# VOSS Automate 24.1 - Microsoft Customers, Upgrade Planning for App Registration

Release 24.1

Jun 19, 2024



## Contents

# Introduction

Automate 24.1 introduces application authentication for Microsoft Teams, which is the security practice that Microsoft recommends, and which it will implement starting July 2024.

This guide describes considerations for upgrade planning, and provides the steps to take pre and post upgrade to VOSS Automate 24.1 in order to add application (app) registration as an authentication and authorization method for MS Teams PowerShell support, and to prevent service disruptions in Automate.

**Note:** This guide is *only* relevant if you're using VOSS Automate with Microsoft.

# Microsoft Multifactor Authentication

Starting July 2024, Microsoft is changing the way it handles resource accounts and is enforcing multifactor authentication (MFA) on all service accounts. These authentication changes will prevent the use of the current service account since administrators will require the `User.Read-Write` permission to add resource accounts.

While Automate supports both app registration authentication and basic authentication (basic auth), basic auth will stop working when Microsoft implements multifactor authentication since basic auth requires service account credentials.

It is strongly recommended that you upgrade your application registration process *prior* to the implementation of Microsoft's changes.

## 2.1 Resource Accounts

Microsoft has paused implementation of application-based authentication for resource accounts while they rebuild the infrastructure for this functionality.

Once Microsoft implements multifactor authentication and the requirement to use application authentication, customers will no longer be able to create, update, or delete resource accounts when upgrading to Automate 24.1.

List (import/sync) of resource accounts is supported with application authentication in Automate 24.1.

**Note:** Contact VOSS support for assistance if you wish to apply a workaround until Microsoft implements this change.

## 2.2 Role Changes

Only Microsoft 365 Global Admins or User Admins will be able to create and manage resource accounts in Automate 24.1.

The following roles will no longer have *user create* permissions on resource accounts:

- Teams Administrator
- Teams Communications Administrator
- Teams Telephony Administrator

Organizations using these Teams roles will require administrators with the user create permission, such as *Microsoft 365 Global Admin* or *User Admin*, to create and manage resource accounts.

Before upgrading to Automate 24.1, you'll need to identify whether your Teams Voice Administrators with responsibilities for creating resource accounts have Microsoft 365 user create and management permissions, and to update their permissions as required.

# App Registration for MS Teams PowerShell in Automate 24.1

The *Application Registration for MS Teams PowerShell* feature (delivered in VOSS-1265 for Automate 24.1) provides:

- (Recommended approach) A single app registration that can be set up for Microsoft Graph, Microsoft Teams PowerShell, and Microsoft Exchange PowerShell - *with certificate*
- A single app registration that can be used for Microsoft Graph and Microsoft Teams PowerShell - *with shared secret*

---

**Note:** For Microsoft Graph, Automate currently (pre-24.1) supports basic auth. In Automate 24.1, app registration is supported with secret or certificate. For Microsoft Exchange, only the certificate method is supported.

---

Customers with Microsoft tenants will need to prepare their tenants before upgrading to Automate 24.1 so that their application registration is configured with the correct roles, permissions, and authentication methods.

Application registration for authentication/authorization is the most secure and controlled way to provide VOSS Automate with access to customer tenants. Removing the dependency on a system account with basic auth provides customers with the ability to leverage certificates and/or secrets in order to provision and manage Teams Administration tasks using VOSS Automate.

---

**Note:** App registration authentication and authorization method replaces *basic authentication* to deliver a more secure method of connectivity. This means it is no longer mandatory to fill out the basic auth fields (username and password) for MS Teams in the tenant details.

---

## 3.1 Service Account and App Registration Changes - New and Existing Tenants

### Existing Tenants

Existing tenants on an upgraded system can continue working as before the upgrade, provided you perform the steps to update the tenant configuration. Once completed, it is no longer mandatory to specify a Teams service account name and password in order to have all the supported functionality that was in place before upgrading (with the current exception of resource account management).

### New Tenants

For new tenant registration it will no longer be mandatory to specify a MS Teams service account name and password in order to have all the supported functionality that was in place before upgrading (with the current exception of Resource Account Management).

The table summarizes the changes resulting from the authentication method change, for new and existing tenants:

| Tenant type | Service User Account Changes | App Registration Changes |
|---|---|---|
| Existing tenants | The legacy service user account will now *only* be required for connecting to sessions to manage Microsoft Teams resource accounts. | The existing application registration will need to be extended to include additional API permissions and to be assigned the Teams Administrator role, similar to the legacy service user account.<br>Additional API permissions include, but are not exclusive to:<br>• Skype and Teams Tenant Admin API full application rights<br>• Exchange Server rights<br>• User.ReadWrite permissions<br>These permissions must be added by a customer administrator for the applications in their tenants. |
| New tenants | The legacy service user account is no longer mandatory, but will be required for each customer tenant entry that wants to manage Microsoft Teams resource accounts. | New Microsoft tenants will have two options for app registration - either of the following:<br>• Shared Central Application Registration<br>• Tenant-specific Tenant Application Registration<br>You can find out more about these options below. |

## 3.2 App Registration Options - New Tenants

This guide describes two application registration options for new tenants:

- Shared Central Application Registration
- Tenant-specific Tenant Application Registration

The table provides an overview of the app registration options for new Microsoft tenants:

| App Registration Option | Description |
|---|---|
| Shared Central App Registration customers | • Click the link to authorize the application<br>• Assign the Teams and Exchange roles to newly created app registration<br>Either VOSS (for hosted and general customers) or a Service Provider Partner (in a reseller environment) builds and maintains the app registration in their Microsoft Entra ID tenant, and performs organizational and application validation with Microsoft.<br>The API permissions are the same as for a *tenant-specific app registration*. The only configuration difference here is that users from multiple tenants/Entra ID organizations are allowed to leverage the application.<br>VOSS or the Service Provider Partner (SPP) provides the customer with an admin grant link, for example, https://login.microsoftonline.com/global/adminconsent?client_id={client-id}.<br>The customer clicks on the link and agrees, using their Global Admin user. Then they need to assign the Teams and Exchange Administrator roles to the application, like any other user in Entra ID.<br>VOSS or the SPP maintains the certificate and/or secrets securely, and ensures that they're added to VOSS when renewal is required. Once updated, PowerShell proxies automatically receive the updated certificates from VOSS Automate. These settings are maintained at a global or reseller level in VOSS Automate, with customer/tenant-level overrides, if required. |
| Tenant-specific app registration customers | • Assign new permissions to the app registration<br>• Assign the Teams and Exchange roles to the app registration<br>Each customer would each have to build the app registration in their own tenant.<br>VOSS can provide a PowerShell script that builds the application with all required API permissions, and triggers the Admin Grant process and role assignments, based on the customer's Global Admin user executing the script.<br>When the script is executed from the PowerShell proxy it can also configure the WinRM setup, certificate loading, and updates.<br>If customers wish to opt out of the script-assisted setup, they can be provided with documentation for manually building the app registration.<br>Each customer is responsible for maintaining the certificates and for updating the certificates before they expire. |

# Pre-upgrade Steps

**Pre-requisites:**

- Microsoft Azure must be set up before starting your upgrade.

## 4.1 Windows PowerShell Server

1. Run the provided script on the Windows server to configure the PowerShell proxy so that Automate is able to deploy certificates to the Windows server.

   Copy the script to `c:\VOSS` on the Windows server, and run it using a PowerShell prompt, such as the following, where `service_account_name` must be replaced as needed:

   ```
   PS C:\voss> .\conf_proxy_task.ps1 -service_account_name WSMan-svc
   ```

   **Note:** A certificate must be installed on the PowerShell server, the public key must be uploaded to the app registration, and the thumbprint must be copied - you can use an existing generated certificate, if available.

   You won't need to copy the thumbprint if the certificate is only installed on the Windows PowerShell server and not on Automate.

2. Optionally, enable the OpenSSH feature of Windows 2019 or greater to improve file transfer performance from Automate to the Windows server.

## 4.2 Microsoft Tenant

It is recommended that Providers managing multiple tenants switch to a shared central application registration to reduce maintenance and errors due to performing repeated manual configuration.

**Note:** In an upgrade scenario, it is assumed that each customer has an app registration that should be transitioned to central app registration. The upgrade adds the *Skype and Teams Tenant Admin API* permission and the *Teams Administrator* role.

Central app registration allows you to make centralized, once-off changes to the permissions that must be updated in all tenants to prepare for upgrades to Automate 24.1 and to allow all tenants to register with the Provider's application.

**Note:** Central app registration does not configure roles. The tenant assigns roles to the app registration.

## 4.3 Automate

If you switched from a tenant-specific to a shared central app reg, update the tenant in Automate to reflect the new application ID.

# Shared Central App Registration

The instructions for using Central App Auth are as follows:

**Note:** In this procedure you'll also assign the *Teams Administrator* role.

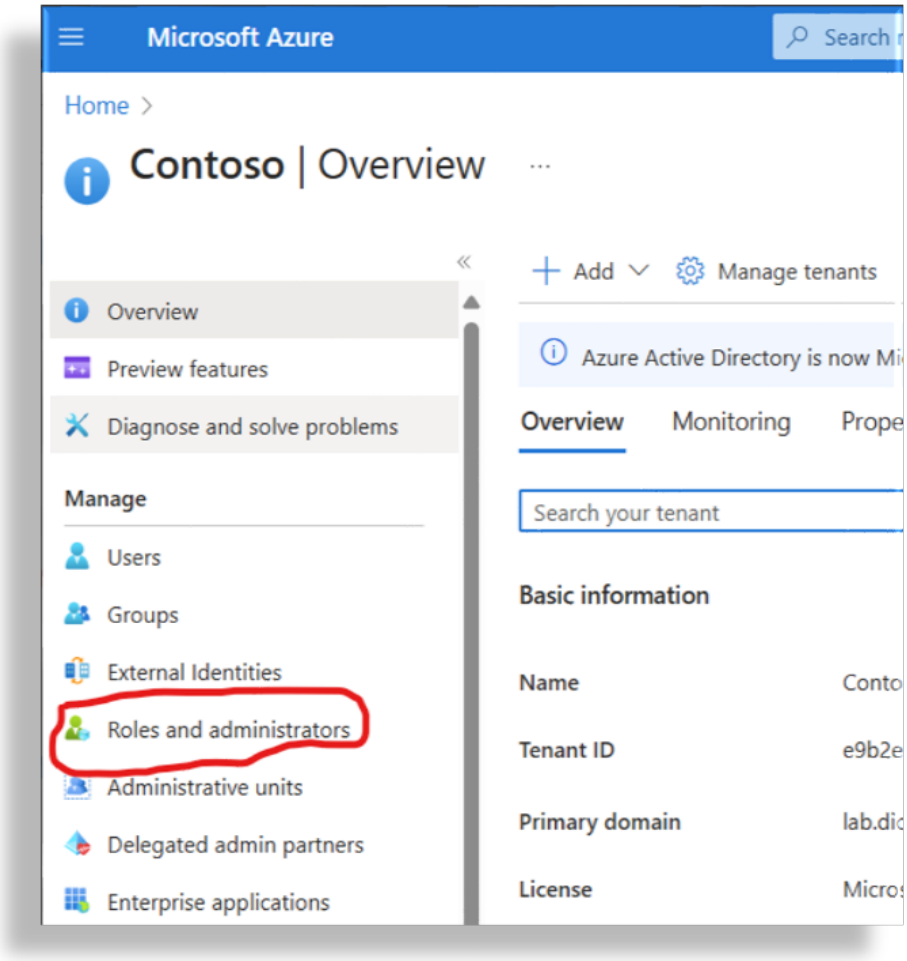
1. Authorize the app in the relevant Microsoft tenant to add Central App to your tenant:

   `https://login.microsoftonline.com/common/adminconsent?client_id={client_ID}`

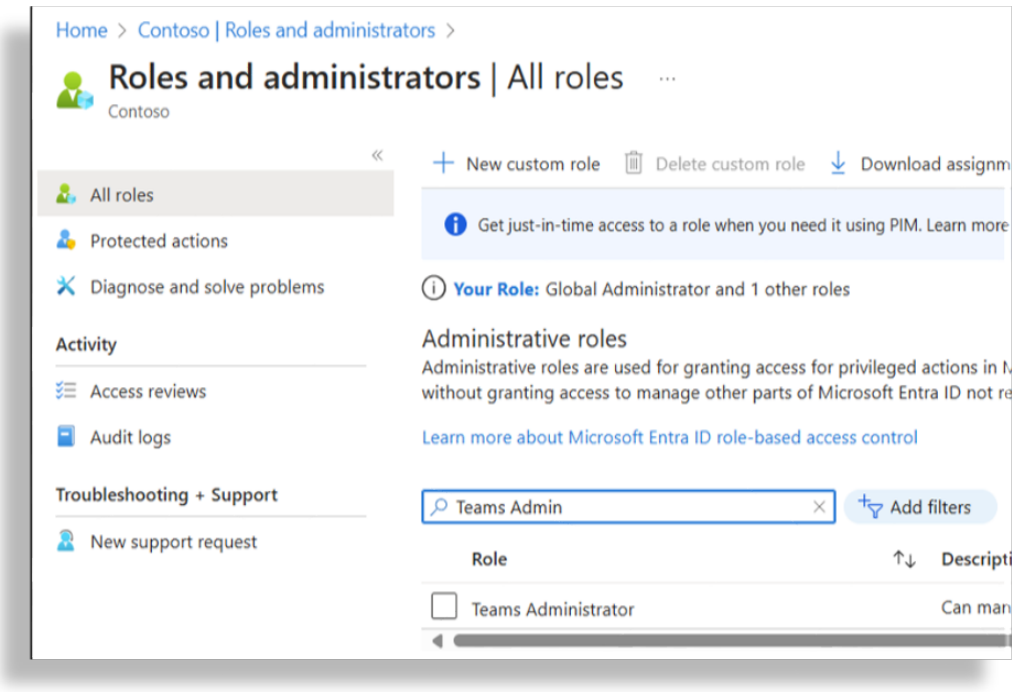
2. Assign the *Teams Administrator* role and the *Exchange Administrator* role to the app:
   a. Go to the **Entra ID** section of the Microsoft Azure Portal:

      `https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Overview`

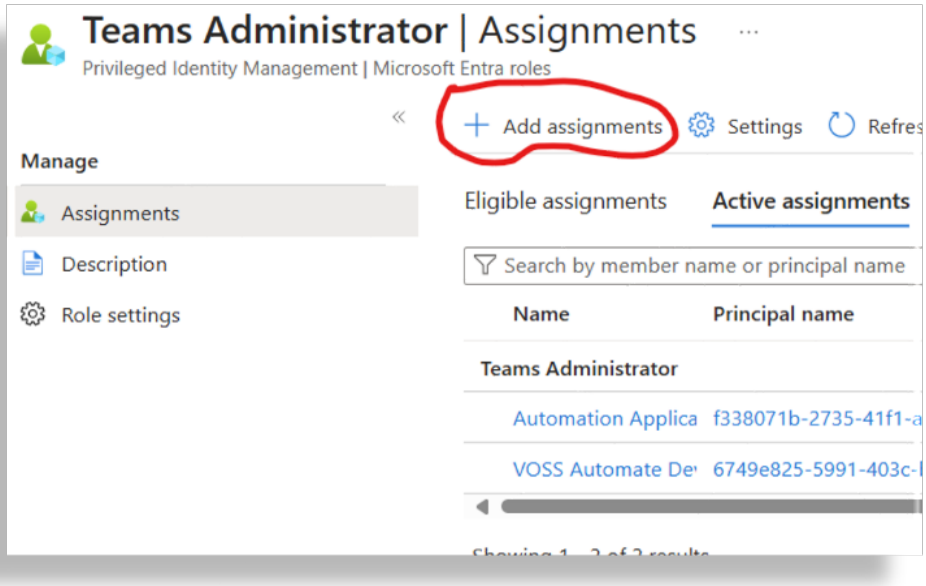
   b. Navigate to **Roles & Administrators**.



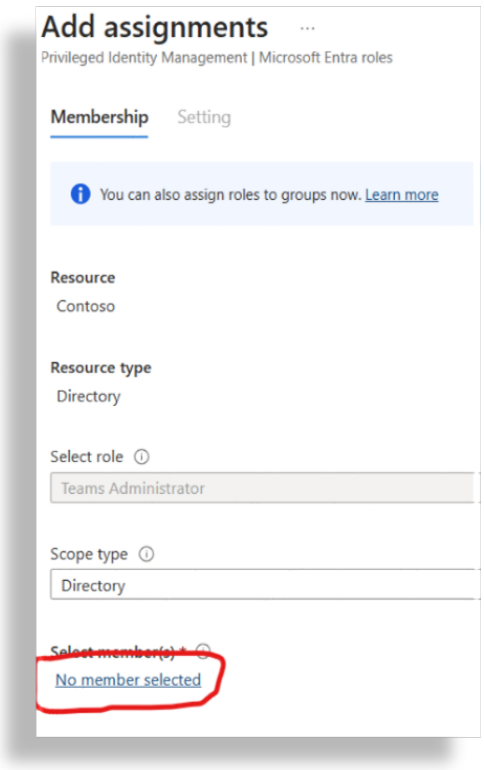

c. Search for *Teams Administrator*.



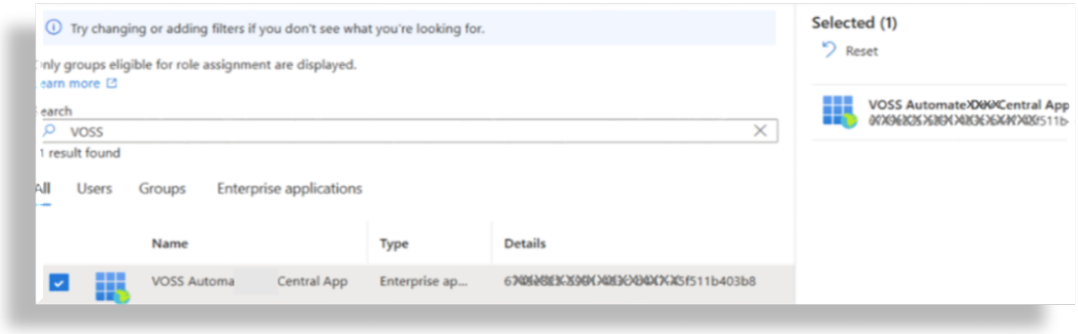

d. Open **Teams Administrator**, then click **Add Assignments**.




e. Select **No member selected**.



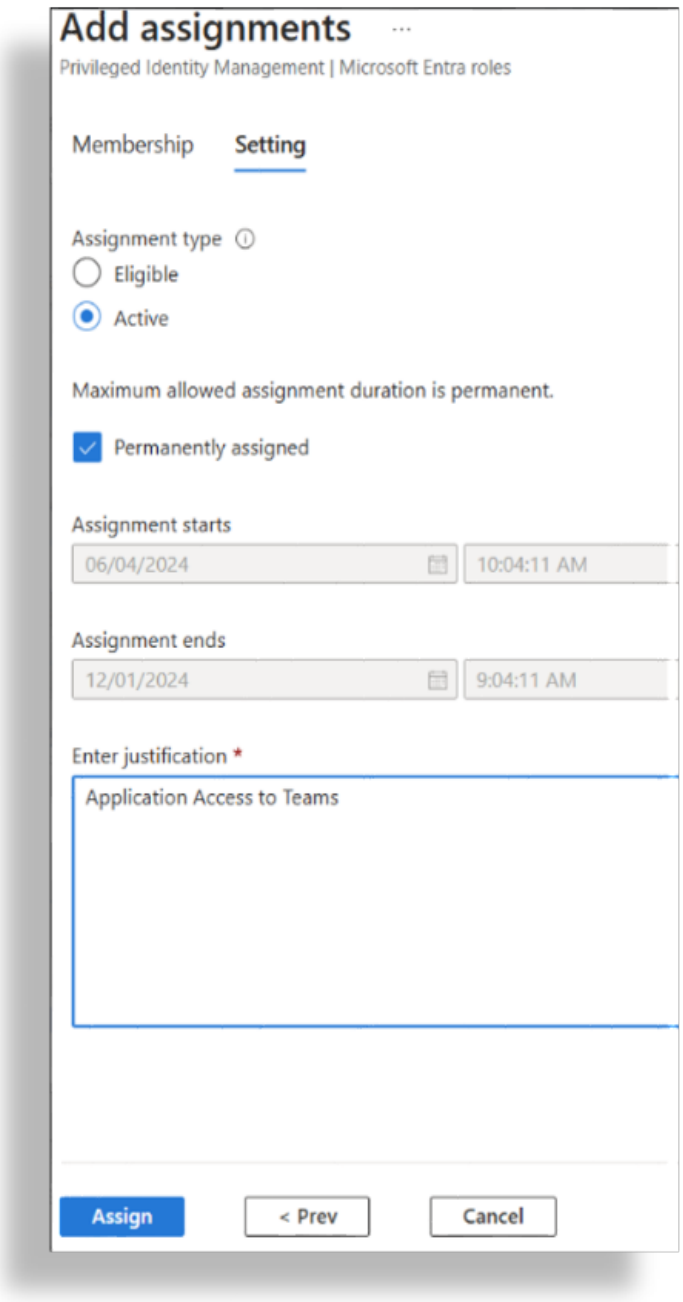

f. Search for *VOSS*, then select the checkbox for **VOSS Automate App**.




g. Click **Next**.

h. At **Enter justification**, fill out a reason for the assignment in the text field.

**Note:** You can add any description in this field.




i. Click **Assign**.

   The new assignment may take a few minutes to complete before it appears in the assignment list (**Teams Administrator | Assignments**).

j. Repeat step 2 from the **Teams Administrator | Assignments** page, but this time, on **Teams Administrator | Assignments**, search for the **Exchange Administrator** role.

3. Install the certificate on the VOSS Automate server.

**Note:** If you're using the VOSS Central App, the certificate is already installed.

4. Configure the VOSS Automate Microsoft tenant to use the “customer” Tenant ID you approved for earlier, along with the App ID (Client ID) and certificate as necessary.

   For example, for VOSS Central App customers:

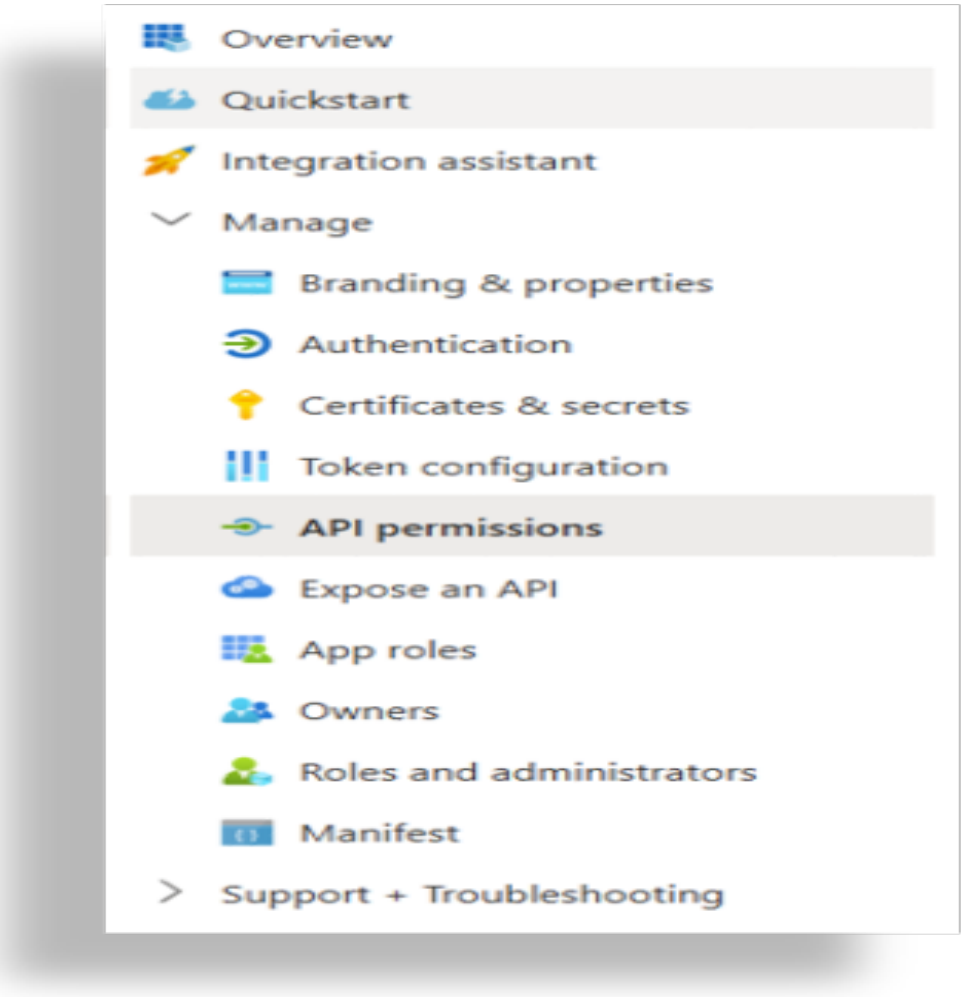
   - App Name: VOSS Automate Central App
   - Client Id: 6749e825-5991-403c-b447-xxxxxxxxxxxx
   - App Created Date Time: 6/4/2024 3:24:31 PM
   - CertificateThumbprint : 2BF36F11BE9317C9217BE6847BEDXXXXXXXXXXXX

## Tenant-Specific App Registration

The instructions for Tenant-specific App Auth are as follows:

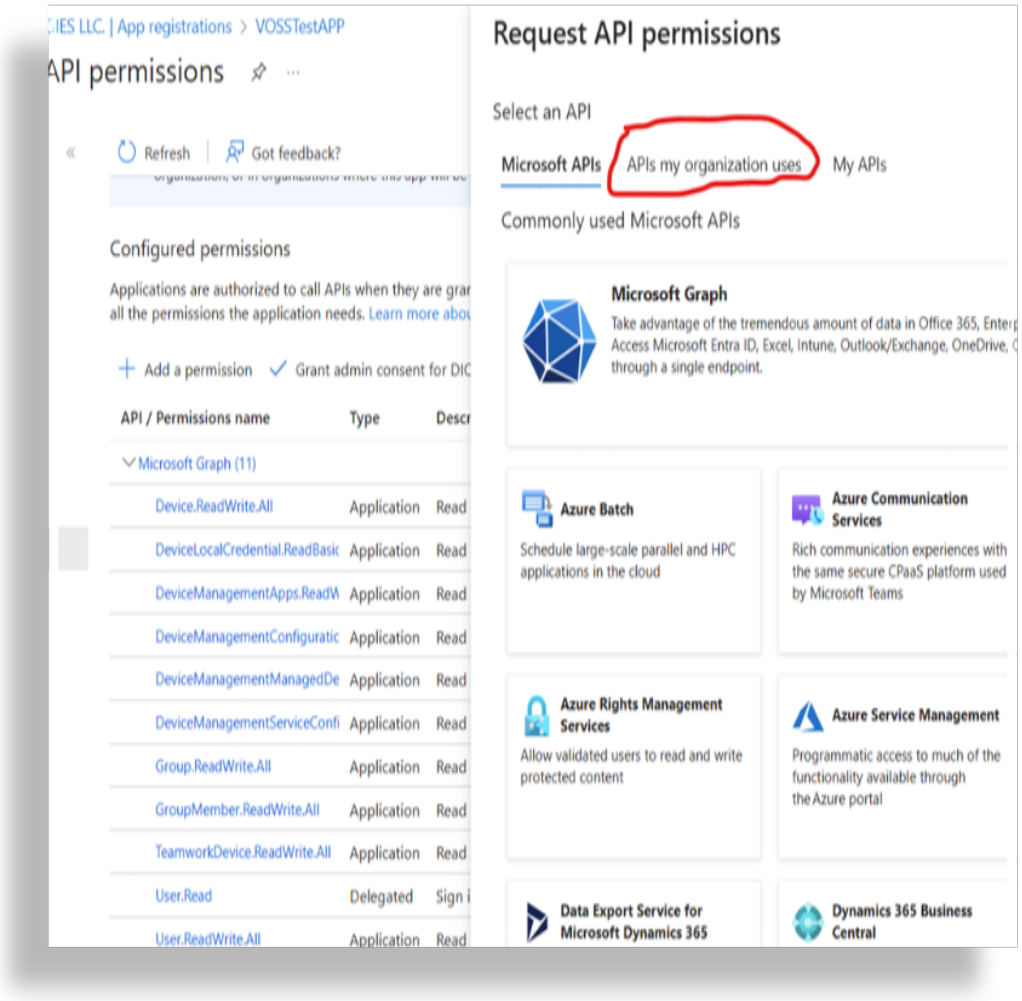
**Note:** In this procedure you’ll also assign the *Teams Administrator* role.

1. Update the API permissions:
   a. Access your existing Application Registration in MS Entra ID or the Azure AD Portal.
   b. Navigate to **API Permissions**.

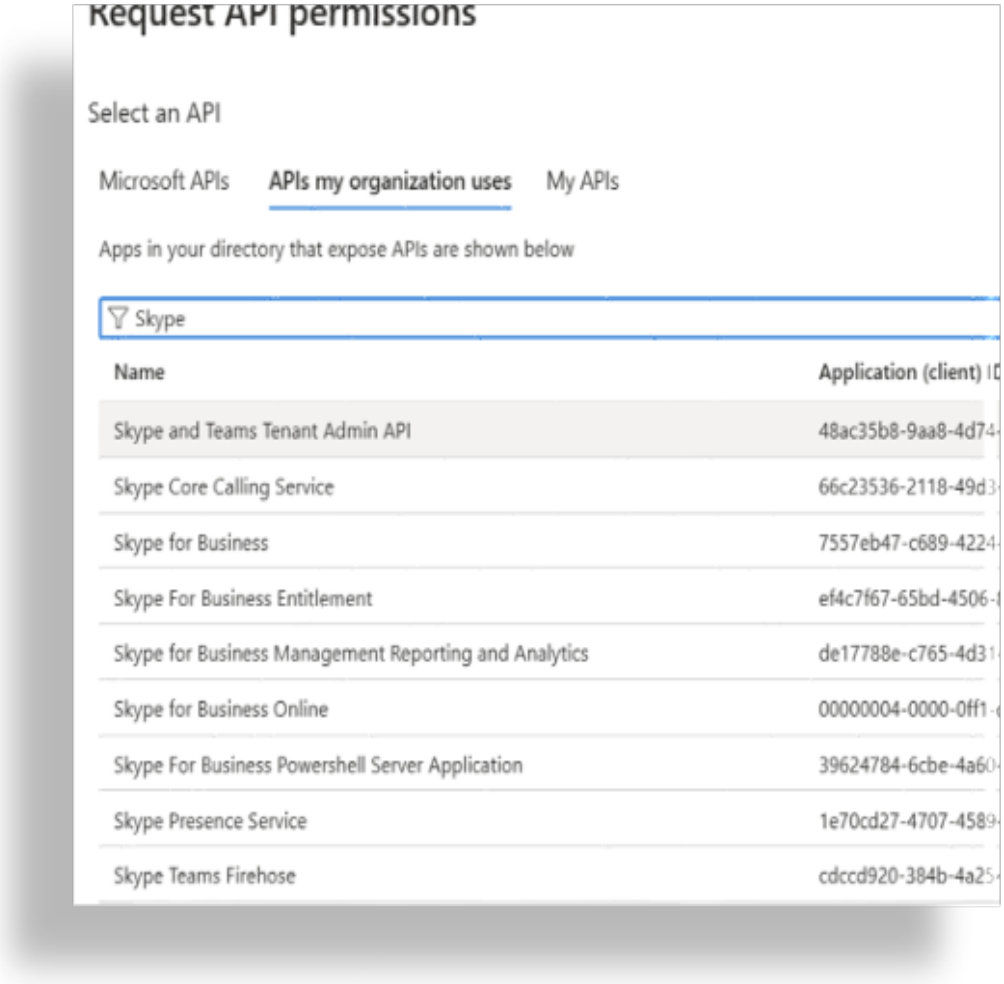



c. In **API Permissions**, select **Add a Permission** to open the **Request API permissions** window.

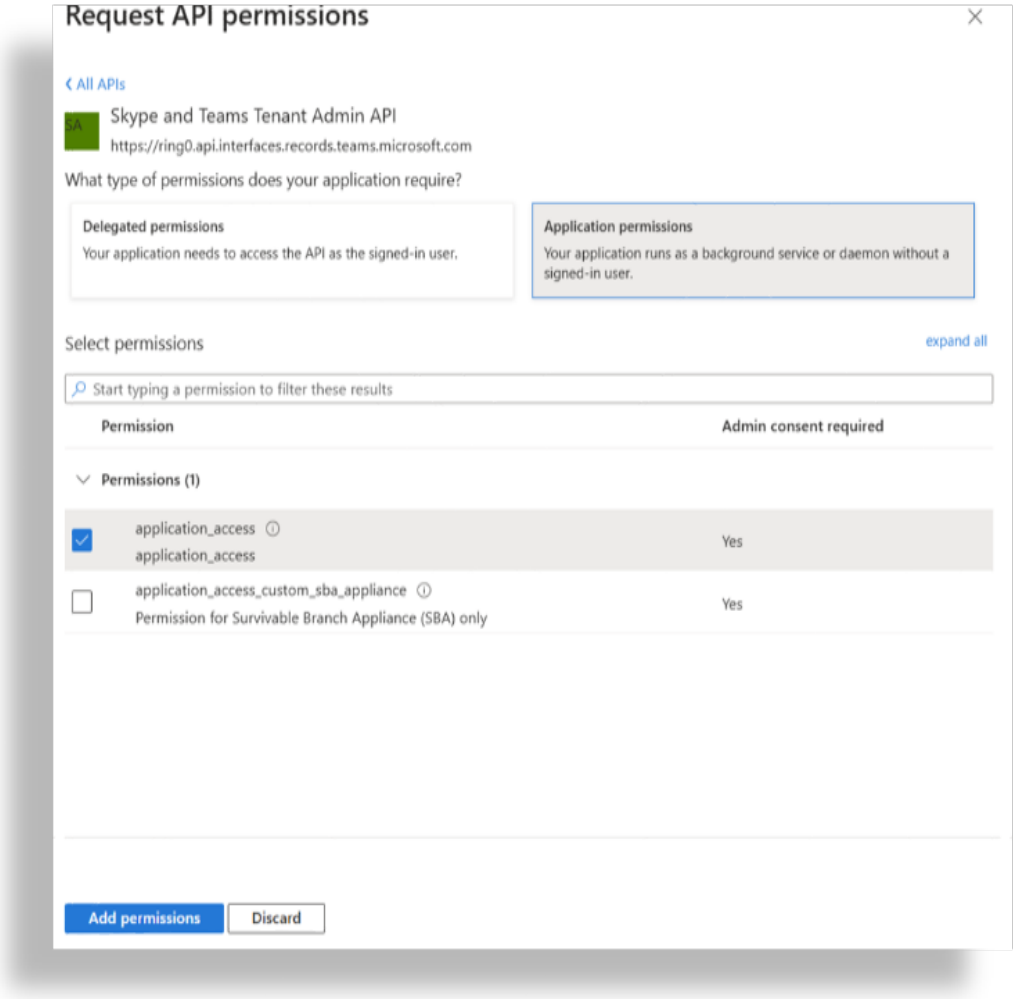
d. In the **Request API permissions** window, select **APIs my organization uses**.



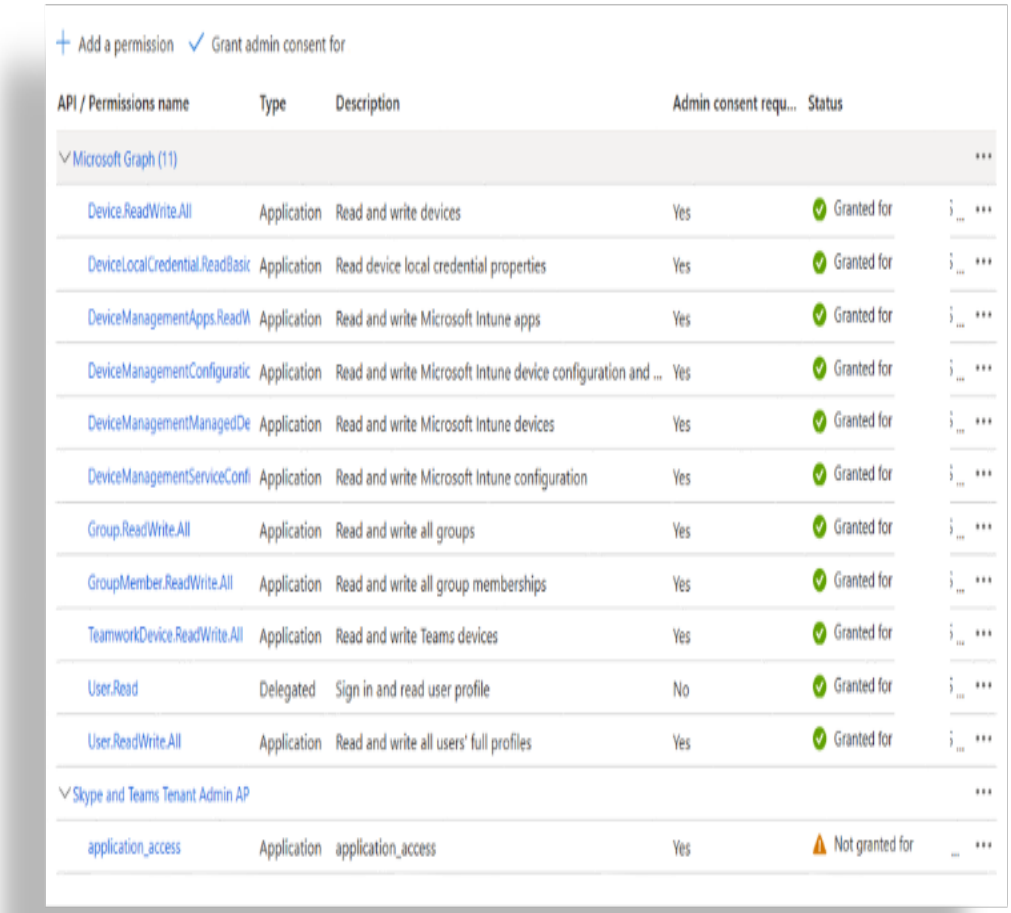

e. In the Search bar, type *Skype*, then select **Skype and Teams Tenant Admin API**.



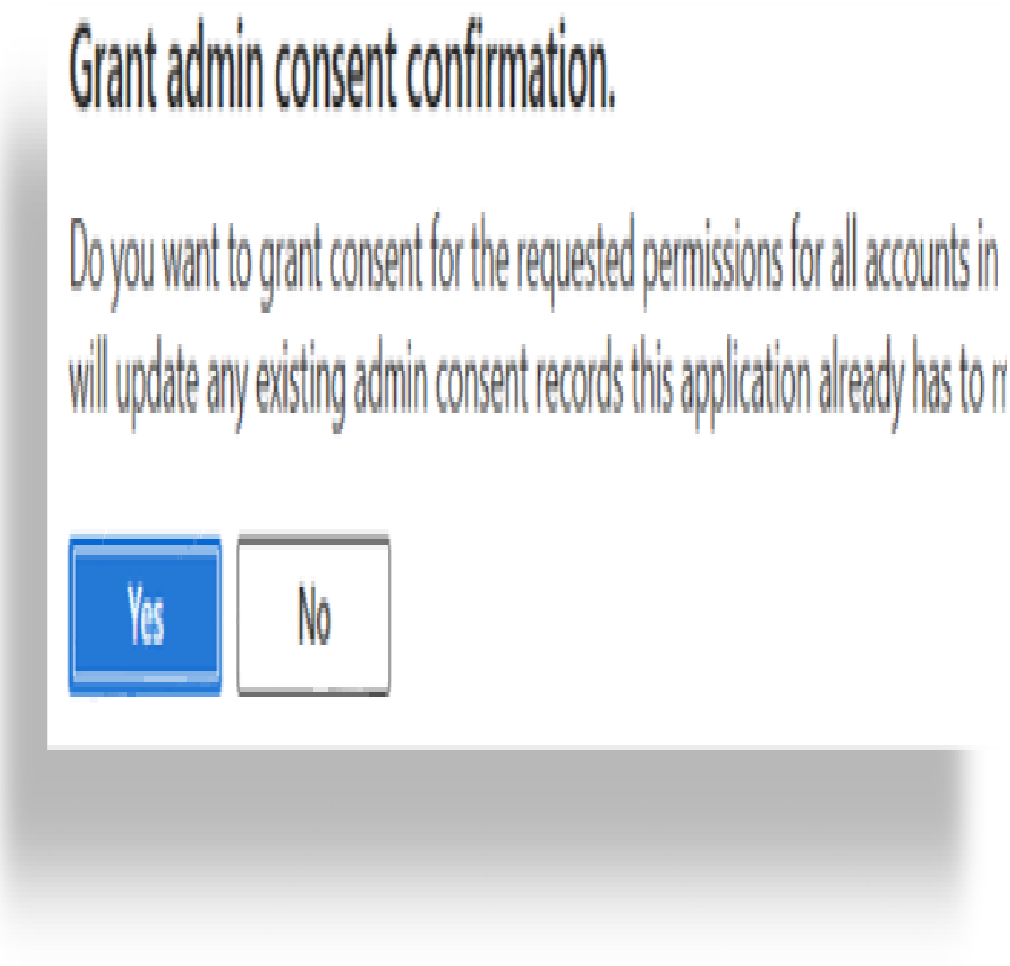

f. Select **Application Permissions**, then select the checkbox for **application_access**, and then click **Add permissions**.




g. View the permission that now displays in the API Permissions list, although it has not yet been granted permission (status is *Not granted for*).



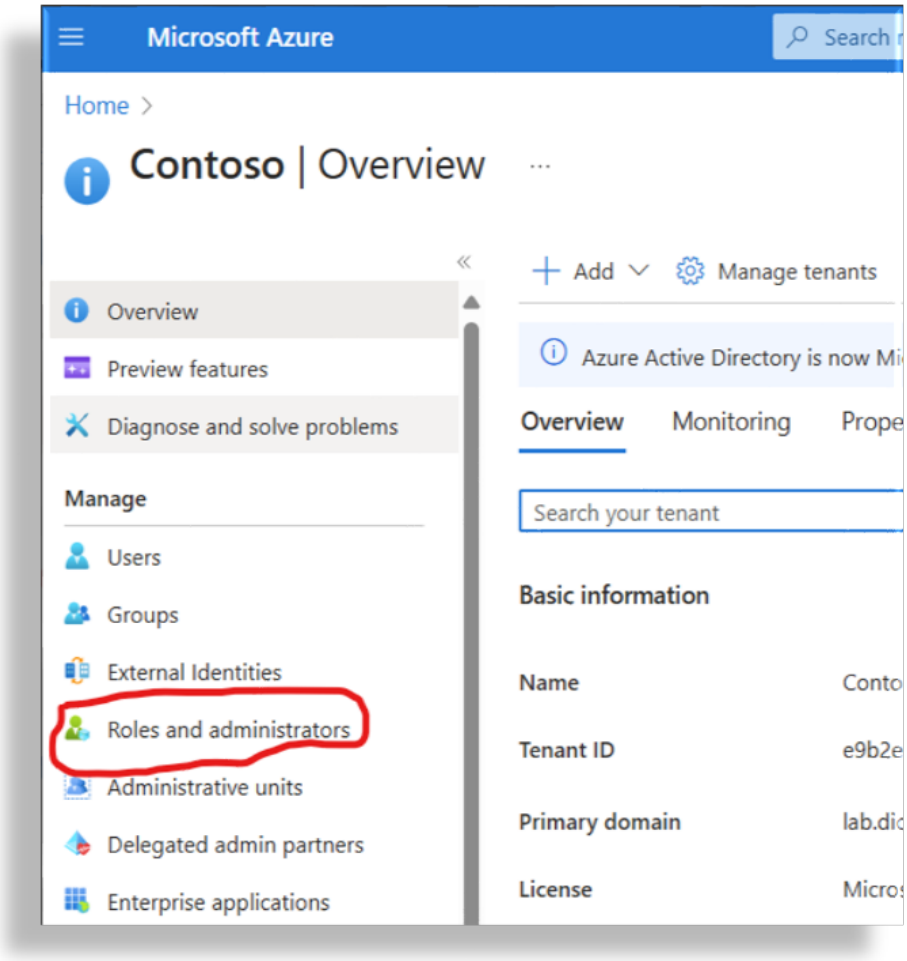

h. At the top of the list, click **Grant admin consent**, and approve the permission.



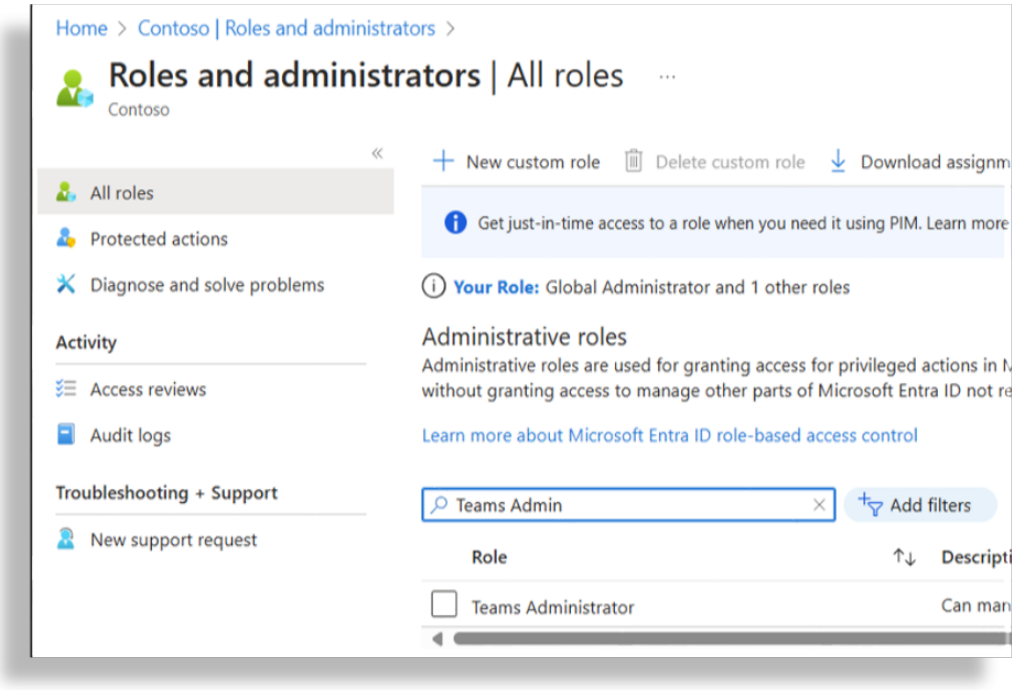

2. Grant the Application the *Teams Administrator* role:
    a. Go to the **Entra ID** section of the Microsoft Azure Portal:

    ```
    https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/
    Overview
    ```

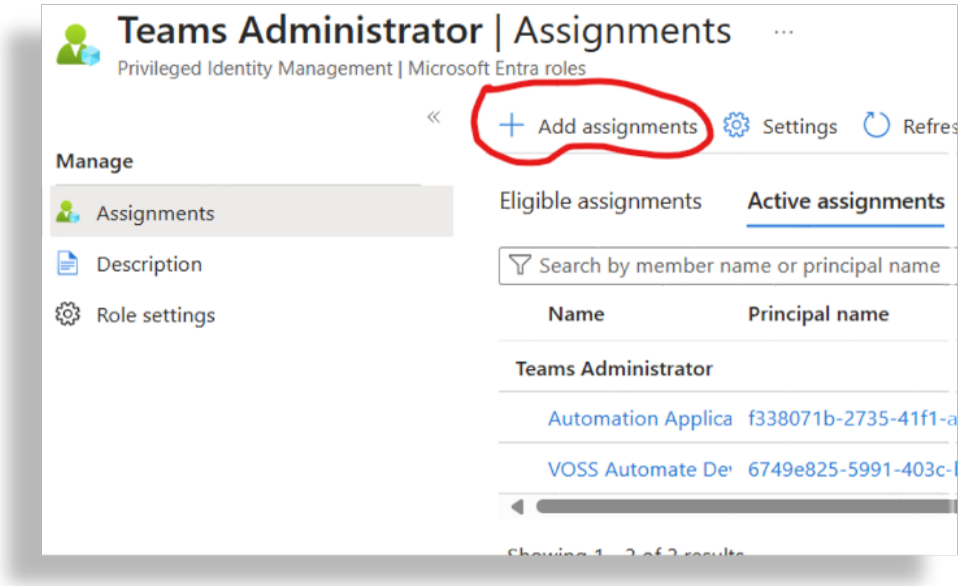
    b. Navigate to **Roles & Administrators**.



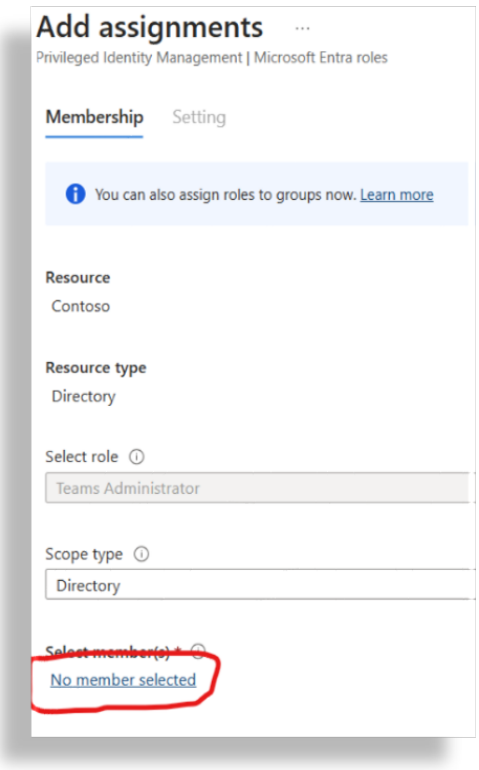

c. Search for *Teams Administrator*.



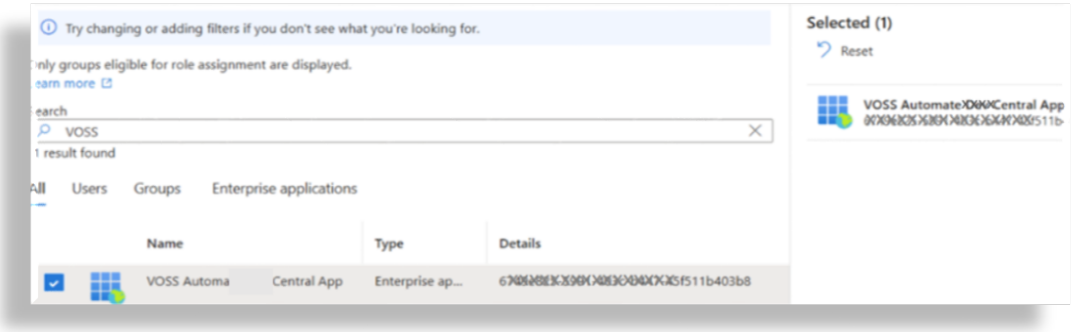

d. Open **Teams Administrator**, then click **Add Assignments**.




e. Select **No member selected**.



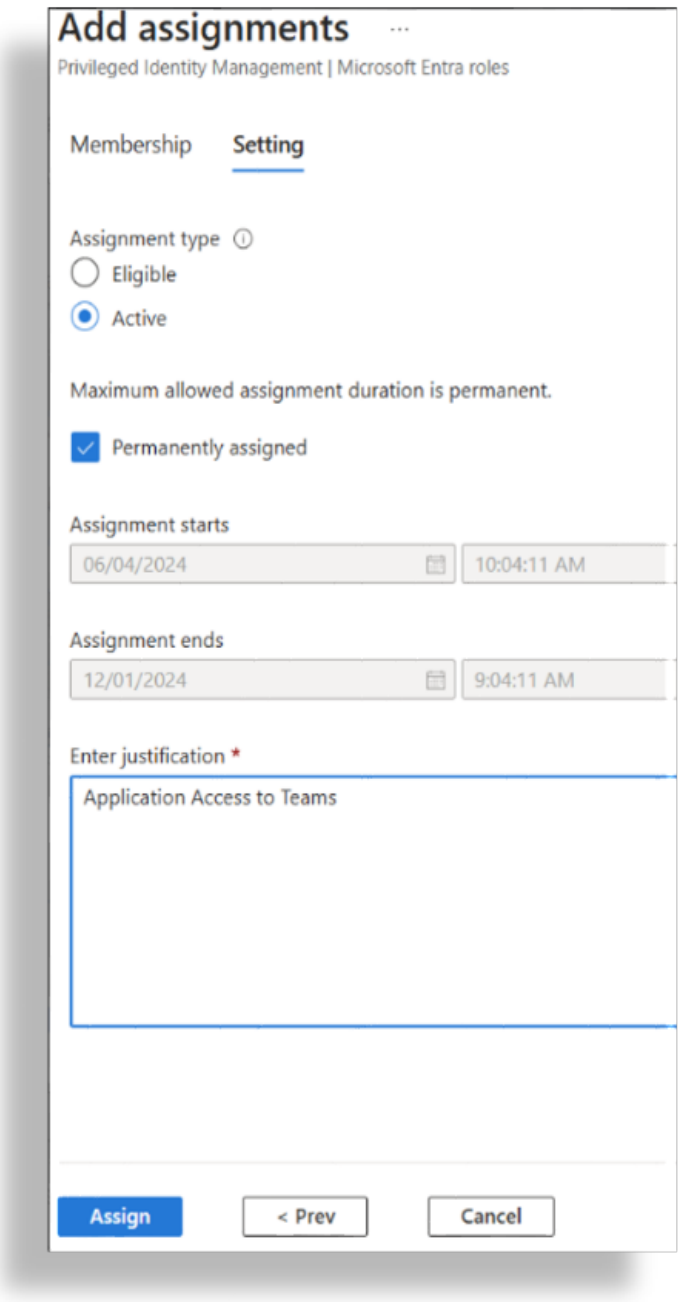

f. Search for *VOSS* (or your app name), then select the checkbox for (in this example) **VOSS Automate App**.




g. Click **Next**.

h. At **Enter justification**, fill out a reason for the assignment in the text field.

**Note:** You can add any description in this field.




i. Click **Assign**.

   The new assignment may take a few minutes to complete before it appears in the assignment list (**Teams Administrator | Assignments**).

j. Repeat step 2 from the **Teams Administrator | Assignments** page, but this time, on **Teams Administrator | Assignments**, search for the **Exchange Administrator** role.

3. Ensure your client/secret and/or certificate are up to date in the application and the correct information is in your Microsoft tenant configuration in VOSS Automate.

# Post-upgrade Troubleshooting

If you're experiencing any issues with Microsoft functionality post-upgrade, you can check the following:

- Restart the Windows Powershell server to ensure that all old sessions are cleared.
- If you have a certificate configured, ensure that it is installed on the Windows Powershell server and on the Azure application registration.