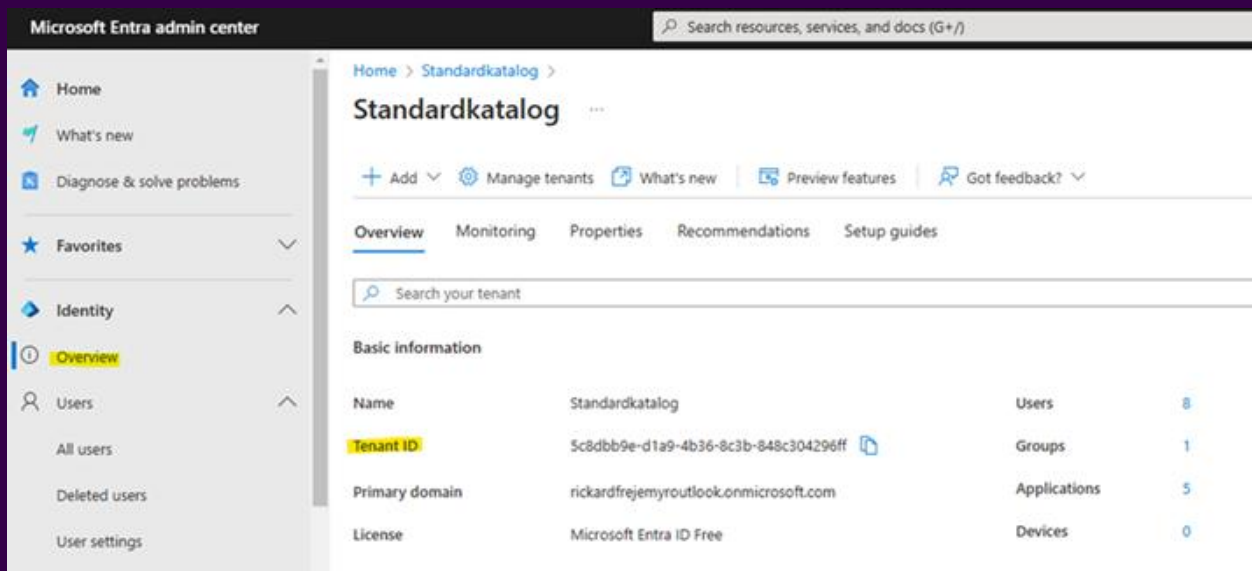


Guide

SSO Setup

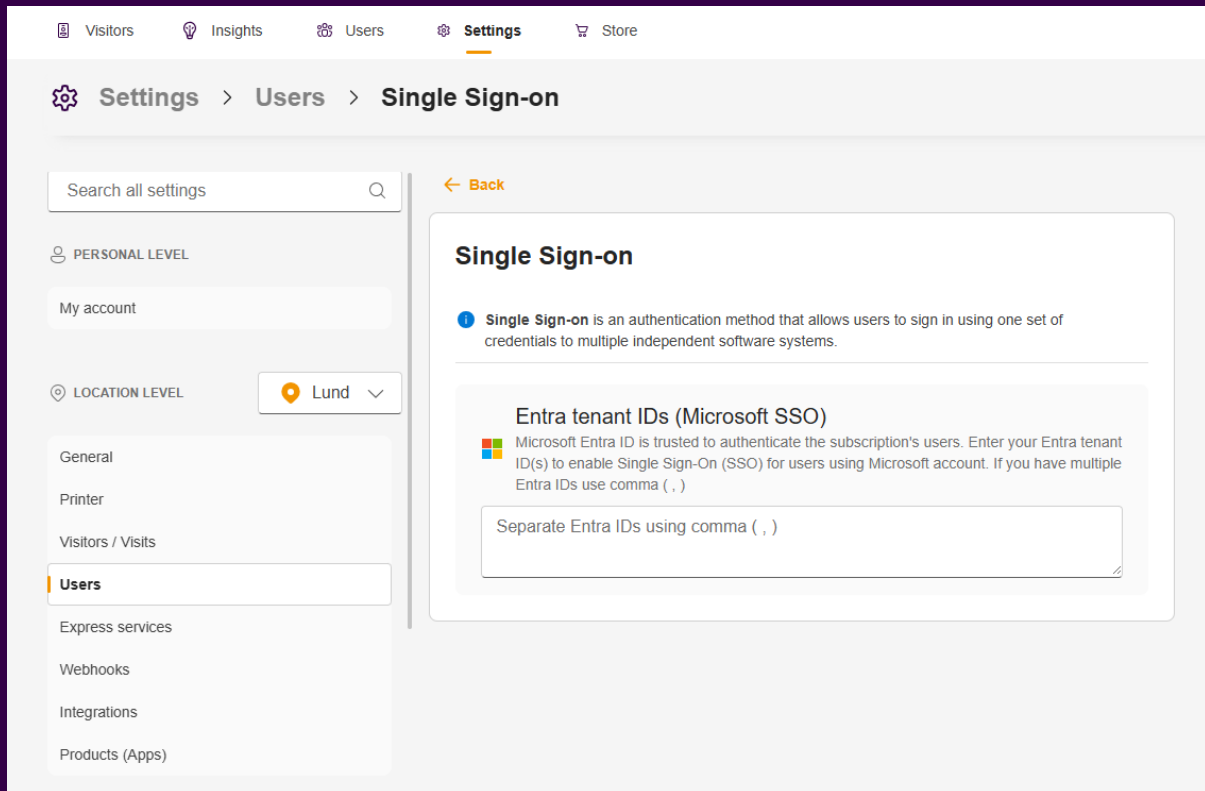
1. Log in to your Microsoft Entra Admin Center and copy your TenantID.



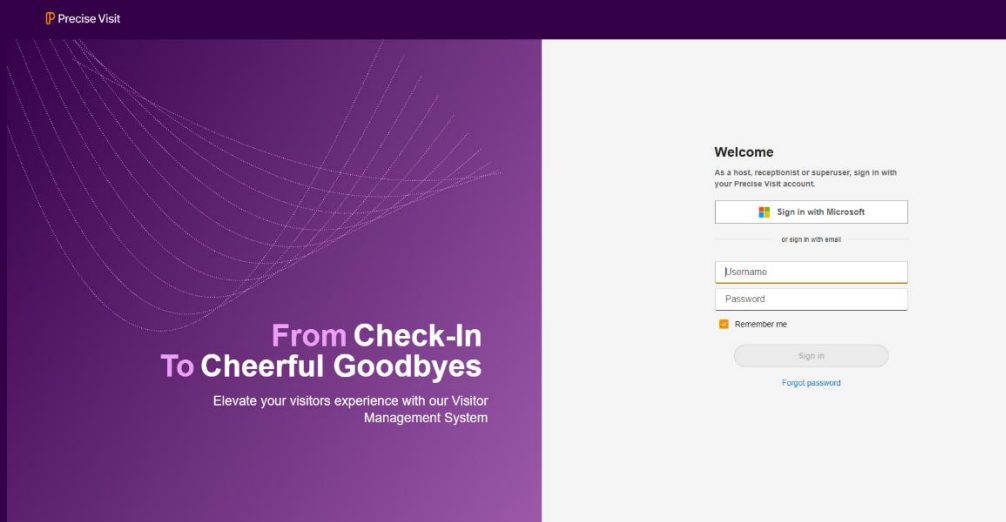
2. Log in (Power User) to Precise Visit.

Go to Settings menu. And click on Users under location level.

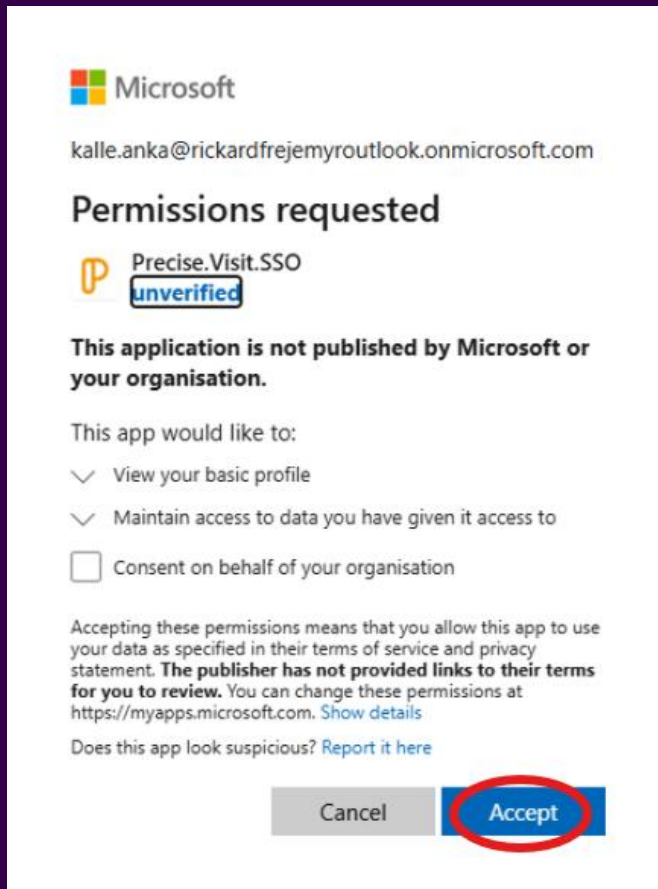
Click on Single Sign On and paste your TenantID.



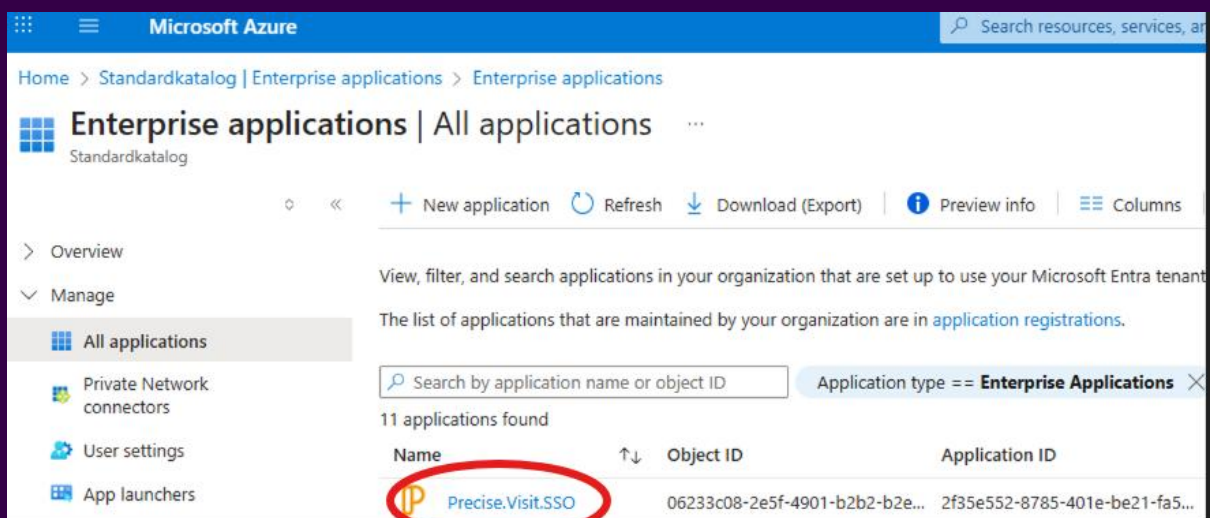
3. Log out of Precise Visit and log in again choosing “Sign in with Microsoft (with an account that is admin in Entra ID and Power User in Precise Visit)”



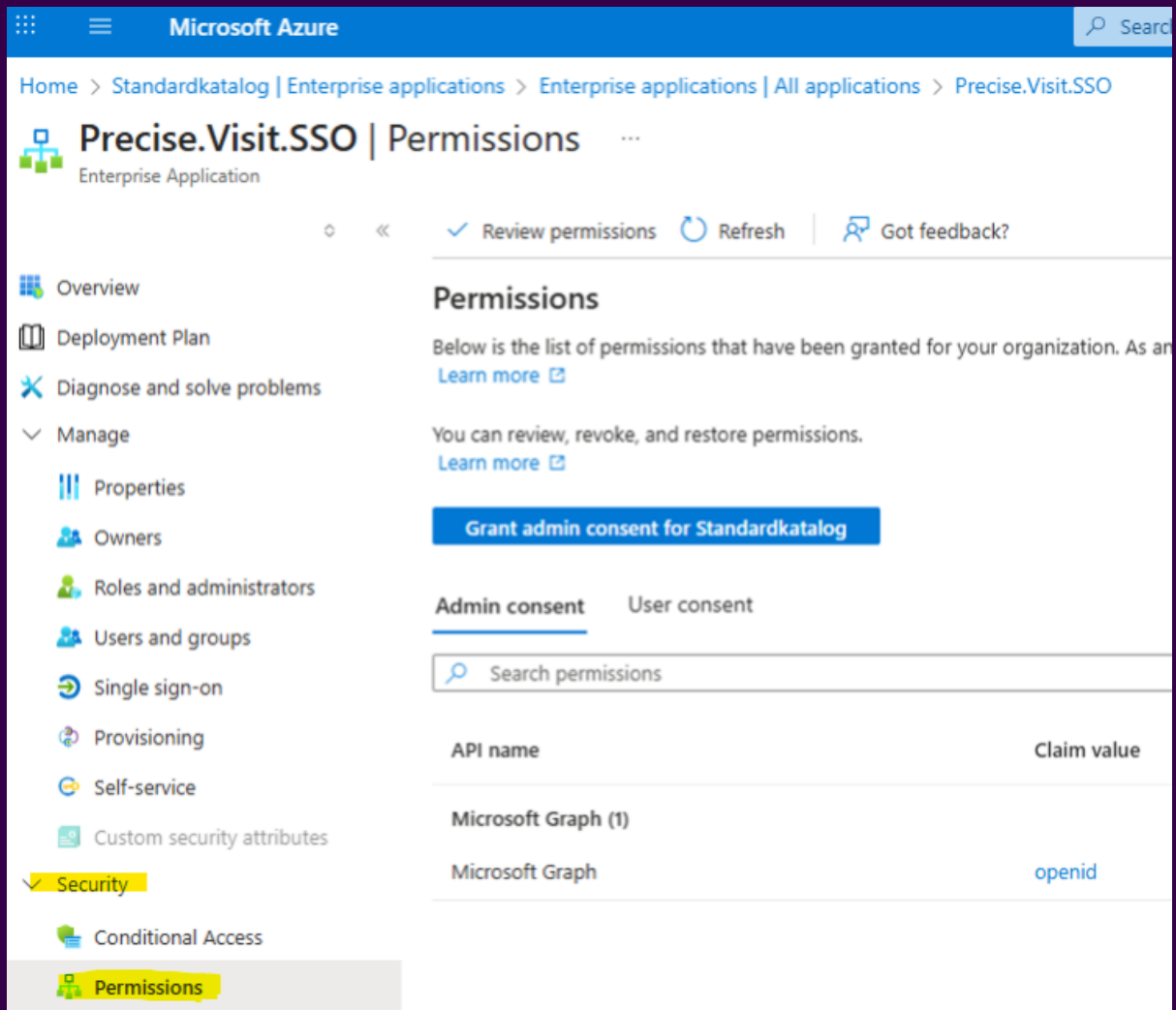
4. Click Accept



5. Back in Entra Admin center, click on Precise.Visit.SSO in Enterprise applications.



6. Click on Security – Permissions.



Microsoft Azure

Home > Standardkatalog | Enterprise applications > Enterprise applications | All applications > Precise.Visit.SSO

Precise.Visit.SSO | Permissions

Enterprise Application

Review permissions Refresh Got feedback?

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes
- Security**
- Conditional Access
- Permissions**

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can review, revoke, and restore permissions. [Learn more](#)

You can review, revoke, and restore permissions. [Learn more](#)

Grant admin consent for Standardkatalog

Admin consent User consent

Search permissions

API name	Claim value
Microsoft Graph (1)	
Microsoft Graph	openid

7. Click on Grant admin consent.

The screenshot shows the Microsoft Azure portal interface. At the top, the breadcrumb navigation reads: Home > Standardkatalog | Enterprise applications > Enterprise applications | All applications > Precise.Visit.SSO. The main heading is 'Precise.Visit.SSO | Permissions' with a sub-heading 'Enterprise Application'. Below this, there are navigation options: 'Review permissions' (checked), 'Refresh', and 'Got feedback?'. The left-hand navigation pane includes 'Overview', 'Deployment Plan', 'Diagnose and solve problems', 'Manage' (expanded), 'Properties', 'Owners', 'Roles and administrators', 'Users and groups', 'Single sign-on', 'Provisioning', 'Self-service', 'Custom security attributes', 'Security' (expanded), 'Conditional Access', and 'Permissions' (highlighted). The main content area is titled 'Permissions' and contains the following text: 'Below is the list of permissions that have been granted for your organization. As an [Learn more](#)'. Below this is another line: 'You can review, revoke, and restore permissions. [Learn more](#)'. A prominent blue button with white text, 'Grant admin consent for Standardkatalog', is circled in red. Below the button, there are two tabs: 'Admin consent' (selected) and 'User consent'. A search bar labeled 'Search permissions' is present. A table with two columns, 'API name' and 'Claim value', is shown. The table contains one entry: 'Microsoft Graph (1)' with a sub-entry 'Microsoft Graph' and a claim value of 'openid'.

8. Log in with admin user again in Entra ID and accept permissions.



kalle.anka@rickardfrejemyroutlook.onmicrosoft.com

Permissions requested

Review for your organization



This application is not published by Microsoft or your organization.

This app would like to:

✓ View users' basic profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

(Recommended) – Click on properties of the Precise.Visit.SSO app and turn assignment required to “Yes”. This way only users (in users and groups) assigned to enterprise app can login. Otherwise, all users can login regardless of that they have received an activation email from a Power User.

Microsoft Azure Search resources, services, and docs (G+)

Home > Standardkatalog | Enterprise applications > Enterprise applications | All applications > Precise.Visit.SSO

Precise.Visit.SSO | Properties


Enterprise Application

Save Discard Delete Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties**
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning
 - Self-service
 - Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
- Troubleshooting + Support

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

Some of the displayed properties that are not editable are managed on the application registration in the application's home tenant.

Enabled for users to sign-in?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Name	Precise.Visit.SSO
Homepage URL	
Logo	
Application ID	2f35e552-8785-401e-be21-fa57d80a3489
Object ID	06233c08-2e5f-4901-b2b2-b2eafcb6d693
Assignment required?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Visible to users?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Notes	