



## SAML Installation Guide

IFU111

Version No: 1.0

Issue Date: July 2022



ASA1.0



CareDx Pty Ltd,  
20 Collie Street,  
Fremantle, WA 6160,  
Australia



For Evaluation Use Only. Not for use in diagnostic procedures. No claim or representation is intended to provide information for the diagnosis, prevention, or treatment of a disease.

© 2022 CareDx, Inc. All service marks or trademarks are owned or licensed by CareDx, Inc. or its affiliates. All rights reserved.

# Table of Contents

**Chapter 1: Introduction ..... 3**

**Chapter 2: Configuring the Server ..... 3**

**Chapter 3: Configuring AlloSeq™ Assign® ..... 12**

    Enabling Integrated Sign In. ....12

    Adding Users. ....15

    Removing Users.....16

    Disabling Integrated Sign In.....16

**Chapter 4: Support and Contact Details ..... 17**

**Chapter 5: Revision History ..... 18**

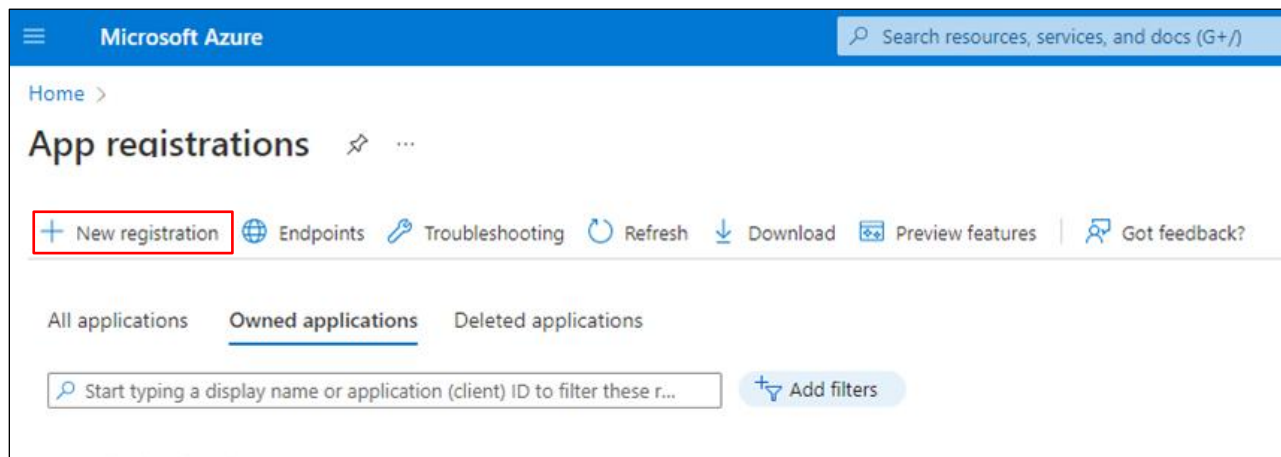
# Chapter 1: Introduction

The AlloSeq Assign software (from here described as “Assign”) has been modified to permit integration with single sign on systems using an implementation of SAML.

## Chapter 2: Configuring the Server

To support single sign on via Azure, Assign must be registered access to the authentication system.

1. Navigate to the azure portal.
2. Create an app registration by clicking “New registration”.



3. Enter "AlloSeq Assign" to identify the software.
4. Select supported account type "Single tenant" as shown below.
5. Click Register.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > App registrations >

## Register an application

**Name**

The user-facing display name for this application (this can be changed later).

alloseq-assign-test ✓

**Supported account types**

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (CareDx only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

**Redirect URI (optional)**

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

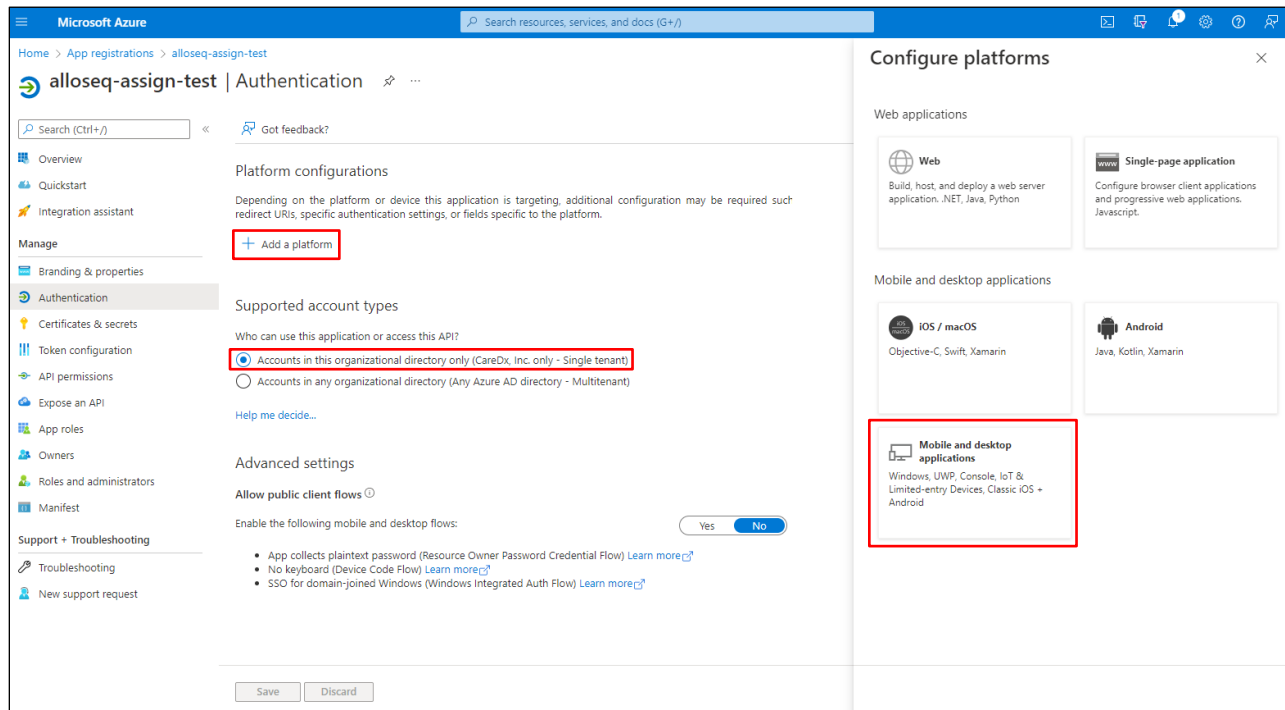
Select a platform ▼ e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

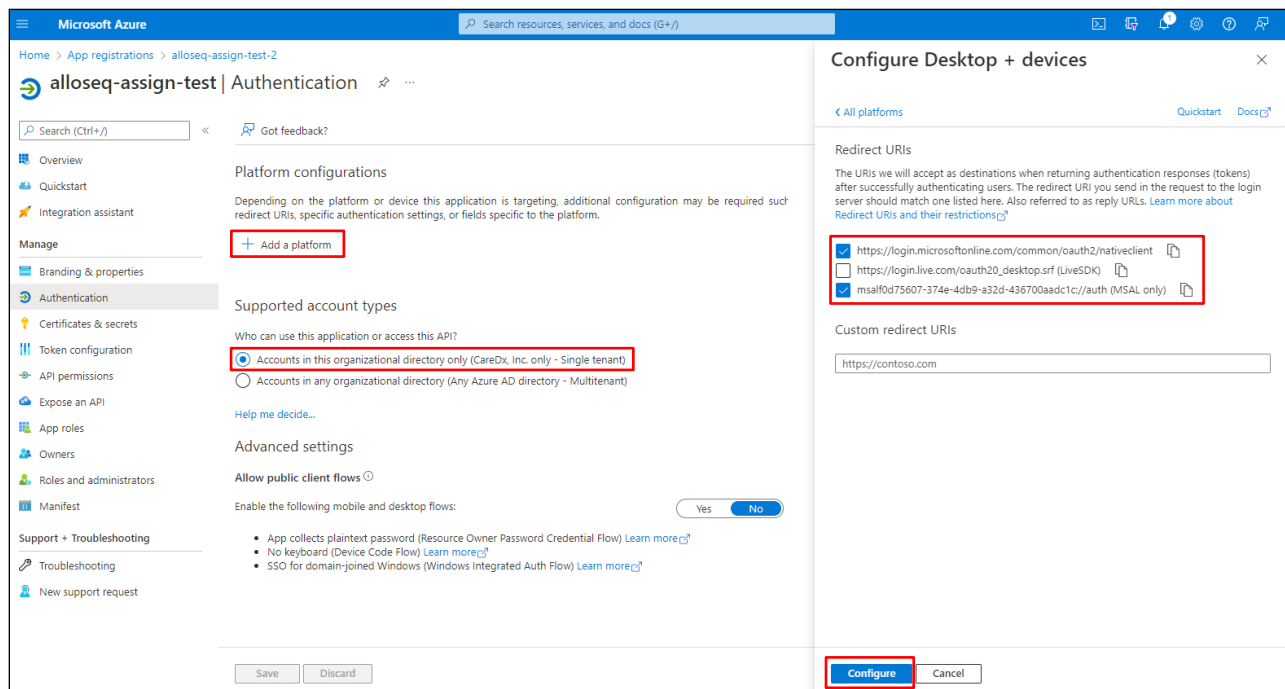
By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

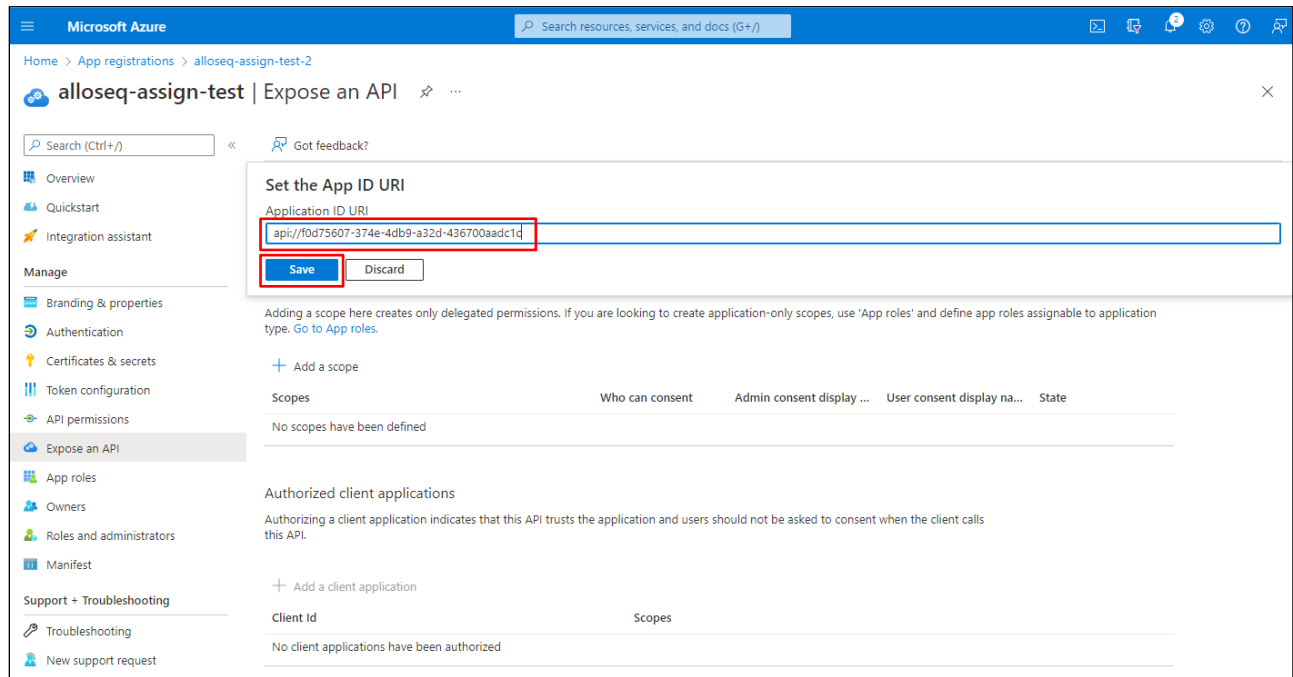
6. Click on “Add redirect URI”.
7. Add platform.
8. Select mobile and desktop.



9. Check the first one and last options for native client and auth (MSAL) only.
10. Click Configure



11. Go back to the previous screen.
12. Click on “Add application URI”.
13. Click Save.



Microsoft Azure

Home > App registrations > alloseq-assign-test-2

alloseq-assign-test | Expose an API

Search (Ctrl+/) « Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

**Set the App ID URI**

Application ID URI

api//f0d75607-374e-4db9-a32d-436700aad1d

Save Discard

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. [Go to App roles](#).

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
No scopes have been defined				

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Client id	Scopes
No client applications have been authorized	

14. Click on “Add a Scope”.

Scope Name: “Read.All”

Who can consent: “Admins Only” should be selected

Admin consent display name: “Read Users”.

Description: “Allow the application to read user information from Azure AD”.

State: “Enabled” should be selected.

15. Click “Add Scope”.

The screenshot displays the Azure AD application configuration interface. On the left, the 'Scopes defined by this API' section shows a table with columns: Scopes, Who can consent, Admin consent display ..., User consent display na..., and State. Below this table, the 'Add a scope' button is highlighted with a red box. The right side of the interface shows the 'Add scope' dialog box, which is also outlined with a red box. The dialog box contains the following fields:

- Scope name \*: Read.All (checked)
- Who can consent?: Admins and users (Admins only selected)
- Admin consent display name \*: Read Users (checked)
- Admin consent description \*: Allow the application to read user information from Azure AD (checked)
- User consent display name: e.g. Read your files
- User consent description: e.g. Allows the app to read your files.
- State: Enabled (selected), Disabled

At the bottom of the dialog box, there are 'Add scope' and 'Cancel' buttons.

16. Click on “Certificates & secrets”.
17. Click on “New client secret”.

Microsoft Azure

Home > App registrations > alloseq-assign-test-2

alloseq-assign-test | Certificates & secrets

Search (Ctrl+/)

Overview

Quickstart

Integration assistance

Manage

Branding & properties

Authentication

**Certificates & secrets**

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

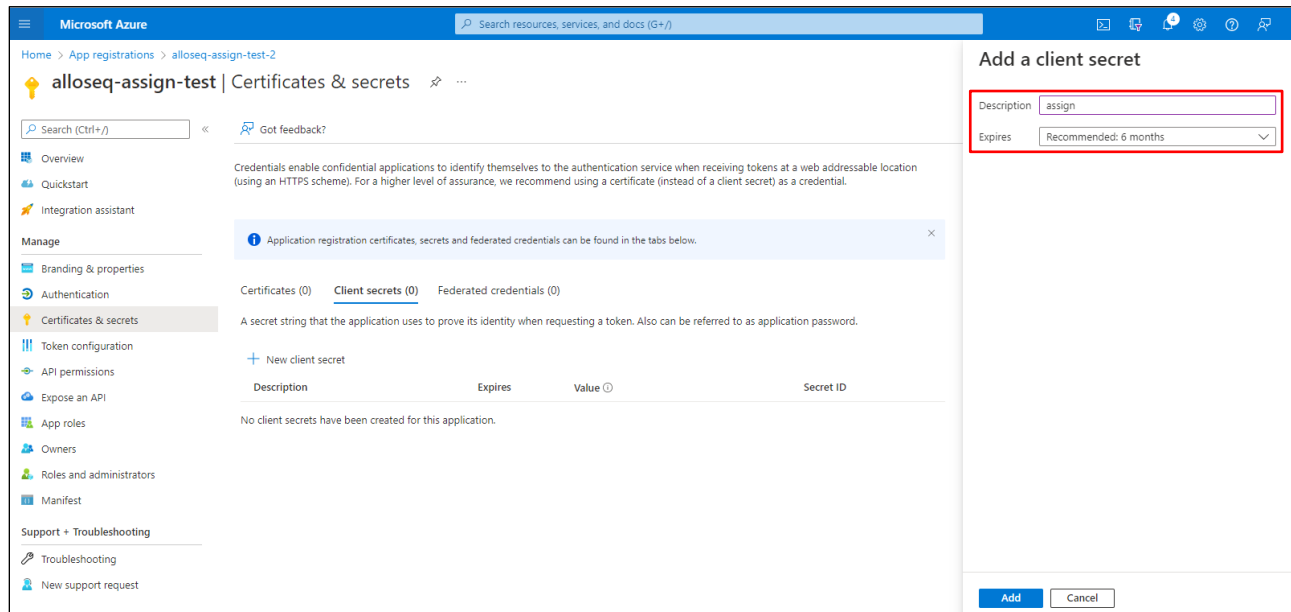
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

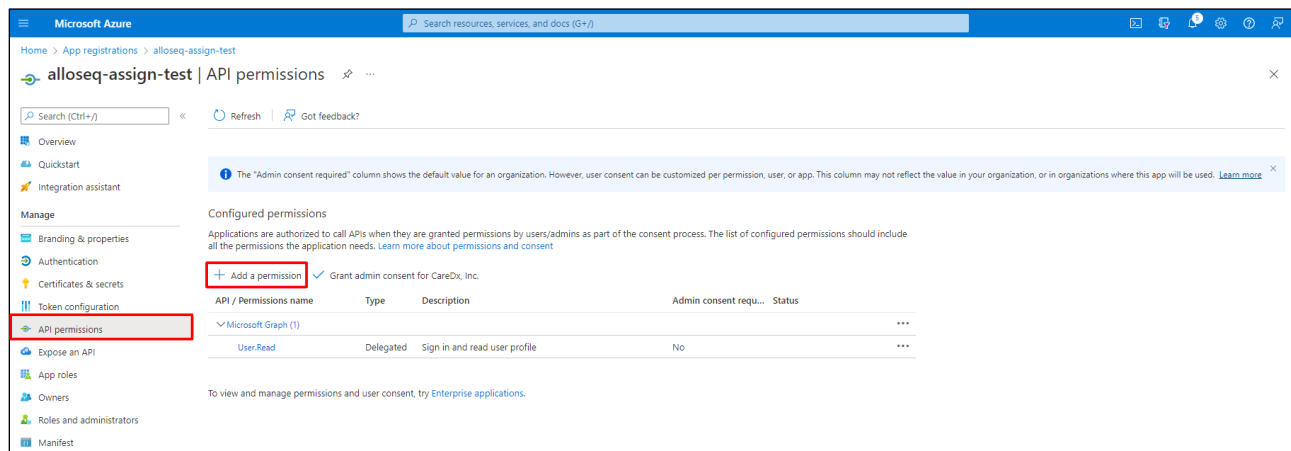
Description	Expires	Value	Secret ID
No client secrets have been created for this application.			



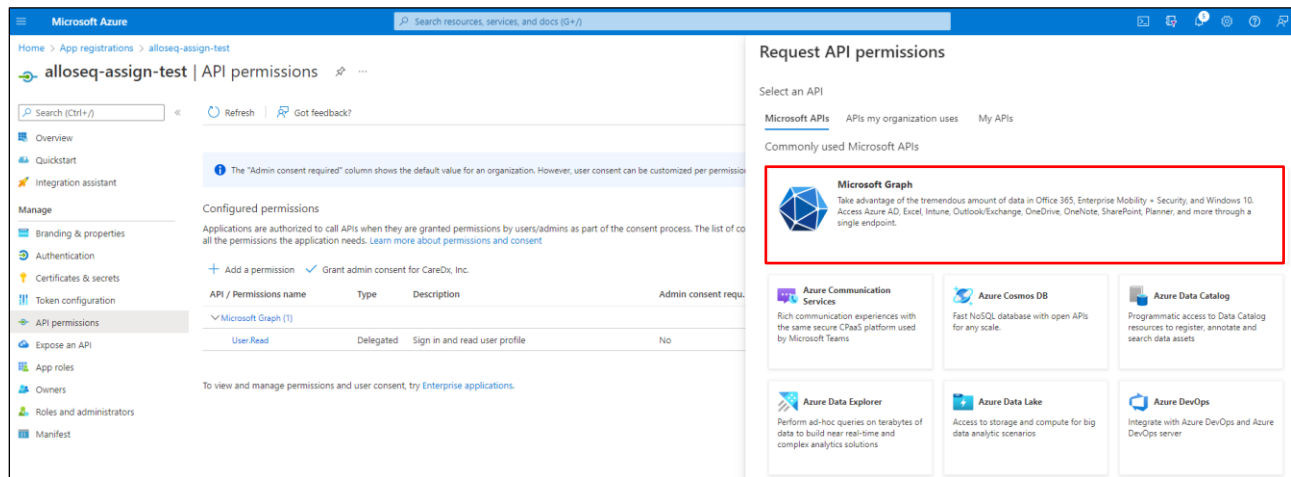
18. Provide a description.
19. Set up the expiration policy in accordance with any security policies.
20. Click Add.



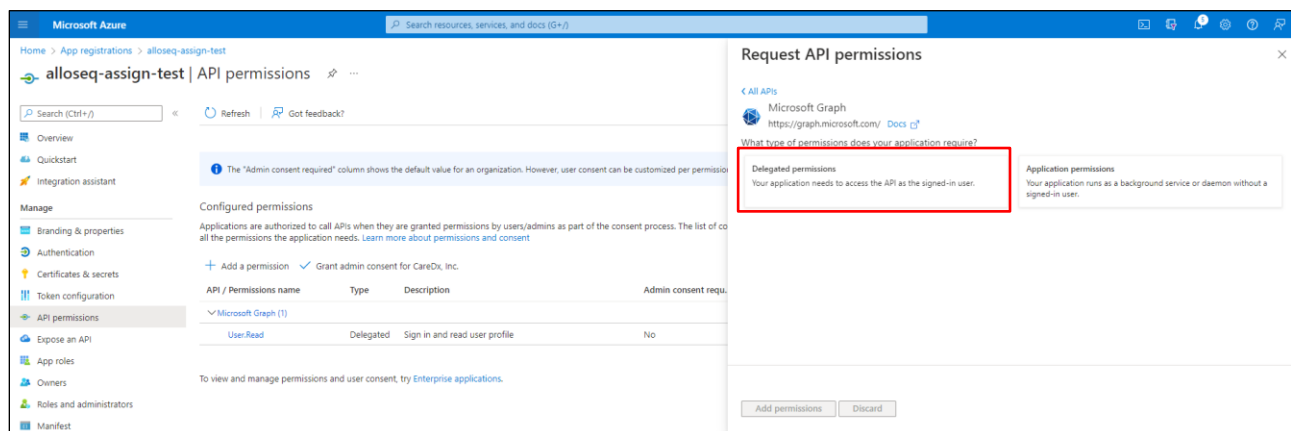
21. Copy the secret and save it somewhere, as it is only showed once. If you need to change the secret, generate a new one and then delete the existing one.
22. Click on “API Permissions”.
23. Click on “Add a permission”.



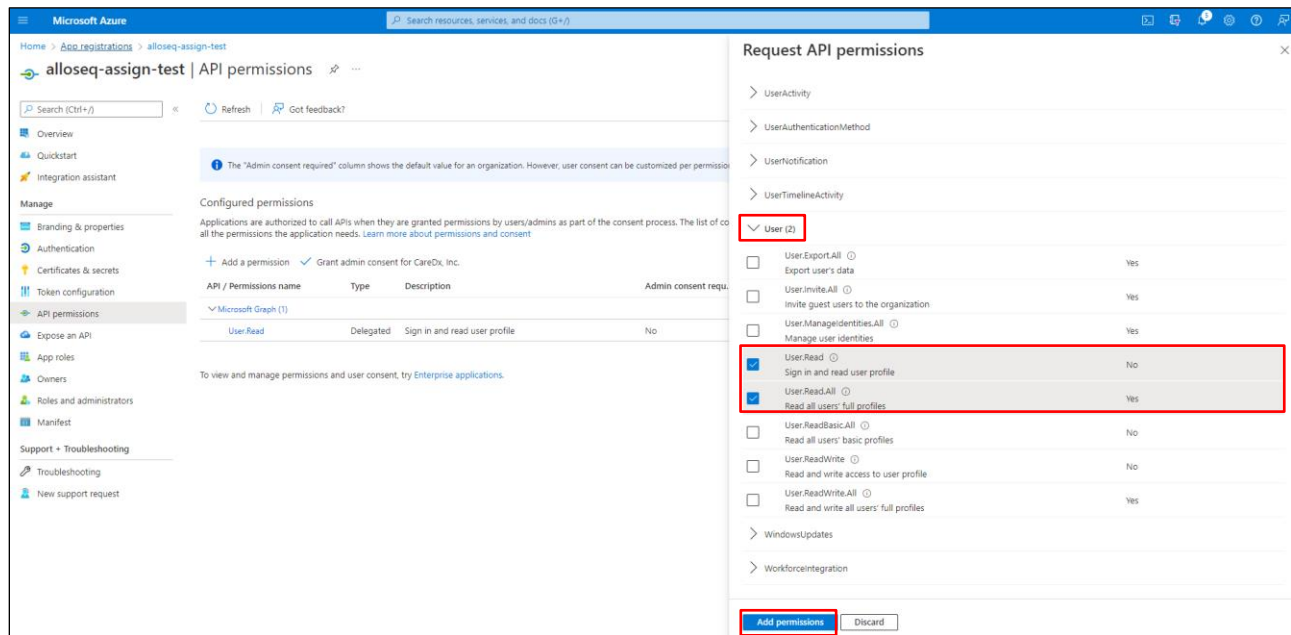
24. Click “Microsoft Graph”.



25. Click on “Delegated permissions”.



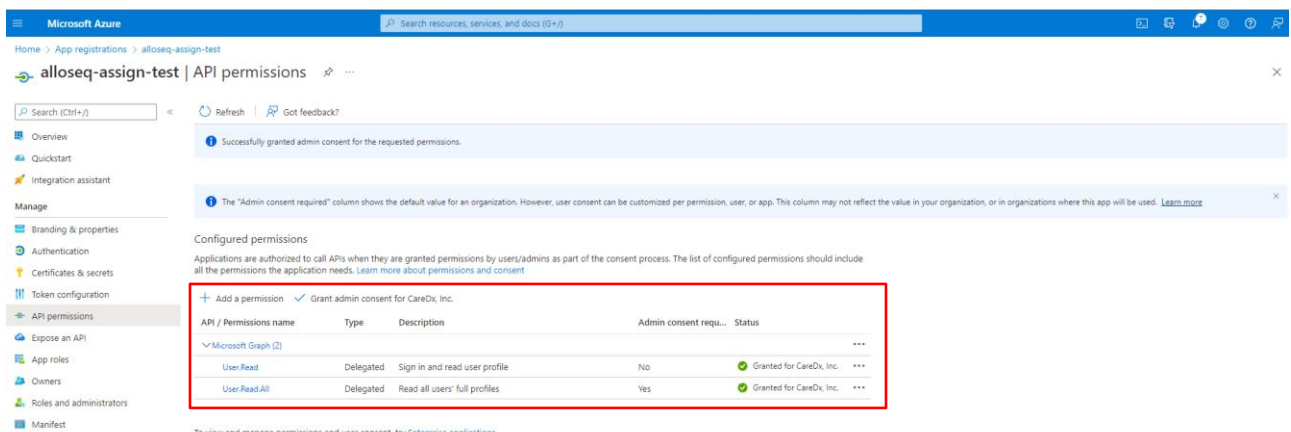
26. Scroll down to the “Users” section and select “User.Read” and “User.Read.All”.



27. Click on “Add permissions”.

28. Click on “Grant admin consent” for your organization.

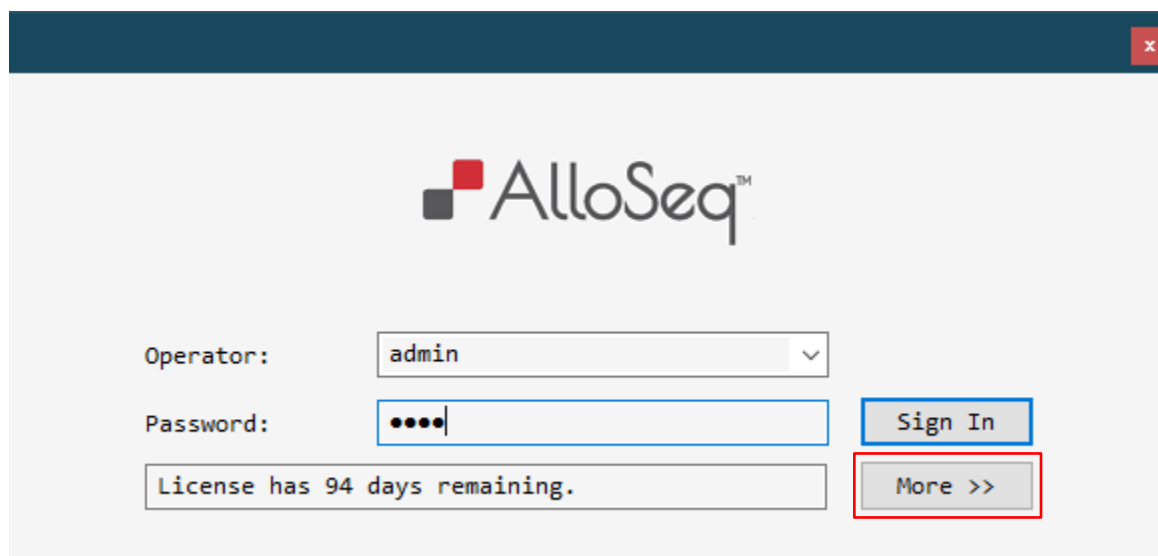
29. Please refer to the screenshot below after granting admin consent to verify that it matches. Close the browser once this is complete.



# Chapter 3: Configuring AlloSeq™ Assign®


## Enabling Integrated Sign In.

1. Launch AlloSeq™ Assign®.
2. Enter the username and password for the administrative user. The default values are “admin” and “cg01”.
3. Click :More”.

The image shows a login dialog box for AlloSeq™ Assign. At the top is a dark blue header bar with a red close button (X) on the right. Below the header is the AlloSeq™ logo, consisting of a red square and a black square followed by the text "AlloSeq™". The login form contains three main elements: a label "Operator:" followed by a dropdown menu showing "admin"; a label "Password:" followed by a password input field with four black dots; and a "Sign In" button. Below the password field is a status bar that says "License has 94 days remaining." To the right of the status bar is a "More >>" button, which is highlighted with a red rectangular box.

The dialog should extend to display additional information, including the option to enable integrated sign in.

×



Operator: admin ▼

Password: •••• Sign In

License has 186 days remaining. Less <<

☐ Enable Integrated Sign In
 Configure

**Edit Users**

Edit Operator: admin ▼

New Password:

Retype Password:  Add / Update

Default settings:  ▼ Remove User

Operator Level: Final reviewer (with full access) ▼

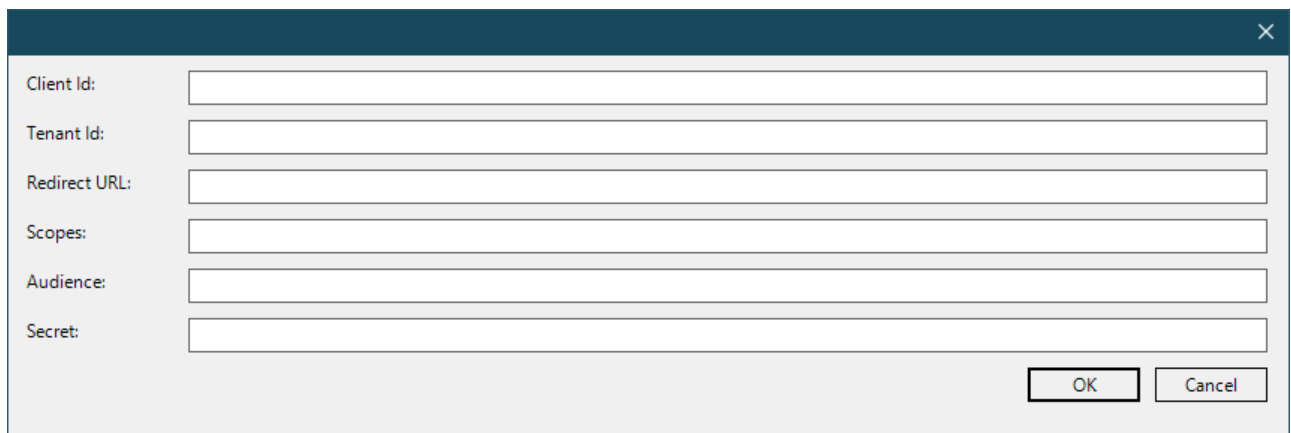
**System File Location**

C:\ProgramData\CareDx\AlloSeq v1.0.3 Browse Move

**Project File Location**

C: Browse

4. To enable integrated sign in, check the highlighted box.
5. **WARNING!** Enabling integrated sign in requires a valid server configuration and will remove any existing usernames and passwords. Click through the warning dialogs to indicate that this is acceptable.
6. Provide the authentication server parameters obtained in the previous section to configure AlloSeq™ Assign®.



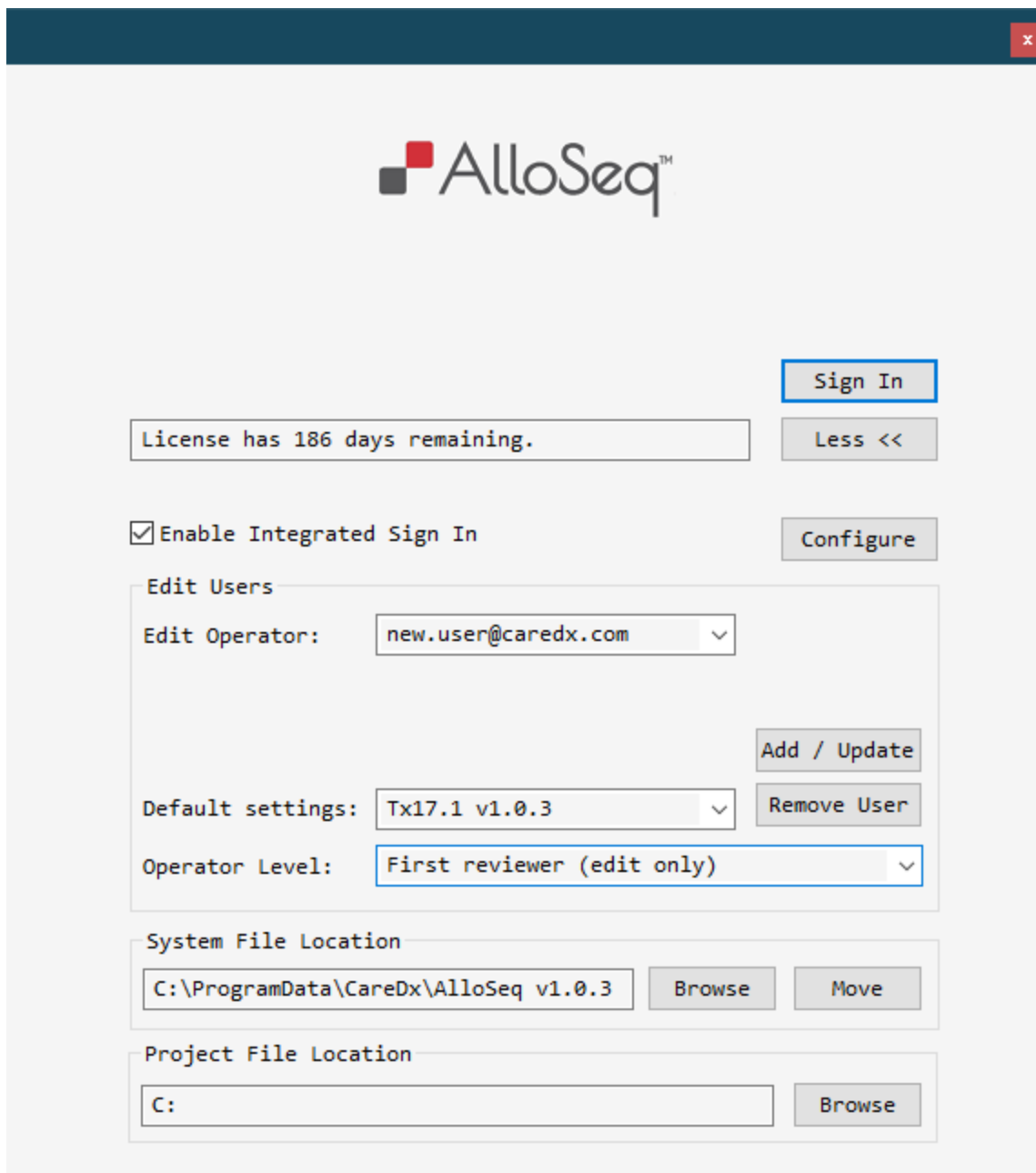
A configuration dialog box with a dark blue header bar containing a close button (X). The dialog contains six input fields with labels on the left: 'Client Id:', 'Tenant Id:', 'Redirect URL:', 'Scopes:', 'Audience:', and 'Secret:'. Each label is followed by a white rectangular input field. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

7. Once the form is completed click “OK” to continue.
8. If the configuration was successful, the user login dialog generated by the authentication server will be displayed.

The first user to be authenticated via the server will be designated as the AlloSeq™ Assign® system administrator. The system administrator is the only user with permissions to add, modify, or remove user access to the system.

## Adding Users.

1. Launch AlloSeq™ Assign®.
2. Click : “More”.
3. Sign in as the system administrator.
4. Enter the login name for the new user, which should match the credentials that they use to access the authentication server.
5. Select the default settings for the new user and the access level to the software.
6. Click “Add/Update”.



The screenshot shows the AlloSeq™ Assign® software interface. At the top, there is a dark blue header bar with a red 'x' button on the right. Below the header, the AlloSeq™ logo is centered. The main content area is light gray and contains several sections:

- License Information:** A text box displays "License has 186 days remaining." To its right is a "Sign In" button and a "Less <<" button.
- Integrated Sign In:** A checkbox labeled "Enable Integrated Sign In" is checked. To its right is a "Configure" button.
- Edit Users Section:**
  - Edit Operator:** A dropdown menu shows "new.user@caredx.com".
  - Default settings:** A dropdown menu shows "Tx17.1 v1.0.3".
  - Operator Level:** A dropdown menu shows "First reviewer (edit only)".
  - Buttons: "Add / Update" and "Remove User" are located to the right of the dropdowns.
- System File Location:** A text box shows "C:\ProgramData\CareDx\AlloSeq v1.0.3". To its right are "Browse" and "Move" buttons.
- Project File Location:** A text box shows "C:". To its right is a "Browse" button.

## Removing Users.

1. Launch AlloSeq™ Assign®.
2. Click :More”.
3. Sign in as the system administrator.
4. Select the user to be removed.
5. Click “Remove”.

## Disabling Integrated Sign In.

1. Launch AlloSeq™ Assign®.
2. Click :More”.
3. Sign in as the system administrator.
4. Uncheck the “Enable Integrated Sign In” box.
5. **WARNING!** Disabling integrated sign in will remove any existing users from the system and reset the administrator account to “admin” with the password “cg01”.
6. If this is acceptable, click through the warning dialog to disable integrated sign in.



## Chapter 4: Support and Contact Details

Website: <https://labproducts.caredx.com/>

For ordering details please refer to the CareDx website: <https://labproducts.caredx.com/>

For Technical Support please email: [techsupport-global@caredx.com](mailto:techsupport-global@caredx.com)

## Chapter 5: Revision History

Version	Date	Modification	Authorized by
1.0	26Jun22	Initial issue of AlloSeq Assign SAML IFU. CR2021-081. Issued by Hira Meraj 01-Jul-22	Damian Goodridge