Elevate access for a Global Administrator

Follow these steps to elevate access for a Global Administrator using the Azure portal.

- 1. Sign in to the <u>Azure portal</u> or the <u>Azure Active Directory admin center</u> as a Global Administrator.
- 2. Search for and select Azure Active Directory.
- 3. NOTE YOU ARE ALREADY SIGNED IN AND WILL BEGIN FROM SELECTING PROPERTIES



4. Under Manage, select Properties. Scroll down once.

Home > Contoso - Properties	
Contoso - Properties Azure Active Directory	
	🛛 « 🖫 Save 🗙 Discard
📍 Password reset	▲
Company branding	Directory properties
🖏 User settings	Name
III Properties	Contoso
in rioperaes	Country or region
Notifications settings	United States
Security	Location
Monitoring	United States, Europe datacenters
Sign-ins	Notification language
	English
Audit logs	▼ 4
	Home > Contoso - Properties Contoso - Properties Azure Active Directory Search (Ctrl+/) Password reset Company branding User settings User settings User settings Properties Notifications settings Security Monitoring Sign-ins Audit logs

5. Under Access management for Azure resources, set the toggle to Yes.

🔚 Save 🗙 Discard
Technical contact
Global privacy contact
Privacy statement URL
Access management for Azure resources
Admin (admin@contoso.com) can manage access to all Azure subscriptions and management groups in this directory Learn more
Yes No
Manage Security defaults

Click on **Save.** Close the Properties box.

When you set the toggle to **Yes**, you are assigned the User Access Administrator role in Azure RBAC at root scope (/). This grants you permission to assign roles in all Azure subscriptions and management groups associated with this Azure AD directory. This toggle is only available to users who are assigned the Global Administrator role in Azure AD.

When you set the toggle to **No**, the User Access Administrator role in Azure RBAC is removed from your user account. You can no longer assign roles in all Azure subscriptions and management groups that are associated with this Azure AD directory. You can view and manage only the Azure subscriptions and management groups to which you have been granted access.

Assigning a Role to a User

- 1. Click on All Services on the menu to the left
- 2. In the main pane click on All Services
- 3. Under All Resources select Management Group
- 4. We will be using the **Tenant root Group** for our example
- 5. Click on Details next to the Tenant root Group
- 6. Select Access Control (IAM) from the menu on the *left (IAM stands for Identity Access Management)*
- 7. Select +Add, select Add Role Assignment
- 8. To the right under Role, click the down arrow and select Contributor
- 9. Under Select select Abbi Parsons and click on Save.
- 10. Click the down arrow twice and close the Access Control(IAM) window.