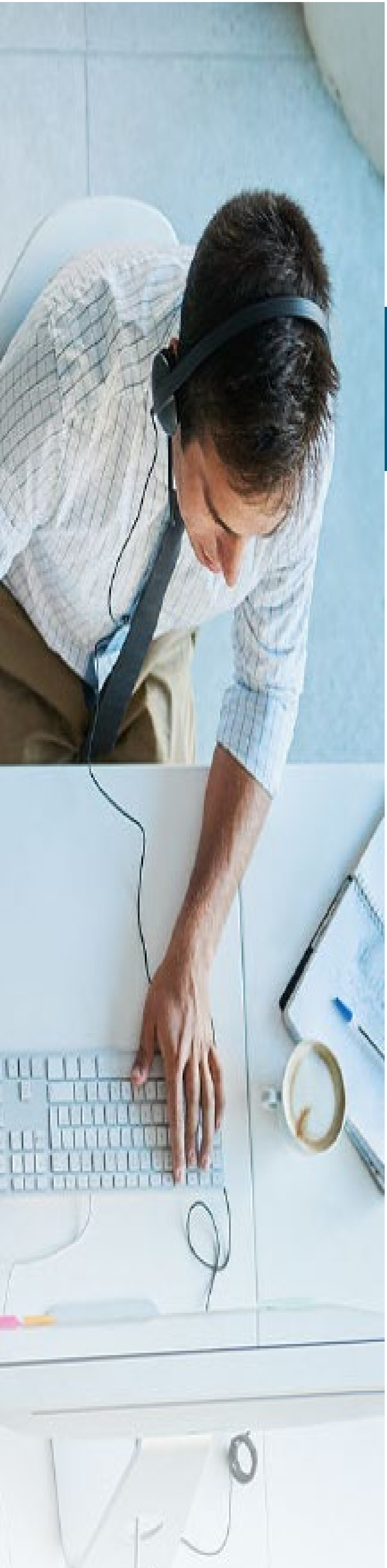


CALL RECORDING

MS Teams Tenant Admin

SSO Administration 101

Quick Reference Guide

MOMENTUM

Powered by: miarec

OVERVIEW

This quick reference guide offers the following instructions for Call Recording **Tenant Administrators** about how to integrate MiaRec with Microsoft Azure AD for Single Sign-On to the Call Recording application:

- Create SSO Connection
- Grant Tenant-wide Admin Consent (Optional)
- Enforce SSO (Optional)
- Configure Restricted Domains (Optional)

The following actions can be performed by a **Tenant Administrator** in the Call Recording web portal.

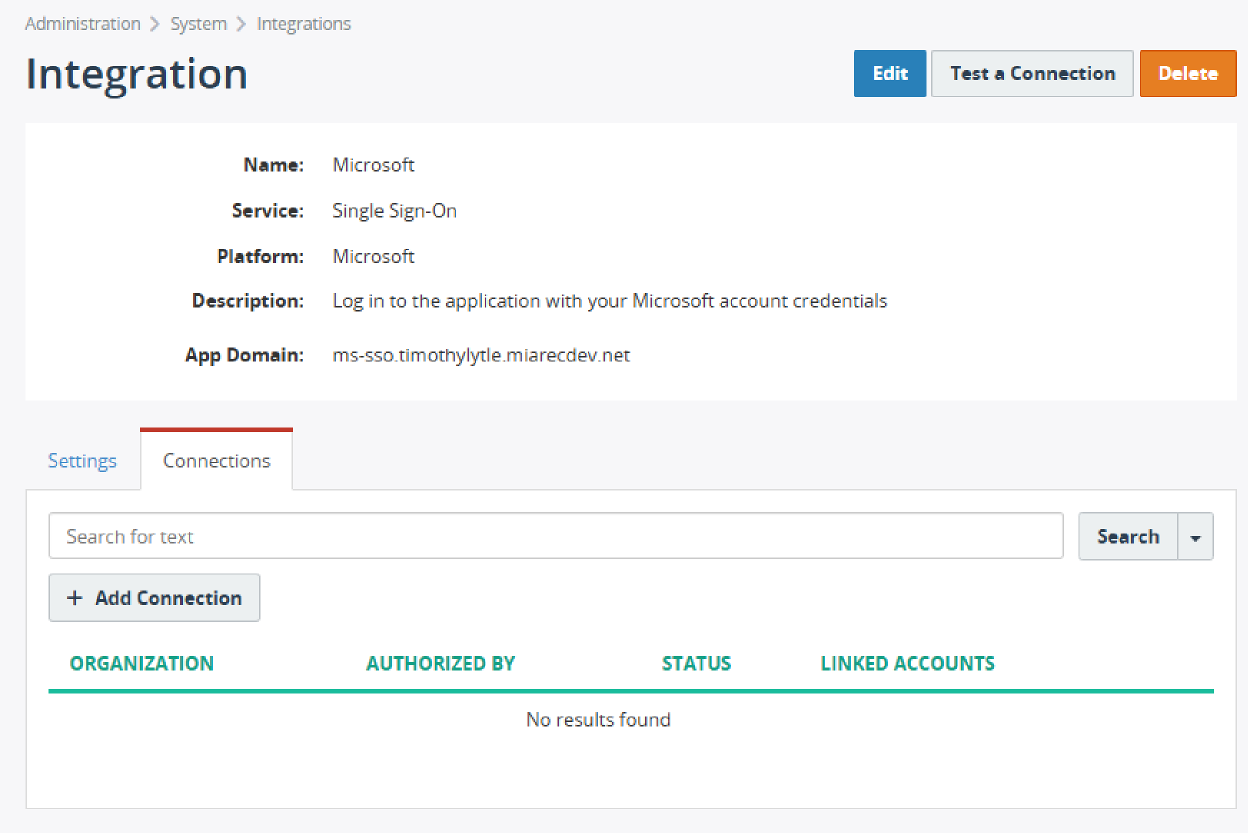
If the “Auto-Active SSO” option was disabled on the Integration, then the tenant admin must log in to Call Recording portal using username/password credentials first and explicitly create SSO Connection for their organization.

Create SSO Connection

Note, this step is required only when “Auto-Activate SSO” option was disabled on the Integration. If the “Auto-Active SSO” option was enabled on the Integration, then the tenant admin can use their Microsoft SSO credentials to log in directly to Call Recording portal

Navigate to **Administration > System > Integrations**

- Select the Microsoft Integration, note it may be named differently in your deployment
- Select the **Connections** tab
- Select **+Add Connection**



Administration > System > Integrations

Integration

Name: Microsoft

Service: Single Sign-On

Platform: Microsoft

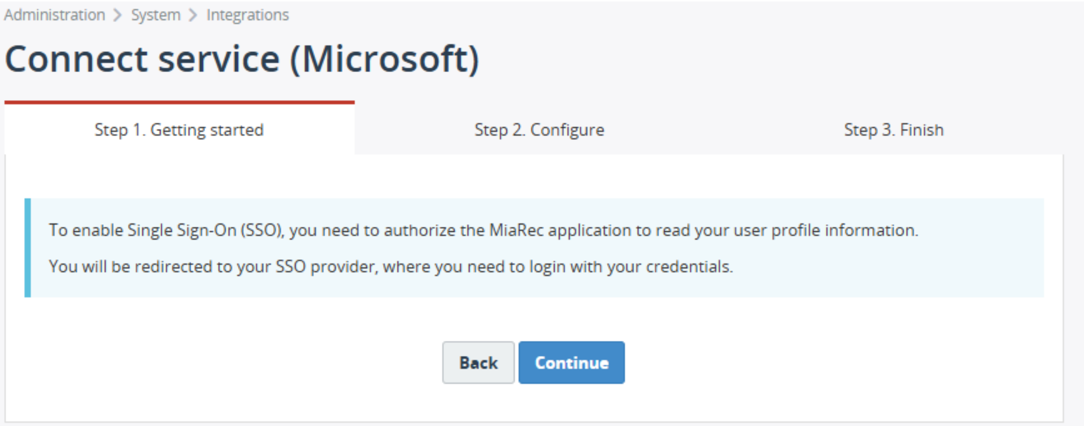
Description: Log in to the application with your Microsoft account credentials

App Domain: ms-sso.timothylytle.miarecdev.net

ORGANIZATION	AUTHORIZED BY	STATUS	LINKED ACCOUNTS

No results found

At *Connect service Step 1*, select **Continue**



Administration > System > Integrations

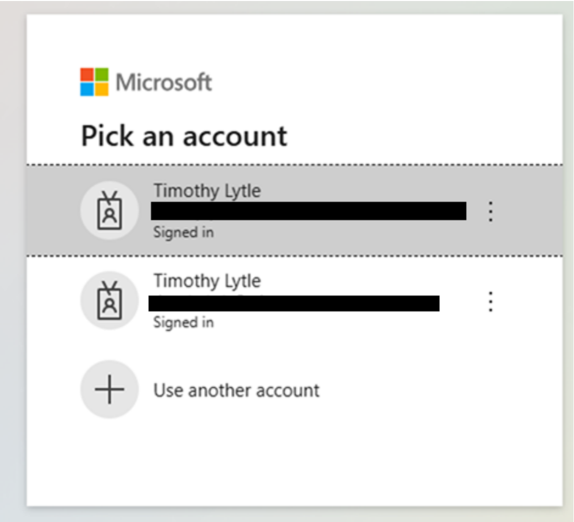
Connect service (Microsoft)

Step 1. Getting started | Step 2. Configure | Step 3. Finish

To enable Single Sign-On (SSO), you need to authorize the MiaRec application to read your user profile information.

You will be redirected to your SSO provider, where you need to login with your credentials.

Choose an admin account, and **Accept** the requested Permissions



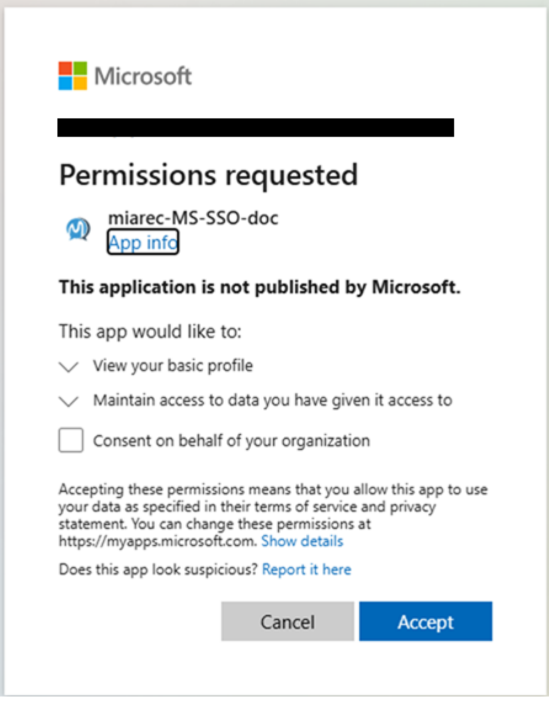
Microsoft

Pick an account

Timothy Lytle
[redacted]
Signed in

Timothy Lytle
[redacted]
Signed in

Use another account



Microsoft

[redacted]

Permissions requested

miarec-MS-SSO-doc
App info

This application is not published by Microsoft.

This app would like to:

- View your basic profile
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

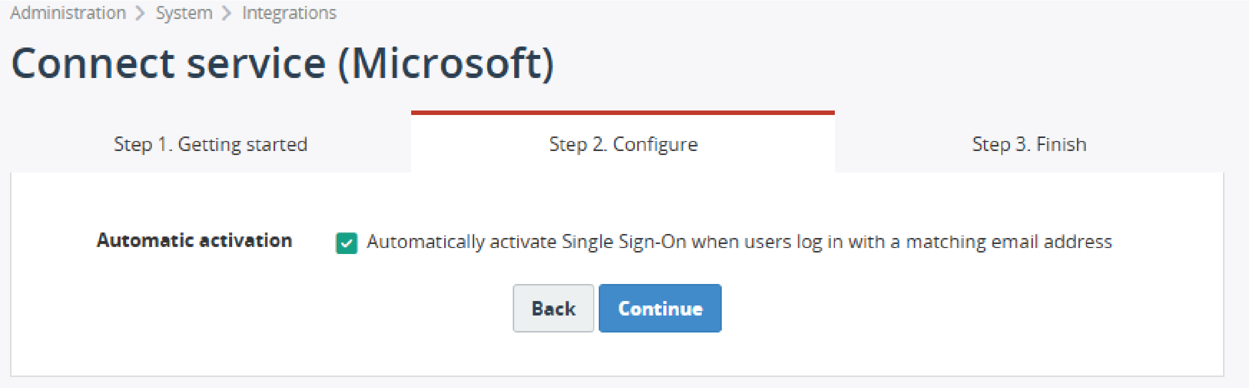
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

At *Connect service Step* 2:

- Set *Automatic activation* to **enabled**. When enabled, users will not need to access Call Recording with username/password on first login, they can use SSO from start.

Select **Continue**

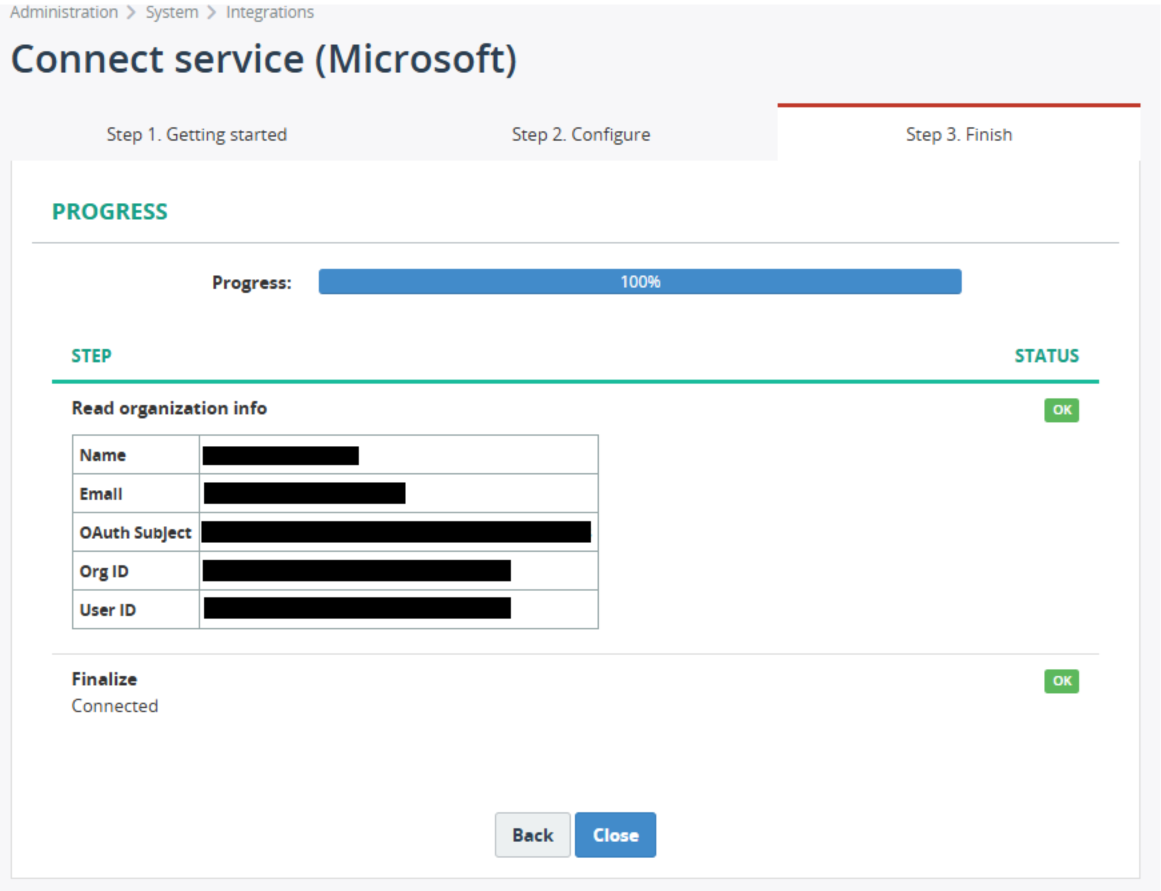


Administration > System > Integrations

Connect service (Microsoft)

Automatic activation ☑ Automatically activate Single Sign-On when users log in with a matching email address

MiaRec/Call Recording will connect to Azure AD and verify access



Administration > System > Integrations

Connect service (Microsoft)

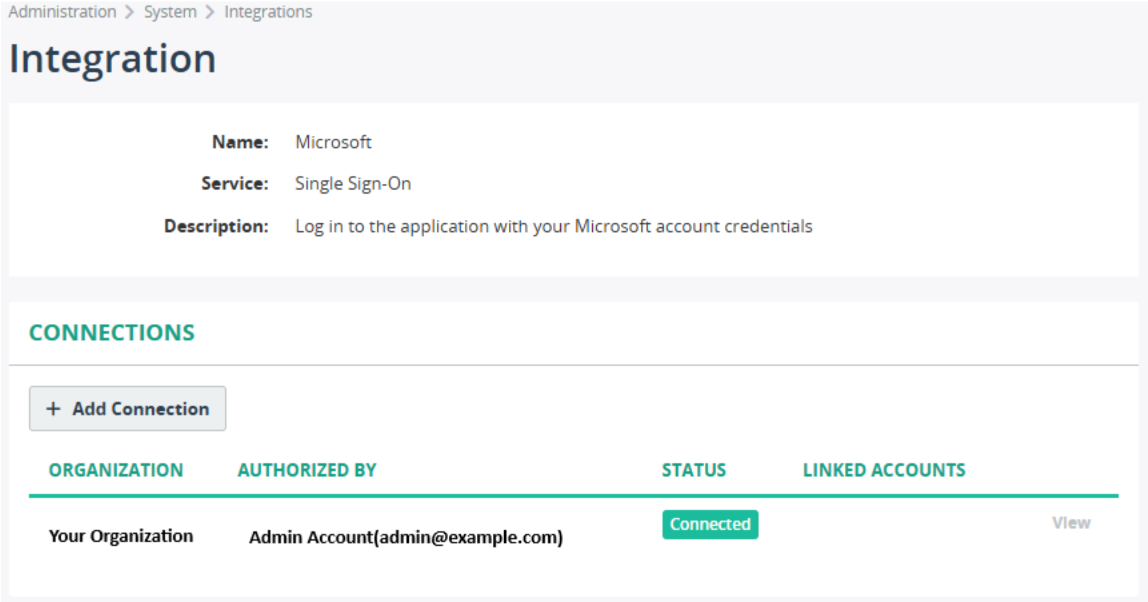
PROGRESS

Progress: 100%

STEP	STATUS
Read organization info	OK
Finalize Connected	OK

Name	[redacted]
Email	[redacted]
OAuth Subject	[redacted]
Org ID	[redacted]
User ID	[redacted]

If successful, you will see **Connected** as the Status of the Connection



Administration > System > Integrations

Integration

Name: Microsoft

Service: Single Sign-On

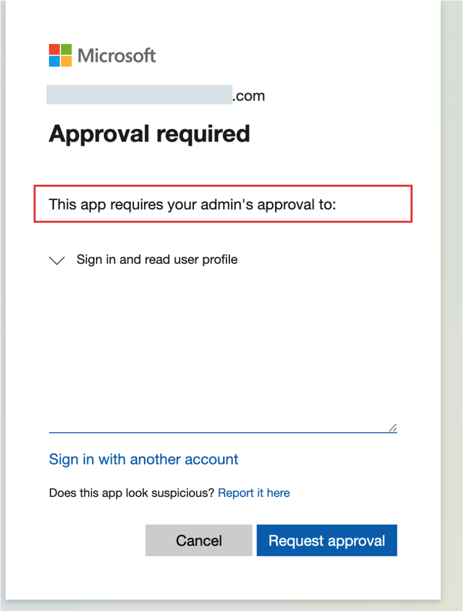
Description: Log in to the application with your Microsoft account credentials

CONNECTIONS

ORGANIZATION	AUTHORIZED BY	STATUS	LINKED ACCOUNTS	
Your Organization	Admin Account(admin@example.com)	Connected		View

Grant Tenant-wide Admin Consent (Optional)

Depending on the organization settings, an admin approval may be required before users can use Microsoft SSO credentials to log into the Call Recording application. When a user first attempts to use their Microsoft credentials to log into the Call Recording application, they will see the error “Approval required. This app requires your admin’s approval to…”, like shown in the following screenshot.



Microsoft

[redacted].com

Approval required

This app requires your admin's approval to:

Sign in and read user profile

Sign in with another account

Does this app look suspicious? Report it here

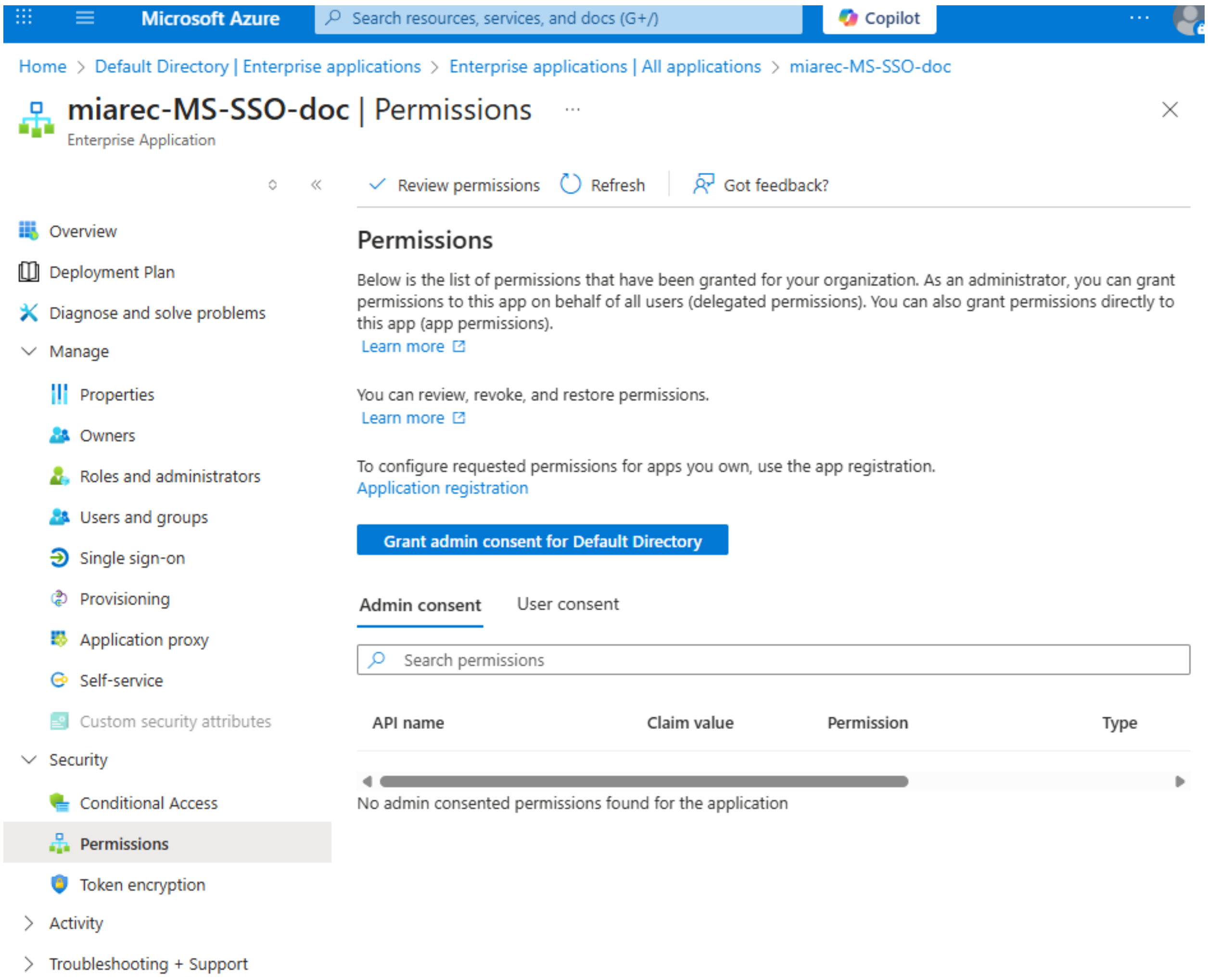
[Additional Information]

The approval should be done by the user who has administrative permission in the Microsoft tenant account.

Sign in to the Azure Portal with an administrator account.

Navigate to **Entra ID > Enterprise apps > All Applications**

- Locate the Call Recording application by its name
- Under *Security*, Select **Permissions**



Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions).
Learn more

You can review, revoke, and restore permissions.
Learn more

To configure requested permissions for apps you own, use the app registration.
Application registration

Grant admin consent for Default Directory

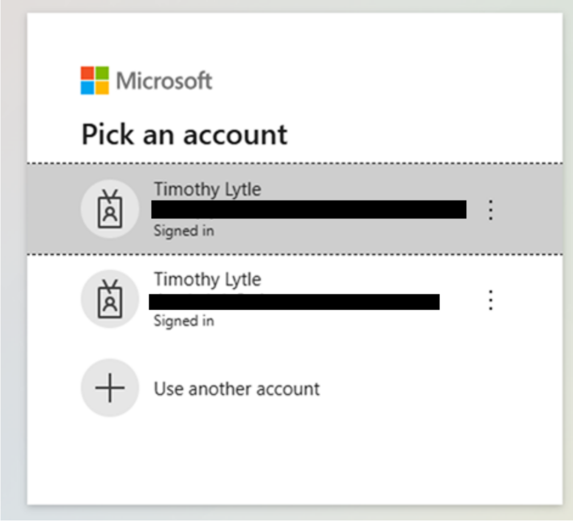
Admin consent | User consent

Search permissions

API name	Claim value	Permission	Type

No admin consented permissions found for the application

- Select the **Grant admin consent for <tenant name>** button
- Choose an admin account, and **Accept** the requested Permissions

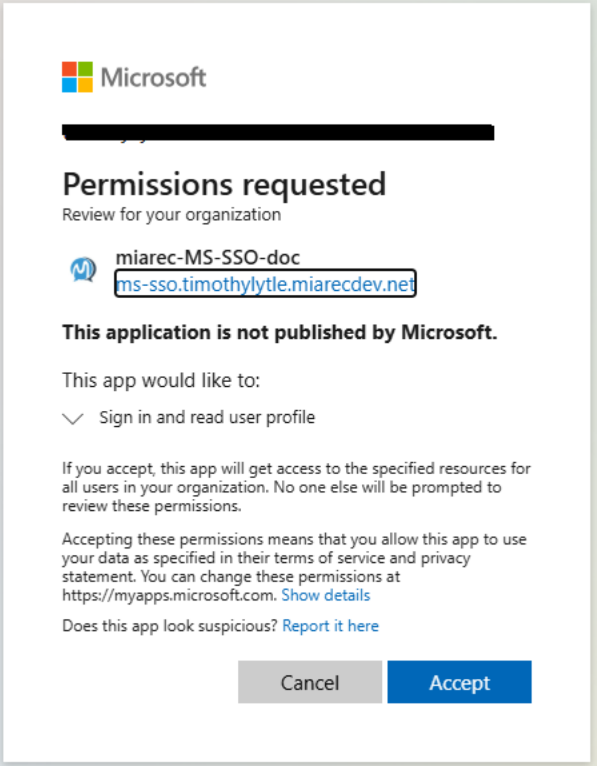


Pick an account

Timothy Lytle
[redacted]
Signed in

Timothy Lytle
[redacted]
Signed in

Use another account



[redacted]

Permissions requested

Review for your organization

miarec-MS-SSO-doc
ms-sso.timothylytle.miarecdev.net

This application is not published by Microsoft.

This app would like to:

Sign in and read user 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. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel | Accept

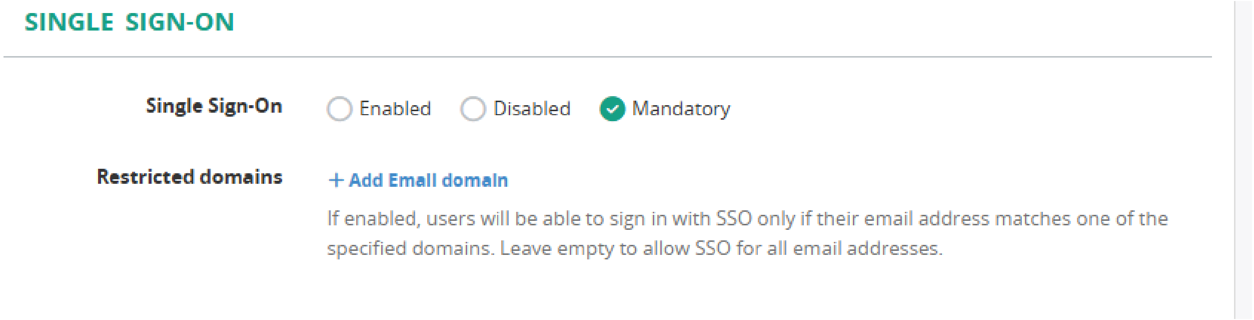
Admin consent for the entire tenant is now granted.

Enforce SSO Login (Optional)

By default, the Single Sign On option is provided as an alternative to the username/password authentication. It is possible to enforce SSO for all users.

Navigate to **Administration > User Authentication > Password Policy**

- Select **Edit Configuration**
- In the *SINGLE SIGN-ON* section, Set **Single Sign-On** to **Mandatory**



SINGLE SIGN-ON

Single Sign-On ○ Enabled ○ Disabled ● Mandatory

Restricted domains + Add Email domain

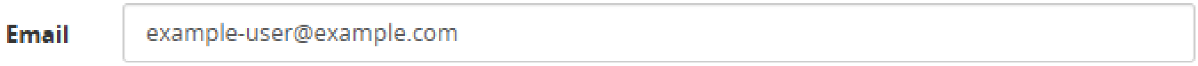
If enabled, users will be able to sign in with SSO only if their email address matches one of the specified domains. Leave empty to allow SSO for all email addresses.

Important: If SSO is enforced for the entire organization, the users will not be able to use their username/password to log into the Call Recording portal. If the SSO integration is unavailable for any reason, a support ticket should be created with the Service Provider to reset the settings.

Enforce for a single User

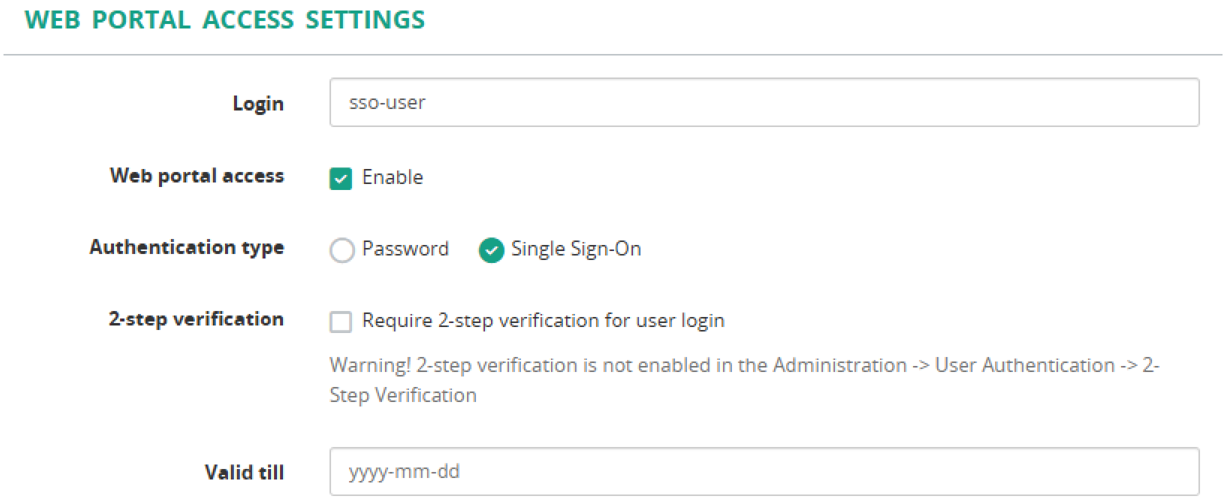
Navigate to a User profile **Administration > User Management > Users,** then select the user:

- Set an **Email** for the user this has to ***be the same email configured for the user in Azure Entra ID***



Email: example-user@example.com

- Set **Authentication type** to **Single Sign-On**



WEB PORTAL ACCESS SETTINGS

Login	sso-user
Web portal access	☑ Enable
Authentication type	○ Password ● Single Sign-On
2-step verification	□ Require 2-step verification for user login Warning! 2-step verification is not enabled in the Administration -> User Authentication -> 2-Step Verification
Valid till	yyyy-mm-dd

Important: If a user is set to *Password*, Single Sign-On is allowed for the user implicitly.

Configure Restricted domains for SSO (Optional)

The Restricted Domains setting allows administrators to control which users can sign in with Single Sign-On (SSO) based on their email domain.

- When populated:
  Users will only be able to authenticate via SSO if the domain portion of their email address matches one of the domains listed here.

  For example, if you add:

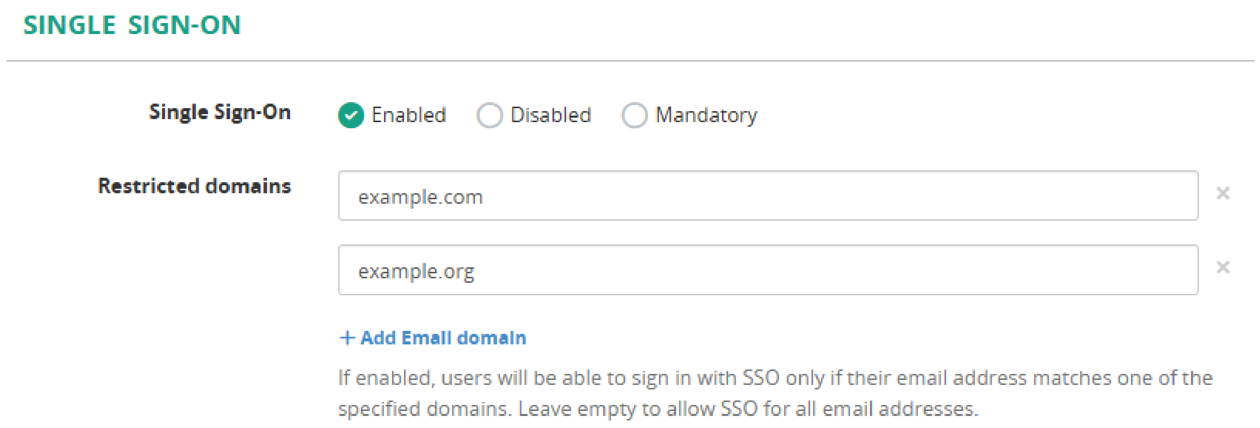
  - example.com
  - example.org

  then only users whose email addresses end with @example.com or @example.org will be allowed to log in using SSO.

- When left empty:
  SSO login is available to any user whose account is otherwise eligible, as long as their email matches to the email address in their user profile in Call Recording.

To Configure:

- Navigate to **Administration > User Authentication > Password Policy**
- Select **Edit Configuration**
- In the *SINGLE SIGN-ON* section, select **+ Add Email Domain**
- Add domains as needed



SINGLE SIGN-ON

Single Sign-On ● Enabled ○ Disabled ○ Mandatory

Restricted domains: example.com ×

example.org ×

+ Add Email domain

If enabled, users will be able to sign in with SSO only if their email address matches one of the specified domains. Leave empty to allow SSO for all email addresses.

Important: If an email domain mismatch occurs, the user will be blocked from logging in via SSO, even if they have valid credentials with the IdP.