



Azure Active Directory (AD)  
Isolocality Platform User Guide

Isolocality

## Azure Active Directory (AD)

Isolocity is now integrated with Azure for Active Directory. Azure AD is a service for identity and access management. It provides administrators with the ability to manage end-user identities and access privileges.

By activating the Azure AD, you will be able to manage end-users in Isolocity.

### Supported Features

1. New users created through Azure will also be provisioned in Isolocity.
2. Any users removed through Azure will also be inactivated in Isolocity.
3. User Roles in Isolocity will be set-up via the default role assigned in Organization settings.

### Prerequisites

1. You will need the following information:
  - An Azure AD account
  - An Azure Admin Account for initial set-up
  - The person completing the set-up must already be a user in Isolocity

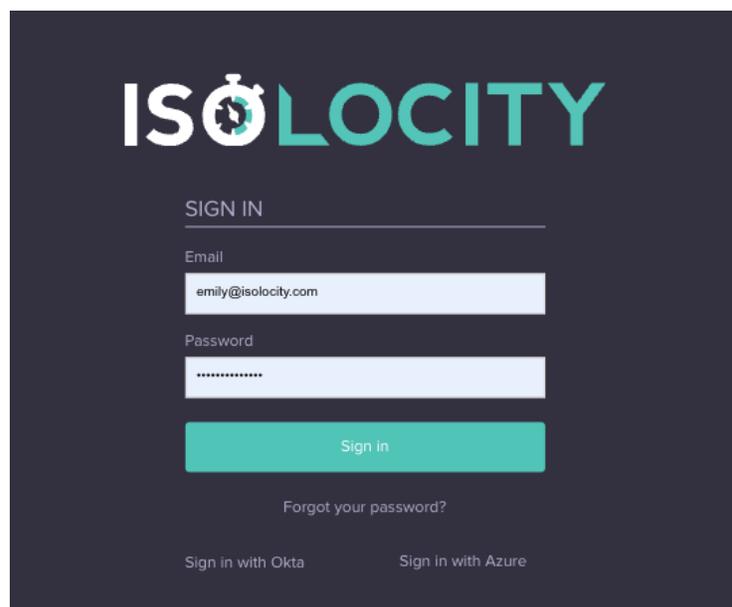
### Important Considerations

1. Inactivating or reducing the permissions of the linked Admin account will interrupt the user sync.
2. Users will be assigned to the default team in Isolocity, if they are a part of multiple teams please navigate to the “User Manager” in Isolocity to add them.

### Setting up Azure AD

1. To link your AD organization with the Isolocity Application, go to the ISOLocality login page and log in to your account.

Note: Ensure you complete the entire set up process using an Azure Admin account.



The image shows a dark-themed login page for Isolocity. At the top, the logo 'ISOLOCITY' is displayed in white and teal. Below the logo, the text 'SIGN IN' is centered. There are two input fields: 'Email' with the value 'emily@isolocity.com' and 'Password' with a masked password '\*\*\*\*\*'. A teal 'Sign in' button is positioned below the password field. At the bottom, there are two links: 'Forgot your password?' and 'Sign in with Azure'. The 'Sign in with Okta' link is also present but less prominent.

2. Navigate to “Organization Settings” by clicking on your initials/profile picture.
3. Navigate to the “Azure Active Directory” section and click on “Authenticate with Azure”

Organization Settings

ISOLOCITY DEMO

ISOLOCITY

Documents

Suppliers

Inventory

Action Items

Single Sign-On

Workspace: demo .isolocity.com

Okta Issuer URL: https://dev-739452.okta.com/oauth2/default

Okta Client ID: 0oaxq64sdzH821toL4x6

Default Team: ISOLOCITY DEMO

Default User Role: Employee

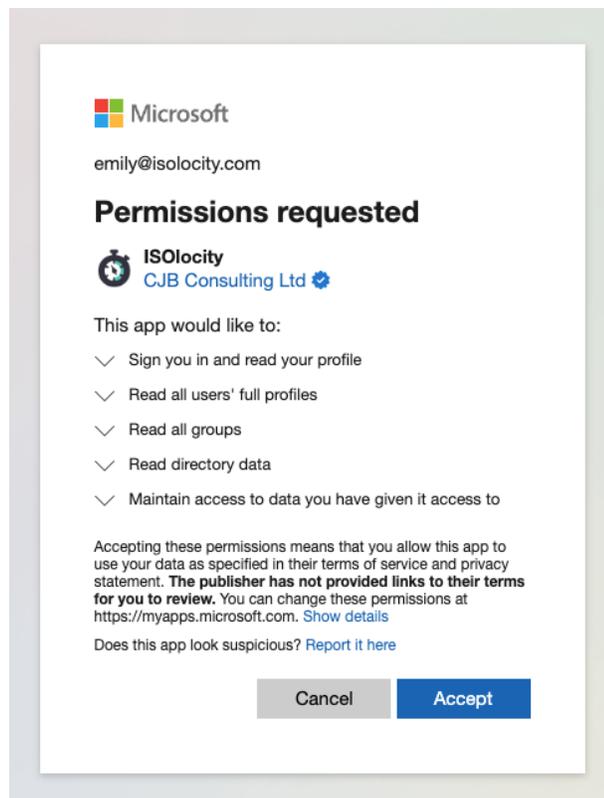
Azure Active Directory

Allow Isolocity to pull selected user groups from AD for easy management.

**Authenticate with Azure**

4. Proceed to follow the prompts from Microsoft to log into your account.
5. Review and accept the requested permissions.

**Note:** Isolocity is a subsidiary of CJB Consulting Ltd.



## **Initiate Users Sync In Isolocity**

1. After accepting the permissions, a “Sync” toggle will appear in “Organization Settings” under the “Azure Active Directory” section.

Organization Settings

Documents

Suppliers

Inventory

Action Items

Single Sign-On

Workspace: demo .isolocity.com

Okta Issuer URL: https://dev-739452.okta.com/oauth2/default

Okta Client ID: 0oaxq64sdzH82t0L4x6

Default Team: ISOLOCITY DEMO

Default User Role: Employee

Azure Active Directory

Sync Users: Initiate

Linked AD Admin Account: Emily UAT

2. Navigate to the Azure Portal and go to “Enterprise Applications” via “Microsoft Entra ID” and then click on “Isolocity.”

Microsoft Azure

Home > ISOLocity | Overview Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Custom security attributes

Security

Permissions

Properties

Name: ISOLOCITY

Application ID: e51d0ff3-56d2-4e1d-a0...

Object ID: 818673fb-e647-48e6-85...

Getting Started

1. Assign users and groups  
Provide specific users and groups access to the applications  
[Assign users and groups](#)

2. Provision User Accounts  
You'll need to create user accounts in the application  
[Learn more](#)

3. Click on “Users and groups” to assign personnel to Isolocity.

4. Select the applicable groups / users.

Microsoft Azure

Home > ISOLocity | Users and groups > Add Assignment

Users and groups

1 user selected

Select a role

None Selected

Users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

14 results found

	Name	Type	Details
<input type="checkbox"/>	All Company	Group	allcompany@isolocity.com
<input type="checkbox"/>	Anne Marie Lorrinan	User	annemarie@isolocity.com
<input type="checkbox"/>	Archana Korat.Test	User	archana@isolocity.com
<input checked="" type="checkbox"/>	Brandon	User	brandon@isolocity.com
<input type="checkbox"/>	chris	User	chris@isolocity.com
<input type="checkbox"/>	Cristian Aldana	User	cristian@isolocity.com
<input type="checkbox"/>	Emily Soares	User	emily@isolocity.com
<input type="checkbox"/>	Evan	User	evan@isolocity.com

Selected (1)

Reset

Brandon

Assign

Select

5. Select an Isolocity User Role for the selected groups / users.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, the breadcrumb trail reads 'Home > ISolocity | Users and groups >'. The main heading is 'Add Assignment' with a dropdown arrow. Underneath, it says 'Isolocity'. A section titled 'Users and groups' shows '1 user selected.' and 'Select a role \*'. Below this, there is a 'None Selected' button. On the right side, a 'Select a role' dialog box is open, displaying a search input field and a list of roles: Isolocity Admin, Isolocity Employee, Isolocity Manager, Isolocity Production, and Isolocity User. At the bottom of the dialog, it says 'Selected Role' and 'You haven't selected any role.' with a 'Select' button. In the main content area, there is an 'Assign' button.

6. Click Assign

7. Once the groups / users are assigned, navigate back to "Organization Settings" in Isolocity and switch the toggle to initiate the sync.

The screenshot shows the Azure Active Directory 'Organization Settings' page. The 'Sync Users' section has a toggle switch labeled 'Initiate' which is currently turned off and highlighted with a red box. The 'Linked AD Admin Account' section shows 'Emily UAT' as the selected account.