User Management and Authentication

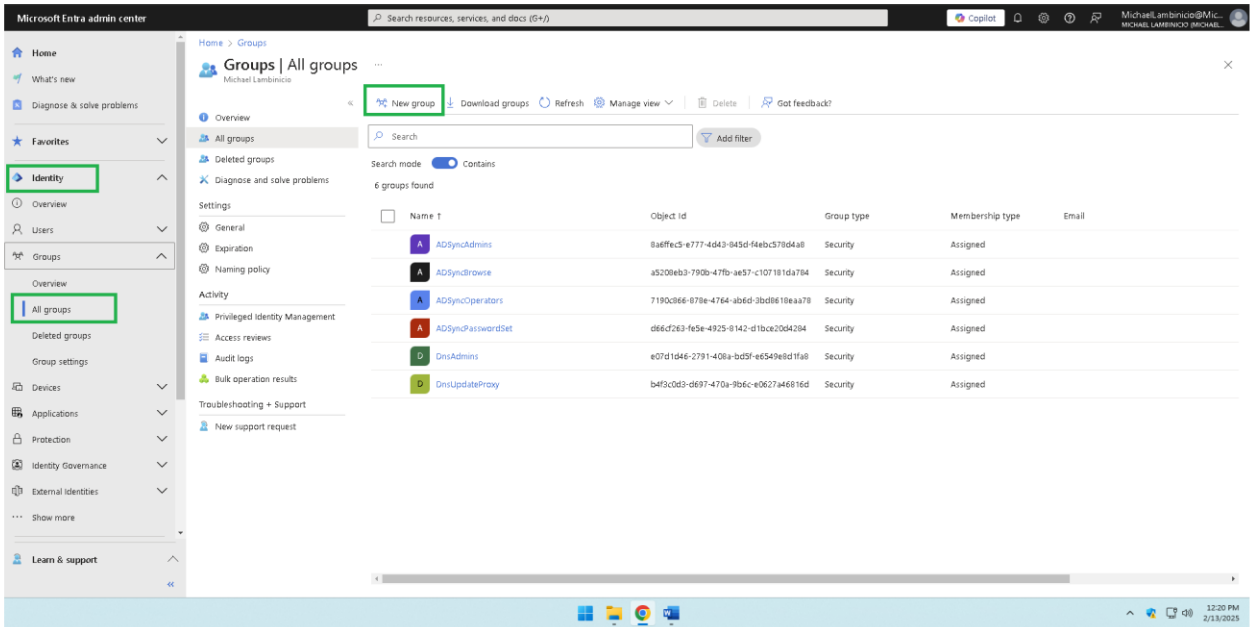
Prepared by:
Michael Lambinicio
CMIT 382

Objective

In Project 2 deliverable, you implemented a strategy for user identity. Managing user identity is equally important as implementing it. Proper management of identity ensures that users have access to resources they need to perform their job functions and accounts are properly secured. In this deliverable, you will demonstrate the creation of user groups, manage Role-Based Access Control (RBAC) roles, view user login activity, the configuration of Azure AD self-service password reset policy, and create a customed banned password.

Part 1: Create Groups

To start, login into Microsoft Entra admin center with your onmicrosoft login account. From the Identity section on the far left, choose “Groups”, then “All Groups”. In the main window, you are then going to click on “New Group” on the top, as shown below:



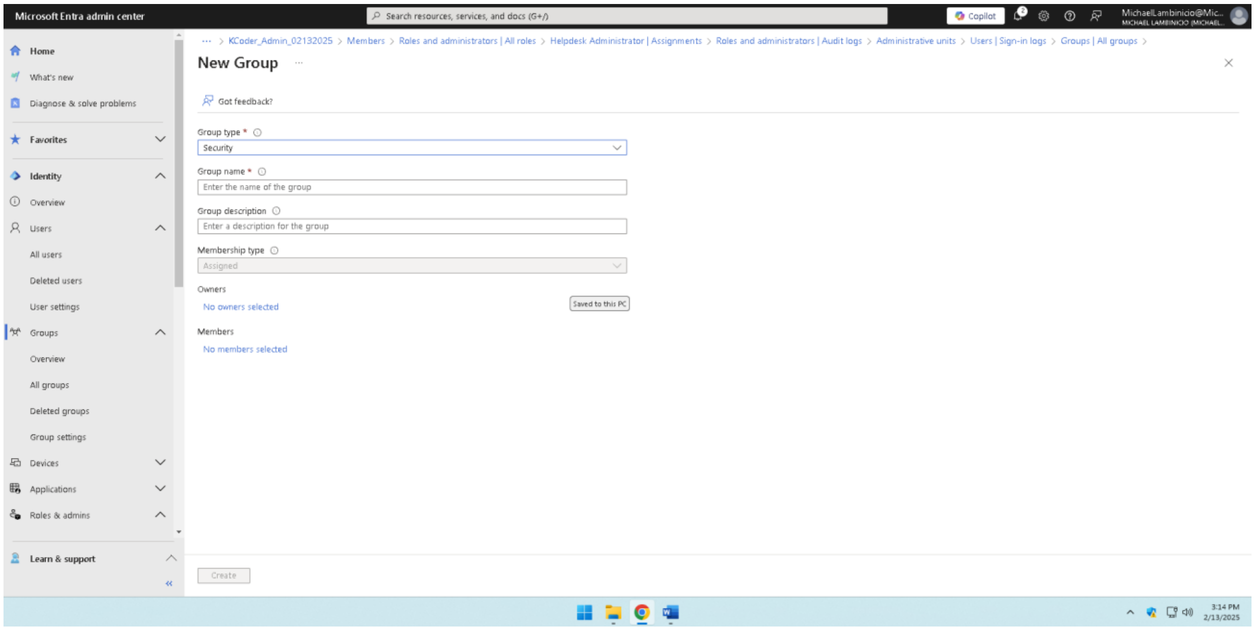
Search mode Contains

6 groups found

Name ↑	Object Id	Group type	Membership type	Email
ADSyncAdmins	8a6ffec5-e777-4d43-845d-f4ebc578d4a8	Security	Assigned	
ADSyncBrowse	a5208eb3-790b-47fb-ae57-c107181da784	Security	Assigned	
ADSyncOperators	7190c866-878e-4764-ab6d-3bd8618eaa78	Security	Assigned	
ADSyncPasswordSet	d66cf263-fe5e-4925-8142-d1bce20d4284	Security	Assigned	
DnsAdmins	e07d1d46-2791-408a-bd5f-e6549e8d1fa8	Security	Assigned	
DnsUpdateProxy	b4f3c0d3-d697-470a-9b6c-e0627a46816d	Security	Assigned	

Next, you will fill in the Group name, Group description, and if applicable, and answering “Yes” to Microsoft Entra roles can be assigned to the group. For group name, you will type **KCoder_Admin_current date (to be changed with today’s date)**. And then description will read **“Group to Manage M365 Portal”**. In the assigned members link, click it and it will take you to the members screen, where you will have to hit add member and check off Larry Ravenson to add him. Then choose save so he will be added to the group. After this is created, you will create another group with the same process, except the second group name will be **KCoder_Support_current date**. When you add a member to this group, choose Susan Pandya for this group, shown below:

Add new group specifics:


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
All users
Deleted users
User settings
Groups
Overview
All groups
Deleted groups
Group settings
Devices
Applications
Roles & admins
Learn & support
... > KCoder_Admin_02132025 > Members > Roles and administrators | All roles > Helpdesk Administrator | Assignments > Roles and administrators | Audit logs > Administrative units > Users | Sign-in logs > Groups | All groups >
New Group
Got feedback?
Saved to this PC
Create

Group type * Security

Group name * Enter the name of the group

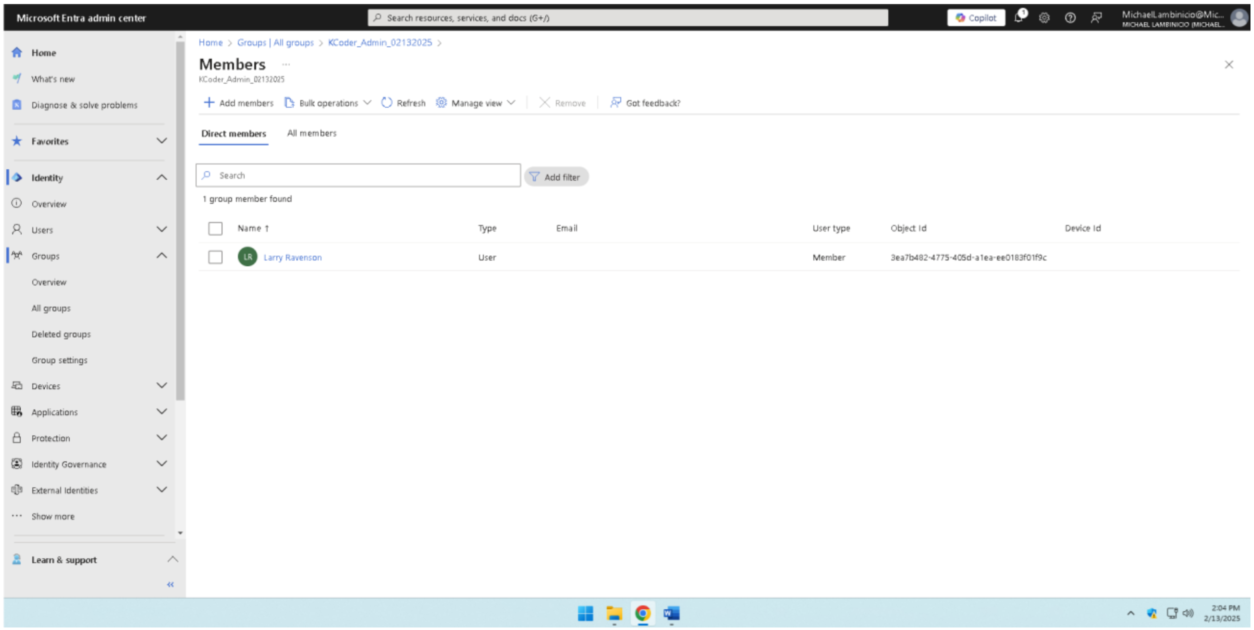
Group description Enter a description for the group

Membership type Assigned

Owners
No owners selected

Members
No members selected

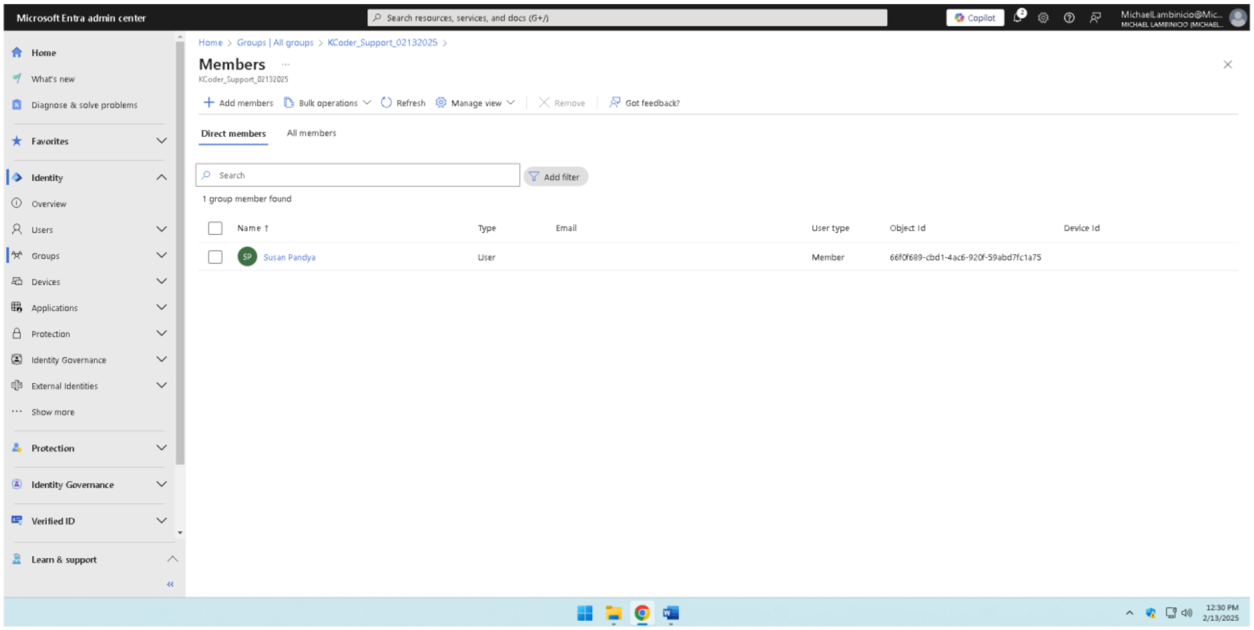
Add Larry Ravenson to the KCoder_Admin group.



1 group member found

Name ↑	Type	Email	User type	Object Id	Device Id
LR Larry Ravenson	User		Member	3ea7b482-4775-405d-a1ea-ee0183f01f9c	

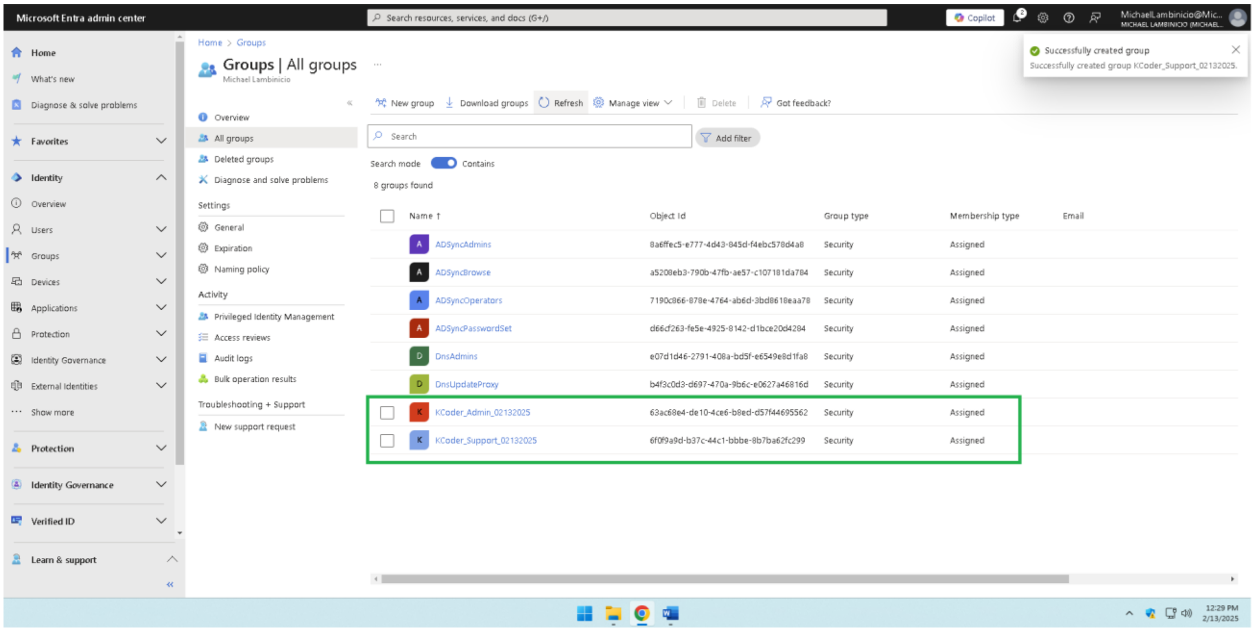
Add Susan Pandya to the KCoder_Support group.



1 group member found

Name ↑	Type	Email	User type	Object Id	Device Id
SP Susan Pandya	User		Member	66f0f689-cbd1-4ac6-920f-59abd7fc1a75	

After the groups are created, they should populate in the All groups section. (You may need to refresh the screen.)



Successfully created group

Successfully created group KCoder_Support_02132025.

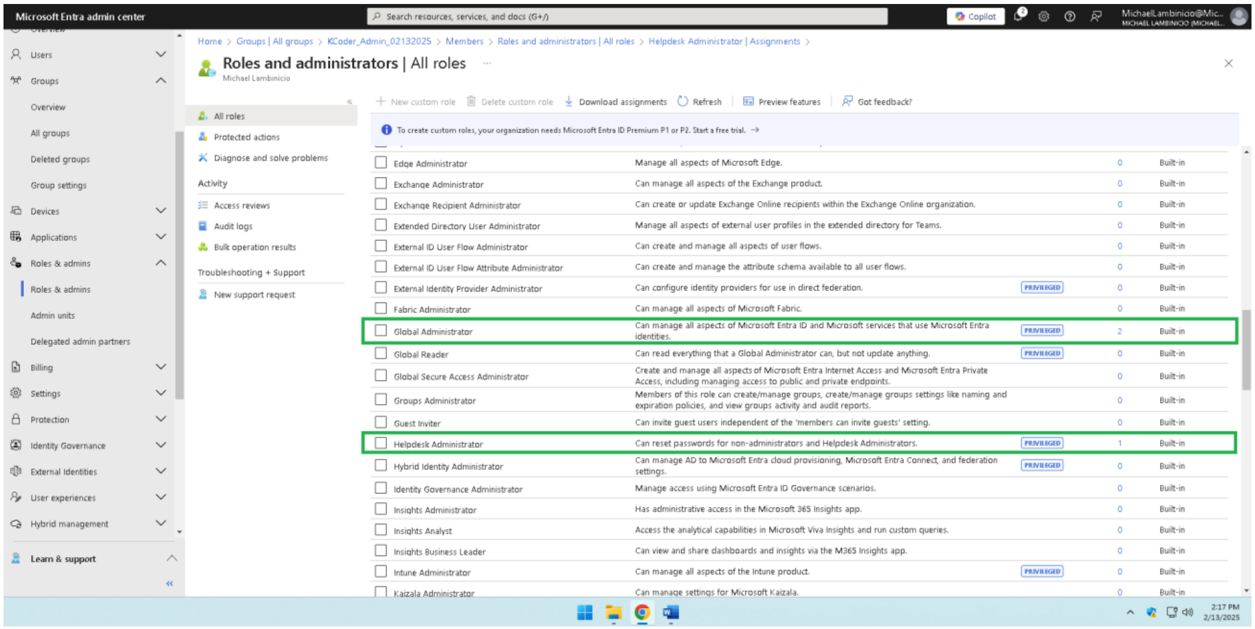
Groups | All groups

8 groups found

Name ↑	Object Id	Group type	Membership type	Email
ADSyncAdmins	8a6ffec5-e777-4d43-845d-f4ebc578d4a8	Security	Assigned	
ADSyncBrowse	a5208eb3-790b-47fb-ae57-c107181da784	Security	Assigned	
ADSyncOperators	7190c866-878e-4764-ab6d-3bd8618eaa78	Security	Assigned	
ADSyncPasswordSet	d66cf263-fe5e-4925-8142-d1bce20d4284	Security	Assigned	
DnsAdmins	e07d1d46-2791-408a-bd5f-e6549e8d1fa8	Security	Assigned	
DnsUpdateProxy	b4f3c0d3-d697-470a-9b6c-e0627a46816d	Security	Assigned	
KCoder_Admin_02132025	63ac68e4-de10-4ce6-b8ed-d57f44695562	Security	Assigned	
KCoder_Support_02132025	6f0f9a9d-b37c-44c1-bbbe-8b7ba62fc299	Security	Assigned	

Part 2: Manage Role-Based Access Control (RBAC) Roles

In this part, you are going to assign roles for users in which they will be responsible for. To do this, you will click on “Roles and admin” on the left pane under the Identity section. It will then populate all the roles available to assign for each member, as shown below:

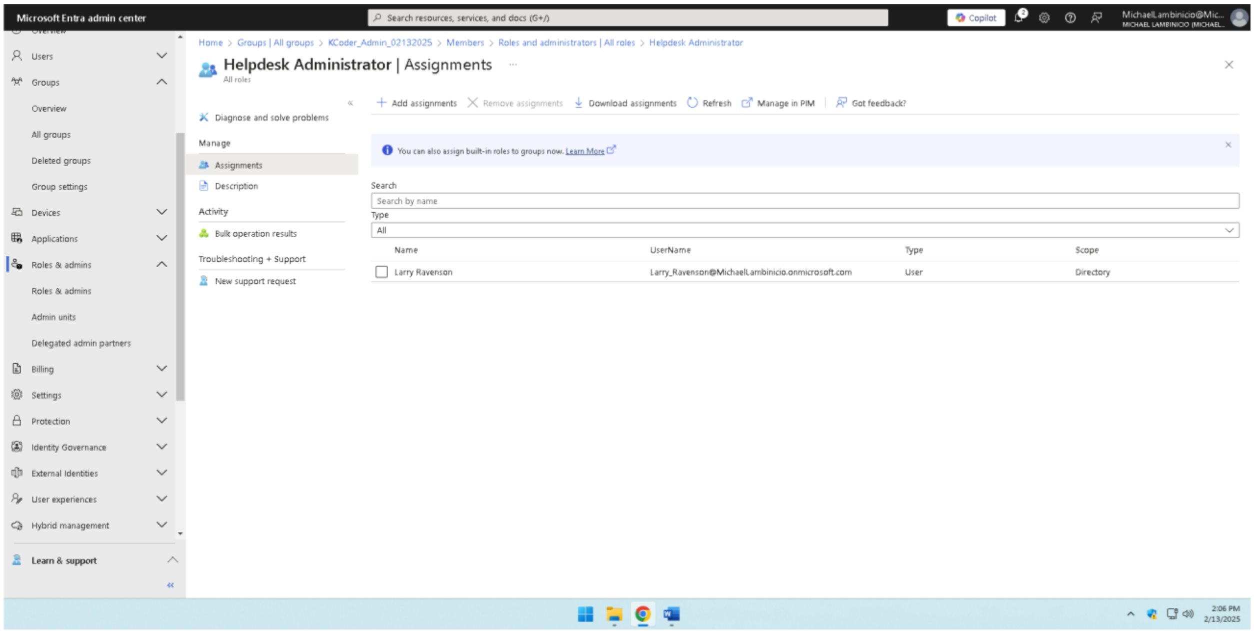


Roles and administrators | All roles

To create custom roles, your organization needs Microsoft Entra ID Premium P1 or P2. Start a free trial.

□	Edge Administrator	Manage all aspects of Microsoft Edge.		0	Built-in
□	Exchange Administrator	Can manage all aspects of the Exchange product.		0	Built-in
□	Exchange Recipient Administrator	Can create or update Exchange Online recipients within the Exchange Online organization.		0	Built-in
□	Extended Directory User Administrator	Manage all aspects of external user profiles in the extended directory for Teams.		0	Built-in
□	External ID User Flow Administrator	Can create and manage all aspects of user flows.		0	Built-in
□	External ID User Flow Attribute Administrator	Can create and manage the attribute schema available to all user flows.		0	Built-in
□	External Identity Provider Administrator	Can configure identity providers for use in direct federation.	PRIVILEGED	0	Built-in
□	Fabric Administrator	Can manage all aspects of Microsoft Fabric.		0	Built-in
□	Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	PRIVILEGED	2	Built-in
□	Global Reader	Can read everything that a Global Administrator can, but not update anything.	PRIVILEGED	0	Built-in
□	Global Secure Access Administrator	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managing access to public and private endpoints.		0	Built-in
□	Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and view groups activity and audit reports.		0	Built-in
□	Guest Inviter	Can invite guest users independent of the 'members can invite guests' setting.		0	Built-in
□	Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	PRIVILEGED	1	Built-in
□	Hybrid Identity Administrator	Can manage AD to Microsoft Entra cloud provisioning, Microsoft Entra Connect, and federation settings.	PRIVILEGED	0	Built-in
□	Identity Governance Administrator	Manage access using Microsoft Entra ID Governance scenarios.		0	Built-in
□	Insights Administrator	Has administrative access in the Microsoft 365 Insights app.		0	Built-in
□	Insights Analyst	Access the analytical capabilities in Microsoft Viva Insights and run custom queries.		0	Built-in
□	Insights Business Leader	Can view and share dashboards and insights via the M365 Insights app.		0	Built-in
□	Intune Administrator	Can manage all aspects of the Intune product.	PRIVILEGED	0	Built-in
□	Kaizala Administrator	Can manage settings for Microsoft Kaizala.		0	Built-in

Above, we will be adding Larry Ravenson to the Helpdesk Administrator role and Susan Pandya to the Global Administrator role. To add Larry, you will check Helpdesk Administrator and click on “add assignment”. Find Larry Ravenson and check his name and choose add, shown below:



Helpdesk Administrator | Assignments

You can also assign built-in roles to groups now. Learn More

Search

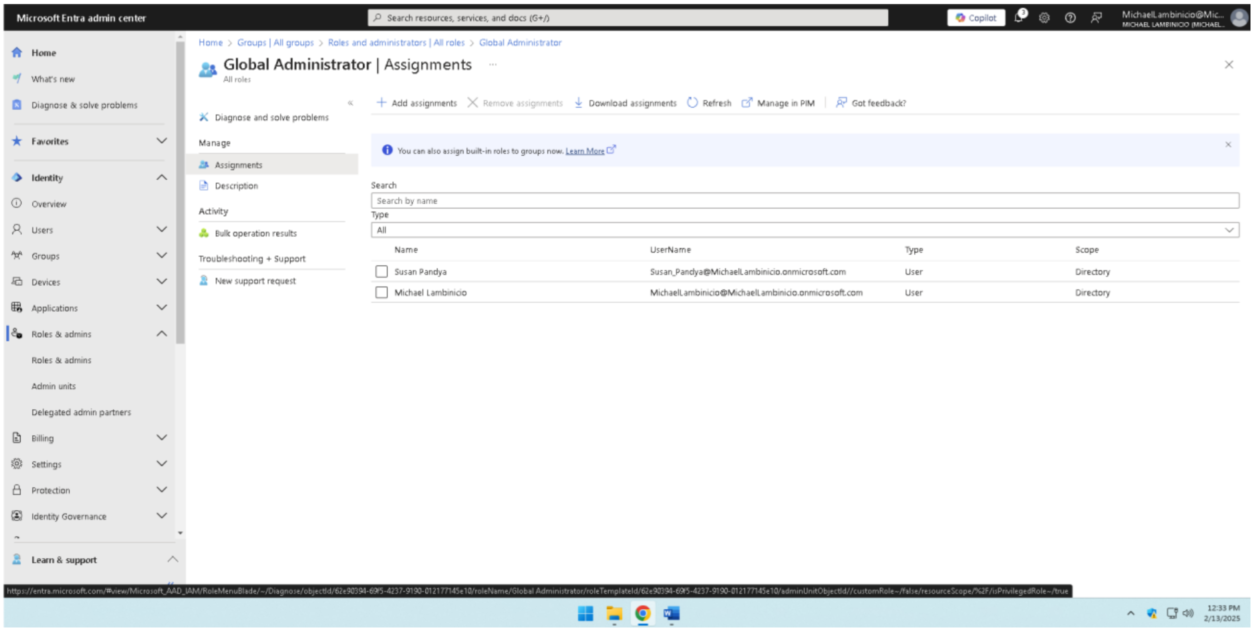
Search by name

Type

All

	Name	UserName	Type	Scope
□	Larry Ravenson	Larry_Ravenson@MichaelLambinicio.onmicrosoft.com	User	Directory

Then, you will do the same for Susan Pandya for the Global Administrator role, as shown below:



Global Administrator | Assignments

You can also assign built-in roles to groups now. Learn More

Search

Search by name

Type

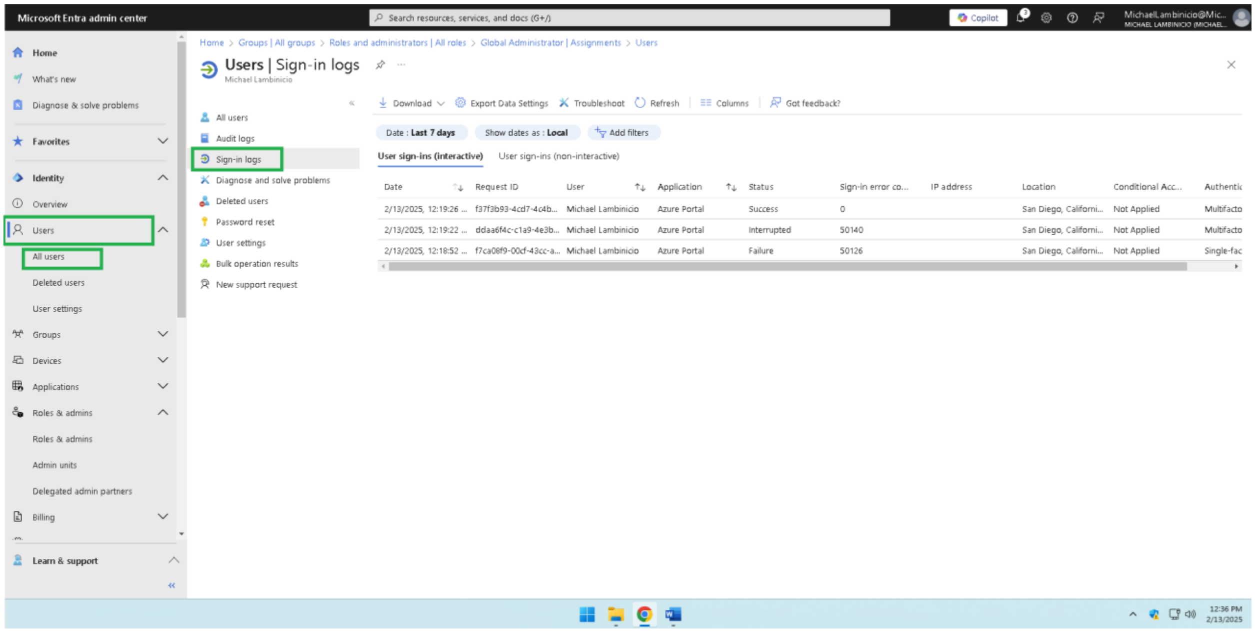
All

	Name	UserName	Type	Scope
□	Susan Pandya	Susan_Pandya@MichaelLambinicio.onmicrosoft.com	User	Directory
□	Michael Lambinicio	MichaelLambinicio@MichaelLambinicio.onmicrosoft.com	User	Directory

This in general enables organizations to apply grandular controls, reducing the attack surface and minimizing the potential impact of security incidents. This approach safeguards sensitive data and ensures the integrity of critical infrastructure components. [1]

Part 3: Examine User Login Activity

To do this, you will have to view “all users” in the users section on the left pane under identity. In the main window, you will then click on sign-in logs to view the sign-in activity for the last 7 days, as shown below:



Date : **Last 7 days**

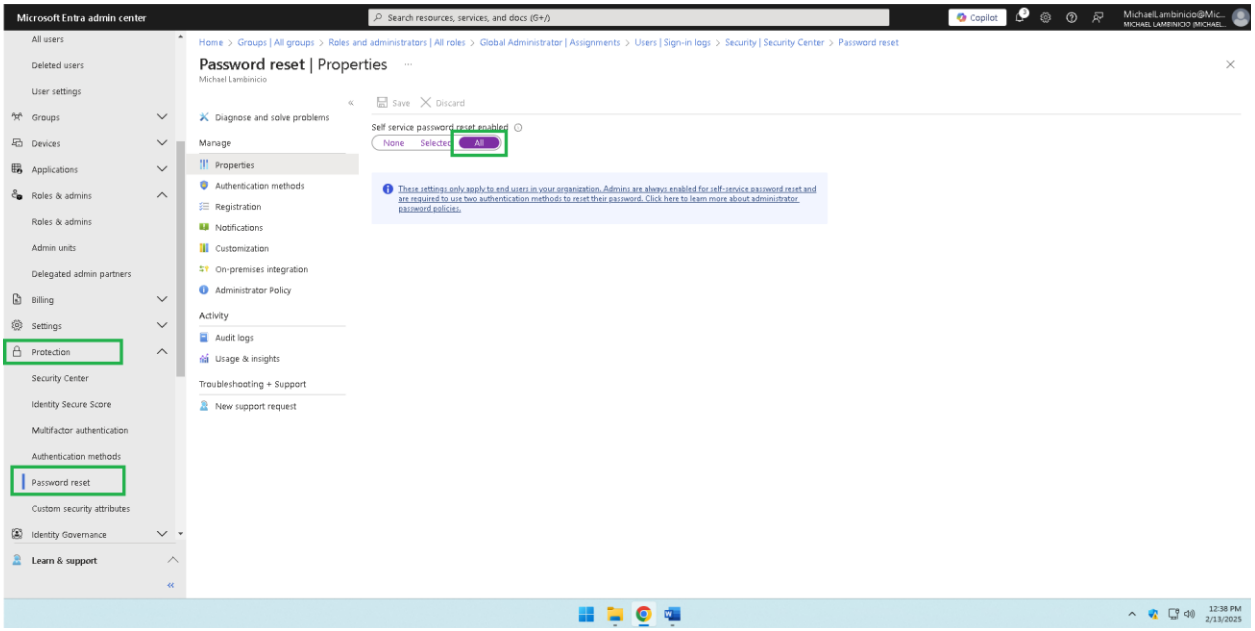
Show dates as : **Local**

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User	Application	Status	Sign-in error co...	IP address	Location	Conditional Acc...	Authentic
2/13/2025, 12:19:26 ...	f37f3b93-4cd7-4c4b...	Michael Lambinicio	Azure Portal	Success	0		San Diego, Californi...	Not Applied	Multifacto
2/13/2025, 12:19:22 ...	ddaa6f4c-c1a9-4e3b...	Michael Lambinicio	Azure Portal	Interrupted	50140		San Diego, Californi...	Not Applied	Multifacto
2/13/2025, 12:18:52 ...	f7ca08f9-00cf-43cc-a...	Michael Lambinicio	Azure Portal	Failure	50126		San Diego, Californi...	Not Applied	Single-fac

Part 4: Entra ID Password Reset

To apply password reset, you will click on “Protection” in the left pane under Identity, and choose “Password reset.” In the main window, you will have three options, choose “All”. Click save to apply your new settings, shown below:



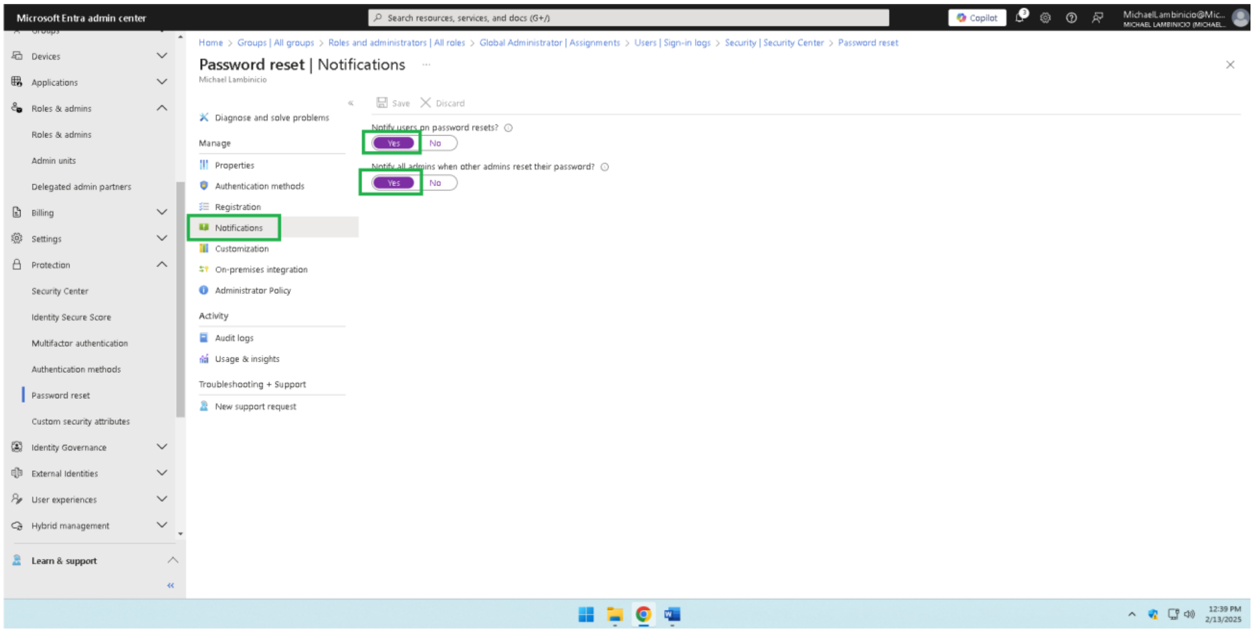
Password reset | Properties

Self service password reset enabled: None Selected [✓ All]

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Part 5: Password Reset Notification

If you would like to receive notifications for the password reset, in the same window from part 4, you would then choose “notifications” to show if you would like notify the users and admin of resetting, shown below:



Password reset | Notifications

Notify users on password resets? [✓ Yes] No

Notify all admins when other admins reset their password? [✓ Yes] No

Part 6: Authentication

The Opportunity: Basic Authentication and Moden Authentication

Using basic authentication would be more vulnerable to attack as it may only require a simple password to login, making it easy for hackers to infiltrate. They like to intercept any data transmitted to gain access to valuable information so they can use it for profit. In the modern authentication, it is now using multi-factor authentication, where you will either have a token (smart card) that has identity certificates designated to you as part of the authentication process, then you will need to either type a password or pincode to log in. Another method is after you type your password in the login section, it will send you an e-mail or notification on another device to use and enter back into the login section to verify you are the actual person. It has even expanded to biometrics where after you log in, you provide facial recognition or a fingerprint scan to verify you are the actual person logging in. These methods are more secure and have a higher grade of protection for any organization that holds valuable information daily.

References

[1] M. Buenning, “Understanding and implementing azure RBAC,” NinjaOne, https://www.ninjaone.com/blog/understanding-and-implementing-azure-rbac/ (accessed Feb. 17, 2025).

Resources

Azure Active Directory Groups: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal

Azure AD Roles: https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-manage-roles-portal

Azure Self Service Password Reset - https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

Azure Active Directory Banned Passwords: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection