Microsoft Entra ID Implementation Guide

Sign-in and automatic user provisioning

Prepared by Centro ASSIST

Version 5.4
October 2026

Material provided by Centro ASSIST as part of the service may not be retransmitted, reproduced or otherwise distributed or used in any form without the express written consent of Centro ASSIST.

© 2026 Holocentric Pty Ltd, trading as Centro ASSIST
ABN 73 052 972 095

Table of Contents

1 Introduction iii

1.1 What this guide covers iii

1.2 Before you start iii

1.3 The two Entra ID applications you will create iii

Part A: Microsoft Sign-In iv

2 Register the Centro ASSIST Application iv

3 Test the Microsoft Sign-In Option vi

3.1 Consent for Profile Access for your Entire Organisation vi

Part B: Automatic User Provisioning vii

4 Getting your Tenant URL and Secret Token vii

5 Create the Provisioning Application vii

6 Assign Who Gets a Centro Account viii

7 Connect Entra ID to Centro viii

8 Attribute Mappings ix

8.1 Required: change the externalId mapping ix

8.2 What syncs to Centro x

9 Start Provisioning x

10 Confirm It Worked xi

11 Key Considerations xi

11.1 Restricting users xi

11.2 What provisioning does and does not do xiii

11.3 Provisioning many people at once xiii

11.4 Deactivation disables, it does not delete xiii

11.5 If you use more than one provisioning system xiii

11.6 Existing Centro users and changes to sign-in addresses xiii

11.7 Notification email xiv

11.8 External (guest) users xiv

12 Troubleshooting xvii

Getting help xviii

1 Introduction

This guide has been prepared for Administrators to assist with connecting Microsoft Entra ID to your Centro web-app.

Note that you will need to liaise with the person within your organisation that has access to the Azure portal (usually the IT department) to carry out the steps below.

1.1 What this guide covers

This guide covers two features, set up in order:

Part A: Microsoft Sign-In	Lets your people sign in to Centro with their Microsoft account.
Part B: Automatic User Provisioning	Lets Entra ID create, update and disable Centro accounts for you. Adding someone to the right group in Entra ID gives them a Centro account, and removing them disables it.

Complete Part A before Part B. People created by provisioning do not have a Centro password, so they can only sign in with Microsoft. If Part A is not working, provisioning will look successful but nobody will be able to sign in.

If you only want Microsoft sign-in, complete Part A and stop there. You can add Part B later without redoing anything.

1.2 Before you start

You will need:

In Entra ID	The **Global Administrator** role, or **Application Administrator** with a **Privileged Role Administrator** for the consent in section 3.1.
In Entra ID	For Part B, to assign a group (section 6): a **Microsoft Entra ID P1 or P2** licence. Without one, assign people individually.
From Centro	The orgName for your organisation's Centro address, which the Centro team will provide.
From Centro	For Part B only: a **Tenant URL** and **Secret Token** (section 4).

1.3 The two Entra ID applications you will create

Part A and Part B each use their own application in Entra ID:

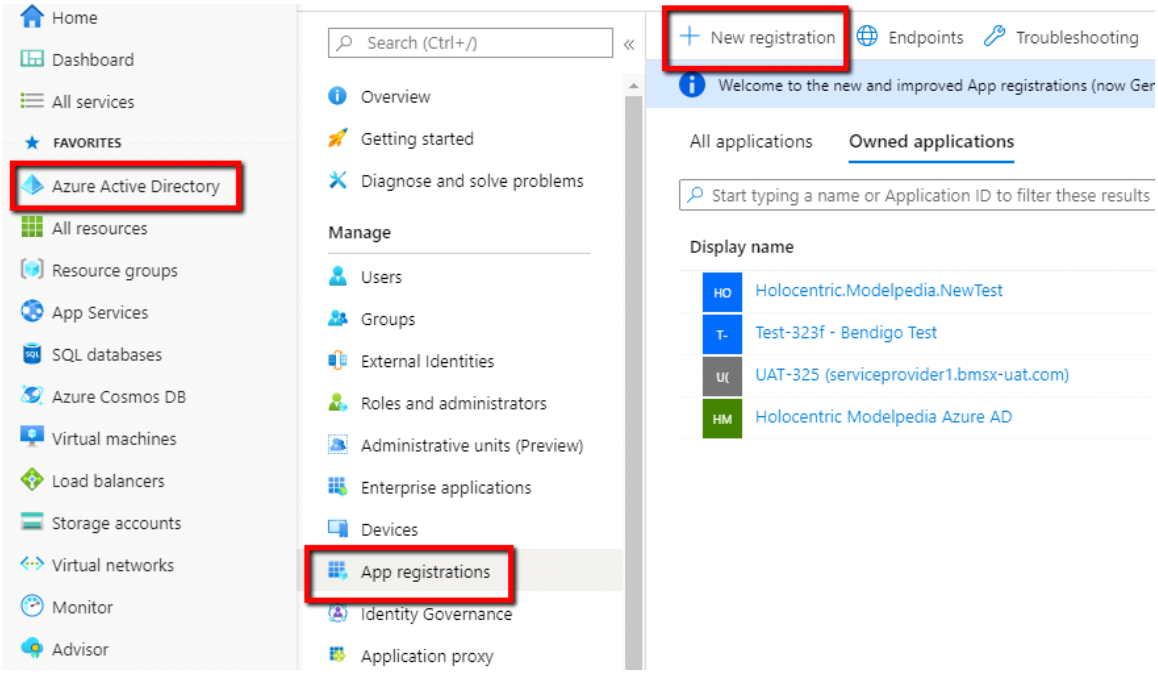
	Created in	Type	Purpose
Part A (section 2)	**App registrations**	Single-page application (SPA)	Lets your people sign in to Centro with Microsoft
Part B (section 5)	**Enterprise applications**	Non-gallery application	Lets Entra ID send user details to Centro

Both stay in place side by side, and one does not replace the other. Give them names that make the difference clear, for example Centro ASSIST and Centro ASSIST Provisioning.

Part A: Microsoft Sign-In

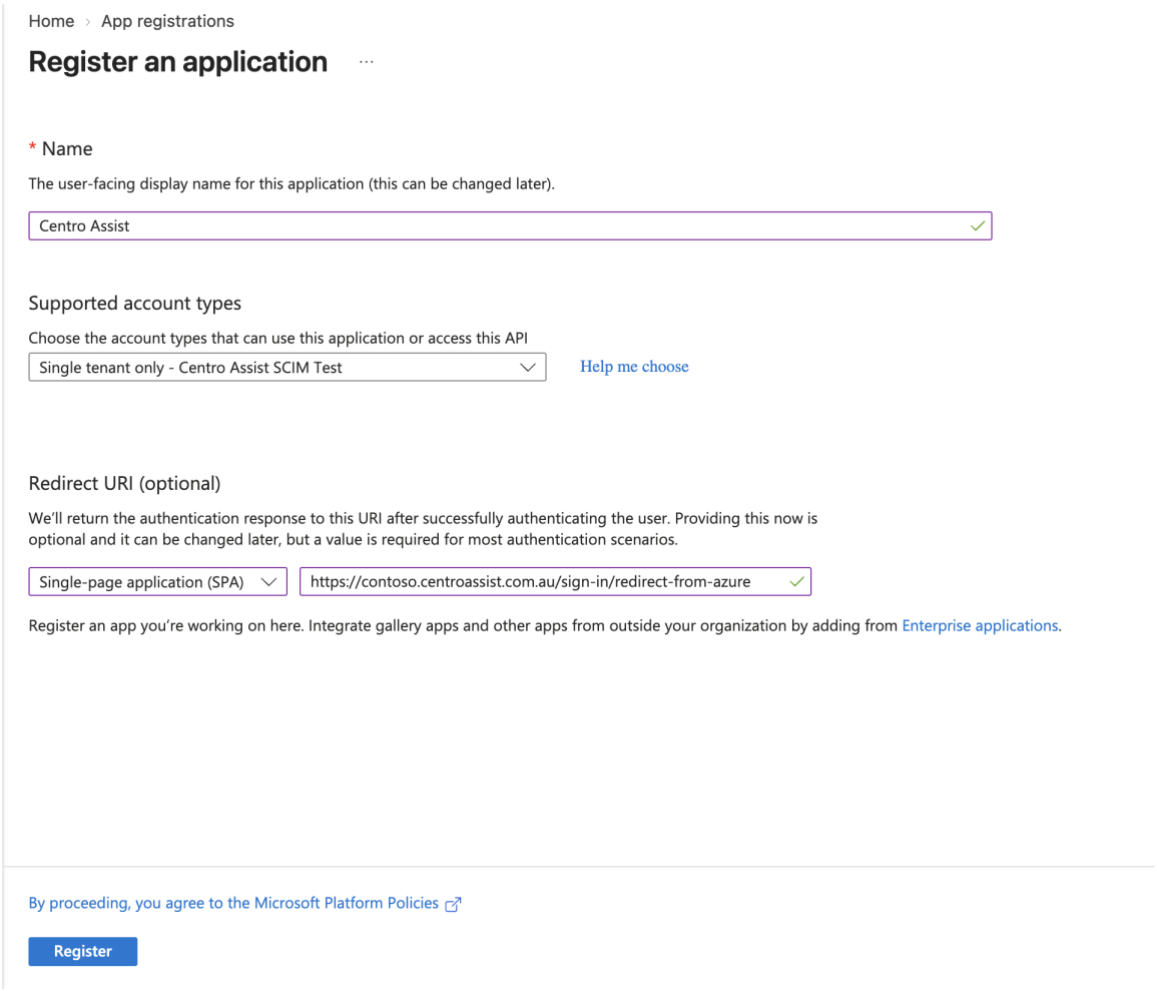
2 Register the Centro ASSIST Application

1. Sign in to the Microsoft Entra admin center or the Azure portal - either works and both reach the same place. Select **Microsoft Entra ID**, then **App registrations**, and click **New registration**.



2. In the following screen that appears, enter the information as follows:

Name	The name you want to give the Centro ASSIST application, for example Centro ASSIST.
Supported account types	Leave the default, **Single tenant only**.
Redirect URI	Select **Single-page application (SPA)** from the platform list, then enter https://orgName.centroassist.com.au/sign-in/redirect-from-azure, where orgName will be provided to you by the Centro team.



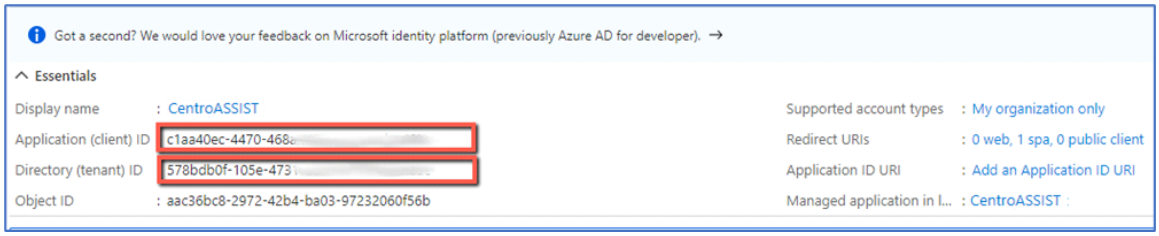
Click **Register**.

Once completed you will be returned to the Overview page of the Centro ASSIST application registration.

3. **Gathering the required items to configure Centro ASSIST**

On the Overview page you will need to record and provide the following items to the Centro team to complete the configuration:

- Application (client) ID
- Directory (tenant) ID



Navigate to the **Branding & Properties** section of the application registration.

Under **Home Page URL**, enter:

https://orgName.centroassist.com.au

(Replace orgName with the domain provided by the Centro team.)

Please also provide confirmation of the email sign-in domain. This is generally the primary domain hosted in Entra ID, or your email domain, for example yourcompany.com.au.

Once this information is provided to the Centro team, we will configure Microsoft sign-in as an option for your organisation.

---

3 Test the Microsoft Sign-In Option

Once the Centro team have confirmed your organisation is configured, navigate to the main page of your organisation sign-in (https://orgName.centroassist.com.au/) and verify that sign-in works for your users.

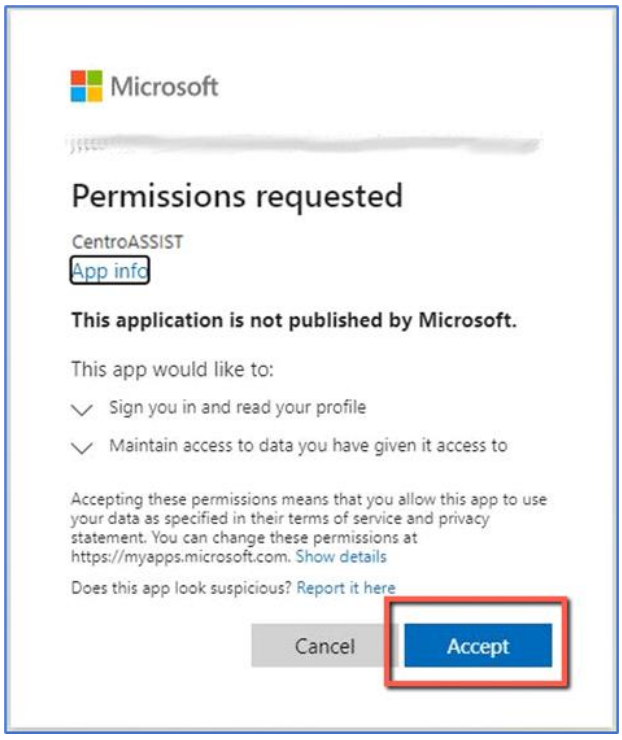
Note that if you would like users to sign in with both Microsoft and a Centro password, please let the Centro team know.

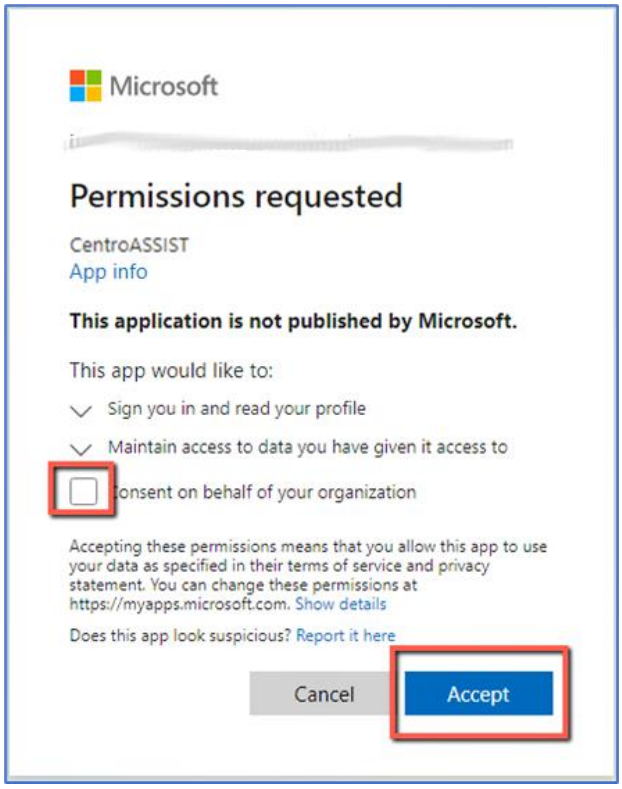
If you are continuing to Part B, make sure sign-in works before you go on.

3.1 Consent for Profile Access for your Entire Organisation

On the initial sign-in, your users will be presented with a consent notification. They will need to accept this to continue to the application. It will only happen on the initial sign-in.

A **Global Administrator** or **Privileged Role Administrator** can instead consent for everyone by ticking **Consent on behalf of your organization**. If **Assignment required** is on (section 11.1), this is required, because your users cannot consent themselves.





Part B: Automatic User Provisioning

4 Getting your Tenant URL and Secret Token

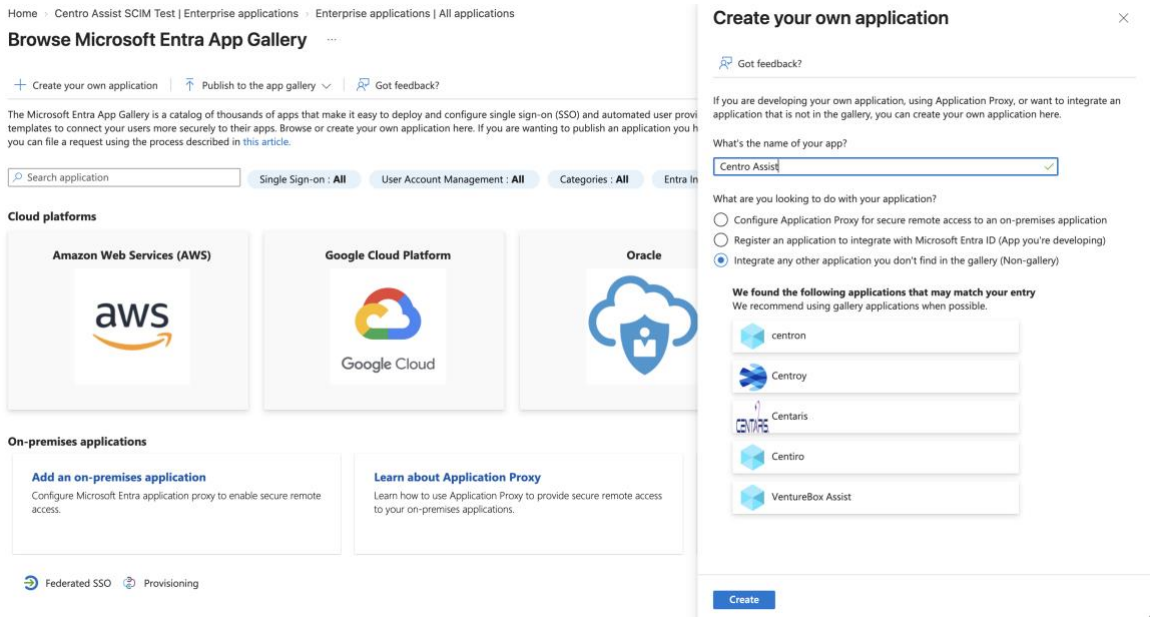
Entra ID connects to Centro using two values: a Tenant URL and a Secret Token. The Centro team creates these with you in a short setup session, so that the token goes straight into Entra ID and is never sent by email or chat. You will paste both into Entra ID in section 7.

The token does not expire. Keep it safe, as you would a password, because it can create and disable users in your Centro organisation. If it is ever exposed, contact Centro support to replace it.

5 Create the Provisioning Application

This is the second of the two applications described in section 1.3. It is separate from the sign-in application you created in section 2.

1. Sign in to the Azure portal or the Microsoft Entra admin center, and go to **Microsoft Entra ID**, then **Enterprise applications**.
2. Select **New application**, then **Create your own application**.
3. Enter a name, for example Centro ASSIST Provisioning.
4. Choose **Integrate any other application you don't find in the gallery (Non-gallery)**, then select **Create**.



6 Assign Who Gets a Centro Account

In the new application, open **Users and groups** and add the people who should have a Centro account.

We recommend adding a security group rather than individual people. Giving someone access to Centro is then simply a matter of adding them to the group. If you do not have a suitable group, create one under **Microsoft Entra ID** → **Groups** → **New group**, with the group type set to Security.

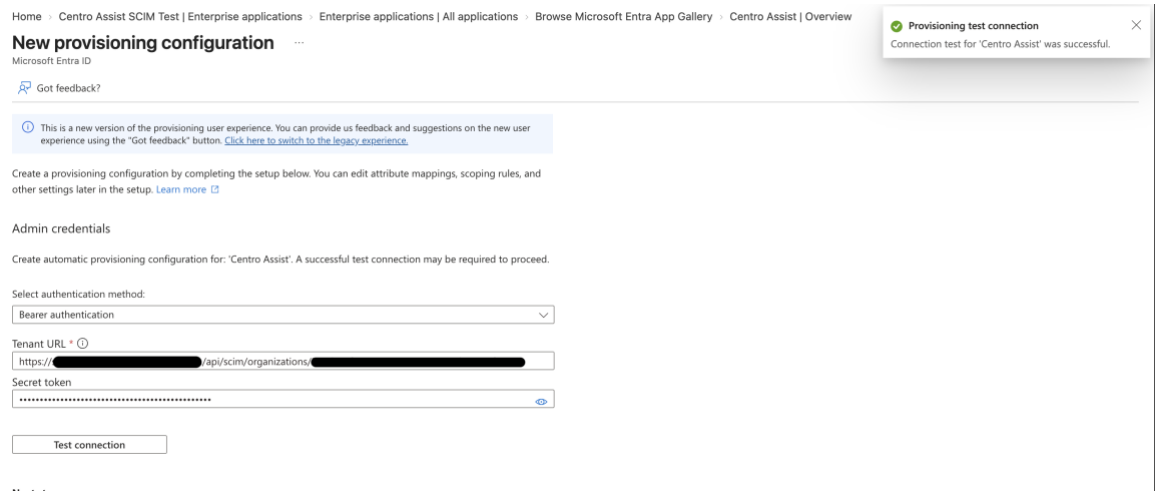
7 Connect Entra ID to Centro

1. In the provisioning application, open **Provisioning** and select **Connect your application**.
2. Enter the following:

Setting	Value
Tenant URL	Your Tenant URL from section 4. It will look like https://orgName.centroassist.com.au/api/scim/organizations/.../v2
Secret Token	Your Secret Token from section 4.

Paste both exactly as copied. Most connection problems come from an extra slash at the end of the Tenant URL, or a space before or after the token.

3. Select **Test Connection**. It should succeed within a few seconds.
4. Select **Create**.



If the test fails, see section 12 before going any further.

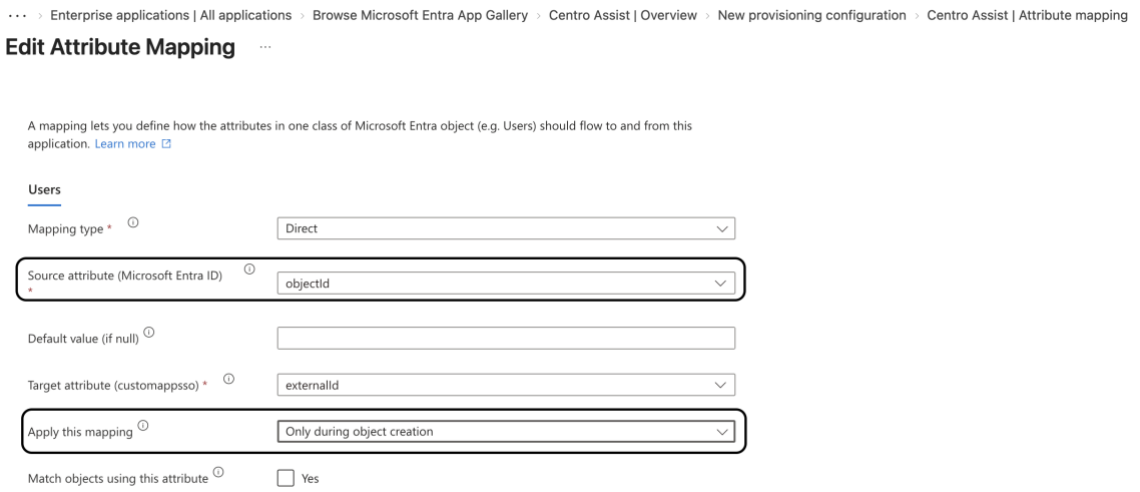
8 Attribute Mappings

Entra ID shows this step as optional, but Centro needs one change here.

8.1 Required: change the externalId mapping

Open **Attribute mapping**. On the **Users** tab, find the row whose target attribute is externalId (its source is mailNickname by default), select its pencil icon and change it to:

Setting	Value
Source attribute	objectId
Target attribute	externalId
Apply this mapping	Only during object creation



Centro uses externalId to recognise each person, so it must never change. The default source, mailNickname, can be edited in Entra ID, while objectId cannot. If the default is left in place, anyone whose mailNickname changes will stop syncing.

This is the only change you need to make, unless you invite external (guest) users (section 11.8). Leave everything else, including the Groups mapping, as it is.

8.2 What syncs to Centro

Entra ID's default setup sends more details than Centro uses. Centro keeps the ones below and ignores the rest, so there is no need to remove anything.

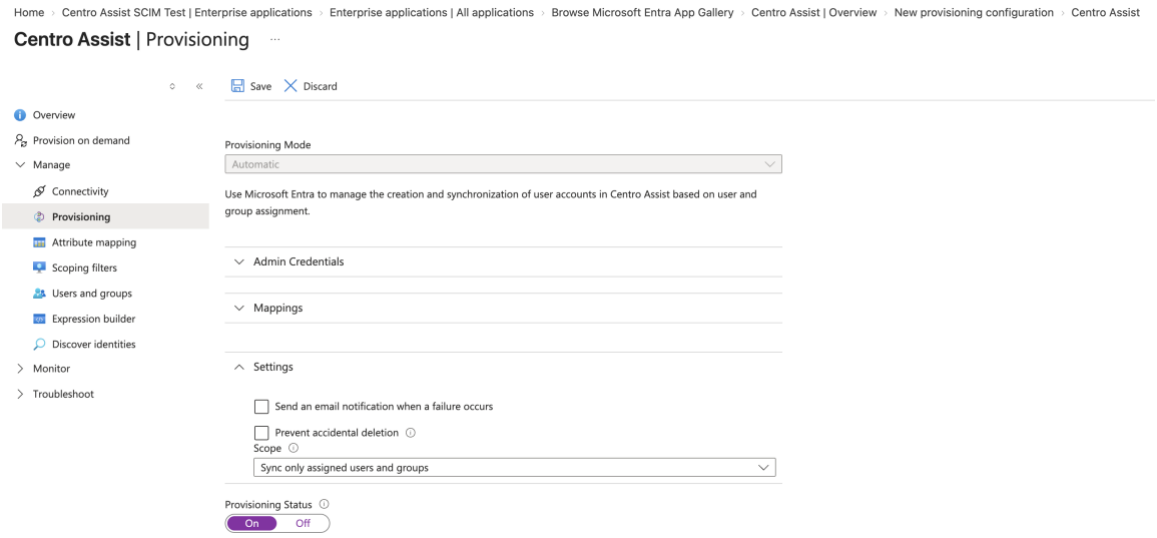
Centro detail	Entra ID source
Sign-in address	userPrincipalName (see section 11.6)
Account active or disabled	Whether the person is still assigned and allowed to sign in
Notification email	mail (see section 11.7)
Display name	displayName
First name	givenName
Last name	surname
Job title	jobTitle
Department	department
Work phone	telephoneNumber
Identifier	objectId (section 8.1)

If your people keep their phone number in Entra ID's Mobile phone field instead, edit the row whose target is phoneNumbers[type eq "work"].value and change its source to mobile.

9 Start Provisioning

In the provisioning application, open **Provisioning** under **Manage** in the left navigation.

1. Expand **Settings** and set **Scope** to **Sync only assigned users and groups**.
2. Set **Provisioning Status** to **On**.
3. Select **Save**.

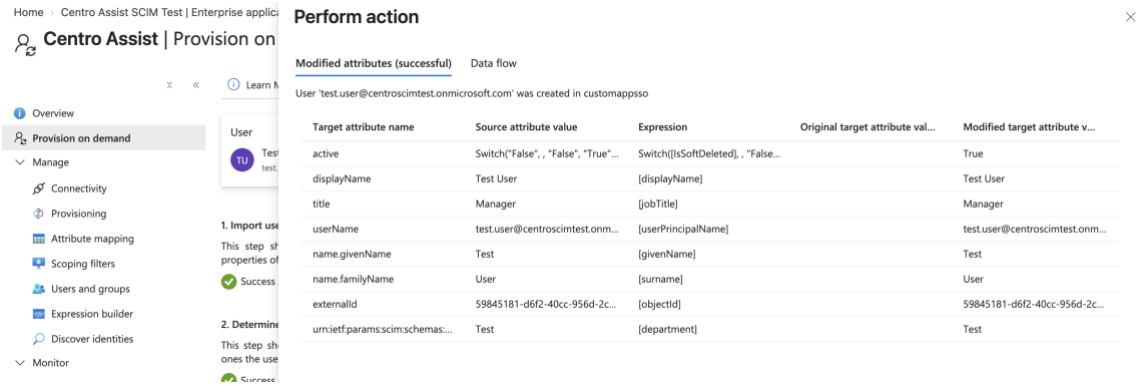


Entra ID will now create accounts for everyone assigned. The first run can take a while. After that, Entra ID checks for changes about every 40 minutes. When the first run has finished, the Overview page shows **Initial sync completed** under **Current cycle status**.

10 Confirm It Worked

Open **Provision on demand**, select one of the people you assigned, and run it. Entra ID should report success.

Choose a person rather than the group. Provision on demand works one person at a time, and selecting the group shows a message that Groups are not supported. That message does not mean anything is wrong with your setup.



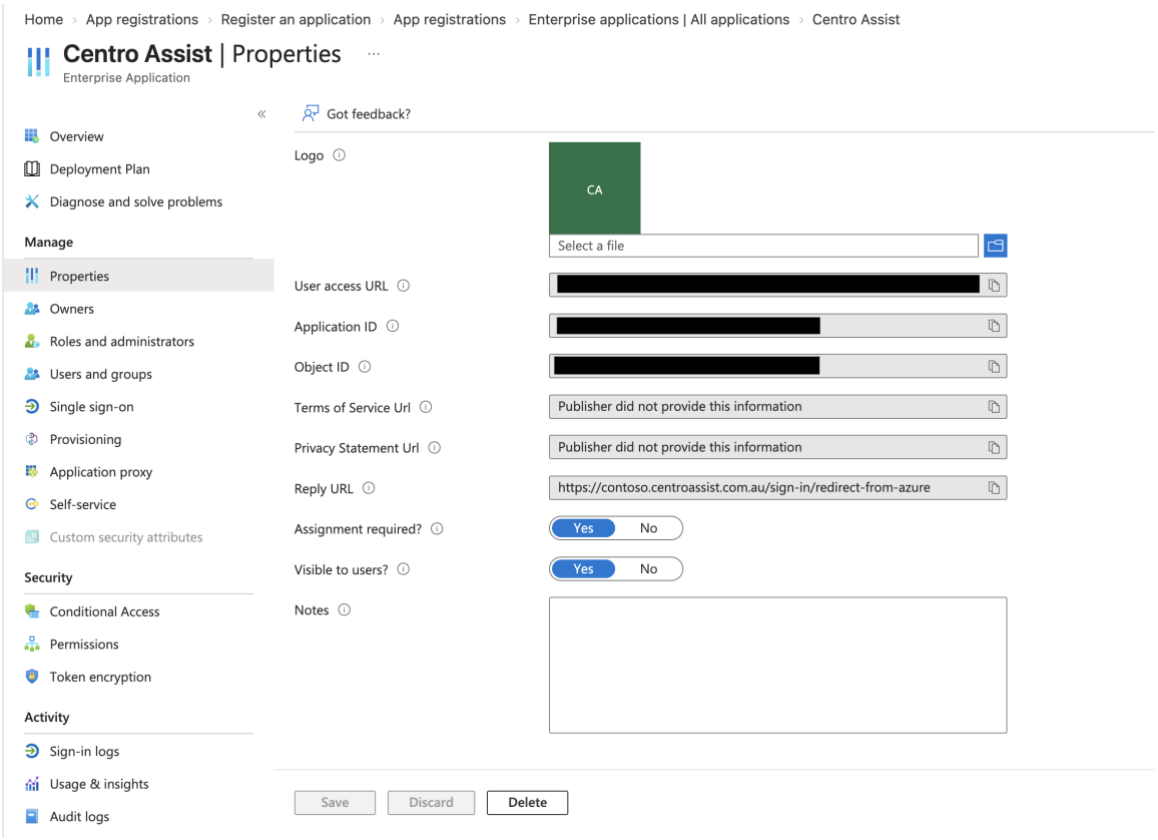
To check that the person has arrived in Centro, ask them to sign in to Centro with Microsoft, or ask Centro support to check for you.

---

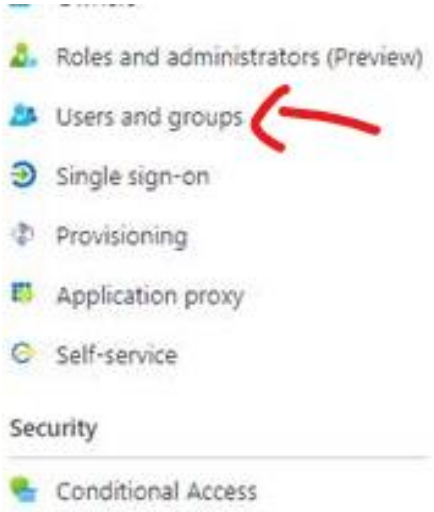
11 Key Considerations

11.1 Restricting users

To limit who can sign in to Centro ASSIST, in **Enterprise applications**, find the application, select **Properties** and set **Assignment required** to **Yes**.



On the left-hand side navigation bar, proceed to assign users and groups with access to the application.



Until this is set, anyone in your directory can sign in with Microsoft and get a Centro ASSIST account.

If you have also completed Part B, note that this applies to the sign-in application (for example Centro ASSIST), not the provisioning application from section 6. Each has its own list of assigned users.

11.2 What provisioning does and does not do

Provisioning creates accounts, keeps the details in section 8.2 up to date (except notification email, see section 11.7), disables accounts when access is removed, and re-enables them if access is restored.

It does not yet sync groups. The group you assigned in section 6 decides who gets an account, but Centro does not receive the group itself or use it to set roles. Entra ID will still try to send the group and Centro will decline it. Your users are not affected, but you will see a recurring error for the group in the provisioning log (see section 12).

Provisioning does not set roles or permissions either. These are managed in Centro in the usual way.

11.3 Provisioning many people at once

Provision on demand is for testing and for urgent one-off changes. To bring in many people, add them to the assigned group and wait for the next cycle, or select **Restart provisioning** on the Overview page to run one straight away.

11.4 Deactivation disables, it does not delete

When someone loses access in Entra ID, their Centro account is disabled, not deleted. They are signed out straight away and cannot sign in again, and their history stays in place for audit purposes. If their access is restored, the same account is re-enabled.

Removing someone from the assigned group and blocking their sign-in in Entra ID both have this effect.

Changes reach Centro on the next cycle, which can be up to about 40 minutes later. If someone must lose access immediately, remove them from the assigned group, then run **Provision on demand** for that person.

11.5 If you use more than one provisioning system

Each provisioning system needs its own credential, and each person should be covered by only one of them. If two systems cover the same person, Centro follows whichever updated them most recently, so one system can disable someone the other still expects to be active.

11.6 Existing Centro users and changes to sign-in addresses

If a person already has a Centro account under the same sign-in address as in Entra ID, provisioning updates that account rather than creating a second one. The first time they sign in with Microsoft, their Microsoft sign-in is linked to the account and their history is kept.

A person’s sign-in address cannot be changed by provisioning. If it changes in Entra ID, for example after a name change or a move to a new domain, that person will stop syncing and Entra ID will show an error for them. Everyone else is unaffected. Contact Centro support, who will update the account.

11.7 Notification email

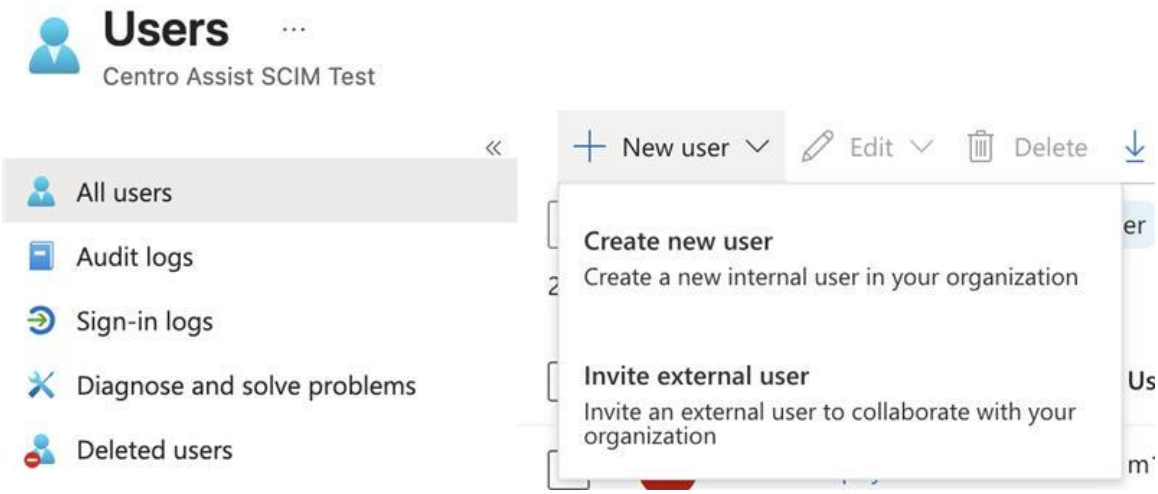
Centro sends its email notifications to each person's notification email address. Provisioning fills this in from the mail field in Entra ID when it is empty, but never replaces an address that is already set. If it is still empty when the person first signs in with Microsoft, their sign-in address is used.

To change someone's address, update it in Entra ID, then contact Centro support to switch to it.

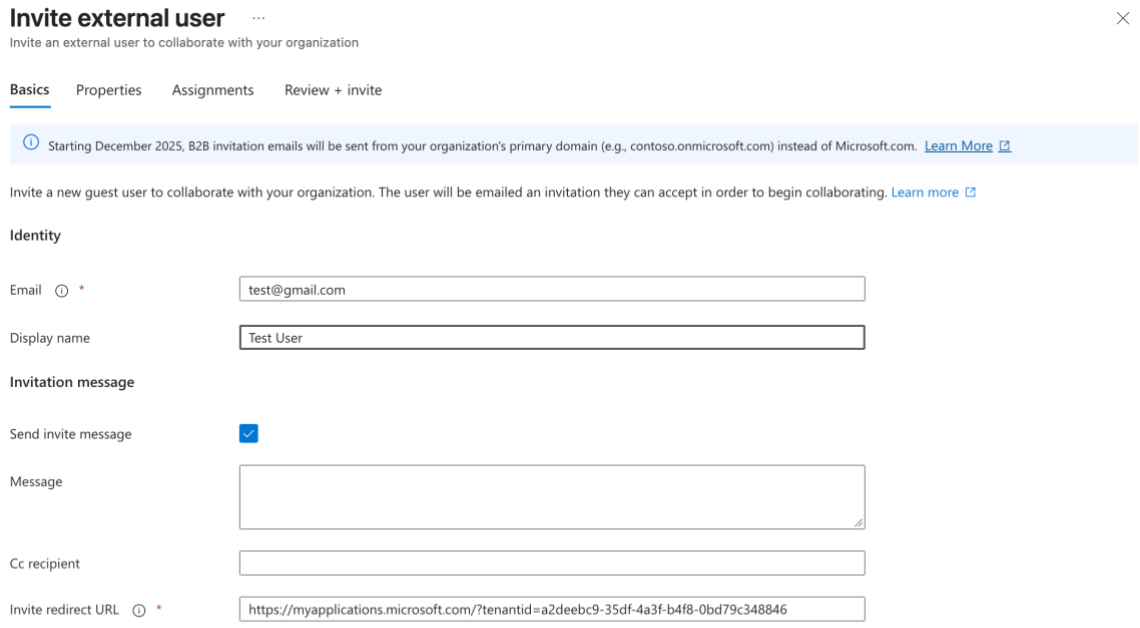
11.8 External (guest) users

People outside your organisation, for example with a Gmail address, can sign in to Centro ASSIST once you invite them to your directory as external (guest) users.

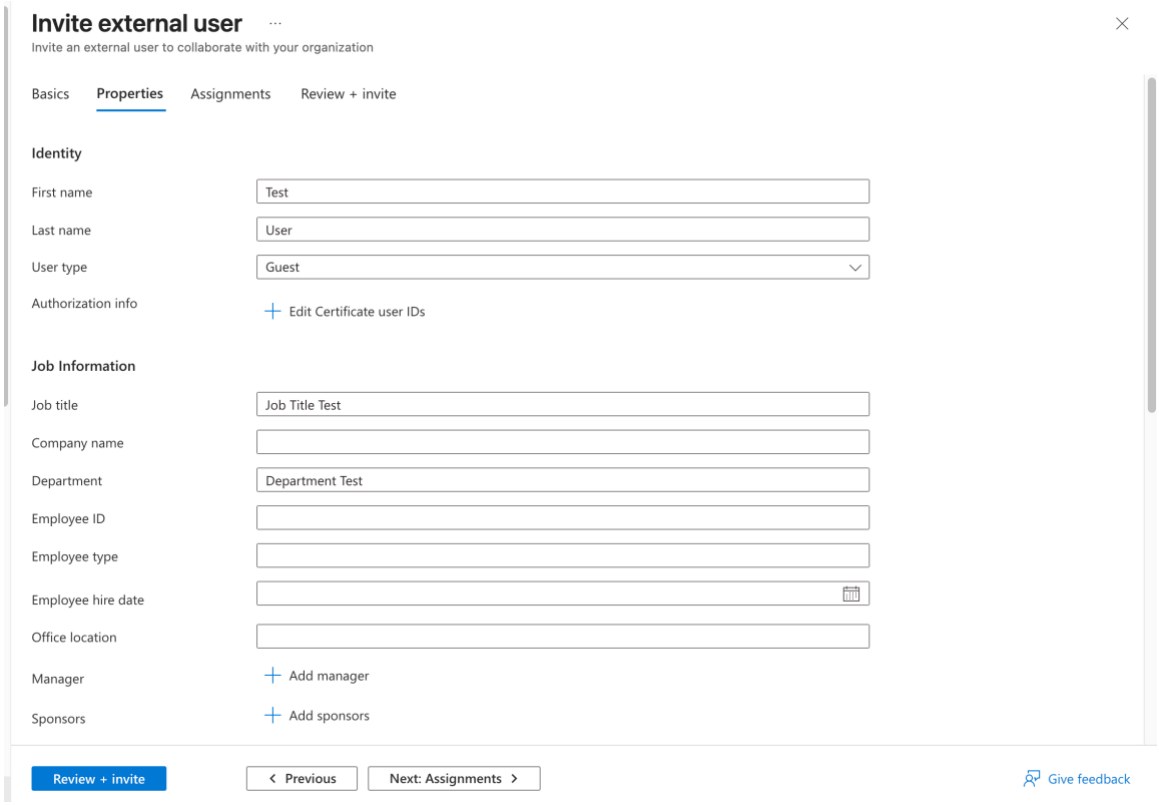
1. In **Users**, select **New user**, then **Invite external user**.



2. On the **Basics** tab, enter their **Email** and a **Display name**.

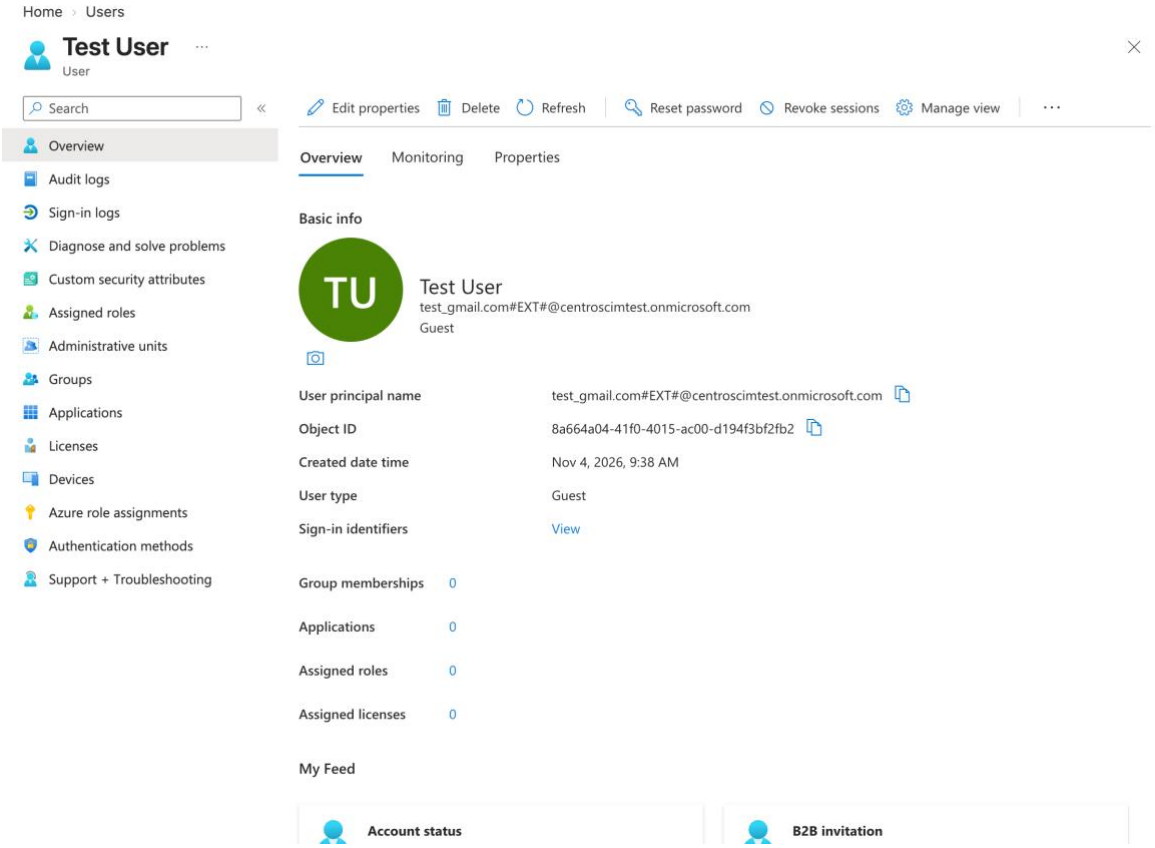


3. On the **Properties** tab, enter their **First name** and **Last name**.

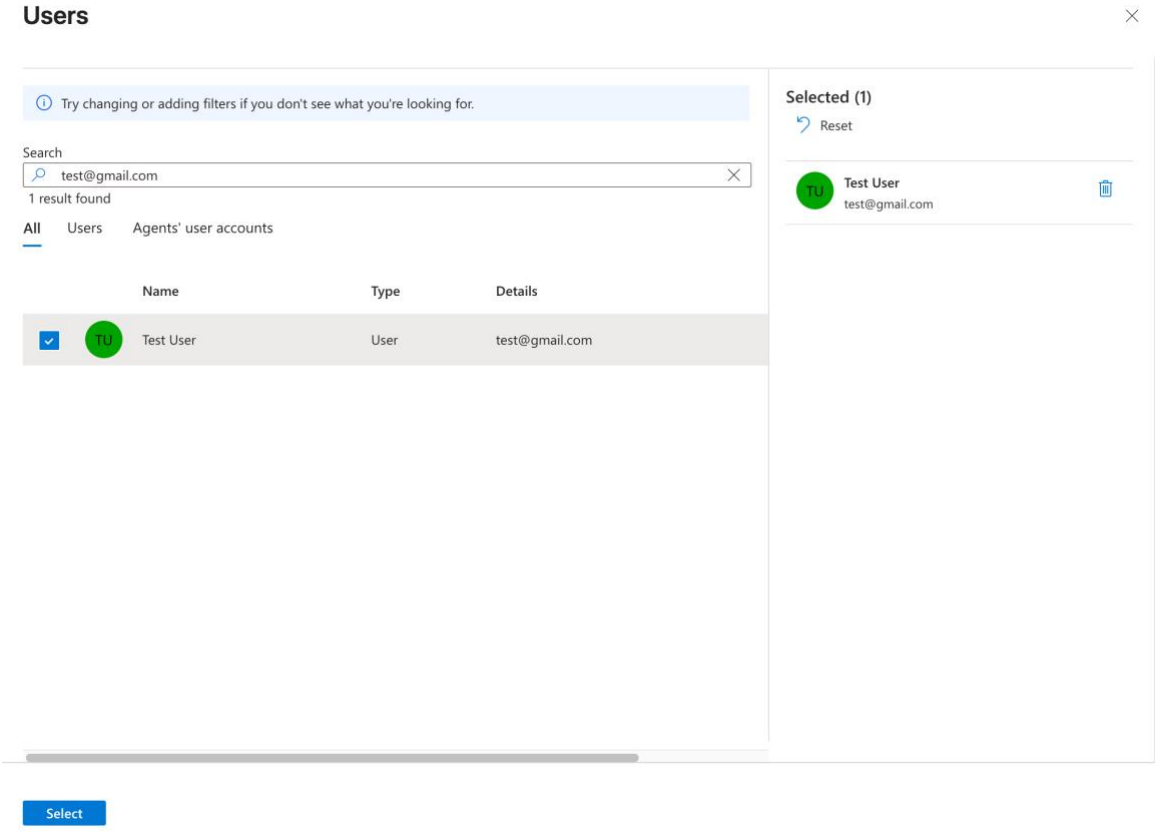


4. Select **Review + invite**, then **Invite**.

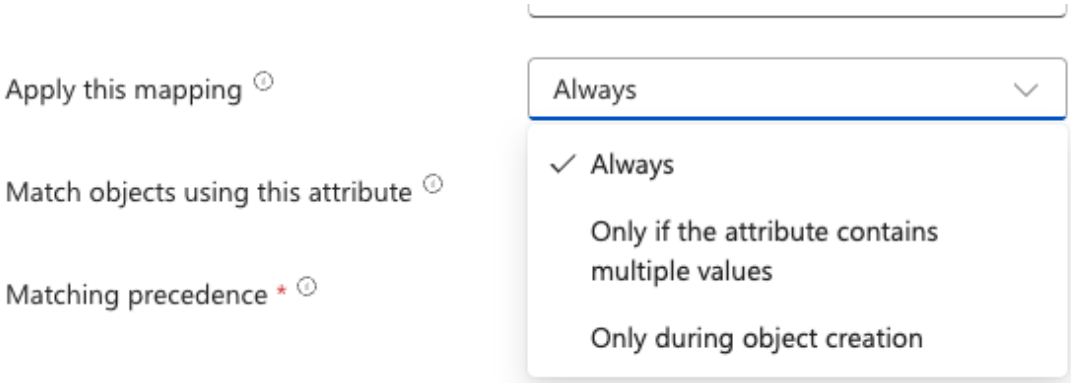
Entra ID gives the guest a sign-in name such as jane.doe_gmail.com#EXT#@yourcompany.onmicrosoft.com. This is expected.



5. If **Assignment required** is on (section 11.1), assign the guest to the Centro ASSIST application in **Users and groups**.



If you have also completed Part B, in **Attribute mapping**, set the userName row's **Apply this mapping** to **Only during object creation**, or updates to guests will fail.



12 Troubleshooting

Symptom	Likely cause and what to do
Test Connection fails	Check that the Tenant URL is your own (not the example in this guide), that it ends in /v2 with nothing after it, and that the token has no spaces before or after it. If it still fails, contact Centro support, as the token may have been replaced or revoked.
People are created but cannot sign in	Microsoft sign-in is probably not set up yet. People created by provisioning can only sign in with Microsoft. See section 1.1.
People are created but show as inactive in Centro	Your organisation has reached its user limit, so new people are saved as inactive. Contact Centro support.
A red "Provisioning errors" card on the Overview page, with a failed Create for your group every cycle	This is expected and nothing is wrong. Centro does not accept groups (section 11.2), and your users are syncing normally. If you would like the error gone, open **Attribute mapping**, switch to the legacy experience using the link in the banner, select **Provision Microsoft Entra ID Groups**, set **Enabled** to **No** and select **Save**. Keep the group assigned, as that is what decides who gets an account.
Provision on demand fails with "'Groups' is not supported", or suggests checking the tenant URL	The group was selected instead of a person. Choose a person and run it again. Your Tenant URL is fine.
One person shows an error mentioning externalId	The mapping in section 8.1 was not changed, and that person's mailNickname has changed.

Symptom	Likely cause and what to do
	Correct the mapping, then select **Restart provisioning**.
One person shows an error mentioning userName	Their sign-in address changed in Entra ID. Contact Centro support (section 11.6).
Someone who left could still sign in for a while	Changes reach Centro on the next cycle, up to about 40 minutes later. Remove them from the group and use **Provision on demand** for immediate effect (section 11.4).
Provisioning slows down or shows temporary errors during the first large sync	Centro limits how many provisioning requests it accepts at once, and Entra ID retries automatically. No action is needed.
Provisioning shows as quarantined	Note the error shown for the affected person and contact Centro support with it.
Nothing happens after provisioning is turned on	Check **Current cycle status** on the Overview page, as the first run can take a while. Make sure **Scope** is set to **Sync only assigned users and groups** and that the right people are assigned (section 6).
People can sign in who should not be able to	**Assignment required** is not turned on for the sign-in application. See section 11.1.

Getting help

Contact Centro support with your organisation name and, where relevant, the affected person's sign-in address and roughly when the problem started. If Entra ID shows an error for a specific person, the detail from that screen is the most useful thing you can send us.