

Obtain visibility and access to Azure Subscriptions/Reserved Instances

Description

This document outlines how to obtain visibility and access to Azure Subscriptions and/or Reserved Instances when you may not have such access initially.

Pre-requisites

This document requires the following pre-requisites.

- Familiarity with Azure Portal (<https://portal.azure.com>)
- Global Administrator account

Detailed Description

The process outlined in this document utilises a Global Administrator account to elevate and assign the role of 'User Access Administrator' against itself to all Azure resources within a tenancy which then can be used to assign the appropriate role permissions to a member for the task required. This document provides details on this process in relation to visibility and access of Azure Subscriptions and Reserved Instances specifically.

For additional details and considerations please see the [Important Links](#) section.

Please note, it is recommended to remove the elevated role when no longer required.

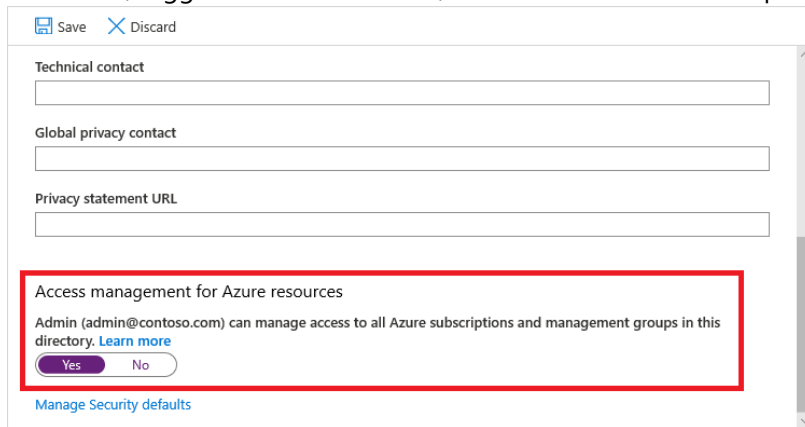
Important Links

- Elevated Access Global Administrator <https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>
- Principals of Least Privilege (POLP) <https://learn.microsoft.com/en-us/azure/active-directory/develop/secure-least-privileged-access>
- Azure Security Technical Capabilities <https://learn.microsoft.com/en-us/azure/security/fundamentals/technical-capabilities>

Steps

Elevate Access

- Log into Azure Active Directory (<https://aka.ms/azad>) utilising your Global Administrator account.
- On the left-hand side under the Manage section, select Properties.
- At the bottom of the page which loads, there is a section called 'Access management for Azure resources', toggle the button to 'Yes', and then hit Save at the top of the page.

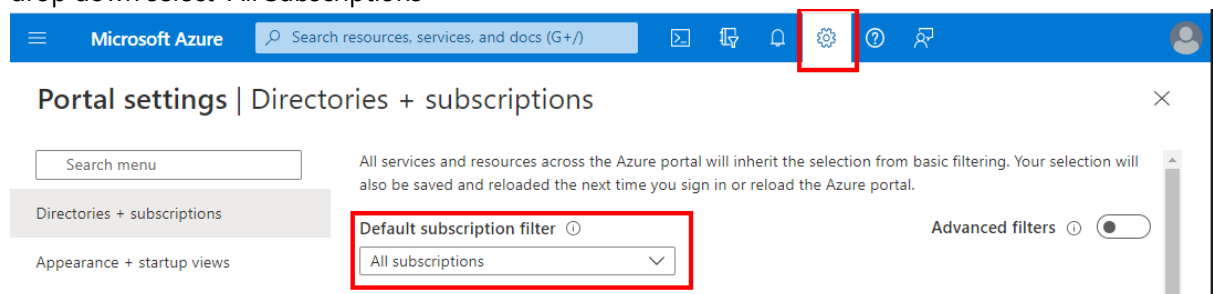


- Sign out and sign back in
- Log into Azure Portal (<https://portal.azure.com>) using your Global Administrator account.
- You now have been assigned the role of 'User Access Administrator' against all Azure Subscriptions and Reserved Instances.

Please note, the 'User Access Administrator' role assigned does not allow you to manage any resources, instead it allows you to assign roles to members of the tenancy against the required resources (Subscriptions, Reserved Instances, etc). Using this elevated role, you can assign yourself permissions to manage resources utilising roles with appropriate access to do so.

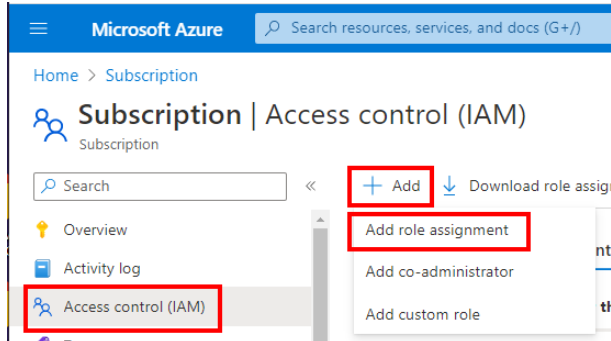
Azure Subscription Access

- Click the Gear icon in the top right, on the page which loads under the 'Default subscription filter' drop down select 'All Subscriptions'



- In the search box at the top of the Azure Portal type in 'Subscriptions' and click the first result with a Key icon. On the page which loads you should have visibility of all available subscriptions under the tenancy.

- Click on each of the Subscriptions you would like access to and under the Overview section click on 'Access Control (IAM)', then click on 'Add', and 'Add role assignment'



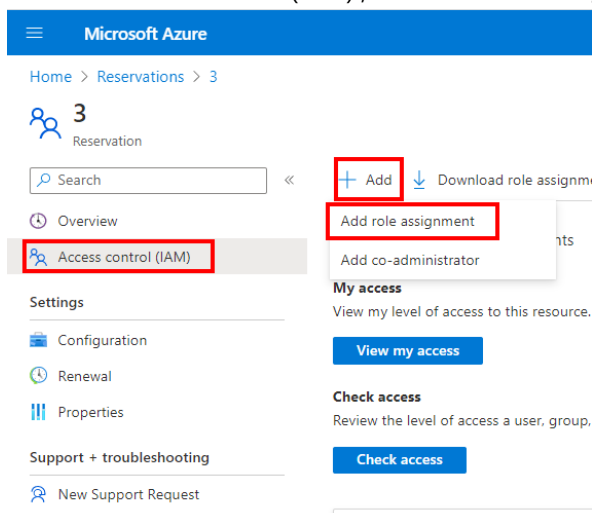
- From the page which loads under the Role tab select the appropriate level of access you require (taking into consideration **principals of least privilege** security model), under the Members tab select the appropriate member(s) to assign the level of access they require, then click 'Review + Assign'
- Permissions are now in place for the member(s) you assigned access to against the selected Azure Subscription.
- If you are assigning permissions against the login used to perform the above steps, you will need to log out, and log back in again for the updated permissions to take effect.

Reserved Instance Access

- In the search box at the top of the Azure Portal type in 'Reservations' and click the first result with a Clock icon. On the page which loads you should have visibility of any Reserved Instances which are in place under the tenancy.

Please note, if no entries are shown then there has been no Reserved Instances purchased.

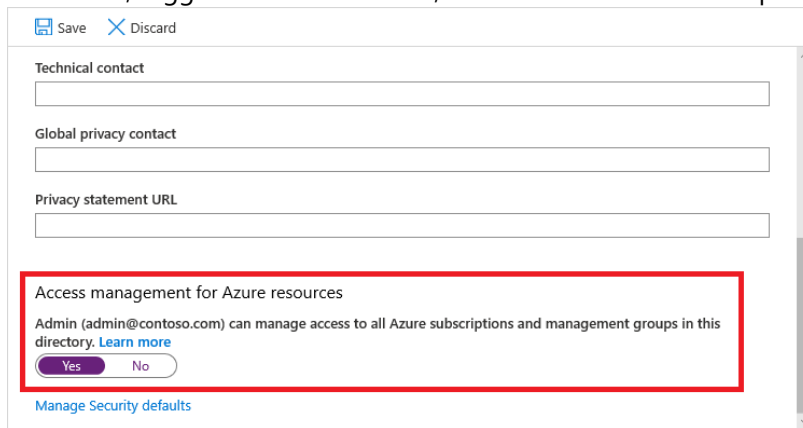
- Click on each of the Reserved Instances you would like access to and under the Overview section click on 'Access Control (IAM)', then click on 'Add', and 'Add role assignment'



- From the page which loads under the Role tab select the appropriate level of access you require (taking into consideration **principals of least privilege** security model), under the Members tab select the appropriate member(s) to assign the level of access they require, then click 'Review + Assign'
- Permissions are now in place for the member(s) you assigned access to against the selected Reserved Instance.

Removing Elevated Access

- To remove your elevated access log into Azure Active Directory (<https://aka.ms/azad>) utilising the same Global Administrator account used previously.
- On the left-hand side under the Manage section, select Properties.
- At the bottom of the page which loads, there is a section called 'Access management for Azure resources', toggle the button to 'No', and then hit Save at the top of the page.

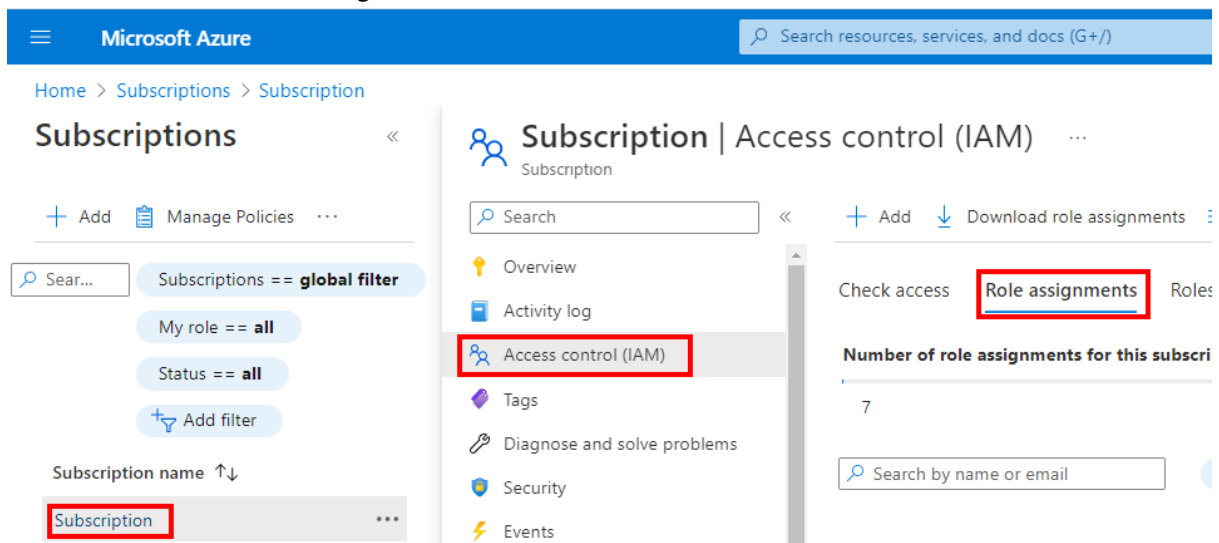


The screenshot shows a web interface for Azure Active Directory. At the top, there are 'Save' and 'Discard' buttons. Below are three text input fields: 'Technical contact', 'Global privacy contact', and 'Privacy statement URL'. A red box highlights the 'Access management for Azure resources' section, which contains the text: 'Admin (admin@contoso.com) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)'. Below this text are two radio buttons: 'Yes' (which is selected) and 'No'. At the bottom of the highlighted section is a link: 'Manage Security defaults'.

- Your elevated access should now be removed.
- Log out and back in to complete the process.

Optional – Confirm Elevated Access has been Removed

- To confirm your elevated access has been removed, ensure you have logged out and back in since removing your elevated access.
- Using the same Global Administrator account used previously, log into Azure Portal (<https://portal.azure.com>) and in the top search box type in 'Subscriptions' and select the first entry with a Key icon.
- On the page which loads, select any Subscription listed, then under Overview, select 'Access Control (IAM)', and then the 'Role assignment' tab.



- The page which loads will list all available permissions currently against the Azure Subscription selected. If you do not have elevated access, you won't see a Role entry under 'User Access Administrator' with your Global Administrator account assigned with a Scope of 'Root (Inherited)'. If you do have elevated access, you will see a Role entry under 'User Access Administrator' with your Global Administrator account assigned with the Scope of 'Root (Inherited)'.