LSEG WORKSPACE
FINANCIAL MEETING PREP ADMINISTRATOR'S ACTIVATION GUIDE

Financial Meeting Prep is an AI-driven Microsoft® application that delivers reports on public companies. It is powered by LSEG® data and news and is easily accessible through Microsoft Teams.

LSEG Workspace users can download Financial Meeting Prep from the Microsoft Teams app store and access their Workspace data in Financial Meeting Prep.

Administrators should follow the instructions below to enable users in their organisation to access Workspace data in Financial Meeting Prep.

Pre-requisites

The pre-requisites for a customer accessing Workspace data in Financial Meeting Prep are:

− The user must have an LSEG Workspace account, and the Workspace User ID must be the same as the Microsoft Entra Email / Entra Principal Name.
− The customer must have an LSEG-granted licence (SCIM access) in place to perform tenant registration.
− The customer's administrator requires Workspace access and an administrator role to access Workspace admin tools.

ⓘ Current access to Workspace admin tools does not cover the tenant registration process; additional privileges are required.

Support

To request Workspace licenses, permissioning, and service issues, contact LSEG Support through MyAccount.

If you experience any problems performing the steps outlined in this document, raise an issue through MyAccount.

If your Workspace ID and Entra ID do not match, contact LSEG Support via MyAccount.

Enabling users to access Workspace data in Financial Meeting Prep

Enabling users to access Workspace data in Financial Meeting Prep involves performing the following steps:

− Accessing the Workspace admin tool
− Finding your Entra Tenant ID
− Registering your tenant in the Workspace admin tool
− Setting up the gallery app in the Entra admin portal
− Setting up attribute mappings
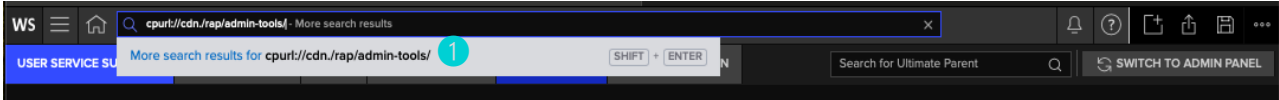− Provisioning users in the Entra admin portal

ⓘ This document also has a section containing Useful links.

Accessing the Workspace admin tool

To access the Workspace admin tool:

1. Log in to Workspace.
2. Either:
   - Navigate to admin tools, or
   - Enter **cpurl://cdn./rap/admin-tools/** into the Search bar. ❶
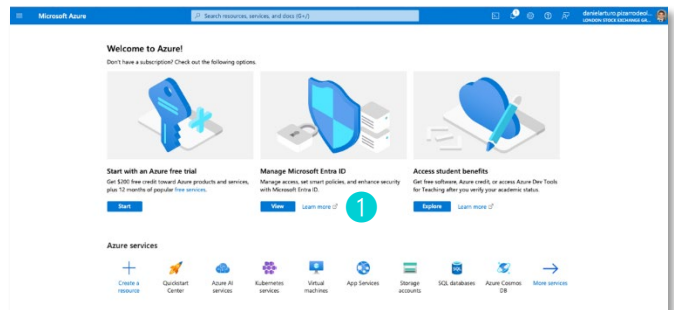

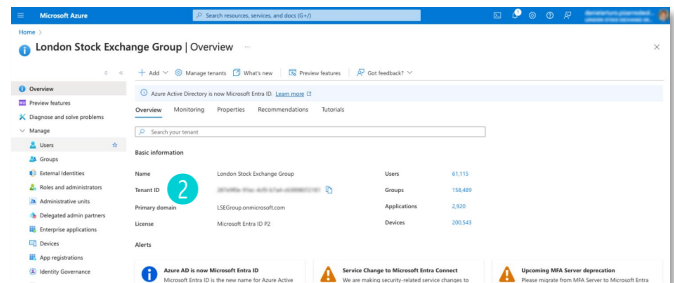The Workspace admin tool is launched.

Finding your Entra Tenant ID

Your Microsoft Entra Tenant ID is the authentication identification code for your organisation that is assigned by Microsoft. You will need this ID to register your tenant in the Workspace admin tool.

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** ❶ button.

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

Registering your tenant in the Workspace admin tool

To register your tenant in the Workspace admin tool:

1. On the SCIM INTEGRATION tab ❶, click **+ NEW TENANT**. ❷

2. Enter your organisation's Tenant Name and Tenant ID, and click **CREATE**.

3. When all the following tasks have been completed (denoted by a green check box), the setup has been successful.

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

4. Make a note of the Tenant URL ❸ and Secret Token ❹ that are generated and displayed.

ⓘ The Secret Token is valid for six months. To obtain another one after it has expired, you must re-link the Entra tenant to Workspace by generating a new Entra Secret Token using the steps described above.
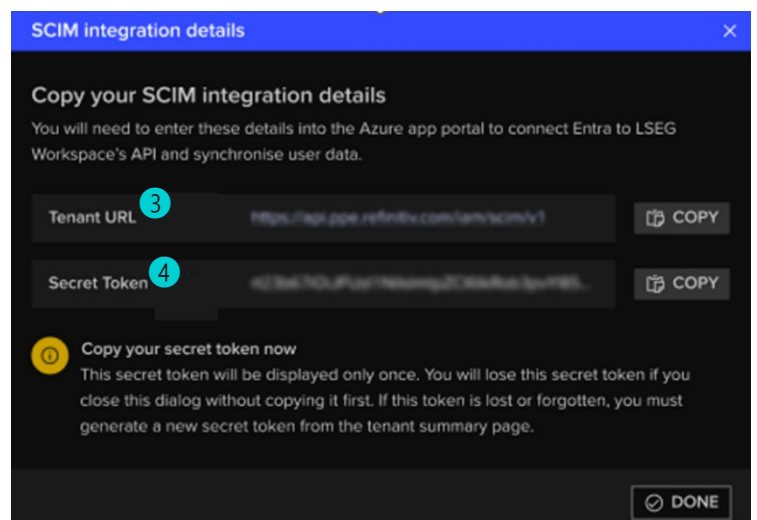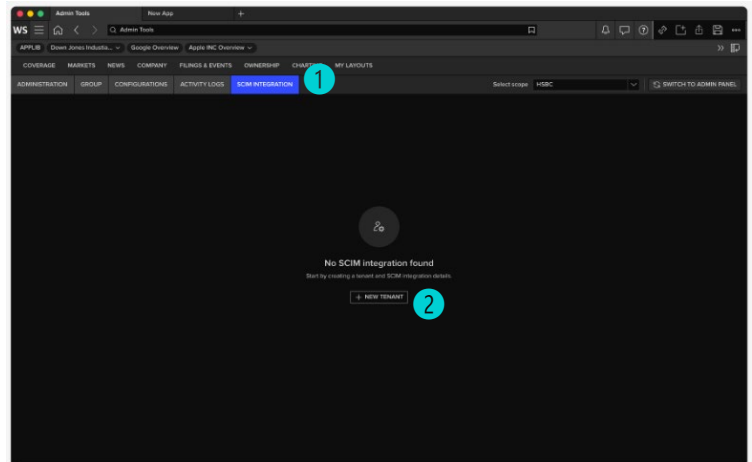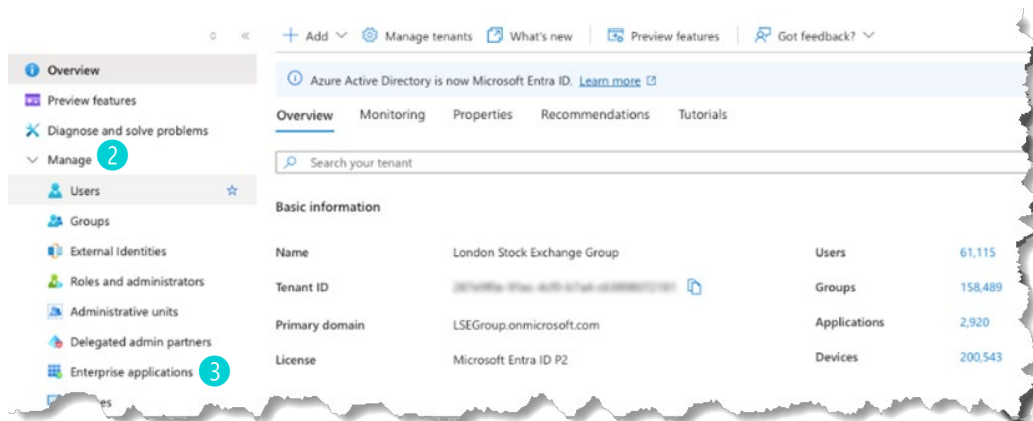
Setting up the gallery app in the Entra admin portal
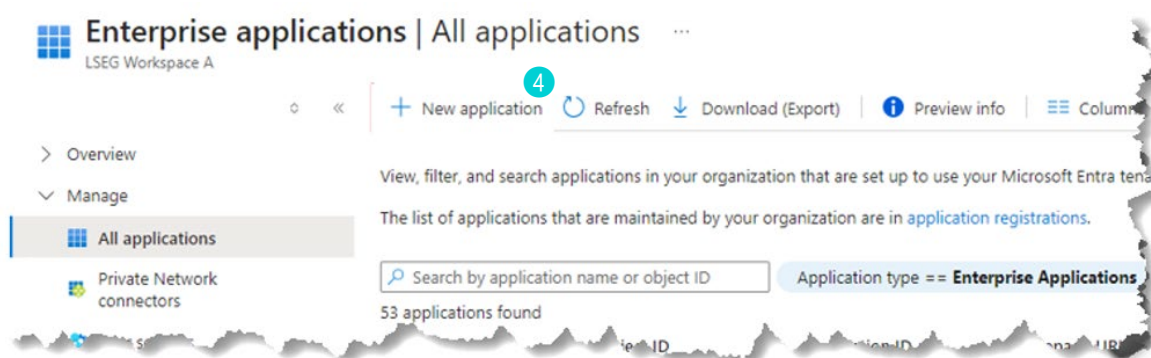
To set up the gallery app in the Entra admin portal:

1. Log in to https://portal.azure.com/#home.

2. Click the **Manage Microsoft Entra ID View** button. ❶
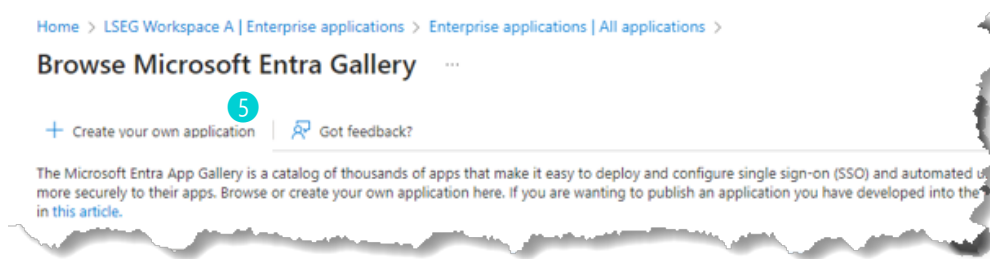
3. The Overview page opens.
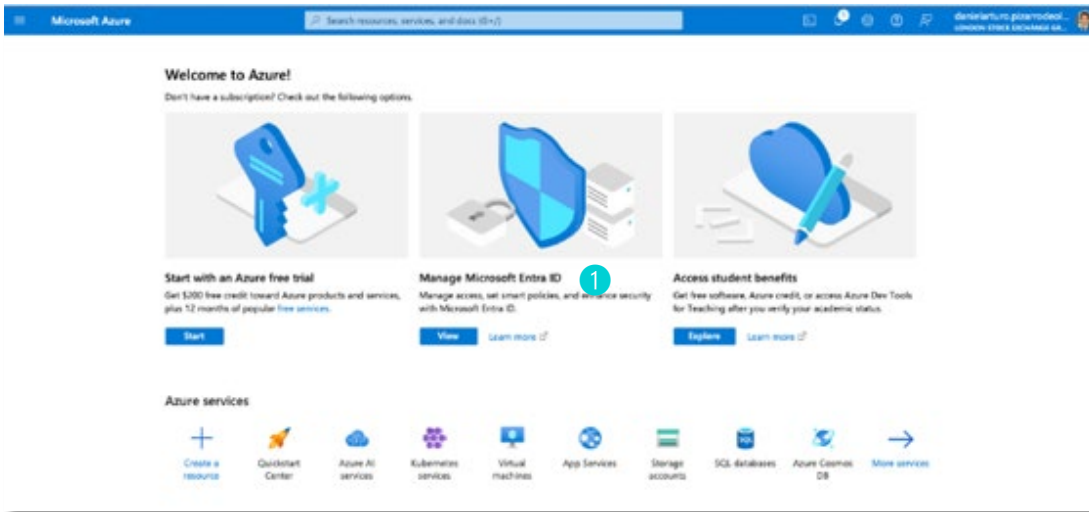
4. To open the menu, click the **Manage** ❷ menu item, and then click **Enterprise Applications**. ❸
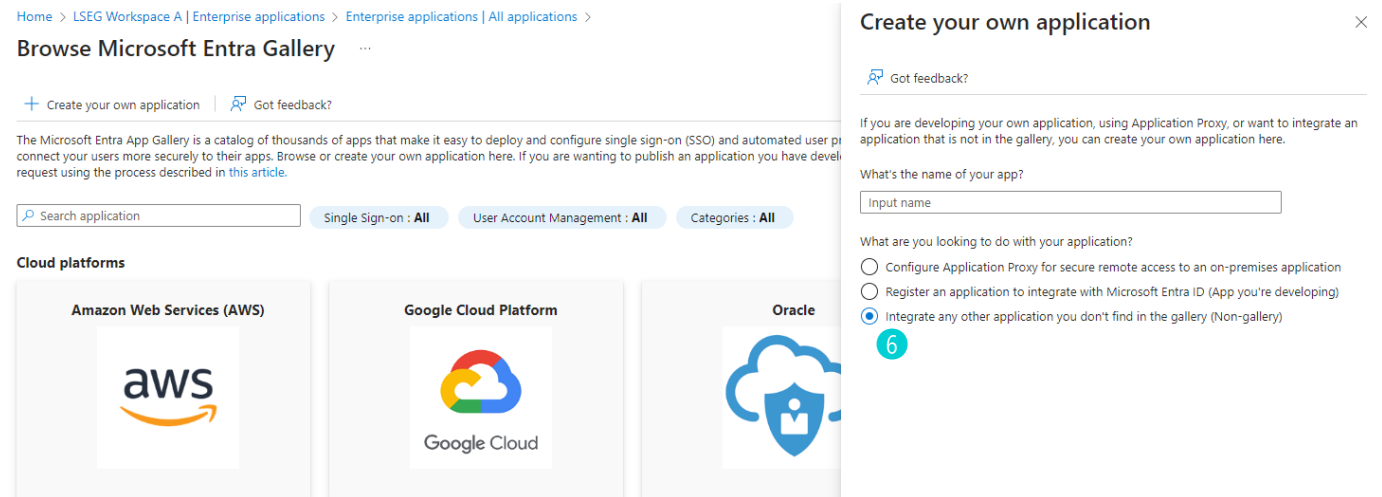

5. Select **New application** in the new page. ❹

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

7. In the resulting side panel, input LSEG SCIM as the app name and select **Integrate any other application you don't find in the gallery (non-gallery)**. ⑥

8. Click **Create**. A new page with the application overview will open.
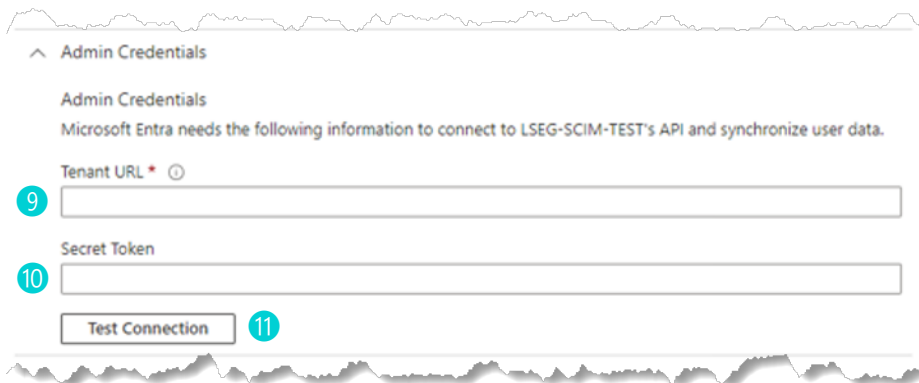
9. Click the **Provisioning** tab on the left-hand side of the screen.

10. Click **Get started** ⑦ on the new page or **Provisioning** ⑧ on the side panel.
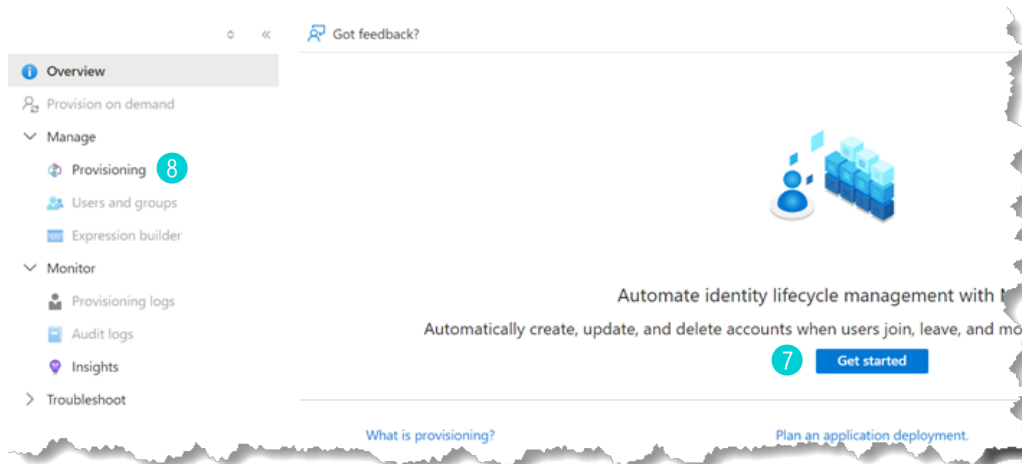
11. Select **Automatic** from the **Provisioning Mode** drop down list.

12. Enter **Tenant URL** (9) and **Secret Token** (10) obtained from Step 4 in Registering your tenant in the Workspace admin tool.

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to LSEG-SCIM-TEST's API and synchronize user data.

Tenant URL * ⓘ

(9)

Secret Token

(10)

[Test Connection] (11)

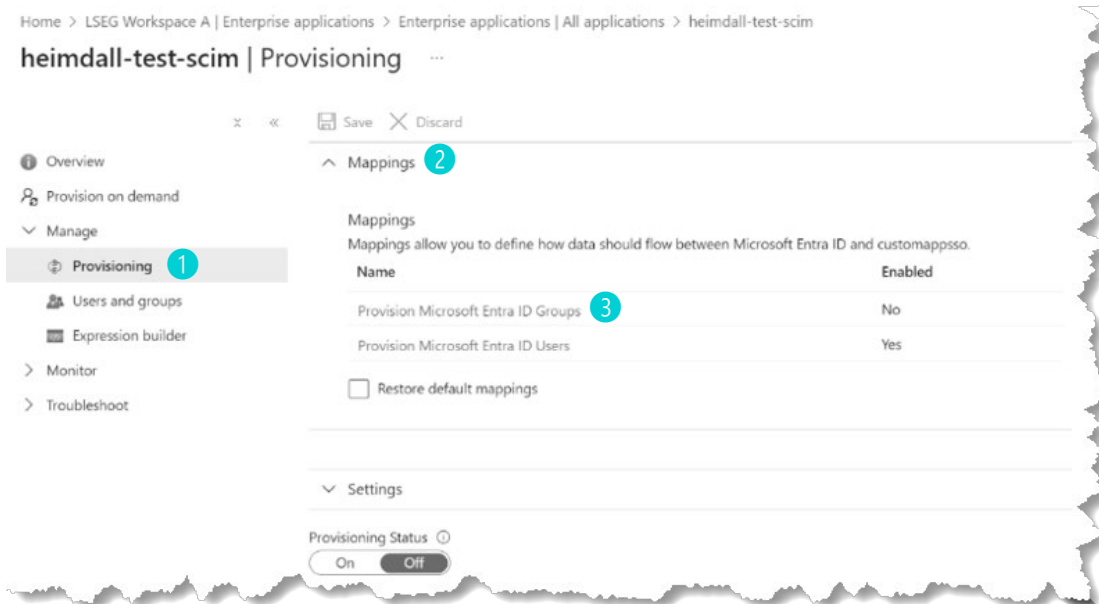ⓘ Ensure Provisioning Status is set to **Off**.

13. Click **Test Connection**. (11)

If successful, a green tick will appear on screen, which means that your app has successfully been registered.
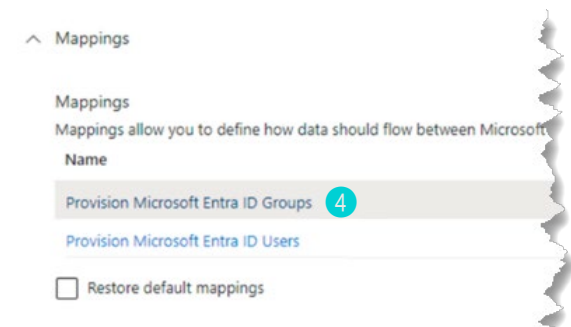
✓ Testing connection to temp-test   ✕

The supplied credentials are authorized to enable provisioning
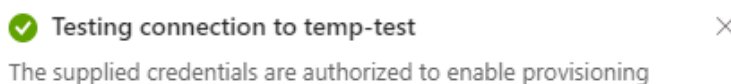
Setting up attribute mappings

To set up attribute mappings:

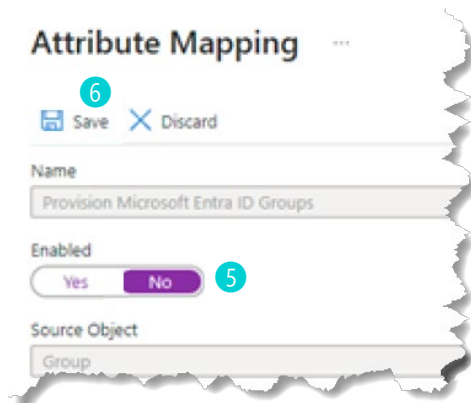1. Click **Manage** > **Provisioning**, (1) and expand the Mappings section. (2)

heimdall-test-scim | Provisioning ···

🖫 Save ✕ Discard

- Overview
- Provision on demand
- ∨ Manage
  - ⊕ Provisioning (1)
  - 🔳 Users and groups
  - 🔲 Expression builder
- > Monitor
- > Troubleshoot

∧ Mappings (2)

Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and customappsso.

Name	Enabled
Provision Microsoft Entra ID Groups (3)	No
Provision Microsoft Entra ID Users	Yes

☐ Restore default mappings

∨ Settings

Provisioning Status ⓘ

[On **Off**]

2. Click **Provision Microsoft Entra ID Groups**. (4)

∧ Mappings

Mappings

Mappings allow you to define how data should flow between Microsoft...

Name
Provision Microsoft Entra ID Groups (4)
Provision Microsoft Entra ID Users

☐ Restore default mappings

3. Under **Enabled**, select **No**. ⑤

4. Click **Save**. ⑥

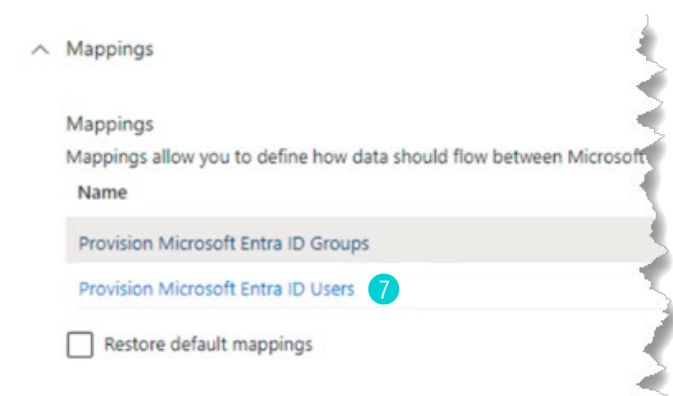**Attribute Mapping** ···

⑥ 🖫 Save ✕ Discard

Name

Provision Microsoft Entra ID Groups

Enabled

(Yes) [No] ⑤

Source Object

Group

ⓘ Note that group provisioning is not currently supported.

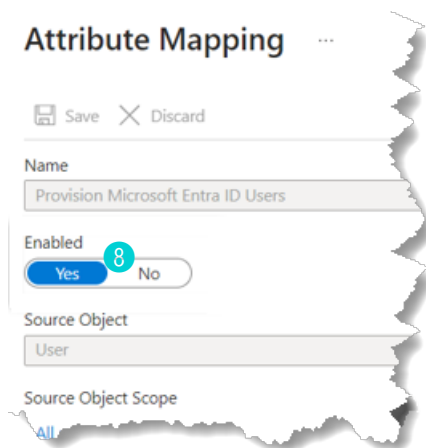5. Go back to the previous 'Provisioning' page and click **Provision Microsoft Entra ID Users**. ⑦

⌄ Mappings

Mappings

Mappings allow you to define how data should flow between Microsoft

Name

Provision Microsoft Entra ID Groups

Provision Microsoft Entra ID Users ⑦

☐ Restore default mappings

6. Under **Enabled**, select **Yes**. ⑧

Attribute Mapping ···

🖫 Save ✕ Discard

Name

Provision Microsoft Entra ID Users

Enabled

[Yes] ⑧ (No)

Source Object

User

Source Object Scope

All

7. In **Target Object Actions**, uncheck **Delete**.

ⓘ A user's Authentication, Authorization and Accounting (AAA) configuration will not be deleted, because they may have another configuration on other identity providers such as Ping.

8. Delete unused **Attribute Mappings** but keep:
   – userName
   – emails[type eq "work"]
   – name.givenName
   – name.familyName

9. Click **Add New Mapping**. 🔵9

Attribute Mappings
Attribute mappings define how attributes are synchronized between Microsoft Entra ID and customappsso

customappsso Attribute	Microsoft Entra ID Attribute
userName	userPrincipalName
emails[type eq "work"].value	mail
name.givenName	givenName
name.familyName	surname
externalId	objectId

Add New Mapping 🔵9

☐ Show advanced options

10. Select **objectId** as a **Source attribute** 🔵10 and **externalId** as a **Target attribute**. 🔵11

Edit Attribute ...

A mapping lets you define how the attributes in one class of Microsoft Entra object (e.g. Users) should flow to and from this application.

Mapping type ⓘ
[Direct ⌄]

Source attribute * ⓘ
[objectId 🔵10 ⌄]

Default value if null (optional) ⓘ
[   ]

Target attribute * ⓘ
[externalId 🔵11 ⌄]

Match objects using this attribute
[No ⌄]

Matching precedence ⓘ
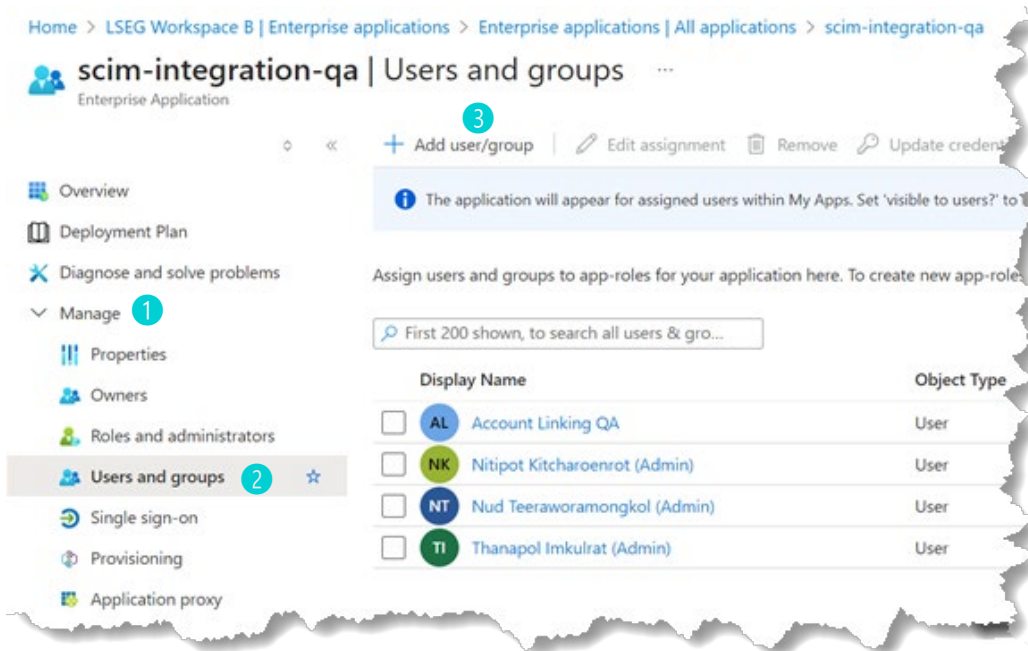[   ]

Apply this mapping ⓘ
[Always ⌄]

[Ok]

11. Click **Ok** to return to the previous page, then click **Save**.

Provisioning users in the Entra admin portal

To provision users in the Entra admin portal:

1. Click **Provisioning** in the left-hand panel.

2. Select **Manage** ❶ > **Users and groups**. ❷

3. On the resulting screen, select **Add user/group**. ❸

4. Click **None Selected** in the resulting Add Assignment screen. A new panel displays on the right side of the screen.

5. Choose the users you want to enable ❹ and click the **Select** button at the bottom of the right hand panel.
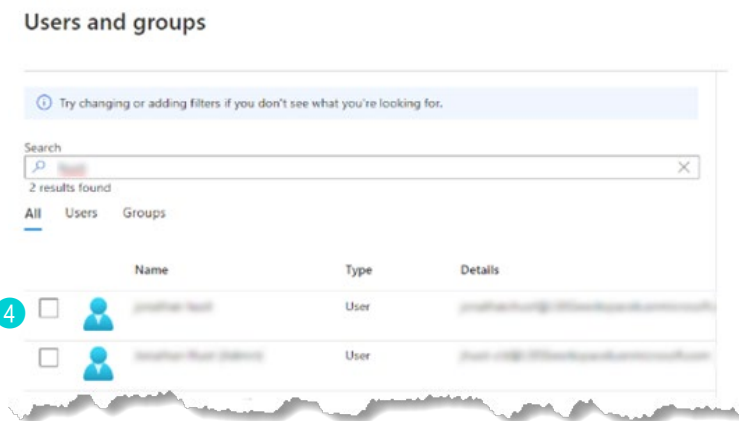
6. Click the **Assign** ❺ button at the bottom of the left side panel.

   A green tick will appear on screen indicating a successful assignment.
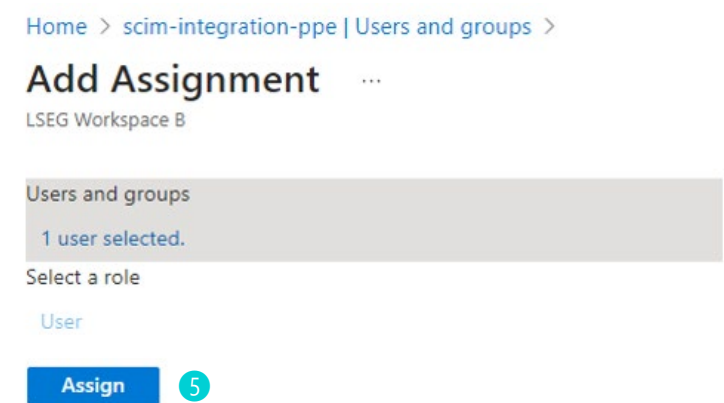
7. Navigate to the **Overview** option in the left side panel and select **Start Provisioning** ⑥ from the top of the page. This will provision all the users that have been added.
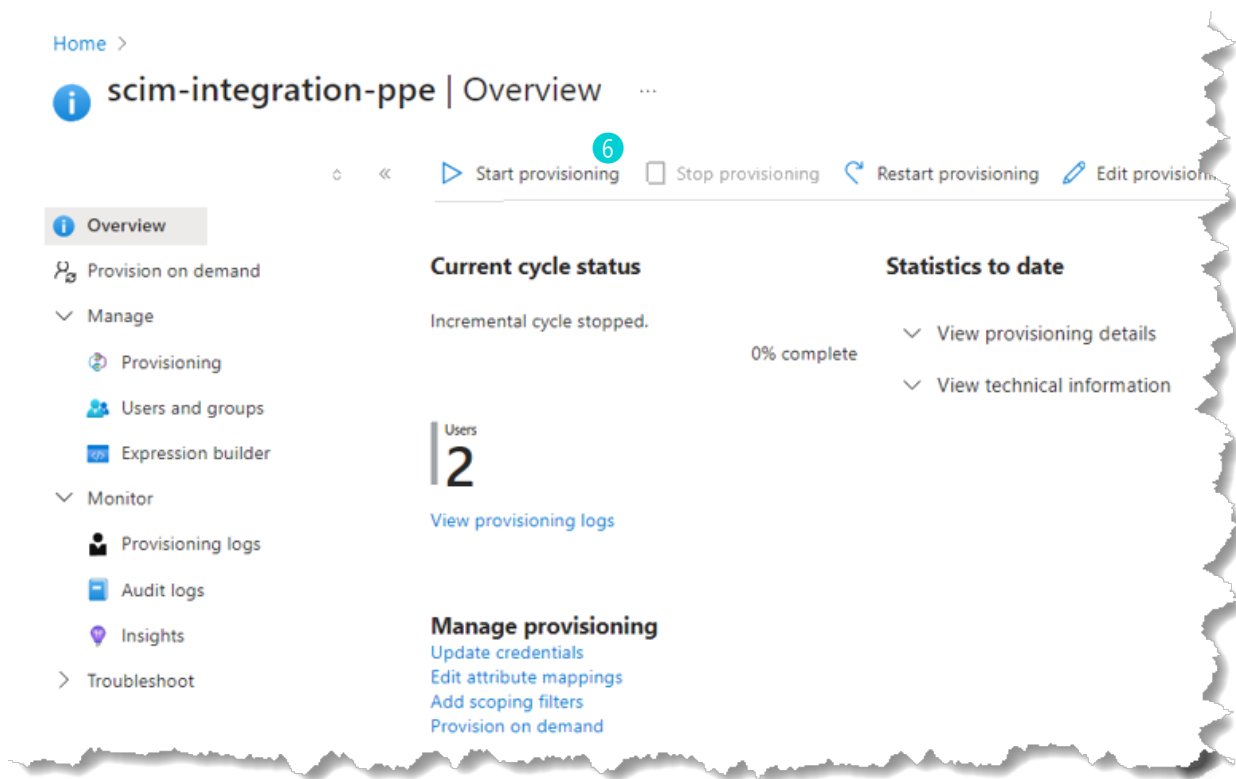
Once complete, the cycle status will display as '100 % complete'.

Useful links

For more information, click the below links.

- [Quickstart: Add an enterprise application](#)
- [Microsoft Entra on-premises application provisioning to SCIM-enabled apps](#)