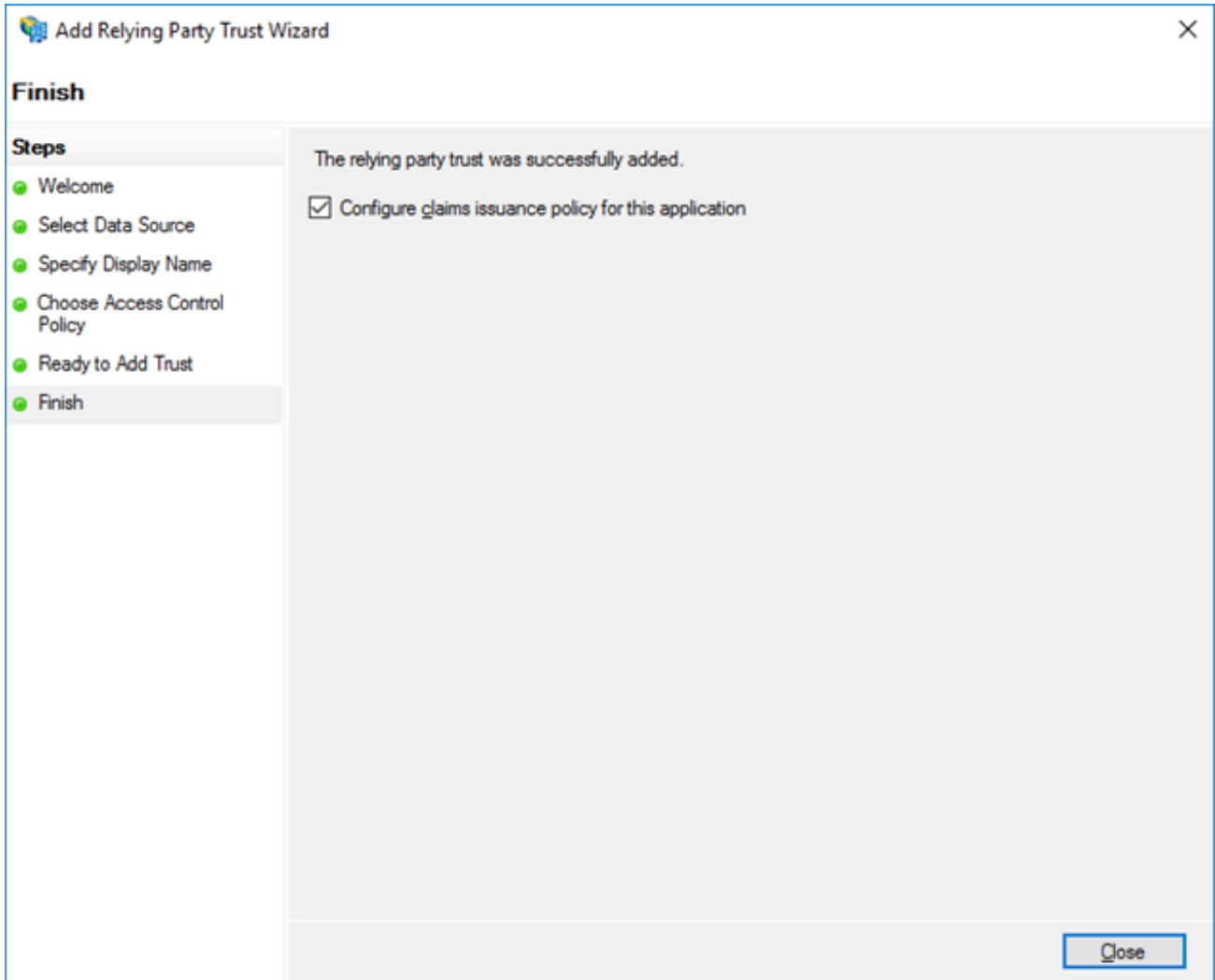
2.7 Finalizing the Addition of the Relying Party Trust

Before finalizing the addition of the relying party trust, the dialog will display several tabs that will indicate the view of the user's configuration. Click **'Next'** to proceed to the final dialog.



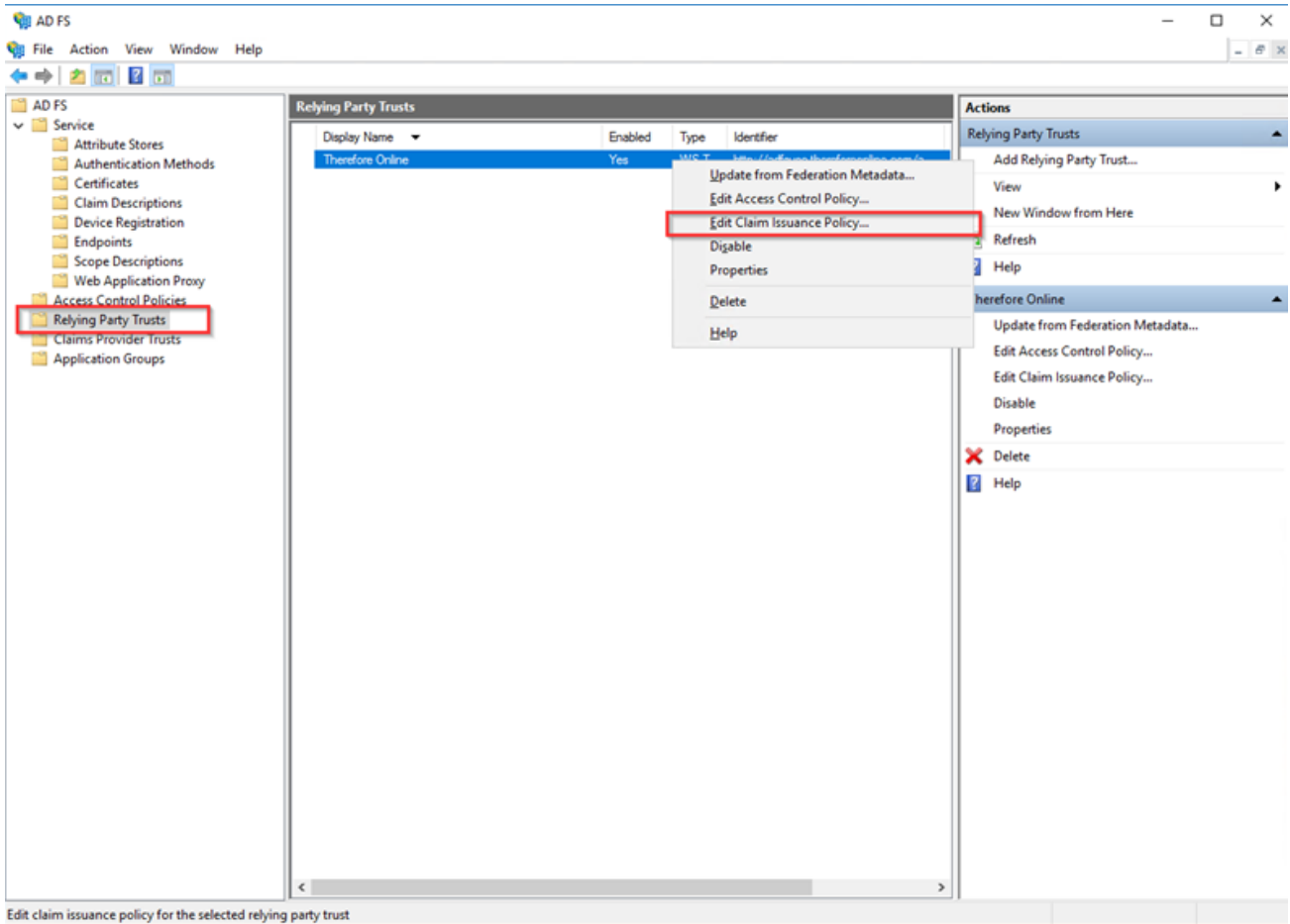
2.8 Configuring Claims Insurance Policy

When the relying party trust has successfully been added, keep the check box, '**Configure claims insurance policy for the application**' ticked. Click '**Close**' once completed.



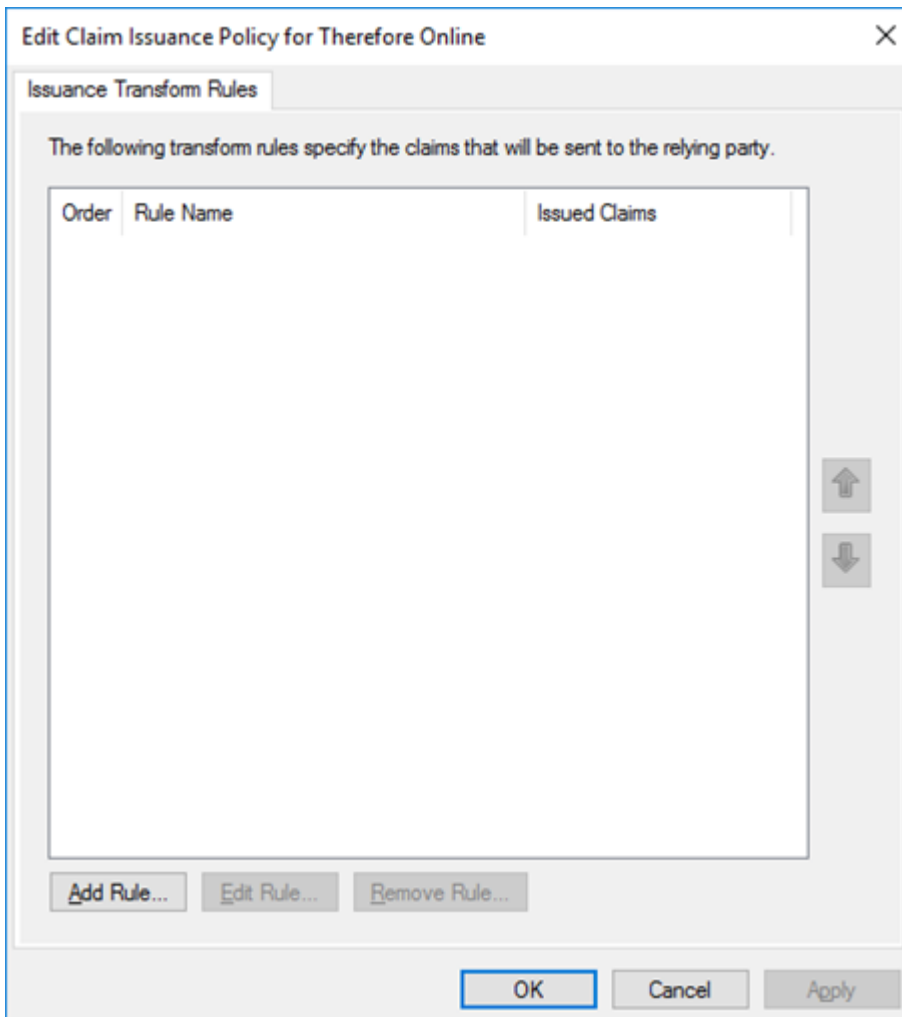
2.9 Editing Claim Insurance Policy

Once completed, return to the **AD FS** dialogue and under the **'Relying Party Trusts'** folder, right-click on the display name of the new trust and select **'Edit Claim Insurance Policy'**.



2.10 Adding a Rule

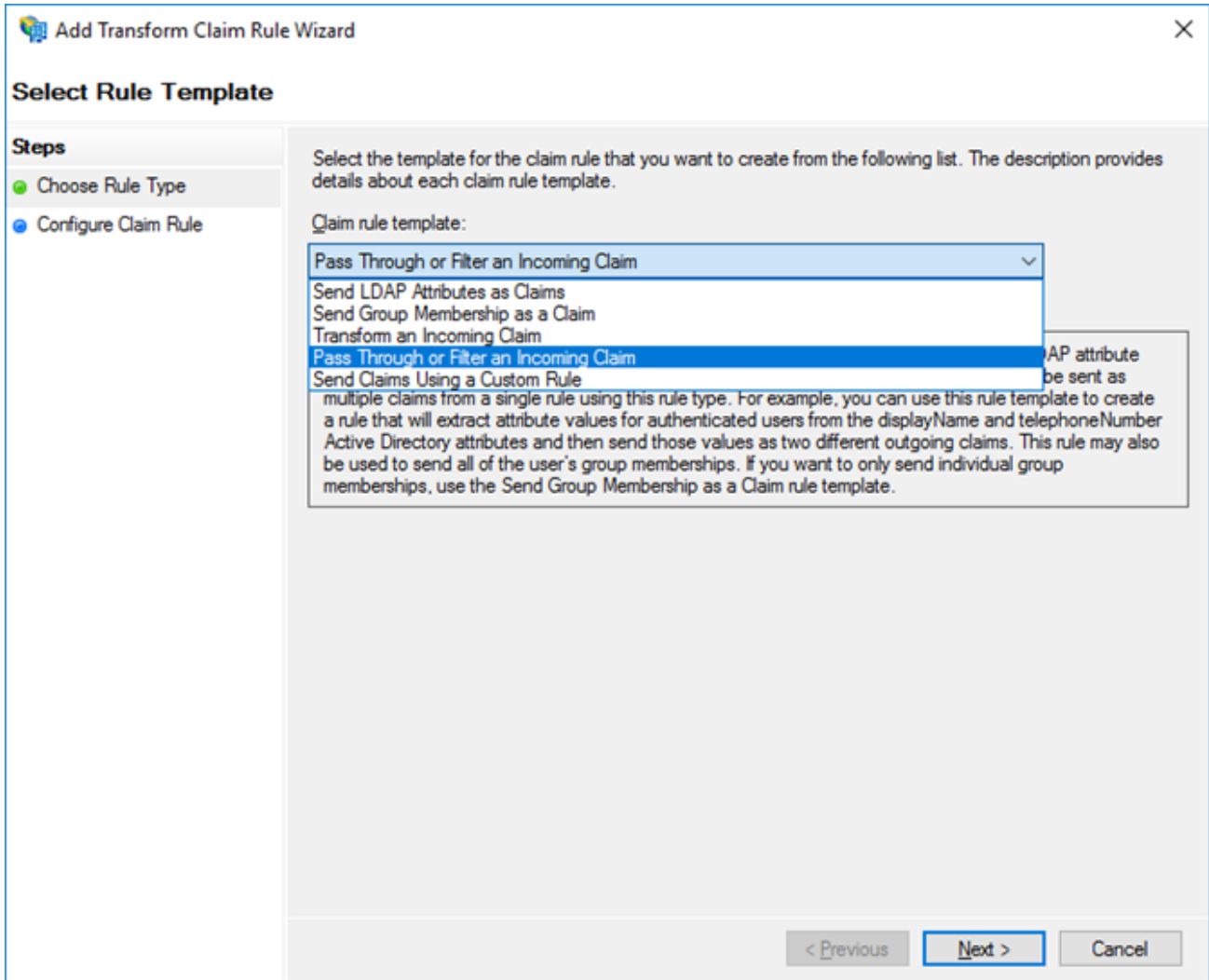
In the new dialog, click 'Add Rule'.



2.11 Choosing a Rule Type

2.11.1 Pass Through of Filter an Incoming Claim

As part of the first step in adding a rule, select the 'Claim rule template' as 'Pass Through or Filter an Incoming Claim' from the options available in the drop-down list.



2.11.1.1 Configuring a Claim Rule

Once the Claim Rule template has been set, add each of the following **'Incoming claim types'** to ADFS by repeating the process with the same template: **'Windows Account Name'** and **'UPN'**.

For each configuration of the claim rule, ensure to name each Incoming claim rule uniquely and mark the option of **'Pass through all claim values'**. It is imperative for each claim rule to be included in order to allow for Single Sign-on and workflow functionality.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name:

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type:

Incoming name ID format:

Pass through all claim values

Pass through only a specific claim value

Incoming claim value:

Pass through only claim values that match a specific email suffix value:

Email suffix value:

Example: fabrikam.com

Pass through only claim values that start with a specific value:

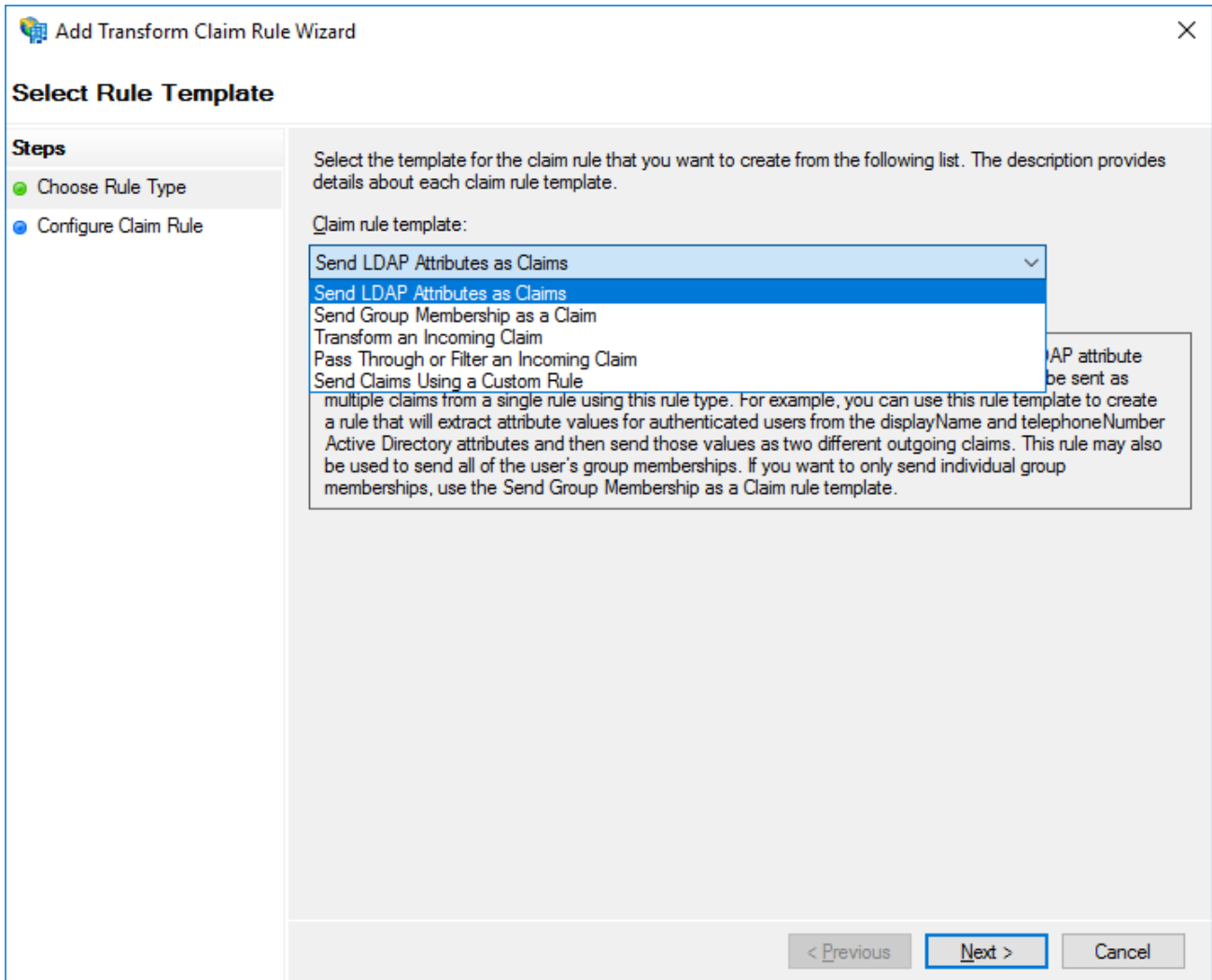
Starts with:

Example: FABRIKAM\

< Previous Finish Cancel

2.11.2 Send LDAP Attributes as Claims

As part of the second step in adding a rule, select the 'Claim rule template' as 'Send LDAP Attributes as Claims' from the options available in the drop-down list.



2.11.2.1 Configuring a Claim Rule

Once the Claim Rule template has been set, add each of the following 'LDAP attributes' to the mapping list: "E-Mail-Addresses", "Display-Name", "Token-Groups - Qualified by Domain Name".

Ensure the **Attribute store** is set to **Active Directory** and the **Outgoing Claim Type** is set as seen in the screenshot below.

Edit Rule - LDAP attributes [X]

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:

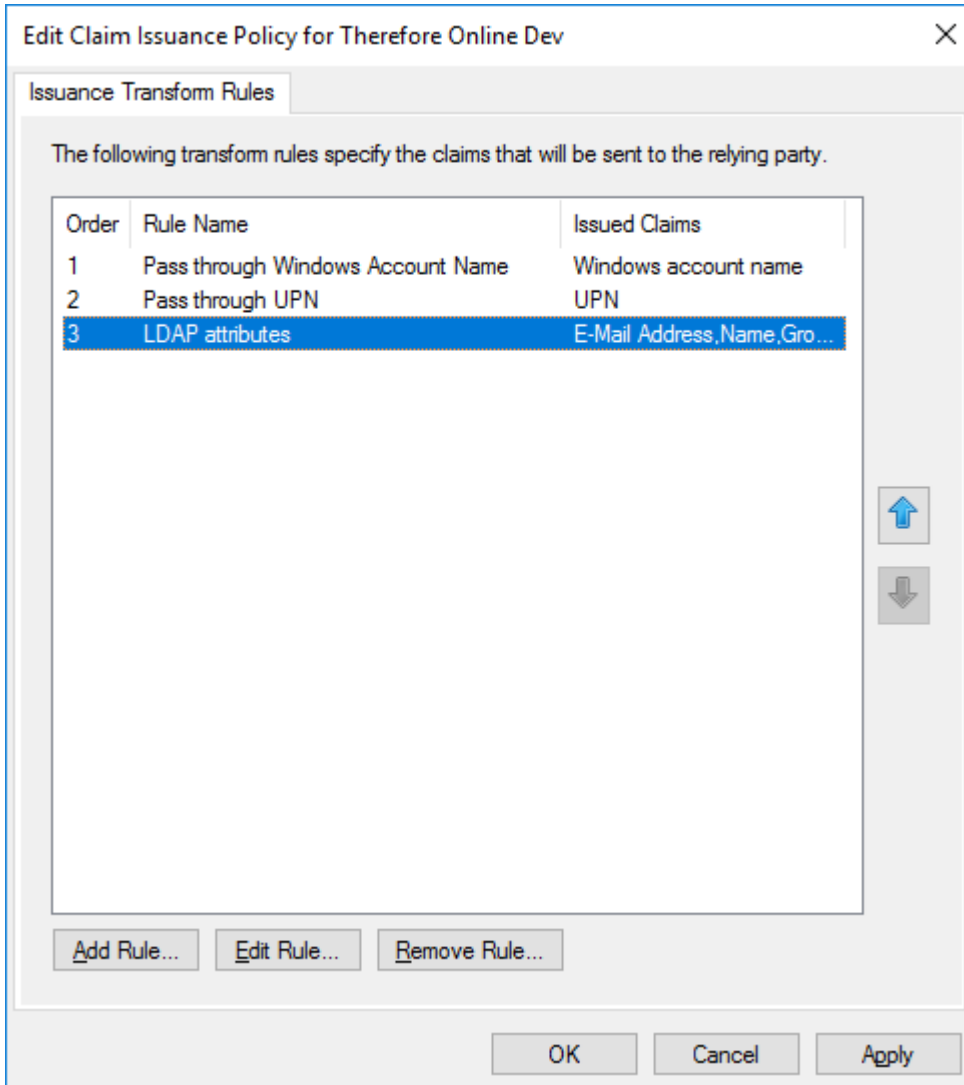
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
	Display-Name	Name
	Token-Groups - Qualified by Doma...	Group
*		

View Rule Language... [OK] [Cancel]

2.12 Setting all the Claim Rules

Once all the claim rules have been set, they will appear in the 'Edit Claim Issuance Policy for Therefore Online'; the order in which they appear does not matter.



2.13 Setting up ADFS configuration on Therefore Server side

Before you can continue with the configuration you need to request Therefore support (just open a ticket or reply to the previous ticket) to set up the ADFS configuration on the Therefore Server side (this can only be done by Therefore support, Canon technicians and customers do not have access to the Therefore server).

In the request mention that the customer side ADFS configuration is done and you are waiting for Therefore support to finish the server side configuration. Please also include the following information in the request:

1. Tenant name
2. Domain name that will be used for Single Sign-On
3. Federation Service name
4. Federation Service identifier
5. Federation metadata document (may not be needed, see important note below)



Note: You cannot do the next configuration steps before Therefore support confirms the setup is done on Therefore Server side and sends you the details for the ADFS connection.

The screenshot shows the ADFS Management console interface. On the left, a tree view shows the 'Service' folder expanded. In the center, the 'Service Overview' window is open, displaying the 'Federation Service Properties' dialog box. The 'General' tab is selected, showing fields for 'Federation Service display name' (set to 'Therefore Online ADFS'), 'Federation Service name' (circled in red), and 'Federation Service identifier' (circled in red). The 'Web SSO lifetime (minutes)' is set to 480. On the right, the 'Actions' pane is visible, with 'Edit Federation Service Properties...' circled in red. A red arrow points from this action to the dialog box.



Note:

It is highly recommended that the federation metadata document for the customer ADFS environment is reachable via the internet. To check if this is the case you can use the following Federation Metadata Explorer from Microsoft: <https://adfs-help.microsoft.com/MetadataExplorer/GetFederationMetadata>. By making sure that the federation metadata document is available via the internet, we can monitor changes that happen on the customer side (like certificate updates), and automatically change ADFS settings accordingly on Therefore Server side.

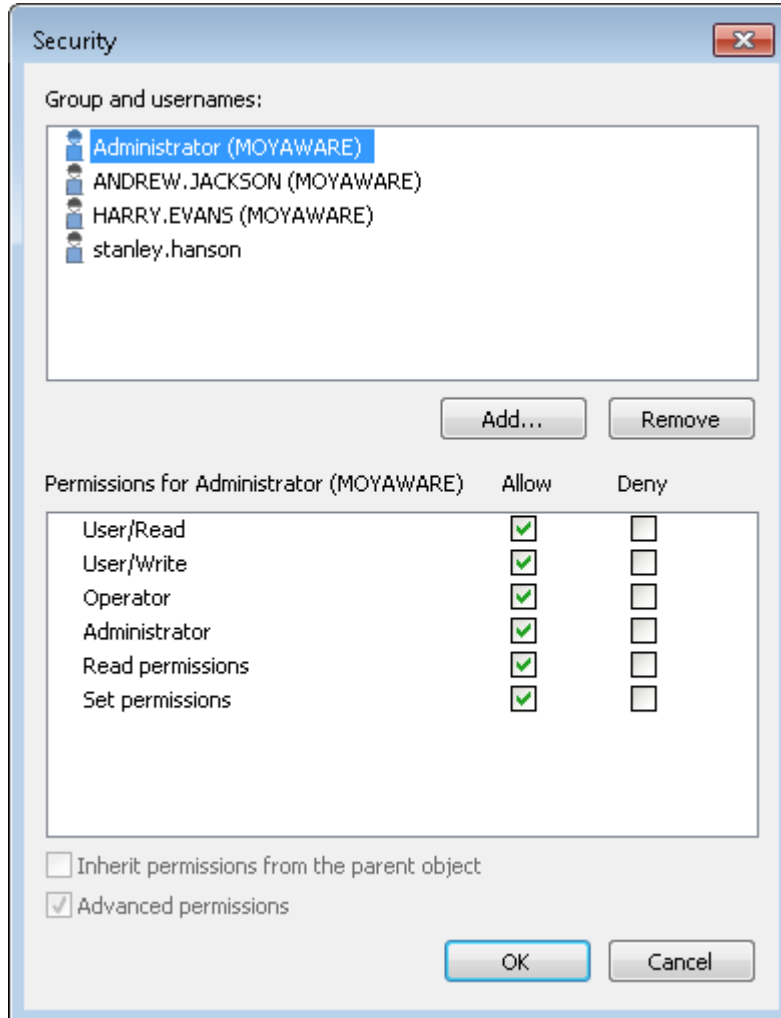
If for some reason it is not possible to make the document available, then you have to export and email the FederationMetadata.xml to Therefore support so we can import data about your claims providers from this file into our ADFS server.

Furthermore, if this document is not reachable via the internet the customer will need to let us know of any certificate changes in their environment and send us their new public key for the changed certificates which we need to manually update on the Therefore Server side. For more information about ADFS certificates please check the following link: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ts-td-certs-ad-fs>. To avoid this situation, always try to make the federation metadata document available for download via the internet.

2.14 Connecting to Therefore™



Note: For details on how to add SAML users, please read the section, '[Configuring Users for ADFS](#)' for automatic and manual configuration. User permissions will have to be set (via the 'Security' option in the Therefore™ Solution Designer) before you can continue to the next step in order to grant access to Therefore™ Online, as demonstrated in the dialog below:



Once the rules have been set the users will be able to log in via ADFS. When connecting to Therefore™ through an installed client application, the connection settings need to be configured. For Authentication provider, select the option for "Active Directory Federation (ADFS)", then click "Update from Server". The settings will be populated automatically.

Server Connection

Local Network

Directly connect to Therefore™ Server inside your LAN (DCOM)

Server name:

Internet

Connect to Therefore™ XML Web Service

Service address:
e.g.: https://machine/TheXMLServer

Authentication provider:

Clear saved logon information to stop automatic login.

Multi-Tenancy Settings

Tenant name:

Use this configuration as default for all users on this machine
Note: This option is only available when running as administrator.



Note: If you are using a Therefore™ Online v22 or older client the button “Update from Server” will not be available. In this case click on Settings and populate the fields with the correct links (these are the links provided by Therefore Support).

The screenshot shows a dialog box titled "Active Directory Federation" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Active Directory Federation Settings" containing four input fields:

Local Server URL:	<input type="text" value="https://adfs.yourdomain.com"/>
Remote Server URL:	<input type="text" value="URL provided by Therefore™ Support"/>
Local Audience URI:	<input type="text" value="URL provided by Therefore™ Support"/>
Remote Audience URI:	<input type="text" value="URL provided by Therefore™ Support"/>

At the bottom right of the dialog box, there are two buttons: "OK" and "Cancel".

3. Configuring Users for ADFS

You will learn:

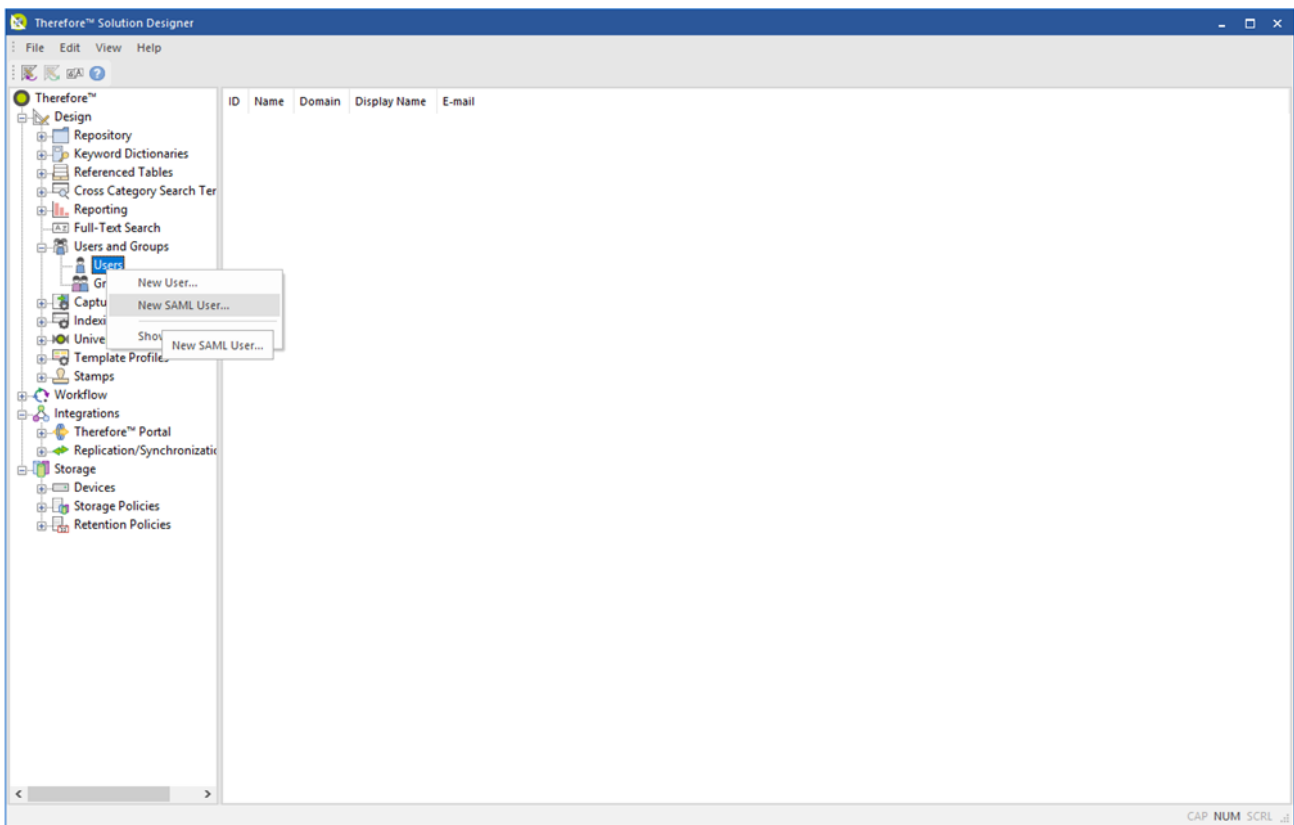
1. How to manually create users with permissions in ADFS.
2. How to automatically add users with ADFS permission.

3.1 Manual Configuration

3.1.1 Selecting SAML User

Once ADFS has been configured, users can be manually included in the permission settings via the **Therefore™ Solution Designer**.

Under the **Design > User and Groups** option, right-click on **'User'** and select **'New SAML User'** from the drop-down list.



3.1.2 Entering Usernames

In the **'SAML User Properties'** dialog, enter the Username(s) of the user(s) to match those in the Active Directory. Each user may also be given Therefore™ access permissions in Therefore™ too.

SAML User Properties

Username:

SAML Domain:

Display Name:

E-mail:

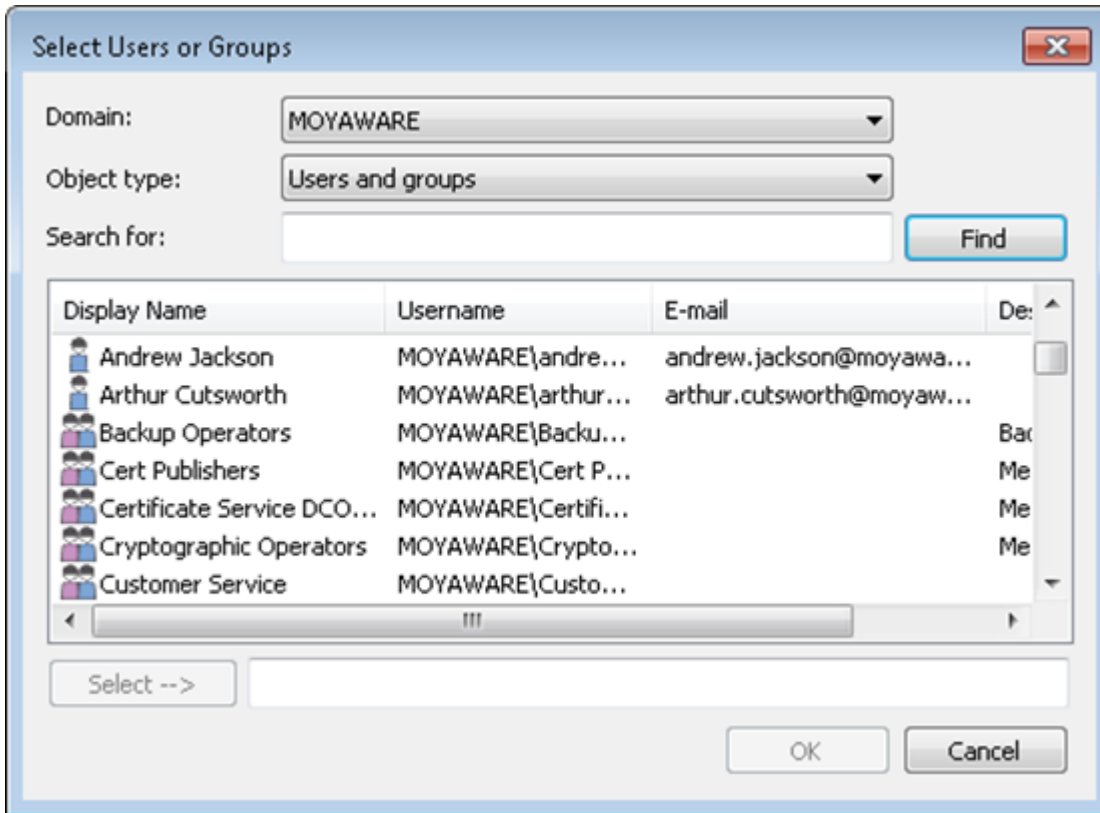
Account is disabled

User must change password at next logon

Member of:

3.1.3 Selecting Users or Groups

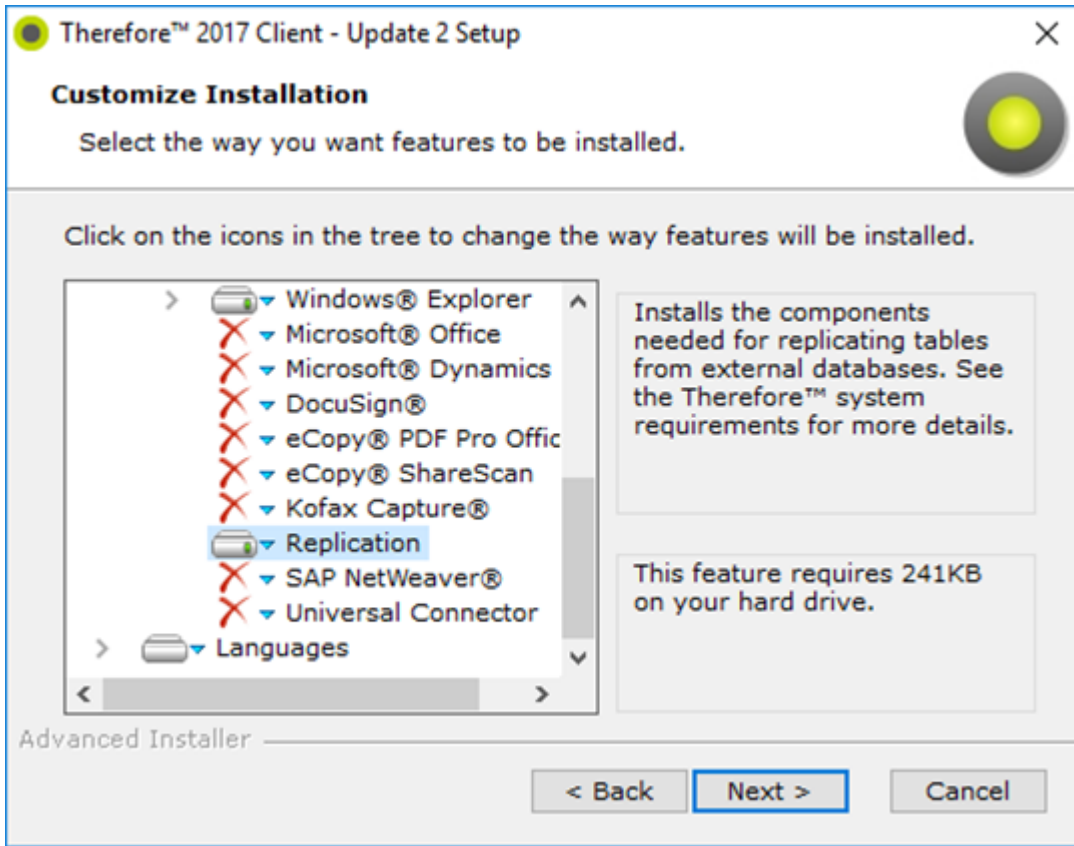
SAML domains can also be listed in Therefore™ under the **Select Users or Groups** dialog.



3.2 Automatic Configuration

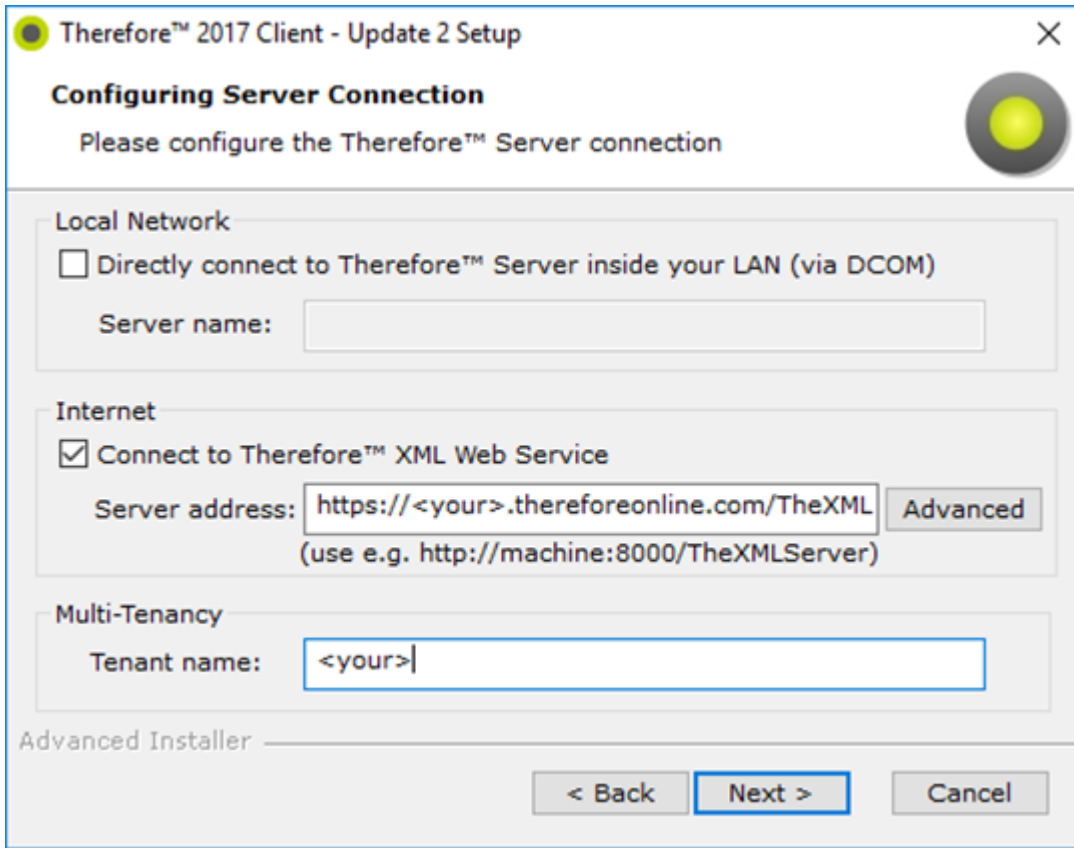
3.2.1 Selecting Replication

Ensure that **Replication** (under **Therefore™ Integrate**) has been selected. Languages can also be selected based on the user's preferences.



3.2.2 Connecting to Therefore™ XML Web Service

While in the Setup wizard, ensure to select the checkbox **Connect to Therefore™ XML Web Service** and enter the URL in order to connect to Therefore™ Online.



This can also be set up in the **Server Connection** settings of the **Therefore™ Solution Designer**.

Server Connection

Local Network

Directly connect to Therefore™ Server inside your LAN (DCOM)

Server name:

Internet

Connect to Therefore™ XML Web Service

Service address:
e.g.: https://machine/TheXMLServer

Advanced...

Clear saved logon information to stop automatic login.

Clear

Multi-Tenancy Settings

Tenant name:

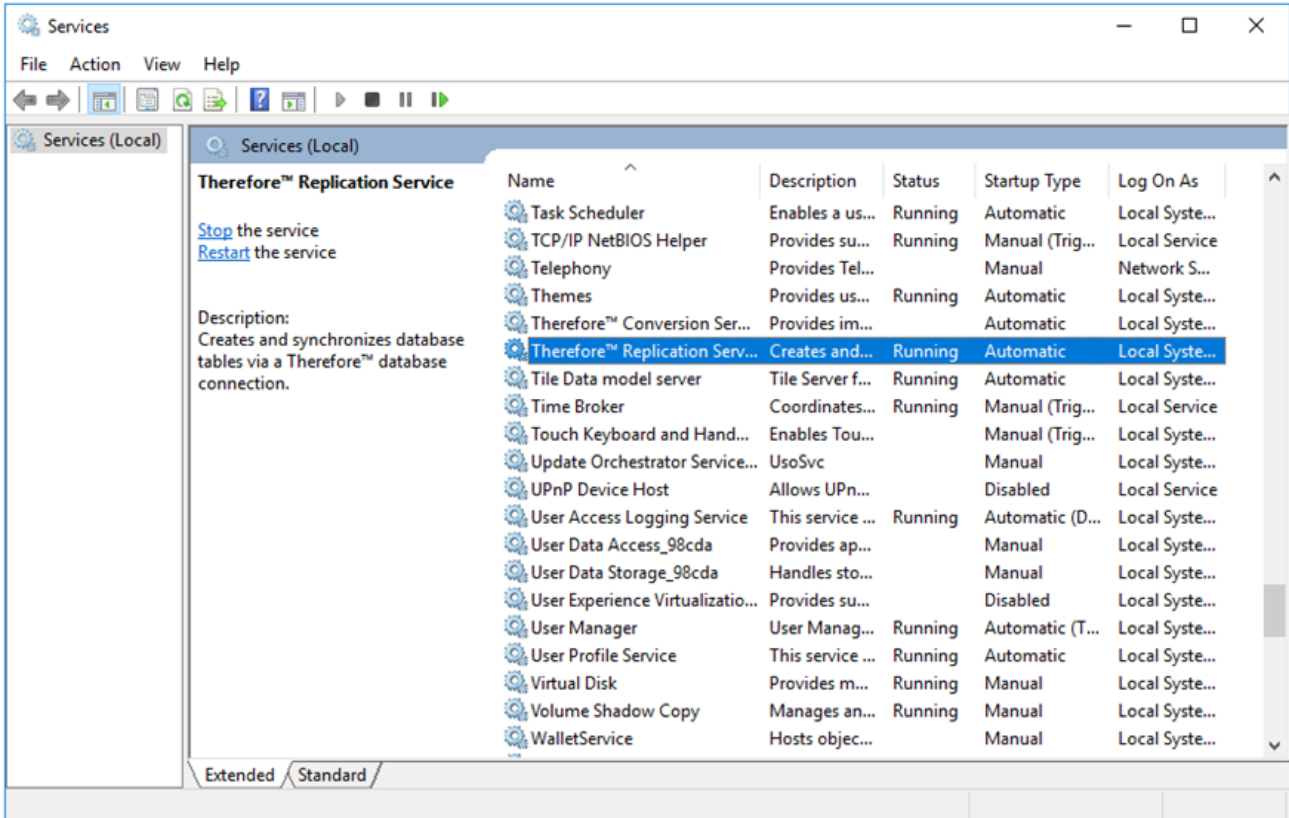
Use this configuration as default for all users on this machine

Note: This option is only available when running as administrator.

OK Cancel

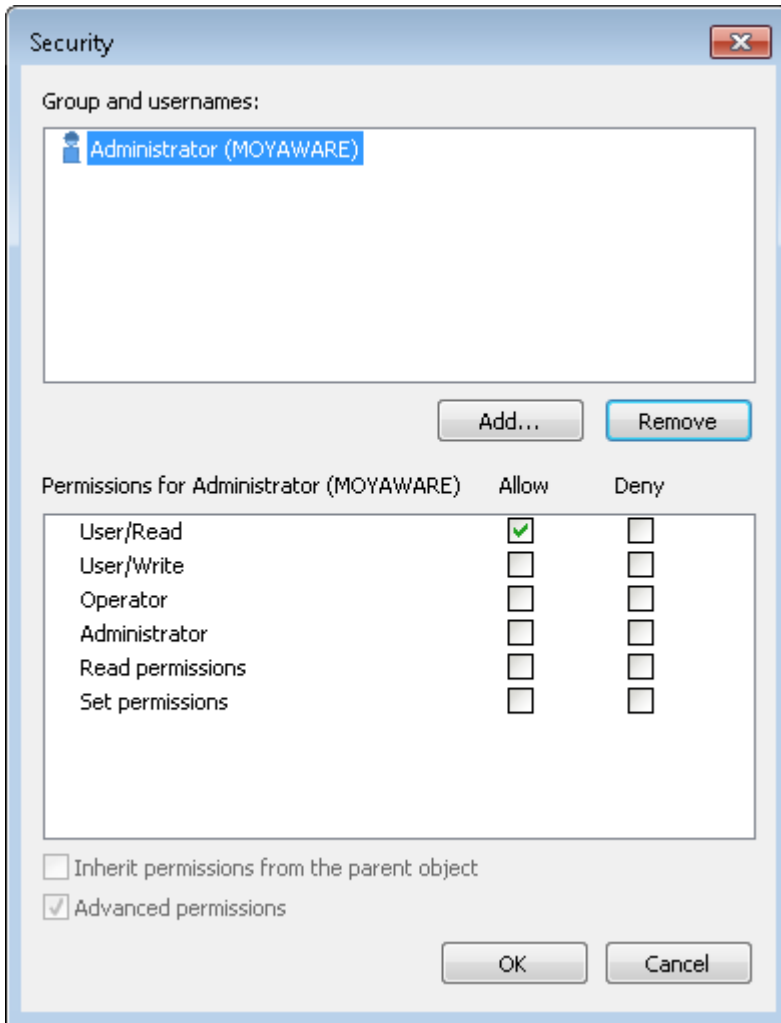
3.2.3 Setting Therefore™ Replication Service to Automatic

Once the setup has been completed, go to the 'Services' application on Windows and set the **Therefore™ Replication Service** (from the list) to automatic.



3.2.4 Setting Security Permissions

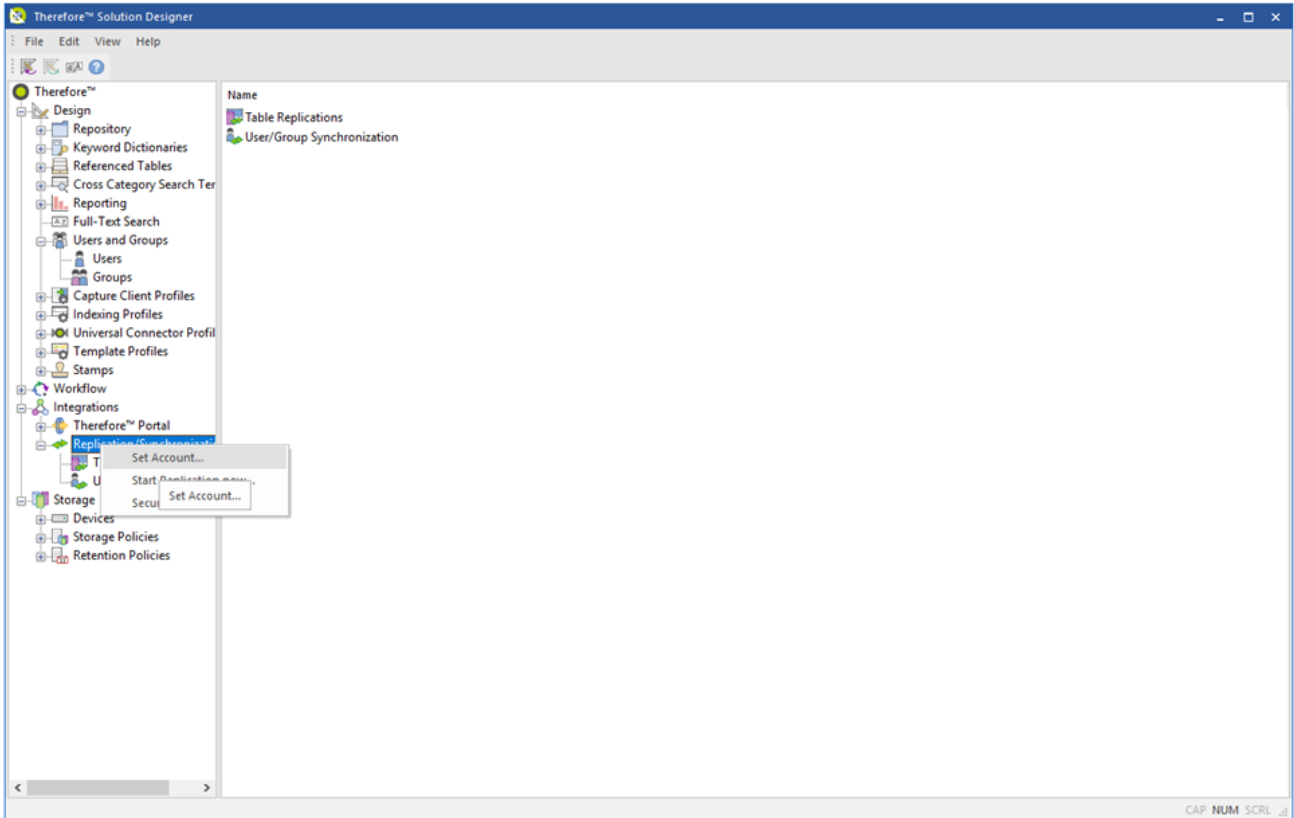
Security permissions can then be set for the replicated user by right clicking the Therefore™ logo at the top of the left-hand pane (and selecting 'Security').



Note: **It is not possible to replicate "Domain Users" and "Domain Admins" groups.**

3.2.5 Setting an Account

Return to **Therefore™ Solution Designer** (running as 'Administrator') and right-click on the **'Replication/Synchronization'** option (under **'Integrations'**) and select **Set Account**.



3.2.6 Providing a Username and Password for Connection

Select the **Provide username/password for connection** option and enter details pertaining to the user.

Set Account [Close]

Use Identity Federation to connect

Provide username/password for connection

Username:

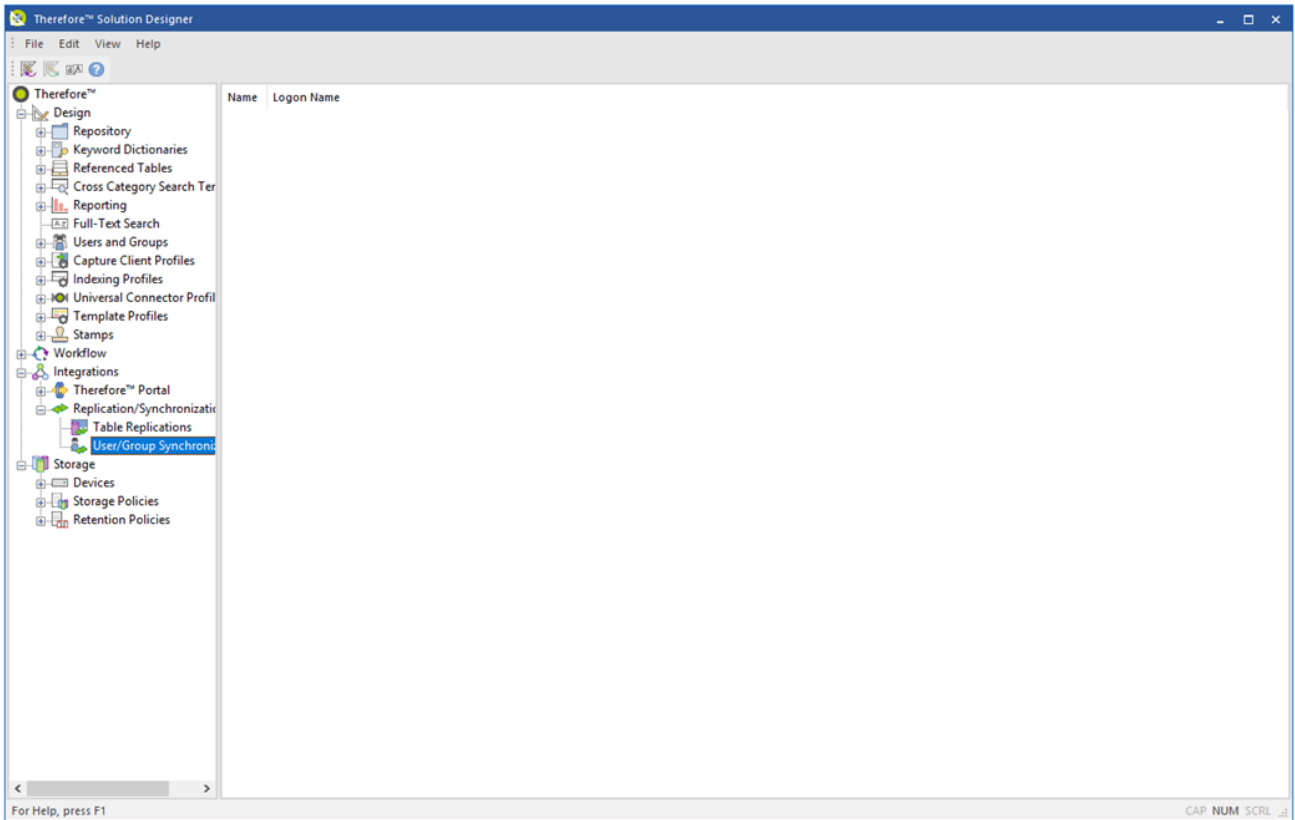
Password:

Set the account the replication service will use to connect to the Therefore™ Server service.

[OK] [Cancel]

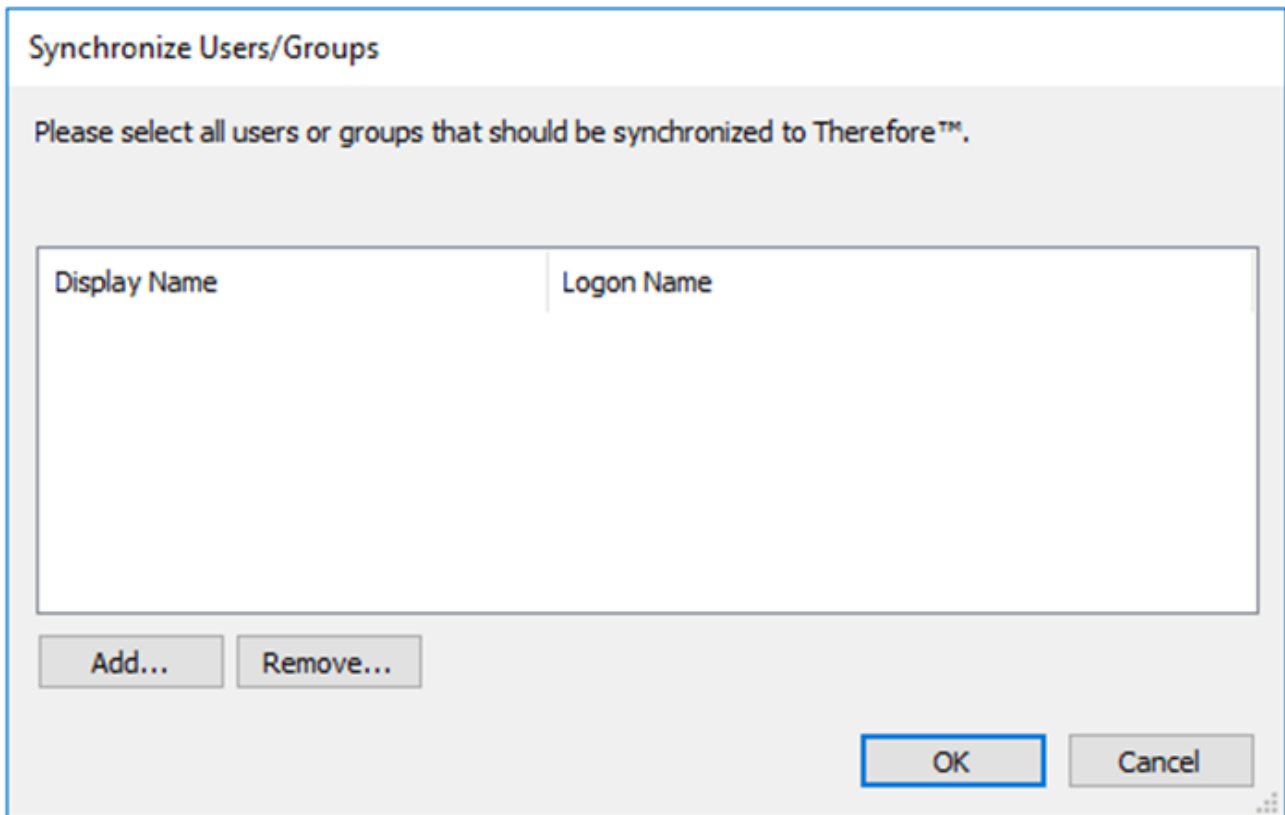
3.2.7 User/Group Synchronization

Under the Replications/Synchronization option, select **User/Group Synchronization**.



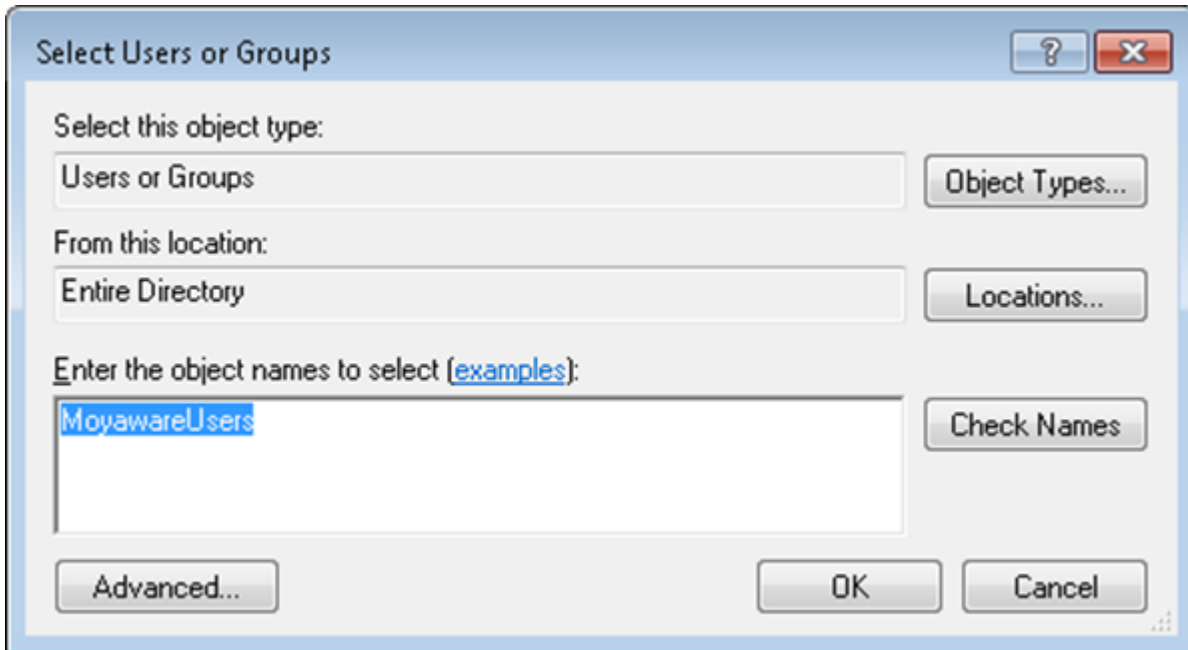
3.2.8 Selecting Users or Groups

In the **Select Users or Groups** dialog, click the **Add** button.



3.2.9 Entering Group Names

Enter the **Group Names** to select from the object type and location.



3.2.10 Synchronizing Users /Groups from the List

Select the Users that need to be synchronized from the displayed list in the dialog.

