



NetIQ® Identity Manager SCIM Driver Deployment Guide for SAP Cloud

January 2021

Legal Notice

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Copyright (C) 2020 NetIQ Corporation. All rights reserved.

Contents

About NetIQ Corporation	5
About This Guide	7
1 Deploying SCIM Driver For SAP Cloud	9
Prerequisites	9
Installing the SCIM Driver Files and Packages	10
Downloading the Driver Files	10
Installing the Driver Files	10
Installing the Driver Packages in Designer	11
Creating SCIM Driver Object for Connecting to SAP Cloud	11
Global Configuration Values (GCVs)	17
Configuring Entitlements for SCIM Driver	17
Supported SCIM Driver Use Cases for SAP Cloud	19
Mapping Attributes for SAP Cloud	20
Known Issue in SCIM Driver Implementation for SAP Cloud	21
Granting User Account Entitlement to a User Fails to Sync the User to SAP Cloud, if the User Already Exists and does not have a Login Name	21

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ♦ Identity & Access Governance
- ♦ Access Management
- ♦ Security Management
- ♦ Systems & Application Management
- ♦ Workload Management
- ♦ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About This Guide

This guide explains how to install and configure the SCIM driver to establish connectivity between Identity Manager and SAP Cloud.

Audience

This guide is intended for administrators implementing Identity Manager, application server developers, Web services administrators, and consultants. You should also have an understanding of DSML/SPML, SCIM, JSON, and HTML.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For more information about the library for Identity Manager, see the following resources:

- ♦ [Identity Manager documentation website \(https://www.netiq.com/documentation/identity-manager-48/\)](https://www.netiq.com/documentation/identity-manager-48/)
- ♦ [Identity Manager drivers documentation website \(https://www.netiq.com/documentation/identity-manager-48-drivers/\)](https://www.netiq.com/documentation/identity-manager-48-drivers/)

1 Deploying SCIM Driver For SAP Cloud

You can configure SCIM (System for Cross-domain Identity Management) driver with Identity Manager to connect to the SAP Cloud Platform (also referred as SAP Cloud in this document) complying to the SCIM protocols.

The SCIM Driver for SAP Cloud:

- ♦ helps to simplify user management operations using SCIM based protocols
- ♦ seamlessly provision and de-provision user identities
- ♦ provides entitlement support to modify and control the resource attributes

This guide explains the steps to install the SCIM Driver files, creating the driver object, and configure the Global Configuration Values (GCVs) and entitlements, which are pivotal procedures to configure the SCIM Driver to connect to SAP Cloud.

You must ensure to have all the required prerequisites and the driver files prior to setting up the driver. The procedures explained in the following sections help you achieve the same.

- ♦ [“Prerequisites” on page 1](#)
- ♦ [“Installing the SCIM Driver Files and Packages” on page 2](#)
- ♦ [“Creating SCIM Driver Object for Connecting to SAP Cloud” on page 3](#)
- ♦ [“Global Configuration Values \(GCVs\)” on page 9](#)
- ♦ [“Supported SCIM Driver Use Cases for SAP Cloud” on page 11](#)
- ♦ [“Mapping Attributes for SAP Cloud” on page 12](#)
- ♦ [“Known Issue in SCIM Driver Implementation for SAP Cloud” on page 13](#)

Prerequisites

1. You must obtain the User ID from SAP Cloud and set your password. These values will be used when you configure the driver using Basic authentication method using the Designer. The procedure to obtain the User ID and setting the password is shown below:
 - a. Login to [SAP Identity Authentication Service](#) portal with your credentials.
 - b. Navigate to **Users & Authorizations > Administrators > SAP Cockpit > Set Password**.
 - c. Copy and save the **User ID** value to a convenient location for future use.
 - d. Enter the **New Password** and **Re-enter New Password**.
 - e. Click **Save**.
2. You need to download and install the SCIM Driver set up files. For more information see, [“Installing the SCIM Driver Files and Packages” on page 2](#)
3. Update and install the required driver packages. For more information, see [“Installing the Driver Packages in Designer” on page 3](#)

Installing the SCIM Driver Files and Packages

To start with installing the driver, you must first download and install the driver files and packages. The following sections explain the procedures to install the driver files and packages.

Downloading the Driver Files

The SCIM Driver build files are available in the [Download Website](#). You can perform a search and download them into your computer.

Installing the Driver Files

You can install the SCIM driver files as a root user or as a non root user in your system. The procedure to install the driver files is similar for any connected application.

You must ensure that you have the required SCIM drivers files such as, **.zip**, **.rpm**, and **.jar** etc, handy to install the SCIM driver in your system.

The following files are required to install the driver:

- ♦ **.zip** file: `NIDm_Driver_SCIM.zip`
- ♦ **.rpm** file: `<netiq-DXMLscim.rpm>`
- ♦ **.jar** file: `<SCIMUtils.jar>`

The following section explains the procedure to install the driver files.

- 1 Download and unzip the contents of the **NIDm_Driver_SCIM.zip** file to a temporary location on your computer.
- 2 To install the driver files as a root user, for IDM 4.7.4 and above:
 - 2a On the server where you want apply the driver jar file, log in as root.
 - 2b Navigate to the extracted **NIDm_Driver_SCIM.zip** directory and perform one of the following actions based on your platform:
 - ♦ **Linux:** Install the new **netiq-DXMLscim.rpm** in your driver installation directory by running the following command in a terminal window:
 - ♦ If you are installing the binary, run the command: `rpm -Ivh (binaries-path)/netiq-DXMLscim.rpm`
 - ♦ **Windows:** Copy the **SCIMShim.jar** file to the driver's installation folder. For example, `\NetIQ\IdentityManager\NDS` (local installation) or `\Novell\RemoteLoader\64bit` (remote installation).
- 3 (Conditional) To update the driver files as a non-root user:
 - 3a Verify that the `/rpm` directory exists and contains the `_db.*` file.

The `_db.*` file is created during a non-root installation of the Identity Manager engine. The absence of this file indicates that the Identity Manager is not installed properly. In such a case, reinstall the Identity Manager to correctly place the file in the mentioned directory.
 - 3b To set the root directory to the location of non-root Identity Vault, enter the following command in the command prompt:
`ROOTDIR=<non-root eDirectory location>`

This command sets the environmental variables to the directory to the location where the Identity Vault is installed as a non-root user.

3c To install the driver files, enter the following command:

For example, to install the SCIM driver rpm, use this command:

```
rpm --dbpath $ROOTDIR/rpm -Ivh --relocate=/usr=$ROOTDIR/opt/novell/  
eDirectory --relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/  
eDirectory=$ROOTDIR/opt/novell/eDirectory --relocate=/opt/novell/  
dirxml=$ROOTDIR/opt/novell/dirxml --relocate=/var=$ROOTDIR/var --  
badreloc --nodeps --replacefiles /home/user/netiq-DXMLscim.rpm
```

NOTE: In the above command `/opt/novell/eDirectory` is the location where non-root Identity Vault is installed, and `/home/user/` is the home directory of the non-root user.

- 4 (Conditional) If the driver is running locally, start the Identity Vault and the driver instance.
- 5 (Conditional) If the driver is running with a Remote Loader instance, start the Remote Loader instance and the driver instance.

Extending the eDirectory (Identity Vault) Schema

You can upload new attributes through the Identity Vault to extend the SCIM schema.

- 1 Copy the following schema file to the system where Identity Manager is installed.

For example:

```
/root/schema/scim-schema.sch
```

- 2 Run the following `ndssch` command.

```
ndssch [-h hostname[:port]] [-t tree_name] [-d] admin_FDN schemafilename  
[schema_description]
```

For example:

```
ndssch -h 10.71.131.123:524 -t SLES12SP3_Quality_131123_TREE -d  
admin.sa.system /root/schema/scim-schema.sch scim-Group
```

- 3 The log file is created in the default location, i.e `/root/schema.log` for troubleshooting.

NOTE: You must reload the Identity Console session for the schema changes to take effect.

Installing the Driver Packages in Designer

You must install the SCIM Base, SCIM Default and the SAP Cloud configuration packages mandatorily.

For more information on the SCIM driver packages that are available in the Designer, see [SCIM Driver Packages](#) in “*NetIQ SCIM Driver Implementation Guide*”.

Creating SCIM Driver Object for Connecting to SAP Cloud

To begin with the configuration, you need to set up the SCIM driver object in the Designer, and configure certain parameters to connect to SAP Cloud.

The procedure to set up the SCIM driver in Designer is similar for any connected application. The generic steps to set up a driver object in Designer is shown from step 1 to step 20. If you are familiar with the generic driver object set up, you can choose to skip [Step 17 on page 4](#) to continue with the configuration parameters specific to SAP Cloud.

- 1 Open Designer.
- 2 In the toolbar, click **Help > Check for Package Updates**.
- 3 Select the required package as shown in “[Installing the Driver Packages in Designer](#)” on page 3 to download and click **OK**. The Designer is updated with the selected packages.
- 4 In **Designer > Outline** view, open your project.
- 5 Right click project > **New > Identity Vault**, or drag and drop Identity Vault from the Palette to Modeler window.
- 6 In the **Add Server Association** screen, select the following field values and click **OK**.
 - ◆ Server DN
 - ◆ Identity Manager Version
 - ◆ Identity Manager EditionThe Identity Vault Credentials window appears.
- 7 In Identity Vault Credentials window, enter:

Field	Description
Host	The identity vault hosting machine's IP address
Username	The name of the user, for example, Admin, if the user is an administrator.
Password	The password of the user to login to the identity vault

- 8 Select **Save Password**, if you want to save your password for easy logins in the future.
- 9 Click **OK**.

The Identity Vault with the Driver Set appears in the **Modeler** window.
- 10 In the right pane, drag and drop the **SCIM** driver icon from **Palette > Tool** tab to the **Modeler** window.
- 11 In the **Driver Configuration Wizard**, select **SCIM Base** (Contains the base functionality for a driver. You must install a driver base configuration package first).

NOTE: You can only select one base package.

- 12 Click **Next**.
- 13 In the **Select Mandatory Features** page, select the **SCIM Default Package**, and click **Next**.
- 14 In the **Select Optional Features** page, select the **SCIM SAPCloud Configuration Package**, and if required select **SCIM JSON Package**, and click **Next**.

IMPORTANT: Though the **SCIM SAPCloud Configuration Package** appears in the **Select Optional Features** page, to configure the SCIM driver for SAP Cloud you must select this package mandatorily.

- 15 Verify if the required **Important Note** items are met, and click **Next**.
- 16 On the **Driver Information** page, specify a name for the driver, then click **Next**. The **Connection Parameters** page appears.
- 17 Select **Basic** in the **Authentication Method** field.


IMPORTANT: The SCIM driver for SAP Cloud is currently certified with Basic authentication only.

- 18 Enter the following fields as shown in the table below:

Field	Sample Values
Authentication Method	Select Basic .
User Name: Specify the User ID obtained from SAP Cloud. The procedure to obtain the User ID is explained in "Prerequisites" on page 1.	<be1a0804-7e91-46a1-be48-8a728fb60ef8>
Password: Specify the password in the Enter Password and Re-enter Password fields that you have set in SAP Cloud. The procedure to set the password is explained in "Prerequisites" on page 1.	<user defined password set in SAP Cloud>

Field	Sample Values
Application Login URL: The login URL of SAP Cloud.	<code><https://tenant_name.accounts.ondemand.com/admin/></code>
Header Fields: Click the  icon to create the header fields. Enter the required header fields and supported values for the selected authentication method.	<ul style="list-style-type: none"> ◆ Name: Content-Type ◆ Value: application/scim+json
Application Truststore File: The path and the name of the keystore file that contains the trusted certificates for the remote server to achieve SSL handshake. The trusted DigiCert CA certificate must be imported from the SAP Cloud portal.	<code></root/scim_configuration/trustSapCloud/SapCloud></code>
Import the keystore file by running the following command: <code>keytool -import -file <name_of_cert_file> -trustcacerts -noprompt -keystore <filename> -storepass <password></code>	
Mutual Authentication: Enable and specify this field, if the authentication is supported by the connected application. You must ensure to have both the server certificates stored in Identity Manager and the connected application.	Mutual Authentication is not mandatory for SAP Cloud.
Proxy Authentication: Defaults to Hide . Select Show if you want to set proxy authentication parameters. Specify the host address and the host port when a proxy host and port are used.	<ul style="list-style-type: none"> ◆ Proxy host name and port: <code><192.168.0.0:port></code>. Choose an unused port number on the proxy server. ◆ Username: <code><user name for proxy authentication></code> ◆ Enter Password: <code><password for proxy authentication></code> ◆ Re-enter Password: <code><password for proxy authentication></code>
HTTPS Connection Timeout: Specify the HTTP connection time out value.	The timeout value must be greater than 0. NOTE: The driver waits for the time specified (in minutes) and terminates the HTTPS connection displaying the error codes that are configured in the Subscriber Options > HTTPS error codes for retry field.
SCIM 2.0 URL: Enter the URL for the SCIM Application. SCIM Resources like User, Group etc. will be appended to this URL.	<code><https://<tenant ID>.accounts.ondemand.com/service/scim/></code>

19 In the **Install SCIM Base** page, specify the **Subscriber Options** and **Publisher Options**, and click **Next**.

Field	Description and Sample Values
Subscriber Options	<p>HTTPS error codes for retry: Specify the HTTPS errors that must return a retry status. Error codes must be a list of integers separated by spaces. For example: <307 408 503 504></p> <p>NOTE: The operation will be retried if these errors are encountered.</p>
Publisher Options	<ul style="list-style-type: none"> ◆ Enable Publisher Channel: Select Yes to enable the Publisher channel. ◆ Polling interval in minutes: The time interval to poll resources from SAP Cloud. Specify the polling interval in minutes. For example: <10> ◆ Heartbeat interval in minutes: This option is used to configure the driver shim to send a periodic status message on the Publisher channel. By default, this is set to 10 minutes. <p>IMPORTANT: Polling Resource Options: This field does not appear when you are setting up the driver for the first time. These fields appear after configuring the driver in Designer. Once the driver is configured, double click the connector line in the modeler window and navigate to Driver Configuration > Publisher Options tab.</p> <ul style="list-style-type: none"> ◆ Select the Configured Resources option to poll on all resources that are configured as part of the schema settings. ◆ Select the Custom Resources option and click  to configure customized polling Resource ID and Resource URL. <ul style="list-style-type: none"> ◆ For User: <ul style="list-style-type: none"> ◆ Resource ID: Specify the schema's Uniform Resource Name (URN) of the user. Example, <code>urn:ietf:params:scim:schemas:core:2.0:User</code> ◆ Resource URL: Specify the schema's Uniform Resource Locator (URL) of the user. Example, <code>https://<tenant ID>.accounts.ondemand.com/service/scim/Users?startIndex=1&count=100</code> <p>NOTE: In the above URL's, the <code>startIndex</code> refers to the resource from where the poll must start and <code>count</code> refers to the number of resources from the <code>startIndex</code> for polling.</p> ◆ For Group: <ul style="list-style-type: none"> ◆ Resource ID: Specify the schema's Uniform Resource Name (URN) of the group. Example, <code>urn:ietf:params:scim:schemas:core:2.0:Group</code> ◆ Resource URL: Specify the schema's Uniform Resource Locator (URL) of the group. Example, <code>https://<tenant ID>.accounts.ondemand.com/service/scim/Groups?startIndex=1&count=100</code>

20 In the **Schema Settings** page, enter the values as shown in the following table:

Table 1-1 Schema Settings

Field	Description with Sample Values
Refresh Schema on Driver Startup	Specify Yes , to refresh the schema. IMPORTANT: You must select Yes only for the first time to load the application schema or if the application schema has changed. It is recommended to change it to No after you load the application schema.
Schema Options	Select SCIM 2.0 . <ul style="list-style-type: none"> ♦ SCIM 2.0: SCIM 2.0 Schema for User and Group, as defined in RFC7643.
Resource Type	Specify the Resource ID and the Resource EndPoint for resources like Users, Groups, Roles, Entitlements etc. in Uniform Resource Name (URN) Format. <ul style="list-style-type: none"> ♦ Resource ID: The schema’s Uniform Resource Name (URN) of the user. For example, <code>urn:ietf:params:scim:schemas:core:2.0:Users</code> ♦ Resource Endpoint: Specify the resource endpoint of the Resource ID. For example, <code>Users</code>. ♦ Modify Method Operation: This option is used to make partial updates to the resources in SAP Cloud. Select PUT. <p>Similarly for Groups:</p> <ul style="list-style-type: none"> ♦ Resource ID: Specify the schema’s Uniform Resource Name (URN) of the group. For example, <code>urn:ietf:params:scim:schemas:core:2.0:Group</code> ♦ Resource Endpoint: <code>Groups</code> ♦ Modify Method Operation: Select PUT.

Table 1-2 Modifier Settings

Field	Description with Sample Values
Custom Java Class	Not Applicable for SAP Cloud.
Document Handling	Not Applicable for SAP Cloud.

- 21 Review the summary of tasks that will be completed to create the driver, then click **Finish**. The configured driver appears in the Designer screen.

Global Configuration Values (GCVs)

After configuring the SCIM driver, you can set the Global Configuration Values (GCVs) as required. These settings must be configured properly for the driver to start and function correctly.

The SCIM driver for SAP Cloud includes predefined GCVs as shown below:

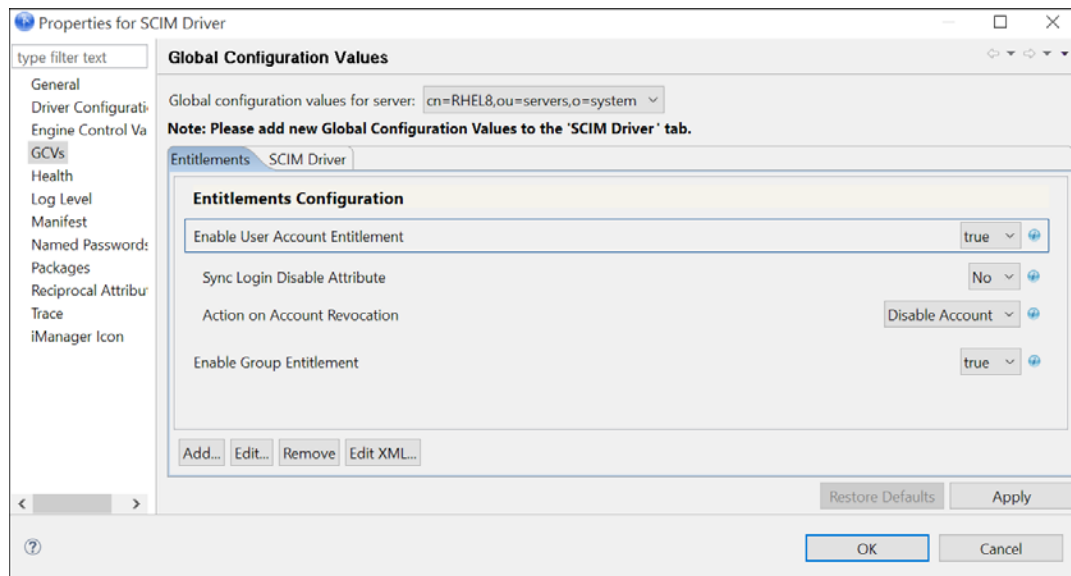
- ♦ **Validate Resource with Required Attributes:** This field validates resources and the required attributes that are available in the schema. Select as **false**.
- ♦ **Connecting to SAP Cloud:** Set this to **true** if you are connecting to SAP Cloud. Defaults to **false**.
- ♦ **Connected Application's Name:** Enter the name of the connected application, such as SAP Cloud. This default name appears in the entitlements. For example, `Account for scim system: SAP Cloud`.
- ♦ **SCIM 2.0 URL:** Auto-populates the **SCIM 2.0 URL** value as provided while creating the driver object.

For more information on GCVs, see [When and How to Use Global Configuration Values](#) in “*NetIQ Identity Manager Driver Administration Guide*”.

Configuring Entitlements for SCIM Driver

You can configure the driver with entitlements enabled or disabled. To configure entitlements, perform the following steps:

- 1 In the modeler window, right-click the driver icon or the driver line, then select **Properties**.
- 2 Click **GCVs > Entitlements** and review the **Entitlement Configuration** settings:



NOTE: These settings are only displayed if you have installed the **SCIM Entitlements** package. The entitlements are supported based on the connected application’s capabilities.

- ◆ **Enable User Account Entitlement:** This field enables the driver to manage user account permissions using the User Account entitlement. Ensure that the value of this parameter is set to **true**. By default, the value is set to **False**. Specify the values as shown in the following table to set User Account Entitlements.

Field	Description/Value
Sync Login Disabled attribute	<p>This field is used to control the Login Disabled attribute for a particular user:</p> <p>Select:</p> <ul style="list-style-type: none"> ◆ Yes, to sync the changes made to the Login Disabled attribute in the Identity Manager, to SAP Cloud. ◆ No, to restricts syncing the changes of Login Disabled attribute in the Identity Manager to SAP Cloud.
Action on Account Revocation	<p>Select the action to be performed in SAP Cloud when the user account entitlement is revoked.</p> <p>The available options are:</p> <ul style="list-style-type: none"> ◆ Disable Account ◆ Delete Account

- ◆ **Enable Group Entitlement:** This option enables the driver to manage group memberships using the Group entitlement. Ensure that the value of this parameter is set to **true**. By default, the value is set to **false**.

IMPORTANT: If the values for **Enable User Account Entitlement** and **Enable Group Entitlement** parameter is set to **False**, the user and group membership synchronization will be managed using the non-entitlement configuration method.

- 3 Click **Apply**.
- 4 Click **OK** when finished.

Supported SCIM Driver Use Cases for SAP Cloud

The following operations can be performed on the subscriber channel:

◆ Operations performed on a user

- ◆ **Adding a user:** A user is added in Identity Manager and synced to SAP Cloud through the SCIM driver. The details of the user such as, user's first name, last name, contact details, email ID, location, department, user name, initial login password are added and synchronized to the SAP Cloud.

The SCIM end point for SAP Cloud to add a user: `https://<tenant ID>.accounts.ondemand.com/service/scim/Users`

Method: POST

- ◆ **Modifying a user:** If there are any changes made to the user details such as, user's first name, last name, contact details, email ID etc, they will be synchronized with SAP Cloud.

The SCIM end point for SAP Cloud to modify a user: `https://<tenant ID>.accounts.ondemand.com/service/scim/Users/<sapcloud-userid>`

Method: PUT

NOTE: The user can be disabled in case of separation or termination of their services.

- ◆ **Migrate a user:** You can migrate an individual or multiple users from Identity Manager to SAP Cloud and vice-versa.
- ◆ **Polling a user:** You can poll a user from SAP Cloud to Identity Manager.

The SCIM end point for SAP Cloud to poll users: `https://<tenant ID>.accounts.ondemand.com/service/scim/Users`

Method: GET

- ◆ **Query a User:** You can query the synced attributes of resource such as user from SAP Cloud through Identity Console. Also, you can query through `dxcmd` utility to fetch required resources or attributes using specific conditions.

The SCIM end point for SAP Cloud to query users: `https://<tenant ID>.accounts.ondemand.com/service/scim/Users/<sapcloud-userid>`

Method: GET

NOTE: Complex JSON attributes cannot be queried from SCIM compliant applications through `dxcmd` utility.

◆ Operations performed on public groups

- ◆ **Adding a group:** A group is added in Identity Manager to manage multiple users with same set of access permissions, rather than managing them individually.

The SCIM end point for SAP Cloud to add a group: `https://<tenant ID>.accounts.ondemand.com/service/scim/Groups`

Method: POST

- ◆ **Modifying a group**

- ◆ **Adding member to a group:** A member is added to a group based on the user's role, department and access permissions that the user qualifies for, so that the access permissions for that designated user role are provisioned accordingly.

The SCIM end point for SAP Cloud to add a member to a group: `https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<sapcloud-groupid>`

Method: POST

- ◆ **Removing member from a group:** A user can be removed from a group if the user's role or designation, or access permissions provided do not qualify a user to belong to that group. This happens in case of a role or designation change of the user, or separation or termination of the user.

The SCIM end point for SAP Cloud to remove a member from a group: `https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<sapcloud-groupid>`

Method: POST

- ◆ **Deleting a group:** Duplicate groups, redundant groups, empty groups or groups that are not required can be deleted, and the group members will be moved to another group as required.

The SCIM end point for SAP Cloud to delete a group: `https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<sapcloud-groupid>`

Method: DELETE

- ◆ **Migrate a Group:** You can migrate an individual or multiple groups from Identity Manager to the SAP Cloud and vice-versa.
- ◆ **Polling a Group:** You can poll all created groups from SAP Cloud to Identity Manager.

Method: GET

The SCIM end point for SAP Cloud to poll groups: `https://<tenant ID>.accounts.ondemand.com/service/scim/Groups`

- ◆ **Query a Group:** You can query the synced attributes of groups from SAP Cloud. Also, you can query through `dxcmd` utility to fetch required resources or attributes using specific conditions.

The SCIM end point for SAP Cloud to query groups: `https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<sapcloud-userid>`

Method: GET

NOTE: Complex JSON attributes cannot be queried from SCIM compliant applications through `dxcmd` utility.

Mapping Attributes for SAP Cloud

The attributes of Identity Manager and SAP Cloud must be mapped as per the schema mapping.

IMPORTANT: You must ensure to change the Identity Manager Attribute `Internet Email Address` to the SCIM attribute `emails:value`, as SAP Cloud does not support email types.

For all the default attributes that are available as a part of SCIM Driver implementation for connected applications, see [Mapping Attributes for Identity Manager and Connected Application](#) in the [NetIQ SCIM Driver Implementation Guide](#).

After the schema is fetched from the SAP Cloud, the attributes of Identity Manager and SAP Cloud are mapped in the back end by default. If any changes are required, you can modify the attributes as needed.

Known Issue in SCIM Driver Implementation for SAP Cloud

This sections explains the known issue that is associated when implementing the SCIM Driver for SAP Cloud.

Granting User Account Entitlement to a User Fails to Sync the User to SAP Cloud, if the User Already Exists and does not have a Login Name

Cause: This occurs because the Matching Policy fails to find the user in SAP Cloud, as the search is done based on the Login Name. If the account in SAP Cloud does not have a login name, the policy tries to create a new object and the sync fails as the user already exists.

The following error is displayed:

```
DirXML Log Event -----
Driver:    \RHEL8_TREE\system\driverset1\SCIM SAP Driver
Channel:   Subscriber
Object:    \RHEL8_TREE\data\users\abcd
Status:    Error
Message:
com.microfocus.nds.dirxml.driver.scim.exceptions.ChannelException: User
profile with email [abcd@xyz.lab] already exists
```

Workaround: You must update the User Account in SAP Cloud with a valid Login Name.

