

Reference document for Integration Guide for SCIM with Azure Entra

[Integration Guide: SCIM and Azure AD Integration](#)

[Objective](#)

[Overview](#)

[Supported endpoints for the SCIM API:](#)

[How to integrate Azure AD to Compliance.ai SCIM API](#)

[Obtaining the Access Token](#)

[Setup Admin Credentials](#)

[Configure Mapping](#)

[Attribute Mapping](#)

[Supported Roles](#)

[Adding Users](#)

[Provision on demand](#)

[FAQ](#)

- [1. To confirm if a user is created on the Compliance.ai application, follow these steps:](#)
- [2. Why does the Testing connection to Compliance.ai fail?](#)
- [3. Why is the user provisioning update not working?](#)

Integration Guide: SCIM and Azure AD Integration

Compliance.ai offers the SCIM API, or System for Cross-domain Identity Management, facilitating automated user provisioning within the Compliance.ai application.

Through the Compliance.ai SCIM API, customers can streamline user provisioning to the Compliance.ai platform by seamlessly integrating it with their existing Identity Provider (IdP) systems. The API aligns with the SCIM standard, providing RESTful APIs tailored to automate user provisioning processes across various systems.



Objective

The objective of this reference document is to provide guidance on integrating Compliance.ai's SCIM API with Azure Active Directory (Azure AD). This document aims to empower users with the knowledge and steps required to integrate the two systems, enabling efficient user provisioning within Compliance.ai's platform via Azure AD.

Overview

The Integration Guide: SCIM and Azure AD Integration serves as a resource for users seeking to integrate Compliance.ai's SCIM API with Azure AD. This guide provides step-by-step instructions and best practices for setting up the integration, configuring attribute mappings, managing user roles, and addressing common challenges.

Supported endpoints for the SCIM API:

The SCIM API provides support for several endpoints, including the following:

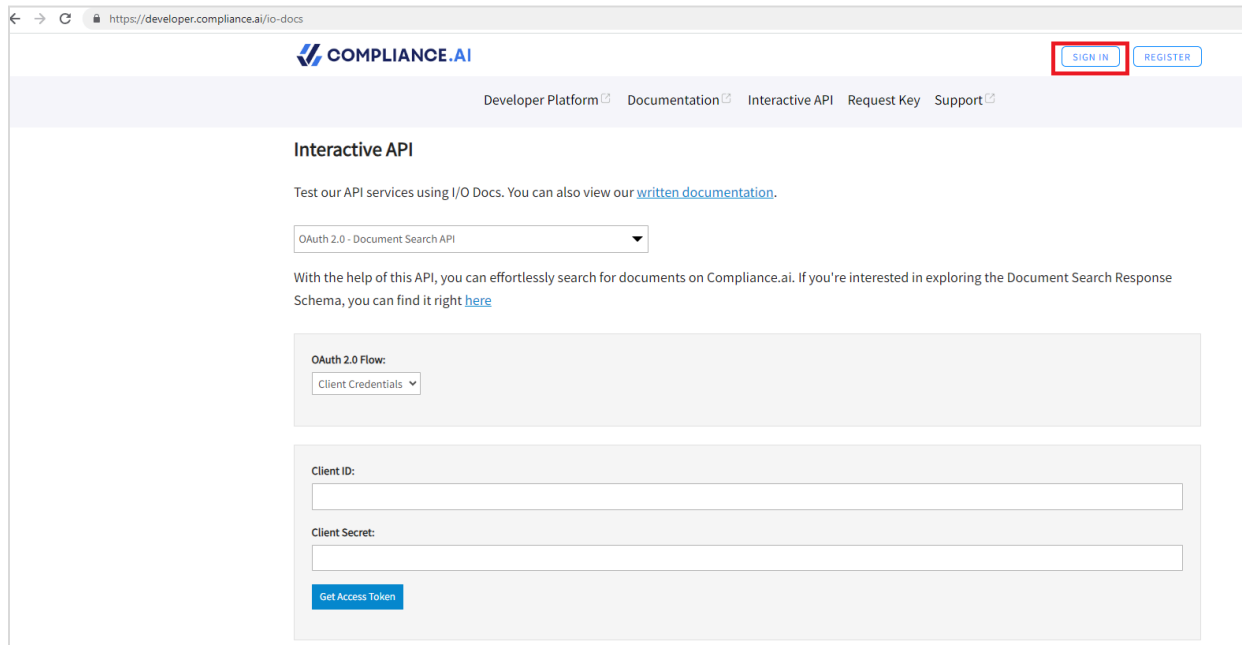
1. **/Users:** This endpoint enables the management of user accounts. It supports creating new user accounts, retrieving user account information, and modifying user account attributes.
2. **/ServiceProviderConfig:** This endpoint provides information about the Compliance.ai service provider. It includes details about supported authentication schemes and endpoint URLs.
3. **/ResourceTypes:** This endpoint provides information about the types of resources supported by the Compliance.ai SCIM API, specifically user accounts.
4. **/Schemas:** This endpoint provides information about the schema for user accounts. It includes details about the attributes that can be modified and any constraints.

How to integrate [Azure AD](#) to Compliance.ai SCIM API

Obtaining the Access Token

To set up Compliance.ai SCIM on Azure, external users require an access token. Follow the steps below to acquire it:

1. Login to <https://developer.compliance.ai/io-docs>



The screenshot shows the 'Interactive API' page on the Compliance.ai Developer Platform. The page has a navigation bar with links for 'Developer Platform', 'Documentation', 'Interactive API', 'Request Key', and 'Support'. The 'SIGN IN' button is highlighted with a red box. The main content area is titled 'Interactive API' and includes a dropdown menu for API services, currently set to 'OAuth 2.0 - Document Search API'. Below this, there is a section for 'OAuth 2.0 Flow' with a dropdown for 'Client Credentials'. Further down, there are input fields for 'Client ID' and 'Client Secret', and a 'Get Access Token' button.

2. Navigate to the menu and select "Interactive API."
3. In the API services dropdown, choose "SCIM."
4. From the Existing Client Credentials dropdown, select the application utilizing the SCIM API.
5. Retrieve the Client ID and Secret.
6. Proceed to obtain the Access Token.
7. Copy the access token for further use.

Interactive API

Test our API services using I/O Docs. You can also view our [written documentation](#).

OAuth 2.0 Flow:

Existing Client Credentials:

Client ID:

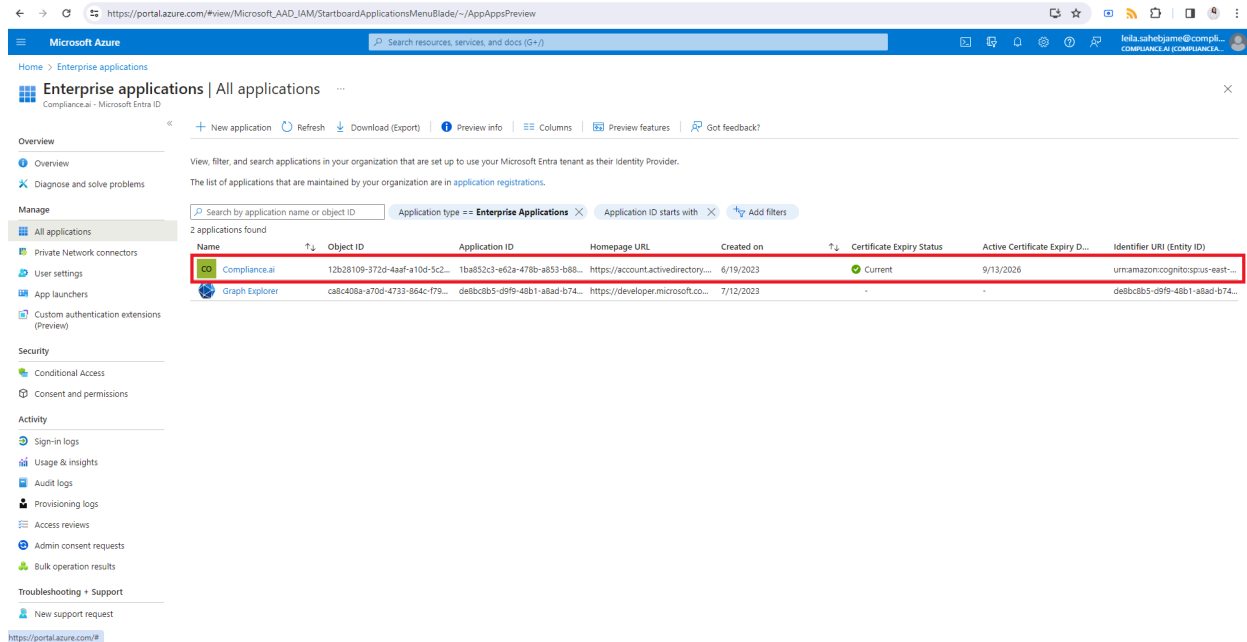
Client Secret:

Access Token:

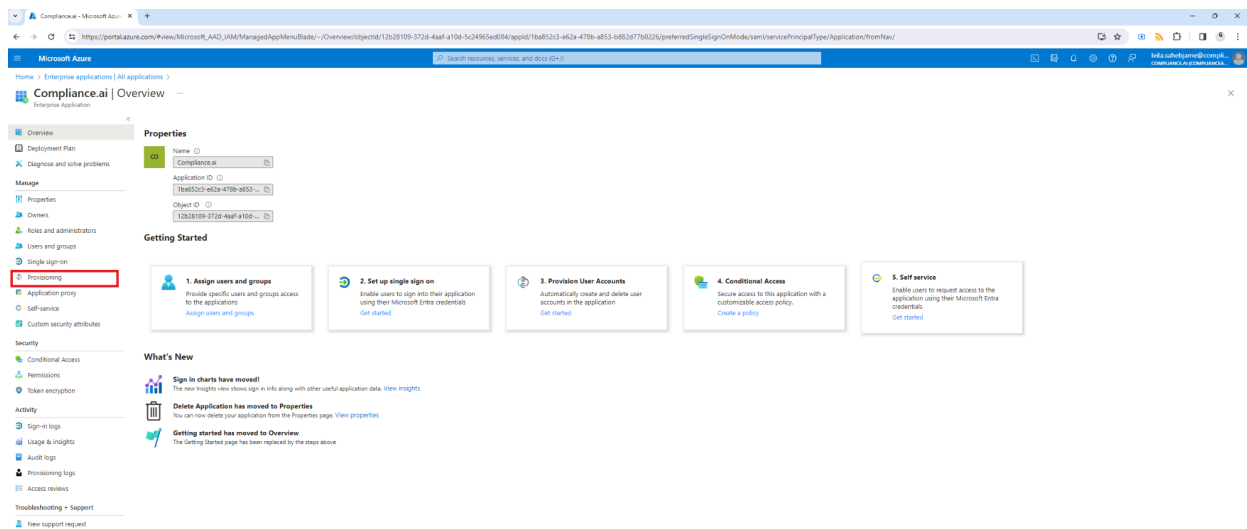
Setup Admin Credentials

Once you have registered the Compliance.ai application on Azure AD, please see [here](#) for more info, follow these steps to set up admin credentials for connecting to the Compliance.ai SCIM API:

1. Go to the Azure Portal.
2. Navigate to "Enterprise Applications | All applications" and select the Compliance.ai App Application.



3. Once in "Compliance.ai Overview" from the sidebar, under the "Manage" section, choose "Provisioning."



4. Select "Automatic" for Provisioning Mode.
5. Add the exact URL "<https://api.compliance.ai/scim/>" in the Tenant URL field.
6. **IMPORTANT:** Apply the hotfix provided by Microsoft at this point. Please refer to the following link for detailed instructions: [Microsoft Hotfix](#)
7. Paste your Access Token for the Secret Token (obtained from the previous step).
8. Test the connection to ensure it returns a successful result.

Home > Enterprise applications | All applications > Compliance.ai | Provisioning > Compliance.ai | Overview >

Provisioning

Save Discard

Provisioning Mode
Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Compliance.ai based on user and group assignment.

Admin Credentials

Admin Credentials
Azure AD needs the following information to connect to Compliance.ai's API and synchronize user data.

Tenant URL

Secret Token

Test Connection

Mappings

Settings

Provisioning Status On Off

Testing connection to Compliance.ai
The supplied credentials are authorized to enable provisioning

Configure Mapping

1. We support the mapping of Users, but Group Mapping is currently unavailable.
2. Start by adding one active user under "Users" to disable Group Mapping.
3. Once the user is added, disable Group Mapping by clicking on "Provision Azure Active Directory Groups."
4. Enable the Provisioning Status to finalize the configuration.

[Home](#) > [Compliance.ai | Overview](#) >

Provisioning

Save Discard

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Compliance.ai based on user and group assignment.

Admin Credentials

Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

| Name | Enabled |
|---|---------|
| Provision Azure Active Directory Groups | No |
| Provision Azure Active Directory Users | Yes |

Restore default mappings

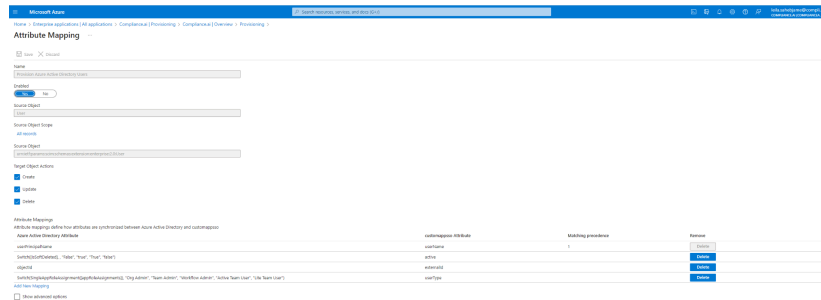
Attribute Mapping

To map Azure user attributes to Compliance.ai attributes:

1. Click on "Provision Azure Active Directory Users."
2. Set the attribute mappings according to the table below.
3. Compliance.ai supports the following user attribute mappings: Users (Create).
4. Click on "Add New Mapping."
5. Add the mappings one by one as described in the table below.
6. Click "Ok" and then "Save" to save the mappings.

Please ensure that the attribute mappings are accurately set to ensure seamless integration between Azure AD and Compliance.ai.

| Azure Active Directory Attribute | customappsso Attribute |
|--|------------------------|
| userPrincipalName | userName |
| Switch([IsSoftDeleted]), "False", "true", "True", "false") | active |
| objectId | externalId |
| Switch(SingleAppRoleAssignment([appRoleAssignments]), "Lite Team User", "Admin", "Org Admin", "Team Admin", "Active Team User", "Lite Team User", "Lite Team User") Note: Lite Team User is the default role when no role is assigned "Admin", "Org Admin" - Admin role in Azure is mapped to Org Admin "Team Admin", "Active Team User" - Team Admin role in Azure is mapped to Active Team User "Lite Team User", "Lite Team User" - Lite Team User role in Azure is mapped to Lite Team User | userType |



Supported Roles

Currently, we support the following roles:

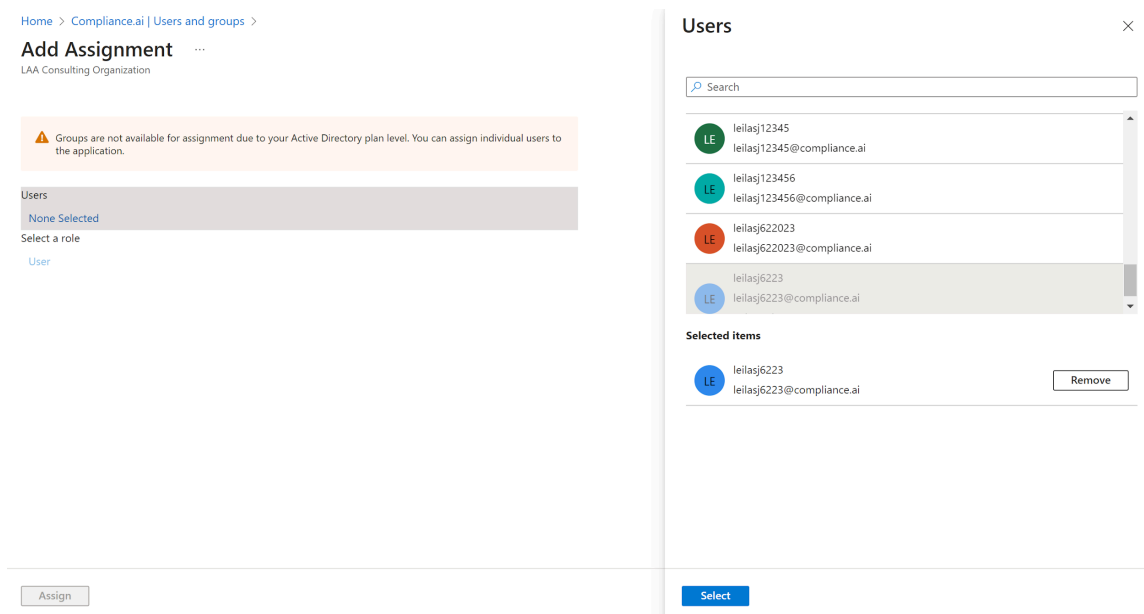
1. "Org Admin"
2. "Team Admin"
3. "Workflow Admin"
4. "Active Team User"
5. "Lite Team User"

Adding Users

To add users from your Active Directory to the Compliance.ai Application, follow these steps:

1. Find the application previously created for Compliance.ai.
2. Go to "Users and groups."
3. Click on "+Add users/groups."
4. Select the Users/Groups you wish to add.
5. Choose the role for the desired user/group.
6. Click "Assign."

Note: Exercise caution to avoid provisioning the same account as a user when adding users.

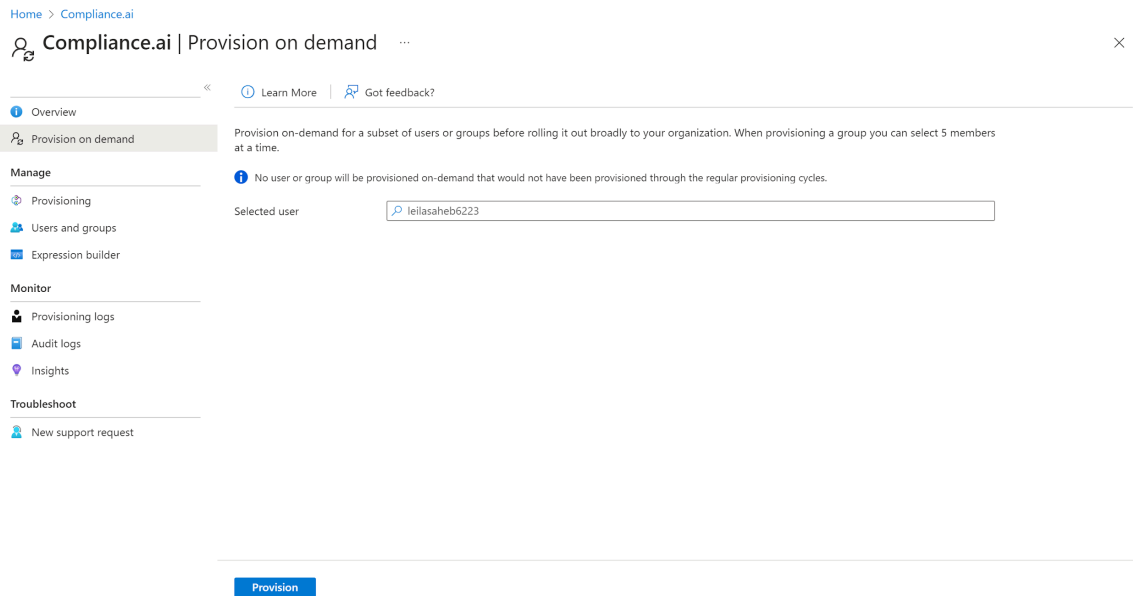


The screenshot shows two overlapping windows from the Compliance.ai interface. The background window is titled "Add Assignment" and shows a warning message: "Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application." Below the warning, there is a "Users" section with "None Selected" and a "Select a role" dropdown. The foreground window is titled "Users" and displays a list of users with search and selection capabilities. The "Selected items" section shows one user selected: leiliasj6223@compliance.ai.

| Avatar | Username | Full Name |
|--------|----------------|------------------------------|
| LE | leiliasj12345 | leiliasj12345@compliance.ai |
| LE | leiliasj123456 | leiliasj123456@compliance.ai |
| LE | leiliasj622023 | leiliasj622023@compliance.ai |
| LE | leiliasj6223 | leiliasj6223@compliance.ai |

Selected items

| | | | |
|----|--------------|----------------------------|--------|
| LE | leiliasj6223 | leiliasj6223@compliance.ai | Remove |
|----|--------------|----------------------------|--------|



Provision on demand

If the users you previously added are not syncing as part of provisioning, you can try to provision them on demand. Here's how:

1. Go to the Compliance.ai application in your Azure portal.
2. Navigate to "Provisioning."
3. Select the "Provision on demand" to provision users on demand.
4. Select the user who has not been provisioned through the regular provisioning cycles

This action should trigger the provisioning process for the users you've added, ensuring they sync correctly with the Compliance.ai application.

FAQ

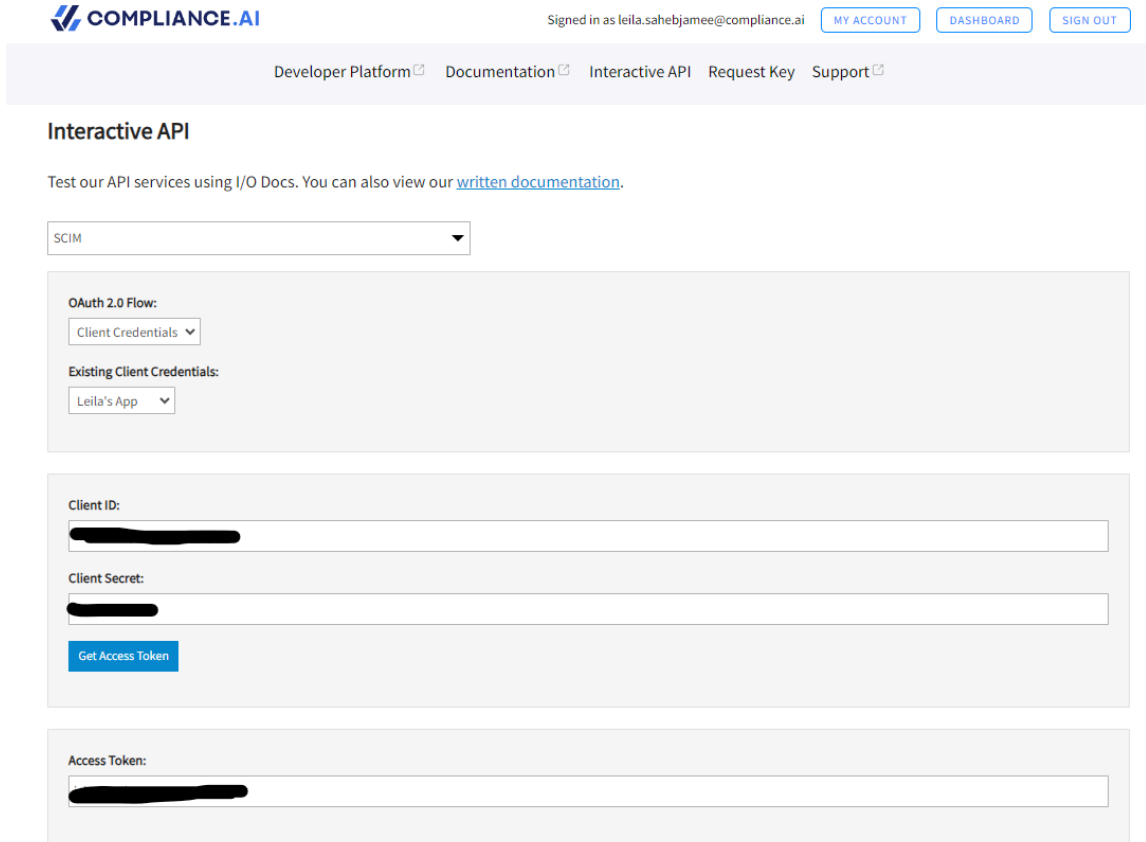
1. To confirm if a user is created on the Compliance.ai application, follow these steps:

- a. Login to <https://developer.compliance.ai/io-docs>.
- b. Navigate to "Interactive API."
- c. Select "SCIM API" from the dropdown menu.
- d. Under "Existing Client Credentials," select your application.
- e. Your Key and Client Secret should automatically be presented.
- f. Click on "Get Access Token."
- g. In the "GET SCIM Users - GET /scim/Users" section:
 - i. Set "Accept-Encoding" to "identity."

- ii. In the "filter" field, provide the value in the format: `userName eq "user@domain.com"`, replacing "user@domain.com" with the username of the user you provisioned.

h. Click "Try It."

This action will verify if the user has been successfully created and can be accessed through the Compliance.ai SCIM API.



The screenshot shows the Compliance.ai web interface. At the top left is the logo. On the right, it says "Signed in as leila.sahebjamee@compliance.ai" with buttons for "MY ACCOUNT", "DASHBOARD", and "SIGN OUT". Below this is a navigation bar with links for "Developer Platform", "Documentation", "Interactive API", "Request Key", and "Support". The main heading is "Interactive API". Below it, a text line says "Test our API services using I/O Docs. You can also view our [written documentation](#)." There is a dropdown menu currently set to "SCIM". Below this is a section for "OAuth 2.0 Flow" with a "Client Credentials" dropdown and "Existing Client Credentials" set to "Leila's App". There are input fields for "Client ID" and "Client Secret", both containing redacted text. A blue "Get Access Token" button is below these fields. At the bottom, there is an "Access Token" field containing redacted text.

Quarantine details:

While attempting to validate our authorization to access your application, we received this unexpected response: Received response from Web resource. Resource:

```
https://api.compliance.ai/scim/Users?
filter=userName+eq+"41556170-d37a-4040-a648-
e1bccd0c69e5" Operation: GET Response Status
Code: Unauthorized Response Headers: Connection:
keep-alive X-Mashery-Responder: prod-j-worker-
us-east-1c-06.use1.mashery.com X-Mashery-
Message-ID: 1aab3a51-021c-41f2-8366-
0b35835d2e4c X-Error-Detail-Header: Not
Authorized X-Mashery-Error-Code:
ERR_403_NOT_AUTHORIZED Date: Wed, 21 Jun
2023 05:29:23 GMT Server: Mashery Proxy WWW-
Authenticate: Bearer realm="api.compliance.ai",
error="invalid_token" Response Content: <h1>Not
Authorized</h1> Please check the service.
```

[View provisioning logs](#)

If you encounter the following error while “Testing the Connection” in Azure AD, it indicates that your access token has expired. To resolve this issue, you need to generate a new access token, as explained in the Access Token section above.

Testing connection to Compliance AI ✕

You appear to have entered invalid credentials. Please confirm you are using the correct information for an administrative account.

Error code:
SystemForCrossDomainIdentityManagementCredentialValidationUnavailable

Details: We received this unexpected response from your application:

Received response from Web resource.
Resource: https://api.compliance.ai/scim/Users?filter=userName+eq+"0d99ce3d-bf54-49b6-8c07-47519566c90d"
Operation: GET
Response Status Code: Unauthorized
Response Headers: Connection: keep-alive
X-Mashery-Responder: prod-j-worker-us-east-1b-02.use1.mashery.com
X-Mashery-Message-ID: 973b6f55-1037-4bc3-83d3-424fc8ea5743
X-Error-Detail-Header: Not Authorized
X-Mashery-Error-Code: ERR_403_NOT_AUTHORIZED
Date: Thu, 22 Jun 2023 03:54:09 GMT
Server: Mashery
Proxy
WWW-Authenticate: Bearer realm="api.compliance.ai", error="invalid_token"
Response Content: <h1>Not Authorized</h1>

Please check the service and try again.
Request-id: 90d0123f-d01e-4ccc-b204-be216d0bfaa5

3. Why is the user provisioning update not working?

This issue is a known issue within the Microsoft Azure solution. A resolution provided by Microsoft can be found in the link below:

<https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/application-provisioning-config-problem-scim-compatibility#flags-to-alter-the-scim-behavior>