

SafeNet Trusted Access IdM Connector

CONFIGURATION GUIDE



CONTENTS

CHAPTER 1: Overview	3
Features	3
Limitations	3
System Requirements	4
Prerequisites	4
CHAPTER 2: Generating an API Key	7
CHAPTER 3: Configuring SafeNet Trusted Access Connector in midPoint	8

CHAPTER 1: Overview

STA IdM Connector is developed using the **Connld framework** to develop, manage, and run along with the other identity connectors for bi-directional synchronization of users and groups with other target systems using SCIM, REST, LDAP, CSV, and other interfaces.

This document provides the ability to configure the STA IdM Connector for synchronization of users, as well as management of their associated user groups between **SafeNet Trusted Access (STA)** and other third-party applications and directories (for example, **Azure AD** and **Active Directory**, and so on), using **midPoint** (an open-source identity management and identity governance solution).

Bidirectional sync is in preview phase and can be available on requirement.

Features

Use Case	Supported ?	Notes
User Synchronization	YES	All CRUD (Create, Read, Update, and Delete) operations are supported.
Group Synchronization	YES	All CRUD (Create, Read, Update, and Delete) operations are supported.
User Password Synchronization	NO	
Live Synchronization	YES	Users only.
Paging Support	YES	

Limitations

Following are the limitations that will be encountered, when syncing to **STA IdM Connector** in midPoint:

- > If any group is associated to a provisioning rule in STA, then group update will fail.
- > Nested groups synchronization to STA are not supported.
- > If there are two groups with the same name in different domains, group creation will fail.
- > User's password sync to STA is not supported in this release.
- > All users from midPoint will be synchronized as STA internal users by default, Therefore, Alias #3 and Alias #4 fields will not be visible under STA users details. You can always map these user attribute as claim and

return attribute like other STA users, whereas, you can also sync users in STA as synchronized user, mentioned in schema handling section.

- > Live sync for Groups is not applicable.

System Requirements

Condition	Description
midPoint environment	midPoint version 4.4.3
Operating System	Ubuntu version 20.0.5
Database	PostgreSQL
Hardware Resources	<ul style="list-style-type: none">> 120 GB HDD> 8 Core CPU> 32 GB RAM
Scenario	Uni-directional sync to SafeNet Trusted Access

Prerequisites


As a prerequisite, perform the following steps:

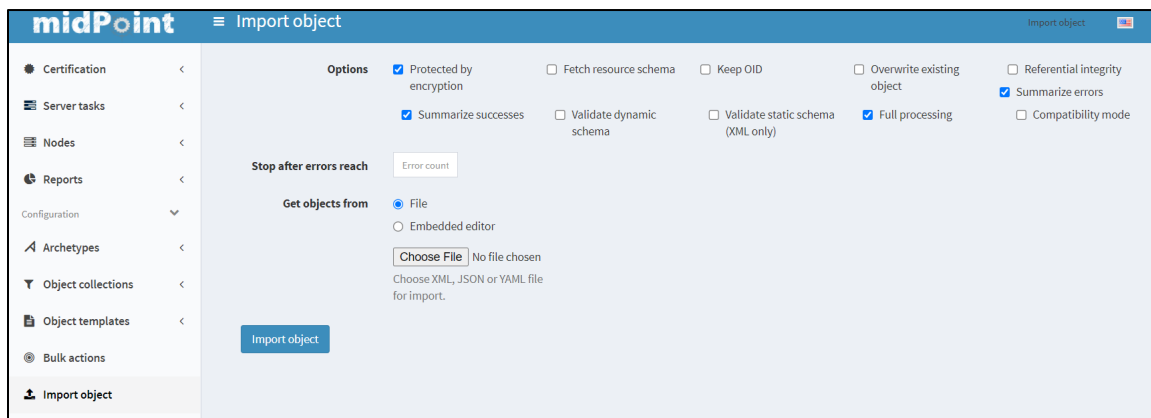
NOTE: Ensure that you have an instance of midPoint Identity Framework installed and running on the machine.

1. Download and deploy the **STA IdM Connector**.
 - a. Go to the URL <https://github.com/ThalesGroup/sta-idm-connector>
 - b. Download the **STA-IdM-connector-1.0.0.jar** available in the release section of the repository.
 - c. Copy the downloaded **STA-IdM-connector-1.0.0.jar** file and paste it in **midpoint-installation-directory/icf-connectors** directory.
 - d. **Schema Extension template:** Download the **Schema-Extension.xsd** file from https://github.com/ThalesGroup/sta-idm-connector/configuration_files and paste it under **midpoint-installation-directory/schema**.

NOTE: It helps you to add and display the STA IdP attributes, for example, UPN, Custom attribute and Alias, etc. in midPoint.

- e. Restart the midPoint server.
2. Import the **Resource Definition** and perform the following steps:

- Go to the URL https://github.com/ThalesGroup/sta-idm-connector/configuration_files/STA and download the **SafeNet_Trusted_Access.xml** file.
- In the left pane, under **Configuration**, click  to **Import Object**.
- In the right pane, in the **Options** field, select **Keep OID**.
- In the **Get Objects** from field, click **Choose File** to select the downloaded **SafeNet_Trusted_Access.xml** file.



Note: This file will let you add the pre-configured STA IdM Connector under midPoint resource. However, you can change the settings as per your preferred configuration.

- Click **Import object**.
- In the left pane, under **ADMINISTRATION**, click **Resources** to verify that the newly created resource, is added.

<input type="checkbox"/>	Name	Connector type	Version	
<input type="checkbox"/>	SafeNet trusted Access	com.connid.sta.connector.STARestConnector	1.0.0	

- Now, perform the following steps to add the STA SSL certificate in the midPoint keystore.

NOTE: Ensure that you download and save the below certificates in your local directory.

- Go to your STA login URL and click the **Lock** icon in the address bar to download the STA certificate.



- Navigate to `midpoint-installation-directory/var`, copy and paste the above downloaded STA certificate, and then execute below command in the terminal window.

```
keytool -keystore <your_keystore_file> -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 stacert -trustcacerts -<midpoint-installation-directory> /var/sta.crt >>
```

4. Download or generate the API key from the SafeNet Trusted Access (STA) Console.

NOTE: On the STA console, you can copy the required fields' values by clicking on the **Copy to Clipboard** icon () available next to the respective fields.

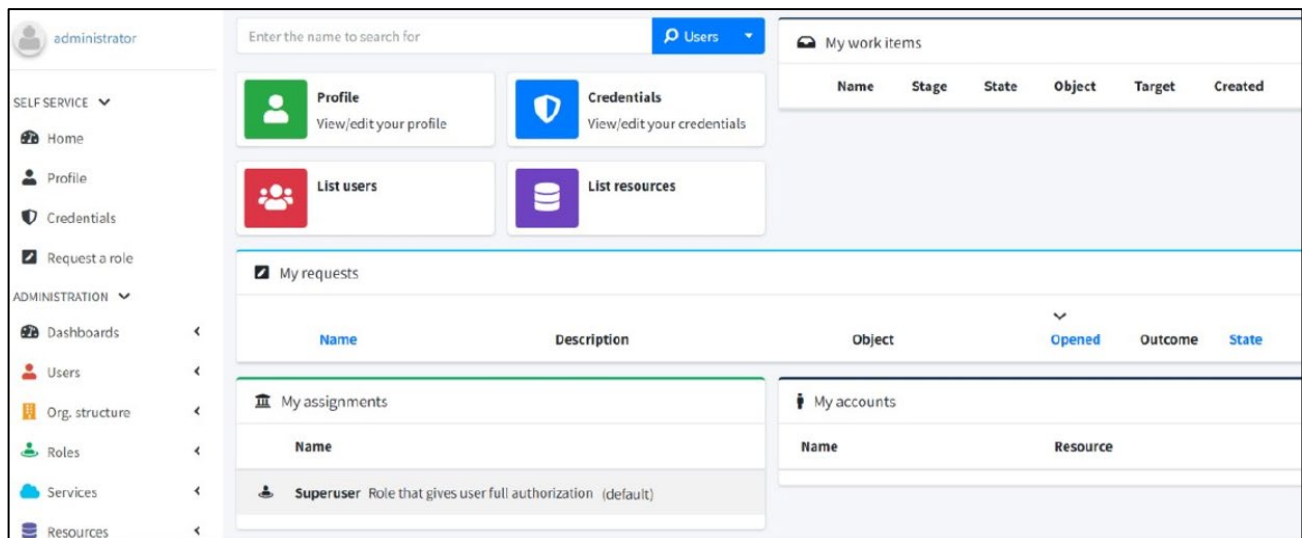
CHAPTER 2: Generating an API Key

You need to generate an API key before configuring SafeNet Trusted Access Connector in midPoint. Refer to [Generate an API key](#) section in STA documentation.

CHAPTER 3: Configuring SafeNet Trusted Access Connector in midPoint

Perform the following steps to configure the STA Connector in midPoint:

1. Log in to midPoint as an administrator.



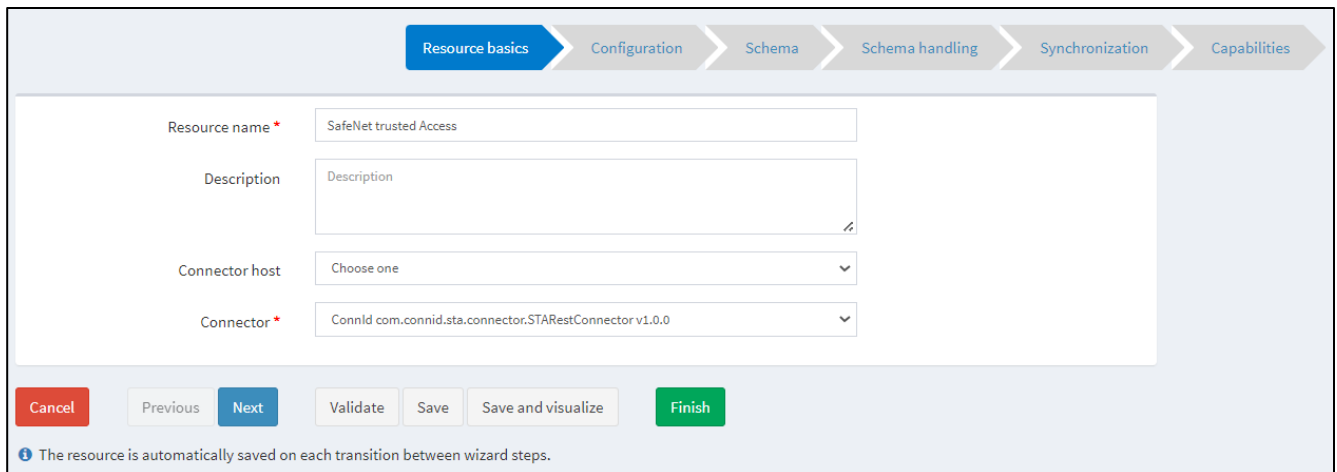
2. On the administrator console, in the left pane, click **Resources > All Resources**.
3. In the right pane, click **Edit using wizard**.

Configuring a STA Connector is a 5-step process.

STEP 1: In the **Resource basics** tab, you can modify the name of the resource and select the STA IdM Connector version.

Under **Resource Basics**, perform the following steps:

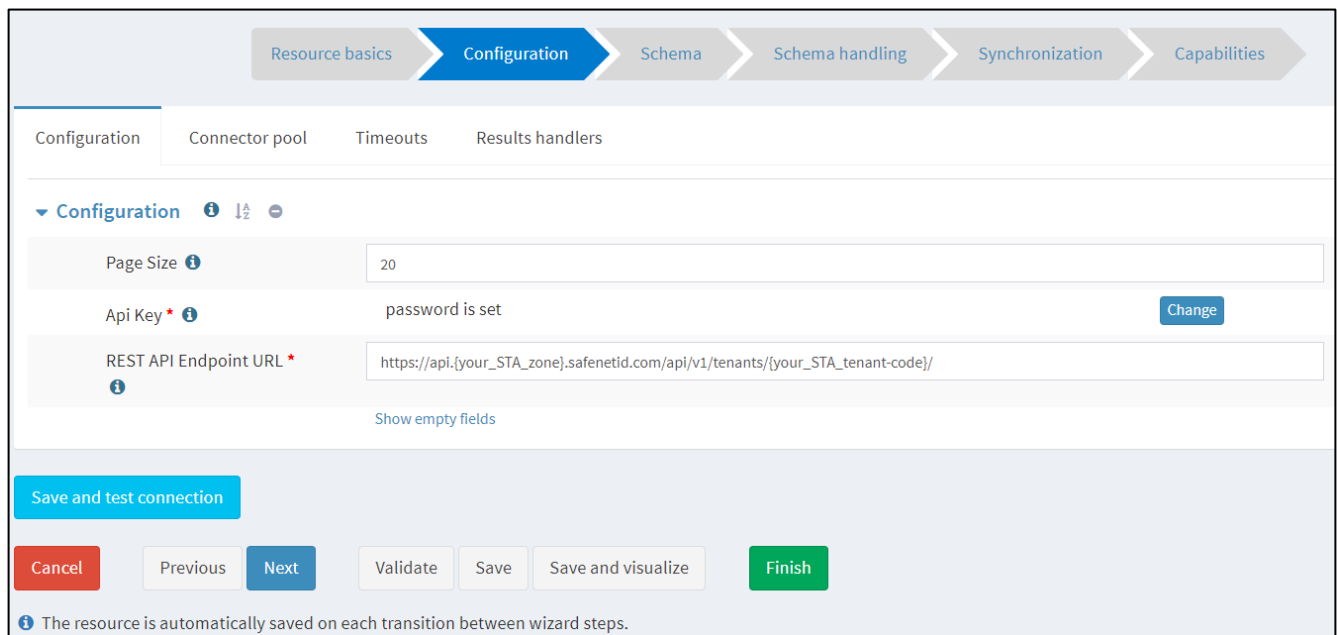
- a. In the **Resource name** field, modify the name of the resource as per your preference. This is for identification purpose only.
- b. [Optional] In the **Description** field, enter a **description of the connector**.
- c. In the **Connector** field, ensure that you select the **STA IdM Connector**.
- d. Click **Next**.



STEP 2: In the **Configuration** tab, you need to configure **STA Rest API endpoint** and its key to connect with the STA tenants.

Under **Configuration**, perform the following steps:

- In the **Page size** field [Optional], enter the **page size**.
- In the **API Key** field, click **Change** and then enter the API key that you downloaded earlier in [Generating an API Key](#) section.
- In the **Repeat Password** field enter the same API key again.
- In the **REST API Endpoint URL** field, enter the **REST API ENDPOINT URL** of STA API that you copied earlier in [Generating an API Key](#) section (for example, **`https://api.safenetid.com/api/v1/tenants/XXXX3`**).
- Click **Save and test connection**. Verify that all the configurations are done successfully and then click **OK**.
- Click **Next**.

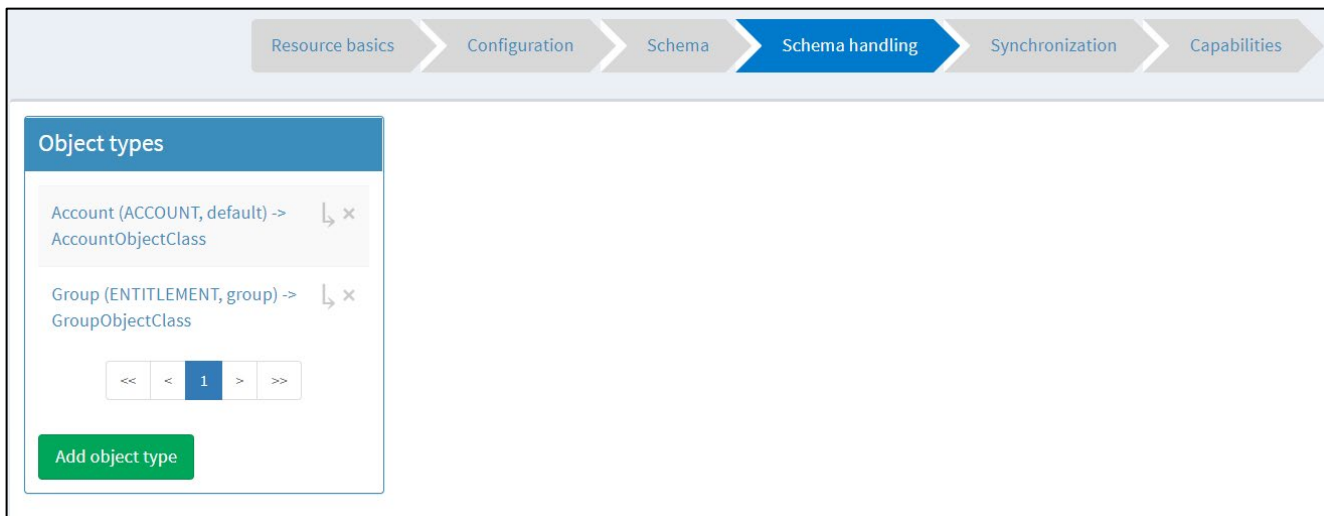


STEP 3: The **Schema** tab displays the STA users and groups schema attributes.

Under Schema, click **Next**.

STEP 4: In the **Schema handling** tab, you can configure STA attribute mapping or skip to proceed with the default mappings.

- a. Under **Schema handling**, under **Object types**, click **Account (ACCOUNT, default) -> AccountObjectClass**.



- b. In the **Account** window, in **Attributes**, you can find the outbound mapping for all the user attributes.

NOTE: The **Attributes** field contains the mapping of **isSynchronized** attribute. The default value for this attribute is false. The users in this case will be synced as STA internal users.

If you modify this mapping to true, then users in STA will be synced as Synchronized users. Thereafter, you cannot edit these users from the STA console.

Also, the **isSynchronized** attribute value can only be set once in the user life cycle.

Object types

Account (ACCOUNT, default) -> AccountObjectClass
Group (ENTITLEMENT, group) -> GroupObjectClass

<< < 1 > >>

Add object type

Account

Kind Account

Intent default

Display name Account

Description

Default ☒ Dependencies

Object class * AccountObjectClass

Attributes

ri: email out: emailAddress			
ri: firstName out: givenName			
ri: lastName out: familyName			
ri: userName out: name			
ri: address out: locality			
ri: city out: city			
ri: mobileNumber out: telephoneNumber			
ri: postalCode out: postalCode			
ri: state out: state			
ri: country out: country			
icfs: name out: name			
ri: userPrincipalName out: userPrincipalName			
ri: isSynchronized out:			

Associations

ri: STA Group (STA Group Membership)			
--------------------------------------	--	--	--

Iteration
Protected

Activation
Credentials

NOTE:

- > If any other schema attribute needs to be added in user details, then the attribute mapping must be done under **Attribute** section (as per your preferred configuration).
- > The above configuration shows the configuration steps for **Users**. It can also be configured for group synchronization by clicking on **Group Handling Object** option from left menu.

Steps to add or modify the attributes.

- Click to add or to edit an attribute (displayed against the attribute). In the **Edit attribute** window, perform the following steps:
- In the **Attribute field**, select an option from the dropdown (for example, userName).
- In the **Outbound field**, click icon (displayed against it) and in **Source**, click icon to enter the attribute name.

Edit attribute

Attribute *

Display name

Description

Limitations

Exclusive strong ☐ Tolerant ☒

Tolerant pattern

Intolerant pattern

Fetch Strategy

Matching rule

Outbound mappings

Inbound mappings

NOTE: You can also edit the above fields as per your preferred configuration.

STEP 5: The **Synchronization** tab contains the action to be taken by midPoint for different situation of Users and Groups.

Edit resource 'SafeNet Trusted Access'

Resource basics > Configuration > Schema > Schema handling > **Synchronization** > Capabilities

Synchronization objects

Account (ACCOUNT, default) => User

Group (ENTITLEMENT, group) => Role

<< < 1 > >>

4. Under **Synchronization**, click **Next**.
5. Click **Finish**.

SafeNet Trusted Access

Operations: Back, Save, Delete object, Edit raw

Resource operations: Test connection, Toggle maintenance, Refresh schema, Show using wizard, Edit using wizard

Resource is UP
STARestConnector
1.0.1.26-SNAPSHOT

Mappings
Source and Target
Synchronization defined

Schema
1 object types
2 schema definitions

Capabilities

Activation, Activation Lockout, Activation Status, Activation Validity, Credentials, Password, Live sync, Test Connection, Script, Auxiliary Object Classes, Create, Update, Add/Remove Values, Delete, Read, Count Objects, Paged Search, Run As

Kind	Object Class	Intent	Synchronization	Tasks
ACCOUNT	AccountObjectClass	default	true	

1 to 1 of 1

Copyright © 2023 Thales Group
All Rights Reserved.