

## Guide

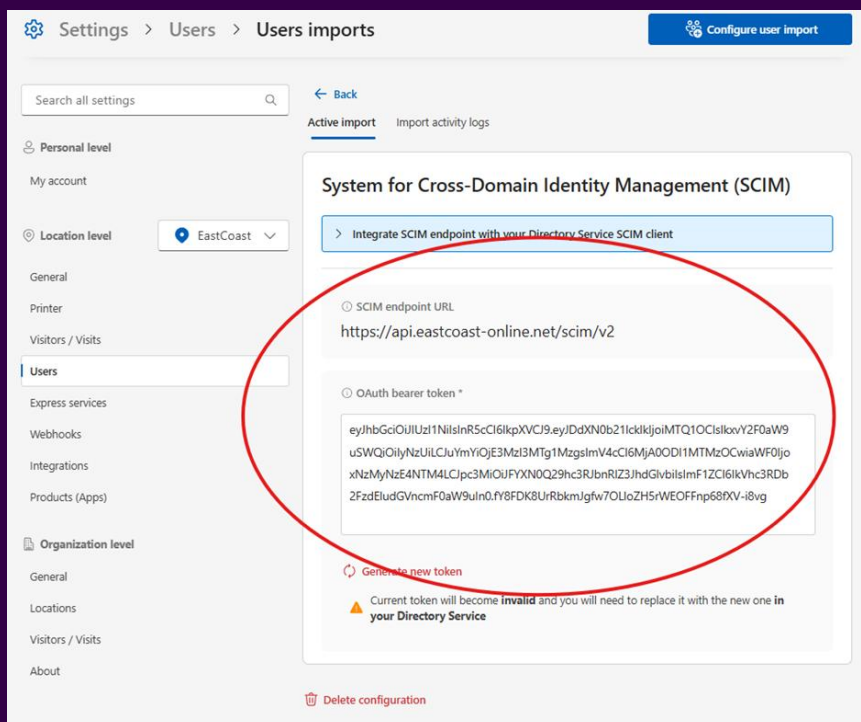
# Microsoft Entra ID SCIM Setup

To set up Microsoft Entra ID SCIM import, an Enterprise app is required in Entra ID. The data needed from Precise Visit setup are SCIM API URL and a Token, which all can be obtained from Settings-User import-SCIM page (Choose correct location that is relevant for the import.). Generate a Token and press “Save” button Unique SCIM setup is needed for each location if there are multiple locations in Precise Visit.

## Precise Visit Settings (Example)

Setup (2025-02-25)

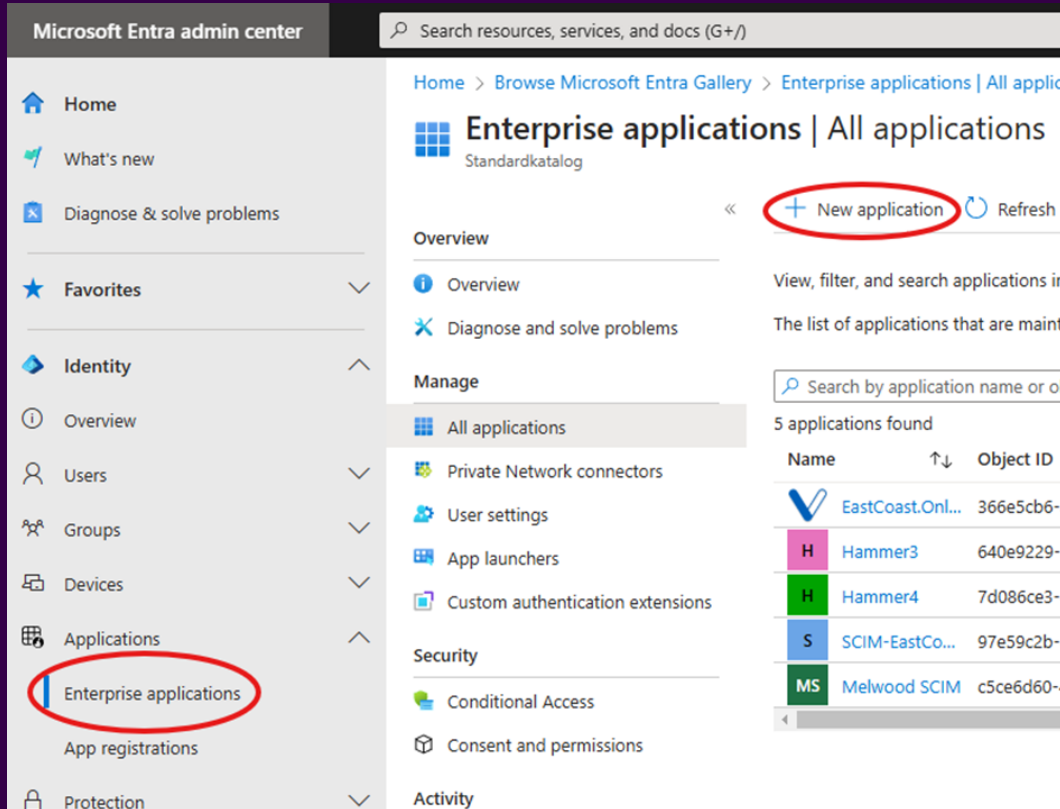
*Note: This is not a complete how-to-guide. Azure Portal views and setups tend to change quite frequently.*



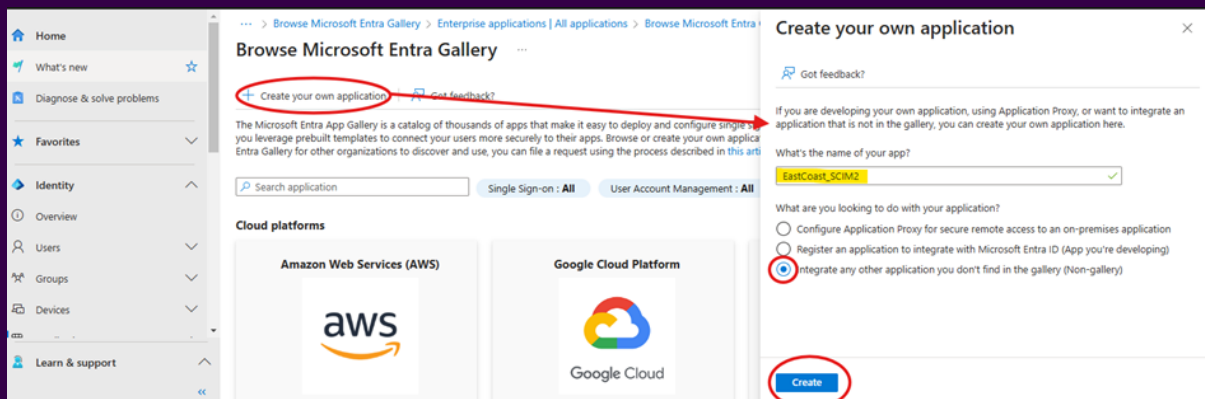
The screenshot shows the Microsoft Entra ID Settings page for 'Users imports'. The page is titled 'Settings > Users > Users imports' and includes a 'Configure user import' button. A search bar is present at the top left. The left sidebar shows navigation options: Personal level (My account), Location level (EastCoast), General (Printer, Visitors / Visits), Users (Express services, Webhooks, Integrations, Products (Apps)), and Organization level (General, Locations, Visitors / Visits, About). The main content area is titled 'System for Cross-Domain Identity Management (SCIM)' and contains a section for 'Integrate SCIM endpoint with your Directory Service SCIM client'. This section includes a 'SCIM endpoint URL' field with the value 'https://api.eastcoast-online.net/scim/v2' and an 'OAuth bearer token' field with a long alphanumeric string. A 'Generate new token' button is located below the token field, with a warning message: 'Current token will become invalid and you will need to replace it with the new one in your Directory Service'. A 'Delete configuration' button is at the bottom of the page.

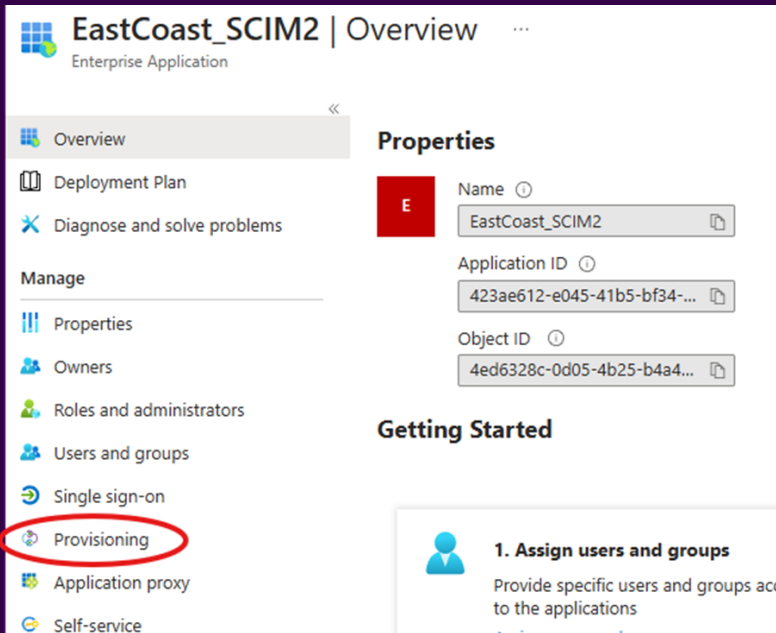
## Create an Enterprise Application

1. Navigate to Microsoft Entra ID > Enterprise application registrations and click “New application”.

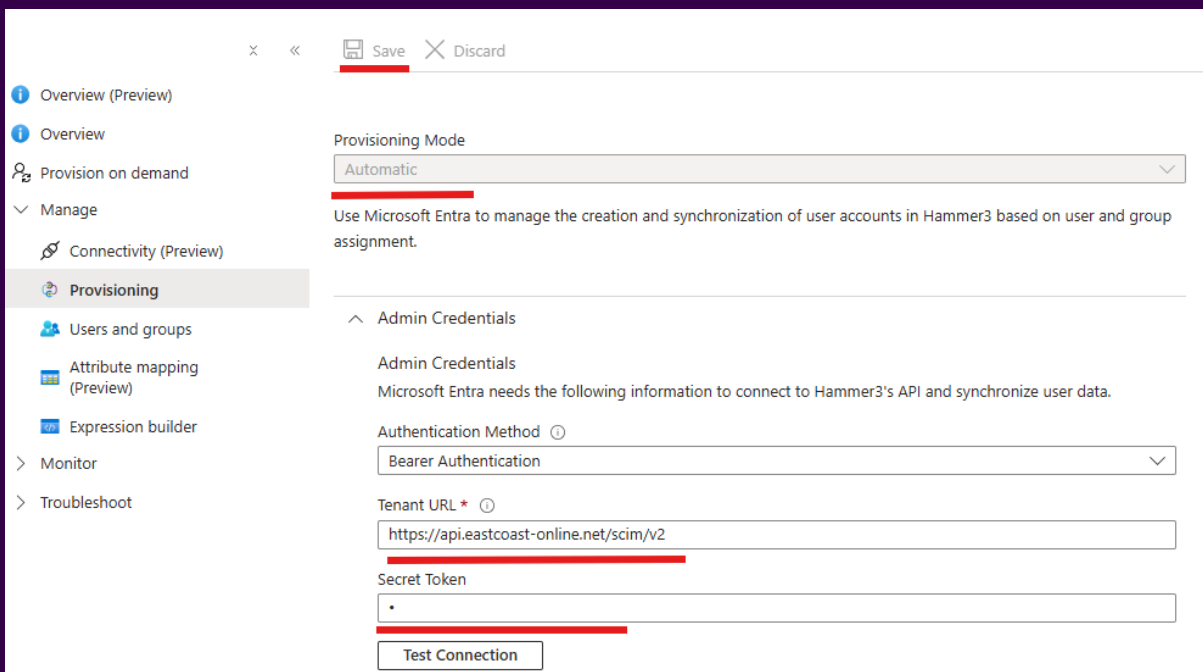


2. Click “Create your own application”. Enter a name for the application, select “Integrate...” and click Create

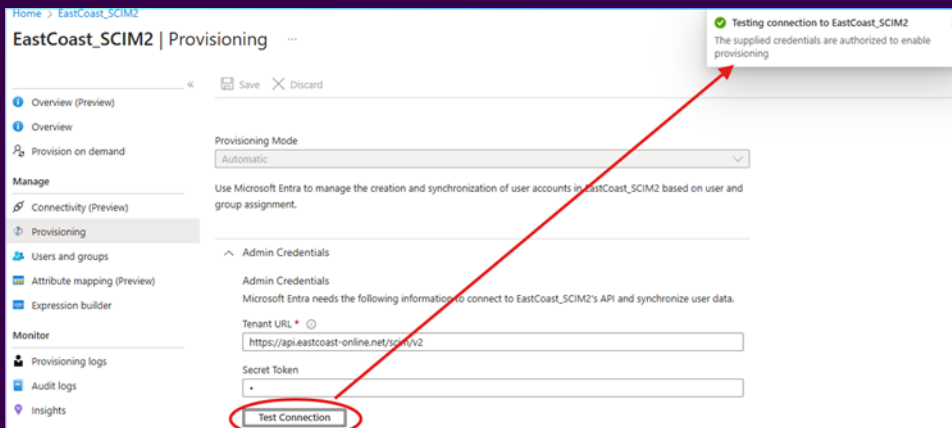




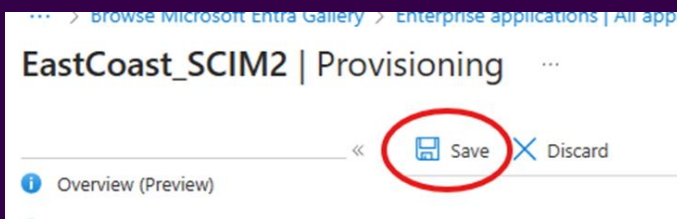
3. Choose “Automatic” under Provisioning Mode. Enter Tenant URL and Secret Token that you have copied from Precise Visit configuration



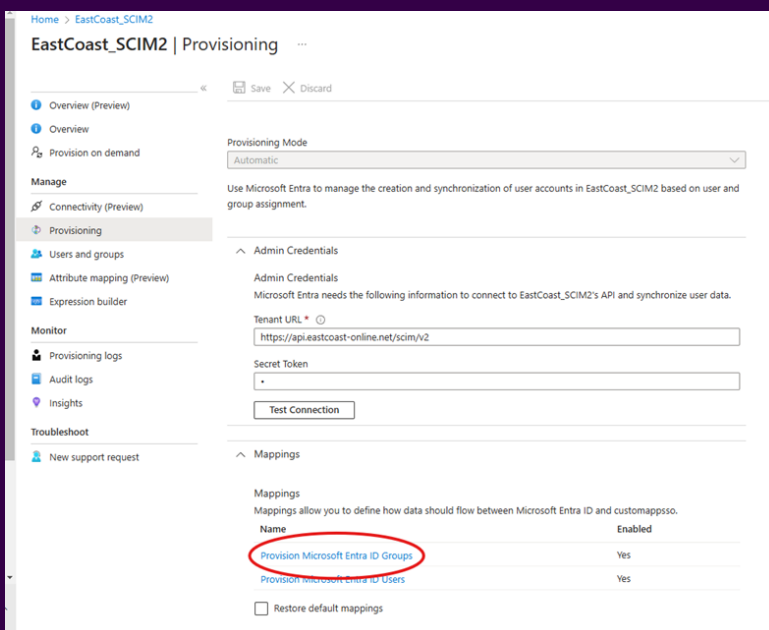
4. Click Test Connection and verify success



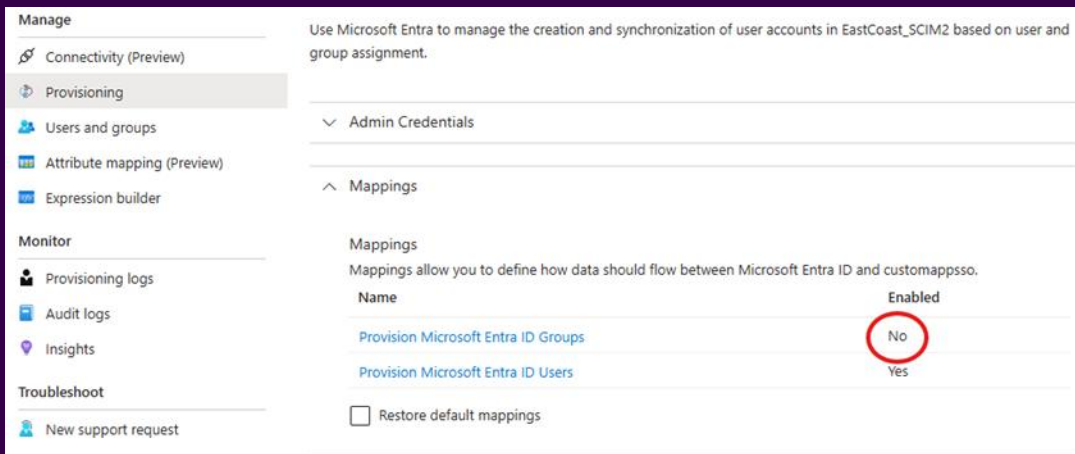
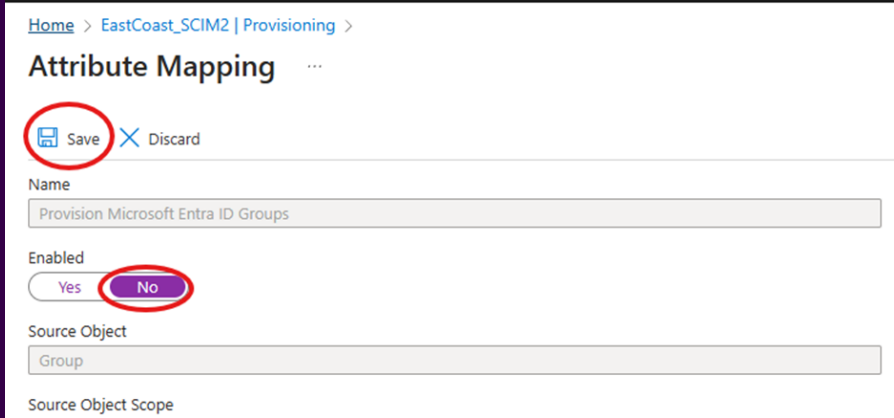
5. Click Save.



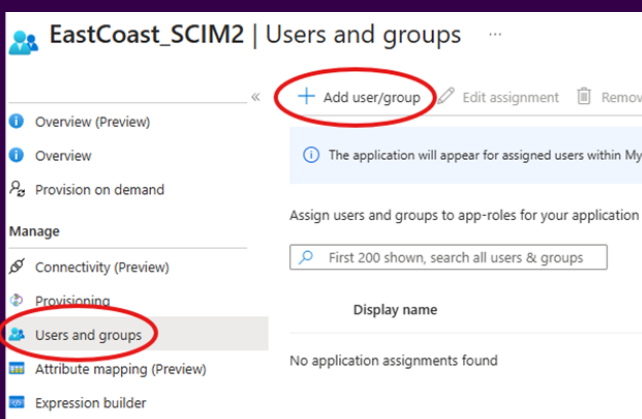
6. After saving, A new heading appears, Mappings.



7. Under Mappings, disable “Provision Azure Active Directory Groups” (This feature is not supported into Precise Visit). Click Save again.

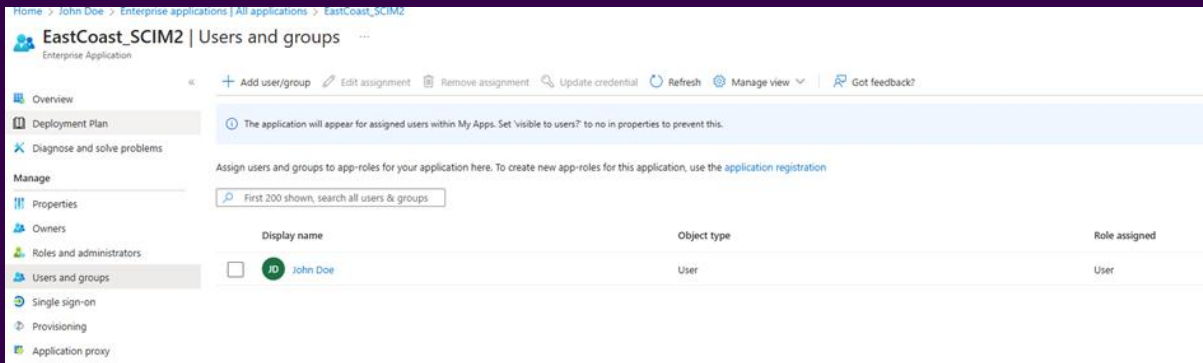


8. Click Users and groups in menu. Then click Add user/group and select them in the right column. These are the users/users in groups that will sync into Precise Visit.

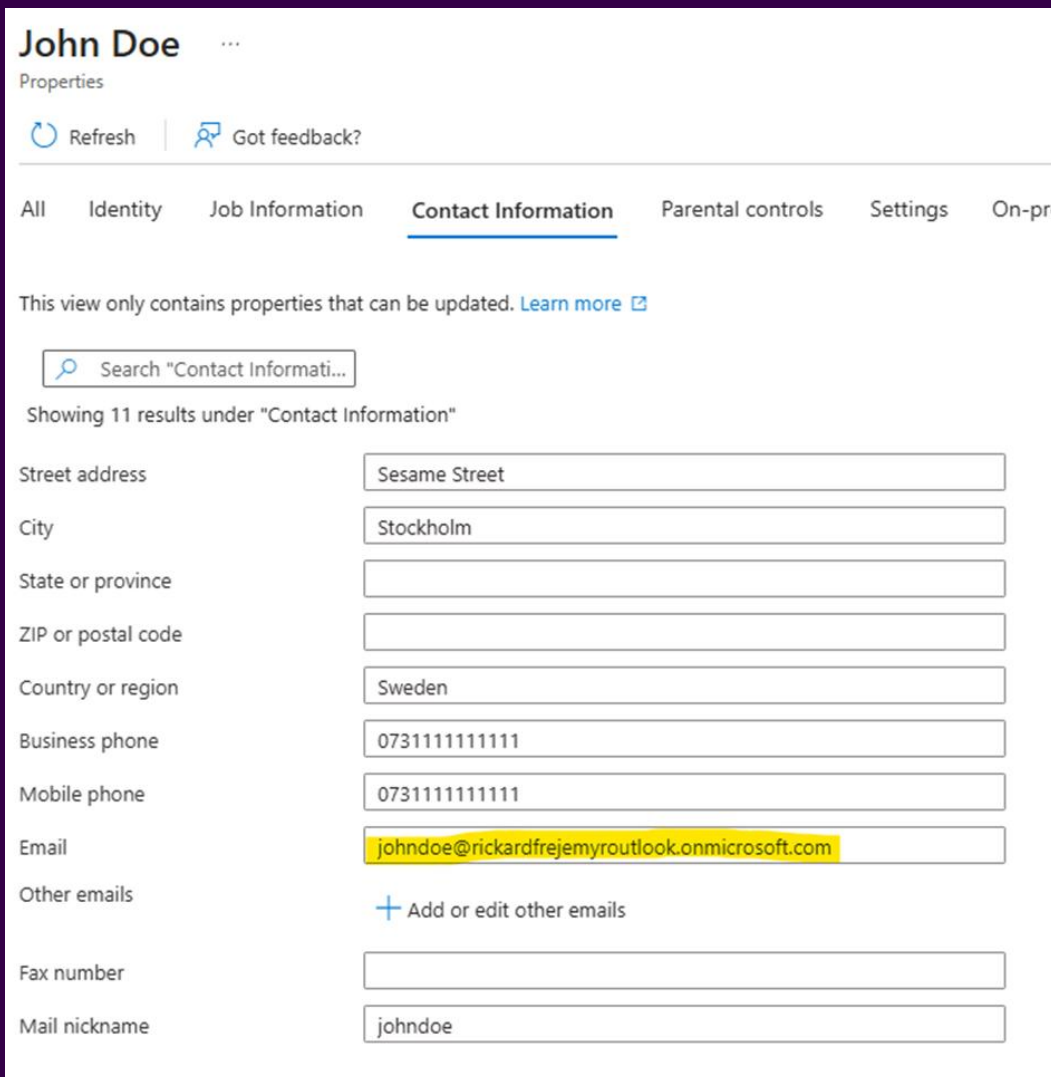


## Example

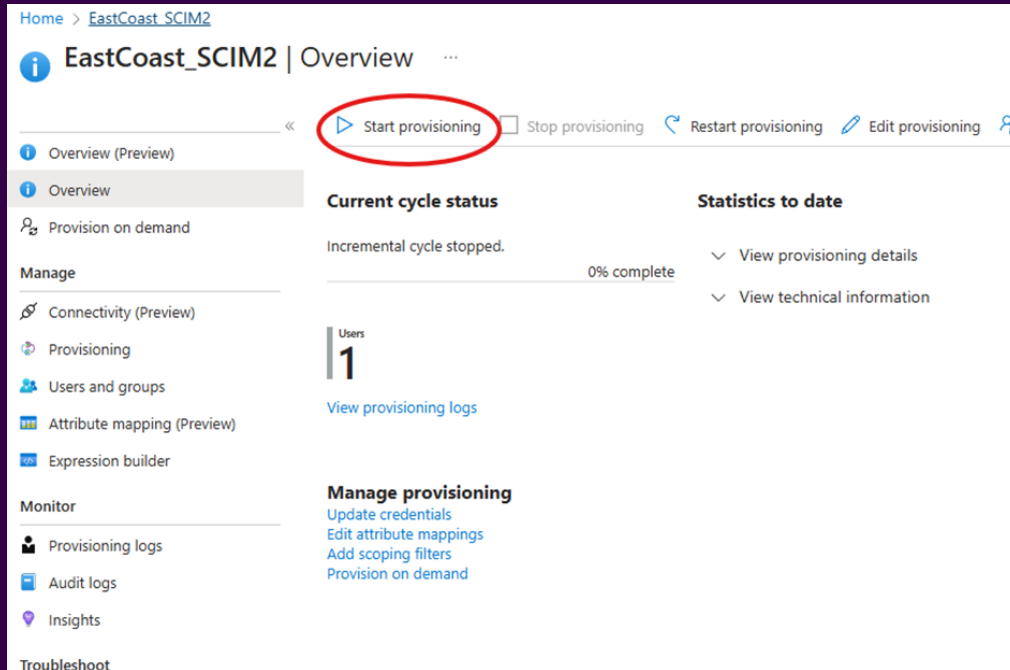
In this example only one user is chosen: John Doe



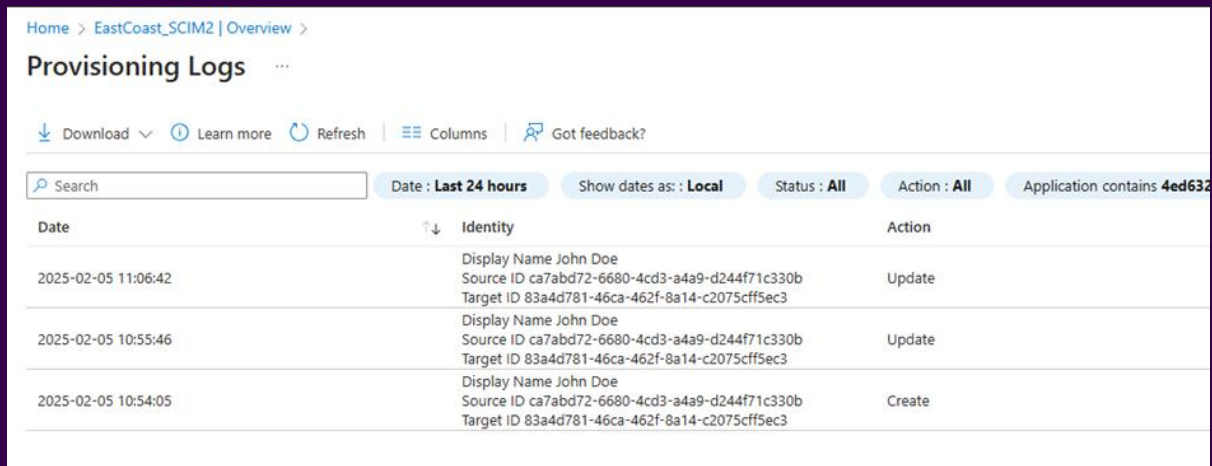
It is important that the user has an email address, as it is a requirement for users in Precise Visit.



On the Overview you can see the status of your sync/provisioning. Click start provisioning to transfer users/users in groups to Precise Visit.

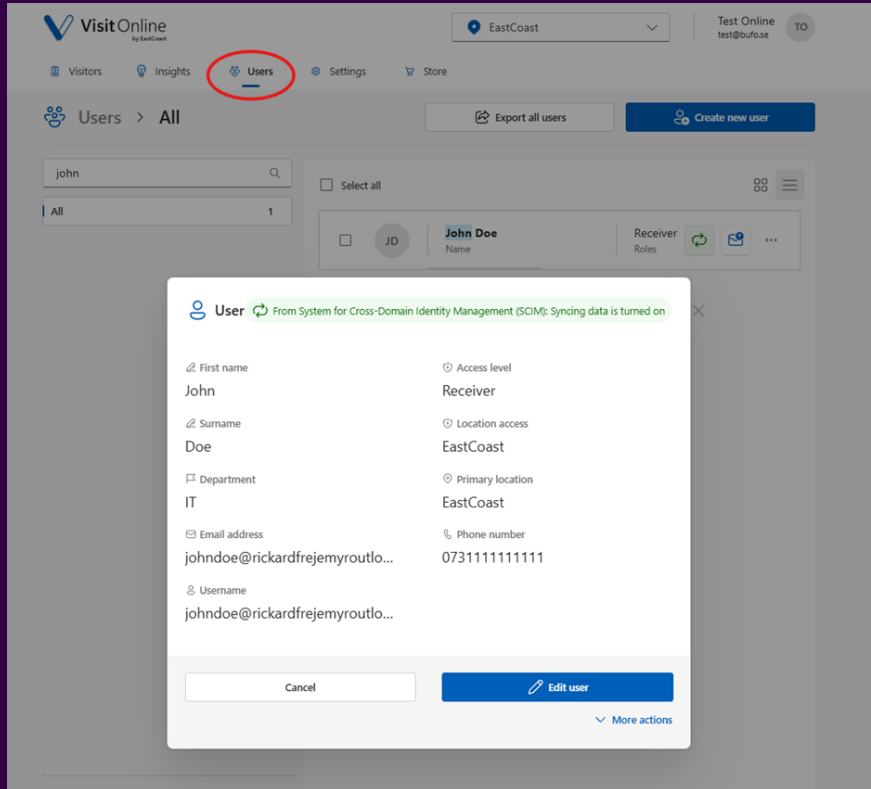


There are logs to view if something goes wrong



The Provisioning interval is 40 minutes by default

In Visit Online the User now appears as a host.



If needed, it is possible to change the mapping if some information is in the “wrong” fields in Entra ID. For example, if the mobile number is in the telephone number field in Entra ID.

The attributes are used to match the users in the Precise Visit app for update operations.

### Required attributes

- Username
- emails[type eq "work"]
- name.givenName
- name.familyName
- active
- ExternalId

### Optional attributes

- phoneNumbers[type eq "mobile"]
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

Home > EastCoast\_SCIM2

### EastCoast\_SCIM2 | Attribute mapping (Preview)

Restore default mappings

Overview (Preview)

Overview

Provision on demand

Manage

Connectivity (Preview)

Provisioning

Users and groups

Attribute mapping (Preview)

Expression builder

Monitor

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

Name	Enabled
Provision Microsoft Entra ID Groups	No
Provision Microsoft Entra ID Users	Yes

Home > EastCoast\_SCIM2 | Attribute mapping (Preview)

### Attribute Mapping

Save Discard

active	Switch([IsSoftDeleted], , "False", "True", "True", "False")	Edit	Delete
displayName	displayName	Edit	Delete
title	jobTitle	Edit	Delete
emails[type eq "work"].value	mail	Edit	Delete
preferredLanguage	preferredLanguage	Edit	Delete
name.givenName	givenName	Edit	Delete
name.familyName	surname	Edit	Delete
name.formatted	Join(" ", [givenName], [surname])	Edit	Delete
addresses[type eq "work"].formatted	physicalDeliveryOfficeName	Edit	Delete
addresses[type eq "work"].streetAddress	streetAddress	Edit	Delete
addresses[type eq "work"].locality	city	Edit	Delete
addresses[type eq "work"].region	state	Edit	Delete
addresses[type eq "work"].postalCode	postalCode	Edit	Delete
addresses[type eq "work"].country	country	Edit	Delete
phoneNumbers[type eq "work"].value	telephoneNumber	Edit	Delete
phoneNumbers[type eq "mobile"].value	mobile	Edit	Delete
phoneNumbers[type eq "fax"].value	facsimileTelephoneNumber	Edit	Delete
externalid	mailNickname	Edit	Delete
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeid	employeeid	Edit	Delete
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department	department	Edit	Delete
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager	manager	Edit	Delete

Add New Mapping

Show advanced options

