

LSEG Workspace | Entra

Administrator's Activation Guide



LSEG DATA &
ANALYTICS

Contents

Contents..... 1

About this document 2

 Intended readership..... 2

 Contact information 2

Prerequisites 3

Entra setup steps 4

Accessing the Client Admin Tools app..... 5

Finding your Entra tenant ID 6

Provisioning the Workspace gallery application 7

 Additional resources 8

Registering your tenant in Client Admin Tools 9

 Generating a new Secret Token 10

Setting up an app in the Entra admin portal 11

Mapping application attributes..... 13

 Mapping group attributes 13

 Mapping user attributes 14

 Changing a non-matching userName..... 15

 Using Expression builder 15

Provisioning users in the Entra admin portal 17

 Accessing Workspace variants with LSEG credentials 18

Useful links..... 19

About this document

LSEG Workspace now supports user authentication through Microsoft Entra. This document describes the steps that are performed to associate users in your organisation with Workspace, allowing them to access the product seamlessly.

Intended readership

The LSEG Workspace – Entra Administrator's Activation Guide is intended for administrators on customer sites that are responsible for the maintenance of Workspace and Microsoft Entra tenants.

Contact information

To:

- Receive further assistance, contact [Support](#).
- Provide feedback on Workspace technical content, contact DocFeedback@lseg.com.

Prerequisites

To enrol users for Entra authentication into Workspace, the following conditions must be met:

- You must have access to Workspace to provision credentials for System Cross-domain Identity Management (SCIM)¹.
- You also require access to the Workspace Admin Tools app to register your Entra tenant.

Important: Initial access to the Workspace Admin Tools app does not include the tenant registration process, for which additional privileges are required.

To request these privileges, either contact LSEG through the [MyAccount Support channel](#) or contact your dedicated Account Team.

¹ SCIM is a protocol used to standardise how identity information is exchanged between entities.

Entra setup steps

Setting up users for Entra access involves performing the following steps, which are discussed in the sections that follow:

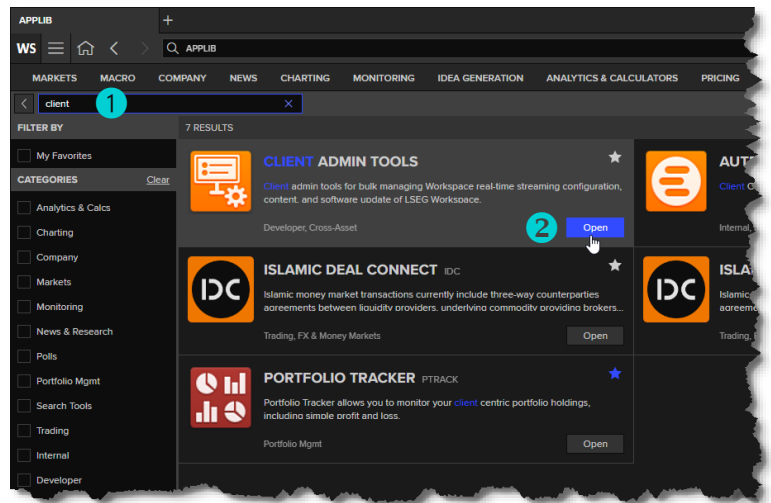
- [Accessing the Client Admin Tools app](#)
- [Finding your Entra tenant ID](#)
- [Provisioning the Workspace gallery application](#)
- [Registering your tenant in Client Admin Tools](#)
- [Setting up an app in the Entra admin portal](#)
- [Mapping application attributes](#)
- [Provisioning users in the Entra admin portal](#)

Also, following these steps, the [Useful links](#) section contains links to additional material provided by third parties.

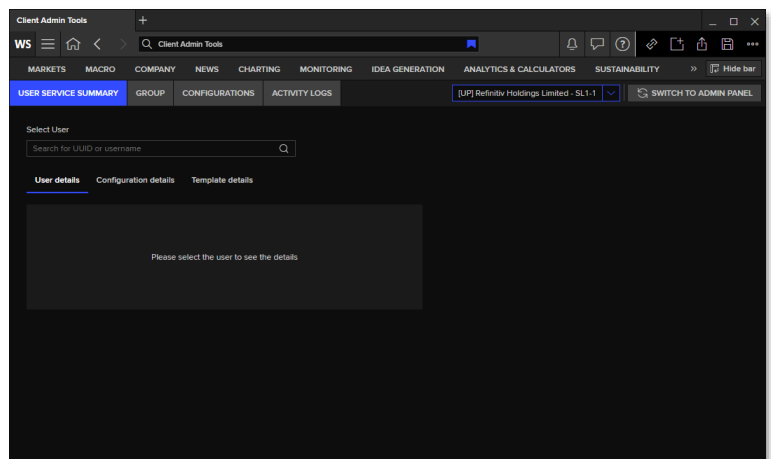
Accessing the Client Admin Tools app

To access the Client Admin Tools app:

1. Log in to Workspace.
2. Select **WS > App Library**.
Alternatively, to open the App Library in a new browser, press **Alt+L**.
3. To filter the app list, in the Search box **1**, type **Client**.
The apps are filtered, as shown in the example, opposite.
4. To run the Client Admin Tools app, click **Open** **2**.



The Client Admin Tools app launches in the same browser window.

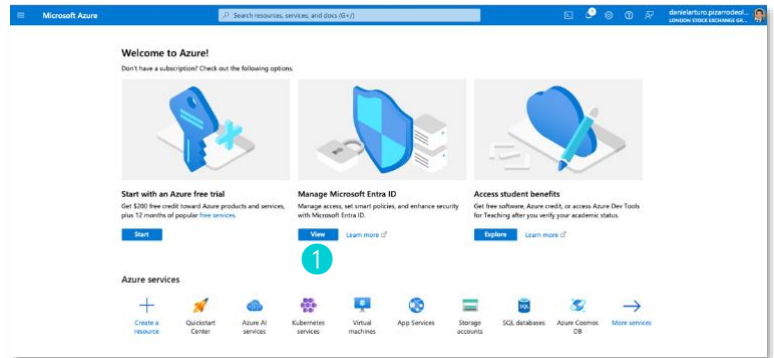


Finding your Entra tenant ID

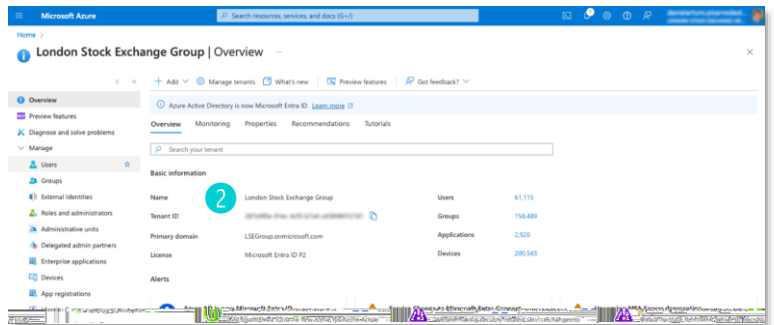
Your Microsoft Entra tenant ID is the unique identifier for your organisation that is assigned by Microsoft. You need this ID to register your tenant in the Client Admin Tools app.

To find this code:

1. Log in to <https://portal.azure.com/#home>.
The Microsoft Azure Welcome page opens (opposite).
2. Click the Manage Microsoft Entra ID **View** 1 button.



The **Overview** page opens (opposite) where the Tenant ID 2 is shown under the Basic Information section.



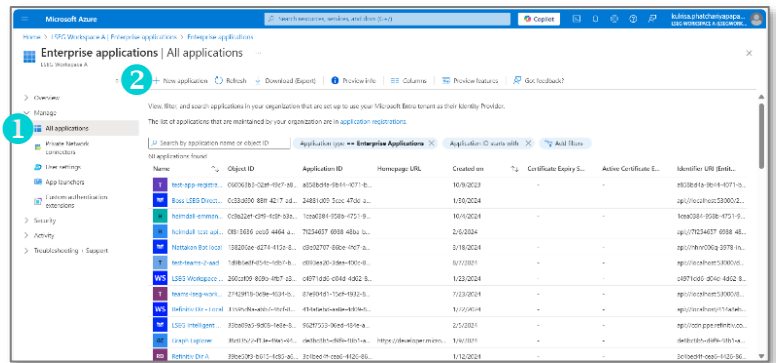
Provisioning the Workspace gallery application

The Workspace gallery application must be provisioned to your Entra tenant. This allows users to access the Workspace application² using their Microsoft credentials.

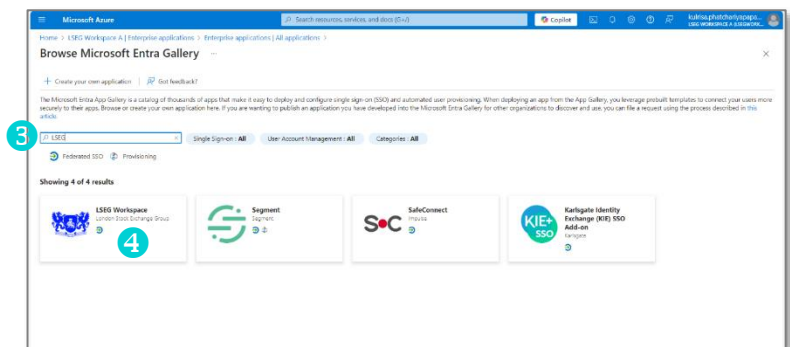
Once the application has been provisioned to the tenant, your conditional access policies, such as MFA, compliant devices, and so on, can be applied. To find further information on conditional access policies, refer to the [Plan a Conditional Access deployment](#) page on Microsoft Learn.

To provision Workspace to your Entra tenant, do the following:

1. On your Microsoft Azure portal, navigate to **Enterprise applications > Manage > All applications** ¹ and select **New application** ².

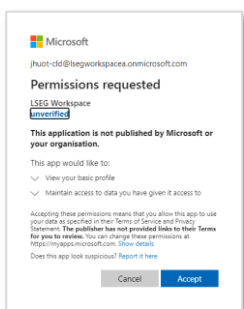


2. In the Search box ³, type **LSEG**.
3. From the filtered list, select the **LSEG Workspace** app ⁴.

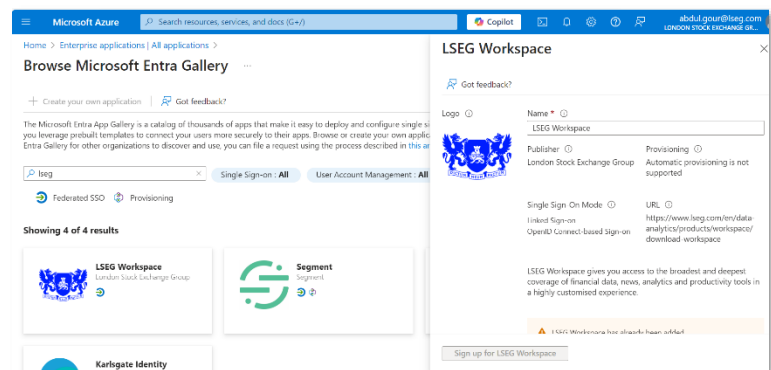


The LSEG Workspace app panel is displayed.

4. Click the **Sign up for LSEG Workspace** button.
5. In the Permissions requested dialog, click **Accept** ³.



Following this, the app is installed to your tenant.



² The currently supported Workspace application variants are **Workspace | Web** and **Workspace | OpenFin**.

³ Currently, as your credentials will not be valid for Workspace, a "We are having trouble logging you in" error message is displayed. This can be ignored and will be fixed in future versions.

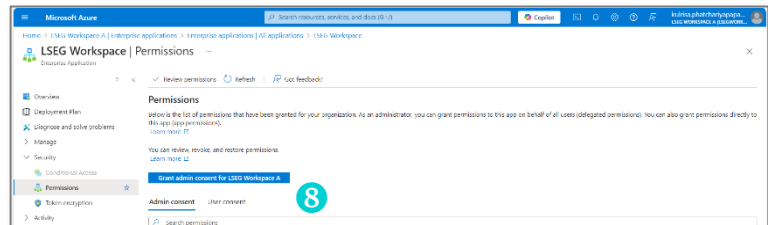
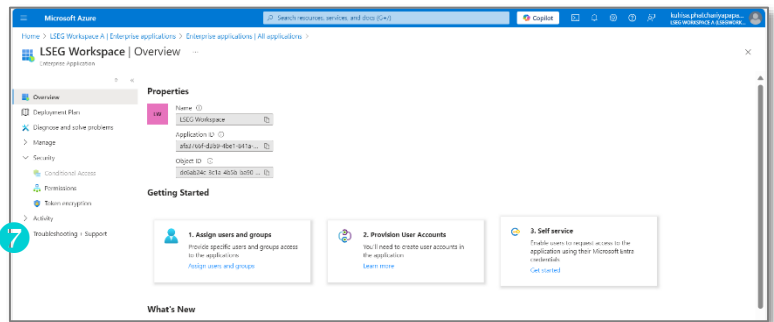
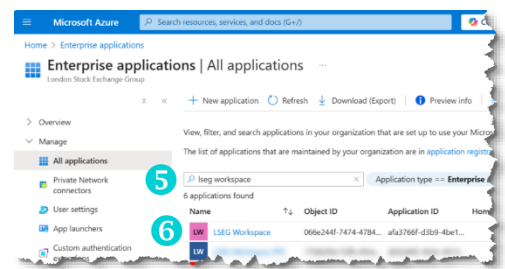
6. Return to **Enterprise applications > Manage > All applications**.
7. In the Search box **5**, type **LSEG Workspace**.
8. From the filtered list, select the LSEG Workspace application with the pink logo, highlighted in the screenshot **6**.

The LSEG Workspace Overview panel is displayed (see step 7, below).

9. In the left-hand menu of the LSEG Workspace Overview panel, select **Security > Permissions** **7**.

The LSEG Workspace permissions panel is displayed (opposite).

10. Select the **Grant admin consent for London Stock Exchange Group** button **8**.



Additional resources

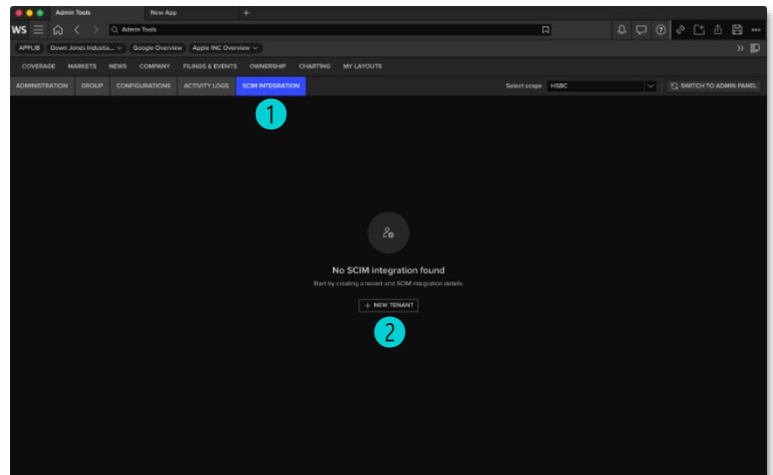
For further information about:

- Granting admin consent to applications, refer to the Microsoft Learn [Grant tenant-wide admin consent to an application](#) page.
- App validation, refer to the Microsoft Learn [What is app provisioning in Microsoft Entra ID?](#) page.

Registering your tenant in Client Admin Tools

To register your tenant in the Client Admin Tools app:

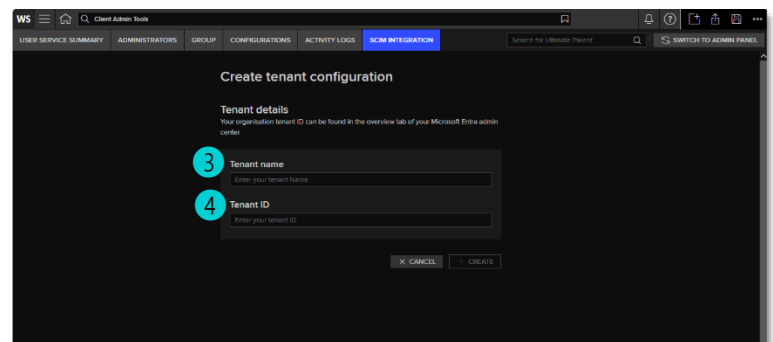
1. Run LSEG Workspace and open the Client Admin Tools app.
2. Select the **SCIM INTEGRATION** menu item **1**.
3. In the centre of the SCIM Integration panel, click the **+ NEW TENANT** button **2**.



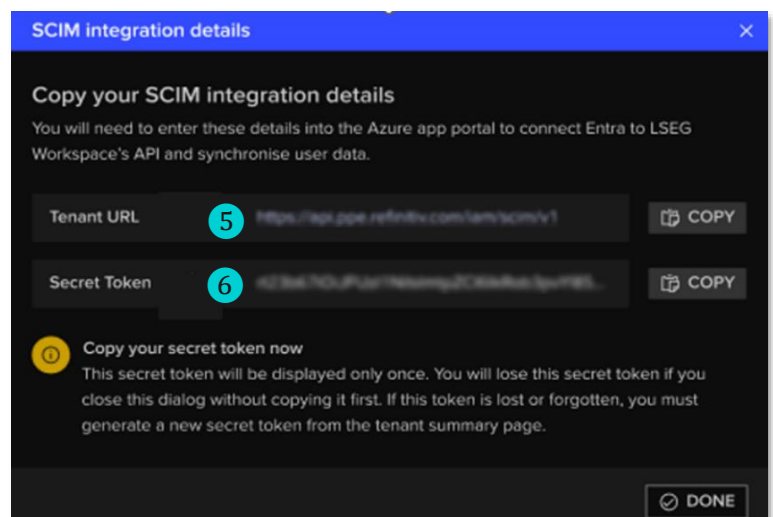
4. Enter the Tenant Name **3** and Tenant ID **4** of your organisation (see [Finding your Entra tenant ID](#)) and click **CREATE**.

Once the following automated tasks have been performed (denoted by a green checkbox), the setup has been successful.

- Creating application
- Certifying application
- Certifying service account
- Assigning license
- Creating tenant configuration



5. Copy the generated Tenant URL **5** and Secret Token **6** individually into a text tool, such as Notepad.

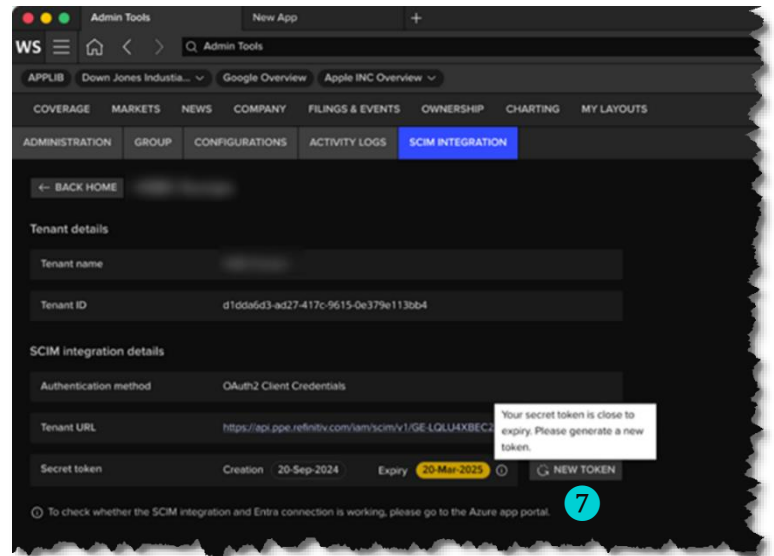


Generating a new Secret Token

The secret token has a validity of six months. When the token is within 30 days of expiry, the date will be highlighted in amber, along with a warning pop-up box.

If the Secret Token has expired, a new token must be generated to re-link the Entra tenant to Workspace This is done by following the steps below:

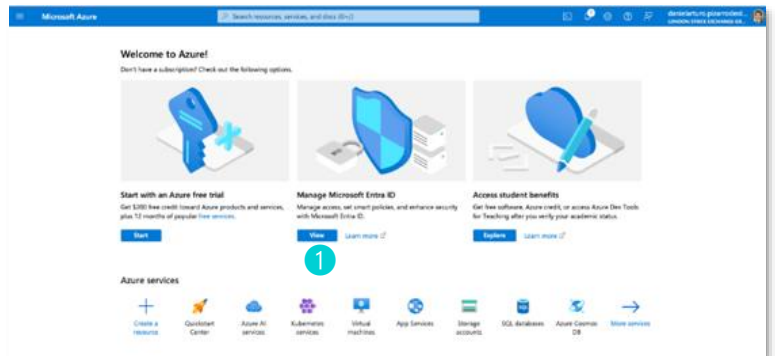
1. Navigate to the Admin Tools app.
2. Select the **SCIM integration** menu item.
3. Select your tenant from the tenant list.
4. Under the SCIM integration details section, select the **New Token** button 7.



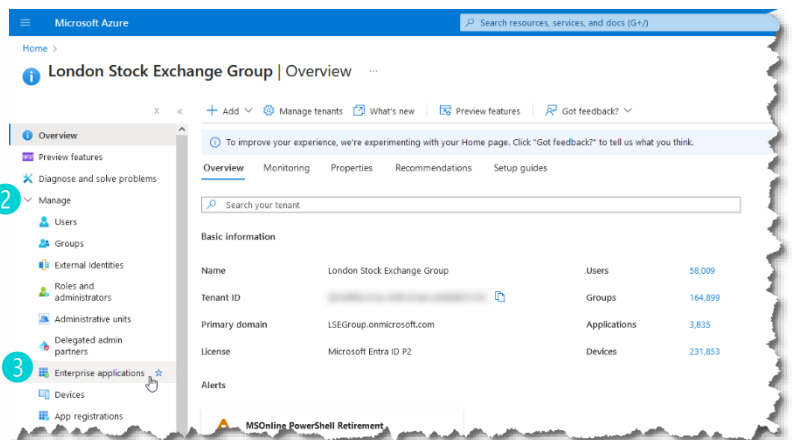
Setting up an app in the Entra admin portal

To set up an app in the Entra admin portal that allows users to be provisioned to any LSEG application that is integrated with Entra, do the following:

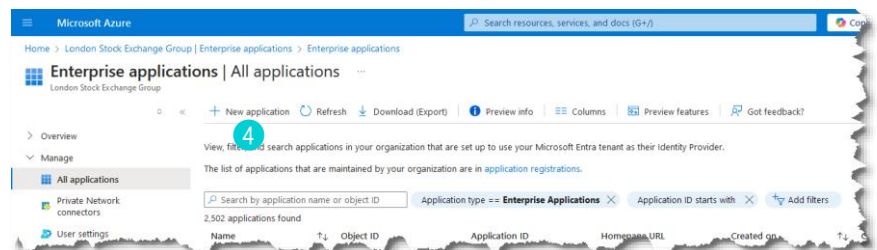
1. Log in to <https://portal.azure.com/#home>.
2. Click the Manage Microsoft Entra ID **View** button ①.
3. The Overview page opens.



4. From the left-side menu, select **Manage** ② > **Enterprise Applications** ③.



5. Under the All applications panel, select **New application** ④.

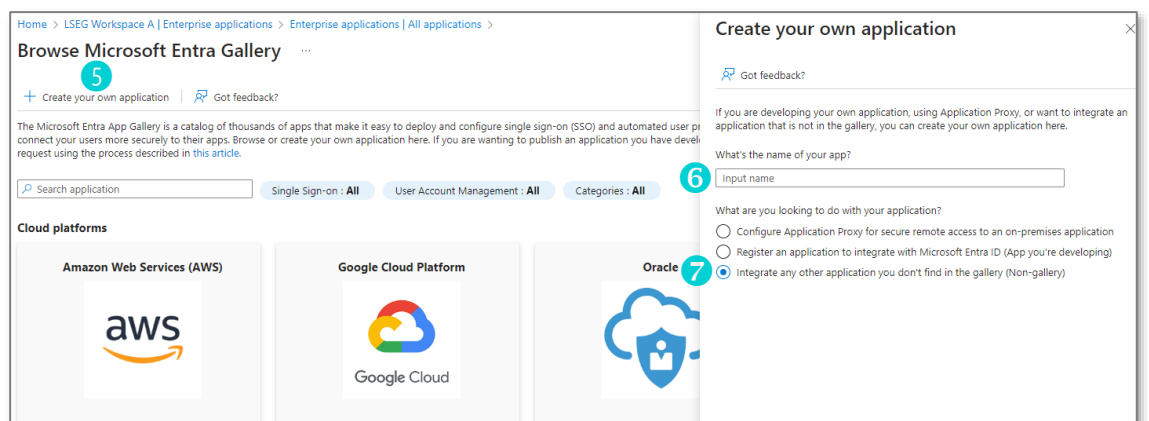


6. Click **Create your own application** ⑤.

The Create your own application side panel appears.

7. In the **What is the name of your app?** box ⑥, type **LSEG SCIM**.

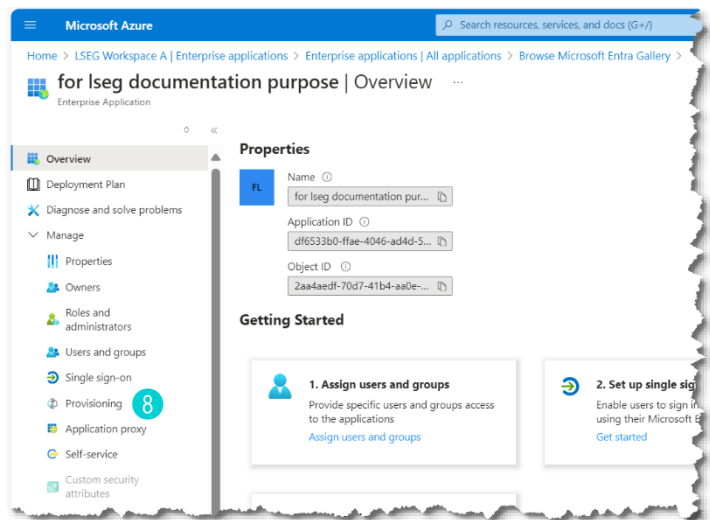
8. Under **What are you looking to do with your application?**, select **Integrate any other application you don't find in the gallery (Non-gallery)** ⑦.



9. Click the **Create** button, at the bottom of the side panel (not shown in the illustration, above).

A new application overview page, opposite, opens.

10. In the left-side menu, select **Manage > Provisioning** ⁸.

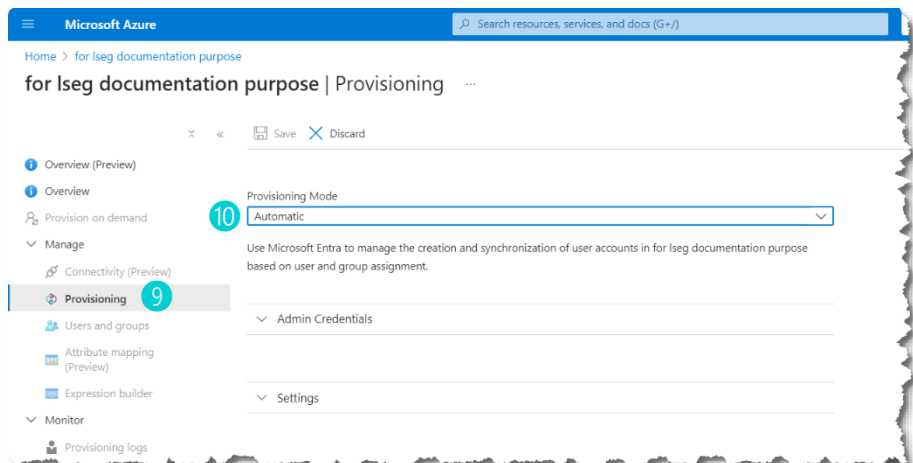


11. In the Overview (Preview) panel, select **Manage > Provisioning** ⁹.

This displays the Provisioning panel, which is comprised of three expandable sections:

- Provisioning Mode
- Admin Credentials
- Settings

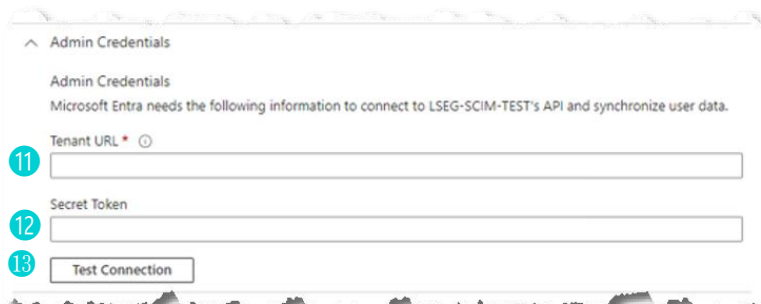
12. In the **Provisioning Mode** section, select **Automatic** ¹⁰.



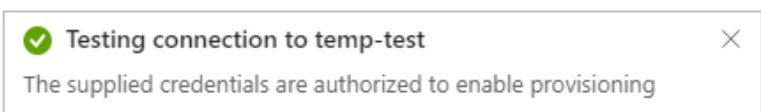
13. In the Admin Credentials section, enter **Tenant URL** ¹¹ and **Secret Token** ¹², obtained from Step 7 above.

14. In the Settings section of the panel, ensure **Provisioning Status** is set to **Off**⁴.

15. Click **Test Connection** ¹³.



If the test is successful, a green tick will appear, together with a message confirming the supplied credentials are authorised to enable provisioning.



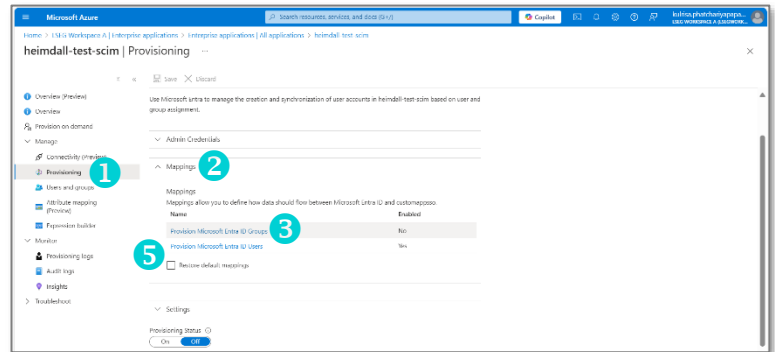
⁴ The **Provisioning Statis** slider switch is shown in the illustration at the top of the following page.

Mapping application attributes

To synchronise user and group attributes between Azure Active Directory and the target Workspace application, follow the instructions in the sections below.

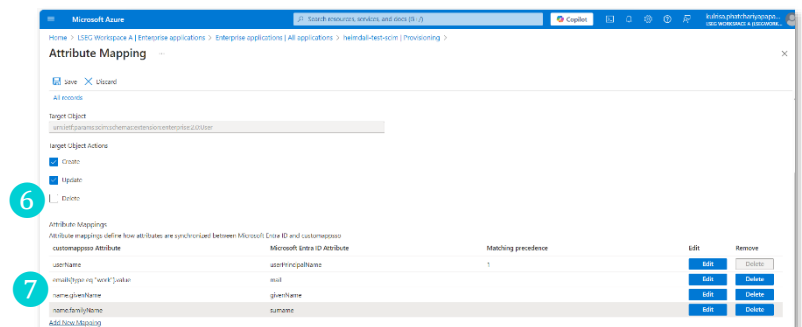
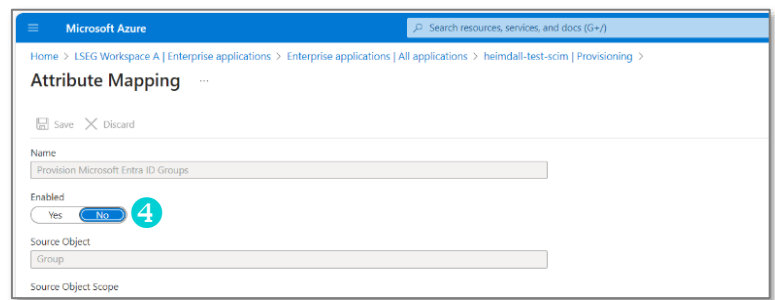
Mapping group attributes

1. From the left-side menu, select **Manage > Provisioning** ¹.
2. Expand the **Mappings** section ² and click **Provision Microsoft Entra ID Groups** ³.



The Attribute Mapping panel is displayed.

3. Set **Enabled** ⁴ to **No**⁵ and click **Save**.
4. Return to the previous page and, from the expanded Mapping section, select **Provision Microsoft Entra ID Users** ⁵.
5. The Attribute Mapping panel is displayed.
6. Set **Enabled** ⁴ to **Yes**.
7. For **Target Object Actions** ⁶, uncheck **Delete**.
8. Delete unused Attribute Mappings but keep the following ⁷, with the illustrated settings:
 - userName
 - emails[type eq "work"].value
 - name.givenName
 - name.familyName



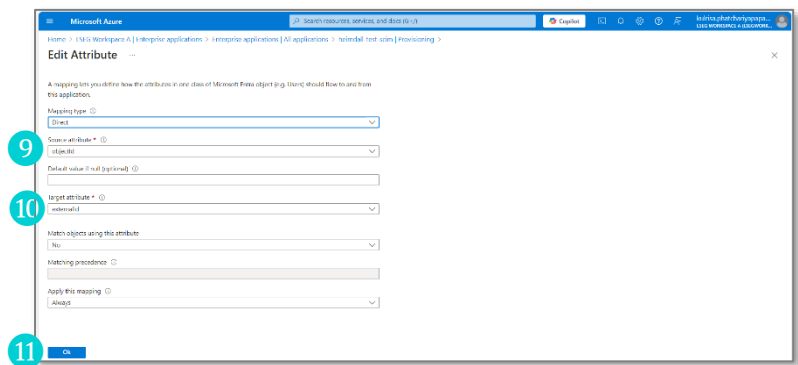
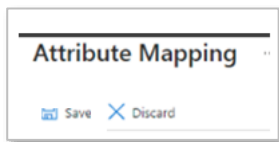
9. Click **Add New Mapping** ⁸, found at the bottom of the Attribute Mappings section.



⁵ Currently, LSEG does not support group provisioning.

The Edit Attribute panel is displayed.

10. From the **Source attribute** dropdown **9**, select **objectId**.
11. From the **Target attribute** dropdown **10**, select **externalId**.
12. To save your settings and return to the Attribute Mapping panel, click **OK** **11**.
13. Found immediately below the Attribute Mapping heading, click the **Save** option.



Mapping user attributes

To provision Workspace users with Entra authentication successfully, you need to set Entra attributes that can be mapped to the Workspace User IDs⁶.

By default, SCIM attempts to map the Entra `userPrincipalName` to their Workspace User ID. However, in some instances, this mapping will not work, as they will not match. In this circumstance, to customise the user attribute mapping and select an Entra attribute that matches the Workspace User ID, follow the steps below:

1. In your Entra tenant, open the app you created. In this example, it is named Workspace SCIM Integration.

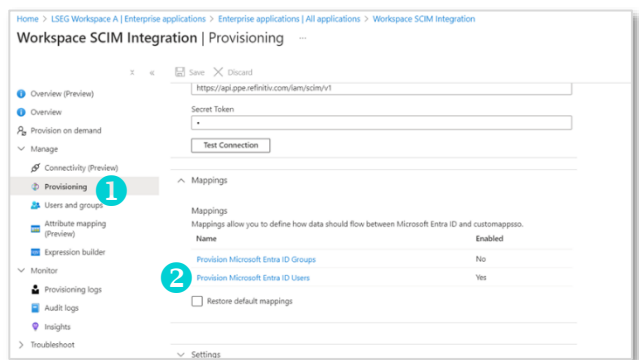
2. From the left side menu, select **Manage > Provisioning** **1**.

The Provisioning panel is displayed.

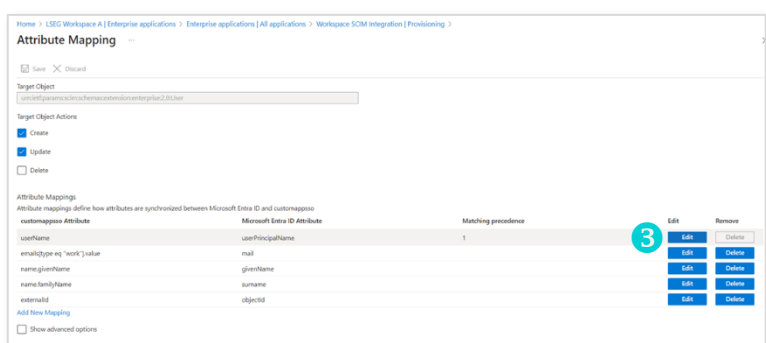
3. Under the Mappings section, select the **Provision Microsoft Entra ID Users** option **2**.

The Attribute mapping panel is displayed.

4. Configure the mappings⁷, as shown in the table below:



This attribute...	Map to...
userName	userPrincipalName
Matching Precedence should only be selected for the username attribute and must be set to 1. No other attribute should have a Matching Precedence setting.	
name.givenName	mail
name.familyName	givenName
emails[type eq "work"].value	surname
externalId	objectId



⁶ The use of Workspace user IDs is specifically for onboarding LSEG Workspace users onto Entra. Other products may use their own user IDs for Entra onboarding.

⁷ It is crucial that these mappings are configured as shown in the table, as incorrect mappings will result in provisioning failure.

Changing a non-matching userName

If the `UserPrincipalName` in Entra does not match the `userName` in SCIM, you need to amend the mapping by changing to another Entra attribute that does match with the `userName`.

To do so:

- Click the **Edit** button, next to `userPrincipalName` 3.

The Edit Attribute panel is displayed.

Mapping an existing Entra attribute

To map an existing Entra attribute to the SCIM `userName`, do the following:

- In the **Source Attribute** field, click v to open the dropdown menu 4.

Customising the attribute mapping

If none of the existing Entra attributes match the SCIM `userName`, to customise the attribute mapping, do the following:

- Open the **Mapping type** dropdown menu and select **Expression**.
- Select **Use the expression builder** 5.

The Expression builder panel is displayed.

This panel can be used to write custom expressions that transform or combine attributes, such as:

- Concatenating first and last names
- Formatting email addresses, or
- Applying conditional logic.

The available functions, such as `Join()`, `Append()`, and `Replace()`, and operators can be used to build expressions.

For more information regarding writing custom expressions, refer to [Reference for writing expressions for attribute mappings in Microsoft Entra Application Provisioning](#).

Using Expression builder

This section provides an example showing how Expression builder can be used to customise the `userName` attribute, by joining the `employeeId` attribute to the `@lseg.com` domain.

To do this:

1. From the **Select a function** dropdown menu, choose the **Join** function **6**.

This is used to join the `employeeId` attribute with the `@lseg.com` domain and must be defined using the structure⁸ shown in the Expression input panel **8**.

2. Click the **Add expression** button **7**.

The expression syntax is generated in the Expression input panel, on the right-hand side **8**.

3. To choose a user on whom to test the expression, in the Test connection section **9** of the Expression builder panel (see the previous page):

- i. Select the **Search user** radio button **10**.
- ii. In the field below **11**, start typing the name of the user. Matching names appear in a dropdown list.
- iii. Select the user⁹ you want to test from the list.
- iv. Click the **Test expression** button **12**.

The resulting output from the expression is shown in the View expression output field **13**.

The output – in this example, `x500014@lseg.com` – is the final custom attribute that SCIM receives from Entra. This attribute is crucial, as it is used to search against the Workspace User ID in LSEG.

4. Once you have successfully tested the expression, click the **Apply expression** button **14** (see previous page) at the bottom of the Expression builder panel.

⁸ When you start typing an attribute name, a list of matching attributes is shown, from which you can select the attribute you want. Static values, such as `@lseg.com`, are entered enclosed in quotation marks (for example, `"@lseg.com"`).

⁹ The selected user must contain the required attribute(s) used in the expression.

Provisioning users in the Entra admin portal

To provision users in the Entra admin portal:

1. Navigate to **Enterprise applications > All applications**, then search for and select your application.
2. Select **Manage > Users and groups** ①.
3. The Users and groups panel is displayed (see the example, opposite).
4. Click **Add user/group** ②.

The Add Assignment panel is displayed.

5. Click **None Selected**.

The Users and groups panel is displayed on the right side of the screen.

6. Choose the users you want to enable ③.
7. Once you have selected all applicable users, click the **Select** button, found at the bottom of the right hand panel.

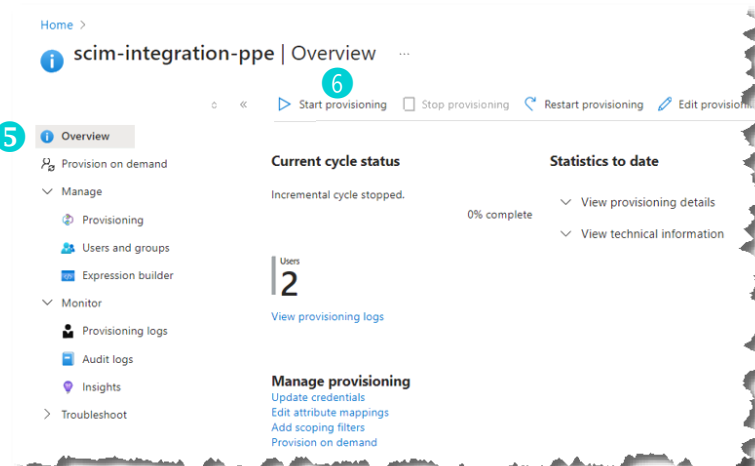
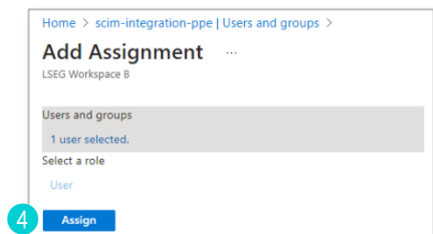
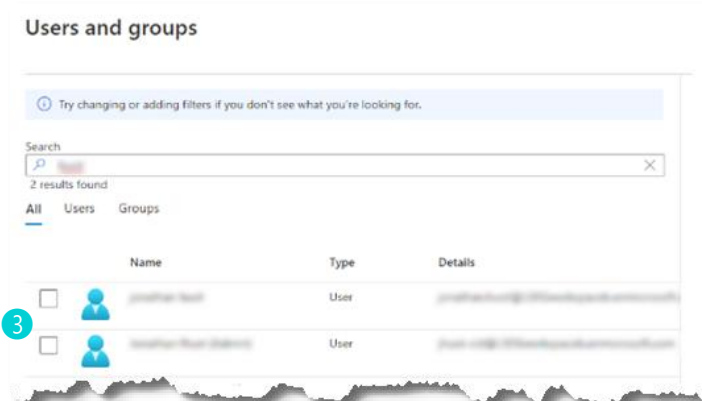
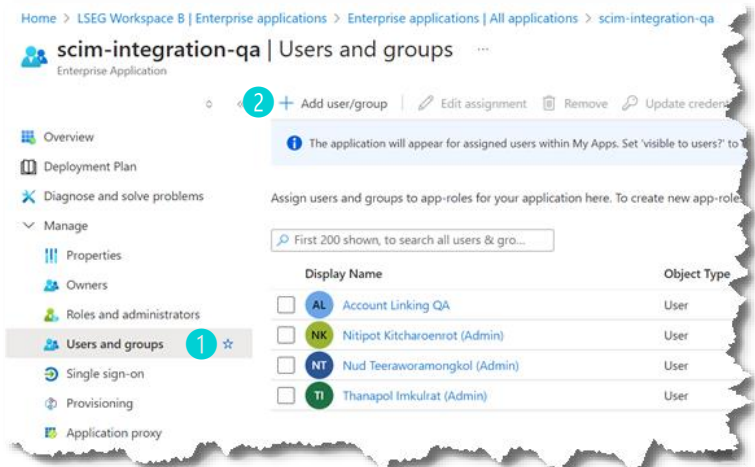
8. Click the **Assign** ④ button at the bottom of the left side panel.
A green tick will appear on screen, indicating successful assignment.

9. Return to the **Overview** panel ⑤.
10. To provision all the users that were selected in step 6, select **Start Provisioning** ⑥.

Once complete:

- **Current cycle status** displays **100 % complete**.
- Provisioned users now have their Microsoft and LSEG accounts linked and can authenticate into Workspace using Entra.

11. (Optional) To add more users, follow steps 1-7 in this section.



Accessing Workspace variants with LSEG credentials

Enabling Entra authentication for Web and OpenFin users does not affect their access to the desktop variant of Workspace. Versions 1.23-1.25 are still accessible using their dedicated authentication.

Whilst being enabled for Entra access, users can also access Workspace | Web using their LSEG issued credentials using the following URLs:

- <https://workspace.refinitiv.com/web>
- <https://workspace.extranet.refinitiv.biz/web>

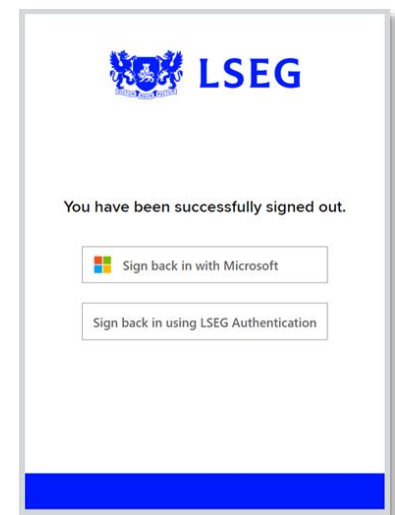
However, once users have logged in through Entra, they will continue to be automatically authenticated into Workspace through their Windows single sign on.

To revert to logging into Workspace using LSEG credentials, do the following:

1. Select WS > **Sign Out** ①.



2. In the resulting panel, select the **Sign back in using LSEG Authentication** button.



Useful links

For more information, click the below links.

- [Quickstart: Add an enterprise application](#)
- [Microsoft Entra on-premises application provisioning to SCIM-enabled apps](#)
- [What is automated app user provisioning in Microsoft Entra ID - Microsoft Entra ID | Microsoft Learn](#)
- [Plan a Microsoft Entra Conditional Access deployment - Microsoft Entra ID | Microsoft Learn](#)

© 2025 LSEG. Republication or redistribution of LSEG content, including by framing or similar means, is prohibited without the prior written consent of LSEG. LSEG is not liable for any errors or delays in LSEG content, or for any actions taken in reliance on such content. LSEG Data & Analytics logo is a trademark of LSEG and its affiliated companies.

lseg.com



LSEG DATA &
ANALYTICS