

Floorsense / Smartalock OIDC Single Sign On (SSO) Setup Guide

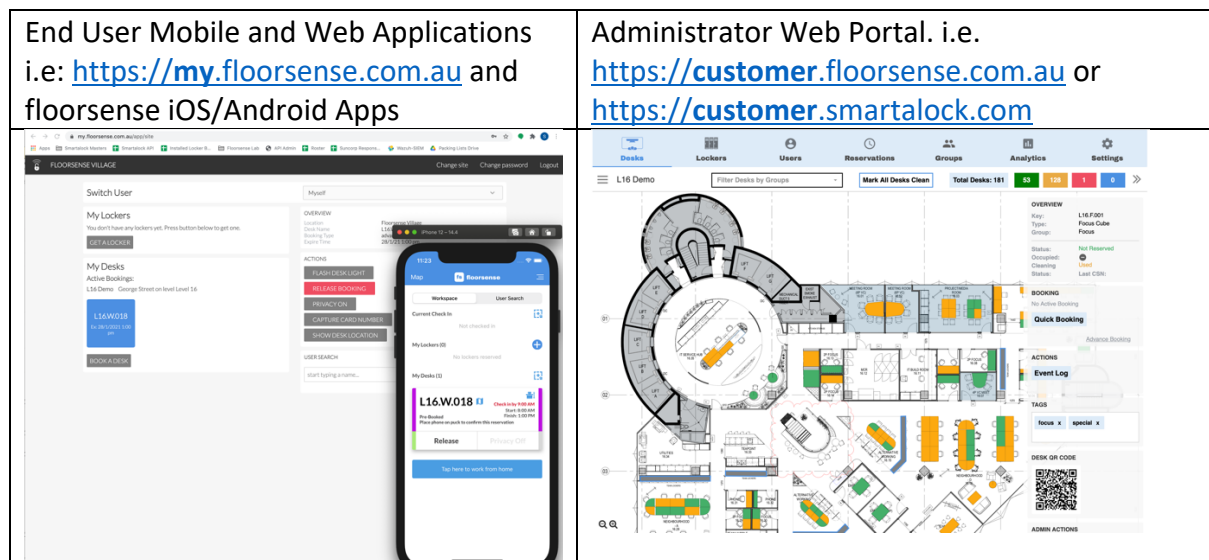
Overview

Floorsense/Smartalock now supports single-sign-on (SSO) via Open ID Connect (OIDC). This feature allows your end users to authenticate using the same credentials they use to log into the corporate network, without sharing any passwords with Floorsense/Smartalock.

SSO should work for any OIDC compatible identity provider (IdP) but we currently only offer setup support for the following providers:

- Microsoft Azure Active Directory
- Okta

There are two Floorsense/Smartalock endpoints which can be protected through SSO



Each endpoint requires a separate OIDC registration with the identity provider but the setup steps for each are similar. This guide walks through both **End User** and **Admin** access noting the differences where appropriate.

Configuration Steps

The steps to get things set up are broadly:

- Register the new applications (End user and/or Admin) with the identity provider
- Provide registration details to your floorsense/Smartalock account manager
- Assign which of your users are allow access to the each of the application – for example every user maybe allowed access to the End user App, but a limited group of users are allowed access to the Admin App.
- Test the application is working correctly

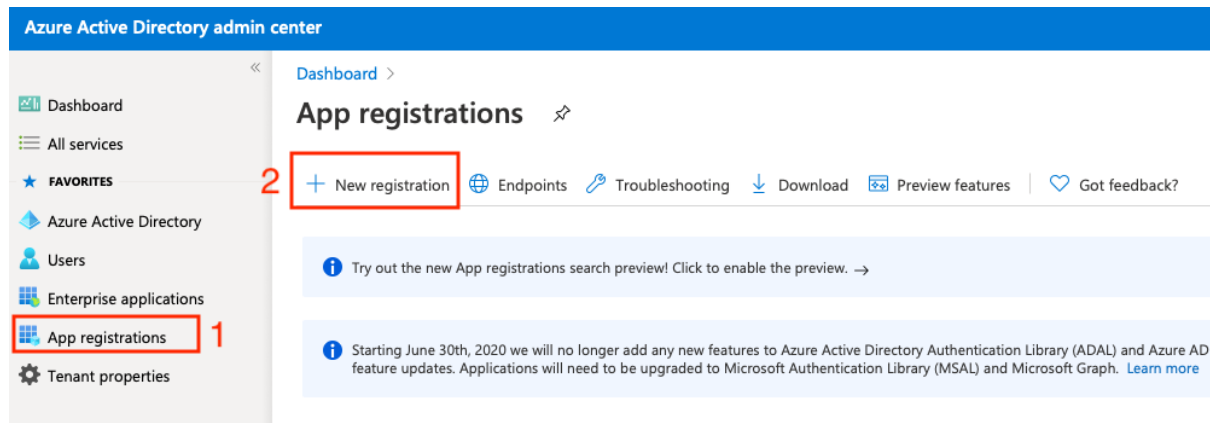
Technical details of the configuration and registration details that are required are listed in the appendices at the end of this document

Registering a new Application

Azure Active Directory

Note the steps listed here can be read in conjunction with the Microsoft provided guide at <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

Register a new application by visiting <https://aad.portal.azure.com/>



The screenshot shows the 'Register an application' form in the Azure Active Directory admin center. The form includes the following sections:

- Name:** The user-facing display name for this application (this can be changed later). The input field contains 'Smartalock End User Access'.
- Supported account types:** Who can use this application or access this API?
 - ☒ Accounts in this organizational directory only (Single tenant)
 - ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 - ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 - ☐ Personal Microsoft accounts only
- Redirect URI (optional):** We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 - Web: e.g. https://myapp.com/auth

At the bottom, there is a link to 'Enterprise applications' and a 'Register' button.

Enter a name for the application registration. This name will be displayed to your end users and can be edited later. Choose the first option for application access (single tenant) and leave the Redirect URI blank – we will fill this in later

Azure Active Directory admin center

Dashboard > App registrations > Smartlock End User Access

Search (Cmd+/)

Delete Endpoints Preview features

Essentials

Display name: Smartlock End User Access

Supported account types: My organization only

Application (client) ID: 4eae730f-375f-4520-b571-61d91133a11e **Client ID**

Directory (tenant) ID: ce29943b-d032-4b7b-b394-6469e5e11489 **Tenant ID**

Object ID: 4ea90d7b-e1e5-4cfc-9f55-590ac478492c

Redirect URIs: Add a Redirect URI

Application ID URI: Add an Application ID URI

Managed application in local directory: Smartlock End User Access

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Call APIs

Documentation

Microsoft identity platform

Authentication scenarios

Authentication libraries

Code samples

Microsoft Graph

Glossary

Help and Support

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

On the application registration page take note of 1. The Client ID, 2. The Tenant ID; these will need to be provided to your floorsense/Smartlock account manager later. Select the "Certificates & secrets" items

Azure Active Directory admin center

Dashboard > App registrations > Smartlock End User Access

Smartlock End User Access | Certificates & secrets

Search (Cmd+/)

Got feedback?

Add a client secret

Description: Smartlock Secret

Expires

☐ In 1 year

☐ In 2 years

☒ Never

[Add](#) [Cancel](#)

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value	ID
No client secrets have been created for this application.			

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Generate a new secret by pressing the “New Client Secret” button. Choose a descriptive name (this won’t be displayed to anyone) and set the “Never” expiry option. Press “Add” to generate the secret.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
Smartalock Secret	12/31/2299	xb7eTs7WWR_7~Dzi...	ed593d19-a1fd-4e63...

Take a copy of the client secret by pressing the copy to clipboard button. **Note that this secret will only be displayed once**, if you return to this page at a later time the secret will be unavailable and a new one will need to be generated

Next visit the “Authentication” section and press “Add a platform”, choose “Web” as the platform type

The screenshot shows the Azure portal interface. On the left, the 'Authentication' link in the 'Manage' section is highlighted with a red box and the number 1. The main area shows the 'Smartalock End User Access | Authentication' page. The 'Add a platform' button is highlighted with a red box and the number 2. The 'Web' application type is highlighted with a red box and the number 3. The 'Single-page application' type is also visible. The 'Mobile and desktop applications' section shows 'iOS / macOS' and 'Android' options. A warning message at the bottom states: 'Due to temporary difference accounts for an existing reg editor. Learn more about it'.

The redirect URIs are different depending on whether you are configuring End user or Admin portal access for floorsense/Smartalock

End User Access

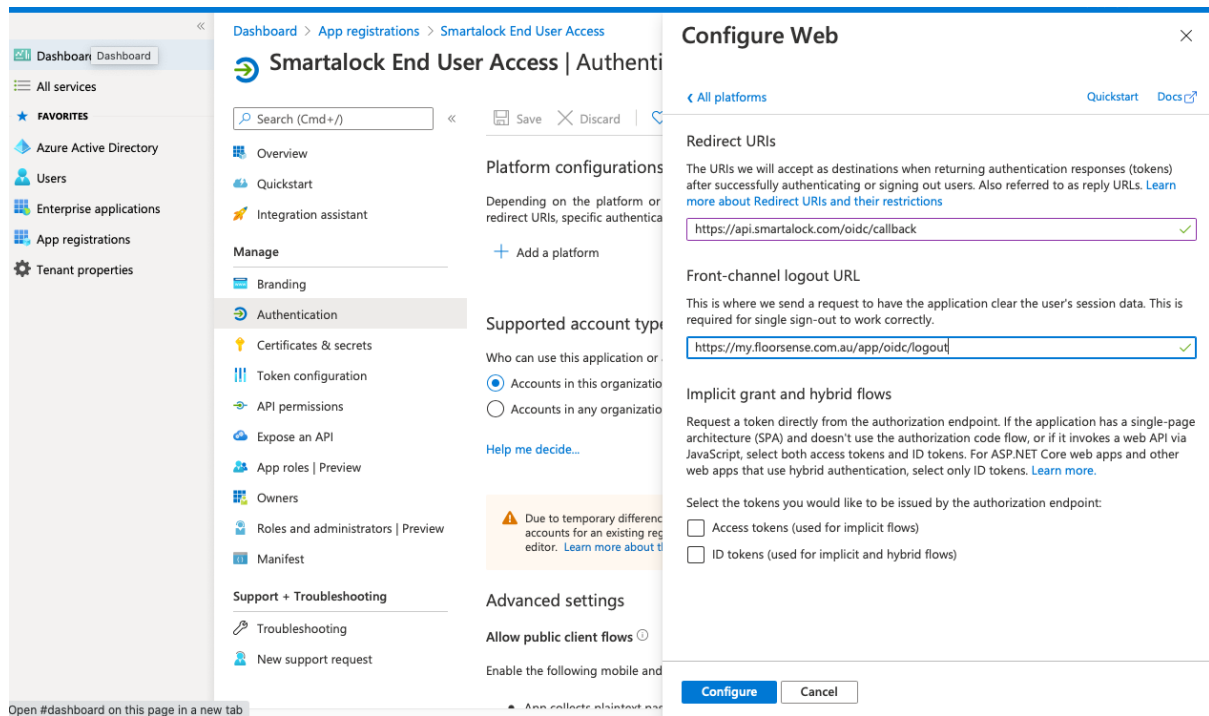
For redirect URI choose <https://api.smartalock.com/oidc/callback> <-- use this redirect URI for both floorsense and Smartalock systems.

For logout URI choose <https://my.floorsense.com.au/app/oidc/logout> ¹

Admin Portal Access

For redirect URI choose https://example.floorsense.com.au/app/redirect_uri ²

Leave logout URI blank



End User App Only

If configuring End-user app access then add additional redirect URIs to match the required web domains that will be used. Press the “Add URI” button, enter the URI. After adding URIs be sure to press the “Save” button

¹ Use the domain of the end-user web application for your region – this may be my.floorsense.com.au, my.smartalock.com, my.floorsense.nz, my.floorsen.se or a domain customised to your organisation

² The specific domain name will be provided by your account manager

Dashboard > App registrations > Smartalock End User Access

Smartalock End User Access | Authentication

Search (Cmd+/) << 3 Save Discard Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles | Preview
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

1	Add URI	
2	https://api.smartalock.com/oidc/callback	Required for mobile apps
	https://my.floorsense.com.au/app/oidc/callback	Required for web app

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

<https://my.floorsense.com.au/app/oidc/logout>

Implicit grant and hybrid flows

The full list of redirect URIs is

- <https://api.smartalock.com/oidc/callback>
- <https://my.floorsense.com.au/app/oidc/callback>
- <https://my.floorsense.nz/app/oidc/callback>
- <https://my.floorsen.se/app/oidc/callback>
- <https://my.smartalock.com/app/oidc/callback>
- Any other custom domain name that may have been used

OKTA

To register a new application on Okta login to the Okta administration portal

Select Applications -> Add Application

The screenshot shows the Okta administration portal interface. At the top, the navigation bar includes the Okta logo, a 'Get Started' button, and several menu items: 'Dashboard', 'Users', 'Applications' (highlighted with a red box and a red '1' next to it), 'API', 'Workflow', 'Customization', 'Settings', and an 'Upgrade' button. Below the navigation bar, the 'Applications' section is visible, with an 'Add Application' button highlighted by a red box and a red '2' next to it. The 'Create New Application' wizard is shown below, with a progress bar indicating two steps: '1 Platform' and '2 Settings'. The 'Platform' step is currently active. Below the progress bar, a message states: 'An application in Okta represents an integration with the software you're building. Choose your platform, and we'll recommend settings on the next step.' Four platform options are displayed as cards: 'Native' (iOS, Android), 'Single-Page App' (Angular, React, etc.), 'Web' (.NET, Java, etc., highlighted with a blue border), and 'Service' (Machine-to-Machine). At the bottom of the wizard, there are three buttons: 'Previous', 'Cancel', and 'Next' (highlighted in green).

Choose “Web” as the platform type

On the Application Settings page:

Choose a name – this will be displayed to end users

Remove any Base URI – this will not be used

The redirect and logout URIs differ depending on whether you are configuring end user access or admin portal access

End User Access

Setup login redirect URIs to the following

- <https://api.smartalock.com/oidc/callback>

- <https://my.floorsense.com.au/app/oidc/callback>
- <https://my.floorsense.nz/app/oidc/callback>
- <https://my.floorsen.se/app/oidc/callback>
- <https://my.smartalock.com/app/oidc/callback>
- Any other custom domain name that may have been used

Setup logout URI to be <https://my.floorsense.com.au/app/oidc/logout> ³

Admin Portal Access

Setup login redirect URI as https://example.floorsense.com.au/app/redirect_uri ⁴

Leave logout URI blank

Ensure “Authorization Code” and “Refresh Token” are ticked in Grant Type

APPLICATION SETTINGS

Name
Smartalock End User Access

Base URIs
Optional
+ Add URI

The domains where your application runs. Trusted Origins are created for these URIs and are the only domains that Okta accepts API calls from. [Docs](#)

Login redirect URIs

- <https://api.smartalock.com/oidc/callback> [X]
- <https://my.floorsense.com.au/app/oidc/callback> [X]
- <https://my.floorsense.nz/app/oidc/callback> [X]
- <https://my.floorsen.se/app/oidc/callback> [X]
- <https://my.smartalock.com/app/oidc/callback> [X]

+ Add URI

Okta sends an OAuth authorization response to these URIs. Add your application's callback endpoint. [Docs](#)

Logout redirect URIs

- <https://my.floorsense.com.au/app/oidc/logout> [X]

+ Add URI

When a user signs out, your application can specify a URI where the browser is redirected. Okta only allows redirects for URIs that are listed here. [Docs](#)

Group assignments
Optional
Everyone [X]

Users can only sign in to apps that they are assigned to. Group assignments are easier to manage than individual users.

Grant type allowed

Client acting on behalf of itself

☐ Client Credentials

Client acting on behalf of a user

- ☒ Authorization Code
- ☒ Refresh Token
- ☐ Implicit (Hybrid)

Okta can authorize your app's requests with these OAuth 2.0 grant types. Limit the allowed grant types to minimize security risks. [Docs](#)

Previous Cancel Done


³ Use the domain of the end-user web application for your region – this may be my.floorsense.com.au, my.smartalock.com, my.floorsense.nz, my.floorsen.se or a domain customised to your organisation

⁴ The specific domain name will be provided by your account manager

{okta} [Get Started](#) ⁴ Dashboard Users Applications API Workflow Customization Settings U

← Back to Applications

Smartlock End User Access

Active  [View Logs](#)

General Sign On Assignments Okta API Scopes

Client Credentials

Edit

1 Client ID

Ooa [redacted] hm4x7

Public Identifier for the client that is required for all OAuth flows.

2 Client secret

j52d [redacted] Mh

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

General Settings

Edit

3 Okta domain

[redacted].okta.com

On the Application details page take note of the “Client ID”, “Client Secret” and “Okta Domain” and provide these to your account manager

Provide Details to your Floorsense/Smartalock Account Manager

To set up SSO for End users the following details are required

Azure

- Tenant ID
- Client ID
- Secret

Okta

- Okta Domain
- Client ID
- Client Secret

For End user app access in addition we require the list of email domains that end users will use to sign in with – e.g. @example.com and @dept.example.com. We also require the “User Provisioning Preference” (see below)

User Provisioning Preference

Your Active Directory contains all of your users and you need to choose the options of which users will be imported into the Smartalock / Floorsense system and when / how this happens. You can choose to:

- Periodically import new users / purge old users (see separate guide)
- Automatically provision new users when they first sign into the mobile or web apps

If automatic provisioning is desired then the system can match existing users on email address, full name or always create new users. Communicate this preference to your Floorsense/Smartalock account manager.

Floorsense/Smartalock will take a upto 1 day to setup SSO on our side. We will email you when it is complete.

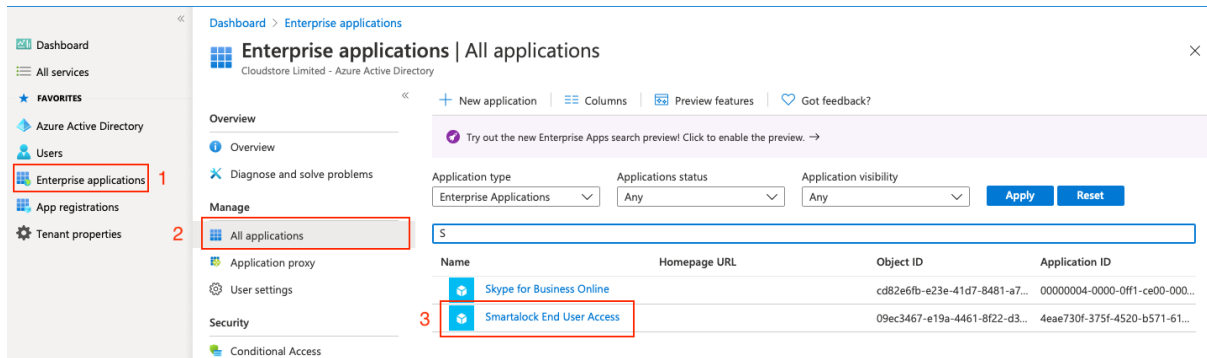
Assigning Access to your End Users

You need to choose which of the users in your domain will have access to the Smartalock / Floorsense mobile and web applications or admin portal via SSO. This can be configured per user or per security group depending on the options available from your identity provider.

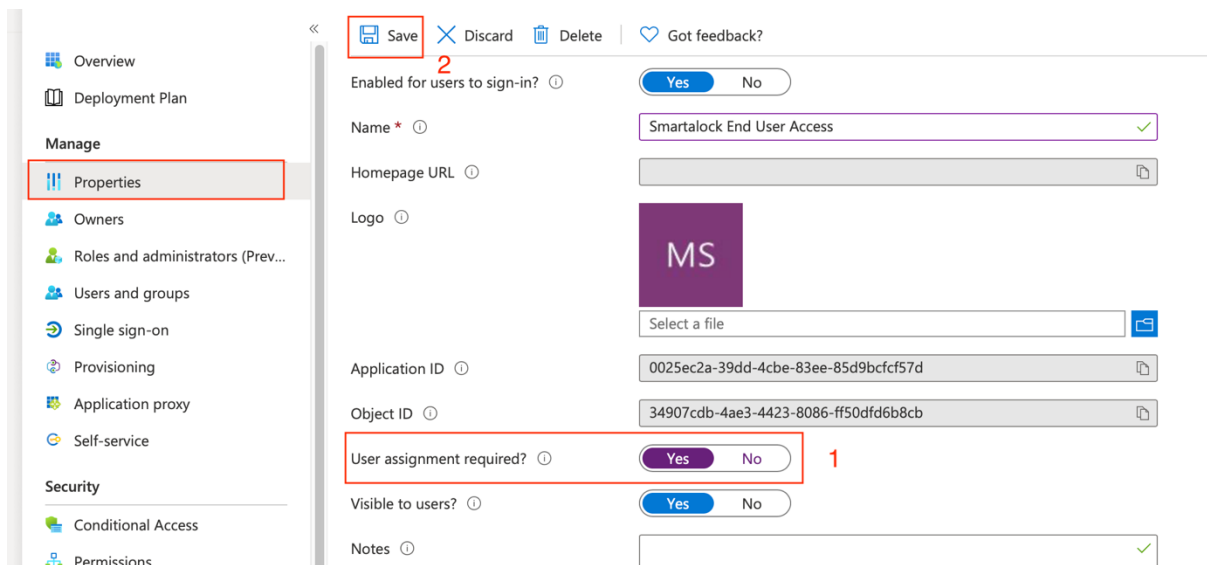
The steps are different for Azure and Okta

Azure Active Directory

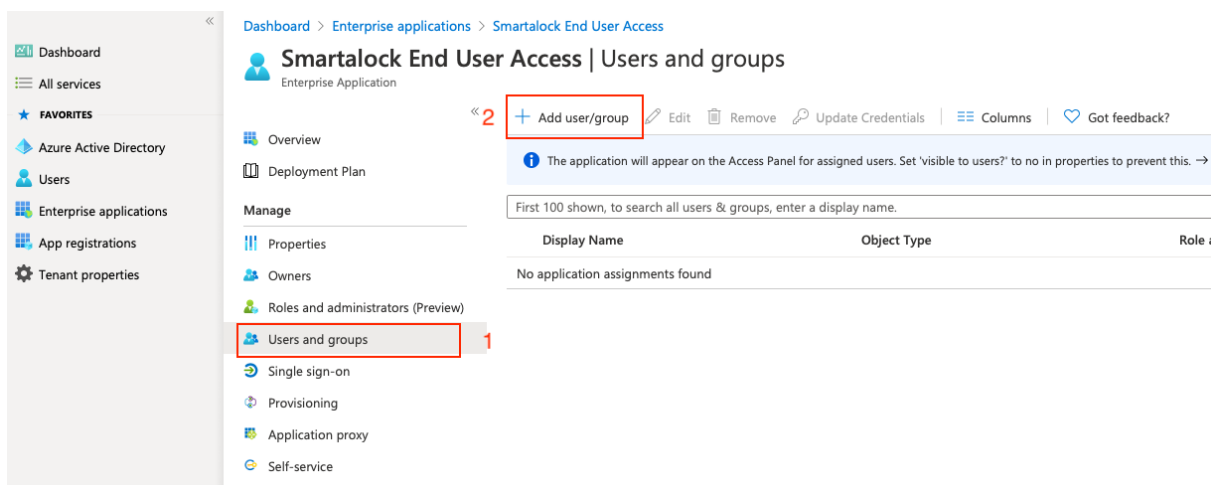
Navigate to the Enterprise Applications section of Azure and select the application that was just registered



Choose “Properties” and enable “User Assignment Required”. Press Save



Choose “Users and Groups” and use the screen to administer which users should be granted access

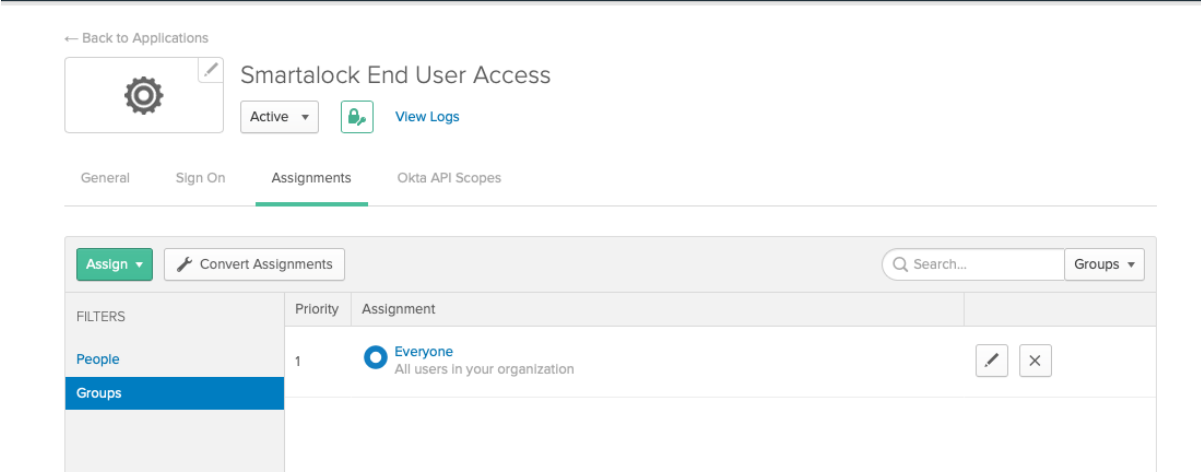


Azure AD allows for fine-grained access control and depending on your organisation setup you may choose to implement conditional access or pre-allow access via the Permissions

screen. These advanced topics are not covered in this guide and you should refer to the Microsoft documentation for further information. A good starting place is the online documentation at <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-access-management>

Okta

Navigate to the application that was created in the above steps and choose the “Assignments” option. From here you can grant access to users and groups



Testing the application integration

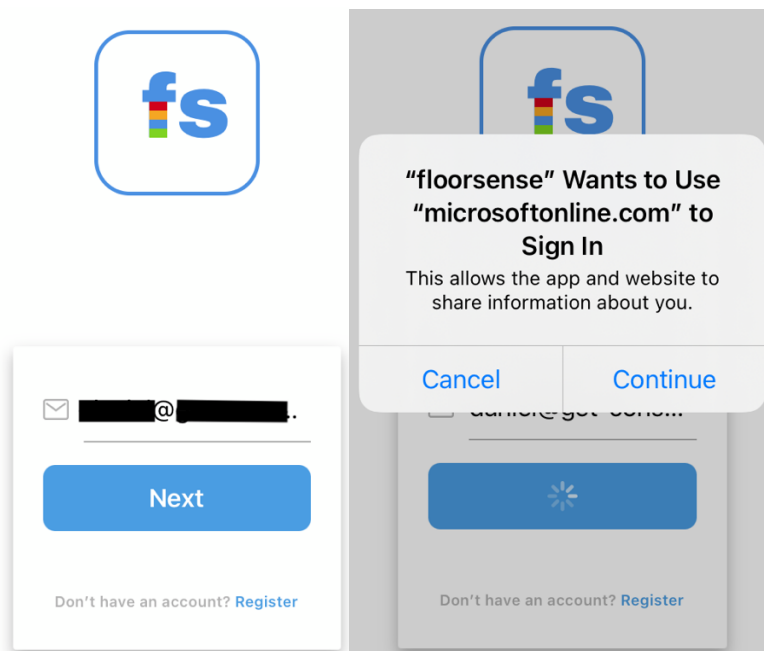
End User - Mobile App

Download the mobile app for free from

- Apple App store - <https://apps.apple.com/nz/app/floorsense/id1462878752>
- Google Play - <https://play.google.com/store/apps/details?id=com.floorsense.app>

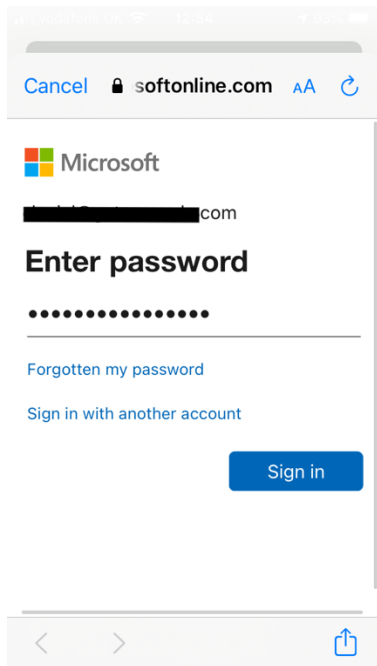
The steps listed below are for the iOS app, but the Android app steps are the same

Open the application and enter your email address



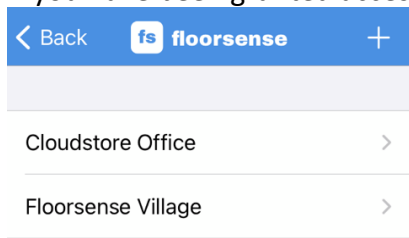
If your email domain has been registered correctly then you will receive a prompt saying that you are being taken to a website to be authenticated. Click Continue

The precise authentication procedures will vary based on your identity provider and may include a password or 2FA, etc. This example shows password authentication



On the first time using the app, your identity provider may require that you grant access to share your email and profile information with the Smartalock / Floorsense website. You will need to grant this access to continue.

If you have been granted access to more than one site, then choose which to connect to



You will now be in the main page of the application. See the application user guide for more details on using the app.

Workspace

User Search

Current Check In



Not checked in

My Lockers (0)



No lockers reserved

My Desks (0)



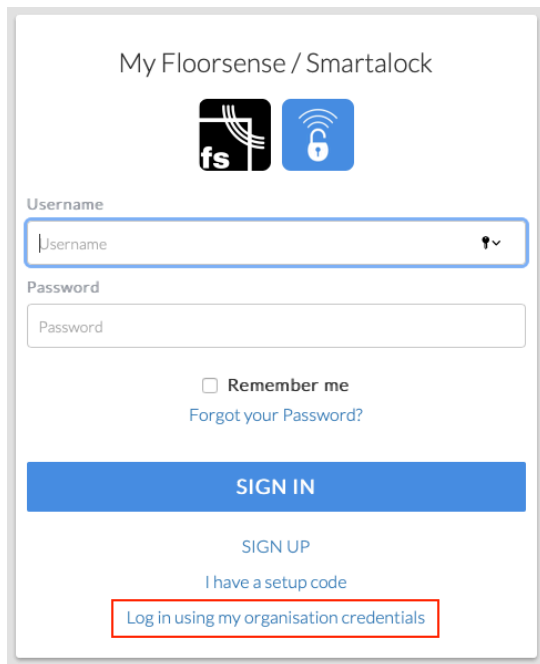
**Place phone on desk puck to reserve
a desk**



End User – Web Application

Navigate to <https://my.floorsense.com.au/> (or to the regional or corporate URL used for the web application).

Choose “Log in using my organisation credentials”



My Floorsense / Smartalock

Username

Password

☐ Remember me

[Forgot your Password?](#)

SIGN IN

[SIGN UP](#)

[I have a setup code](#)

[Log in using my organisation credentials](#)

Enter your email address and you should be redirected to the identity provider login page, or straight to the application if you are already signed in.

On the first time using the web app the user will need to grant permission for the web app to see their email and name so that it can be used for auto-provisioning. This can be either granted on a per-user basis, or from the Azure control panel the administrator can automatically approve all users.

Appendix A – OIDC Setup Parameters

This section contains the technical details of OIDC configuration that customers will require to setup applications on their Identity Provider SSO platform

End User Applications (Mobile & Web)

Redirect URIs	https://api.smartalock.com/oidc/callback https://my.floorsense.com.au/app/oidc/callback https://my.floorsense.nz/app/oidc/callback https://my.floorsen.se/app/oidc/callback https://my.smartalock.com/app/oidc/callback
Logout URI	https://my.floorsense.com.au/app/oidc/logout
Scopes	openid email profile
Grant Types	Authorization Code, Refresh Token

Admin Portal

Redirect URIs	https://example.floorsense.com.au/app/redirect_uri
Logout URI	(blank)
Scopes	openid email
Grant Types	Authorization Code

Appendix B – OIDC Integration Parameters

This section contains the technical details of OIDC parameters generated by the customer's Identity Provider SSSO platform that are required to be supplied to the Smartalock / Floorsense account manager

Parameter	Example Data	Required For
Meta data URL	https://login.microsoftonline.com/4d1d7010-3d31-4072-ba89-78ba2a23034c/v2.0/.well-known/openid-configuration	End User, Admin Portal
Client ID	8aa4d19e-a632-4274-b9ed-fa82f9a0bd47	End User, Admin Portal
Client Secret	Us8Drv~CbDJ.g7LXN-5uqE4	End User, Admin Portal
Email Domains	@example.com	End User
Provisioning Preference	Match on unique email, if not found auto-create a new user on floorsense/Smartalock system	End User