Step 2: Adding a Cloud Service Account - Azure

https://campus.barracuda.com/doc/78808235/

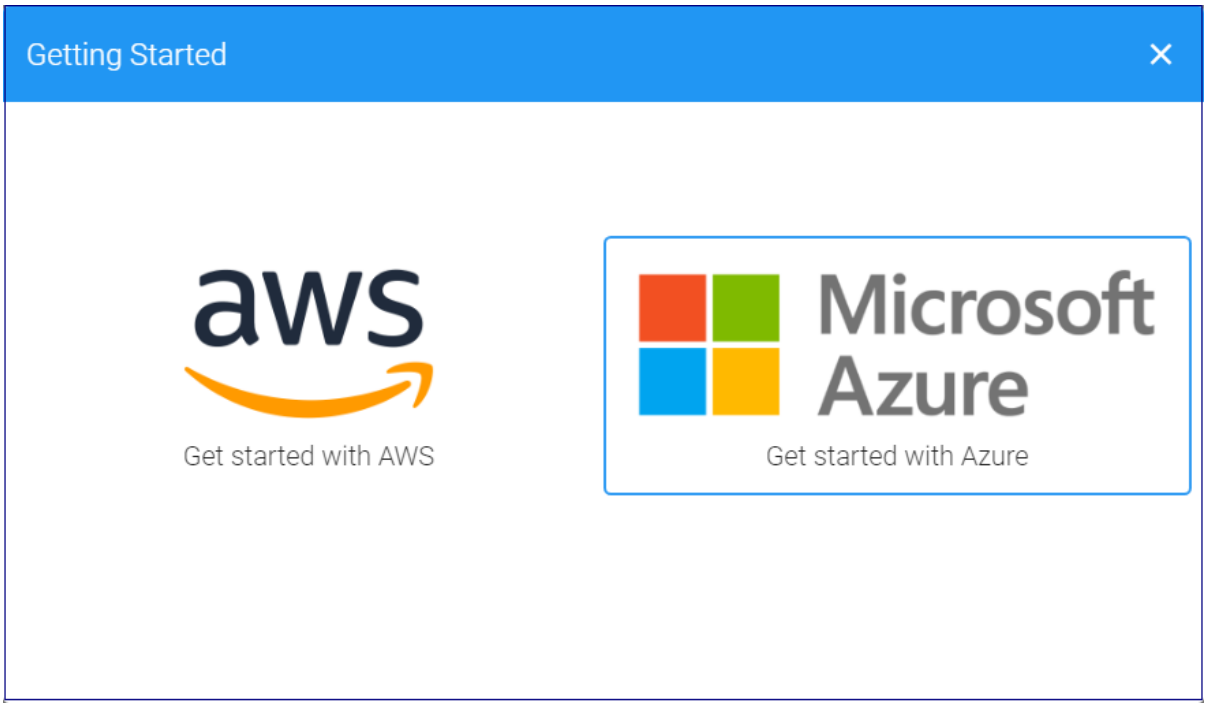
Barracuda Cloud Security Guardian must be able to communicate with your Cloud Service account. Perform the following steps to enable communication.

If you prefer, you can set up communication through the Azure Command Line Interface. Refer to Using the Command Line Interface (CLI).

> You must complete Step 1: Creating a Cloud Security Guardian Account - AWS before proceeding with this step.
>
> Barracuda Cloud Security Guardian is automatically licensed for 30 days, as part of the free trial. After you purchase Barracuda Cloud Security Guardian, you must specify the license. Refer to Licenses for details.

Beginning the Process

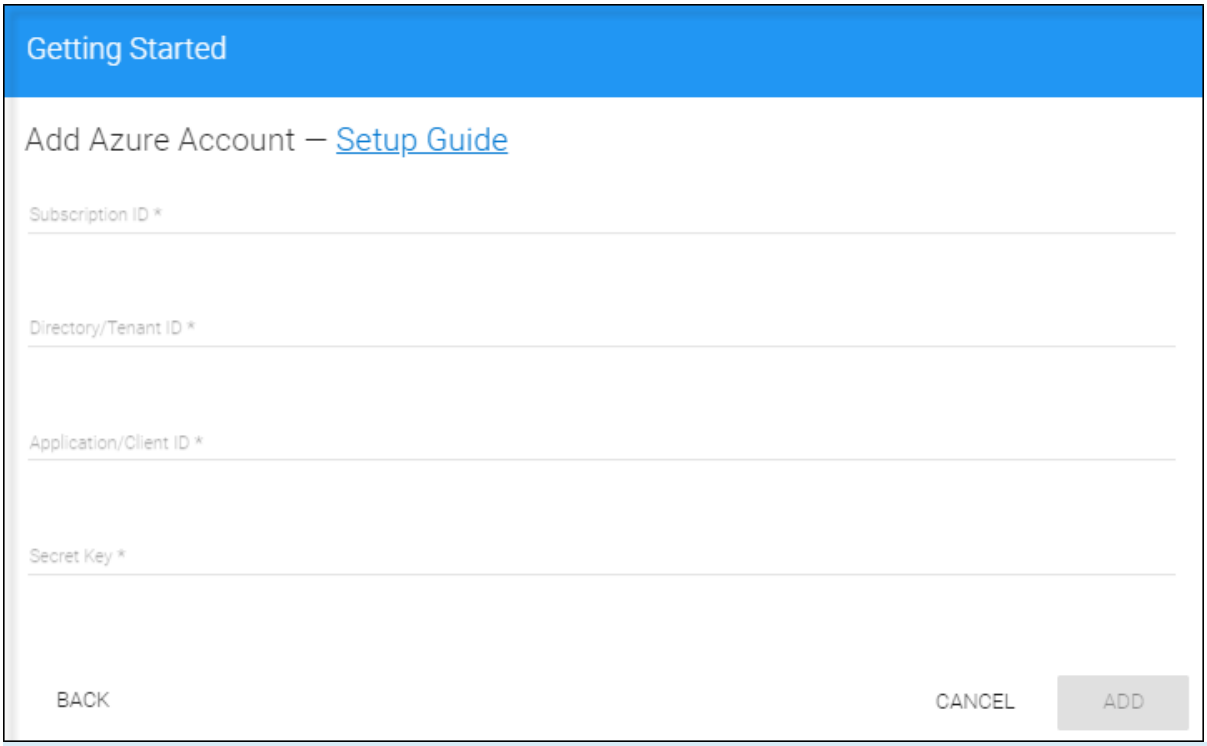
1. Continuing from Step 1: Creating a Cloud Security Guardian Account, click **Get Started with Azure**.



   If you are not already at this screen follow these steps to get there:
   1. In Barracuda Cloud Security Guardian, navigate to **Settings > Cloud Service Providers**.

2. Click **Add Account** to open the Barracuda Cloud Security Guardian onboarding wizard.

2. The **Add Azure Account** window displays. You will need to gather the information from Azure to make the entries in the wizard.

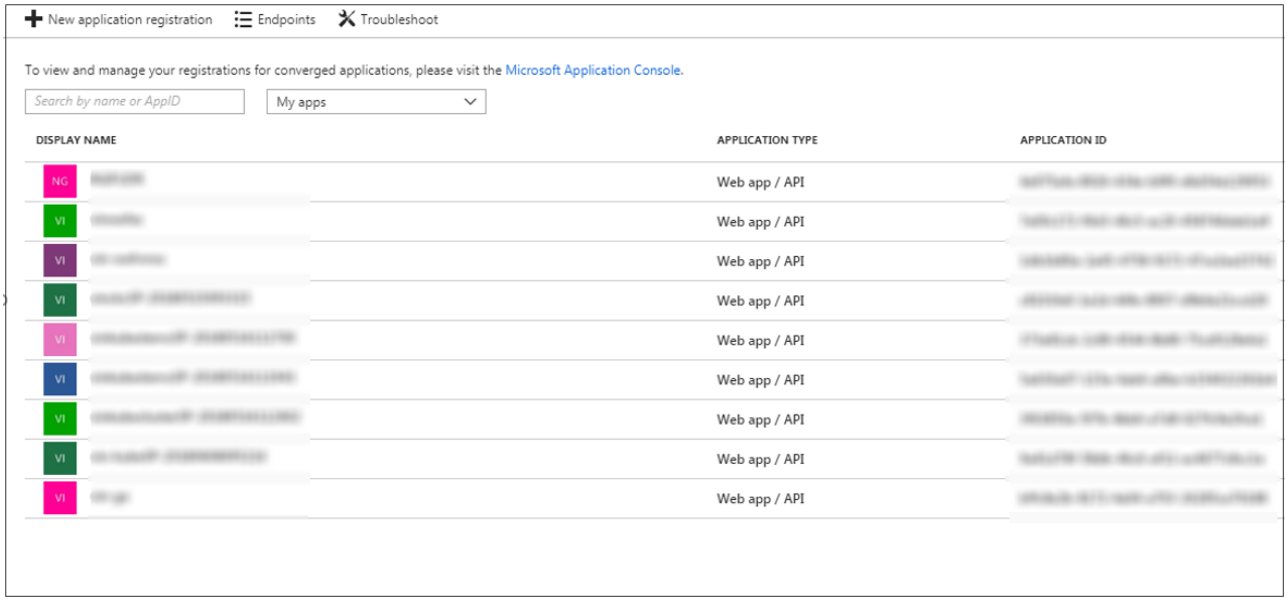


Throughout this process, you will be copying data from your Azure account and pasting it into the Barracuda Cloud Security Guardian onboarding wizard.
Steps with the double-dagger symbol (‡) denote where copying occurs.
If you choose, you can copy the data into a text file as an intermediate step.

3. In a separate browser tab or window, open your Azure account.

Creating a Service Principle

4. *In Azure*, navigate to **Azure Active Directory**, then **Manage > App registrations**.

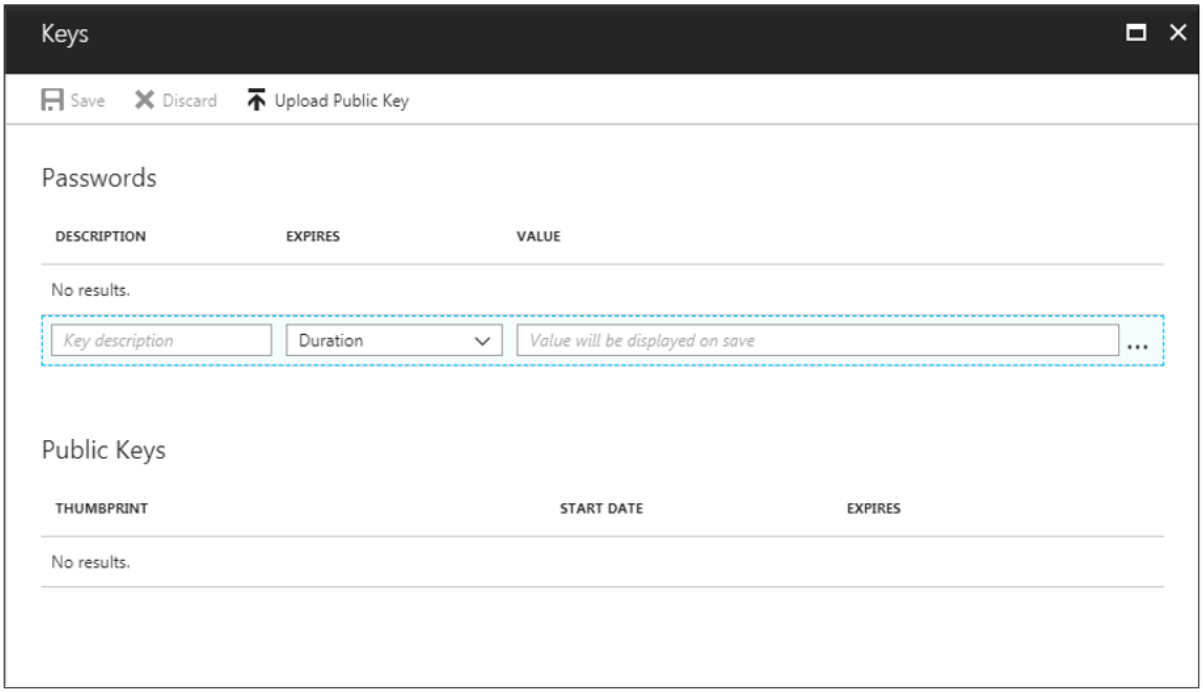


5. Click **New Application Registration**. In the new window, enter the following information, then click **Create**.
    1. **Name** – Give this application a unique name that you will remember.
    2. **Application Type** – Usually Web Application
    3. **Sign-on URL** – The base URL for your Barracuda Cloud Security Guardian application. Switch to the browser tab with running Barracuda Cloud Security Guardian and copy the portion of the URL up to and including the .com, and paste it into this field in the Azure tab. This is often `https://guardian.barracuda.com`.

6. **‡ When Azure has created the application, copy the Application ID and paste it into the Application/Client ID field in Barracuda Cloud Security Guardian.**

    Creating the Keys

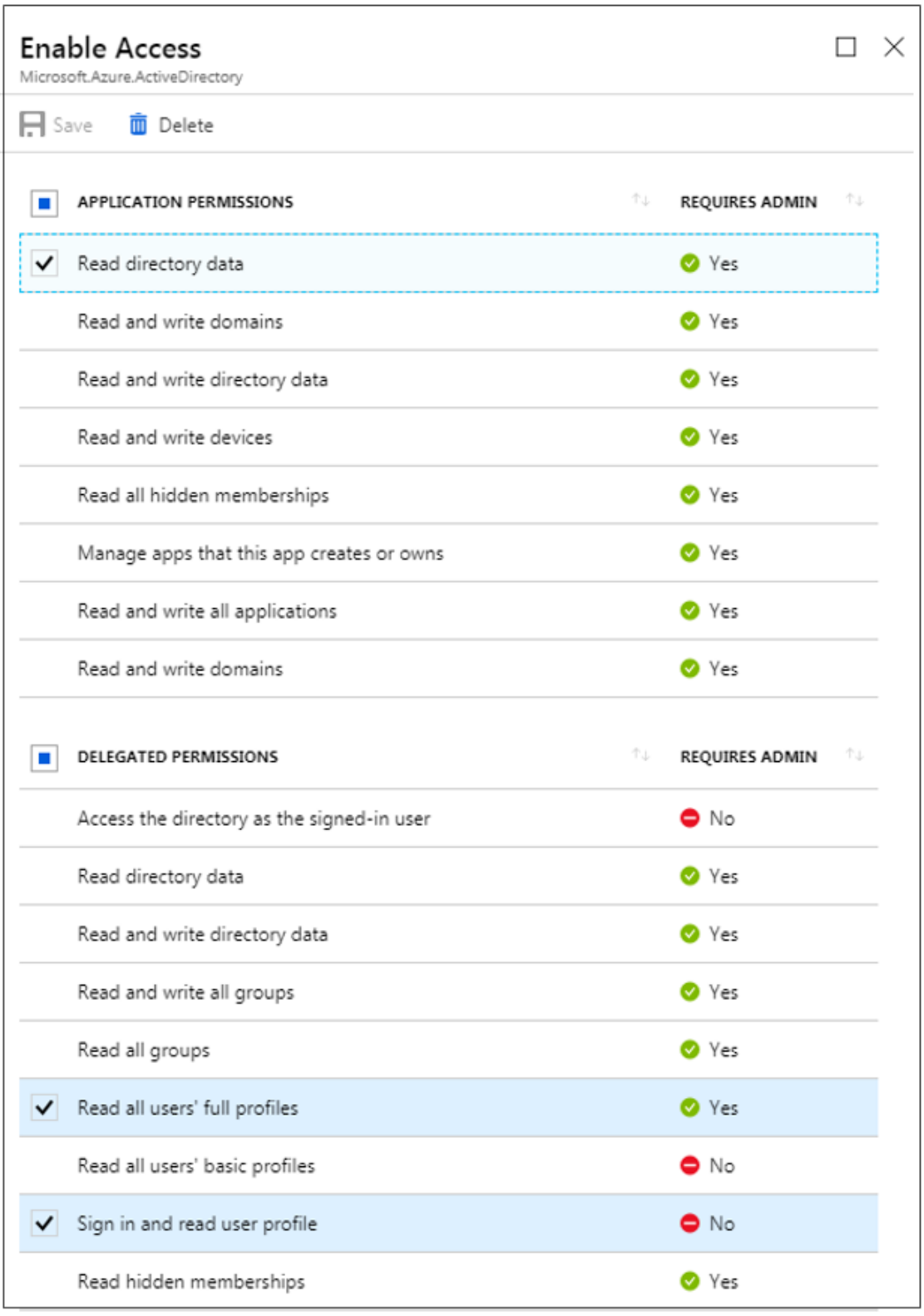
7. In Azure, close the current window. Under **Manage > App registrations**, open the new application you just created. It will likely be at the bottom of the list.
8. Click **Settings**. In the **Settings** panel, click **Keys**.
9. In the **Keys** panel, under **Passwords**, enter a **Description** of your key (usually correlated with the application name) and select the **Duration** you want for the key. Then click **Save**.



10. **‡ Azure automatically generates a key Value. Copy the value from here and enter it in Barracuda Cloud Security Guardian as the Secret Key. Close the Key window.**

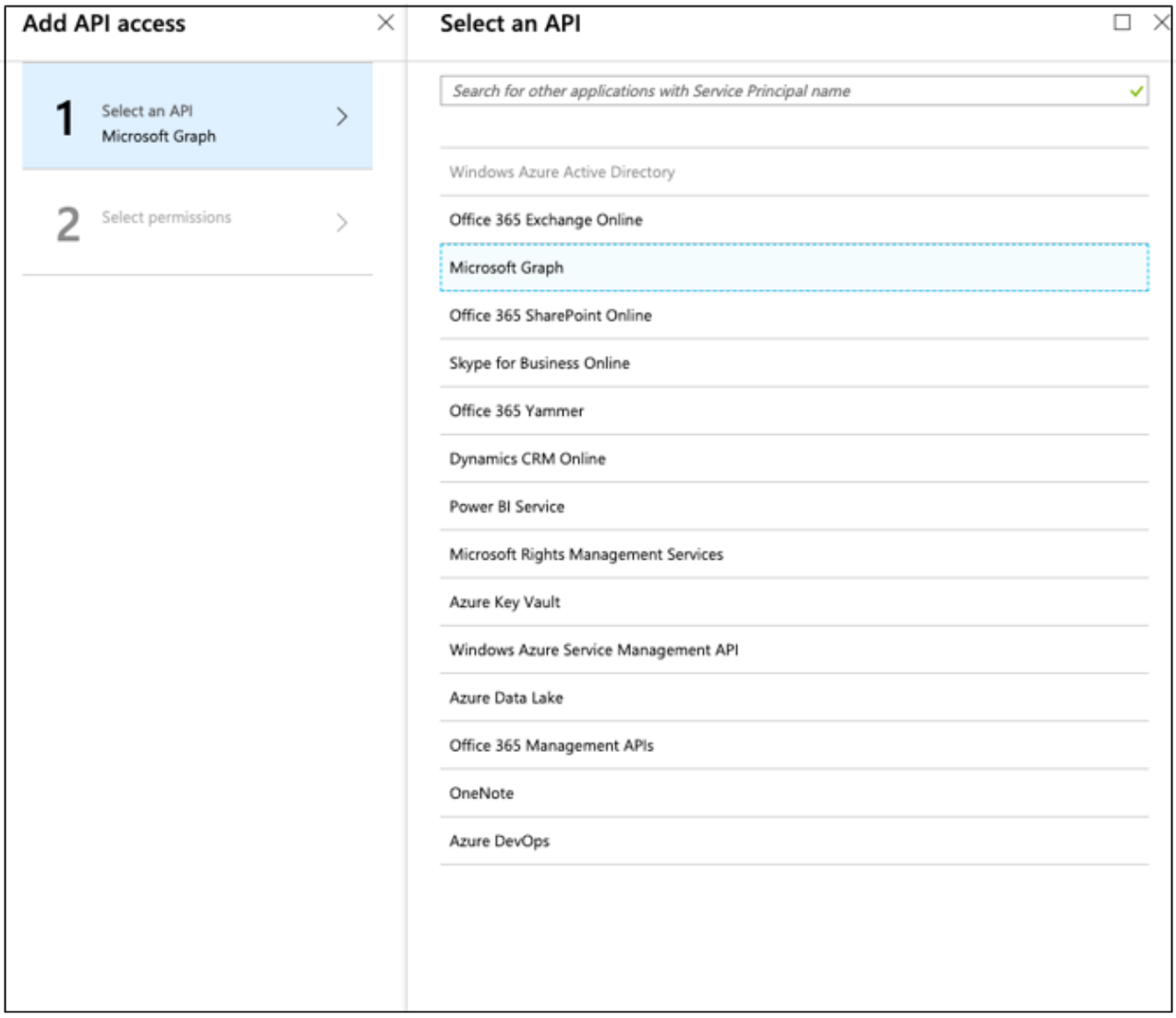
    Setting Permission for Your Application

11. In Azure **Settings**, click **Required Permissions**. Then click **Windows Azure Active Directory**.
    Note: Ensure that the administrator adding the account is a Global Administrator.
12. In the **Enable Access** window, enable the following permissions, then click **Save**.
    - **Application Permissions**
      - Read directory data
    - **Delegated Permissions**:
      - Read all users' full profiles
      - Sign in and read user profile

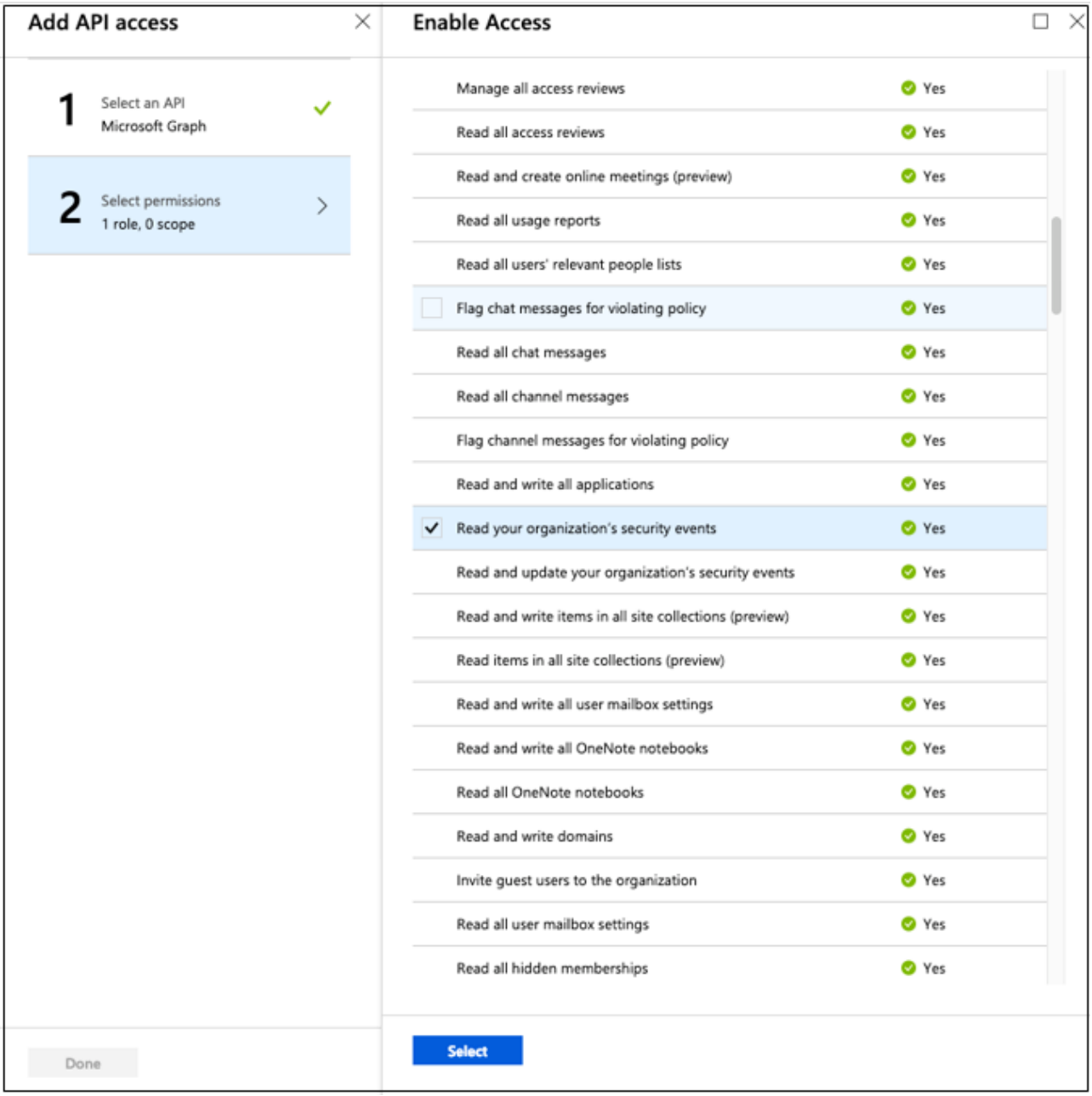


Read Your Organization's Security Events

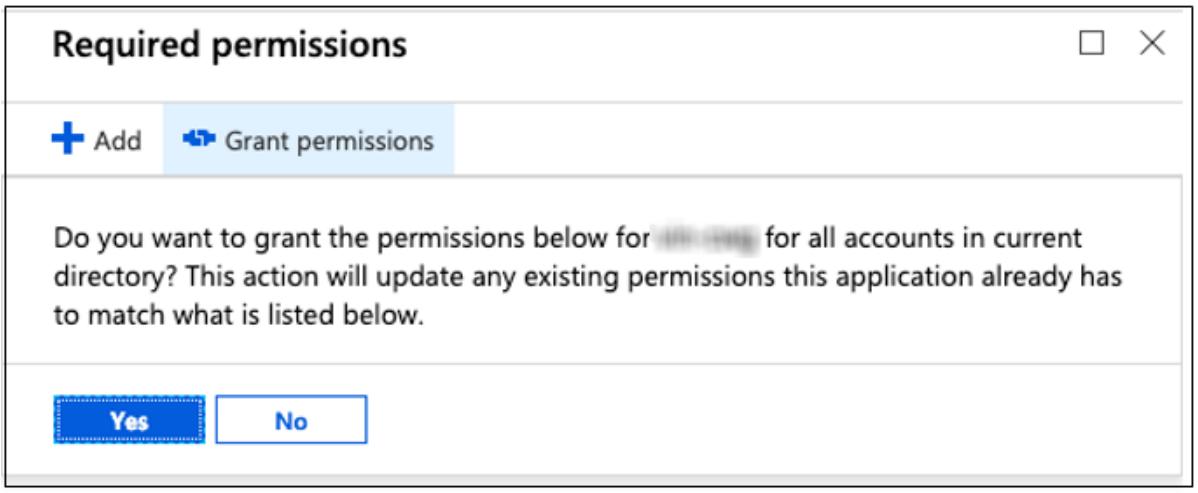
13. Under **Required Permissions**, click **Add**.
14. In the **Select an API** section, select **Microsoft Graph**.



15. In the **Enable Access** section, select **Read your organization's security events**. Click **Select**, then click **Done**.

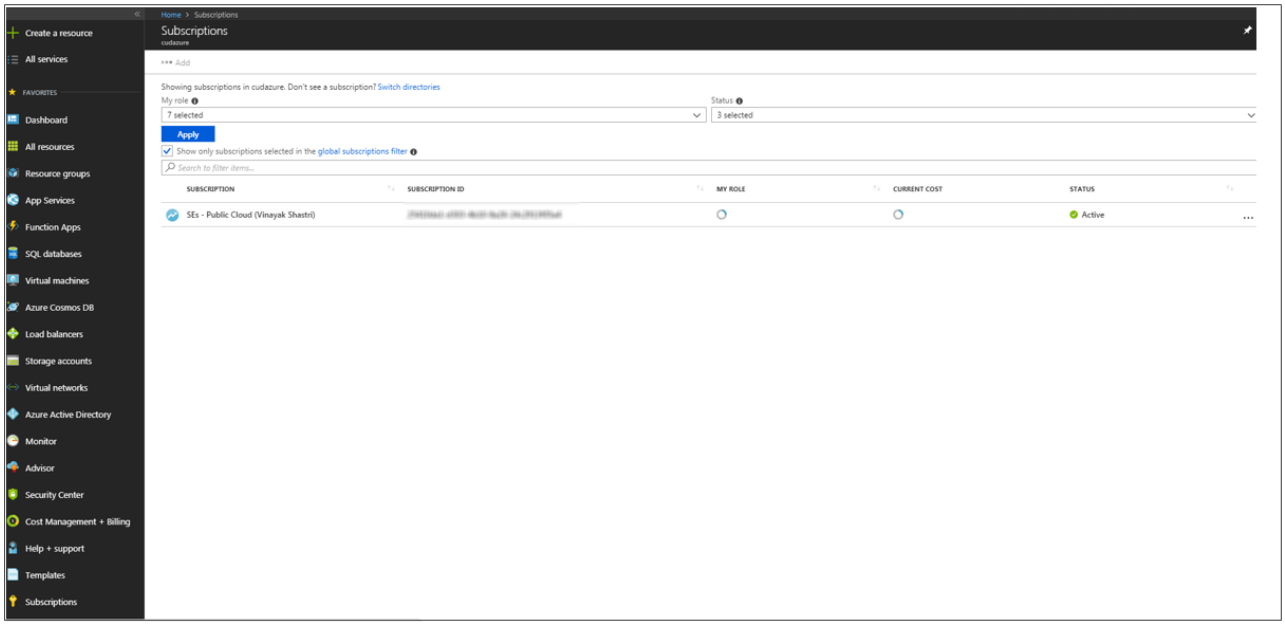


16. **When you are asked if you are sure about granting permissions, click Yes.**



Locating Your Subscription ID

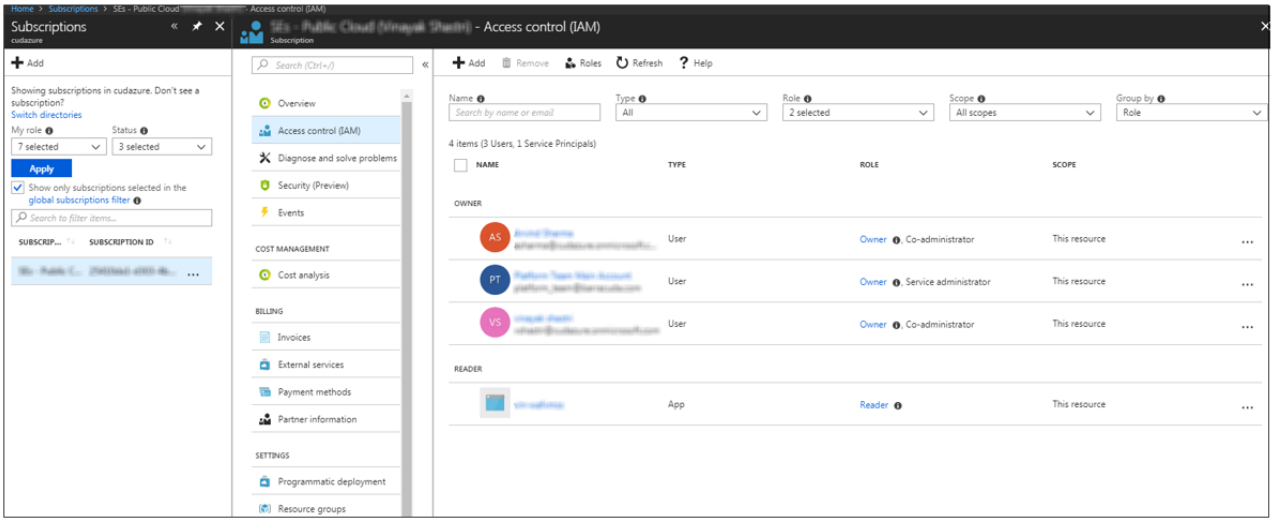
17. In Azure, navigate to **Subscriptions**, then double-click on your subscription.



18. **‡ Copy the Subscription ID. Switch to the browser tab running Barracuda Cloud Security Guardian and paste this value into the Subscription ID field.**

Assigning the Contributor Role to Your New Application

19. Select **Access Control (IAM)**, then click **Add** to add permission.



20. In the **Add permissions** window, select the following information, then click **Save**.
    - **Role** – Contributor
    - **Assign access to** – Azure AD user, group, or service principal.
    - **Select** – Select the application you created for use with Barracuda Cloud Security Guardian in Step 5 above.

‡ Navigate to Active directory, then Manage > Properties. Copy the Directory ID. On the browser tab running Barracuda Cloud Security Guardian, paste this information into the Directory/Tenant ID field.

Completing the Process

21. *In the Barracuda Cloud Security Guardian onboarding wizard*, you should now have all of the field information entered. Click **Add**. Barracuda Cloud Security Guardian creates the connection to your Azure account.

Deploying the stack takes about 10 minutes.

The setup wizard continues to enable Security & Compliance. To perform this setup, continue to Step 3: Enabling Security and Compliance - Azure.

Figures

1. getStartedAzure.png
2. AzureSetup2.png
3. addAppReg.png
4. sign-onURL.png
5. keys.png
6. EnableAccess1.png
7. selectAnApi.png
8. EnableAccess.png
9. requiredPermissions.png
10. subscription.png
11. IAM.png