

SafeNet Trusted Access for Identity Management with Active Directory

CONFIGURATION GUIDE



Document Information

Document Part Number	007-001867-001
Release Date	18 January 2023

Revision History

Revision	Date	Reason
A	18 January 2023	Initial release

Trademarks, Copyrights, and Third-Party Software

Copyright © 2023 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make **any change or** improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect,

special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

CHAPTER 1: Overview	6
Supported Use cases	6
Limitations	7
Test Environment Details	7
CHAPTER 2: Pre-requisites	8
Add Active Directory Certificate in the midPoint keystore.....	8
Import Connector xml File in midPoint.....	9
Import xml Template File in midPoint.....	10
CHAPTER 3: Configure your SafeNet Trusted Access (STA) Connector in midPoint.....	13
CHAPTER 4: Configure your Active Directory (AD) Connector in midPoint	14
Resource basics.....	14
Configuration	15
Schema handling	16
Users.....	17
Groups	19
Add or Edit Mappings	20
Synchronization.....	22
Users.....	22
Groups	25
Capabilities.....	26
CHAPTER 5: Task Creation	28
Import Tasks	28
Users.....	28
Groups	29
Live synchronization tasks	30
Users.....	30
Groups	31
Reconciliation Tasks	33
Users.....	33
Groups	34
CHAPTER 6: Test your Configuration	36
Import groups from Active Directory to midPoint	36
Import users from Active Directory to midPoint	37
Verifying users and groups in STA	38
Users.....	38
Groups	39
Deleting user and group from midPoint	39
Users.....	39

Groups	40
CHAPTER 7: Running the Solution	43

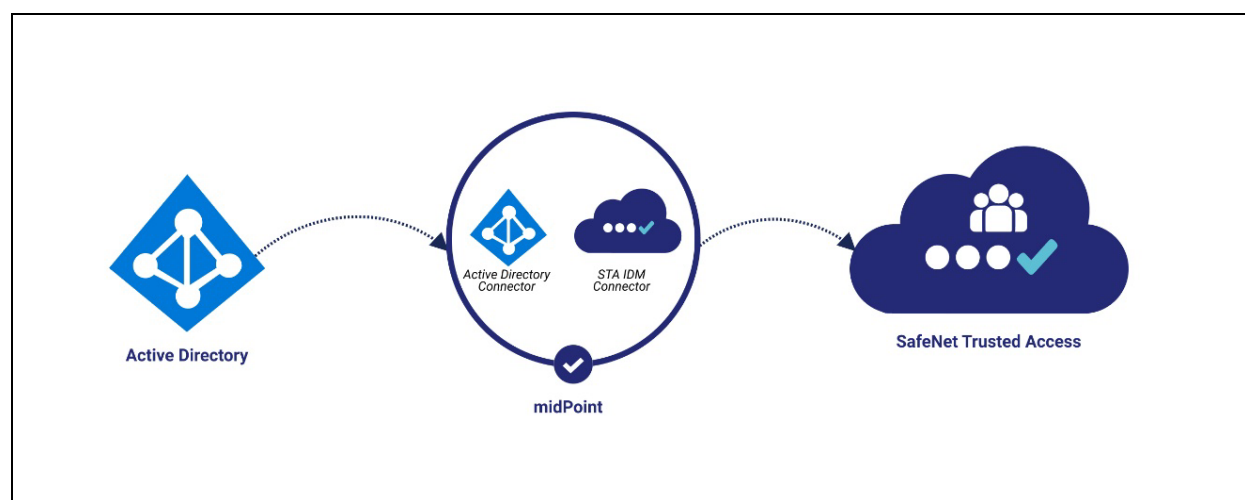
CHAPTER 1: Overview

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.

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

This solution provides you with preconfigured 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 informs about the use cases supported by **Active Directory (AD)** connector when syncing with **SafeNet Trusted Access (STA)** using midPoint.

- > User synchronization
- > Group synchronization
- > User live synchronization
- > Group live synchronization
- > User activation

Limitations

Following are the limitations that **Active Directory (AD)** connector faces when syncing with **SafeNet Trusted Access (STA)** using **STA IDM Connector** in midPoint.

- > 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.
- > If any group is associated to any provisioning rule in STA, midpoint would not be able to update the same.
- > Nested groups synchronization to STA is not supported.
- > If there are two groups with same name in different domains in AD, only one group will be created in STA.
- > 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 environment which consist of Active Directory connector and the STA IdM Connector.

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

NOTE: We have validated 2000 User's and 20 Group's synchronization in this release.

CHAPTER 2: Pre-requisites

This chapter will guide you through the steps to add a certificate, xml files and connectors which are pre-requisites in order for midPoint to work successfully.

The following are the required pre-requisites:

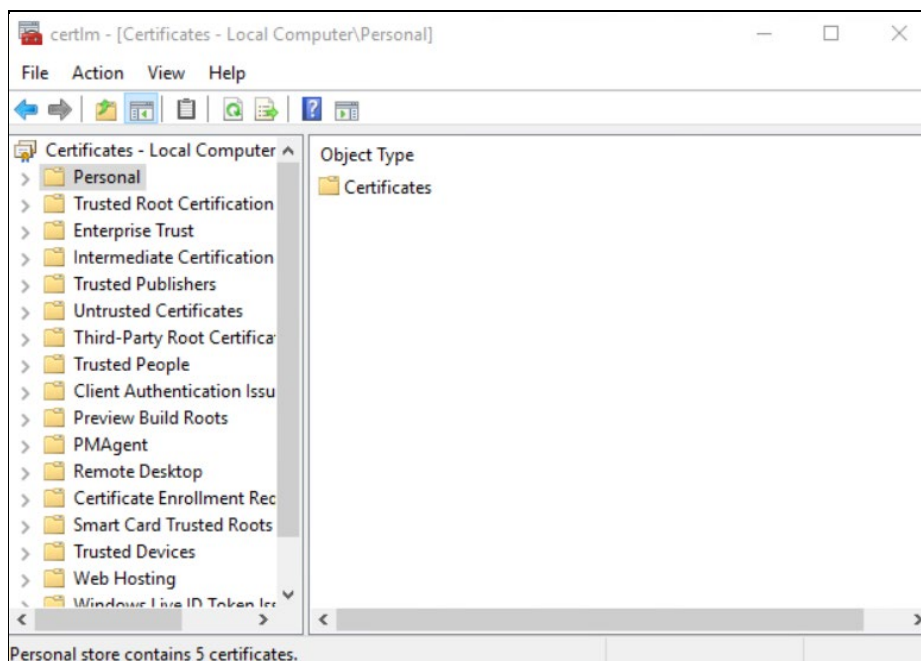
1. [Add Active Directory Certificate in the midPoint keystore](#)
2. [Import Connector.xml File in midPoint](#)
3. [Import Template.xml File in midPoint](#)

Add Active Directory Certificate in the midPoint keystore

To connect to the resource successfully, it is essential that you add the Root CA Certificate from the Active Directory into the midPoint keystore.

Follow the below steps to add the Root CA Certificate to keystore of midPoint:

- a) In the Active Directory (AD) server, open the Certificate Authority application by navigating to **Start > Run > certsrv.msc**.



- b) Right click the Root CA certificate and select **Properties**.
- c) On the **General** tab, click **View Certificate** button then on **Details** tab, select **Copy to File**.

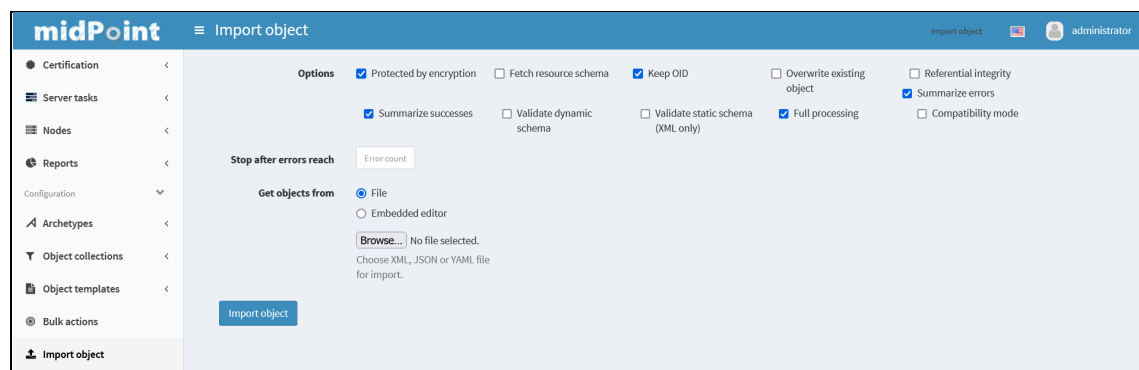
- d) Ensure that **DER Encoded binary X.509** in (.cer) format is selected.
- e) Click **browse** and save the certificate then click **Next > Finish**.
- f) On the machine where midPoint is installed, goto **<midpoint-installation-directory>/var** and copy the downloaded <active-directory-certificate>.cer certificate then execute the below command on the terminal window:

```
keytool -importcert -alias <certificate-alias-name> -file <active-directory-certificate name>.cer -
keystore <your_keystore_file>
```

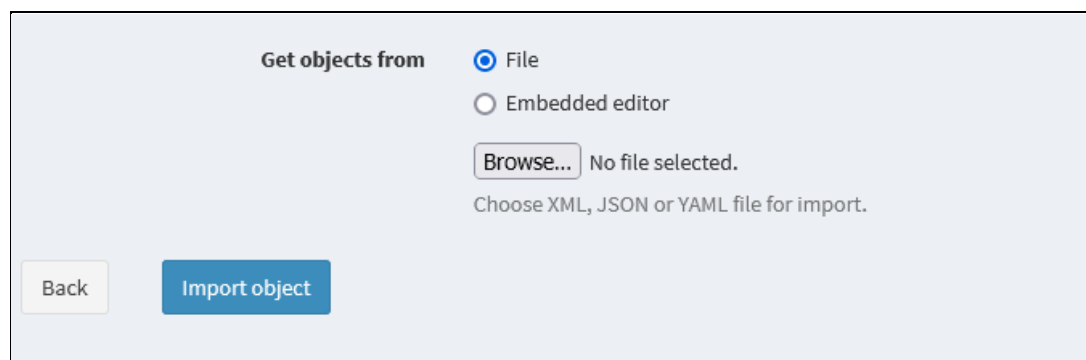
Import Connector xml File in midPoint

This section provides information on how to add the Active Directory Connector xml File to midPoint.

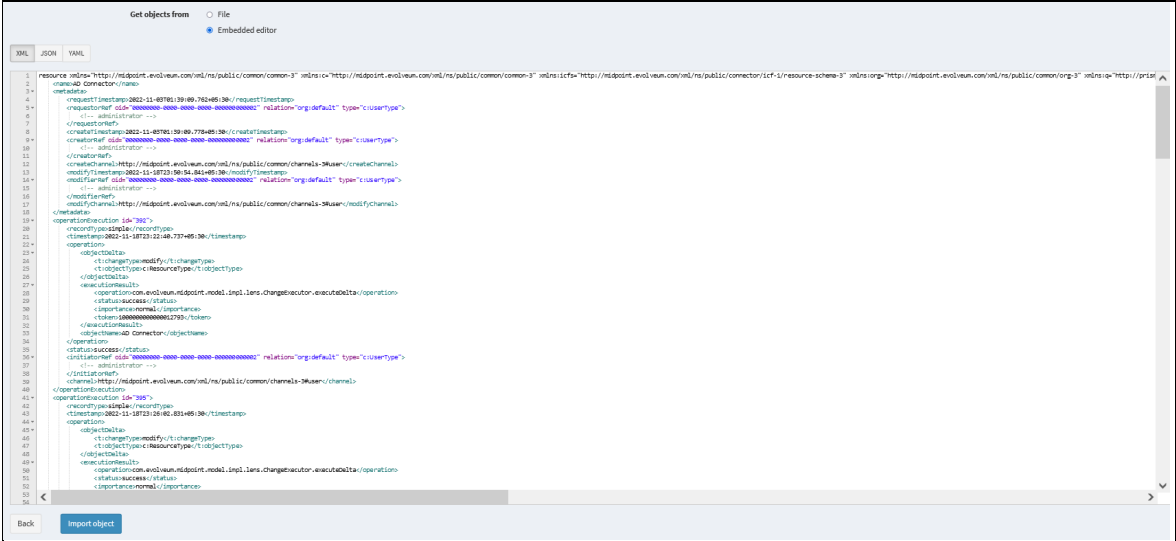
1. Download the **Active_Directory.xml** file from URL, <<https://github.com/ThalesGroup/sta-idm-framework>> and save the file.
2. On the midPoint Administrator console on the left pane, scroll down and click **Import object** and in the **Get objects from** field, perform either one of the **steps (a or b)** listed below to setup the connector xml file:



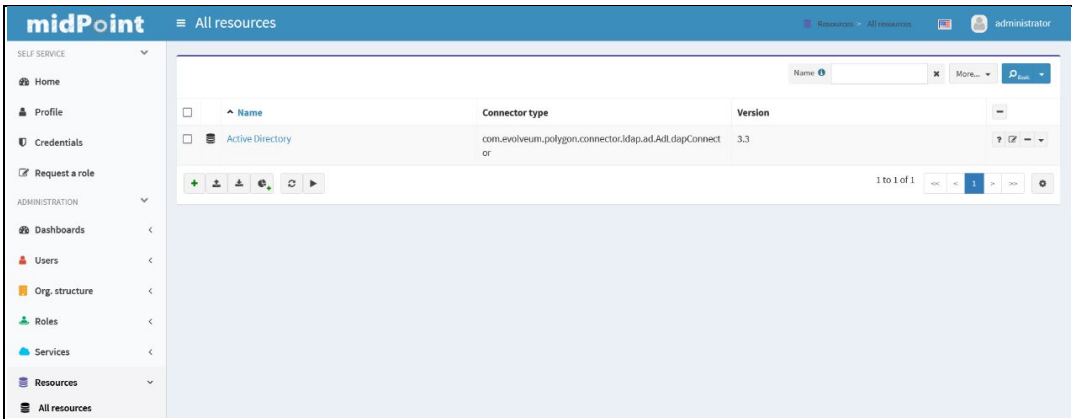
- a. Select the **File** > click **Browse** to upload the **connector xml file**, then click **Import object**.



- b. Select the **Embedded editor** and paste the contents of connector xml file in the editor then click **Import object**.



- On the left pane, click **Resources** > **All resources** and confirm that you can view newly created resource in the right window.

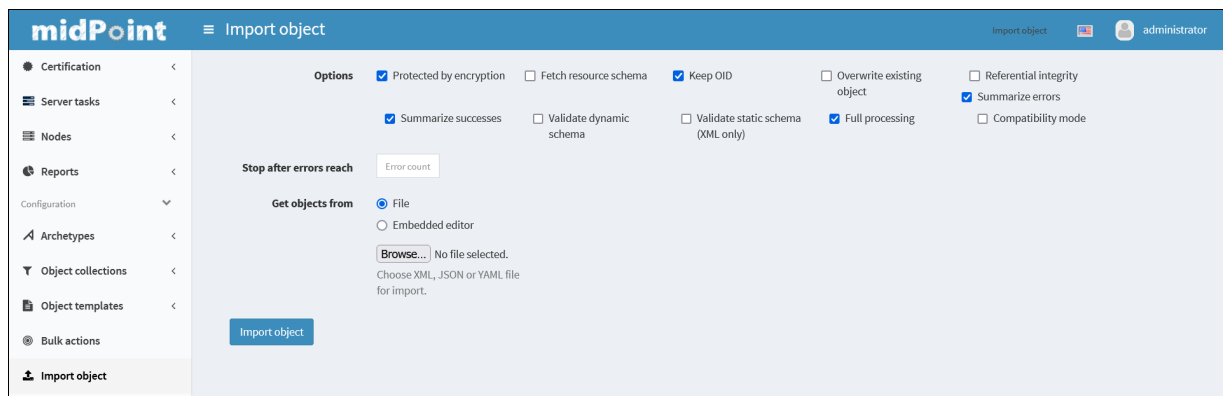


Import xml Template File in midPoint

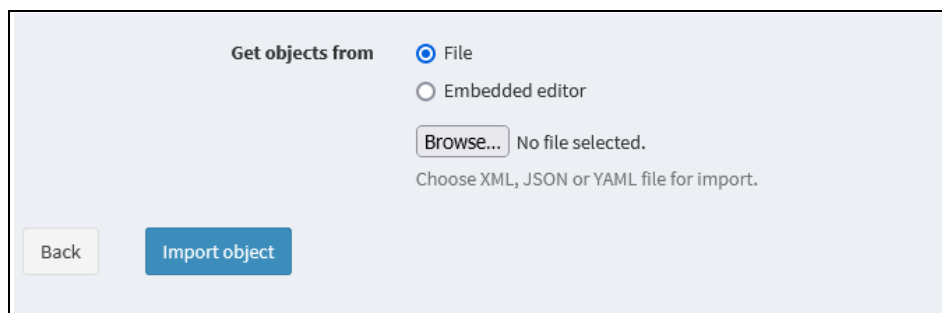
This section provides information on how to add xml template file to midPoint. These templates will help you in syncing **users** and **groups** to **STA**.

1. Download the following xml template files from URL <<https://github.com/ThalesGroup/sta-idm-framework>> and save the files:
 - a. **RoleTemplate_for_AD.xml**: This template contains the mappings that assign a metarole to groups being imported from Active Directory.
 - b. **UserTemplate_for_AD.xml**: This template contains the mappings that assign a role (STA user role) to users being imported from Active Directory.
 - c. **MetaRole_for_STA.xml**: This template is used to create a metarole in midpoint. This metarole act as super role and is used to create groups in STA along with their membership.

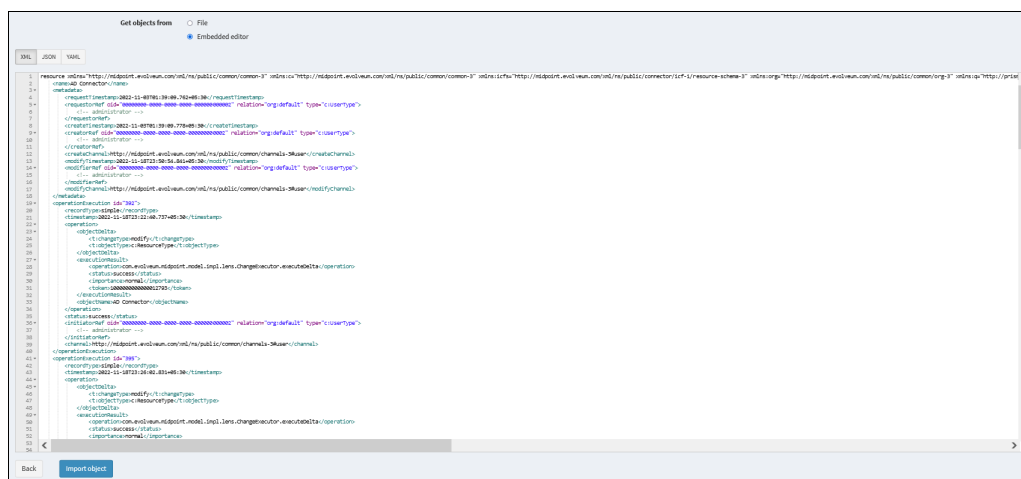
- d. **STA_user_role.xml**: This template is used to create a role in midpoint. This role is used to create user(s) in STA automatically.
2. On the midPoint administrator console, on the left pane, scroll down and click **Import object** and in the **Get objects** from field, perform either one of the **steps (a or b)** listed below to setup the template xml file:



- a. Select **File** > click **Browse** to upload the **template xml file** > then click **Import object**.



- b. Select **Embedded editor** and paste the contents of template xml file in the editor then click **Import object**.



NOTE: You must follow the above **step (a or b)** to setup all the templates files one by one as mentioned in [Step 1.](#)

NOTE: Before importing these, **MetaRole_for_STA.xml** & **STA_user_role.xml** files, **you** need to import **SafeNet_Trusted_Access.xml** file as mentioned in the STA IdM Connector documentation guide in chapter 3, to avoid any validation error while importing the files.

CHAPTER 3: Configure your SafeNet Trusted Access (STA) 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 setup **SafeNet Trusted Access (STA) Connector** in **midPoint**, you can perform the steps mentioned in **SafeNet Trusted Access (STA) Connector Guide**, <https://github.com/ThalesGroup/sta-idm-connector>.

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

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

On the left pane, click **Resources** > **All resources** and in the **All resources** window click **Active Directory** resource you have created in [step 2](#) of prerequisites section. On the **Resource operations** tab, click **Edit using wizard**.

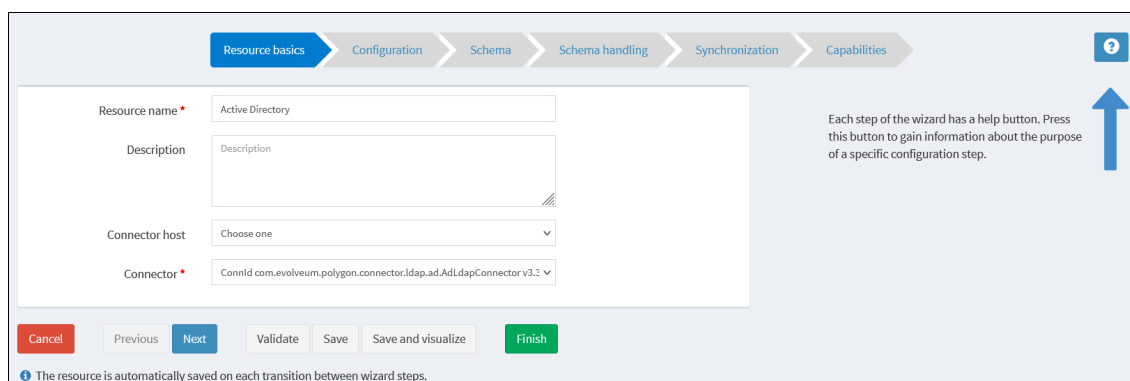
The configuration is divided into the following sections:

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** tab:

- a. In the **Resource name** field, modify the name of the connector as per your preference for the identification purpose (for example, **Active Directory (AD) Connector**).
- b. In the **Connector** field, ensure the Active Directory connector is selected, (for example, **com.evolveum.polygon.connector.ldap.ad.AdLdapConnector v3.3**).
- c. Click **Next**.



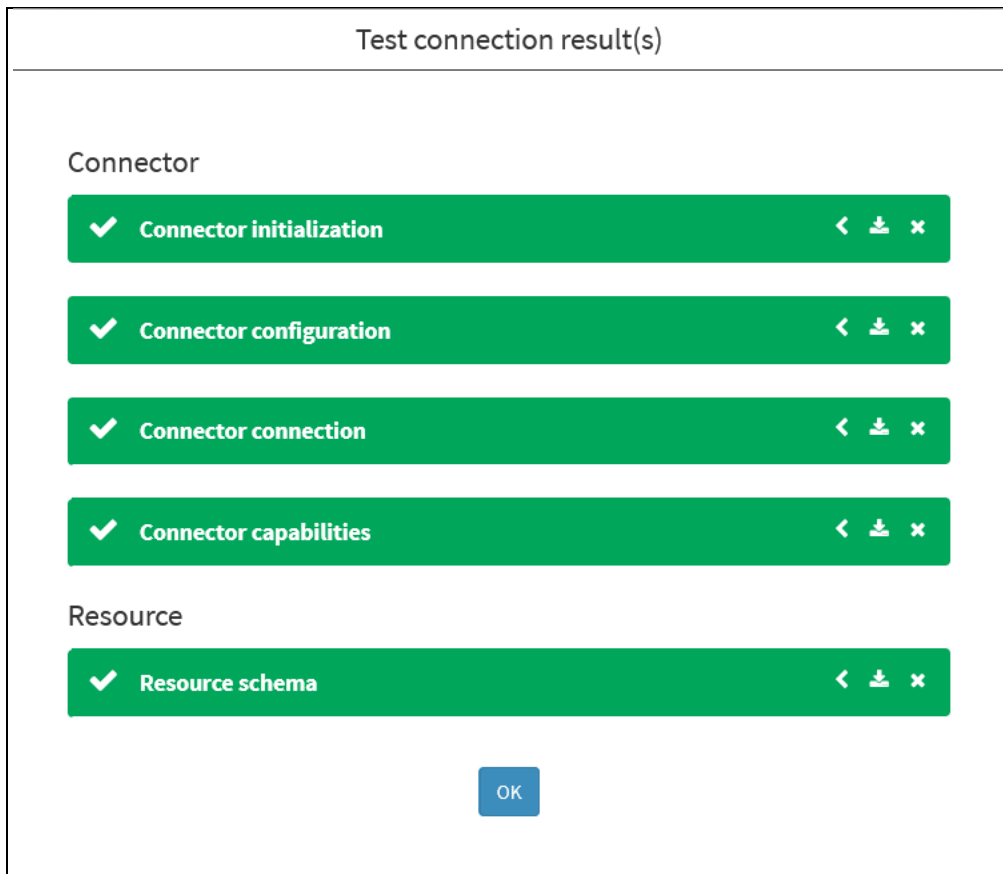
Configuration

In this section, you will find prefilled values, you need to update these values with information corresponding to your Active Directory instance.

1. On the **Configuration** tab, perform the following steps:
 1. In the **Host** field, update the field with the host name/ip address of your **Active Directory Server** (for example, **example.com**).
 2. In the **Port** field, ensure the value is **636**.
 3. In the **Connection security** field, ensure the value is **ssl**.
 4. In the **SSL protocol** field, ensure the standard name for the protocol is **SSL**.
 5. In the **Bind DN** field, update the field with the **Distinguished Name (DN)** of your Active Directory service account (for example, **CN=Administrator,CN=Users,DC=example,DC=com**).
 6. In the **Bind password** field, click on **Change** and then enter the password for your service account. In the **Repeat Password** field enter the same password again.
 7. In the **Base context** field, update the field with the base context of your Active Directory server (for example, **DC=example,DC=com**).
 8. In the **Paging block size** field, update the value as per your preference.
 9. Click **Save and test connection**.

The screenshot shows the 'Configuration' tab in the midPoint interface. The 'Host' field is set to 'example.com', 'Port number' to '636', 'Connection security' to 'ssl', 'SSL protocol' to 'SSL', 'Bind DN' to 'CN=Administrator,CN=Users,DC=example,DC=com', 'Bind password' to 'Password is set' (with a 'Change' button), 'Base context' to 'DC=example,DC=com', and 'Paging block size' to '30'. A 'Save and test connection' button is located at the bottom left of the configuration area. Below this, there are navigation buttons: 'Cancel', 'Previous', 'Next', 'Validate', 'Save', 'Save and visualize', and 'Finish'.

2. **Test Connection result(s)** pop-up window will display the success or failure for the test connection.



NOTE: If you find any error on testing the connection, please check your active directory configuration. For any error related to certificate, ensure that you have added the Active Directory Root CA Certificate in your midPoint keystore as mentioned in [step 1](#) of Pre-requisites chapter.

3. Click **OK**.
4. Click **Next** twice to go to **Schema handling** tab.

Schema handling

This section contains attributes mapping for both **users** and **groups** for their synchronization.

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

NOTE: Ensure 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 > in **Object types** section > click **Account (ACCOUNT, default) ->user** to view or edit the mapping.



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

Fields	Values
Kind	Account
Intent	default
Object class	user

Object types

Account (ACCOUNT, default) -> user
Group (ENTITLEMENT, group) -> group

<< < 1 > >>

Add object type

Account

Kind Account
Intent default
Display name Account
Description

Default ☒
Dependencies

Object class user

Attributes

ri: dn (Distinguished Name) in: fullName			
ri: sAMAccountName (Login name) in: name			
ri: sn in: familyName			
ri: givenName in: givenName			
ri: userPrincipalName in: userPrincipalName			
ri: telephoneNumber in: telephoneNumber			
ri: streetAddress in: locality			
ri: description in: description			
ri: postalCode in: postalCode			
ri: l in: city			
ri: co in: country			
ri: displayName in: additionalName			
ri: mail in: emailAddress			
ri: st in: state			

Associations

ri: group (AD Group Membership) in: assignment			
--------------------------------------------------	--	--	--

Iteration
Protected
Activation
Credentials

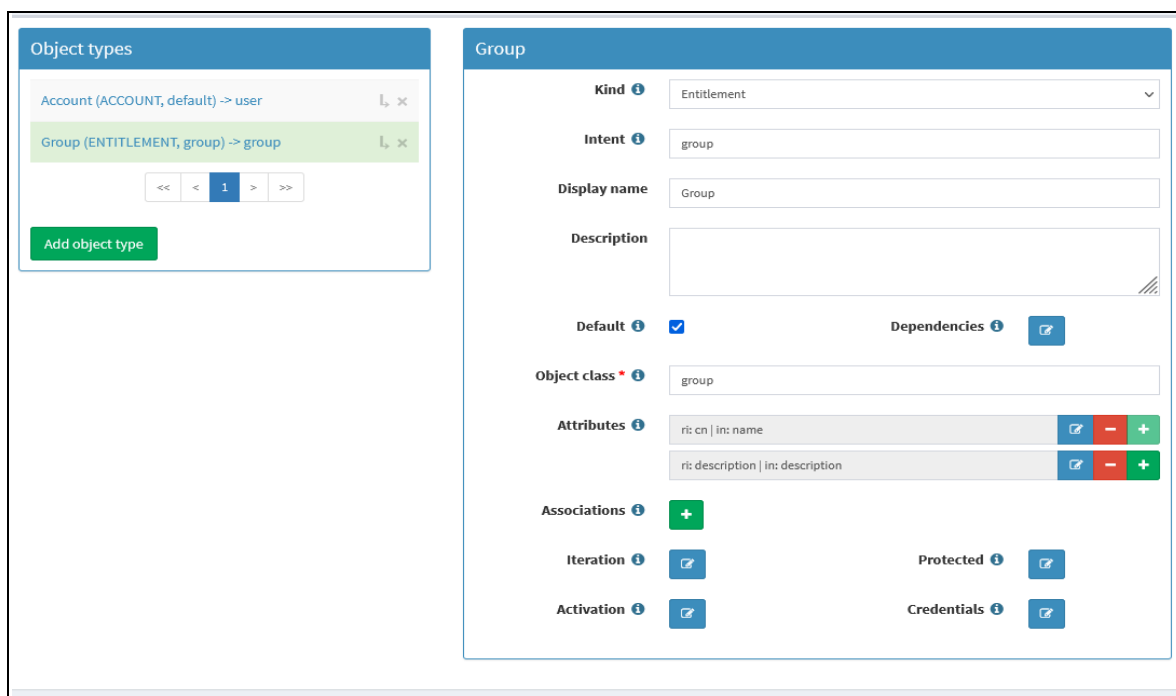
Groups

On the **Schema handling** tab > in **Object types** section > click **Group (ENTITLEMENT, group) -> group** to view or edit the mapping.




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

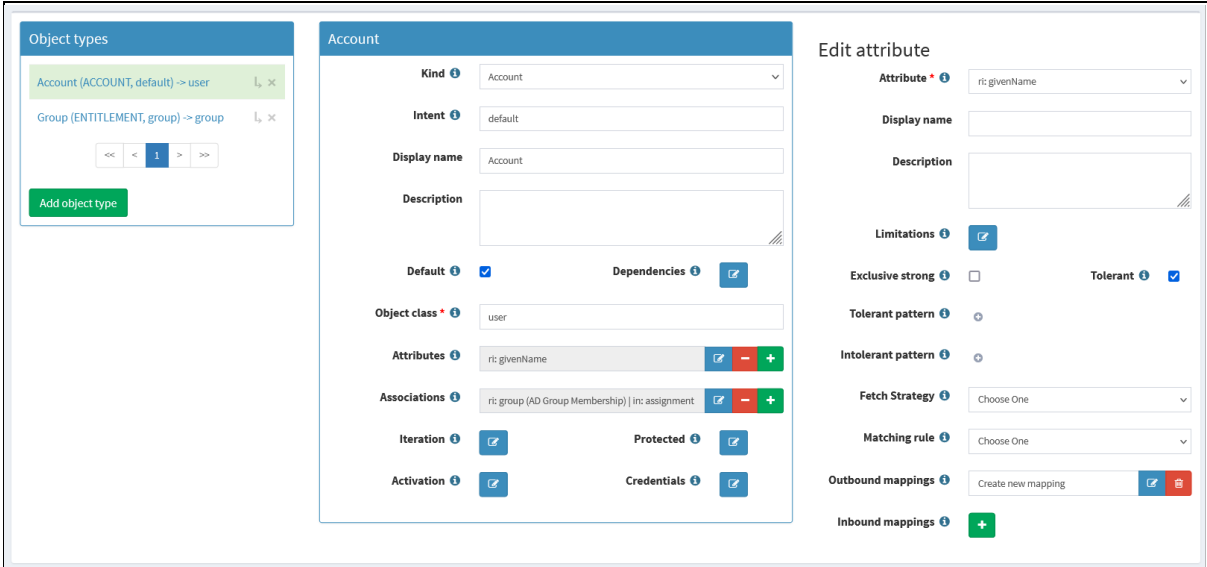
Fields	Values
Kind	Entitlement
Intent	group
Object class	group




Add or Edit Mappings

- To add or edit an attribute in Schema handling, click  icon or  icon respectively right next to the Attributes field and in the **Edit Mapping** attribute tab, perform the following steps:

- In the **Attribute** field, select a value from the dropdown (for example, **givenName**).



The screenshot displays the midPoint configuration interface. On the left, the 'Object types' panel shows 'Account (ACCOUNT, default) -> user' and 'Group (ENTITLEMENT, group) -> group'. The main area is titled 'Account' and contains several fields: 'Kind' (Account), 'Intent' (default), 'Display name' (Account), 'Description', 'Default' (checked), 'Object class' (user), 'Attributes' (ric:givenName), 'Associations' (ric:group (AD Group Membership) | inc:assignment), 'Iteration', 'Protected', 'Activation', 'Dependencies', 'Limitations', 'Exclusive strong', 'Tolerant' (checked), 'Intolerant pattern', 'Fetch Strategy' (Choose One), 'Matching rule' (Choose One), 'Outbound mappings' (Create new mapping), and 'Inbound mappings' (+). The 'Edit attribute' tab is active, showing the 'Attribute' field with 'ric:givenName' selected, and the 'Display name' and 'Description' fields.

- In the **Inbound mappings** field, click  icon right next to it and in the **Target** enter name of the user attribute that you want to set for the attribute you just selected in [step a](#) (for example, **givenName**), click **Apply**.

Edit Mapping

Name

Description

Authoritative ☒

Exclusive ☐

Strength

Channel

Except channel

Source

Target

Expression type

Expression

1

Condition type

Condition

1

c. After the successful update of the Attribute mapping, following window will appear:

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

2. Click **Next**.

Synchronization

This section provides the details about the reaction for both users and groups. It contains the action to be taken by midPoint for different situation of users and groups.

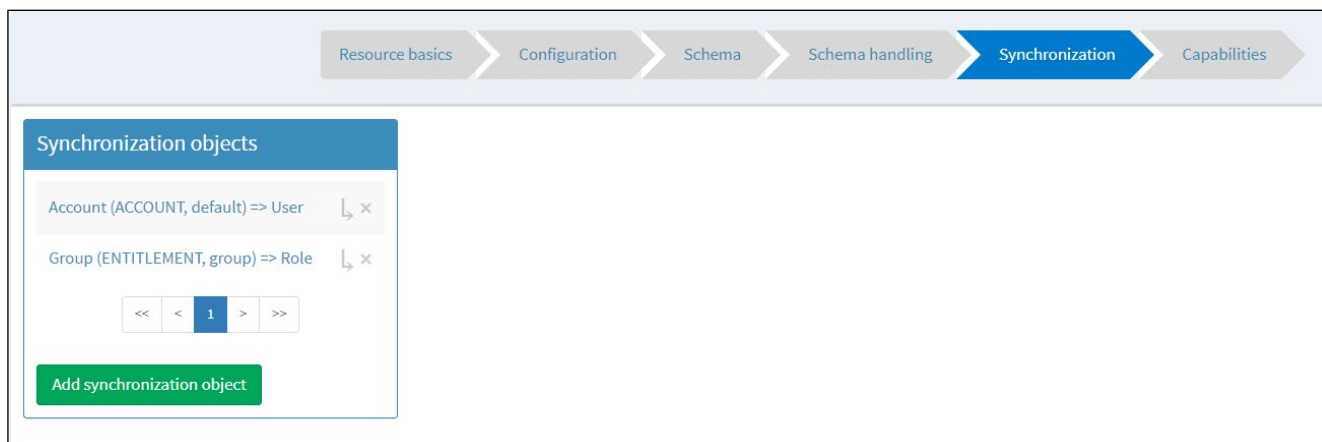
NOTE: Ensure the default set values are case sensitive.

The information in this section is divided into two sub sections:

1. [Users](#)
2. [Groups](#)

Users

On the **Synchronization** tab > in **Synchronization objects** section > click **Account (ACCOUNT, default)**
=> **User**



The Synchronization window for users is displayed. Ensure all the values are set as in the below table:

Fields	Values
Kind	Account
Intent	default
Object class	user
Focus	UserType

- Ensure that **Enabled** checkbox is selected.
- In the **Object template** field, select the value **User Template for AD**.

Synchronization objects

Account (ACCOUNT, default) => User
Group (ENTITLEMENT, group) => Role

<< < 1 > >>

Add synchronization object

Edit 'Account'

Name: Account

Description:

Kind: Account

Intent: default

Object class: user

Focus: UserType

Enabled: ☒
Reconcile: ☐

Correlation: (name not specified)

Confirmation:
Condition:

Object template: User Template for AD

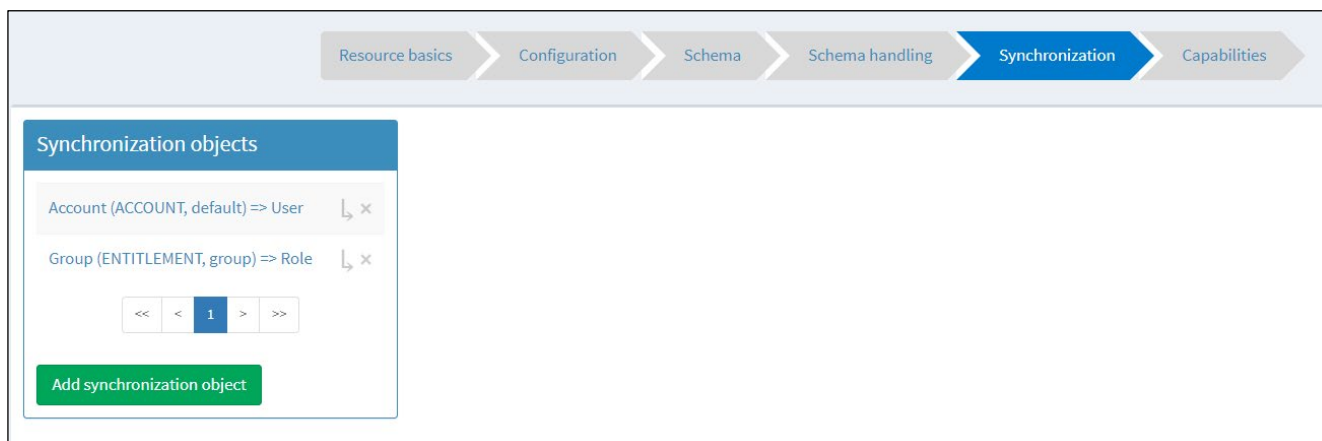
Opportunistic: Undefined

Reaction:

- (LINKED -> sync)
- (DELETED -> deleteFocus)
- (UNLINKED -> link)
- (UNMATCHED -> addFocus)

Groups

On the **Synchronization** tab > in **Synchronization objects** section > click **Group (ENTITLEMENT, group) => Role**.



The Synchronization window for groups is displayed. Ensure all the values are set as in below table:

Fields	Values
Kind	Entitlement
Intent	group
Object class	group
Focus	RoleType

- Ensure that **Enabled** checkbox is selected
- In the **Object template** field, select the value **Role Template for AD**.



The screenshot displays two panels in the midPoint configuration tool. The left panel, titled 'Synchronization objects', shows a list of objects: 'Account (ACCOUNT, default) => User' and 'Group (ENTITLEMENT, group) => Role'. The 'Group' object is selected and highlighted in green. Below the list is a green button labeled 'Add synchronization object'. The right panel, titled 'Edit Group', contains various configuration fields for the selected group. Fields include 'Name' (set to 'Group'), 'Description' (empty), 'Kind' (set to 'Entitlement'), 'Intent' (set to 'group'), 'Object class' (set to 'group'), 'Focus' (set to 'RoleType'), 'Enabled' (checked), 'Reconcile' (unchecked), 'Correlation' (set to '(name not specified)'), 'Confirmation' (set to a blue icon), 'Condition' (set to a blue icon), 'Object template' (set to 'Role Template for AD'), and 'Opportunistic' (set to 'Undefined'). At the bottom, there is a 'Reaction' section with four entries: '(LINKED -> sync)', '(DELETED -> deleteFocus)', '(UNLINKED -> link)', and '(UNMATCHED -> addFocus)', each with edit, delete, and add icons.

- Click **Next**.

The screenshot shows a horizontal navigation bar with several buttons. From left to right, the buttons are: 'Cancel' (red), 'Previous' (light blue), 'Next' (blue), 'Validate' (light blue), 'Save' (light blue), 'Save and visualize' (light blue), and 'Finish' (green).

Capabilities

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

1. On the **Capabilities** tab > click **Activation** and perform the following steps:
 - a. Ensure that **Enabled** checkbox is selected.
 - b. In the **Attribute name** field, select **userAccountControl**.
 - c. In the **Enable list** field, click  icon then enter the value **Enabled**.
 - d. In the **Disable list** field, click  icon then enter the value **disabled**.
 - e. Click **Finish** to save the connector configuration.

Capabilities

- Live sync ⓘ
- Test connection ⓘ
- Create ⓘ
- Update ⓘ
- Delete ⓘ
- Script ⓘ
- Credentials ⓘ
- Auxiliary object classes ⓘ
- Read ⓘ
- Activation ⓘ

Activation configuration

Status

Enabled ⓘ ☒

Returned by default ⓘ ☐

Ignore attribute ⓘ ☐

Attribute name ⓘ

Enable list ⓘ

Disable list ⓘ

Lockout

Enabled ⓘ ☐

Returned by default ⓘ ☐

Ignore attribute ⓘ ☐

Attribute name ⓘ

Normal list ⓘ

Locked list ⓘ

Valid from

Enabled ⓘ ☐

Returned by default ⓘ ☐

Valid to

Enabled ⓘ ☐

Returned by default ⓘ ☐

Buttons: Cancel, Previous, Next, Validate, Save, Save and visualize, Finish

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

CHAPTER 5: Task Creation

This chapter guides you to create task in midpoint for various actions. These tasks are used to synchronize the users and groups.

You can create the following tasks in midpoint:

1. [Import Task](#)
2. [Live Synchronization Task](#)
3. [Reconciliation Task](#)

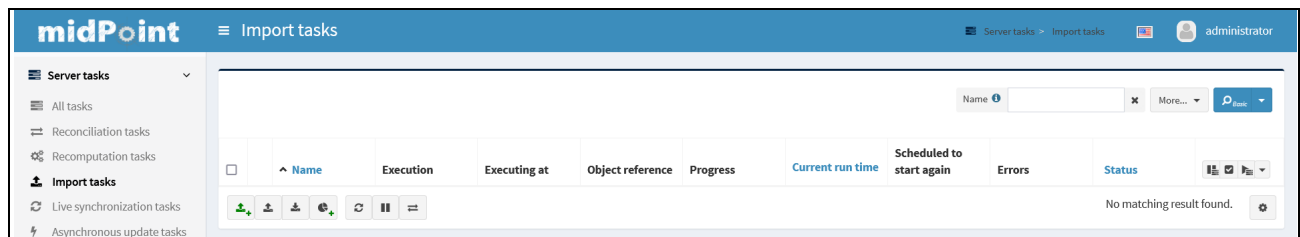
Import Tasks

This section explain, the steps to create import tasks for the users and groups.

1. [Users](#)
2. [Groups](#)

Users


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



2. In the **New Import task** window, in the **Resource objects** section, perform the following steps to create a task:
 - a. In the **Resource** field, click **Edit** and select **Active Directory**.
 - b. In the **Kind** field, select **Account**.
 - c. In the **Intent** field, select **default**.
 - d. In the **Object class** field, select **user**.

3. Click **Save** to create the task.

Groups

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

2. In the **New Import task** window, in the **Resource objects** section, perform the following steps to create a task:
 - a. In the **Resource** field, click **Edit** and select **Active Directory**.
 - b. In the **Kind** field, select **Entitlement**.
 - c. In the **Intent** field, select **group**.
 - d. In the **Object class** field, select **group**.

- Click **Save** to create the task.

Live synchronization tasks

This section explain, steps to create live synchronization tasks for the users and groups.

- [Users](#)
- [Groups](#)

Users

- In the left pane, scroll down and click **Server tasks** > **Live synchronization tasks** and In the **New Live synchronization tasks** window click  icon to add a new task.

- On the **New Live Synchronization task** window, in the **Live synchronization** section, perform the following steps to create a task:
 - 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**).

New Live synchronization task

Server tasks > Live synchronization tasks > New Live synchronization task

administrator

Operations

Back Save Save & Run

Basic Live synchronization

Schedule

Batch size 100

3. On the **New Live synchronization task** window, in the **Resource objects** section, perform the following steps to create a task:
 - a. In the **Resource** field, click **Edit** and select **Active Directory**.
 - b. In the **Kind** field, select **Account**.
 - c. In the **Intent** field, select **default**.
 - d. In the **Object class** field, select **user**.

Resource objects

Resource	Edit Active Directory; ResourceType	
Kind	Account	
Intent	default	
Object class	user	

Show empty fields

4. On the **New Live synchronization task** window click **Schedule** and in the **Schedule** section, enter the value of **Interval** in seconds (for example, 86400).

Operations

Back Save Save & Run

Basic Schedule

Interval 86400

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

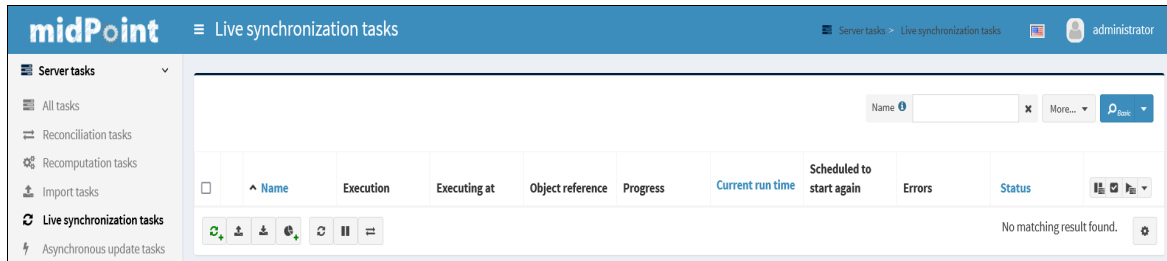
5. Click **Save** to create the task.

Operations

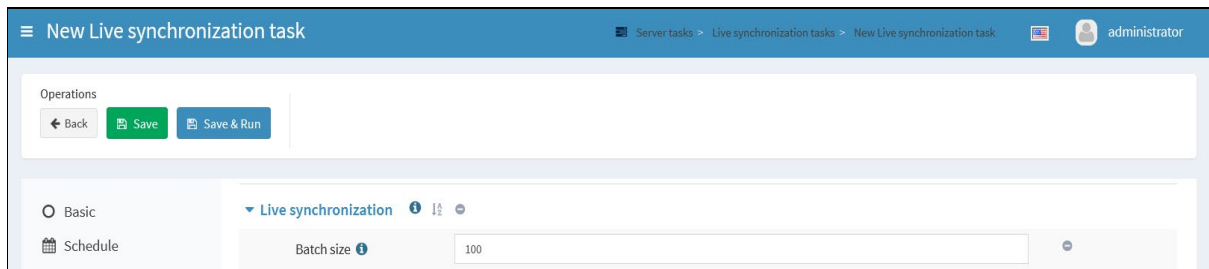
Back Save Save & Run

Groups

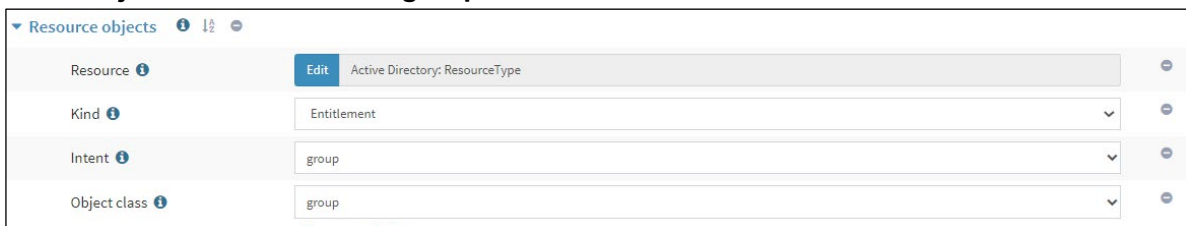
1. In the **New Live synchronization tasks** window click  icon to add a new task.



2. On the **New Live synchronization task** window in the **Live synchronization** section, perform the following steps to create a task:
 - a. 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).



3. On the **New Live synchronization task** window, in the **Resource objects** section, perform the following steps to create a task:
 - a. In the **Resource** field, click **Edit** and select **Active Directory**.
 - b. In the **Kind** field, select **Entitlement**.
 - c. In the **Intent** field, select **group**.
 - d. In the **Object class** field, select **group**.

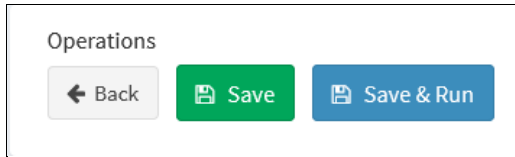


4. On the **New Live synchronization task** window, click **Schedule** and in the **Schedule** section, enter the value of **Interval** in seconds (for example, 86400).



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

- Click **Save** to create the task.



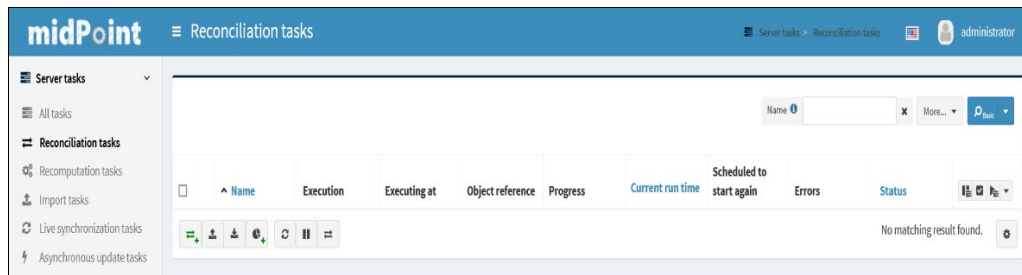
Reconciliation Tasks

This section explain steps to create reconciliation tasks for the users and groups.

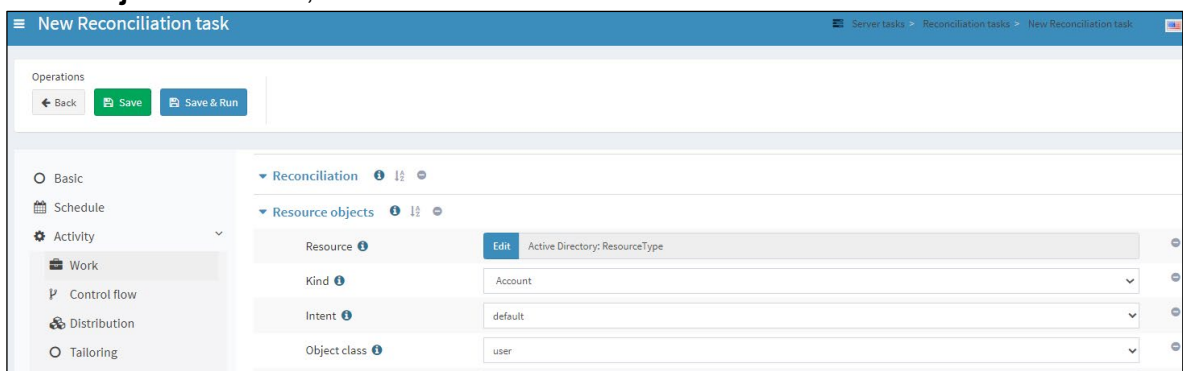
- [Users](#)
- [Groups](#)

Users

- In the left pane, scroll down and click **Server tasks > Reconciliation tasks** and in the **Reconciliation tasks** window click  icon to add a new task.



- On the **New Reconciliation task** window, in the **Resource objects** section, perform the following steps to create a task:
 - In the **Resource** field, click **Edit** and select **Active Directory**.
 - In the **Kind** field, select **Account**.
 - In the **Intent** field, select **default**.
 - In the **Object class** field, select **user**.



- On the **New Reconciliation task** window click **Schedule** and in the **Schedule** section, enter the value of **Interval** in seconds (for example, 86400).

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

- Click **Save** to create the task.

Groups

- In the **Reconciliation tasks** window click icon to add a new task.

- On the **New Reconciliation task** window, in the **Resource objects** section, perform the following steps to create a task:
 - In the **Resource** field, click **Edit** and select **Active Directory**.
 - In the **Kind** field, select **Entitlement**.
 - In the **Intent** field, select **group**.
 - In the **Object class** field, select **group**.

- On the **New Reconciliation task** window, click **Schedule** and in the **Schedule** section, enter the value of **Interval** in seconds (for example, **86400**).

Operations

← Back Save Save & Run

○ Basic ▾ Schedule ⓘ ⓘ ⓘ

📅 Schedule Interval ⓘ 86400 ⓘ

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

4. Click **Save** to create the task.

Operations

← Back Save Save & Run

CHAPTER 6: Test your Configuration

This chapter will guide you through the steps to validate the above configurations in midPoint.

To test synchronization, you must have some test users and groups in your Active Directory.

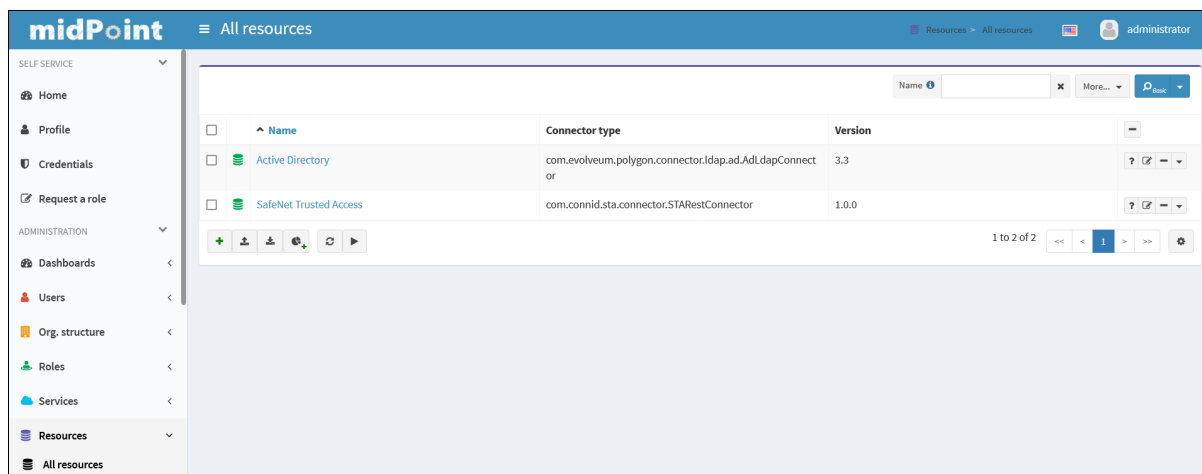
1. [Import groups from Active Directory to midPoint](#)
2. [Import users from Active Directory to midPoint](#)
3. [Verifying users and groups in STA](#)
4. [Deleting user and group from midPoint](#)


NOTE: You need to always import the group before the user in order to sync the group memberships to STA.

Import groups from Active Directory to midPoint

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

1. On the left pane, click **Resources** > **All resources**.



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


NOTE: After successful import, the value of situation field will be changed to **Linked**.

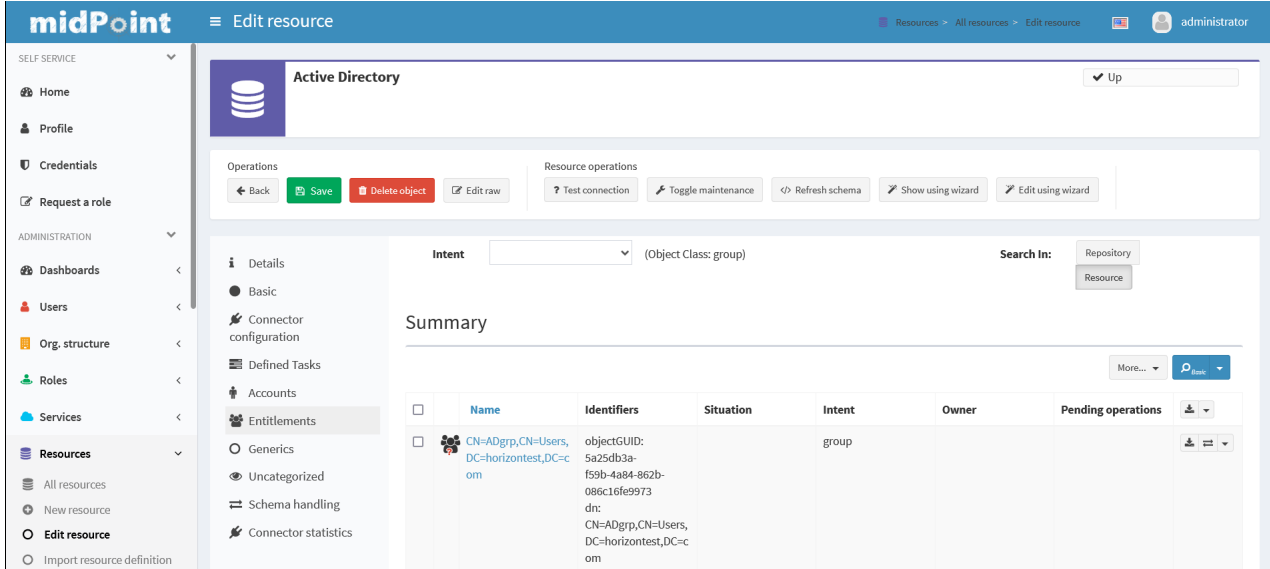
Import users from Active Directory to midPoint

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

1. Login to **midPoint**, on the administrator console, on the left pane, click **Resources** > **All resources**.

2. On the **All resources** window, click **Active Directory** and perform the following steps:
 - a. In the Active Directory Connector, click **Accounts** > then on right side in the **Search In** field click **Resource**.

b. All the **Active Directory** users will be displayed in the below section. Click  icon to import the user into **midPoint**.



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

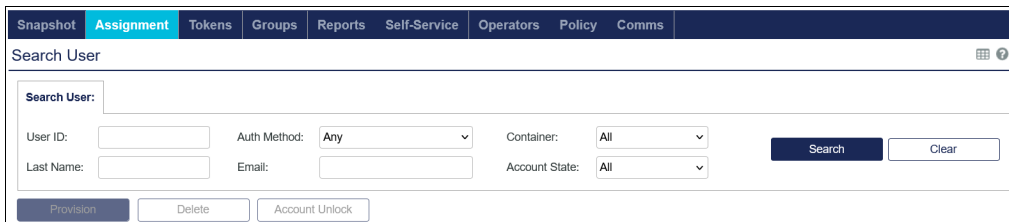
Verifying users and groups in STA

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

Users

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

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

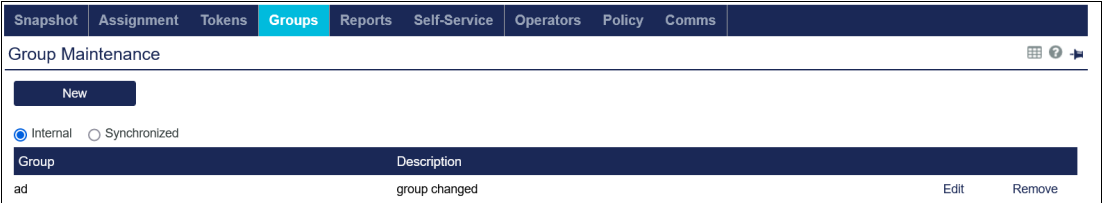


2. In the **Search User** module, you can find the list of users that are pushed from **Active Directory**. Alternatively, you can search for individual users to verify if the users are provisioned.

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 see all the **Active Directory** groups that are provisioned to STA.

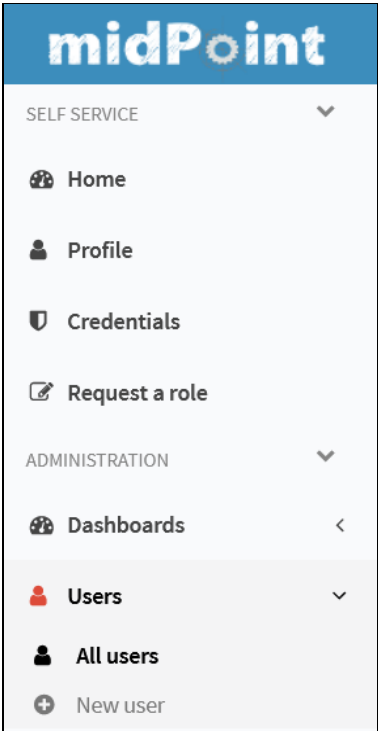


Deleting user and group from midPoint

This section provides the steps for deleting the user and group from **midpoint**.

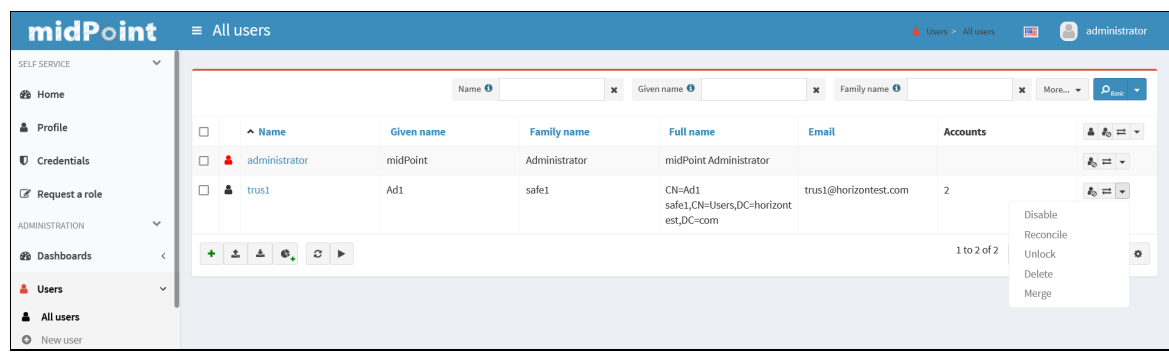
Users

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

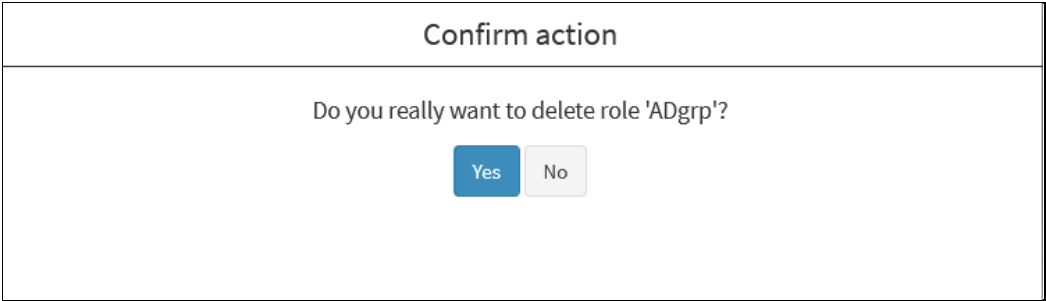


2. On the **All users** window in the right pane, perform the following steps for the deletion of the user:

- a. Click  icon and select **Delete** button to delete a **User**.



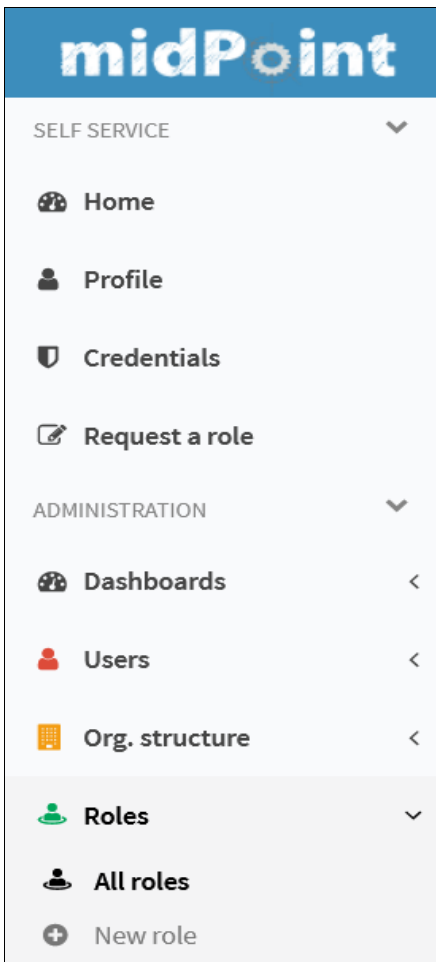
b. On the **Confirm action** window, click **Yes**.



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

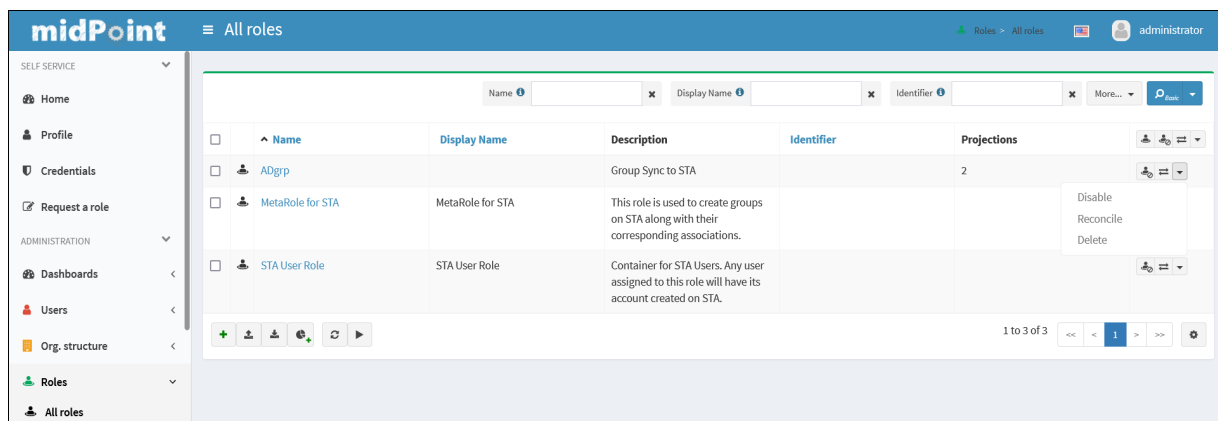
Groups

1. On the administrator console, in the left pane, click **Roles > All roles**.



2. On the **All roles** window in the right pane, perform the following steps for the deletion of the group:

- a. Click  icon, and select **Delete** button to delete **role (group)** in midPoint.



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

Confirm action
<p>Do you really want to delete role 'ADgrp'?</p> <p><input type="button" value="Yes"/> <input type="button" value="No"/></p>

NOTE: Now, you can verify that the group is deleted from midPoint, SafeNet Trusted Access and Active Directory

CHAPTER 7: Running the Solution

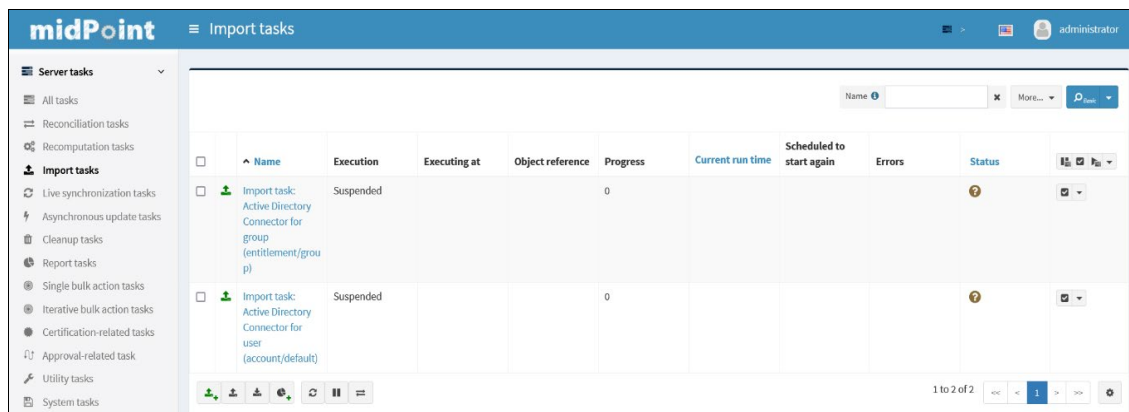
This chapter will guide you through the detailed steps on how to run the task created earlier for synchronization of users and groups to STA.

NOTE: You must always run **Group Import** task before the **User** Import task in order to sync the **Group memberships** to STA.

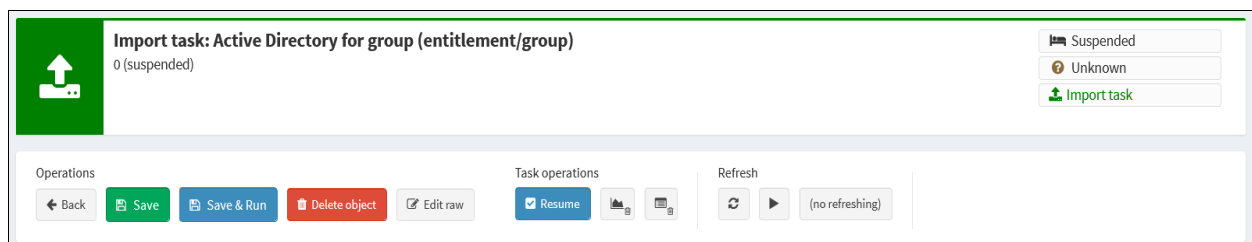
NOTE: Duplicate users and groups cannot be synced to STA using midpoint.

The following steps will guide you to run the task for importing **groups**:

1. On the Administrator console, in the left pane, scroll down and click **Server tasks > Import tasks** and In the **Import tasks** window, click on the task for groups that you have created earlier in the [Task Creation section](#).



2. Click **Save and Run** to execute the task.



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