

Bring Your Own Cloud Deployment Guide

PoliteMail v.21.5.0.0.1
August 2021

What is Bring Your Own Cloud? (BYOC)

In PoliteMail 5.0, you can now deploy a “bring your own cloud” infrastructure using Microsoft Azure. Compared to traditional on-premises deployment, BYOC offers a more streamlined setup process using cloud services.

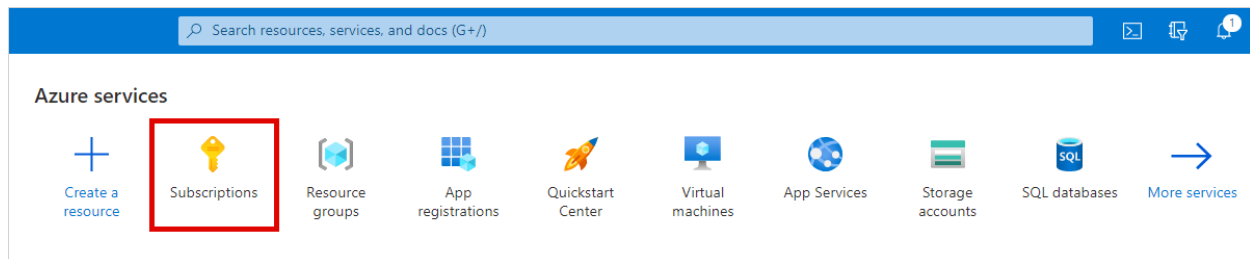
For PoliteMail to deploy your BYOC infrastructure, you will need the following information from your Microsoft Azure services:

- Subscription Name
- Subscription ID
- Application (client) ID
- Directory (tenant) ID
- Client Secret

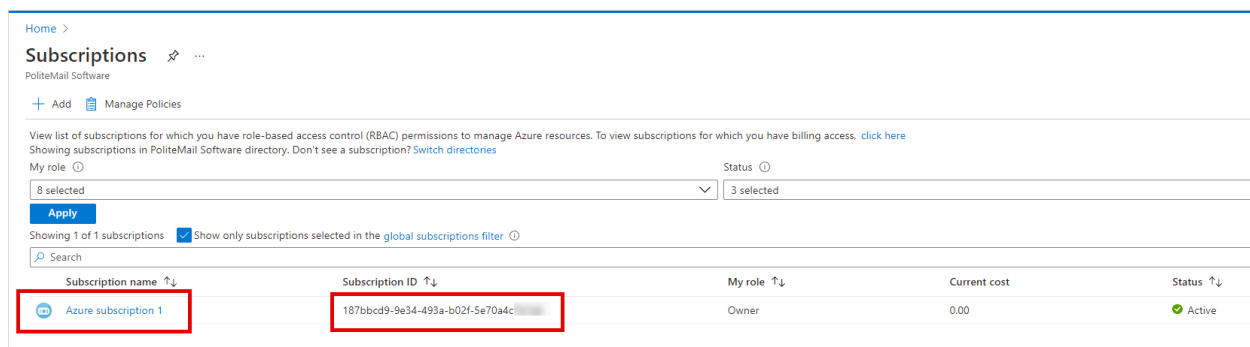
With this information, PoliteMail technicians can add your service connection and fully deploy the PoliteMail infrastructure for your company.

Locate Your Subscription Name and Subscription ID

To locate your subscription information, go to your [Azure Portal](#) and sign into your Microsoft Azure account. Then click **Subscriptions**. If you don't see Subscriptions listed under your Azure services, use the search bar to locate it.



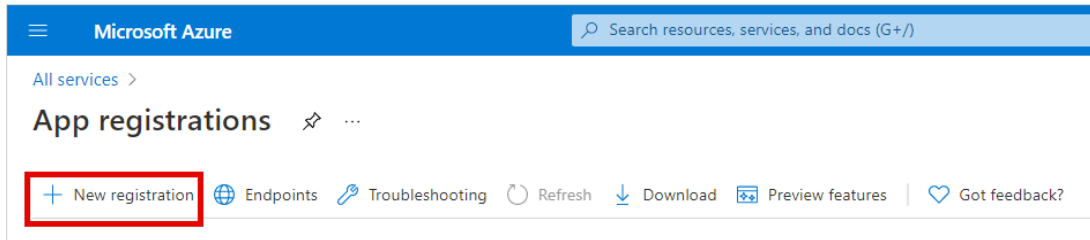
You'll see your Subscription name and Subscription ID. Copy both values to a place you can easily access, such as your clipboard or a word document.



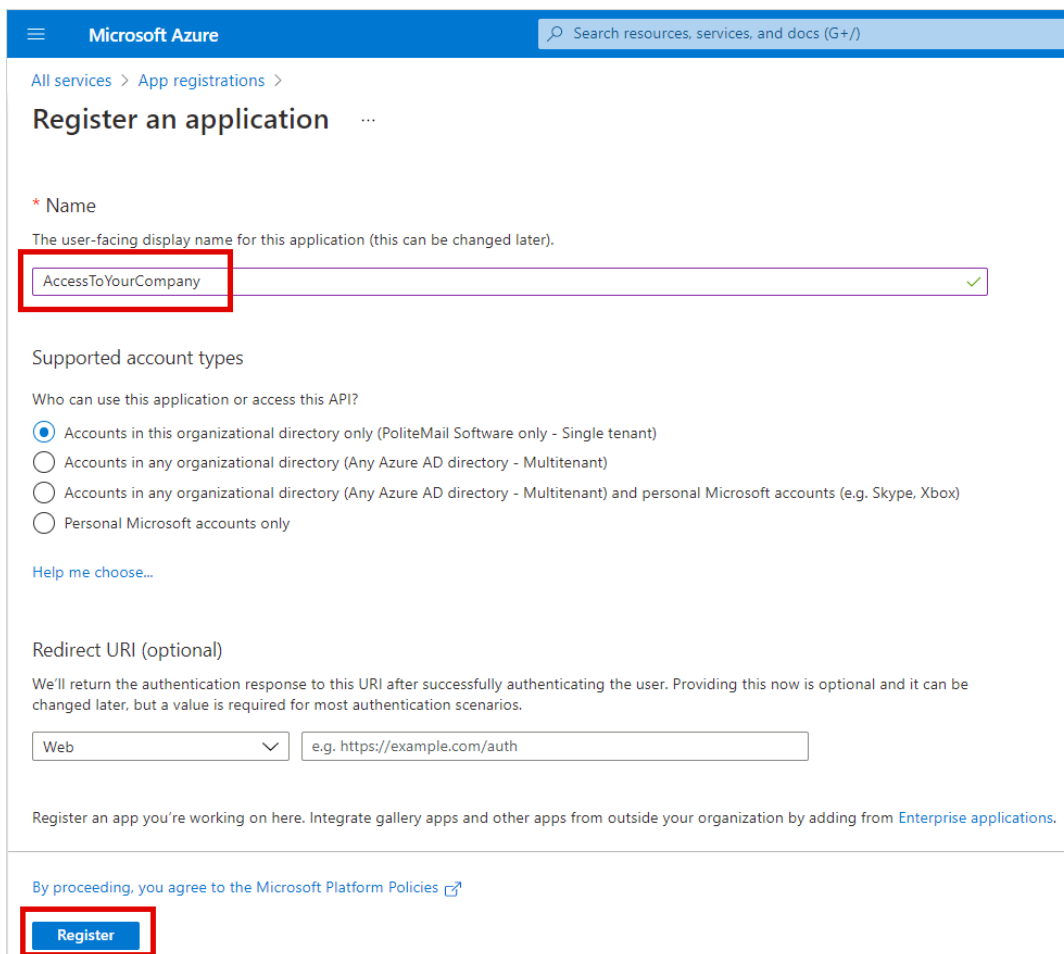
Create A New App Registration

Next, you will need to create a new app registration. This allows you to set security permissions for your (to-be-created) resource group and give PoliteMail permission to create the resources needed for deployment.

Navigate to **Home > App Registration**. Click **New registration**.



Enter a name for the application. Then click **Register**.

A screenshot of the 'Register an application' page in the Microsoft Azure portal. The breadcrumb trail shows 'All services > App registrations > Register an application'. The main heading is 'Register an application'. Below the heading, there is a section for '* Name' with a description: 'The user-facing display name for this application (this can be changed later)'. A text input field contains 'AccessToYourCompany' and has a green checkmark on the right. Below this, there is a section for 'Supported account types' with the question 'Who can use this application or access this API?'. There are four radio button options: 'Accounts in this organizational directory only (PoliteMail Software only - Single tenant)' (selected), '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)', and 'Personal Microsoft accounts only'. Below the radio buttons is a link 'Help me choose...'. There is a section for 'Redirect URI (optional)' with a description: '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.' Below this is a dropdown menu set to 'Web' and a text input field containing 'e.g. https://example.com/auth'. At the bottom, there is a link 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.' and a footer that says 'By proceeding, you agree to the Microsoft Platform Policies'. A blue 'Register' button is highlighted with a red box.

Once your app registration is created, you will see it under listed Owned applications. Click on your new app registration.

Home > App registrations ✨ ...

+ New registration 🌐 Endpoints 🛠 Troubleshooting 🔄 Refresh ⬇ Download 📄 Preview features | ❤ Got feedback?

All applications **Owned applications** Deleted applications (Preview)

🔍 Start typing a name or Application ID to filter these results

Display name	Application (client) ID
AccessToYourCompany	d9db3654-9287-4f55-8b1f-d91da1efa49e

Copy the values for Application (client) ID and the Directory (tenant) ID to a place you can easily access. PoliteMail will need this information to finish setting up deployment.

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

All services > App registrations > AccessToYourCompany ✨ ...

🔍 Search (Ctrl+/) << Delete 🌐 Endpoints 📄 Preview features

Overview

- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration

^ Essentials

Display name : AccessToYourCompany

Application (client) ID : d9db3654-9287-4f55-8b1f-d91da1e

Object ID : 3fc365f7-db92-475d-8674-e7a54ee8a2a8

Directory (tenant) ID : a6cceedf-3dc8-4f34-aa8a-0ad788cf

Supported account types : My organization only

Client credentials : Add a certificate or secret

Redirect URIs : Add a Redirect URI

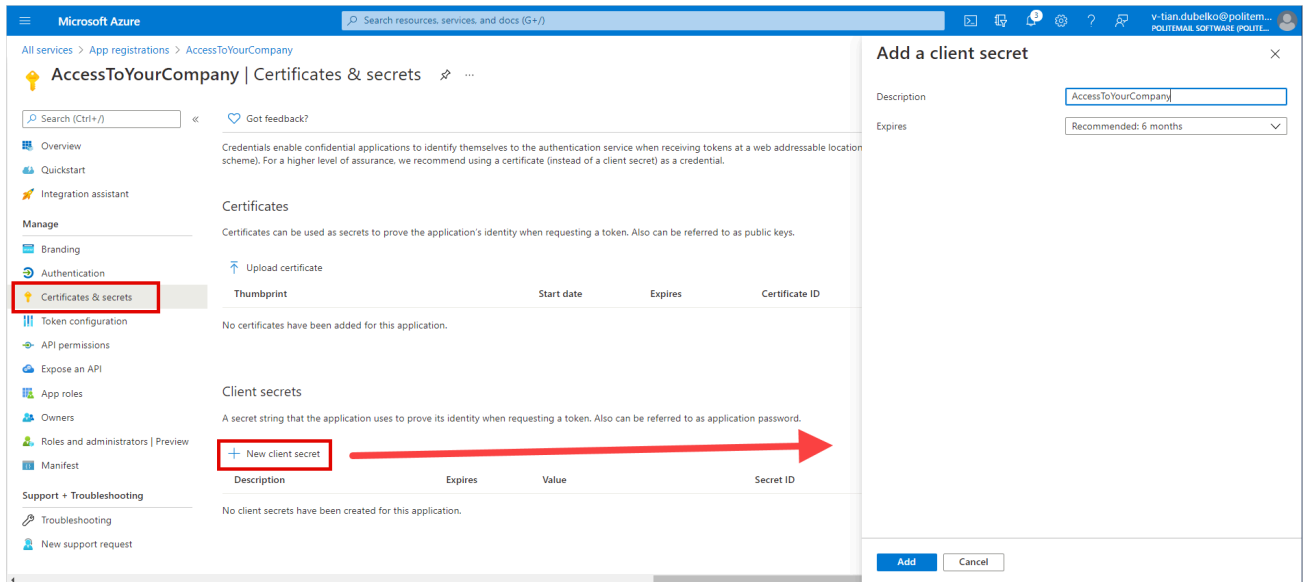
Application ID URI : Add an Application ID URI

Managed application in L... : AccessToYourCompany

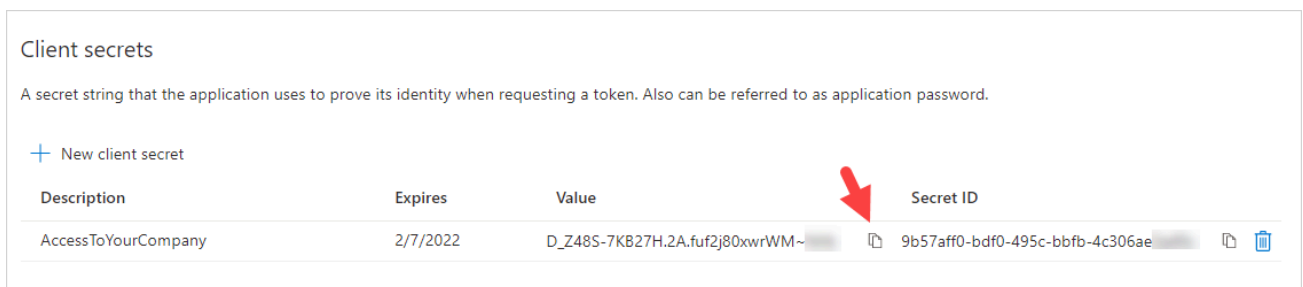
📘 Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Create A Client Secret

After you have created your new app registration, you will need to create a client secret. Click on Certificates & secrets. Then click **New client secret**. Depending on your company's security policy, you may upload a certification instead of creating a new secret.



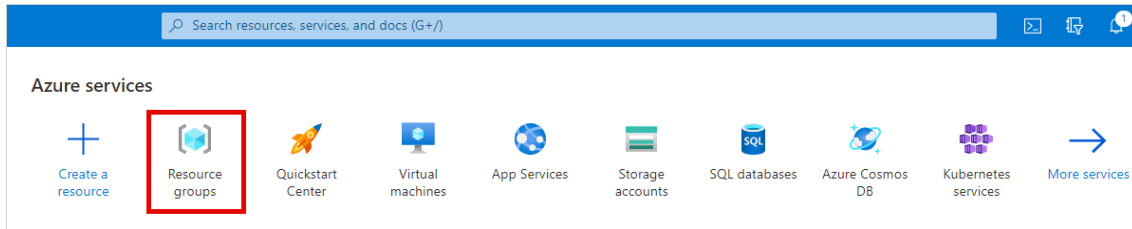
Once added, you will see your new client secret. Copy this unique value to a place you can easily access.



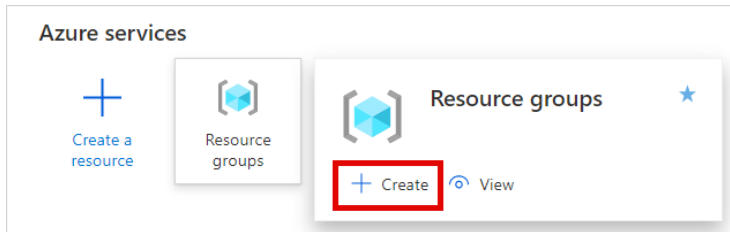
Create A New Resource Group

Next, you'll need to create a new resource group. This is where your BYOC infrastructure will be managed and stored.

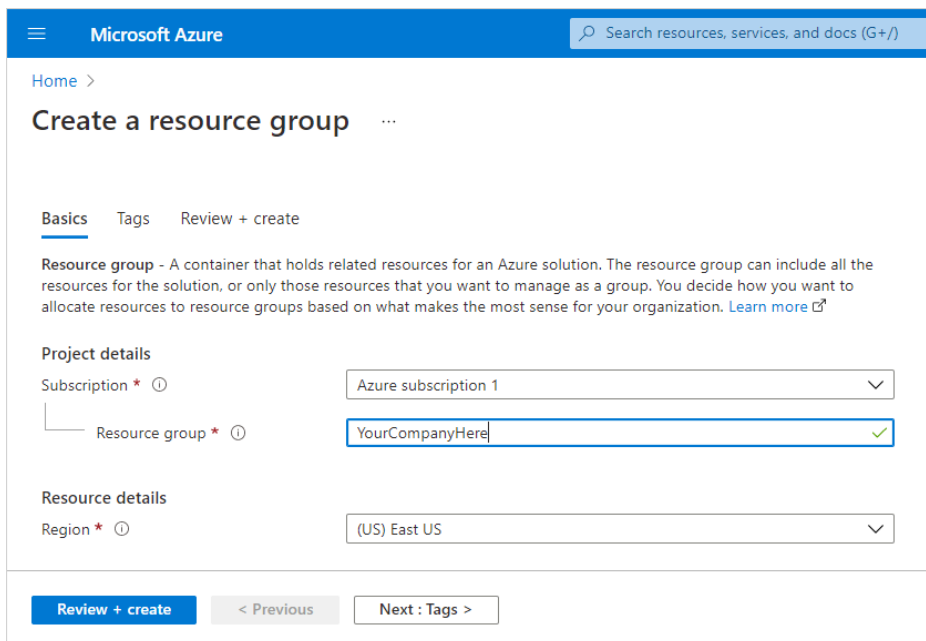
On the Azure home page, locate **Resource groups** under Azure services.



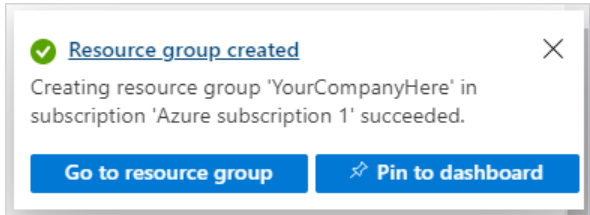
Hover your mouse over the icon for Resource groups to open the pop-up window. Click Create.



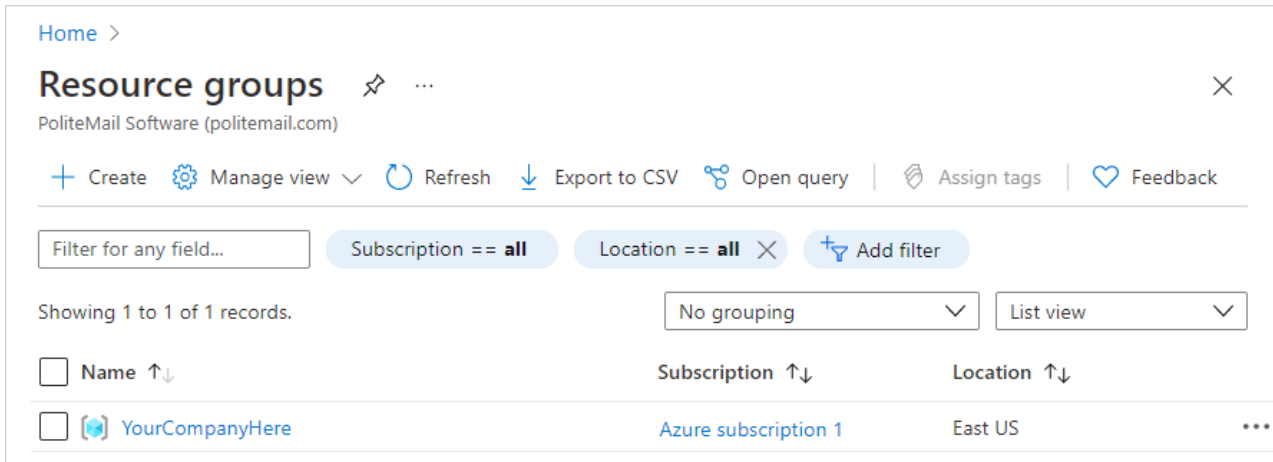
On the next page, you'll be asked to give your resource group a name. You can also add tags to the new resource group. Click **Review+Create** to review your current information. Then click **Create** to finalize your new resource group.



You will see a confirmation message if the creation process was successful.

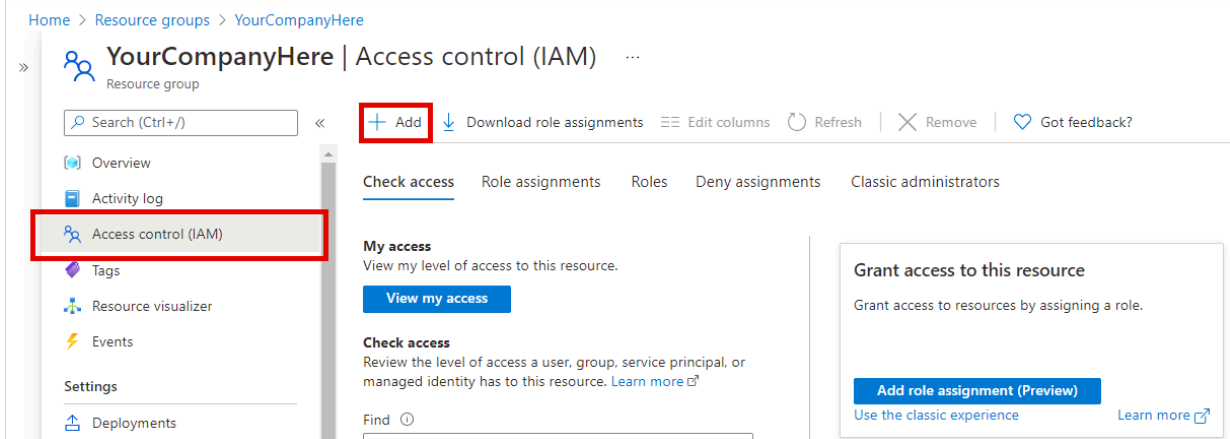


You can view your new resource group via **Home > Resource groups**.

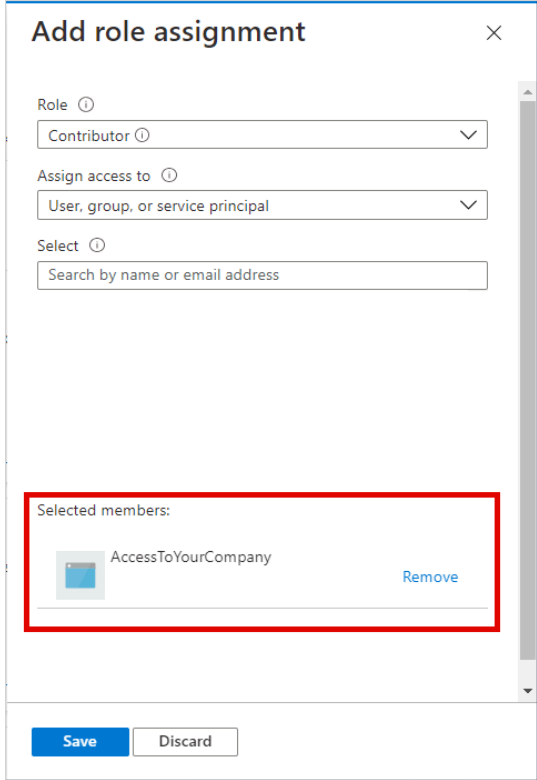


Give PoliteMail Permission to Your Resource Group

Finally, PoliteMail will need access to your new resource group to create resources to deploy your BYOC infrastructure. Navigate back to your newly created resource group via **Home > Resource groups**. Open your created resource group. Click **Access Control (IAM)**. Then click **Add** to add a new role assignment.

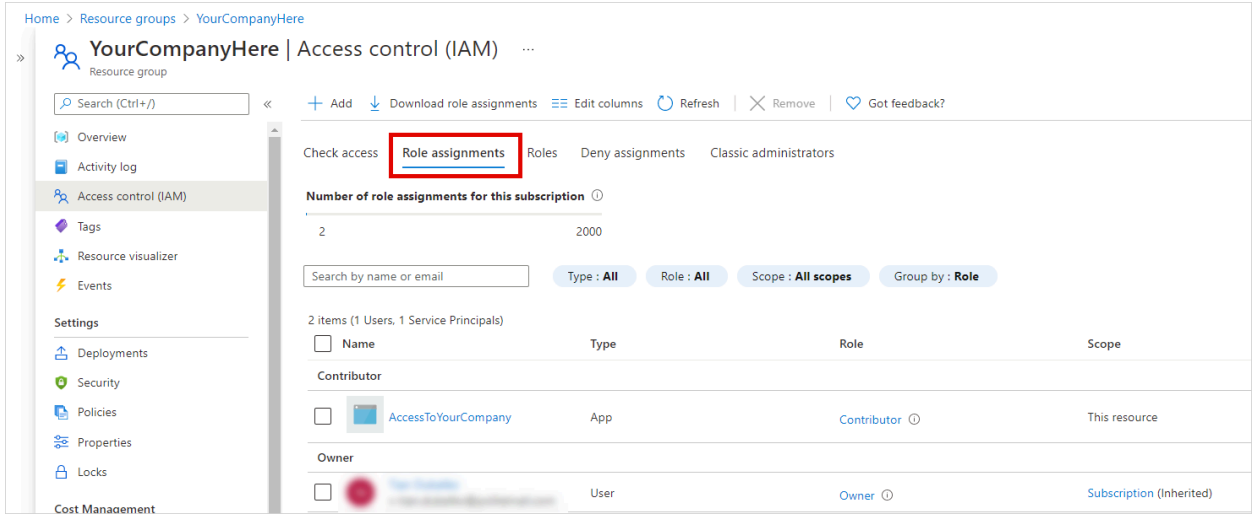


Set the role as Contributor. Under Select, type in the name of your new app registration. Click **Save**.



This gives the app registration you just created contributor access to this specific resource group. Now PoliteMail will have admin access to that resource group, allowing PoliteMail technicians to use that app registration to create the resources needed for deployment.

If the creation process was successful, you will see your new created role under Role assignments.



Finalizing Your BYOC Deployment

Now that you have created a new resource group, a new app registration, and a new client secret, your BYOC deployment is ready for implementation.

Contact your PoliteMail customer service representative and share with them the following information:

- Subscription Name
- Subscription ID
- Application (client) ID
- Directory (tenant) ID
- Client Secret

PoliteMail technicians will then create and finalize all the resources needed to fully deploy your BYOC infrastructure. This process can take up to several hours.

Once your BYOC infrastructure is up and running, we recommend you revoke PoliteMail's access to your resource group. In the list of role assignments, add a checkmark next to PoliteMail's contributor role. Click Remove. In the remove role assignment message that appears, click Yes.