THALES

SafeNet Trusted Access for Identity Management with Azure Active Directory

CONFIGURATION GUIDE

CONTENTS

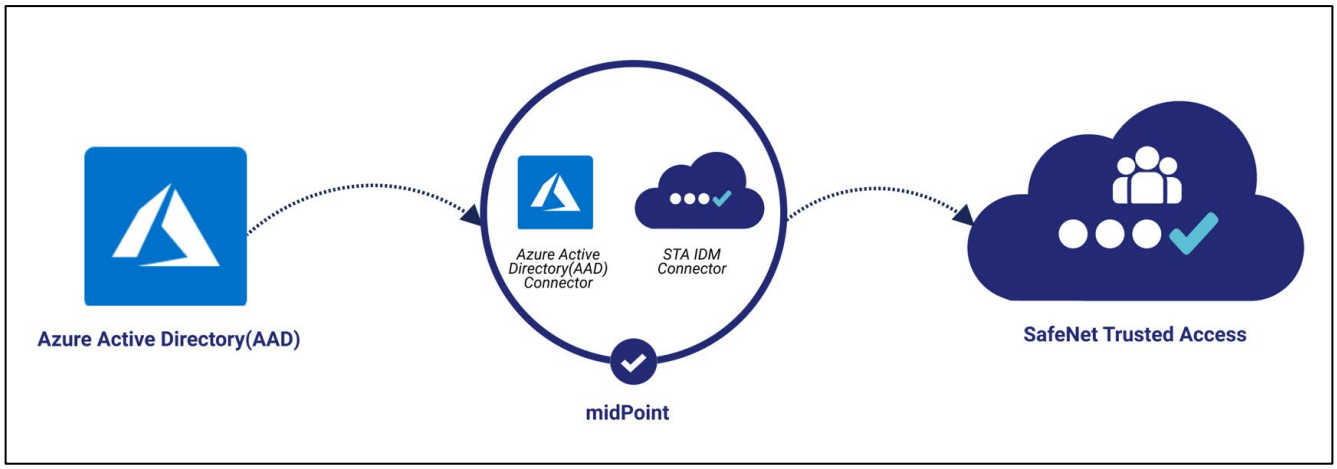
CHAPTER 1: Overview

This document contains information on Identity Management (IdM) platform solution, **midPoint**, offered by **Evolveum**, to be strategized in line with Identity provider (IdP) solution of SafeNet Trusted Access (STA).

This solution provides the ability for synchronizing users as well as their associated user groups from **Azure Active Directory (AAD)** to **SafeNet Trusted Access (STA)** using **midPoint**. If you have existing users and groups in **Azure Active Directory (AAD)**, you can take advantage of midPoint to synchronize them from **Azure Active Directory (AAD)** to **SafeNet Trusted Access (STA)**. It can connect both using custom connectors and can create, update, and delete both users and groups.

This solution is provided with a pre-configured configuration using XML files. However, you can always modify them as per your preferred configuration.

The following diagram illustrates the solution architecture`:



Supported Use Cases

This section specifies the use cases supported by Azure Active Directory Connector when syncing with SafeNet Trusted Access using midPoint.

- User synchronization
- Group synchronization
- User activation

Limitations

Following are the limitations that are encountered while syncing the **Azure Active Directory (AAD) Connector** with **SafeNet Trusted Access (STA)** using **STA IdM Connector** in midPoint:

- If any group is associated to a provisioning rule in STA, then the group update will fail.

- Nested groups synchronization to STA is not supported.
- If there are two groups with the same name in different domains, then the group creation will fail.
- If the outbound value of **isSynchronized** attribute in the STA Connector schema handling section is false, then all the users from midPoint will be synchronized in STA as internal users, therefore, Alias #3 and Alias #4 fields will not be visible under STA user's details. You can always map these user attribute for claim and return attribute like other STA users.
- User's password sync to STA is not supported in this release.

Test Environment Details

The following table contains the information about the tests conducted in the test environment, which consist of Azure Active Directory Connector and the STA IdM Connector:

midPoint environment	midPoint version 4.4.3
Operating System	Ubuntu version 20.0.5
Database	PostgreSQL
Hardware Resources	> 120 GB HDD > 8 Core CPU > 32 GB RAM
Scenario	Uni-directional sync from Azure Active Directory to SafeNet Trusted Access

NOTE: We have validated 2000 User's and 50 Group's synchronization in this release.

CHAPTER 2: Prerequisites

This chapter will guide you through the steps to setup a certificate, XML files and connectors which are required for AAD Connector to work successfully with midPoint.

As a prerequisite, **ensure that you must have an instance of midPoint Identity Framework installed and running on the machine.**

Perform the following steps:

1. Download and install Microsoft Azure (Graph API) Connector
2. Create your application in Azure Active Directory in Microsoft Azure Portal
3. Import Resource Definition in midPoint
4. Import Template XML file
5. Add DigiCert Certificate in midPoint KeyStore

Download and install Microsoft Azure (Graph API) Connector

1. Go to Microsoft Azure (Graph API) Connector - Evolveum Docs.
2. Click **download jar** under **Versions** > **Binary** column to download **Microsoft Azure (Graph API) Connector Version 1.0.0.1**.
3. Copy the downloaded **connector-msgraph-1.0.0.1.jar** file and paste it into **midpoint-installation-directory\icf-connectors**.

Versions

Version	Origin	Binary	Sources	Build Date	Description
1.0.0.1	Evolveum	download jar	Evolveum git repository (master)	Jan 21 2022	Stable version
1.0.1.0	Evolveum	download jar	Evolveum git repository (master)	Nov 15 2022	Fixes related to Licence handling and Group management improvements.

Create your application in Azure Active Directory in Microsoft Azure Portal

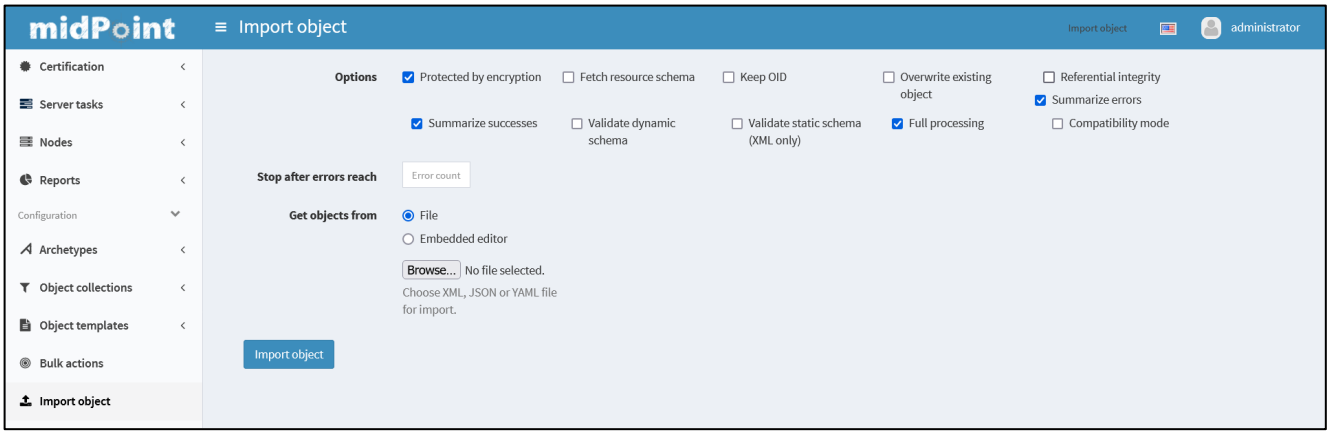
1. For more information on how to create and register a Web/API application in Azure Portal, refer to https://docs.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016-connector-graph.
2. Add all DELEGATED permissions in the newly created web application. Refer to **Permissions** section in https://docs.evolveum.com/connectors/resources/msgraph/.
3. Copy the value of following fields and paste them in a text editor to configure Azure Connector:

- **Application (client) ID**
- **Client Secret Value**
- **Directory (tenant) ID**

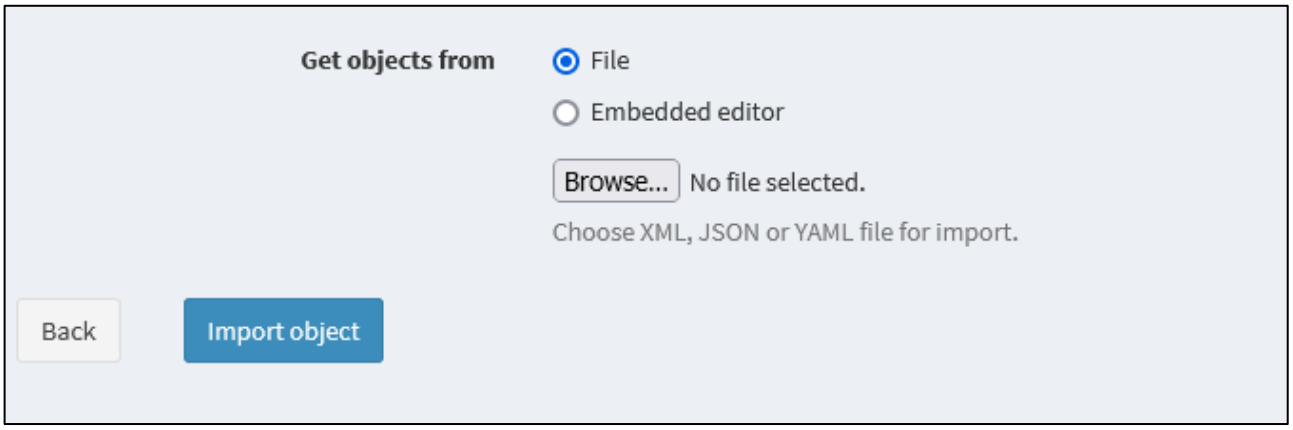
Import Resource Definition in midPoint

This section informs on how to import the Azure Active Directory Connector XML file in midPoint.

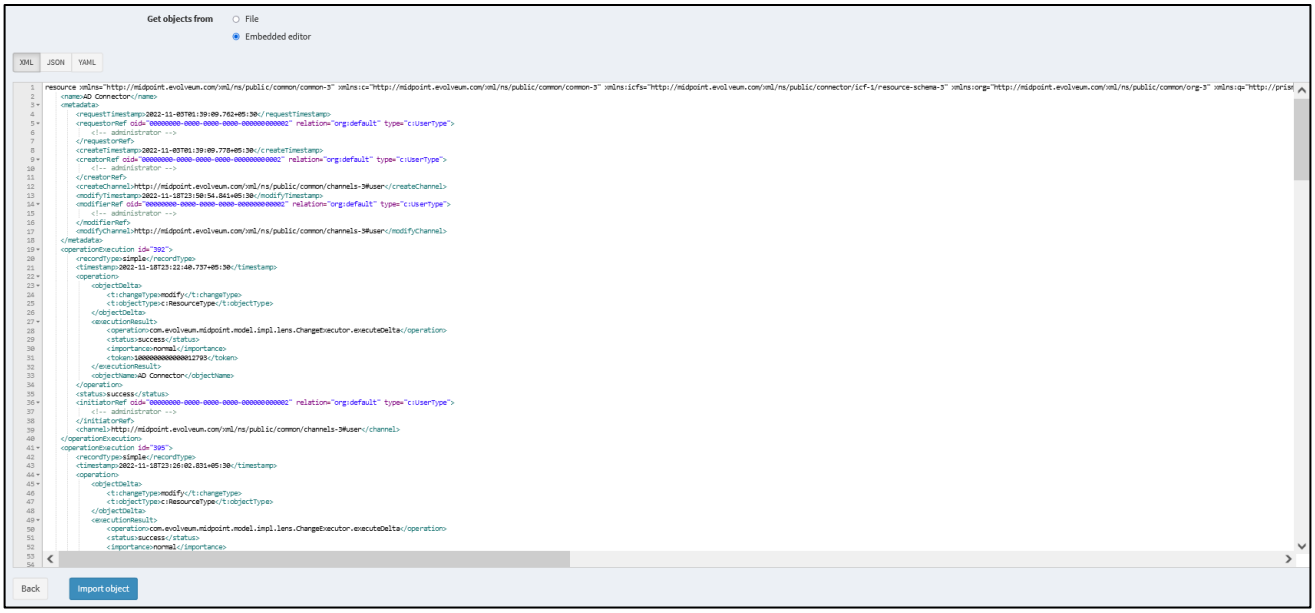
1. Download the **Azure Active Directory.xml** file from https://github.com/ThalesGroup/sta-idm-connector/Configuration_files/AzureAD and save the file.
2. On the midPoint administrator console, in the left pane, click **Import object**.
3. In the **Get objects from** field, perform either of the steps (a or b) listed below to import the connector XML file:



   a. Select **File** and click **Browse** to upload the **connector XML file**, and then click **Import object**.



   b. Select **Embedded editor**, copy and paste the contents of connector XML file in the editor, and then click **Import object**.

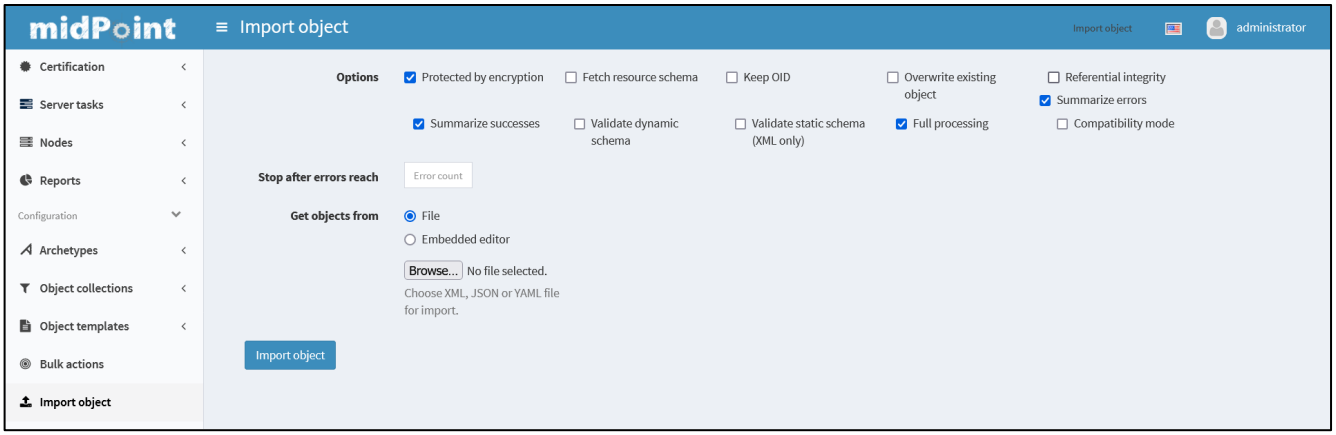


4. On the left pane, click **Resources** > **All Resources** and verify that the newly created resource is added in the right window.

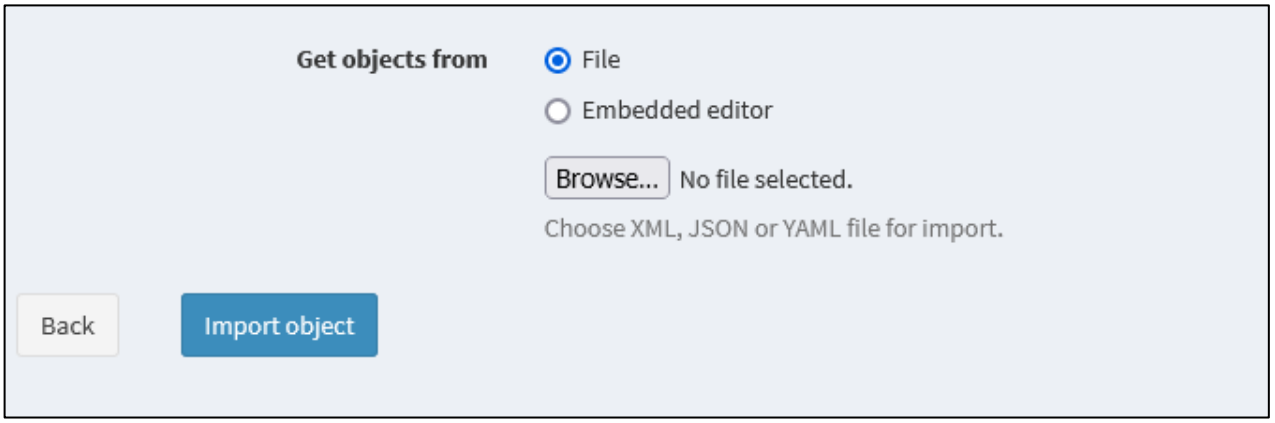
Import Template XML file

This section informs on how to import Template XML file in midPoint. These templates will help you to sync **users** and **groups** to **STA**.

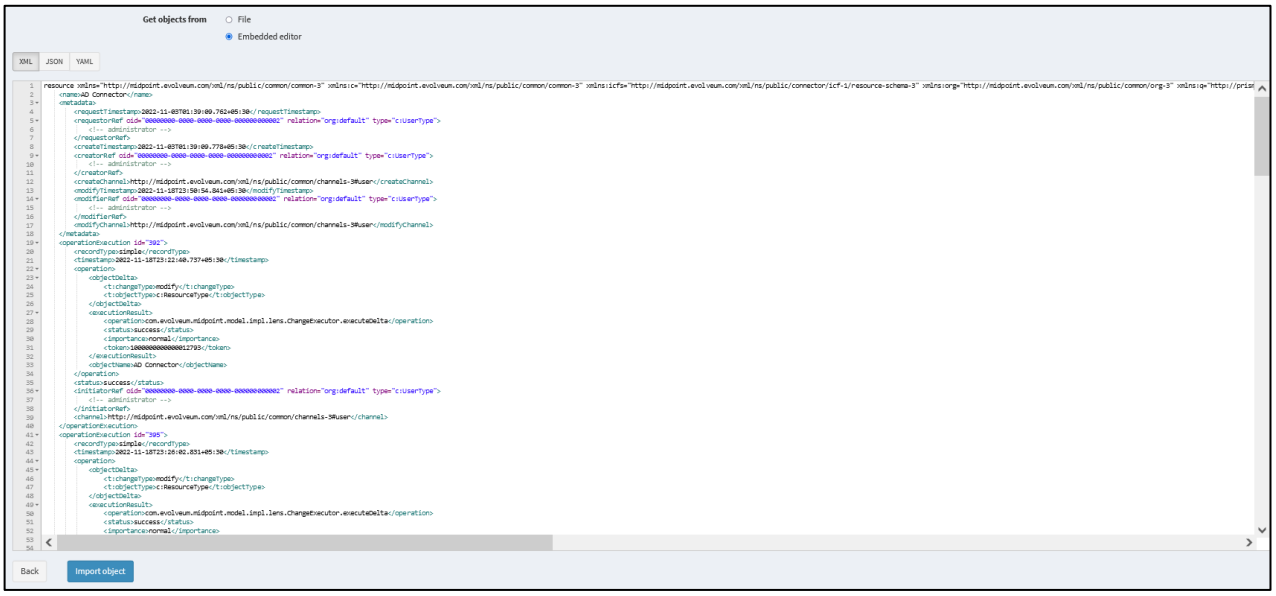
1. Download the following Template XML files from https://github.com/ThalesGroup/sta-idm-connector/Configuration_files/AzureAD and save the files:
   a. **RoleTemplate_for_AzureAD.xml**: This template contains the mappings that assign a meta role to groups being imported from Azure.
   b. **UserTemplate_for_AzureAD.xml**: This template contains the mappings that assign a role (STA user role) to users being imported from Azure.
   c. **MetaRole_for_STA.xml**: This template is used to create a meta role in midPoint. This meta role acts as super role and is used to create a group in STA along with their membership.
   d. **STA_user_role.xml**: This template is used to create a role in midPoint. This role is used to create a user(s) in STA automatically.
2. On the midPoint administrator console, in the left pane, click **Import object**.
3. In the **Get objects from** field, perform either of the steps (a or b) listed below to import the above Template XML files:



a. Select **File**, click **Browse** to upload the **<template_name>.xml** file as mentioned above, and then click **Import object**.



b. Select **Embedded editor**, copy and paste the contents of Template XML file in the editor, and then click **Import object**.



NOTE: You must follow the above **a** or **b** step to setup all the template files one-by-one as mentioned in Step 1 above.

Add DigiCert Certificate in midPoint KeyStore

You need to import the Azure certificates to build the trust between **Azure Graph API** and **Azure Connector in midPoint.**

This step will help you to add the SSL certificate used by Azure in midPoint Keystore. You must download and save the below certificates in your local directory using https://www.digicert.com/kb/digicert-root-certificates.htm:

- **DigiCert Global Root CA**
- **DigiCert Global Root G2**

1. Go to **midpoint-installation-directory/var**, copy and paste the above downloaded DigiCert certificates.
2. Open the terminal and then enter the following command:

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepass changeit -import -alias <Alias Name> -trustcacerts -<midpoint-installation-directory var/<Above downloaded certificate name>>
   ```

   For example,

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepass changeit -import -alias DigiCert -trustcacerts -<midpoint-installation-directory /var/DigiCert Global Root CA>
   ```

NOTE: You must run the above command for both the downloaded certificates.

CHAPTER 3: Configuring SafeNet Trusted Access Connector in midPoint

This chapter will guide you through the detailed steps to setup a working SafeNet Trusted Access (STA) Connector in midPoint for user synchronization.

To configure as per the STA IdM documentation, click https://github.com/ThalesGroup/sta-idm-connector/Documentation.

CHAPTER 4: Configure your Azure Active Directory (AAD) Connector in midPoint

This chapter will guide you through the detailed steps to setup a working **Azure Active Directory (AAD) Connector** in **midPoint**.

On the left pane, click **Resources > All Resources**. In the **All Resources** window, select the **Azure Active Directory** resource that you have created in Step 3 of prerequisites section. Under the **Resource Operations** tab, click **Edit using wizard**.

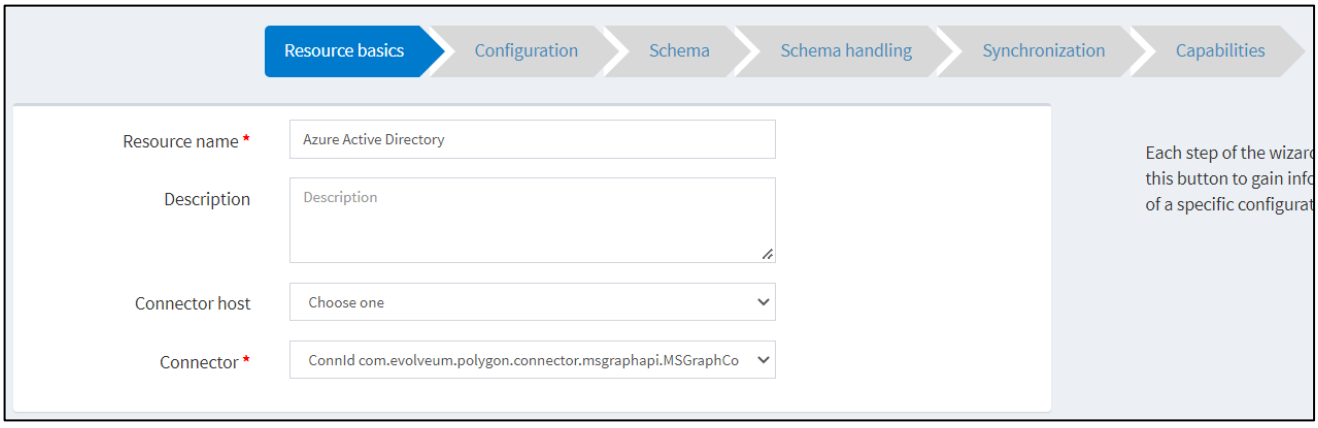
The configuration is divided in the following sections:

1. Resource basics
2. Configuration
3. Schema handling
4. Synchronization
5. Capabilities

Resource basics

Perform the following steps to configure the fields in the **Resource basics** section:

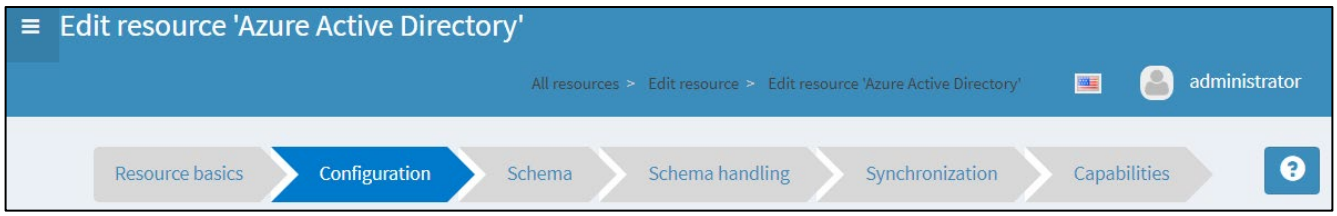
1. In the **Resource name** field, edit the name for the connector (for example, **Azure Active Directory**) for the identification purpose. (Optional)
2. In the **Description** field, enter a description of the connector. (Optional)
3. In the **Connector** field, ensure that the Azure connector, that is, **ConnId com.evolveum.polygon.connector.msgraphapi.MSGraphConnector V1.0.0.1** is selected.



4. Click **Next.**

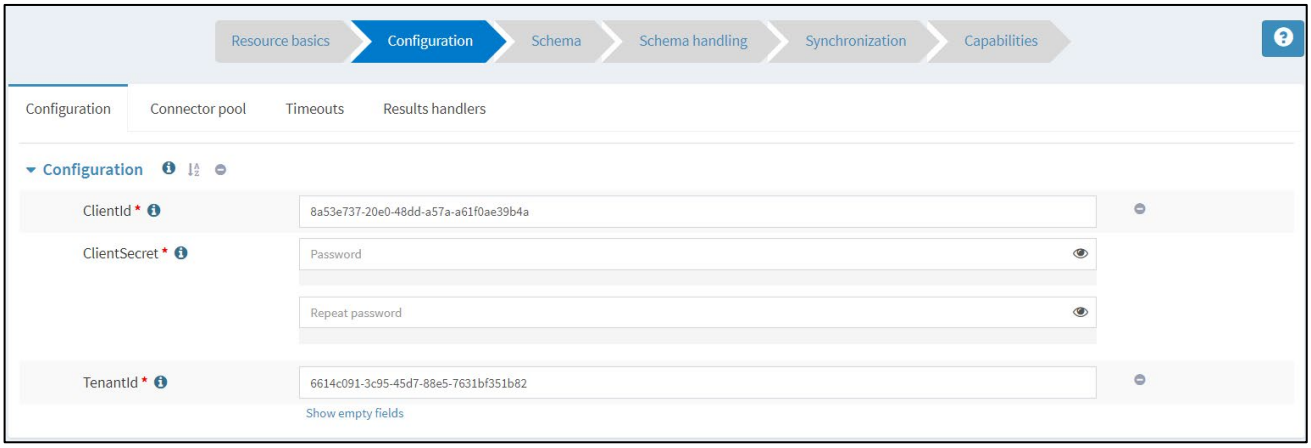
Configuration

In this section, the values are pre-filled, which you need to update with the information corresponding to your Azure Active Directory application.



Perform the following steps:

1. In the **ClientId** field, update the **Application (client) ID** that you copied in Step 3 of Create your application in Azure Active Directory in Microsoft Azure Portal.
2. In the **ClientSecret** field, click **Change**, and then enter the **Client Secret Value** that you copied in Step 3 of Create your application in Azure Active Directory in Microsoft Azure Portal.
3. In the **Repeat Password** field, re-enter the **Client Secret Value**.
4. In the **TenantId** field, update the **Directory (tenant) ID** that you copied in Step 3 of Create your application in Azure Active Directory in Microsoft Azure Portal.
5. Click **Save and test Connection**. Verify that all the configurations are done successfully and then click **OK.**



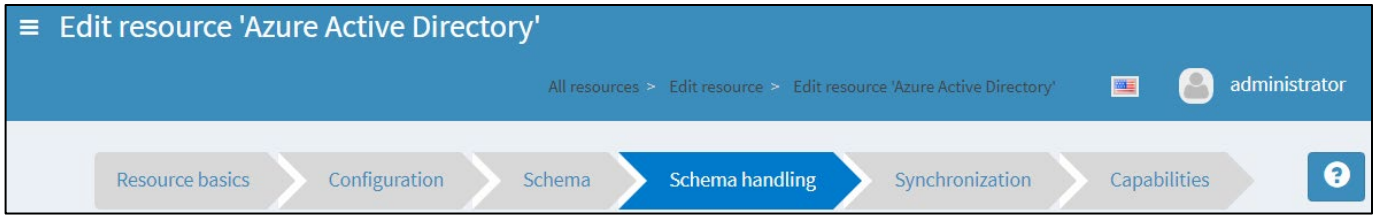
6. Click **Next.**
7. Click **Next.**

> **NOTE:** If you find any error on Test connection, please check your Azure application configuration.

Schema handling

This section contains Attributes Mapping for both users and groups for synchronization.

The following steps provides information on how to add a new attribute mapping or edit an existing attribute mapping.



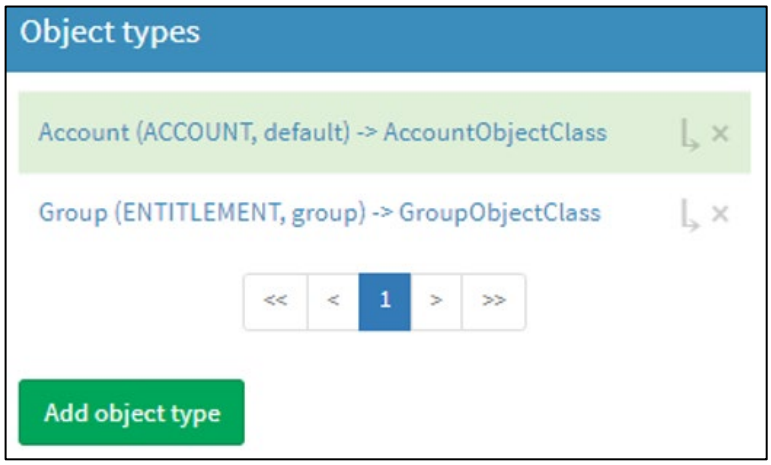
NOTE: The default set values are case sensitive.

The information in this section is divided into three sub-sections:

1. Users
2. Groups
3. Add or Edit Mappings

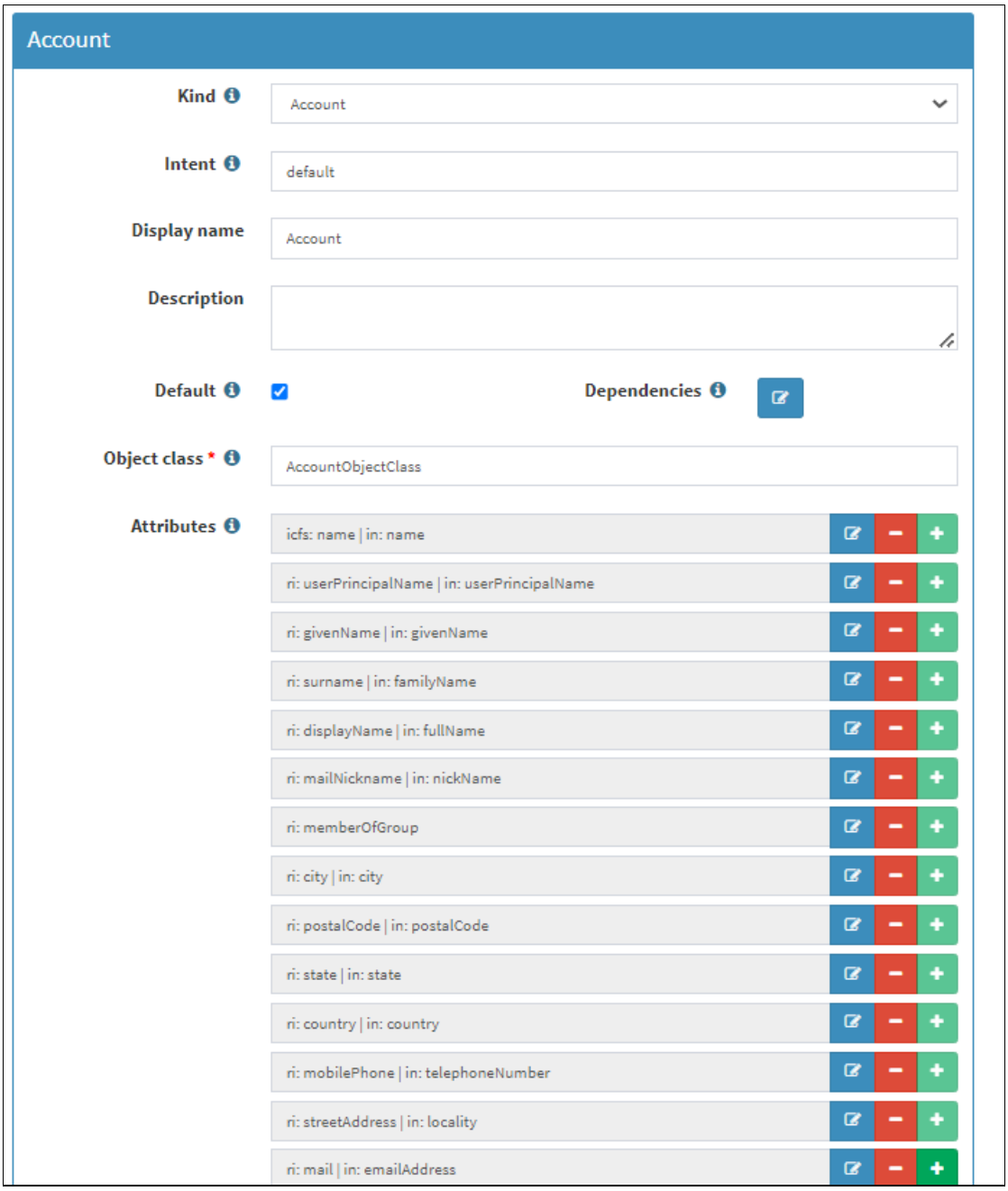
Users

On the **Schema handling** tab, under **Object types**, click **Account (ACCOUNT, default) -> AccountObjectClass**.



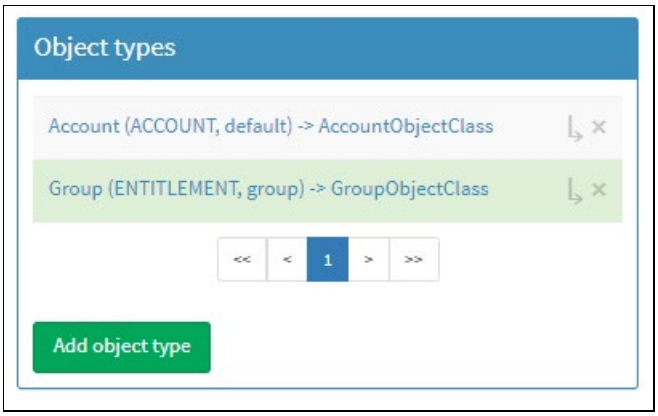
The **Attribute mapping** window for users is displayed. Ensure that all the values are set, as in the below table:

Fields	Values
Kind	Account
Intent	Default
Object class	AccountObjectClass



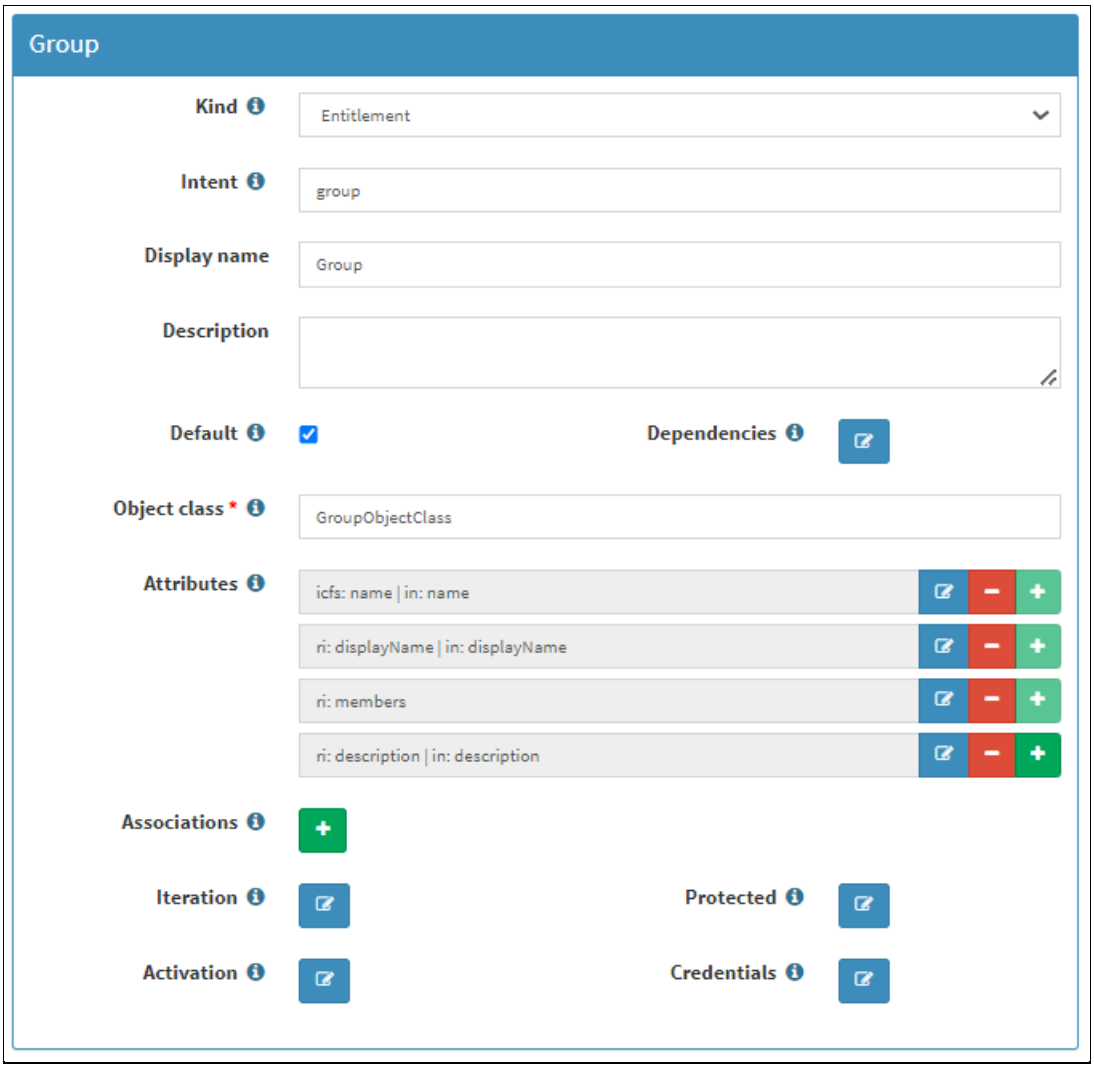
Groups

On the **Schema handling** tab, under **Object types**, click **Group (ENTITLEMENT, group) -> GroupObjectClass**.



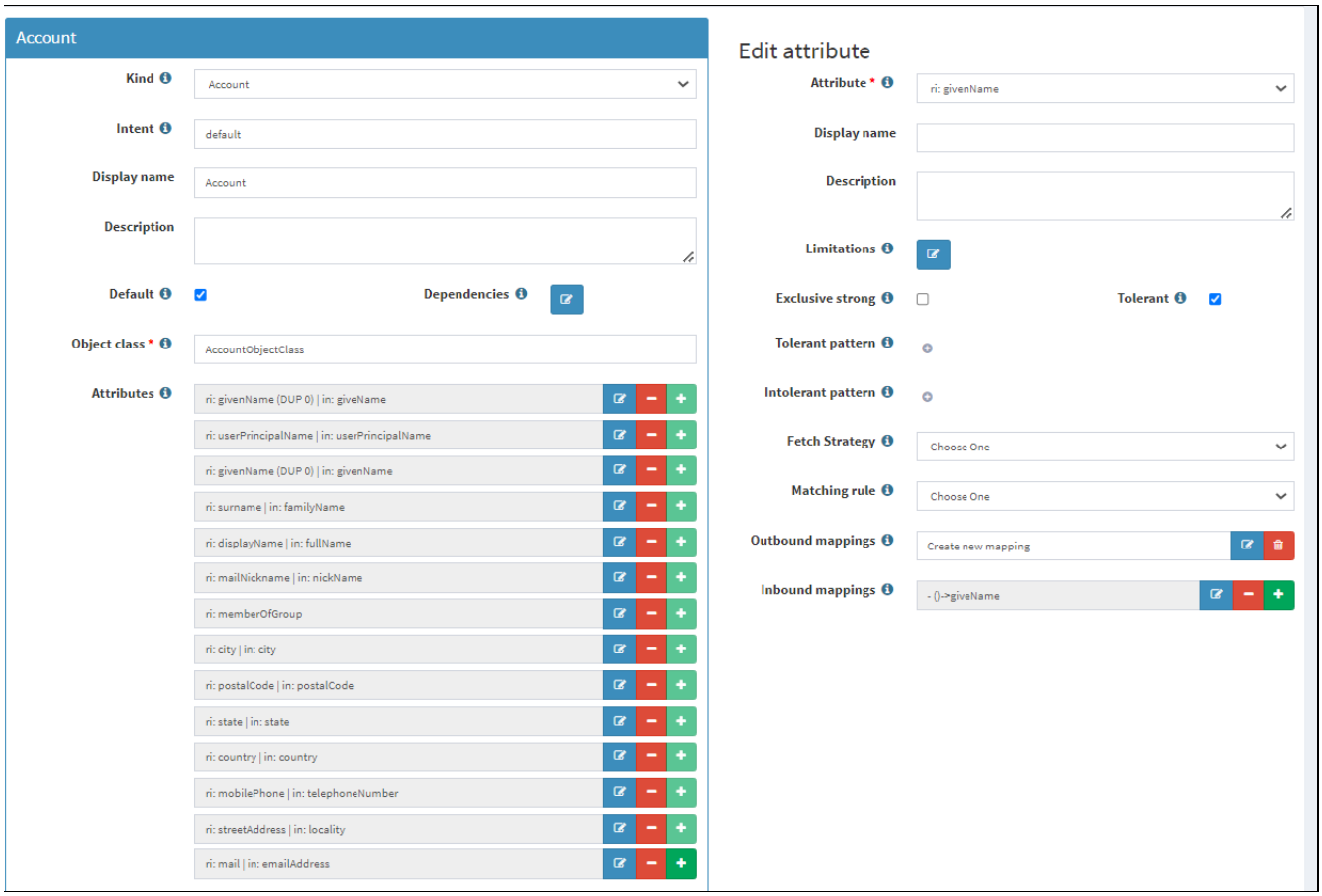
The **Attribute mapping** window for groups is displayed. Ensure that all the values are set, as in the below table:

Fields	Values
Kind	Entitlement
Intent	Group
Object class	GroupObjectClass

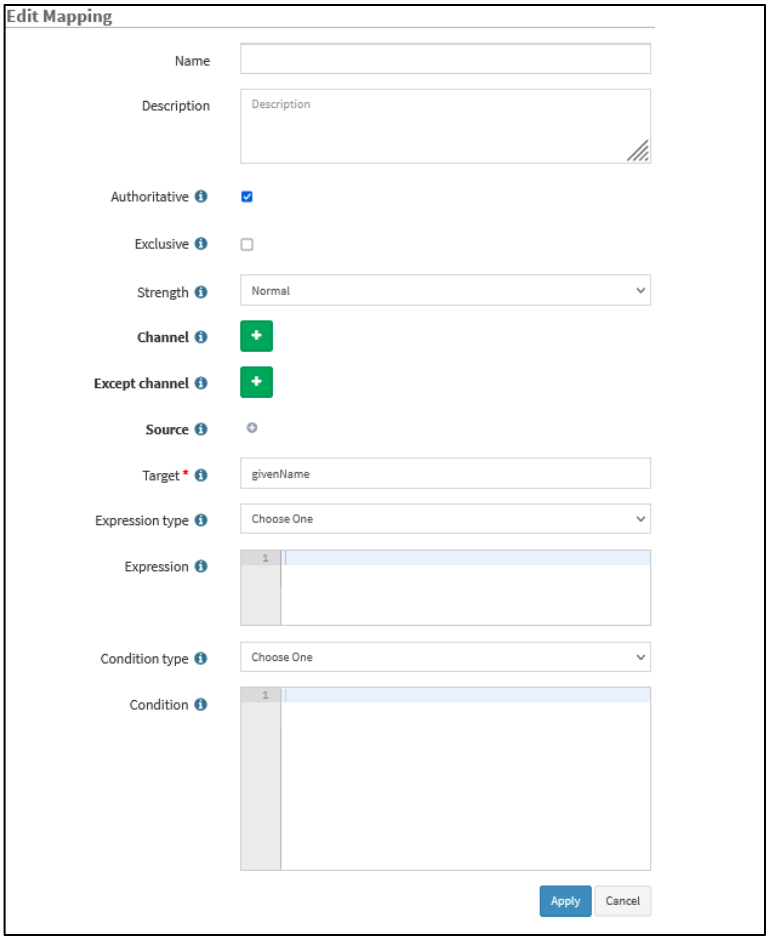


Add or Edit Mappings

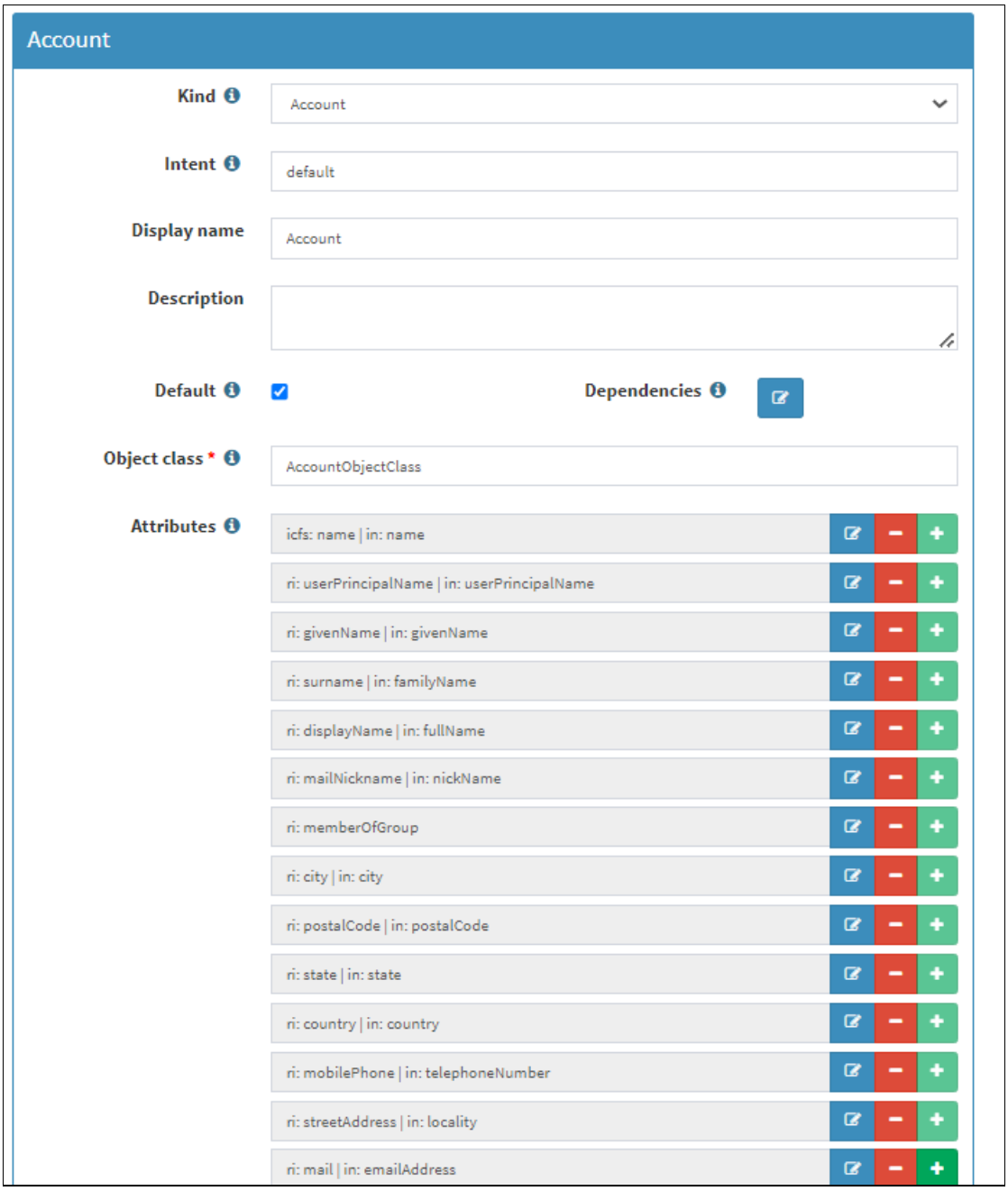
1. Click + to add or ✎ to edit an attribute in Schema handling (displayed against the attribute). To edit the mappings, perform the following steps:
   a. In the **Edit attribute** window, perform the following steps:
      i. In the **Attribute** field, select a value from the dropdown (for example, **givenName**).



ii. In the **Inbound mappings** field, click + icon (displayed against it) and in **Target**, enter name of the user attribute that you want to set for the attribute selected in Step 1 (for example, **givenName**). Click **Apply**.

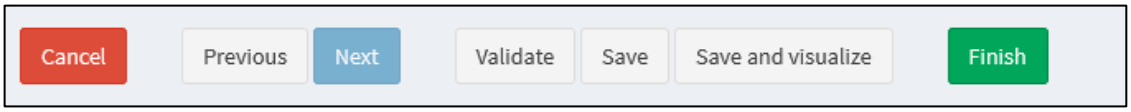


b. After updating the Attribute mapping, following window will appear:



NOTE: Similarly, you can perform the above steps to add/update mapping for Groups.

c. Click **Next**.



Synchronization

This section contains the action to be taken by midPoint for different situation of users and groups.

NOTE: The default set values are case sensitive.

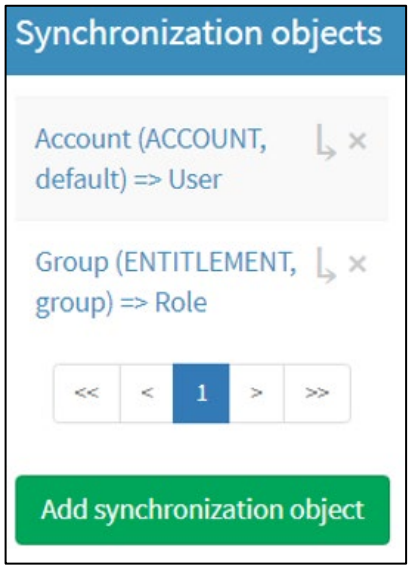
The information in this section is divided into the following sub-sections:

> Users

> Groups

Users

On the **Synchronization** tab, under **Synchronization objects**, click **Account (ACCOUNT, default) => User** to view or edit the Reaction mapping.

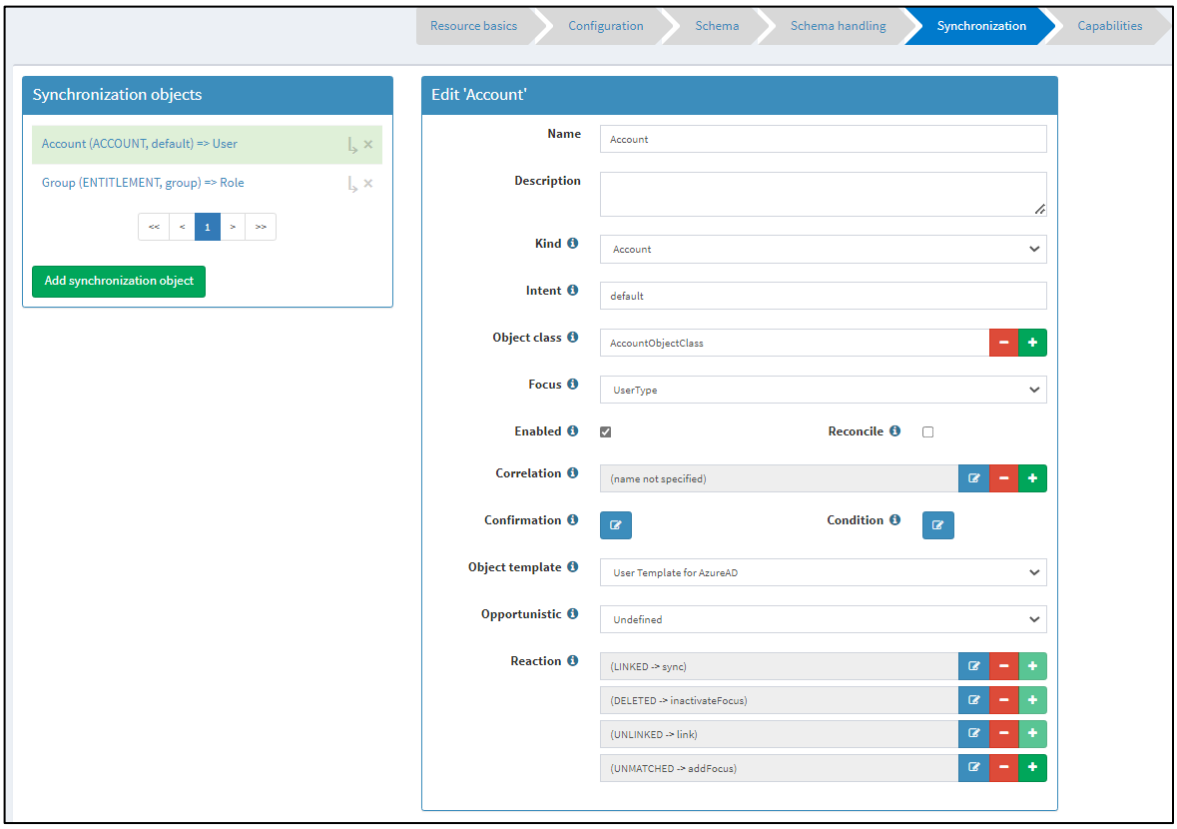


The **Attribute mapping** window for users is displayed. Ensure that all the values are set, as in the below table:

Fields	Values
Kind	Account
Intent	Default
Object class	AccountObjectClass
Focus	UserType

> Ensure that the **Enabled** checkbox is selected.

> In the **Object template** field, select **User Template for AzureAD**.



Groups

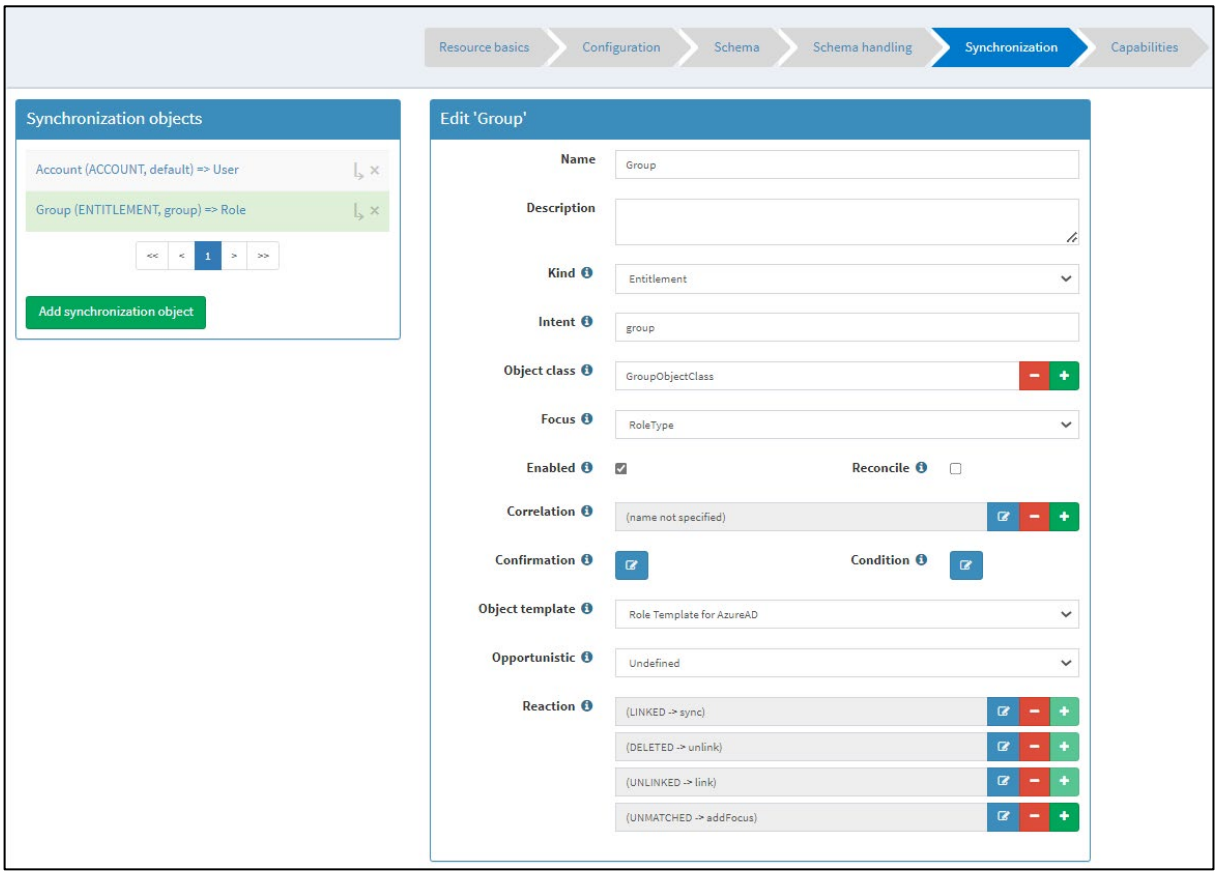
On the **Synchronization** tab, under **Synchronization objects**, click **Group (ENTITLEMENT, group) => Role** to view or edit the Reaction mapping.

The **Attribute mapping** window for users is displayed. Ensure that all the values are set, as in the below table:

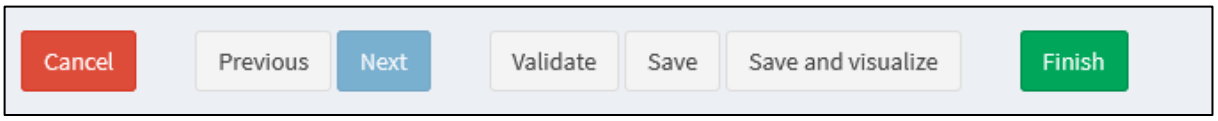
Fields	Values
Kind	Entitlement
Intent	Group
Object class	GroupObjectClass
Focus	RoleType

> Ensure that the **Enabled** checkbox is selected.

> In the **Object template** field, select **Role Template for AzureAD**.

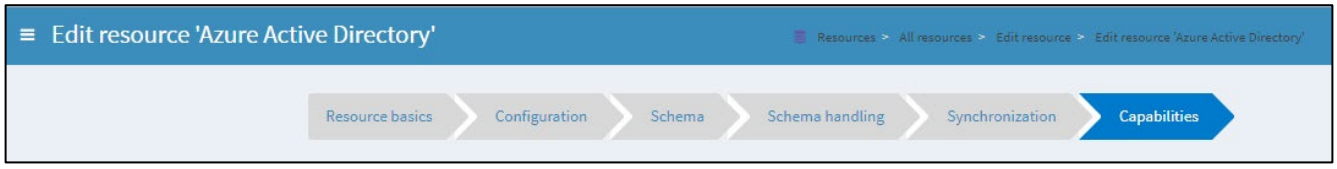


> Click **Next**.



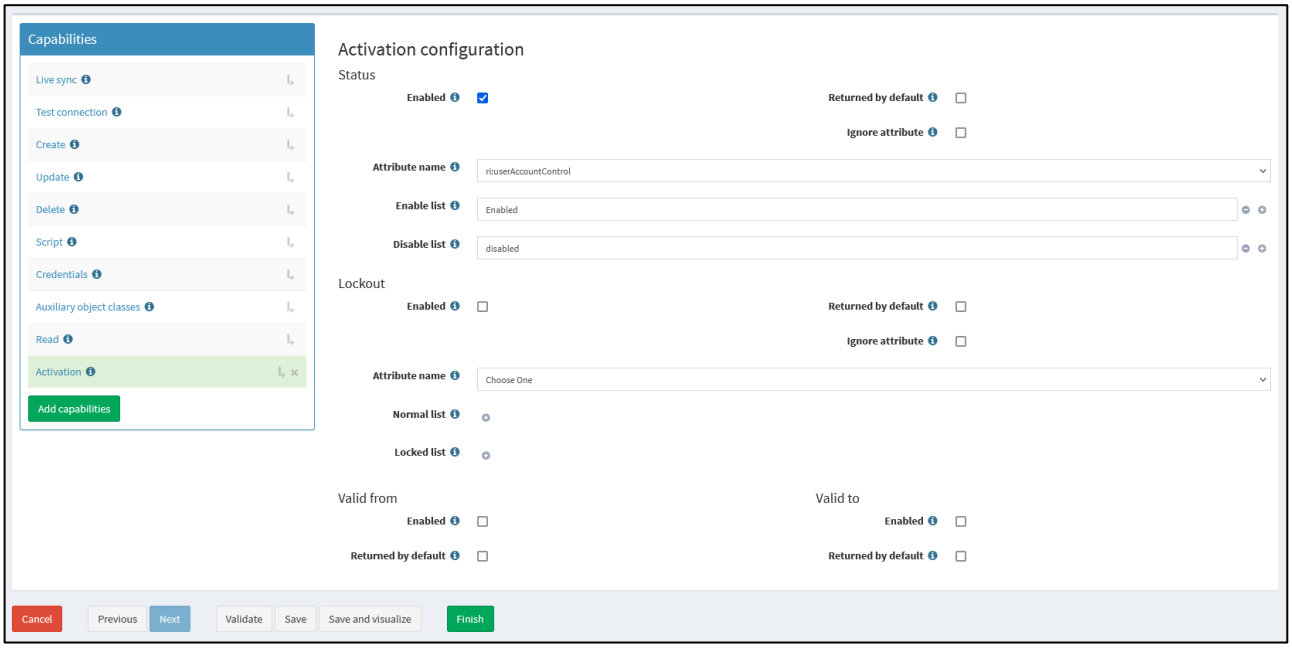
Capabilities

This section helps you to configure the Capabilities of Azure Active Directory Connector.



1. On the **Capabilities** section, in the left pane, click **Activation**, and then perform the following steps:
   a. Ensure that the **Enabled** checkbox is selected.
   b. In the **Attribute name** field, select **userAccountControl**.
   c. In the **Enable list** field, click ⓘ icon then enter **Enabled**.
   d. In the **Disable list** field, click ⓘ icon then enter **disabled**.

e. Click **Finish** to save the connector configuration.



NOTE: After saving the configuration, above connector status must be up (in green color). If your connector status is in down/disable/broken state, you must click **Test Connection**.

CHAPTER 5: Task Creation

This chapter will guide you to create task in midPoint for various actions. These tasks are used to synchronize the users and groups at specific time automatically. You can create the following tasks in midPoint.

> Import Task

> Live Synchronization Task

> Reconciliation Task

Import Task

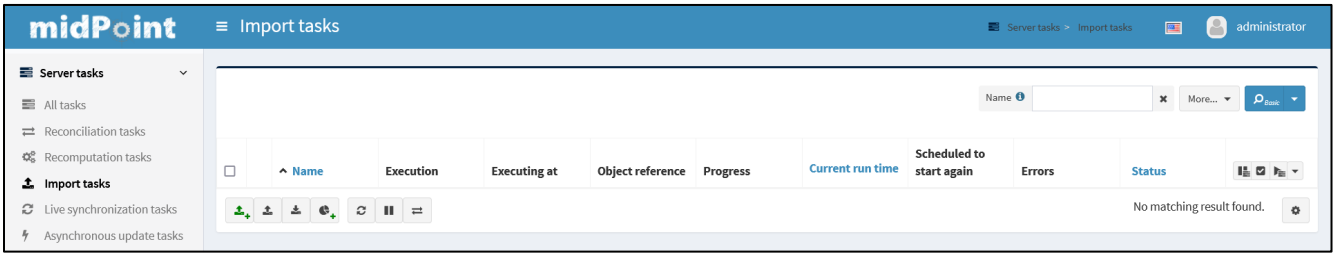
This section explains the steps to import tasks for the users and groups.

> Users

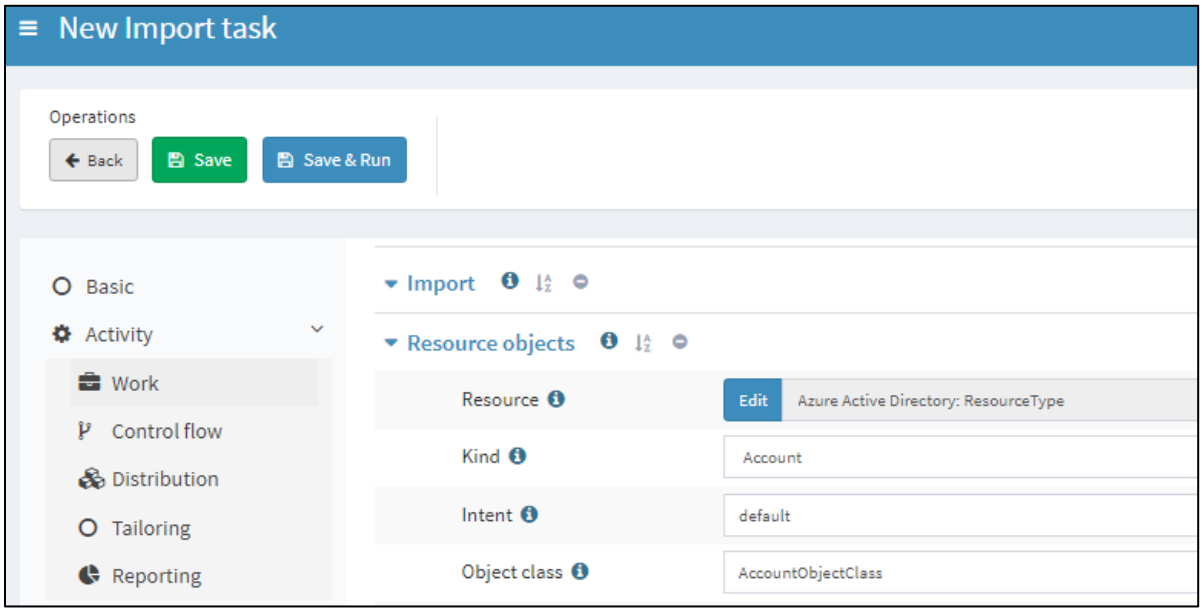
> Groups

Users

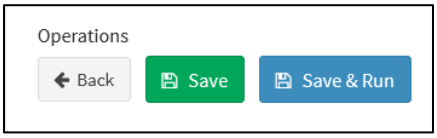
1. On the midPoint administrator console, in the left pane, click **Server tasks** > **Import tasks**.
2. On the **Import tasks** window, click  icon to add a new task.



3. On the **New Import task** window, under **Resource objects**, perform the following steps to create a task:
   a. In the **Resource** field, click **Edit** and then select **Azure Active Directory Connector**.
   b. In the **Kind** field, select **Account**.
   c. In the **Intent** field, select **default**.
   d. In the **Object class** field, select **AccountObjectClass**.



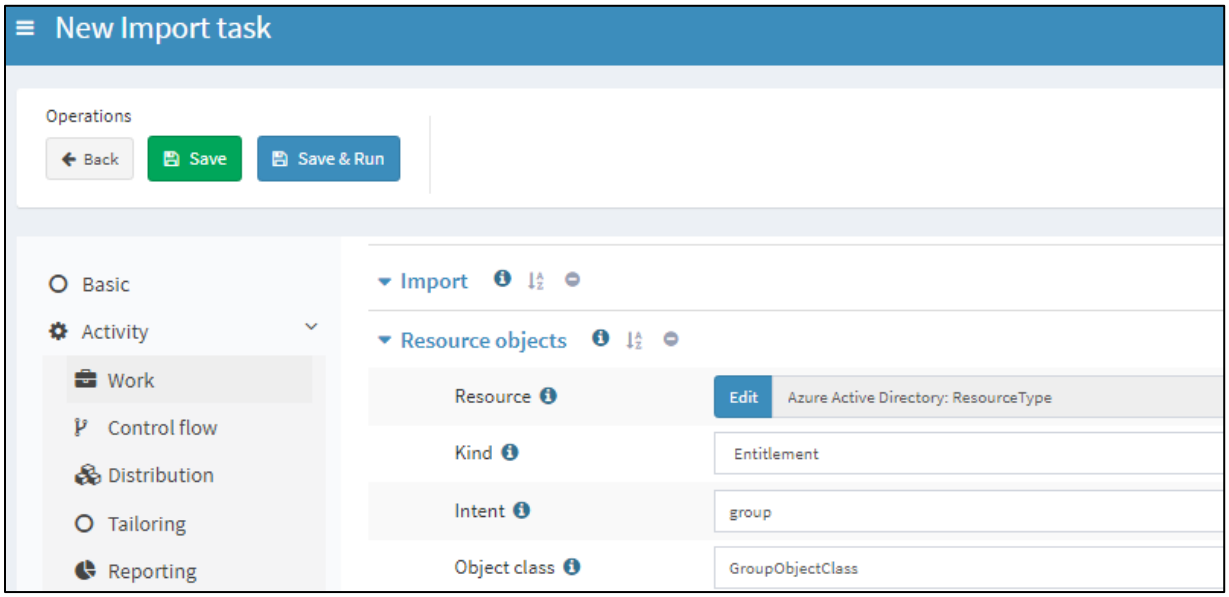
4. Click **Save**.



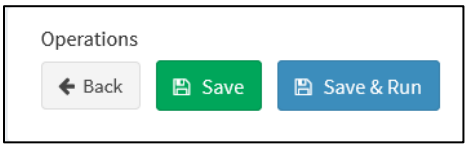
Groups

1. On the **Import tasks** window, click  icon to add a new task.

2. On the **New Import task** window, under **Resource objects**, perform the following steps to create a task:
   a. In the **Resource** field, click **Edit** and then select **Azure Active Directory Connector**.
   b. In the **Kind** field, select **Entitlement**.
   c. In the **Intent** field, select **group**.
   d. In the **Object class** field, select **GroupObjectClass**.



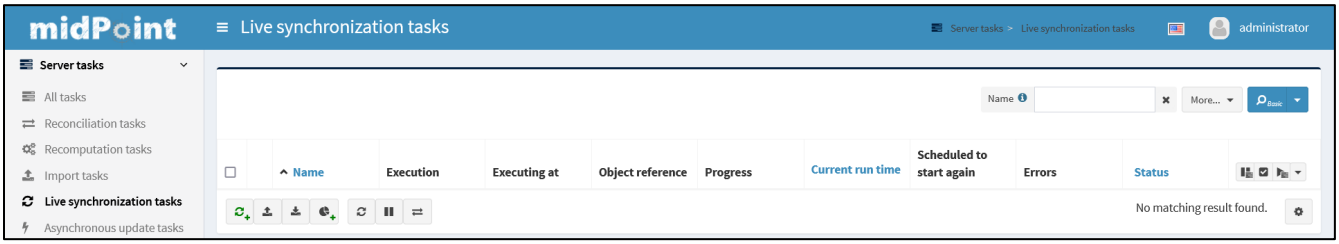
3. Click **Save**.



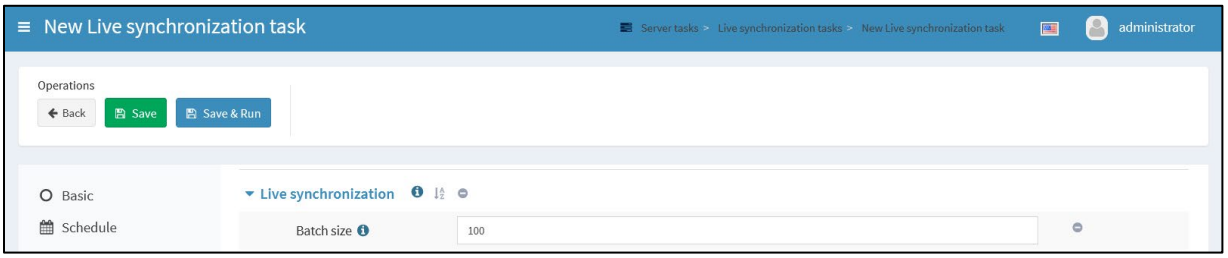
Live Synchronization Task

This section explains the steps to create Live synchronization tasks for the users.

1. In the left pane, click **Server tasks** > **Live synchronization tasks.**
2. On the **New Live synchronization tasks** window, click  icon to add a new task.



3. On the **New Live synchronization task** window, perform the following steps to create a task:
   a. Under **Live synchronization**, perform the following steps:
      i. In the **Batch size** field, enter a value for the number of records that you want to fetch in a Live sync (for example, **100**).



b. Under **Resource objects**, perform the following steps:

i. In the Resource field, click Edit and then select Azure Active Directory Connector.

ii. In the **Kind** field, select **Account**.

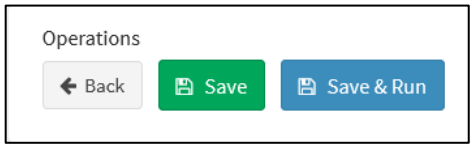
iii. In the **Intent** field, select **default**.

iv. In the **Object class** field, select **AccountObjectClass**.

c. Under **Schedule**, in the **Interval** field, enter the value of **Interval** in seconds (for example, **86400**).

NOTE: Interval is the time period after which the task will be repeated until stopped.

d. Click **Save**.



Reconciliation Task

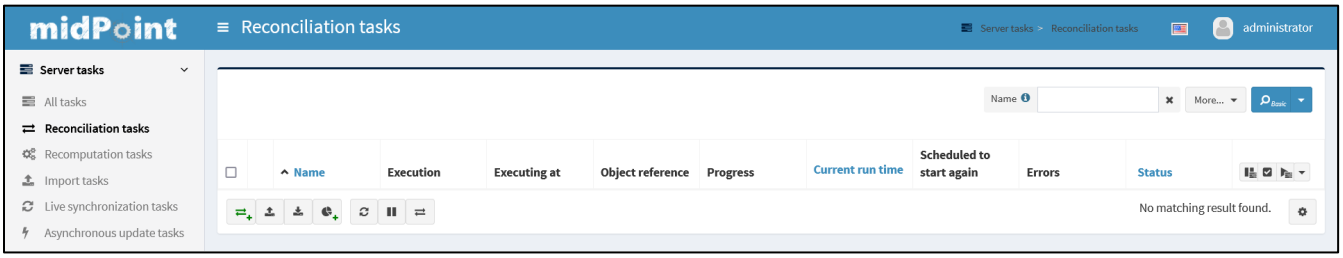
This section explains the steps to create reconciliation task for the users and groups.

> Users

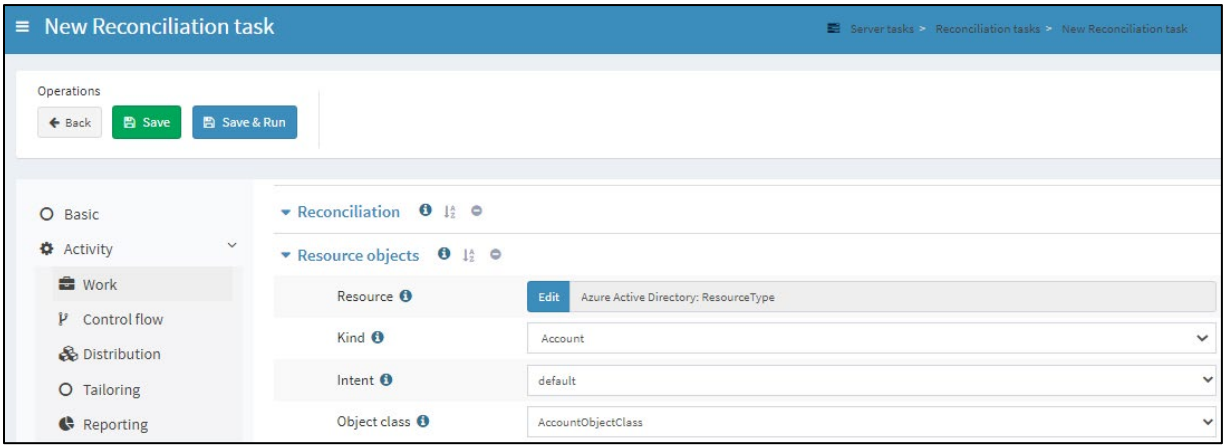
> Groups

Users

1. In the left pane, click **Server tasks** > **Reconciliation tasks**.
2. On the **Reconciliation tasks** window, click icon to add a new task.



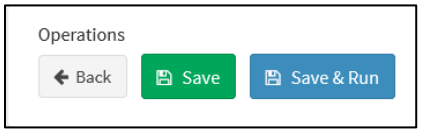
3. On the **New Reconciliation task** window, perform the following steps to create a task:
   a. Under **Resource objects**, perform the following steps:
      i. In the **Resource** field, click **Edit** and then select **Azure Active Directory Connector**.
      ii. In the **Kind** field, select **Account**.
      iii. In the **Intent** field, select **default**.
      iv. In the **Object class** field, select **AccountObjectClass**.



   b. Under **Schedule**, in the **Interval** field, enter the value of **Interval** in seconds (for example, **86400**).

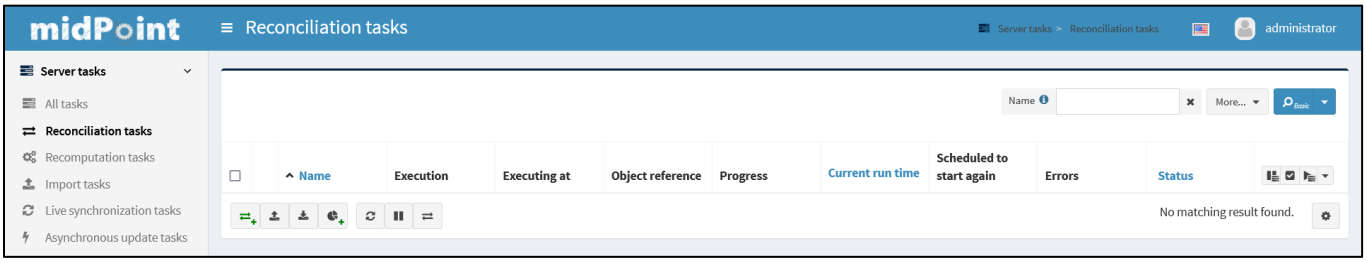
NOTE: Interval is the time period after which the task will be repeated again until stopped.

   c. Click **Save**.

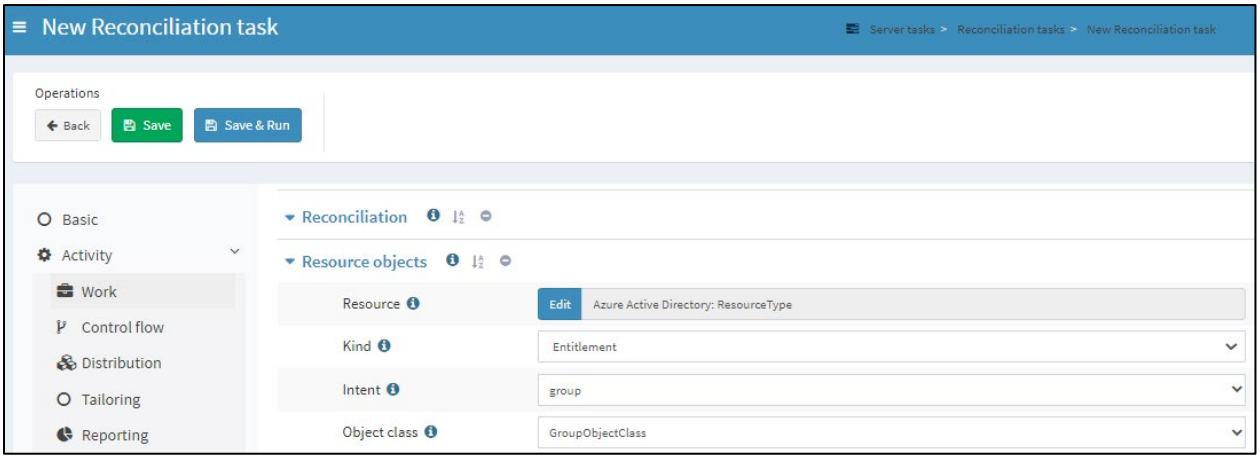


Groups

1. On the **Reconciliation tasks** window, click icon to add a new task.



2. On the **New Reconciliation task** window, perform the following steps to create a task:
   a. Under **Resource objects**, perform the following steps:
      i. In the **Resource** field, click **Edit** and then select **Azure Active Directory Connector**.
      ii. In the **Kind** field, select **Entitlement**.
      iii. In the **Intent** field, select **group**.
      iv. In the **Object class** field, select **GroupObjectClass**.



   b. Under **Schedule**, in the **Interval** field, enter the value of **Interval** in seconds (for example, **86400**).

NOTE: Interval is the time period after which the task will be repeated until stopped.

   c. Click **Save**.

CHAPTER 6: Test your Configuration

This chapter will guide you through the steps to validate the above configurations from midPoint. To test the configuration, ensure that you have some test users and groups in Azure Active Directory.

After creating the test objects, perform the following steps:

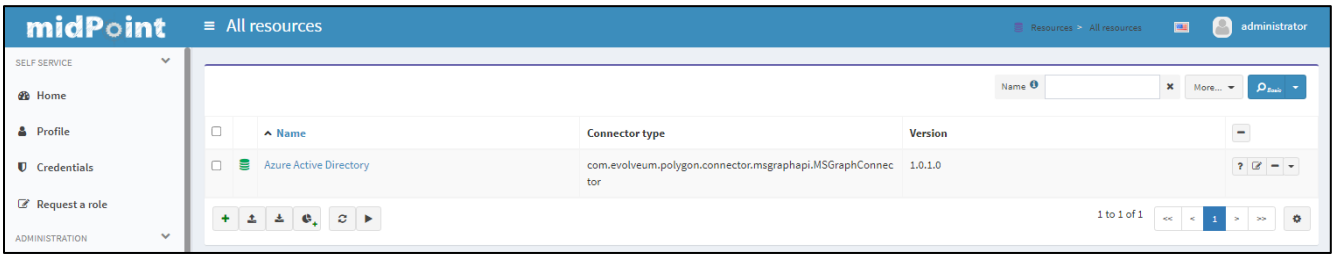
1. Import groups from Azure Active Directory to midPoint
2. Import users from Azure Active Directory to midPoint
3. Verifying users and groups in STA
4. Deleting users and groups from midPoint

> **NOTE:** Ensure that you always import the Group(s), before the **User(s)**, in order to sync the **Group memberships** to **STA**.

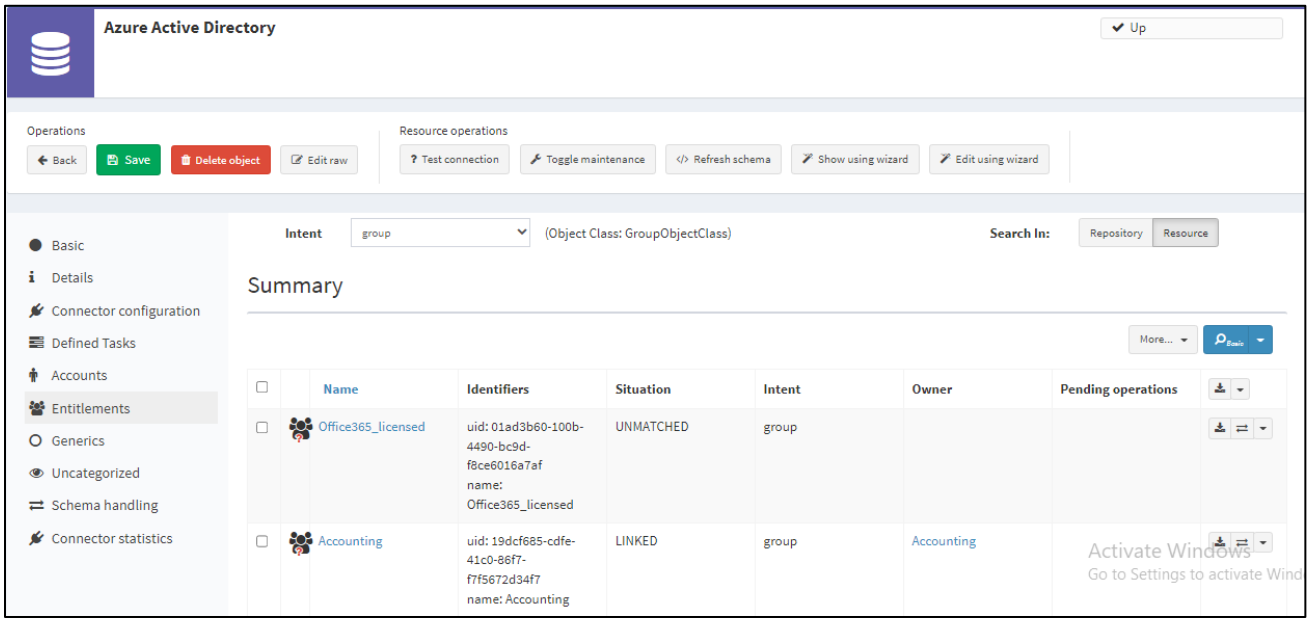
Import groups from Azure Active Directory to midPoint

This section helps you in testing your connector configuration by importing a group from **Azure Active Directory** to **midPoint**.

1. On the midPoint administrator console, in the left pane, click **Resources** > **All Resources**.



2. On the **All resources** window, click **Azure Active Directory Connector** and perform the following steps:
   a. In the Azure Active Directory Connector, click **Entitlements**. Then, on the right pane, in the **Search In** field, click **Resource**.
   b. All the **Azure Active Directory** groups will be displayed in the below section. Click icon to import the group into **midPoint**.

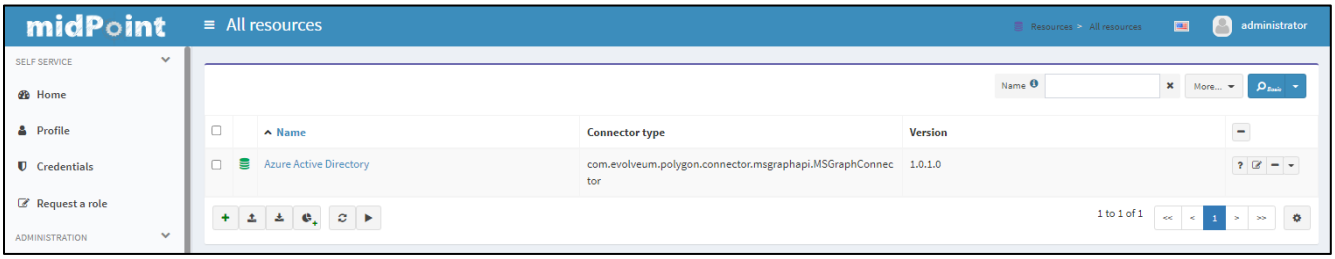


NOTE: After the import is successful, the value of **Situation** column will be changed to **Linked.**

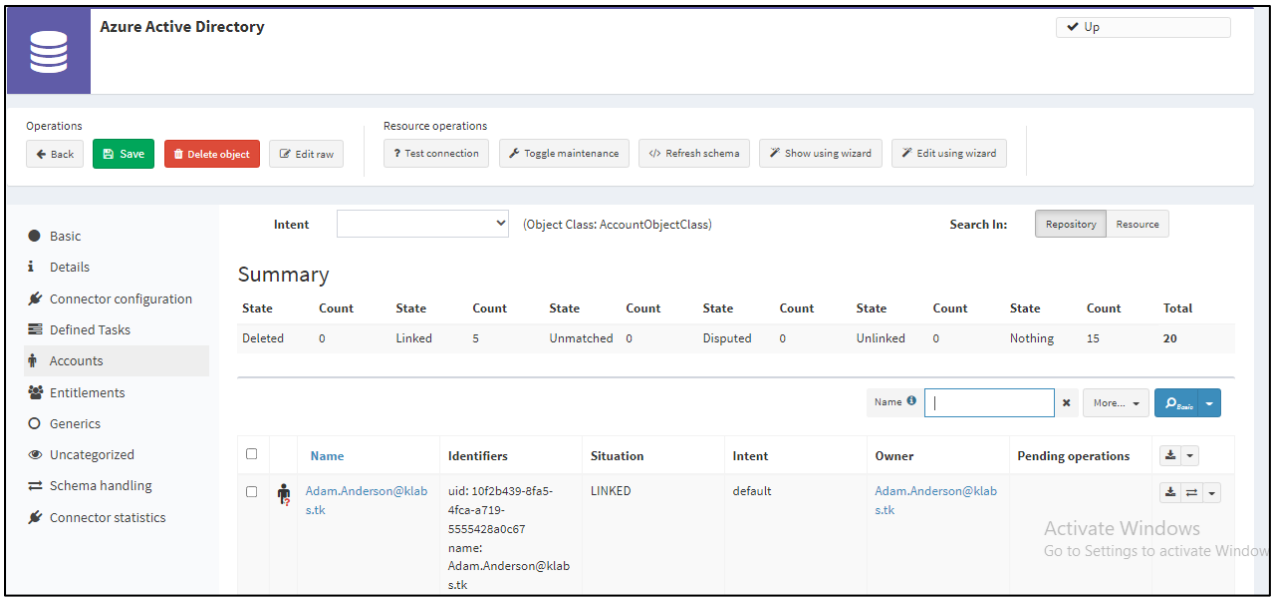
Import users from Azure Active Directory to midPoint

This section helps you in testing your connector configuration by importing a user from **Azure Active Directory** to **midPoint**.

1. On the midPoint administrator console, in the left pane, click **Resources** > **All Resources**.



2. On the **All resources** window, click **Azure Active Directory Connector** and perform the following steps:
   a. In the Azure Active Directory Connector, click **Accounts**. Then on the right pane, in the **Search In** field, click **Resource**.
   b. All the **Azure Active Directory** users will be displayed in the below section. Click icon to import the user into **midPoint**.



NOTE: After the import is successful, the value of **Situation** column will be changed to **Linked.**
If the Situation column status is UNMATCHED, please check the error logs.

Verifying users and groups in STA

This section helps you to verify if the users and groups are successfully synced to **STA**.

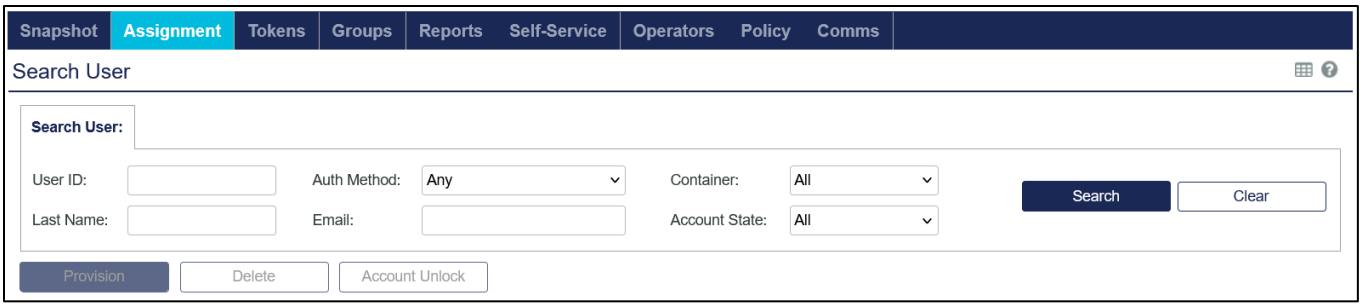
> Users

> Groups

Users

To verify the users sync to STA, perform the following steps:

1. Go to the **STA Management console** and select the **Assignment** tab.

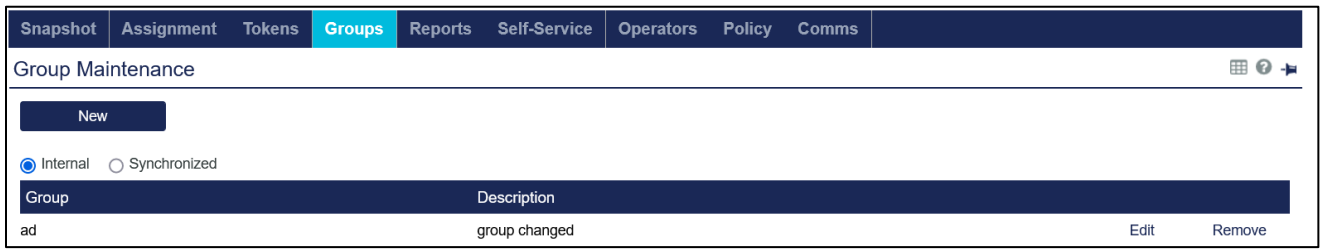


2. In the **Search User** module, you can find the list of users that are pushed from **Azure Active Directory**. Alternatively, you can search for individual users to verify if the users are synchronized.

Groups

To verify the group sync to STA, perform the following steps:

1. Go to the **STA Management console** and select the **Groups** tab.
2. Under **Group Maintenance** > **Internal**, you can find all the **Azure Active Directory** groups that are synchronized to STA.



Deleting users and groups from midPoint

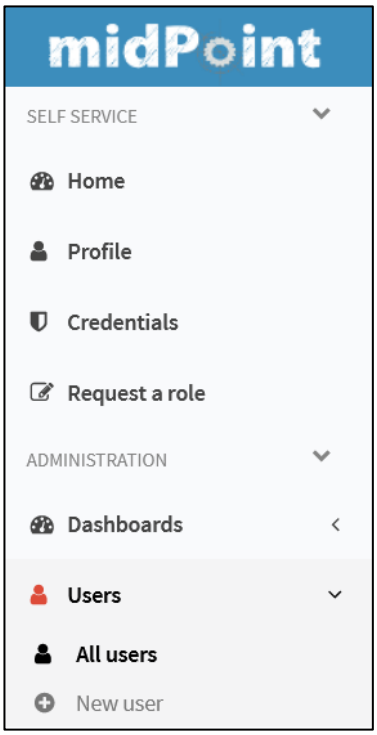
This section provides the steps for deleting the users and groups from **midPoint.**

> Users

> Groups

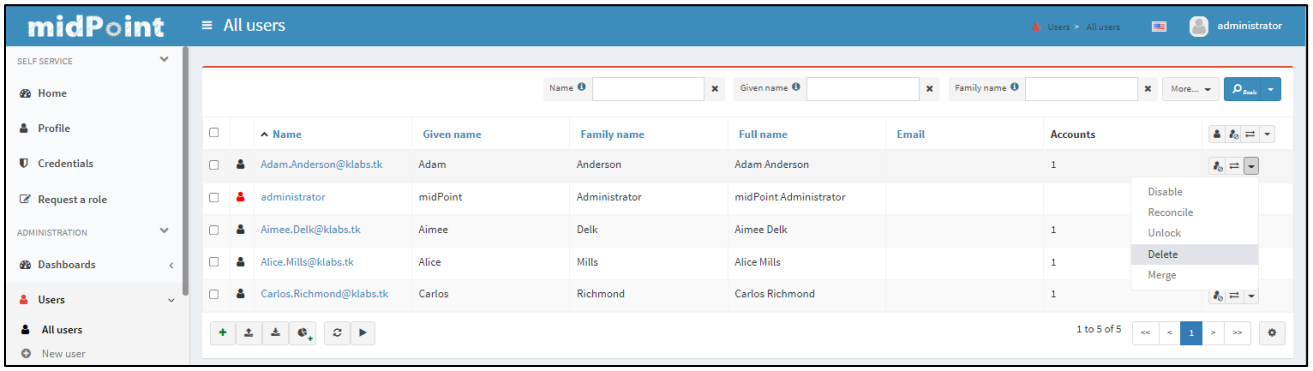
Users

1. On the midPoint administrator console, in the left pane, click **Users** > **All users**.



2. On the **All users** window, in the right pane, perform the following steps to delete a user:

   a. Click icon and select **Delete**.

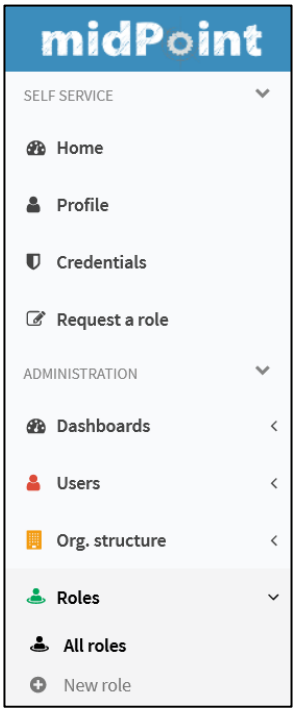


   b. On the **Confirm action** window, click **Yes**.

   Now, you can verify that the user is deleted from **midPoint, SafeNet Trusted Access** and **Azure Active Directory**.

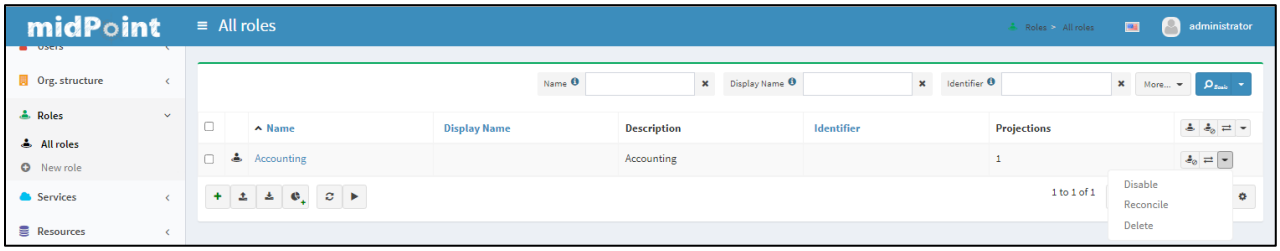
Groups

1. On the midPoint administrator console, in the left pane, click **Users** > **All users**.

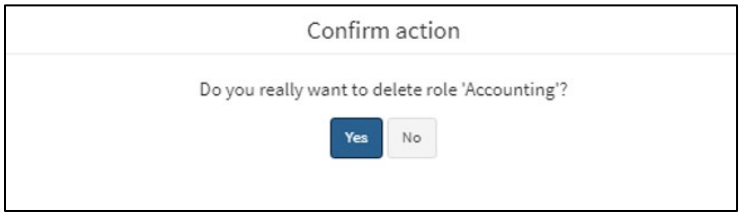


2. On the **All roles** window, in the right pane, perform the following steps to delete a group:

   a. Click icon and select **Delete**.



   b. On the **Confirm action** window, click **Yes**.



   Now, you can verify that the group is deleted from **midPoint, SafeNet Trusted Access** and **Azure Active Directory**.

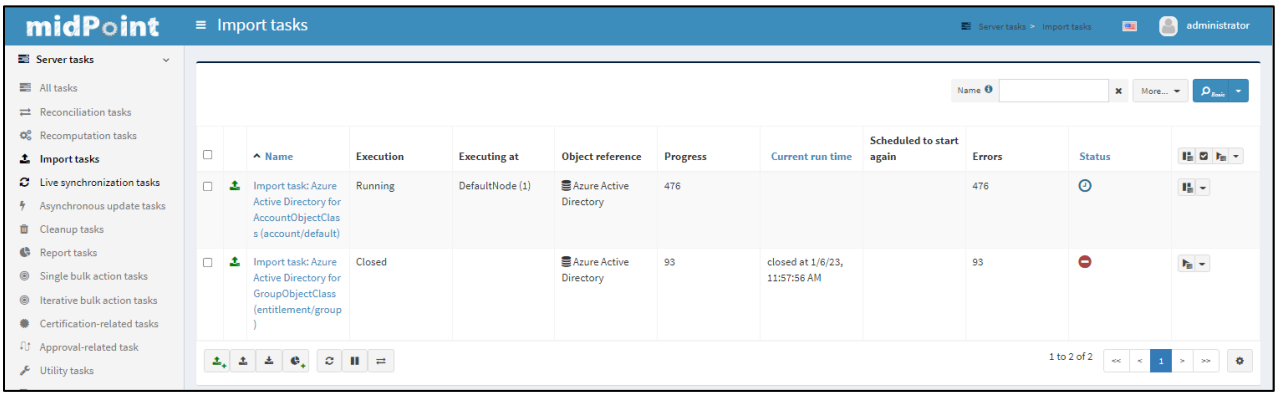
CHAPTER 7: Running the Solution

This chapter will guide you through the detailed steps on how to run the task that you created earlier for synchronization of users and groups to STA.

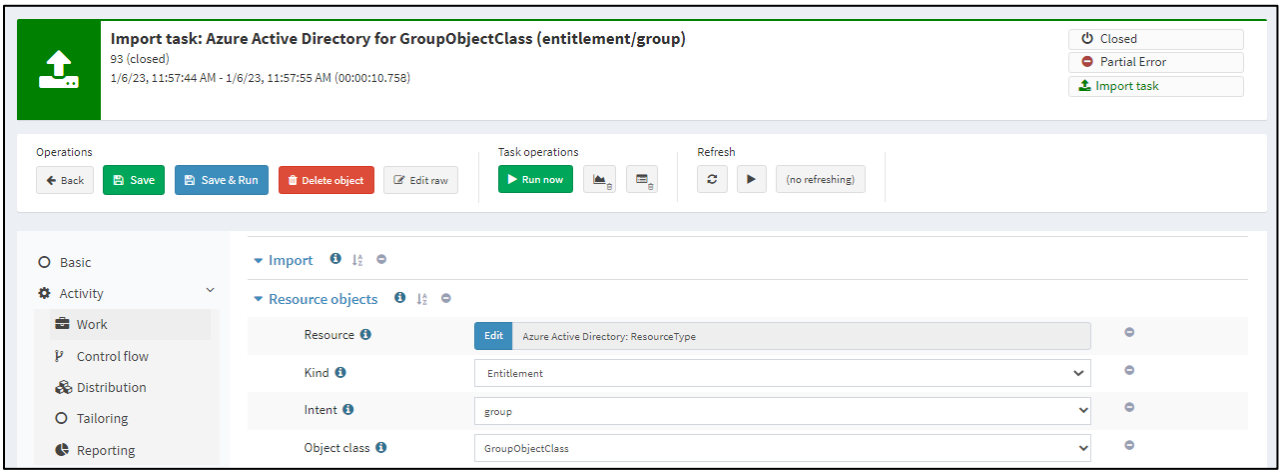
NOTE:
> Ensure that you always run **Group Import** task before the **User Import** task, in order to sync the **Group memberships** to **STA**.
> Duplicate users and groups cannot be synced to STA using midPoint.

Perform the following steps to run the **Import task for groups**:

1. On the midPoint administrator console, in the left pane, click **Server tasks** > **Import tasks**.
2. Under **Import tasks**, click on the task for groups that you created earlier in Task Creation.



3. Click **Save & Run** to execute the task.



Similarly, you can run all the other tasks like Live Synchronization Task and Reconciliation Task by following the above mentioned steps for users and groups.