



360° Online authentication

Version June 2019

This document will help you set up a trust for authentication of 360° Online users between the organization's 360° Online service and either Office 365/Azure AD or Active Directory Federation Services.

Contents

1	Introduction	2
2	Authentication using Office 365	2
2.1	Introduction	2
2.2	Prerequisites	3
2.3	Step by step	3
3	Authentication using on-premise Active Directory Federation Services	6
3.1	Introduction	6
3.2	Prerequisites	6
3.3	Integration setup – step by step	7
3.4	Finding the WS-Federation URL	14
4	Authentication using Microsoft accounts	15
4.1	Introduction	15
4.2	Prerequisites	15
4.3	Step by step	15

1 Introduction

Users of a 360° Online service needs to be authenticated through a central authentication source for their organization. 360° Online supports several sources:

- Office 365 (utilizing embedded Azure AD)
- On-premise Active Directory Federation Services.
- Microsoft accounts – through organization’s own Azure AD

This document explains how to configure the authentication at the customer side.

2 Authentication using Office 365/Azure Active Directory

2.1 Introduction

The following steps are required to enable authentication of 360° Online users with Office 365:

- a. Create an Azure account
- b. Configure 360° Online as a new application in your organization’s Azure Active Directory

2.2 Prerequisites

The administrator account for your organization's Office 365 subscription.

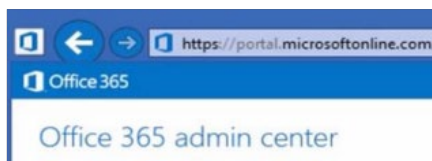
A valid credit card for the registration of the Windows Azure account. The Azure Active Directory is a free service, but registration might require a valid credit card for payment method.

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

2.3 Step by step

STEP 1: Verify that you have the administrator account

Open <https://portal.office.com> in your browser and log in. If you can see Office 365 admin center, you have the correct account information.

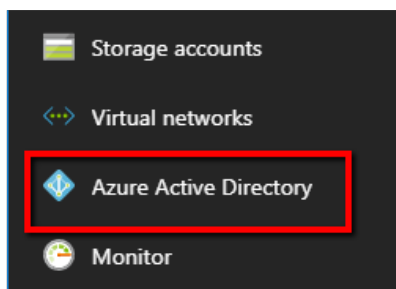


STEP 2: Register for an Azure account

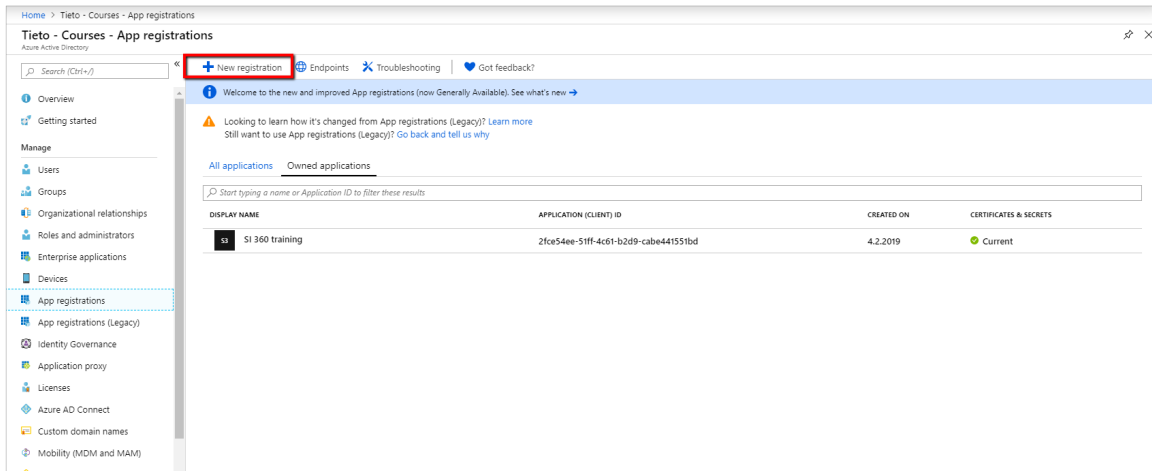
1. Open <https://azure.microsoft.com/en-us/free/> in your browser and create your account.
2. Sign in with your Office 365 administrator account and complete registration.

STEP 3: Add an application to Azure Active Directory

1. Open <https://portal.azure.com> in your browser and log in with your Azure account.
2. Scroll down and select **Azure Active Directory** in the left-hand menu.



3. Select **App registrations** in the top menu and click **New application registration**.



4. Enter the following information in the form and click **Register**:

- a. Name: Public 360
- b. Supported account types: Accounts in this organizational directory only
- c. Redirect URI:
https://customername.public360online.com/_layouts/si/loginresponse.aspx

Home > Tieto - Courses - App registrations > Register an application

Register an application

*** Name**
 The user-facing display name for this application (this can be changed later).

Supported account types
 Who can use this application or access this API?

Accounts in this organizational directory only (Tieto - Courses)
 Accounts in any organizational directory
 Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

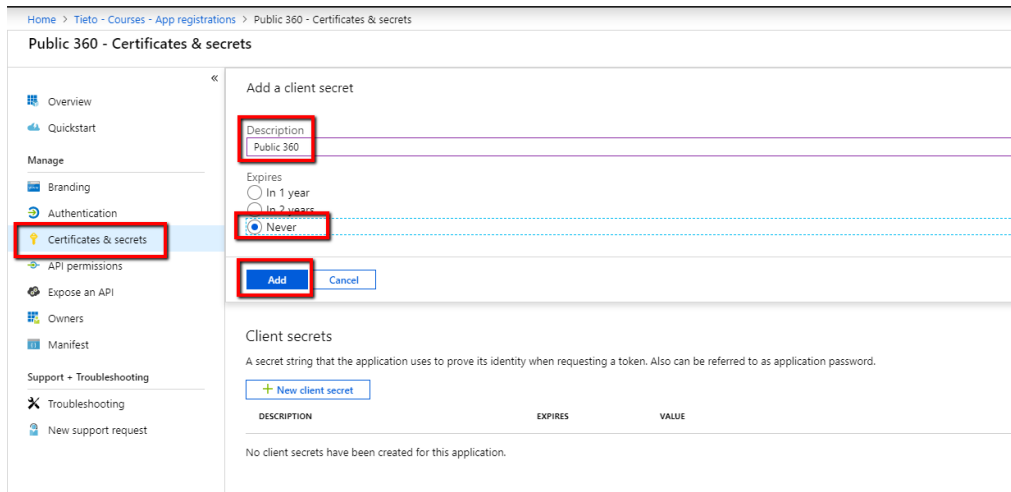
Redirect URI (optional)
 We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

If your organization is using the same app for multiple 360° Online environments, go to **Authentication** and add a REDIRECT URI for each environment.

- Click on **Certificates and secrets**, enter "Public 360" in the description, select **Never**, then click **Add**.



Copy the key value.

Client secrets

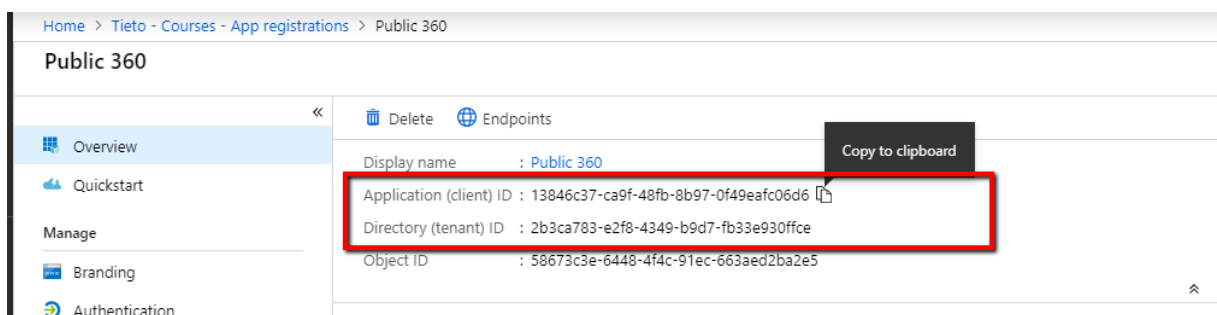
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

DESCRIPTION	EXPIRES	VALUE
Public 360	31.12.2299	Gd:OG*D-3U0E8kUVTvEpMmR5aPY:14WR

Copy to clipboard

- Go back to the application **Overview** and copy the **Application (Client ID)** value and the **Directory (tenant) ID** value.



- Send **Directory ID**, **Application ID** and **key value** to your contact person at Tieto or add the information to the purchase order form. The setup is now complete.

3 Authentication using on-premise Active Directory Federation Services

3.1 Introduction

The following steps are required to enable authentication of 360° Online users via on-premise Active Directory:

- a) On-Premise deployment of Active Directory Federation Services (ADFS) to enable Active Directory federation
- b) Configure on-premise ADFS with your organization's 360° Online service as trusted relying party

This document describes (b). (a) is a prerequisite, as described below.

3.2 Prerequisites

The following are prerequisites for enabling ADFS – 360° Online service integration:

- ADFS server (ADFS 2.0 or higher/Windows Server 2008 R2 or higher) has been setup on-premise.

These documents provide relevant information:

[TechNet - ADFS Deployment Guide](#)

[TechNet - Best Practices for Secure Planning and Deployment of AD FS](#)

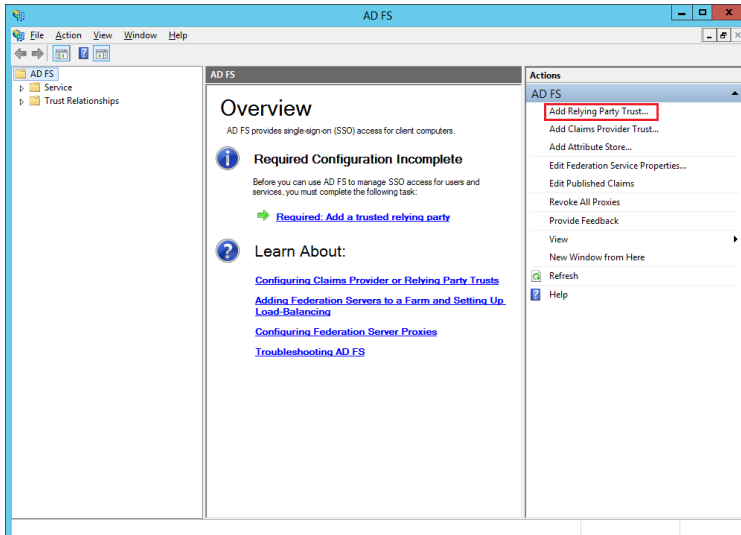
ADFS Federation metadata URL of the following format should be publically accessible

<https://ads.contoso.com/FederationMetadata/2007-06/FederationMetadata.xml>

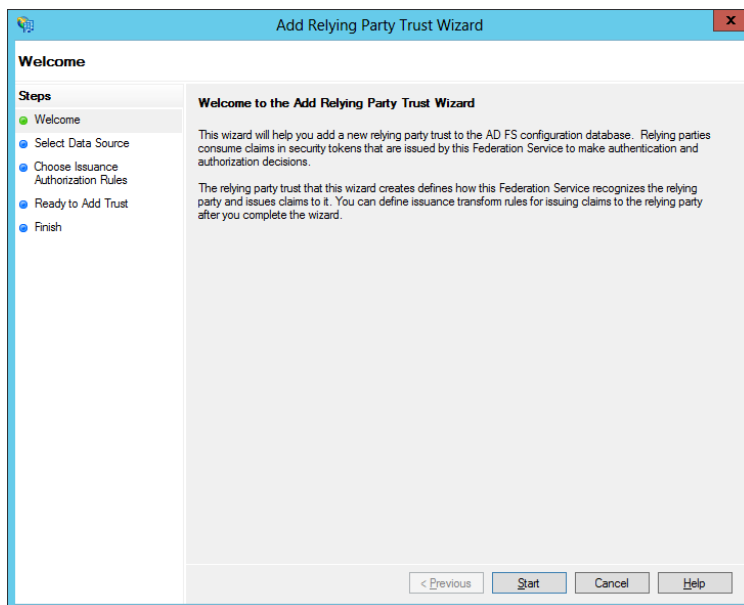
3.3 Integration setup – step by step

The following steps setup trust between ADFS and your organization's 360° Online service.

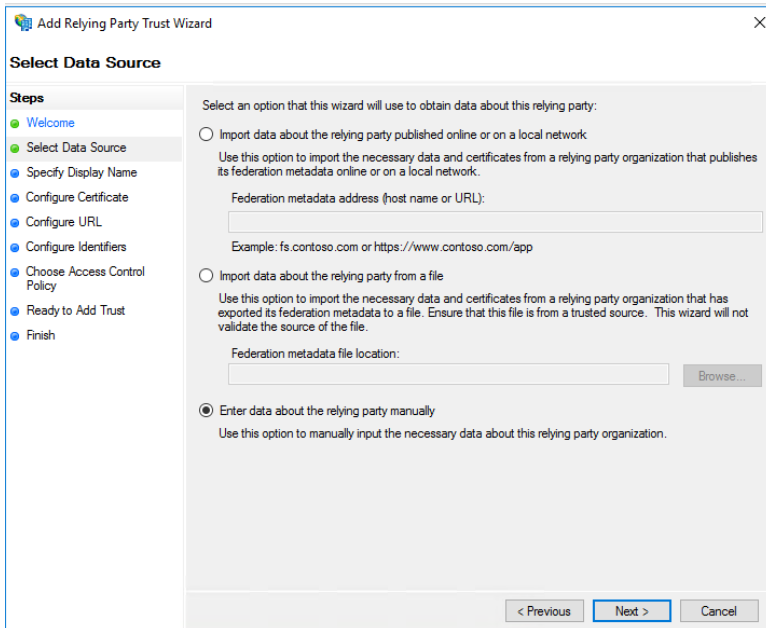
STEP 1: Navigate to ADFS management screen and click on **Add Relying Party Trust**



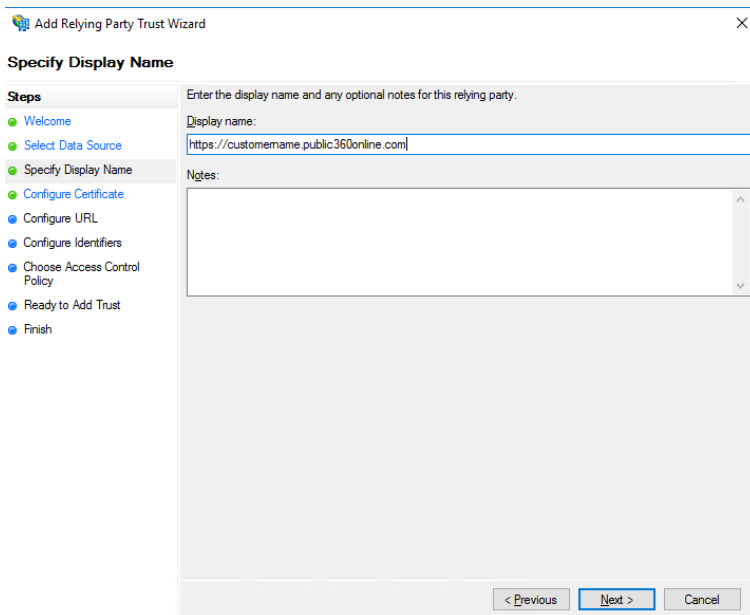
STEP 2: Click on **Start** to initiate addition of relying party



STEP 3: Select **Enter data about the relying party manually** and click **Next** to continue.

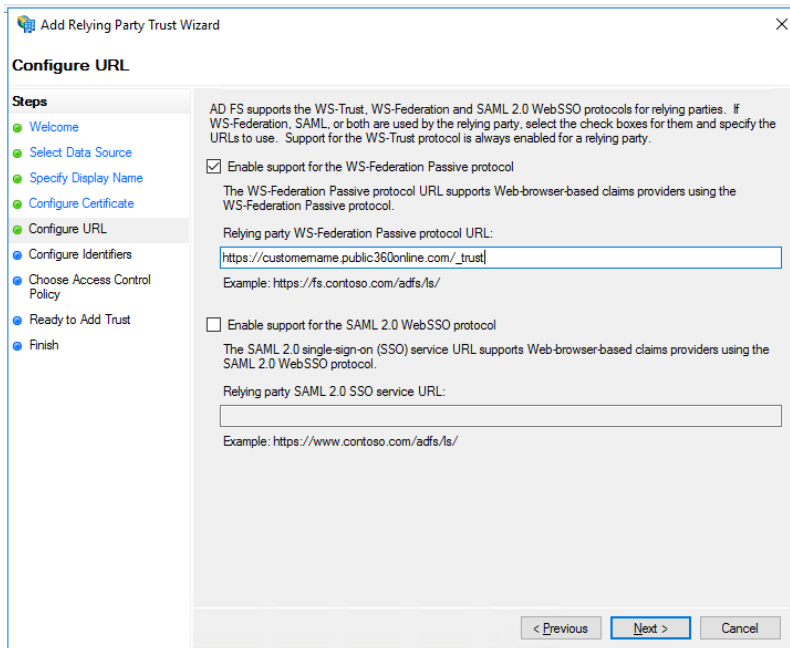


STEP 4: Enter the URL for your organization’s 360° Online service as the **Display name** and click on **Next** to continue to next step. On the step, “Configure Certificate”, click **Next** again.



STEP 5: Select **Enable support for the WS-Federation Passive protocol**, and enter the URL of your 360° Online service, followed by **/_trust** in the textbox **Relying party WS-Federation Passive protocol URL**.

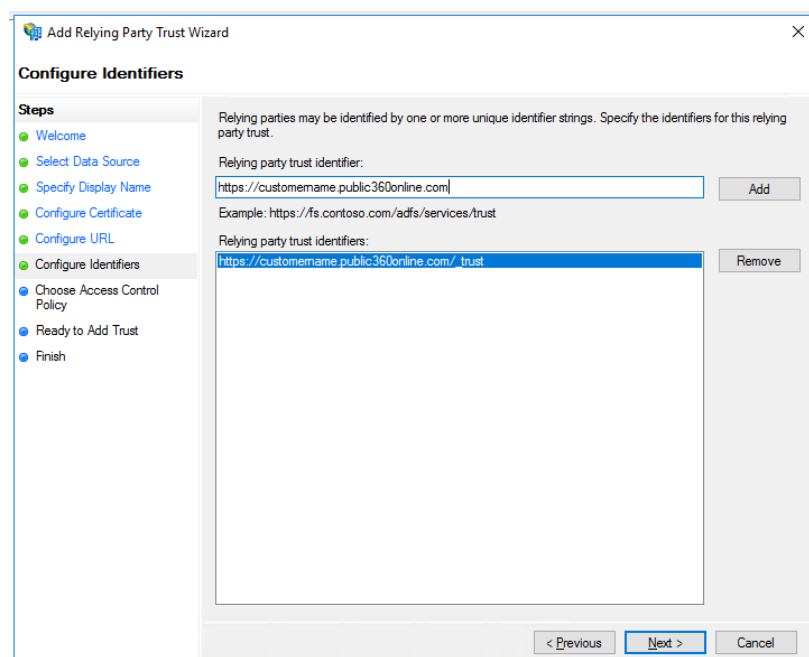
Example: `https://customername.public360online.com/_trust`



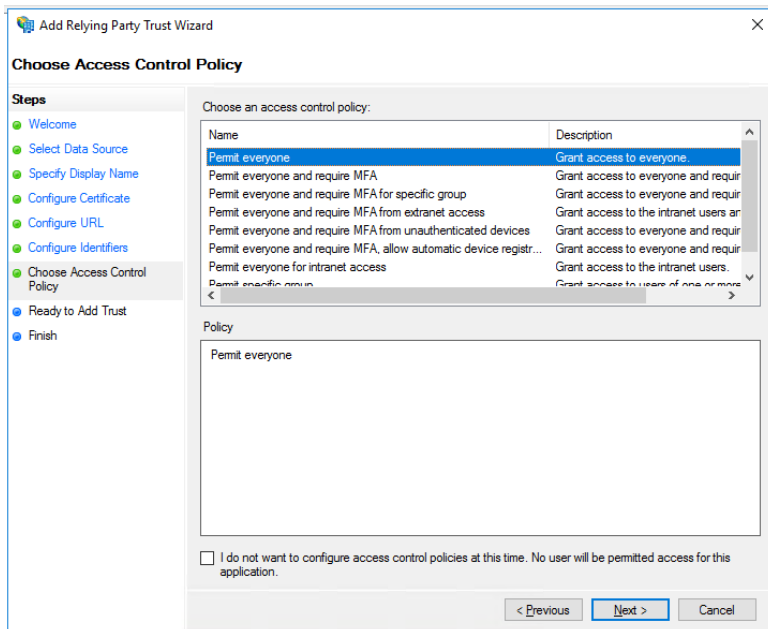
STEP 6: Enter the URL of your 360° Online service in the text box **Relying party trust identifier** and click **Add**.

Example: `https://customername.public360online.com`

You should then have two entries in this list. Click **Next**.

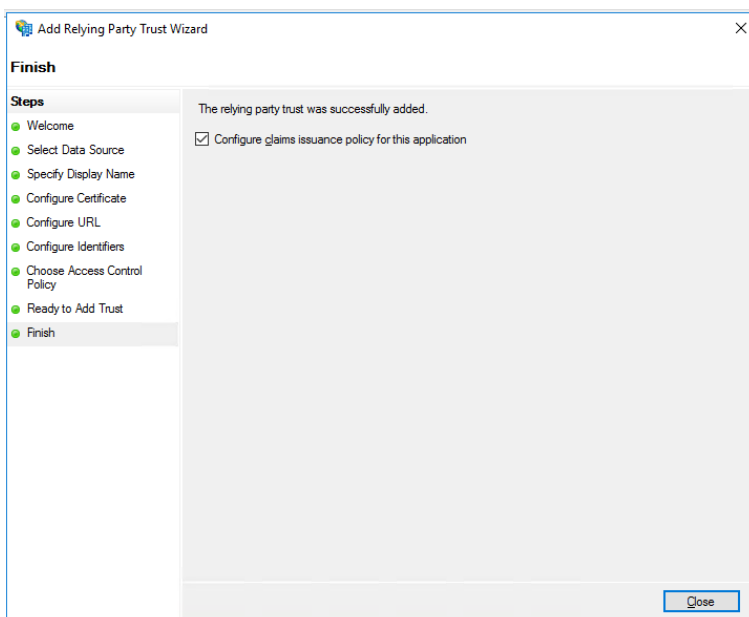


STEP 7: Select **Permit everyone** from the list and click **Next** to continue.

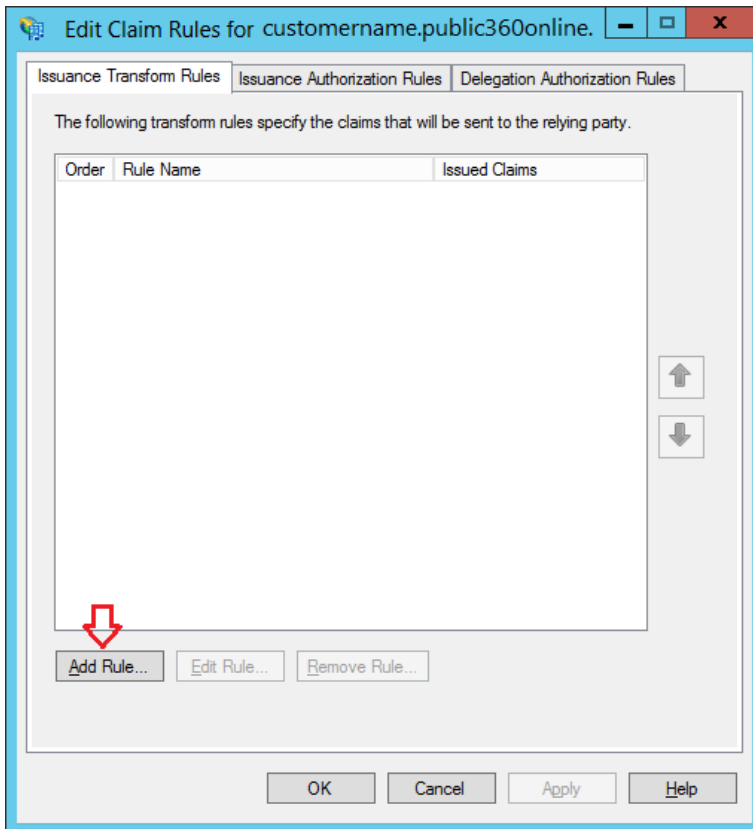


STEP 8: On the next step "Ready to add trust" click **Next** without making any changes.

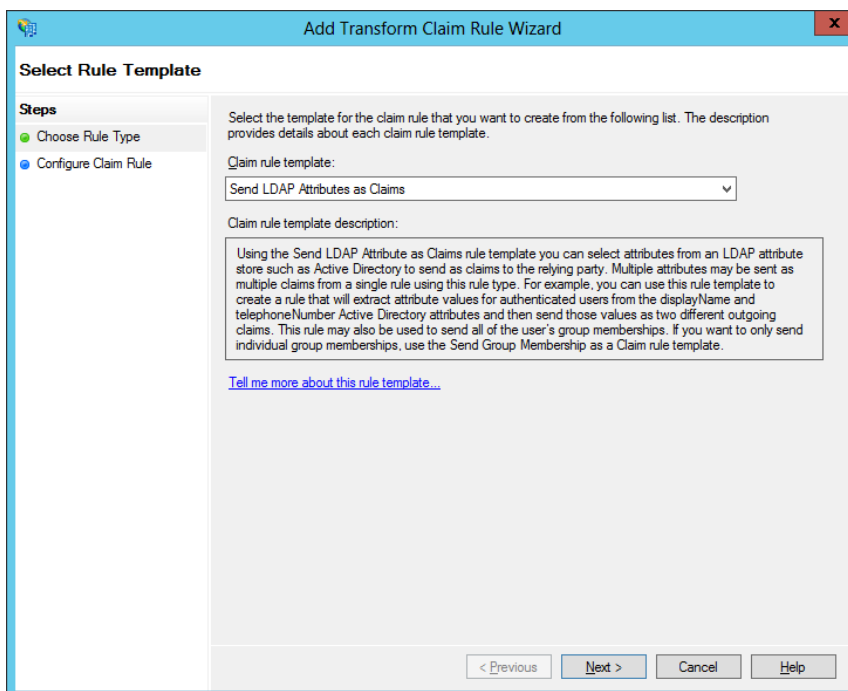
STEP 9: Click on **Close** to launch **Edit Claims Rules** dialog.



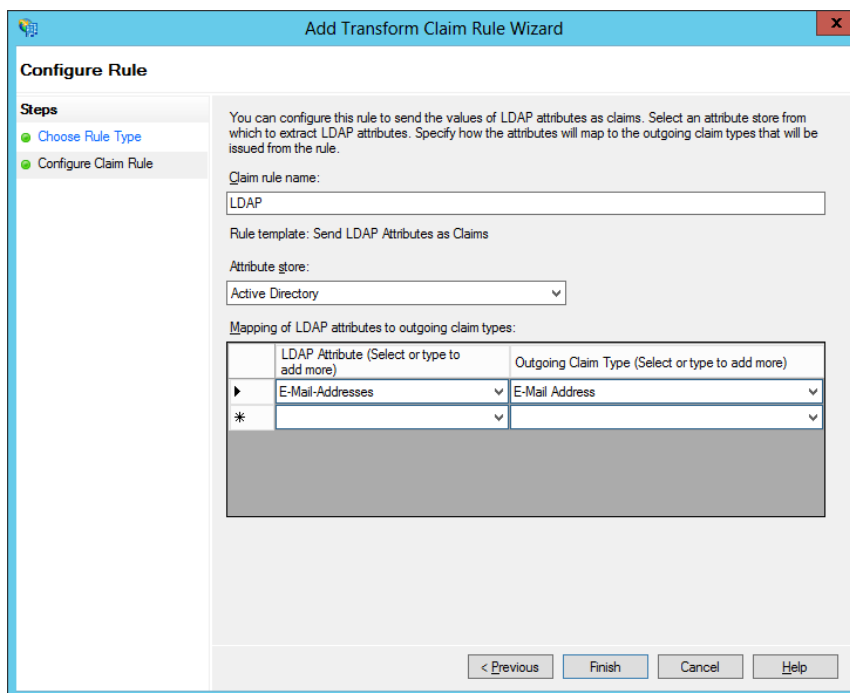
STEP 8: In the **Edit Claim Rules** dialog, click **Add Rule** to add claims rules.



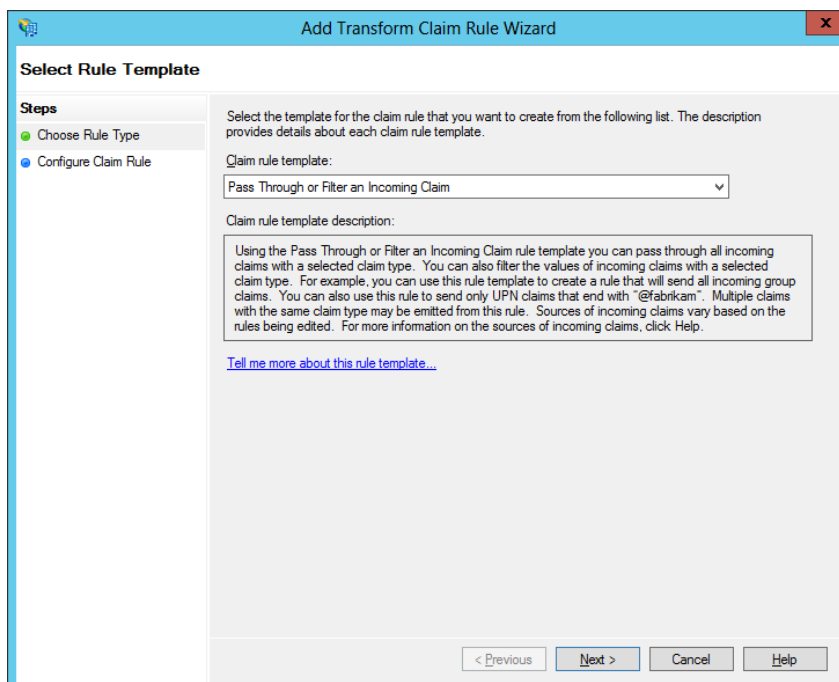
STEP 9: Select **Send LDAP Attributes as Claims** and click **Next**.



STEP 10: Add **E-Mail-Addresses** as displayed in the dialog below. Click **Finish** to continue



STEP 11: Click on **Add Rule** again to add **Windows Account Name** to the set of claims. Select **Pass Through or Filter an Incoming Claim** and click **Next** to continue.



STEP 12: Add **Windows Account Name** as mentioned in the dialog below. Click **Finish** to end the wizard.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The title bar reads 'Add Transform Claim Rule Wizard'. On the left, a 'Steps' pane shows 'Choose Rule Type' and 'Configure Claim Rule' (the current step). The main area contains the following fields and options:

- Claim rule name:** A text box containing 'Windows account name'.
- Rule template:** A dropdown menu set to 'Pass Through or Filter an Incoming Claim'.
- Incoming claim type:** A dropdown menu set to 'Windows account name'.
- Incoming name ID format:** A dropdown menu set to 'Unspecified'.
- Options:**
 - Pass through all claim values
 - Pass through only a specific claim value
 - Incoming claim value: [Text box]
 - Pass through only claim values that match a specific email suffix value:
 - Email suffix value: [Text box]
 - Example: fabrikam.com
 - Pass through only claim values that start with a specific value:
 - Starts with: [Text box]
 - Example: FABRIKAM\

At the bottom, there are four buttons: '< Previous', 'Finish', 'Cancel', and 'Help'.

STEP 13: Click on **Add Rule** again to add **UPN** to the set of claims. Select **Pass Through or Filter an Incoming Claim** and click **Next** to continue.

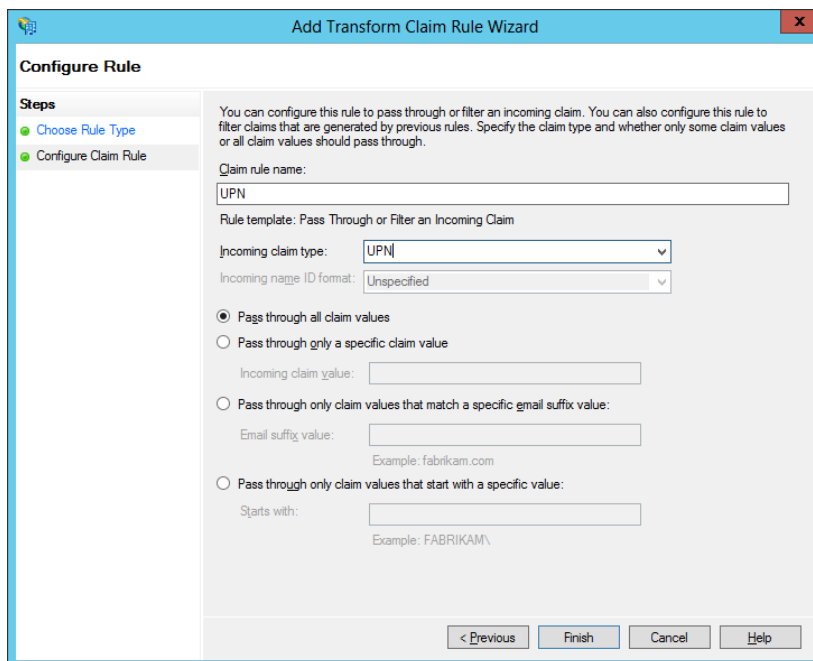
The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Select Rule Template' step. The title bar reads 'Add Transform Claim Rule Wizard'. On the left, a 'Steps' pane shows 'Choose Rule Type' and 'Configure Claim Rule' (the current step). The main area contains the following fields and options:

- Claim rule template:** A dropdown menu set to 'Pass Through or Filter an Incoming Claim'.
- Claim rule template description:** A text box containing the following text:

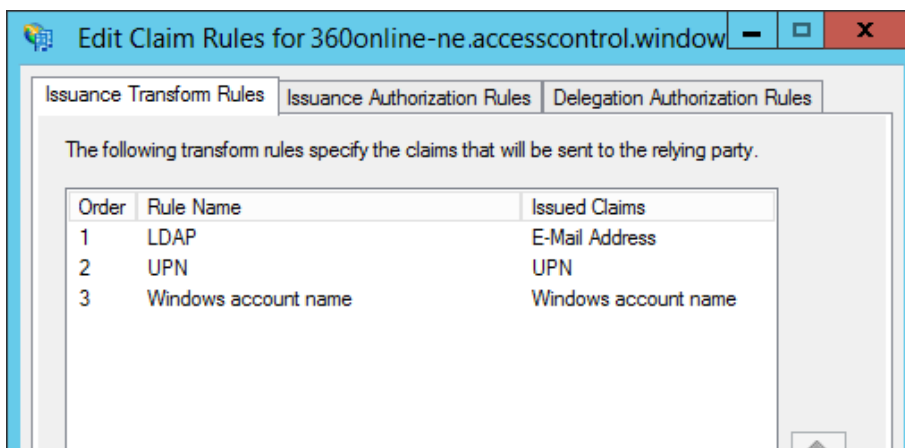
Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". 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.
- [Tell me more about this rule template...](#)

At the bottom, there are four buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

STEP 14: Add **UPN** as mentioned in the dialog below. Click **Finish** to end the wizard.



STEP 15: Click **OK** to close the Edit Claim Rules dialog and end the configuration setup.



3.4 Finding the WS-Federation URL

The URL for the FederationMetadata.xml is standardized for all ADFS installations. Assuming your ADFS instance is hosted at <https://adfs.contoso.com>, the WS-Federation URL with the FederationMetadata.xml is located at <https://adfs.contoso.com/FederationMetadata/2007-06/FederationMetadata.xml>.

Return the WS-Federation URL to your contact person at Tieto or add the information to the purchase order form. The setup is now complete.

4 Authentication using Microsoft accounts

4.1 Introduction

The following steps are required to enable authentication of 360° Online users with Microsoft accounts:

- a. Create new or use existing Microsoft account for one of your organization's 360° Online service's dedicated contact person.
- b. Create new Azure AD with that Microsoft Account.
- c. All 360° Online users in the organization must create new or use their existing Microsoft accounts.
- d. Add Microsoft accounts for other 360° Online users in your organization.
- e. Configure 360° Online as a new application in your organization's Azure Active Directory.

4.2 Prerequisites

Internet connection and a web browser.

A dedicated contact person for your organization's 360° Online service who will perform step by step.

A valid credit card for the registration of the Azure account. The Azure Active Directory is a free service, but registration might require a valid credit card for payment method.

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

Information about each 360° Online user's Microsoft account name. New users can also be added at later time.

4.3 Step by step

STEP 1: Create a new Microsoft Account if, you don't already have one.

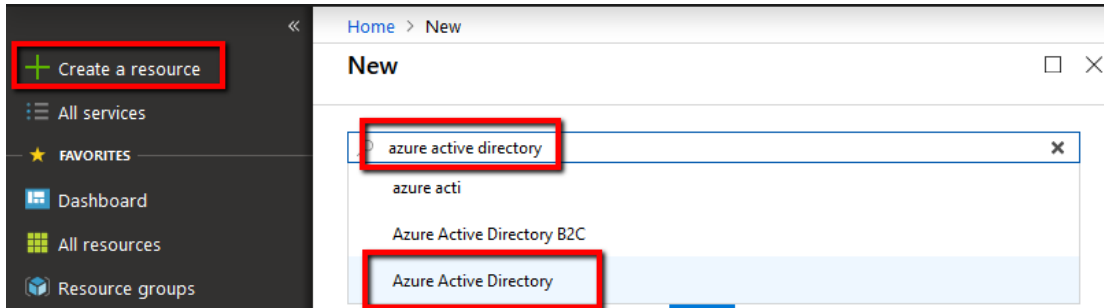
Open the Microsoft account sign-up page below and select **No account? Create one!**

<https://login.live.com/login.srf?lw=1>

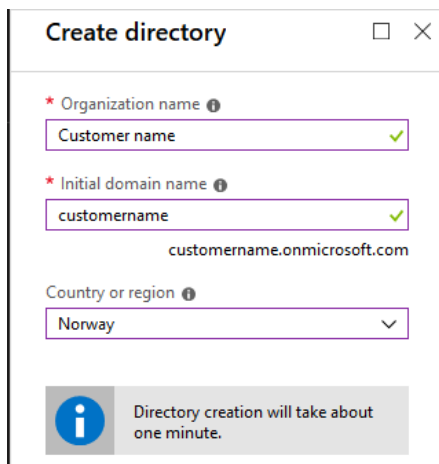
If you need help in that process, check out Microsoft's help page:

<https://support.microsoft.com/en-us/help/4026324/microsoft-account-how-to-create>

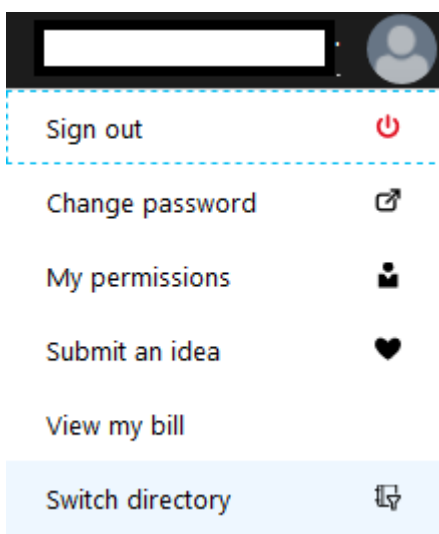
STEP 2: Click **Create a resource**, search for “Azure Active Directory” and select **Azure Active Directory** from the search result. Click **Create** on the next page.



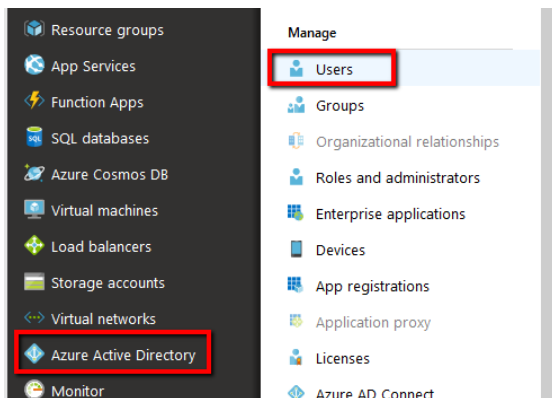
STEP 3: Enter **name of your organization, your preferred domain** (lower case letters) and the **country** your organization reside in, then click **Create**. Wait until it’s been created.



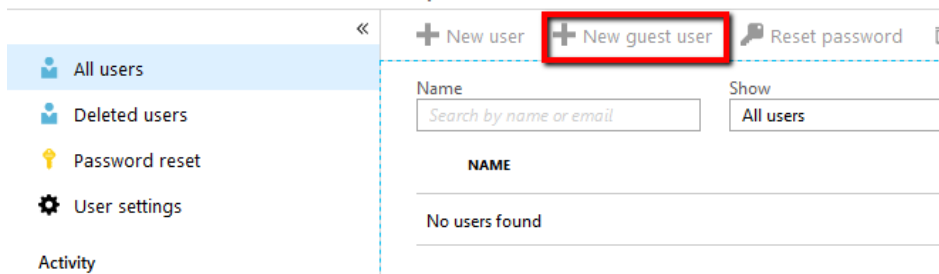
STEP 4: Once created, click the user dropdown menu in the top right corner of the browser, and select **Switch Directory**.



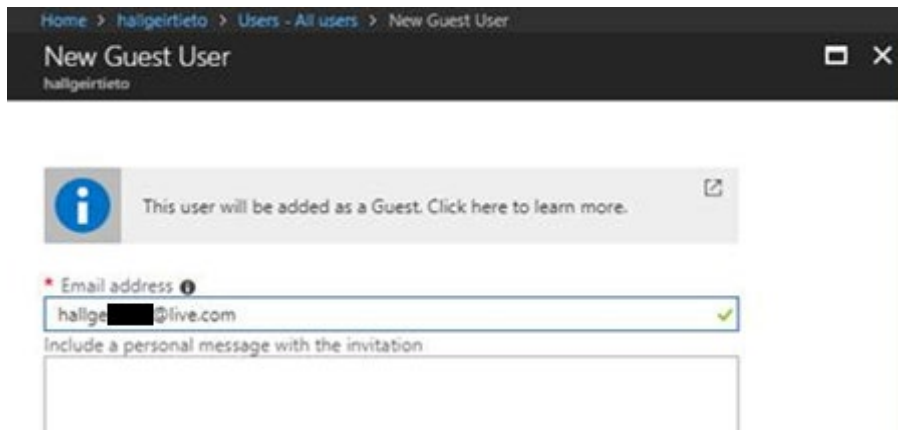
STEP 5: Click **Azure Active Directory**, then **Users**.



STEP 6: Click **New guest user**.



STEP 7: Enter a 360° Online user's Microsoft account username/email and click **Invite**.



STEP 8: Repeat steps to add guest users for all the 360° Online users in your organization.

STEP 10: Go to **STEP 3** of the "Step by step" section in the chapter **Authentication for Office 365/Azure Active Directory** to set up a new application for your organization's 360° Online service, and send **Directory ID**, **Application ID** and **key value** to your contact person at Tieto as described.