AUSTRALIAN CATHOLIC UNIVERSITY

Evolve and Thrive with M365:

Enhancing Security for Tomorrow

With:

Mark Laffan – Cyber Security Operations Engineer

Daniel Silver – IDAM Lead

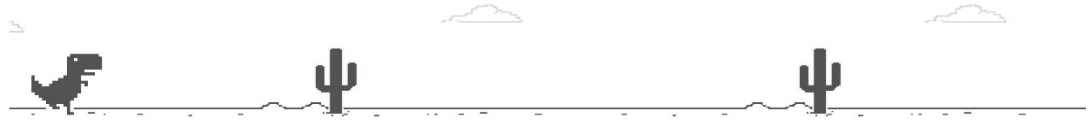
Todays Agenda

Documents will be uploaded here:
https://github.com/markslaffan/Auscert2025

PIM

- What is it, how to set it up (tips, tricks)
- IAM ,Governance,Training
- Demo’s

Morning tea 10:30am – 11am



Azure Automation/PowerShell

- Using Automation/PowerShell
- Creating playbooks

SOA/EOP

- Overview of SOA, Example output
- EOP Tips & Tricks

Phishing Sim

- Creating a simulation
- Tips and tricks

People, Process and Technology model

(invented circa 10,000 B.C, before the wheel)

People – The human element - how you deal with the peopley part of the model, like training and awareness.

Process – The “Frying pan” - Governance of the PIM model, how you use it? What are the roles and responsibilities.

Technology – The “fire”- how you use technology in the model, what rules do you want to enforce, how?

There’s always one…

user…

“In cybersecurity, we are only as strong as our weakest link.”

– Unknown

Privileged Identity Management (PIM)

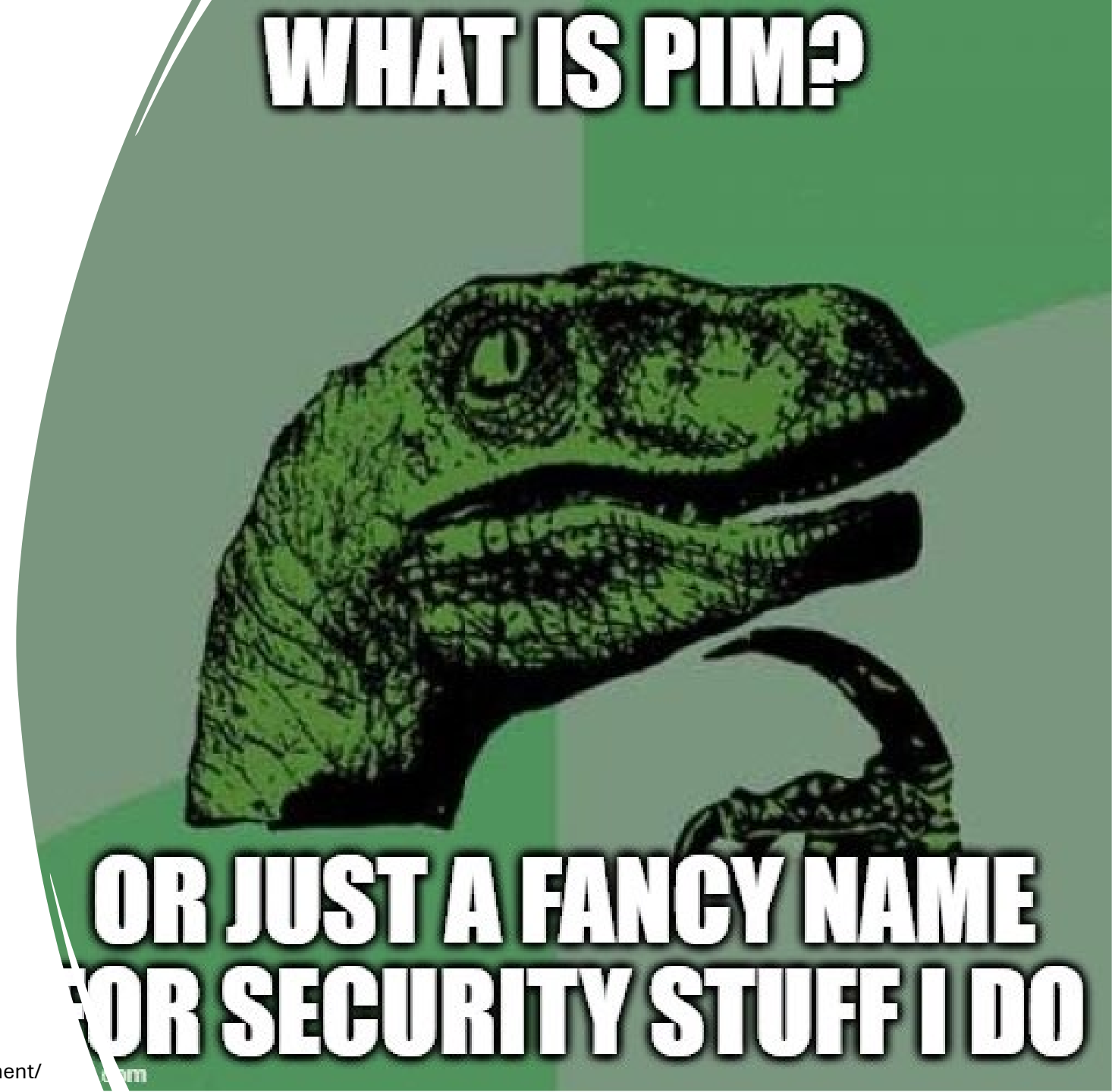
Agenda

- History of PIM at ACU – how it started
- What is PIM? Who has used PIM? Hands up!
- How to set it up – tips/tricks (not a how-to)
- IAM & Dynamic groups etc
- Governance – procedure/policy template
- Training your Staff?

What is PIM?

Features

- Time-based and approval-based role activation to reduce the risks of excessive or misused access.
- Multifactor authentication for role activation.
- Access reviews to ensure users still need their roles.
- Audit history for internal and external audits



https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/

Setting up PIM - tips

Strongly suggest getting external help – Use your Microsoft engineers if you have support hours! Also, setup Azure MFA!

The most important role is "Privileged Role Administrator" make sure you have this role and limit its assignment! – (this role can give anyone access to GA!)

Make sure you have a "Breakglass" account – no MFA and password is kept by your CIO/CISO etc.

Plan out what roles IT staff will need – remove any directly assigned roles.

Global Administrator (GA) role should only be Active for the "Break glass" account!

Limit GA to max 5 "eligible" Staff, no Active assignments!

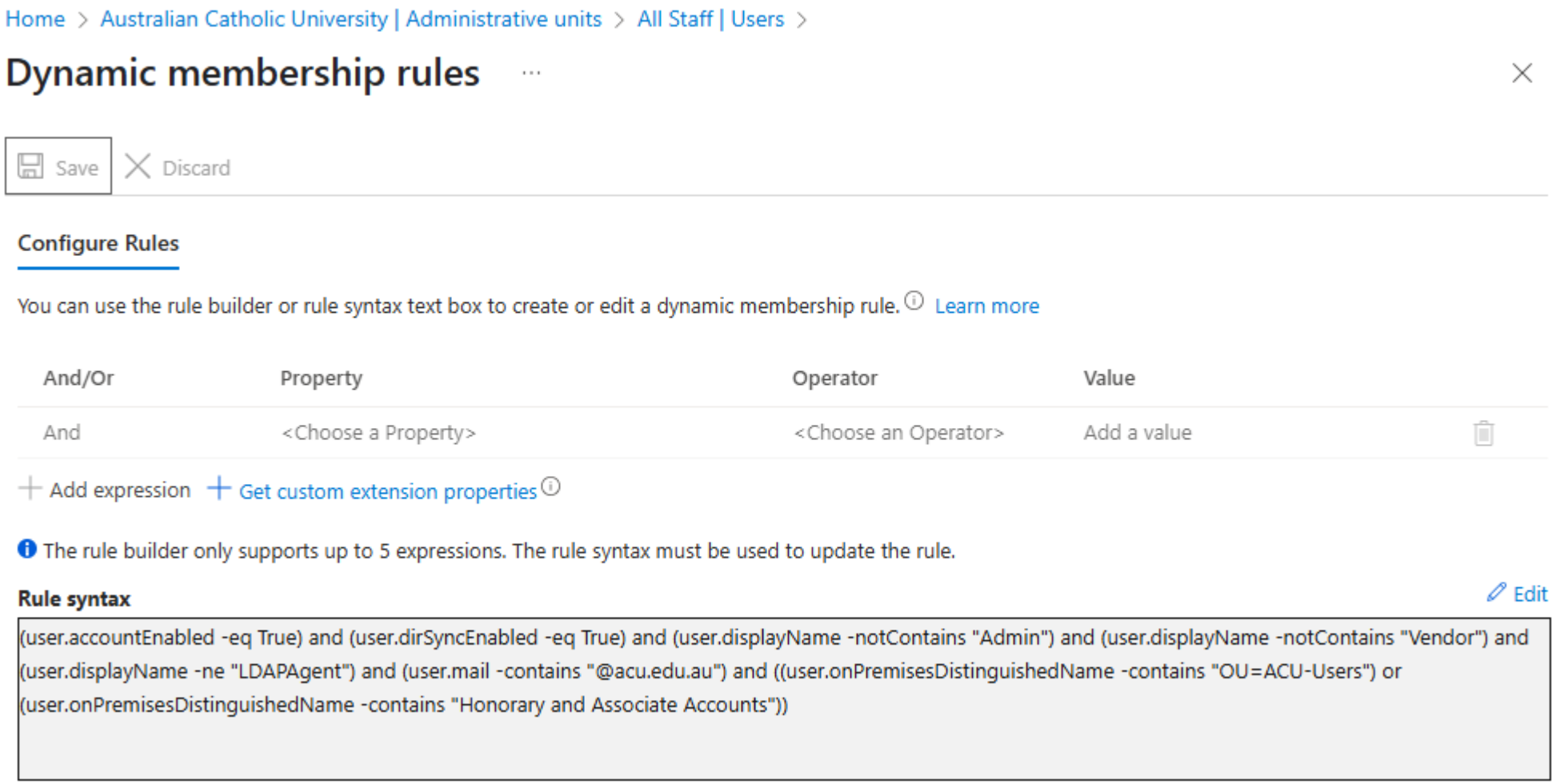
IAM and Dynamic Groups

- Administrative Units
- Access controls – can do what to who
- Active vs. Eligible roles
- IAM Tips & tricks

Administrative Units

- **Delegated Administration**: Allows you to delegate administrative tasks to specific users or groups within defined scopes, such as departments or regions.
    - E.g. Student helpdesk can only change student passwords
- **Enhanced Security**: Helps implement least privilege access by restricting permissions to only what is necessary for specific roles.
- **Simplified Management**: Makes it easier to manage users, groups, and devices by organizing them into logical units.
- **Improved Compliance**: Ensures that administrative roles and permissions are aligned with organisational policies and compliance requirements
- **Scalability**: Supports large organisations with multiple divisions or departments by providing a structured way to manage resources
- Basically, uses the same dynamic group rules to select users, groups or devices
- Tips
    - You can’t assign a dynamic group to a unit, then they can only modify that group and not the members!

Example of Administrative Unit



Rule syntax

- Use the “Add expression” to build the dynamic rule

E.g.

(user.accountEnabled -eq True) and

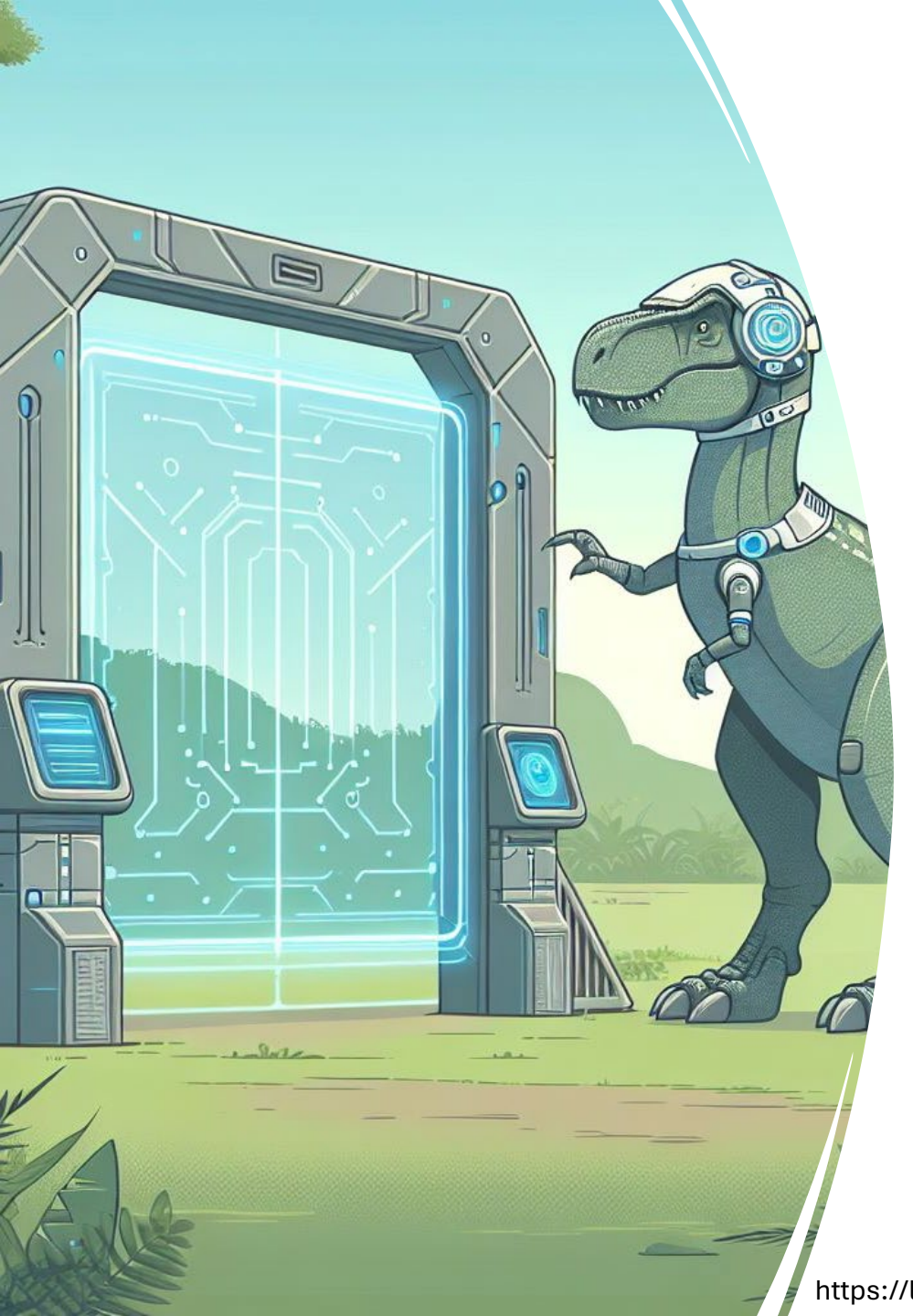
(user.dirSyncEnabled -eq True) and

(user.mail -contains "@domain.edu.au") and

(user.onPremisesDistinguishedName -contains "OU=Users")

Dynamic Group Rules & Limitations

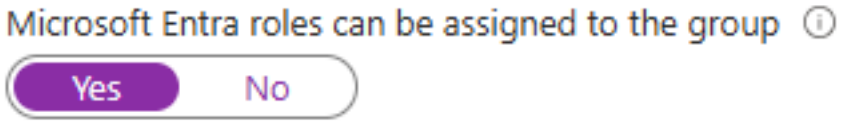
Dynamic Group Rules	When creating a dynamic group, there is the option to either use the rule builder or the rule syntax. The rule builder looks easier at first, but has limitations: • Can only support up to 5 expressions • Some expressions aren't available through the rule builder
Dynamic group Limitations	You can create a dynamic membership groups for users or devices, but you can't create a rule that contains both users and devices. You can't create a device membership group based on the user attributes of the device owner. A Microsoft Entra ID P1 license / Intune for Education license required



Access controls

Role assignable groups

- **Simplified Management**: Assigning roles to groups instead of individuals makes it easier to manage permissions.
- **Consistent Permissions**: Ensures that all members of the group have the same permissions, reducing the risk of discrepancies.
- Only **Privileged role administrators or Owners** can edit groups, User Administrators are restricted from editing them.
- When not to use groups?
- TIP: Make sure you turn on Entra roles when creating the group!



https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-create-eligible?tabs=admin-center

Active vs. Eligible roles

Audience participation

- Active – well, always active
- **Question for the room**
  - **Why is this bad?**
  - **Why is it good?**
- Should be assigned to someone that is using roles all the time
  - Try not to overuse this!

- Eligible roles, or Just In Time Admin
- **Question for the room**
  - **Why is this bad?**
  - **Why is it good?**
- Some users do not need that access all the time!
  - Most assignments should be Eligible, enforce this!
  - What groups of people should use this?

Define primary and secondary role managers

This requires some knowledge of your organisation structure; this is the hardest part!

- Assign **Primary** & **Secondary** role approver and manager
  - These will be required to approve assignments and elevation
- Discuss with CIO/CISO on who will approve **Global Administrator** elevation – need to ensure that they are aware of how powerful this role is!
  - Backup approver for this role as well

PIM roles .... (some of them)

- **Global Administrator (Privileged):** Has access to all administrative features in Microsoft Entra and other Microsoft services.
- **Privileged Role Administrator (Privileged):** Manages role assignments in PIM, including activating and deactivating roles.
- **User Administrator:** Manages users and groups, including resetting passwords and monitoring service health.
- **Billing Administrator:** Manages billing, subscriptions, and support tickets.
- **Security Administrator (Privileged):** Manages security-related features, such as conditional access and identity protection.
- **Exchange Administrator (Privileged):** Manages Exchange Online settings and features.
- **SharePoint Administrator (Privileged):** Manages SharePoint Online settings and features.
- **Teams Administrator (Privileged):** Manages Microsoft Teams settings and features.
- **Compliance Administrator (Privileged):** Manages compliance-related features, such as data loss prevention and eDiscovery.
- **Application Administrator:** Manages application registrations and enterprise applications.
- **Helpdesk Administrator:** Provides limited administrative access to reset passwords and monitor service health.
- **Intune Administrator (Privileged):** Manages Intune settings and features for device management.
- **Directory Readers:** Has read-only access to directory information.

Plus many more! https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

PIM model (Governance) – template overview

- Define purpose – why are we doing this?
- Features and support the principles with industry standards
- Rules for setting up accounts – MFA, Naming conventions, auditing
- Approving requests workflow – roll your own
- Auditing/alerts
- Define all Roles and responsibilities
- Access review – setup cycle

- **Note:** Entra and Azure resource roles are different

Purpose

This document provides guidance on managing Microsoft 365 tenants for <company name>. It should be reviewed every 6 months and follows the principle of least privilege to ensure governance.

Privileged Identity Management (PIM) helps manage, control, and monitor access to critical resources in Azure AD, Azure, and other Microsoft Online Services like Microsoft Office 365. PIM offers just-in-time (JIT) and just-enough access (JEA) to minimize the number of users with administrative privileges, reducing the risk of:

- Malicious actors gaining access.
- Authorized users inadvertently impacting sensitive resources.

PIM also enables auditing of administrative activities to mitigate risks of excessive, unnecessary, or misused access rights. Each tenant includes an emergency "BreakGlass" account for emergency access only.

Audience

This document is intended for System Administrators who need elevated privileges in Microsoft 365 tenants for daily maintenance. Regular users of Microsoft 365 services do not require access to PIM or related information.

Privileged Identity Management (PIM) Model

Azure PIM in the Azure portal offers time-based and approval-based role activation to minimize privilege exposure and enhance visibility, reducing risks of excessive or misused access. The PIM model allows specific actions within defined scopes.

Key features of PIM:

- Just-in-time privileged access to Azure AD and Azure resources.
- Eligibility assignment for privileged access group membership or ownership.
- Time-bound access with start and end dates.
- Approval requirement for activating privileged roles.
- Multi-factor authentication enforcement for role activation.
- Justification for role activation.
- Notifications for privileged role activations.
- Access reviews to confirm ongoing role necessity.
- Audit history downloads for internal or external audits.

PIM PRINCIPLES

There are 3 main principles of PIM. These principles are mapped back ISO 27002:2022 controls to demonstrate how the implementation will adhere to Security and Compliance requirements.

PRINCIPLES	ISO 27002:2022
Controlling Logical Access Privileges and Implementing Least Privilege Access	B.5.15 – Business requirement of access control B.5.15 – Access to networks and network services B.5.18 – User access provisioning B.8.2 – Management of privileged access rights B.8.3 – Information access restriction
Enforcing Separation of Duties	B.5.3 – Segregation of duties
Access Logging / Monitoring / Auditing	B.8.15 – Event logging B.8.15 – Administrator and operator logs

Privileged Accounts – Configuration

All accounts created for PIM need to adhere to the following:

- **Admin Accounts:** Must be cloud-only and follow this naming convention
  - Staff: FirstName.LastName.Admin@[tenant].onmicrosoft.com
  - Vendors: Company.FirstName.LastName.Admin@[tenant].onmicrosoft.com
- **Conditional Access Policy:** All admin accounts must be members of the conditional access policy group (e.g., "MFA REQUIRED ADMINS CONDITIONAL").
- **No Shared Accounts:** Each account must be owned by an individual with Multi-Factor Authentication (MFA) enabled and registered before roles are added.
- **Self-Service Password Reset (SSPR):** Must be enabled and registered before roles are added.
- **Service Accounts:** Must never have global administrator rights, with exceptions approved by the <IT Senior Leadership Team/CIO/CISO>. Service accounts must have passwords of at least 30 characters.
- **Auditing:** All administrative actions will be audited with indefinite log retention.
- **Vendor Accounts:** Must have expiry dates and only be granted eligible roles necessary for their tasks. Accounts must be disabled when the vendor's engagement ends, with notice given to the <Security/governance team> by the responsible manager.

- **Manual Audits:** Conducted monthly or quarterly to ensure appropriate access levels and remove stale accounts (inactive after X days). Reports will be presented to PIM managers and the <IT Senior Leadership Team/CIO/CISO>.
- **Automated Auditing:** Requires PIM approvers to review assignments in the Azure portal.
- **Account Removal:** IT Managers must report accounts needing removal to the <Security/governance team> immediately when staff leave their position (movers or leavers).
- **BreakGlass Accounts:** Tested yearly, with updated phone numbers for <IT Senior Leadership Team/CIO/CISO> & <Security/governance team>.

PIM Roles

Certain roles must be limited to specific teams. For example, the Global Administrator role should be restricted to no more than 5 users, including the BreakGlass account.

In emergencies or MFA failures, the BreakGlass account, owned by the <CIO/CISO>, will be activated and used only in emergencies.

General Rules

Not all roles are equal, some higher privileges must be restricted.

- **Global Administrator:** Maximum of 4 eligible users, with the BreakGlass account as the only active user. As recommended by Microsoft (Secure score metric).
- **Privilege Role Administrator:** Limited to the <Security/Governance team>.
- **Security Administrator:** Most security roles, except Security Reader, should be restricted to the <Security/Governance team>.
- **Restricting Role available:** Only commonly used roles can be requested via the <your ticketing system>. Other roles require prior discussion with the <Security/Governance team> manager.
- **Use of Administrative Units:** to restrict access to different types of accounts rather than applying the role to the entire tenant. E.g. Student administration service desk can only change Student passwords by using a “students” unit. This restricts “password admins” to Students and not all accounts in the tenant. Administrative Units use the same filter rules like Dynamic groups, so careful planning is required.

Other Roles

Azure AD Privileged Identity Management (PIM) manages privileged access policies for Azure AD users. PIM assigns users to roles as either Active or Eligible, with roles having permanent or expiry-based assignments. Eligible roles require self-approval or “PIM role approver” action for elevation, with a maximum elevation time of <insert hours here> hours (up to 24 hours).

Role Assignments:

1. **Eligible:** Requires actions to use the role. Users can activate the role as needed, with no difference in access between active and eligible roles. Vendors should have eligible roles during their engagement, not active roles.
    - **With Approval:** For roles accessing sensitive information, approved by responsible managers.
    - **Without Approval (Self-approving):** For roles with minimal impact or single-person responsibility.
2. **Active:** Always usable without actions, for required roles.

All roles can have a set duration, either permanent or with an expiry date. Vendors must have expiry dates for role removal. Most IT staff may have permanent roles based on responsibilities, but casual staff or vendors should have expiry dates, typically no longer than 6 months.

Requesting PIM: Roll your own workflow

- Work out who can request roles?
- Built a list of roles that can be requested
- Who will approve roles – with backups
- Approval process – example
- How long they can be allocated?
- User Support model?

O365 Admin Role	Description	Primary Approver	Secondary Approver	Can self-approve? (If eligible)
Application Administrator	Users with this role can create and manage all aspects of app registrations and enterprise apps	AD Enterprise systems	CIO	No
Application Developer	Users with this role can create application registrations independent of the 'Users can register applications' setting	AD Enterprise systems	CIO	No
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	National security manager	AD Enterprise systems	yes
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	National security manager	AD Enterprise systems	no
Authentication Administrator	Can access to view, set and reset authentication method information for any non- admin user.	National security manager	AD Enterprise systems	No
Authentication Policy Administrator	Can create and manage all aspects of authentication methods and password protection policies.	National security manager	AD Enterprise systems	no
Azure AD Joined Device Local Administrator	Users assigned to this role are added to the local administrators group on Azure AD-joined devices.	National Manager, Digital Platform Services	AD Enterprise systems	no
Azure DevOps Administrator	Can manage Azure DevOps organization policy and settings.	AD Enterprise systems	CIO	no
Azure Information Protection Administrator	Can manage all aspects of the Azure Information Protection product.	National security manager	AD Enterprise systems	no
B2C IEF Keyset Administrator	Manage secrets for federation and encryption in the Identity Experience Framework.	Associate Director,Service Delivery, IT Client Services	CIO	No
B2C IEF Policy Administrator	Create and manage trust framework policies in the Identity Experience Framework.	Associate Director,Service Delivery, IT Client Services	CIO	No

Who can request roles?

Audience participation – two different methods:

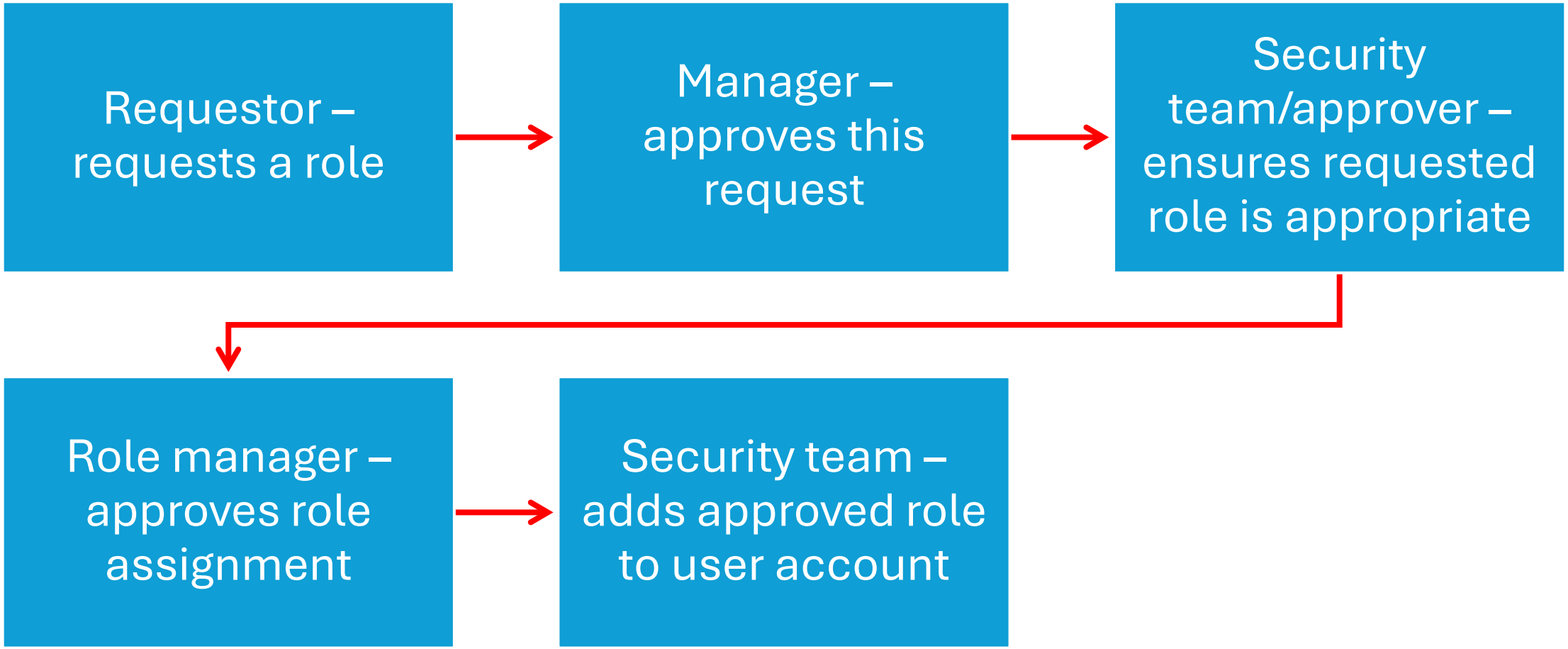
- Staff can request any role, but Manager will need to approve this

Question: what are the Pro's? Cons ?

- Managers request roles for their staff

Question: what are the Pro's? Cons ?

Role request workflow *



* Suggested only, but kinda working at ACU

Requesting a Role - Process

Defined Positions:

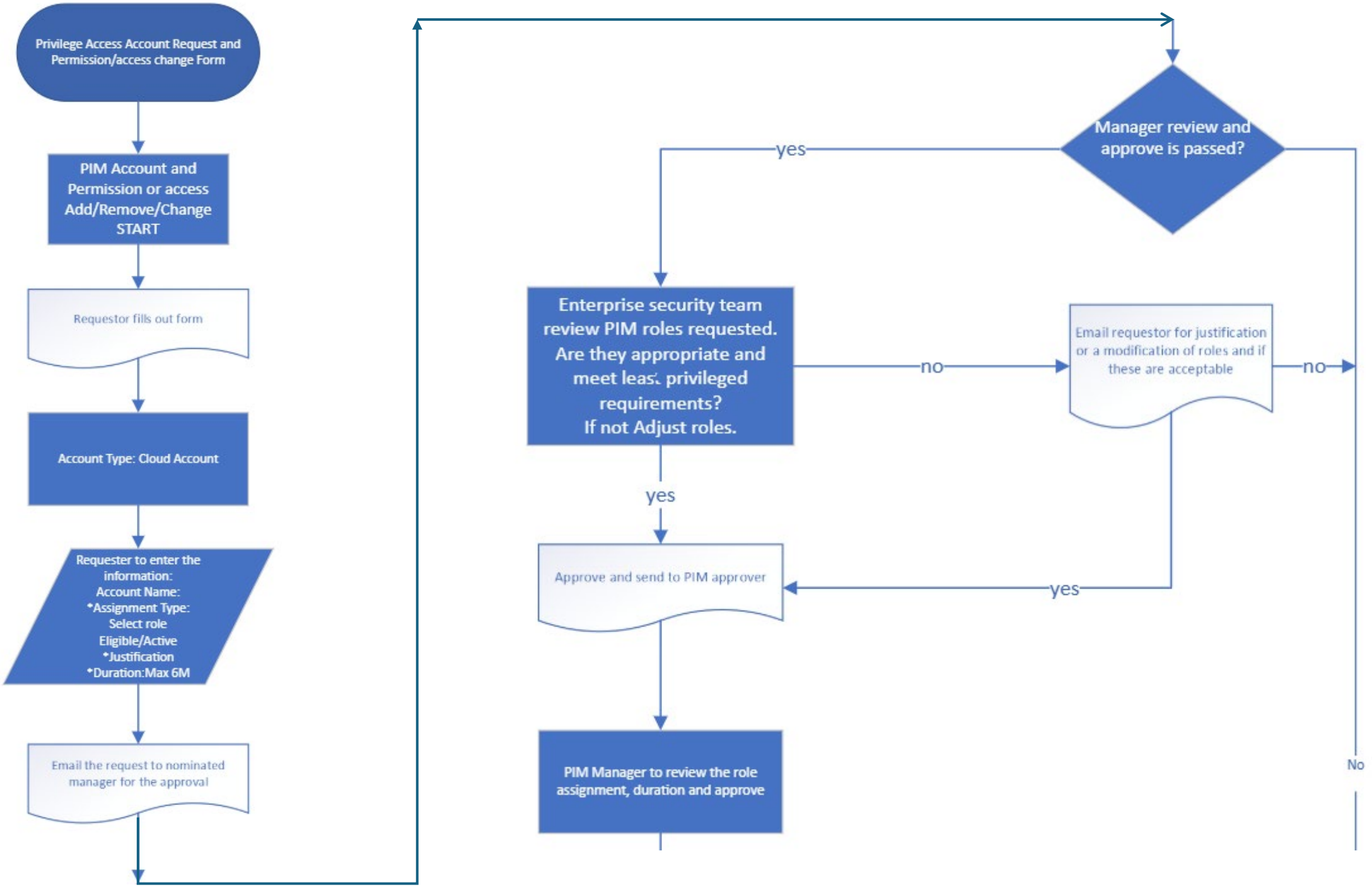
- **Requestor:** Assigned the role for administrative tasks.
- **Requestor's Manager:** The requestor's supervisor.
- **PIM Role Manager:** Approves privileged roles, approves elevation.
- **<Security/Governance Team>:** Reviews and assigns roles.

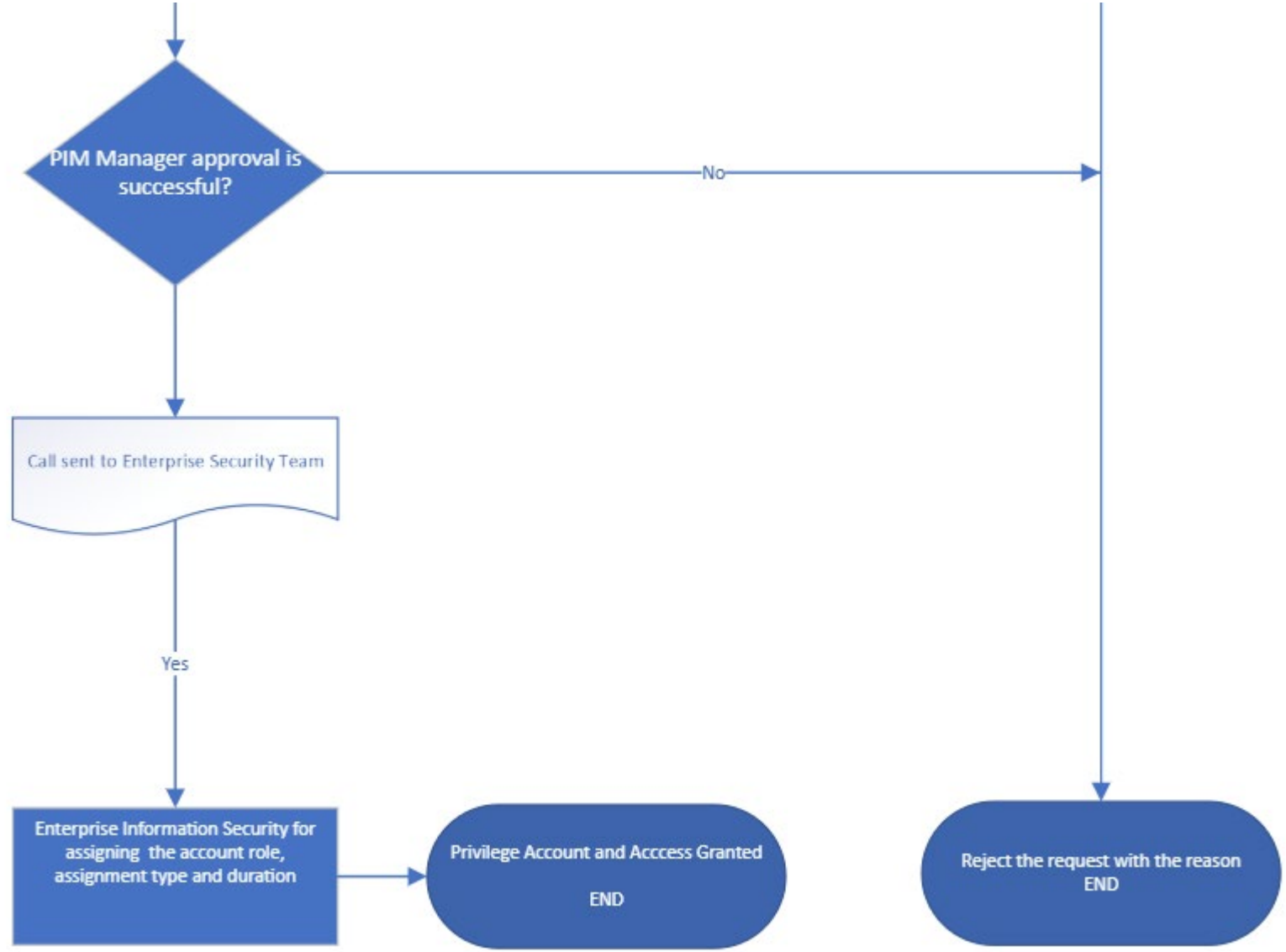
Role Request Submission: <your ticketing system>

Suggested Workflow:

1. **Submission:** Requestor or Manager submits the request. If the manager's approval is missing, it will be sought.
2. **Review:** <Security/Governance team> ensures:
    - Role suitability for the team/staff member's responsibilities.
    - Appropriate least privilege access with correct expiration.
    - Justification for the role.
3. **Approval:** Sent to the PIM Role Manager for access approval.
4. **Application:** Security/Governance team applies roles after all approvals.

Role requests can be rejected with justification by the manager, security/governance, or role manager.


Privilege Access Account Request and Permission/access change Form
PIM Account and Permission or access Add/Remove/Change START
Requestor fills out form
Account Type: Cloud Account
Requester to enter the information:
Account Name:
*Assignment Type:
Select role
Eligible/Active
*Justification
*Duration:Max 6M
Email the request to nominated manager for the approval
Manager review and approve is passed?
yes
Enterprise security team review PIM roles requested. Are they appropriate and meet least privileged requirements?
If not Adjust roles.
no
Email requestor for justification or a modification of roles and if these are acceptable
no
yes
Approve and send to PIM approver
yes
PIM Manager to review the role assignment, duration and approve
No


PIM Manager approval is successful?
No
Call sent to Enterprise Security Team
Yes
Enterprise Information Security for assigning the account role, assignment type and duration
Privilege Account and Acccess Granted
END
Reject the request with the reason
END

What should you do as part of reviewing a request?

Audience participation

From the view of security team and role approvers

Security team's role

Questions to ask before approving access:

- Why do users need access to a role?
- What will users do with that access?
- How often is the role required? – Eligible vs Active
- What can they do with that level of access?
- Is the role within their responsibilities?
- Do the Managers understand the roles that their team are using?
- Is this based on least privileged access?

Roles and Responsibilities

Sets the culture – depends on your organisation

- Define each team's role in the model
- Define R&R for CIO/CISO
- Set expectations! Audits, approvals/denials
- Create a RASCI Matrix?

Example Roles next…

Roles	Responsibilities	who	recommendation
Approvers	• Responsible for ensuring each person approved to have an administrative role has adequate training to perform their job function. • View pending approvals (requests) within a timely manner • Approve or reject requests for role elevation (single and bulk) • Provide justification for approval or rejection	Business system owners: • CIO • CISO • Associate directors • National managers	IT is ultimately responsible for the management of the Microsoft 365 tenants.
Global administrators	• Eligible accounts for Global Admin (these accounts are eligible to be promoted as Global Admin, every time a	• Microsoft 365 Administrator/s • Cyber Security Operations Staff	No more than 5 eligible accounts assigned at a time. Guests should/must not be assigned.

Auditing	Ensure controls within M365 meet all IT Security and Compliance requirements. Perform security investigations and compliance reporting. Manually audit all PIM roles monthly or quarterly	Security team	E-discovery Managers
M365 Administrators	M365 administrator is responsible for ensuring that tenant wide controls are up to date. This includes ensuring service availability. (Microsoft 365 Administrator)	EXO, SharePoint, Teams administrators.	Changes done using elevated Global Admin rights on tenants must be recorded and in line with CAB policies.
Application Administrators	Manage applications, create app registrations, enterprise apps etc	Security team/Apps team	Changes done using elevated Admin rights on tenants must be recorded and in line with CAB policies. Applications must have security/privacy reviews before connected to tenant
Desktop support	Manage hybrid connected or Intune connected devices	Desktop support teams	

Training your Staff

Training

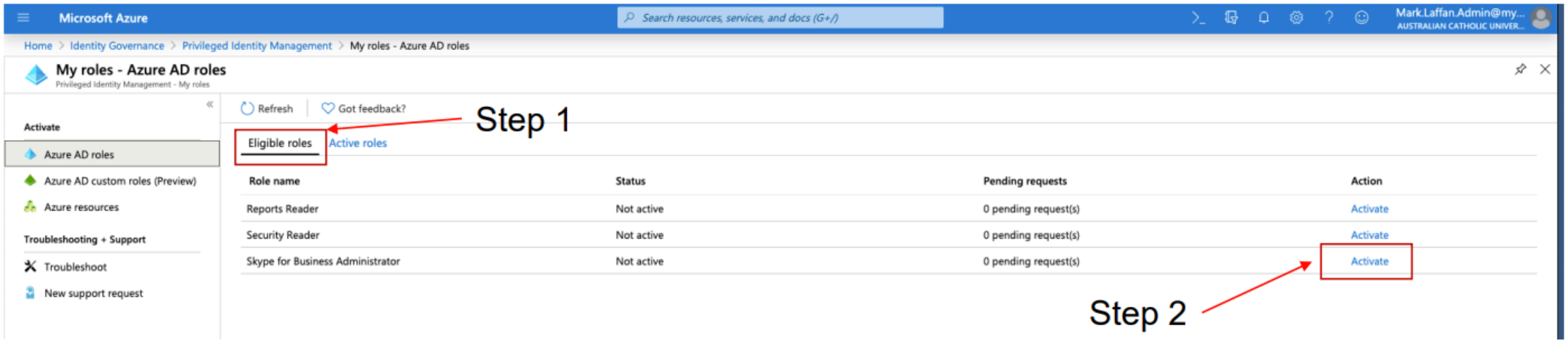
This is the “peoplely” part of PIM – sorry it needs to be done

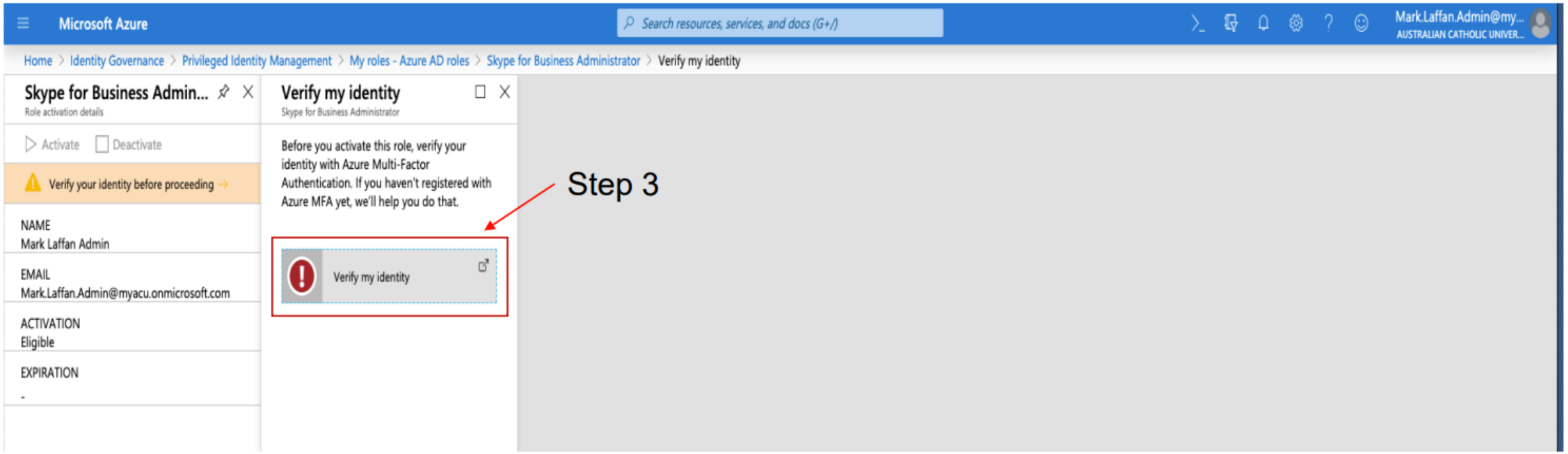
- You need to socialise the PIM model once approved
- Show how PIM requests work (insert your ticket system here)
  - Include Requestors & approvers!
- Show how the elevation process works
- Show PIM role managers how to approve elevation
- Record sessions for future reference!
- Document everything in a knowledgebase!
- You may need to look at a support model – but include this in the overall PIM model as well

Step 1: Ensure that you have been approved to be ‘eligible’ for specific administrative roles that you require.

- To check, login with your admin account to https://portal.azure.com
- Navigate to Identity Governance > Privileged Identity Management > Azure AD roles – My roles
- **Eligible** roles tab shows roles you have been approved to request
- **Active** roles tab shows permanent roles that are applied on your admin account.

Step 2: On Eligible roles tab, click on **Activate** for the role you need elevated.





Step 3: Once you have clicked on **Activate**, you will be directed to Verify your identity. This where you will need to register for Multi-Factor Authentication (MFA) if you have not done so.

- MFA registration can be done by installing the MS Authenticator app on your mobile device or [not recommended] you can also choose to have a push SMS or voice call sent to your nominated device.
- MFA is required for all privileged administrative accounts.

Live Demo

Everyone loves Barney, I mean live demos….

- Settings for each role
  - Activation period – max activation period
  - Self-elevation or approval
  - Notification settings
  - Approval settings
- Activation of a role – from request to activate

Role settings

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	Yes
Require approval to activate	Yes
Approvers	3 Member(s), 0 Group(s)

If you are seeing this, the demo went poorly

Role settings

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

Role settings

Send notifications when members are assigned as eligible to this role:

Type	Default recipients
Role assignment alert	Admin
Notification to the assigned user (assignee)	Assignee
Request to approve a role assignment renewal/extension	Approver

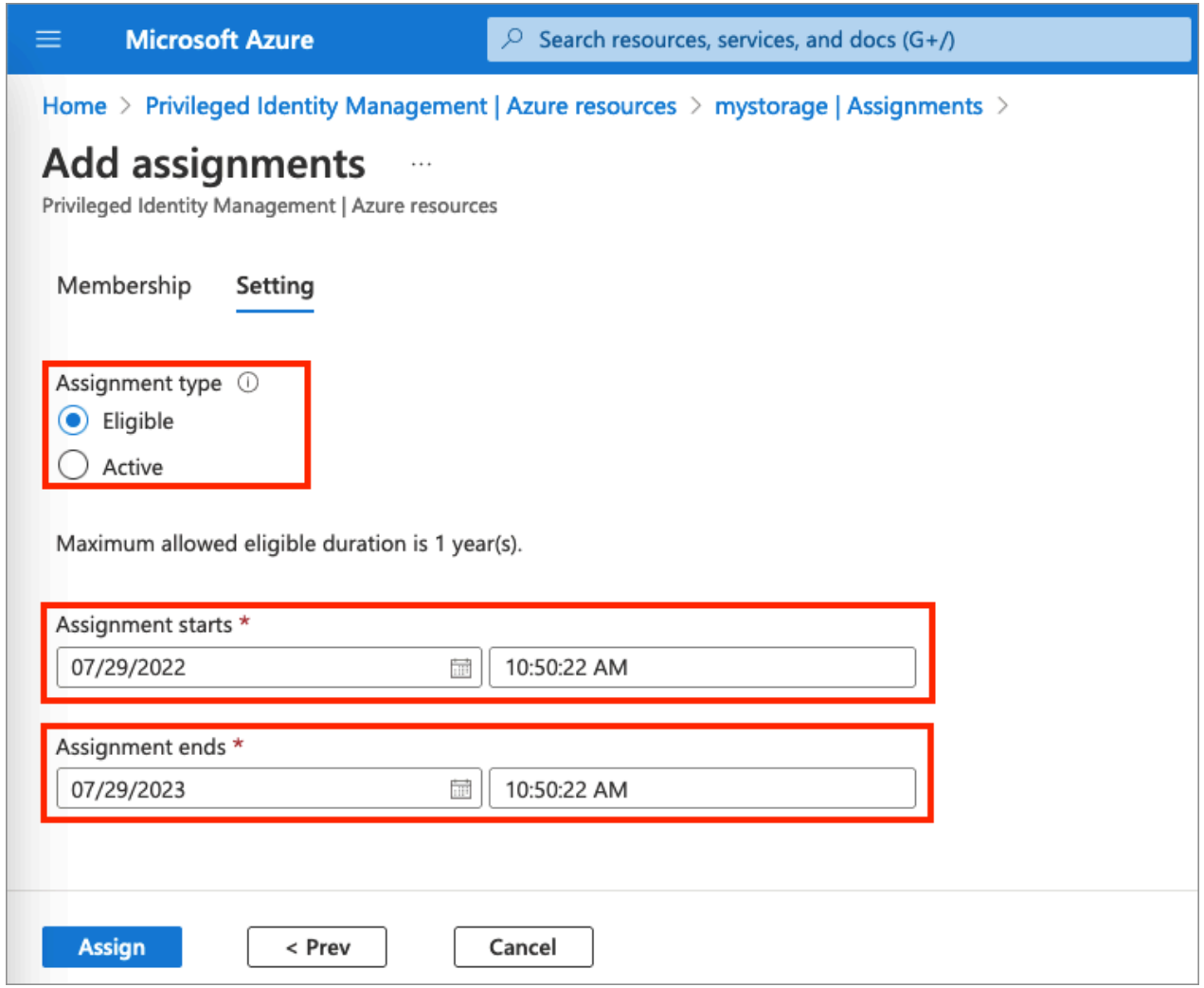
Send notifications when members are assigned as active to this role:

Type	Default recipients
Role assignment alert	Admin
Notification to the assigned user (assignee)	Assignee
Request to approve a role assignment renewal/extension	Approver

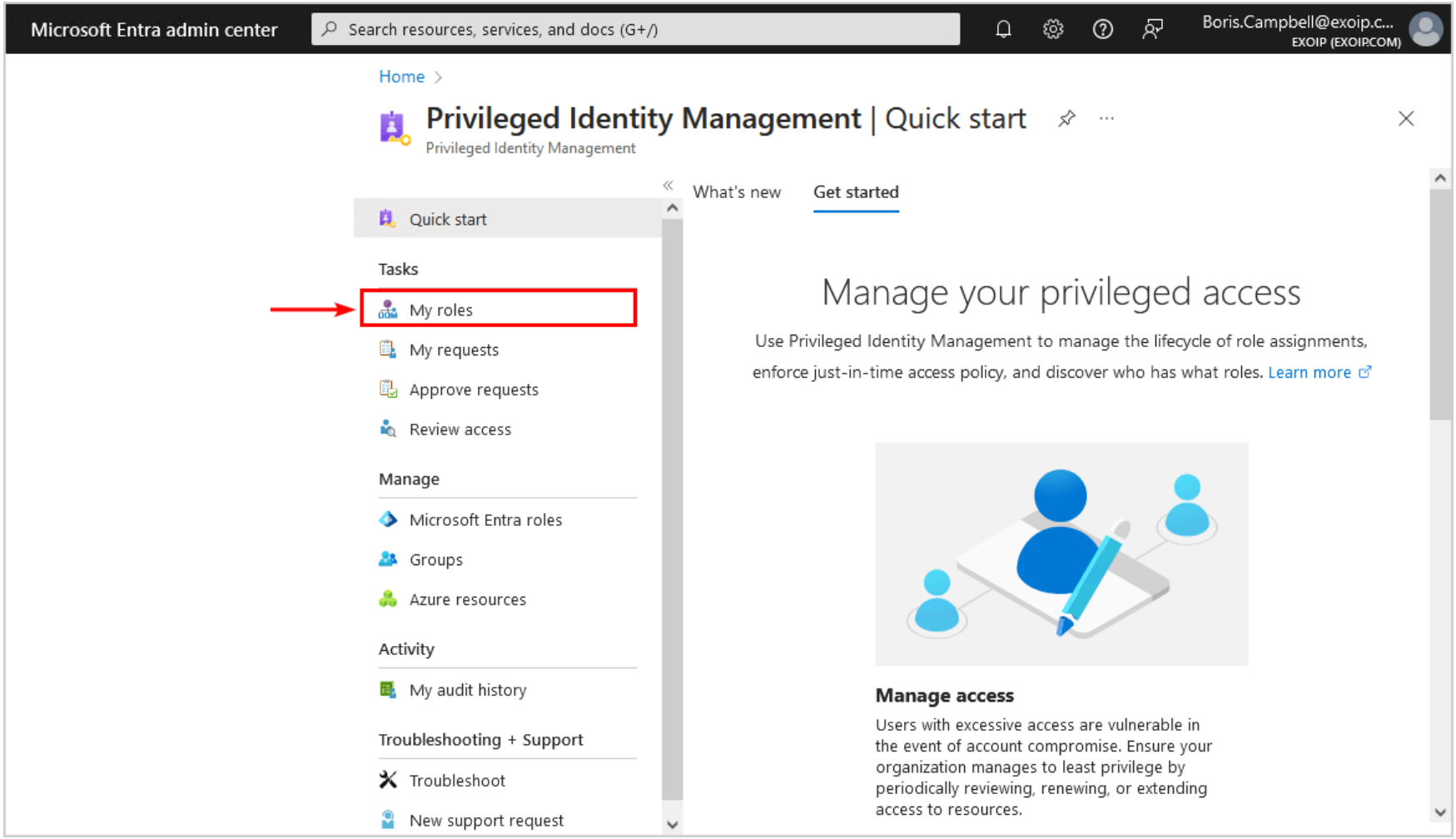
Send notifications when eligible members activate this role:

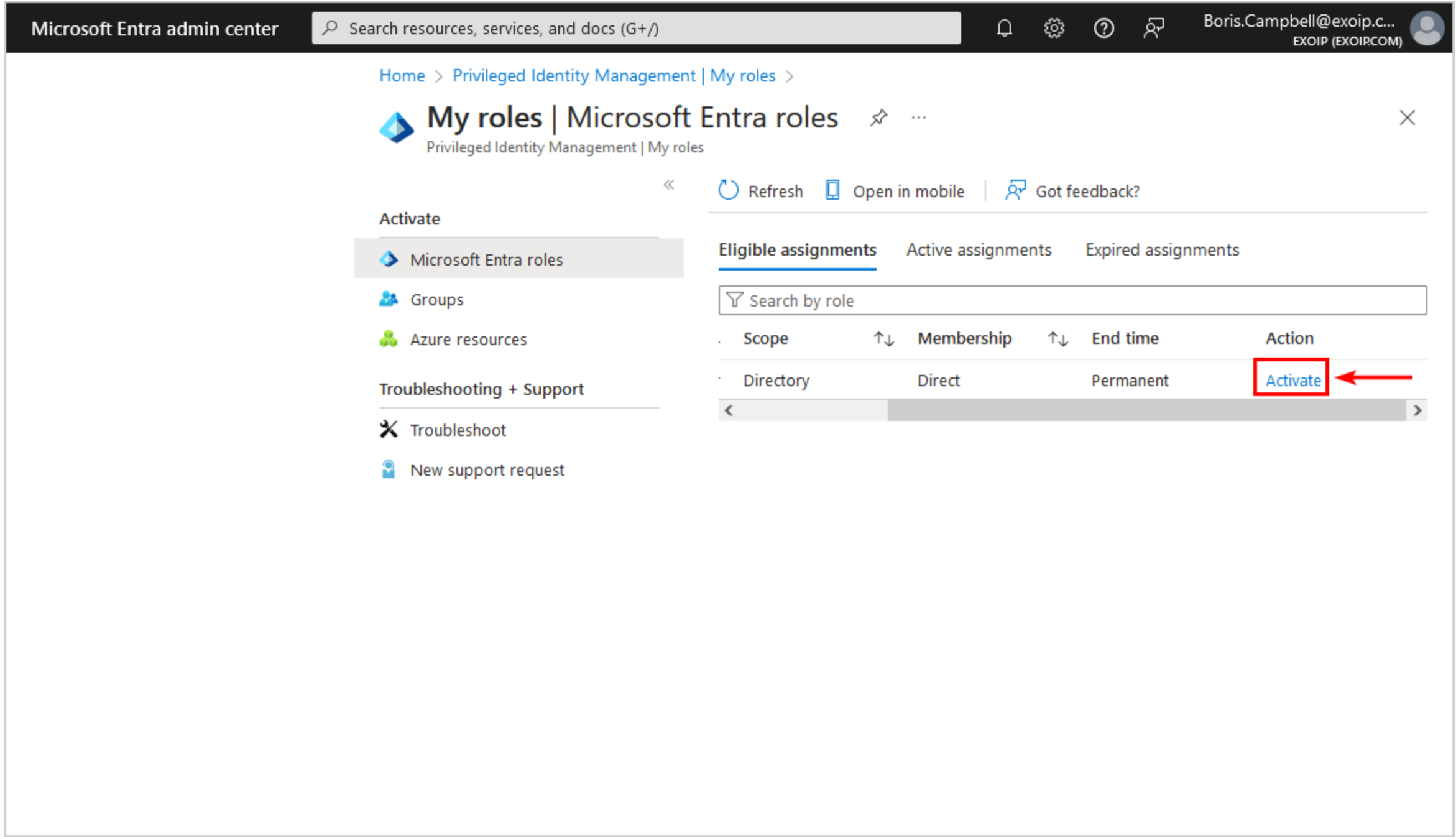
Type	Default recipients
Role activation alert	Admin
Notification to activated user (requestor)	Requestor
Request to approve an activation	Approver

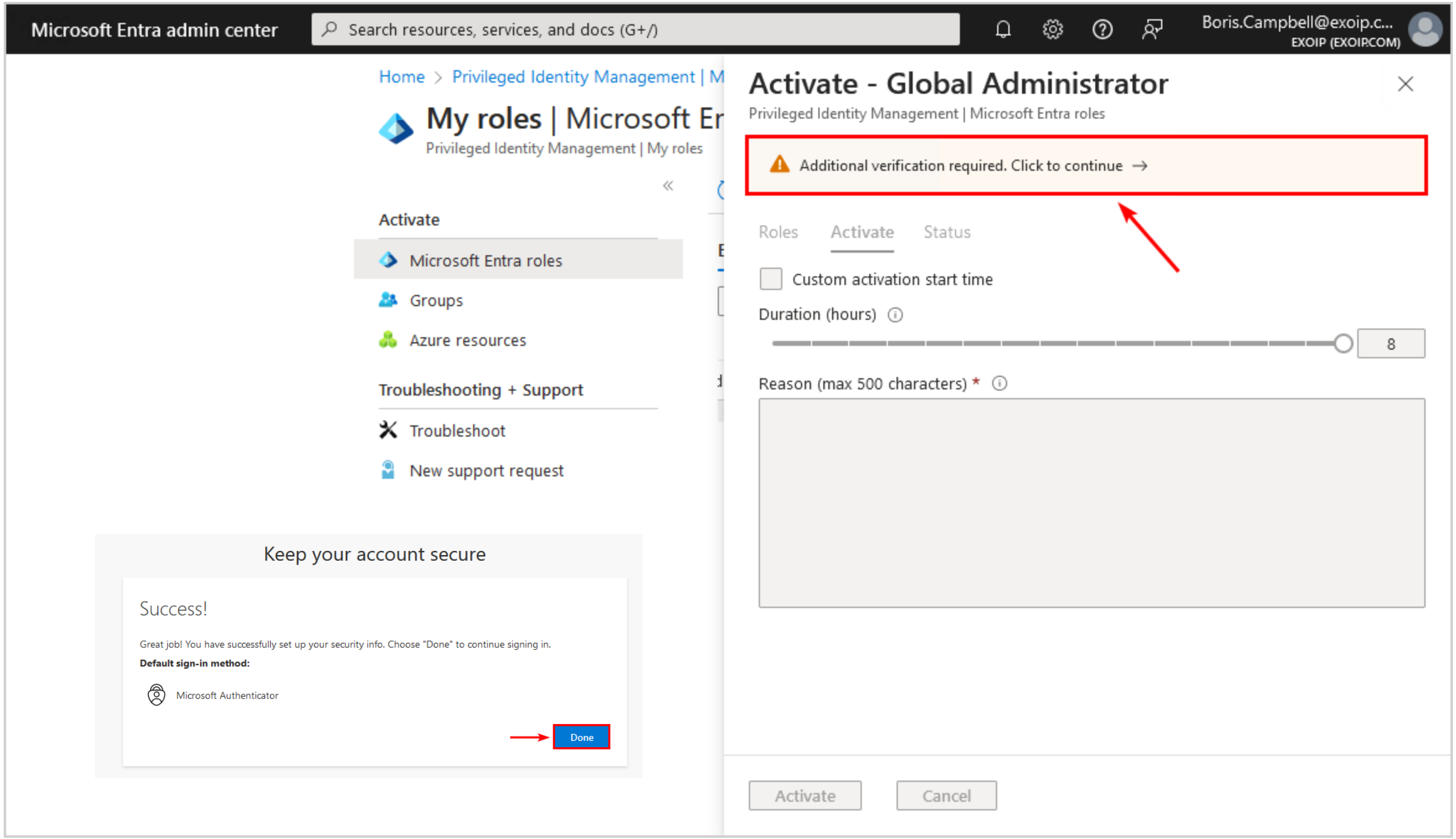
Eligible role example

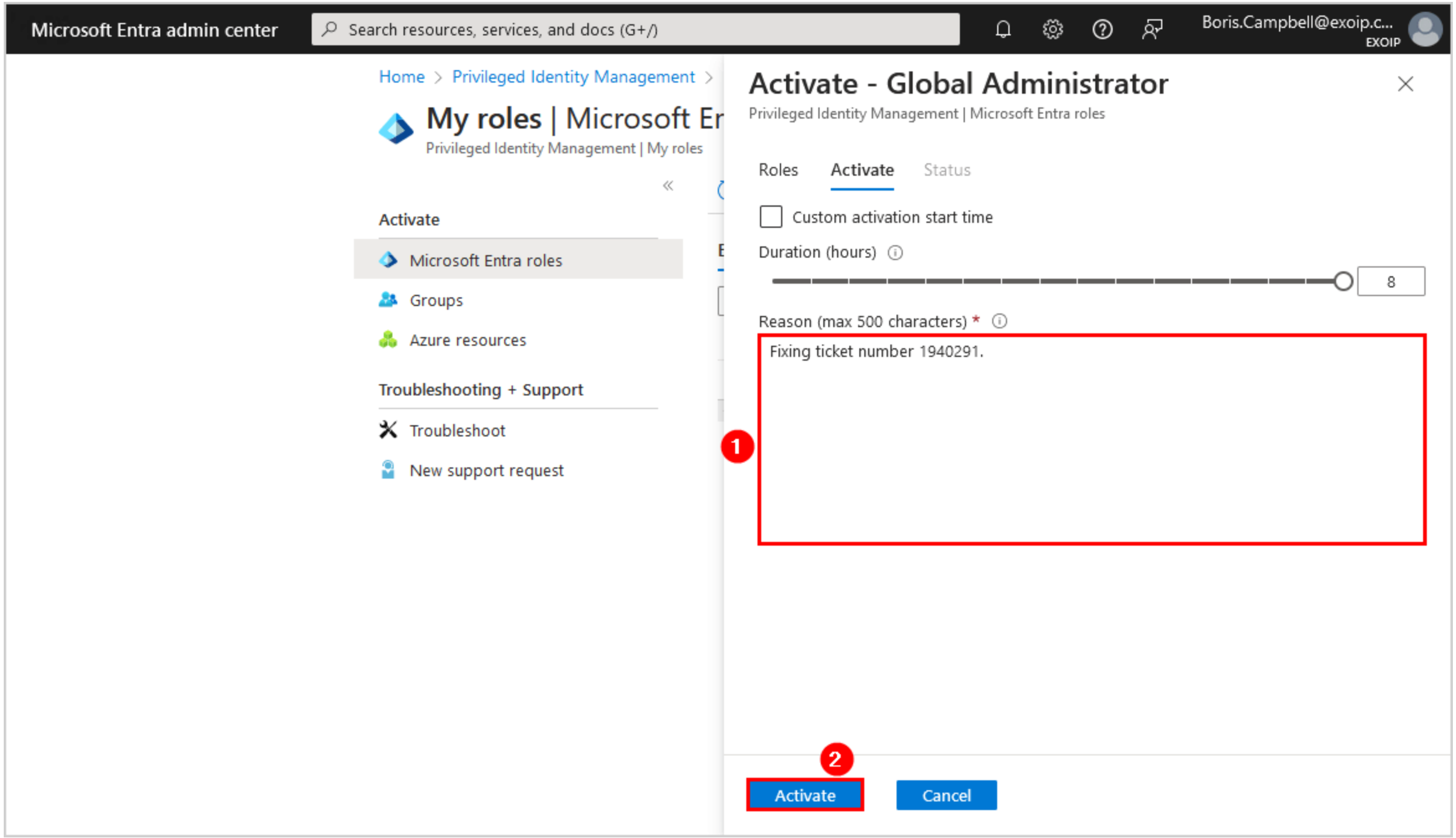


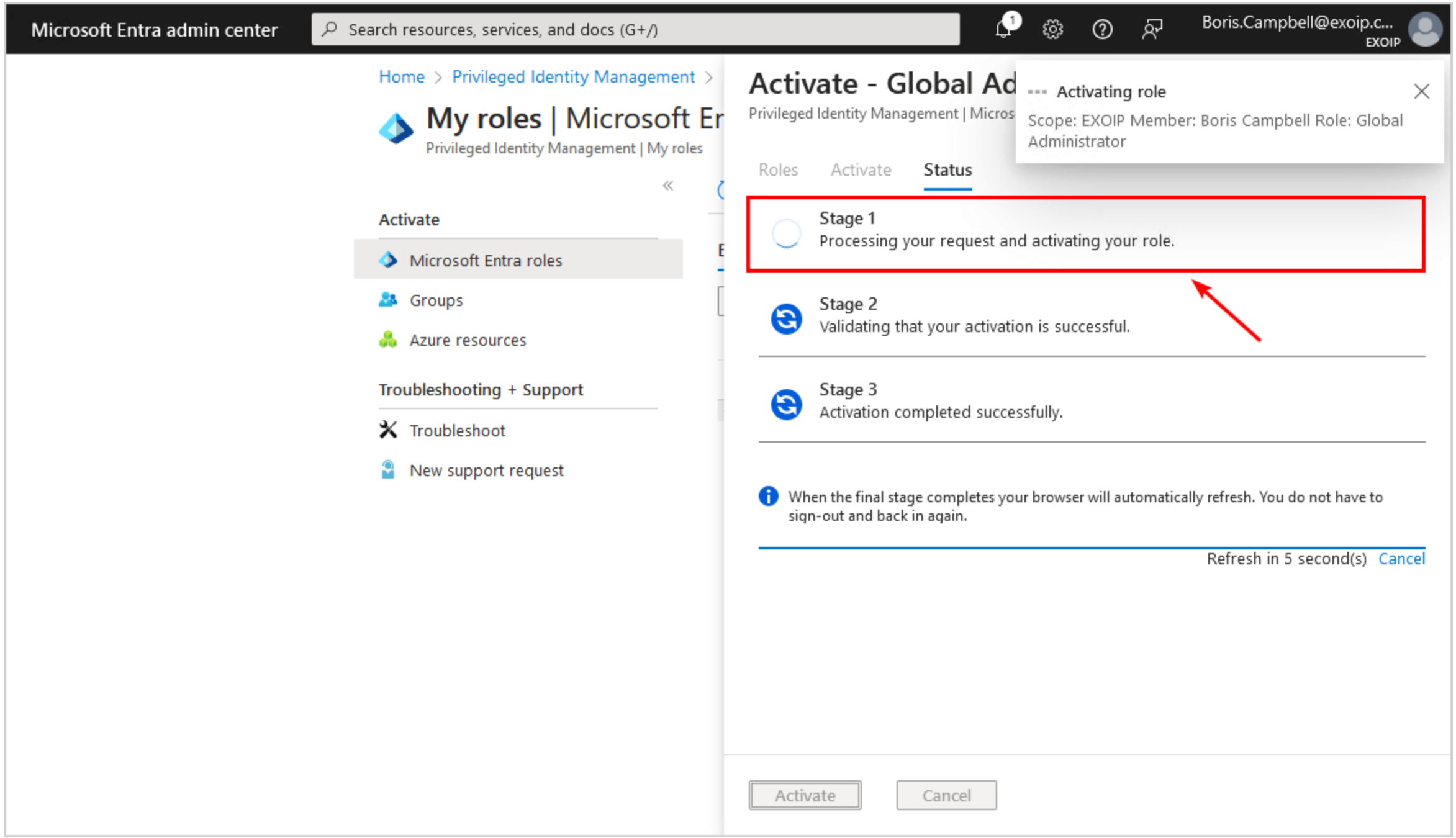
Activate eligible role example

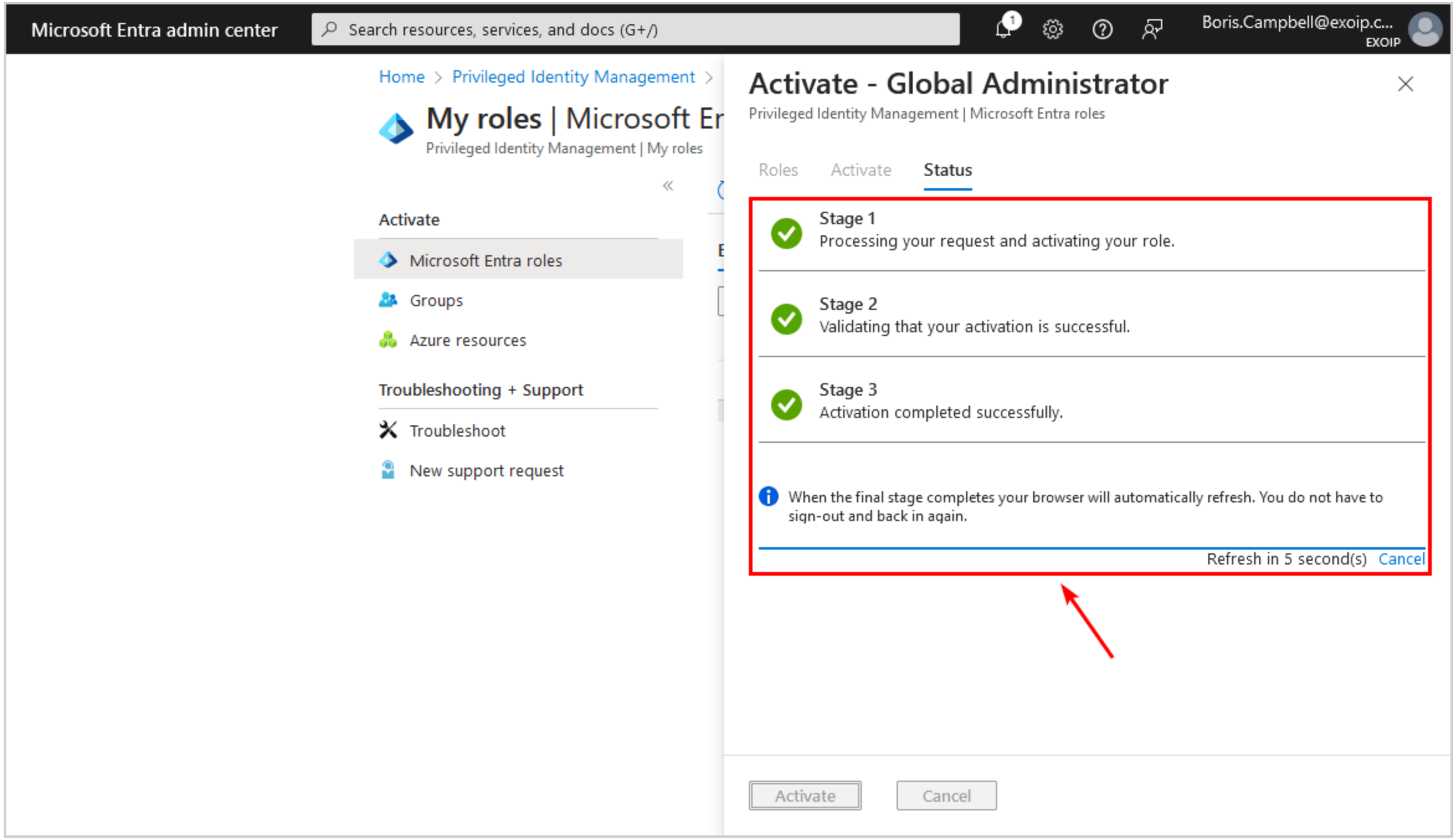


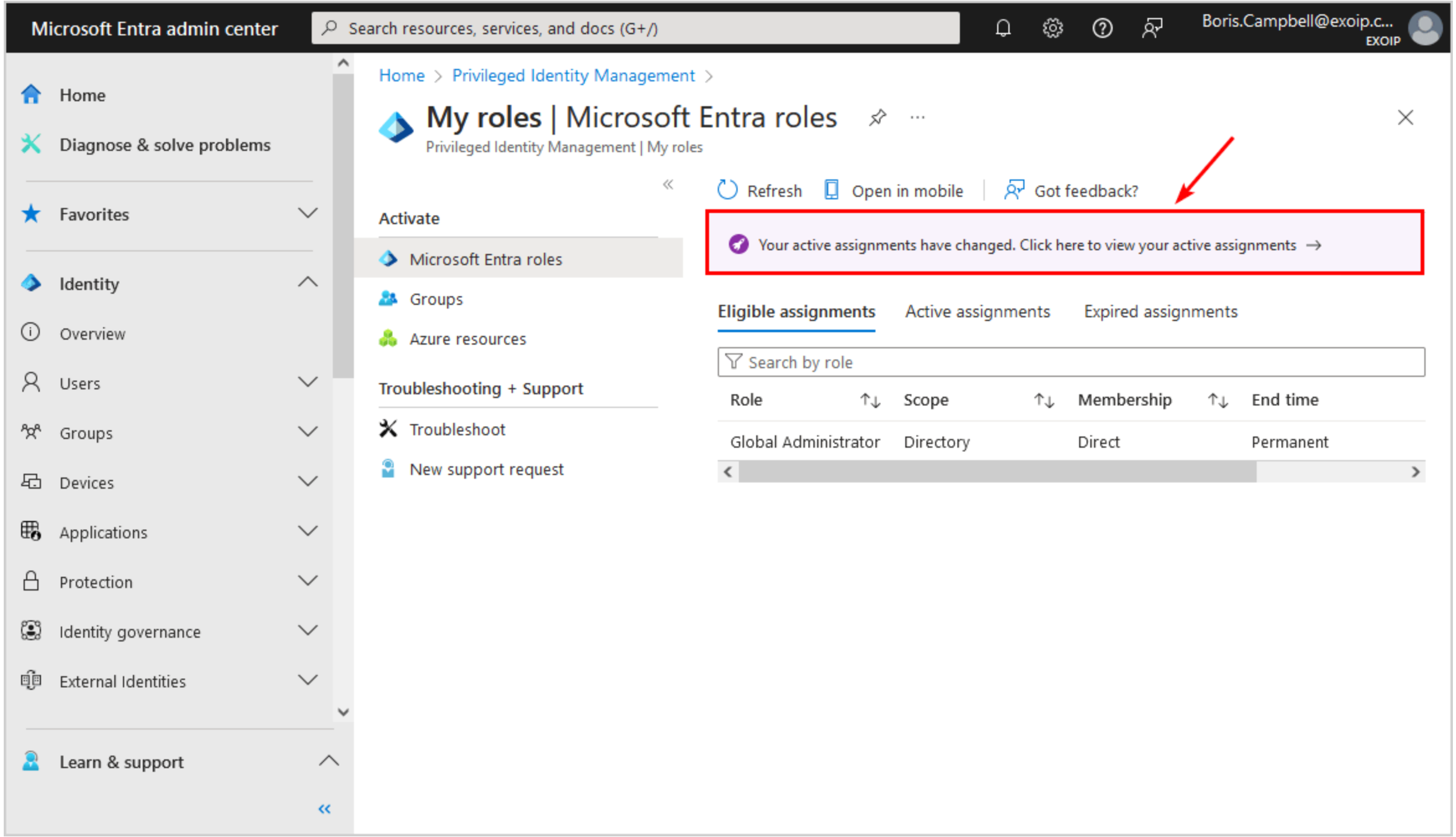

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Boris.Campbell@exoip.c...
EXOIP (EXOIP.COM)
Home > Privileged Identity Management | My roles >
My roles | Microsoft Entra roles
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Refresh
Open in mobile
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by role
Scope
Membership
End time
Action
Directory
Direct
Permanent
Activate

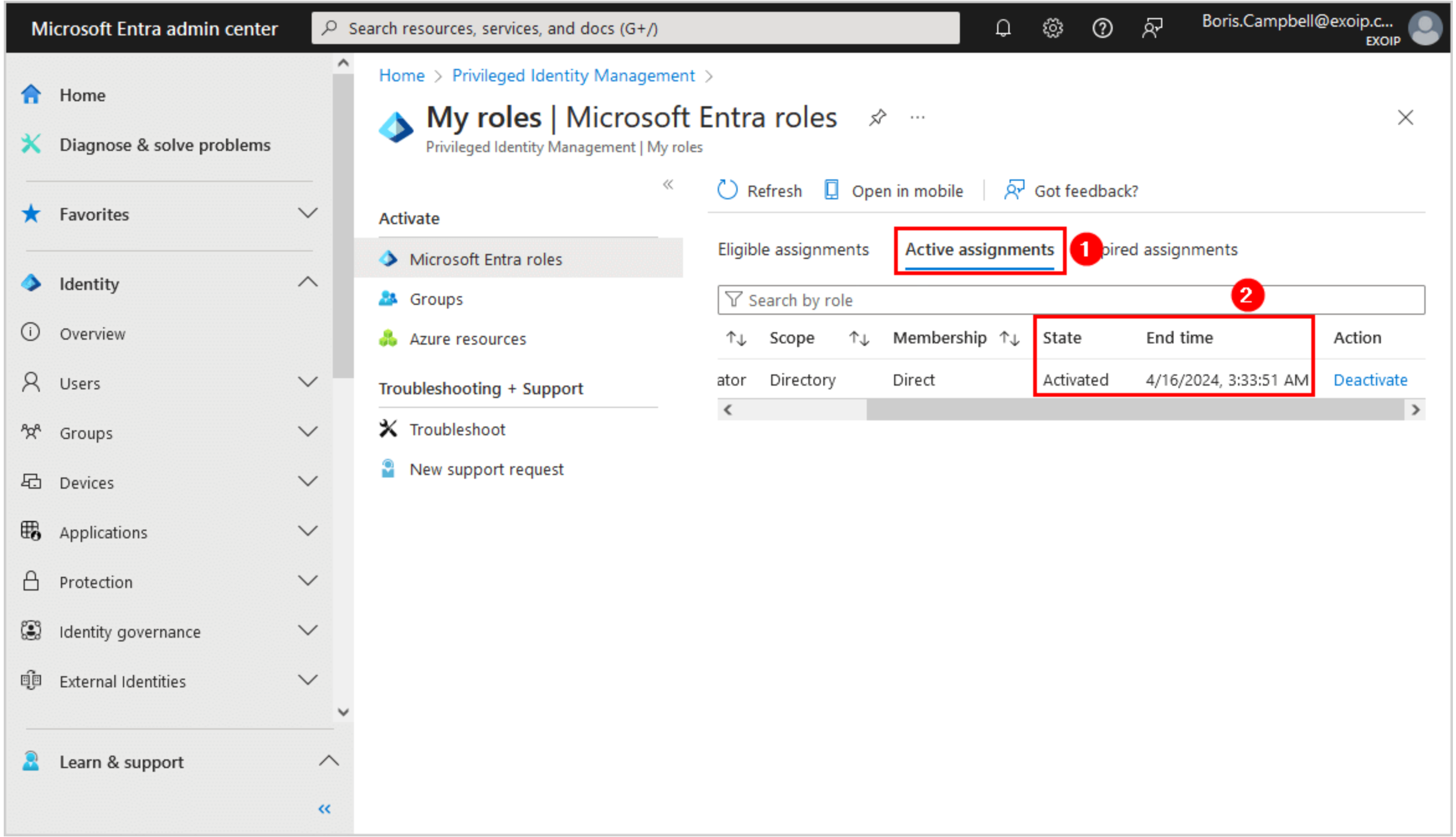

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Boris.Campbell@exoip.c...
EXOIP (EXOIP.COM)
Home > Privileged Identity Management | M
My roles | Microsoft Er
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Keep your account secure
Success!
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.
Default sign-in method:
Microsoft Authenticator
Done
Activate - Global Administrator
Privileged Identity Management | Microsoft Entra roles
Additional verification required. Click to continue
Roles
Activate
Status
Custom activation start time
Duration (hours)
8
Reason (max 500 characters) *
Activate
Cancel


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Boris.Campbell@exoip.c...
EXOIP
Home > Privileged Identity Management >
My roles | Microsoft Er
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Activate - Global Administrator
Privileged Identity Management | Microsoft Entra roles
Roles
Activate
Status
Custom activation start time
Duration (hours)
8
Reason (max 500 characters) *
Fixing ticket number 1940291.
1
2
Activate
Cancel

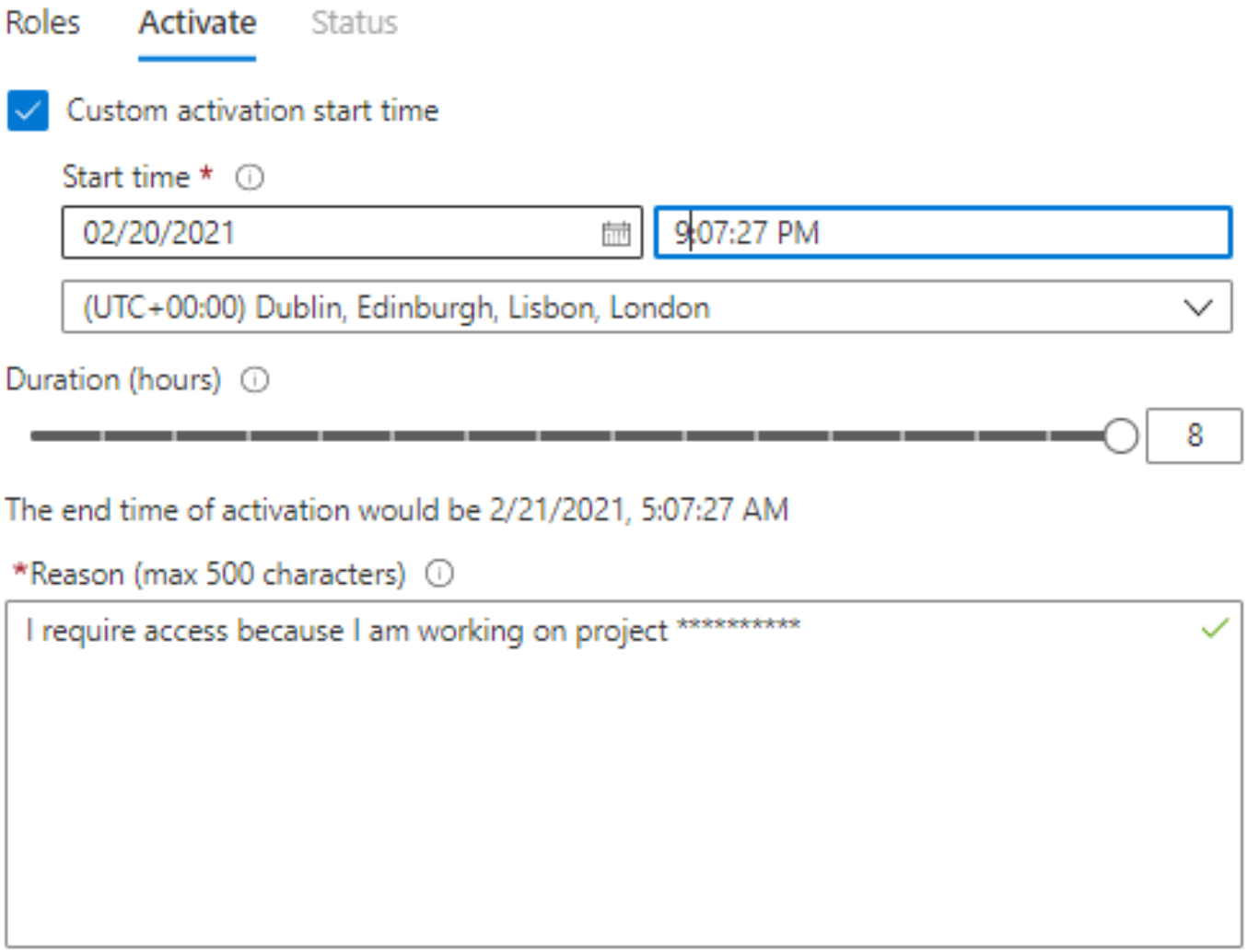

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Boris.Campbell@exoip.c...
EXOIP
Home > Privileged Identity Management >
My roles | Microsoft Er
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Activate - Global Ad
Privileged Identity Management | Micros
Activating role
Scope: EXOIP Member: Boris Campbell Role: Global Administrator
Roles
Activate
Status
Stage 1
Processing your request and activating your role.
Stage 2
Validating that your activation is successful.
Stage 3
Activation completed successfully.
When the final stage completes your browser will automatically refresh. You do not have to sign-out and back in again.
Refresh in 5 second(s) Cancel
Activate
Cancel


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Boris.Campbell@exoip.c...
EXOIP
Home > Privileged Identity Management >
My roles | Microsoft Er
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Activate - Global Administrator
Privileged Identity Management | Microsoft Entra roles
Roles
Activate
Status
Stage 1
Processing your request and activating your role.
Stage 2
Validating that your activation is successful.
Stage 3
Activation completed successfully.
When the final stage completes your browser will automatically refresh. You do not have to sign-out and back in again.
Refresh in 5 second(s) Cancel
Activate
Cancel


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Boris.Campbell@exoip.c...
EXOIP
Home
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity governance
External Identities
Learn & support
Home > Privileged Identity Management >
My roles | Microsoft Entra roles
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Refresh
Open in mobile
Got feedback?
Your active assignments have changed. Click here to view your active assignments →
Eligible assignments
Active assignments
Expired assignments
Search by role
Role
Scope
Membership
End time
Global Administrator
Directory
Direct
Permanent

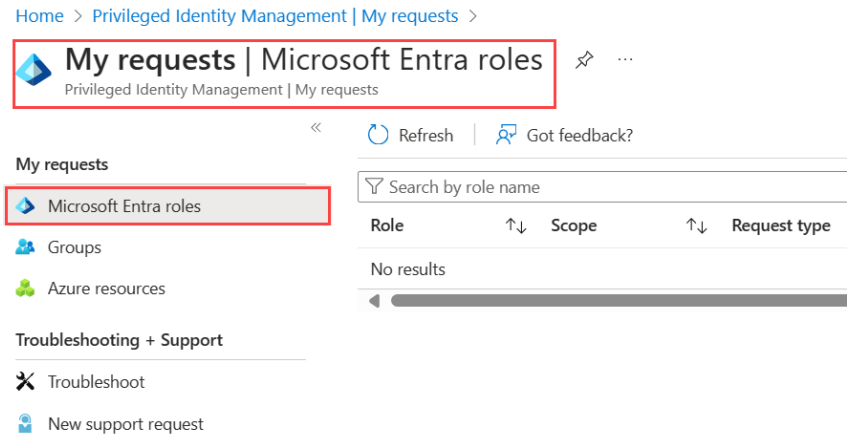

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Boris.Campbell@exoip.c...
EXOIP
Home
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity governance
External Identities
Learn & support
Home > Privileged Identity Management >
My roles | Microsoft Entra roles
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Refresh
Open in mobile
Got feedback?
Eligible assignments
Active assignments
1
pired assignments
Search by role
2
Scope
Membership
State
End time
Action
ator
Directory
Direct
Activated
4/16/2024, 3:33:51 AM
Deactivate

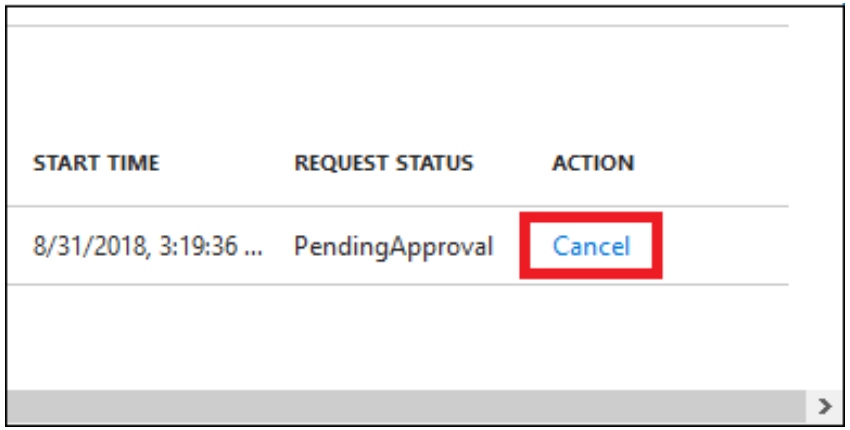
Custom activation time



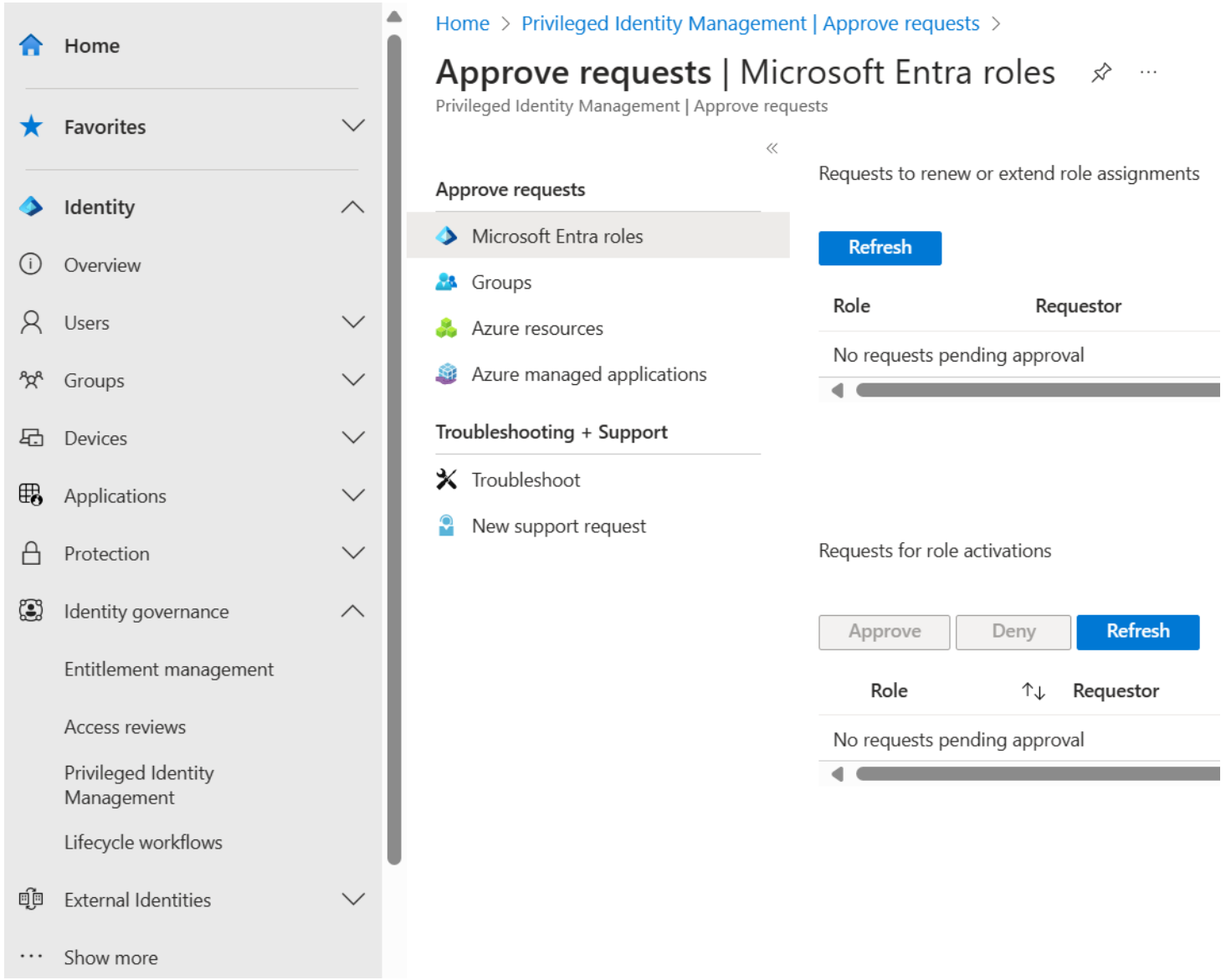
PIM activation approval

- If a role requires approval, an email will be sent to the approver to Approve or Deny
- You can cancel a request by clicking on the Cancel action in “My requests”





Approve requests



Access reviews

Access Reviews in PIM allow organizations to **regularly review and validate** who has privileged roles (like Global Administrator or Security Administrator) in Azure AD and other Microsoft services.

Key Features:

- **Automated Reviews**: Schedule recurring reviews of role assignments.
- **Reviewer Assignment**: Assign reviewers (e.g., managers or role owners) to approve or deny continued access.
- **Recommendations**: Microsoft can suggest actions based on user activity (e.g., remove access if not used).
- **Audit Trail**: All decisions are logged for compliance and auditing.

Why Use It?

- **Enhance security** by ensuring only the right people have privileged access.
- **Meet compliance** requirements for access governance.
- **Reduce standing access** by encouraging just-in-time (JIT) role activation.

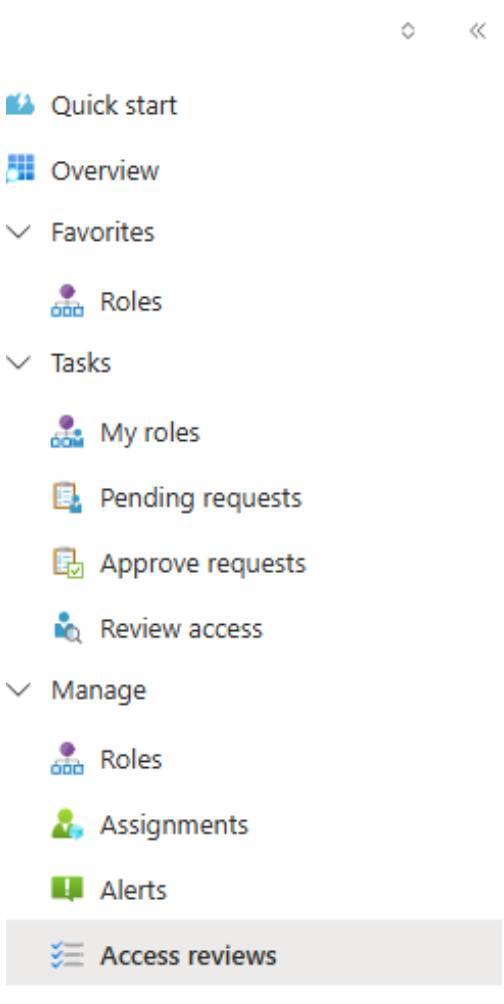
Access review steps

- **Scheduling** – Set up recurring or one-time access reviews.
- **Reviewer Assignment** – Assign users (e.g., managers or role owners) to review access.
- **Review Process** – Reviewers evaluate whether access should be continued.
- **Decision Making** – Approve or deny access based on necessity and usage.
- **Audit Logging** – All actions are logged for compliance and reporting.

Example

Australian Catholic University | Access reviews

Privileged Identity Management | Microsoft Entra roles



New Filter Group Settings

Access reviews for Microsoft Entra ID directory roles

Search by name or owner

Role	Owner	Start Date
Other role review cycle		
Cloud Application Administrator	Mark Laffan Admin Mark.Laffan.Admin@myacu.onmicrosoft.com	11/16/2022
Directory Readers	Mark Laffan Admin Mark.Laffan.Admin@myacu.onmicrosoft.com	11/16/2022
Global Reader	Mark Laffan Admin Mark.Laffan.Admin@myacu.onmicrosoft.com	11/16/2022
Global Administrator	Mark Laffan Admin Mark.Laffan.Admin@myacu.onmicrosoft.com	11/16/2022
Exchange Administrator	Mark Laffan Admin Mark.Laffan.Admin@myacu.onmicrosoft.com	11/16/2022
Directory Writers	Mark Laffan Admin Mark.Laffan.Admin@myacu.onmicrosoft.com	11/16/2022
Exchange Recipient Administrator	Mark Laffan Admin Mark.Laffan.Admin@myacu.onmicrosoft.com	11/16/2022
Application Administrator	Mark Laffan Admin	11/16/2022

Tips & Tricks

- Use the “extend” option if updating soon to expire roles
  - Adding the role again will just fail

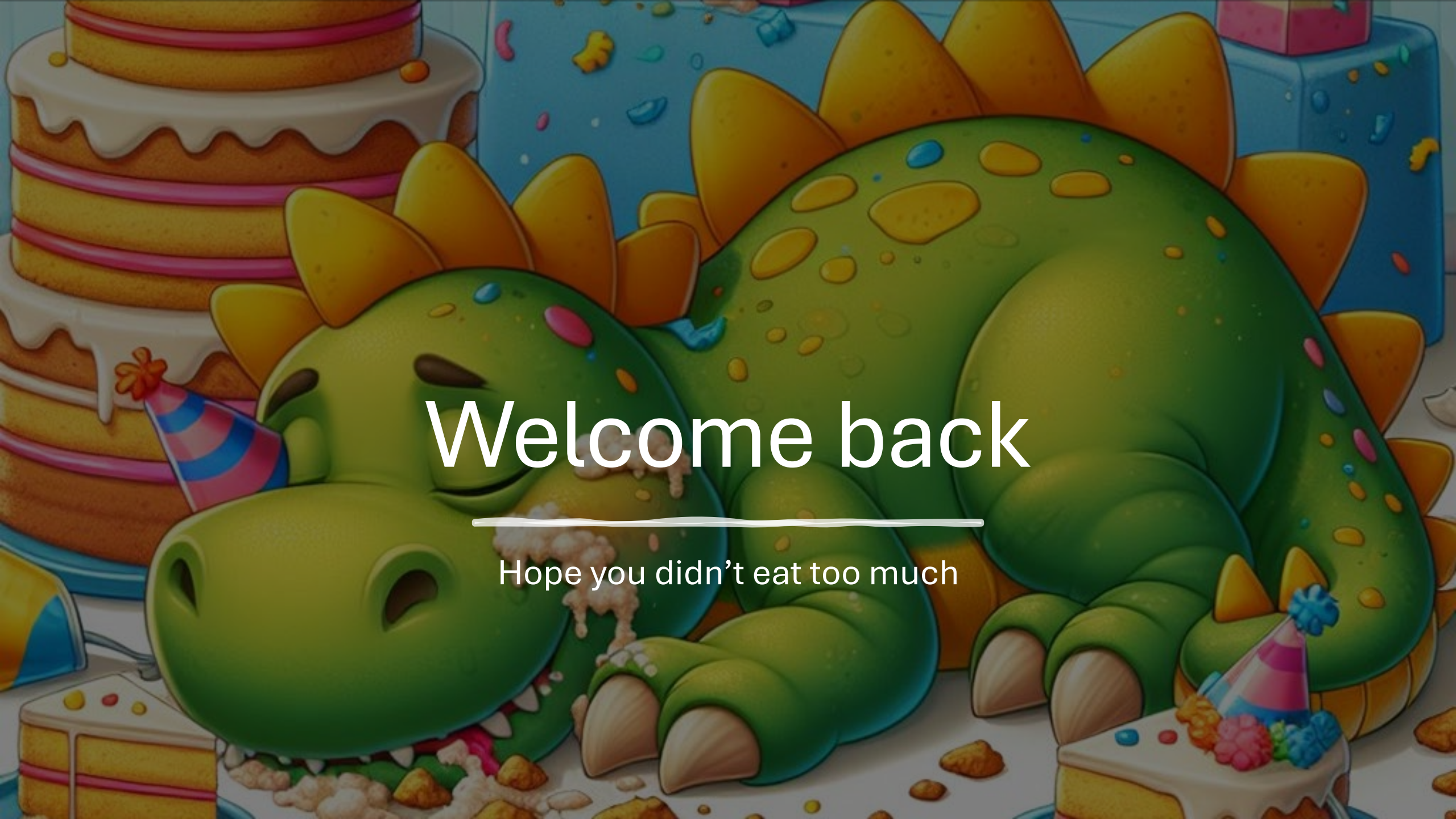
Teams Administrator	M	Directory	Direct	Active	10/14/2024, 12:27:00 PM	10/14/2025, 12:27:01 PM	Remove | Update Extend
Skype for Business Administrator	M	Directory	Direct	Active	10/14/2024, 12:28:36 PM	10/14/2025, 12:28:40 PM	Remove | Update Extend

- Fun fact, for some reason 6 months = 179 Microsoft days,
  If you set a 6-month end date you might get some strange results
- Ensure that MFA/SSPR is enrolled before assigning roles to accounts!
- Don’t forget to add Admin units to “scope” when assigning, you can’t edit it later!

Role	P..	Scope	Membership	Start time	End time	Action
Authentication Administrator	M.	All Students (Administrative unit)	Direct	7/30/2024, 11:43:23 AM	7/30/2025, 11:41:06 AM	Remove | Update | Extend

Questions? & Morning teatime!

Back at 11am!


Welcome back
Hope you didn’t eat too much

Agenda

Azure automation/powershell

- Azure automation
- Powershell
- Playbooks
- Tips & Tricks

Security Optimization Assessment

- SOA – an introduction
- Collection script
- Example output

Exchange Online Protection

- ACU history
- Settings you should consider
- Tips & Tricks

Phishing simulations

- Tips and tricks
- Examples
- Questions?

Azure Automation/PowerShell

- Using Azure Automation
- Creating playbooks
- Tips & Tricks

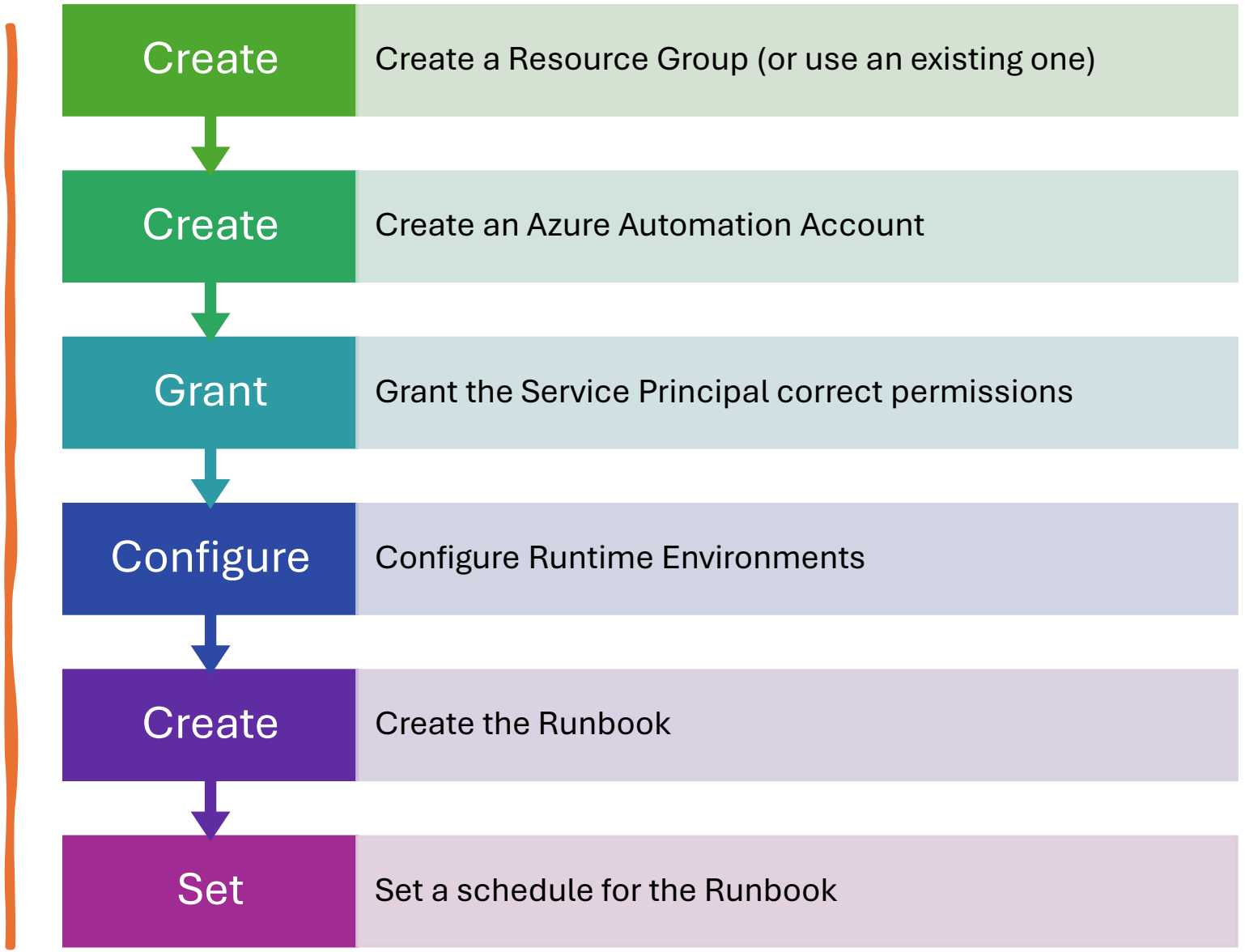
What is Azure Automation and what are Runbooks (a co-pilot response)

Azure Automation is a cloud-based service provided by Microsoft Azure that helps you automate repetitive tasks, manage configurations, and orchestrate processes across Azure and non-Azure environments.

Runbooks in Azure Automation are scripts or workflows that automate tasks and can be written in PowerShell, Python, or created using a graphical interface.

Runbooks can be triggered manually, scheduled to run at specific times, or initiated through webhooks or alerts.

Steps required to run PowerShell in Azure Automation



1. Create a Resource Group

There are multiple ways to create an Azure Resource Group, but the simplest are via the Azure Portal (GUI) or PowerShell.

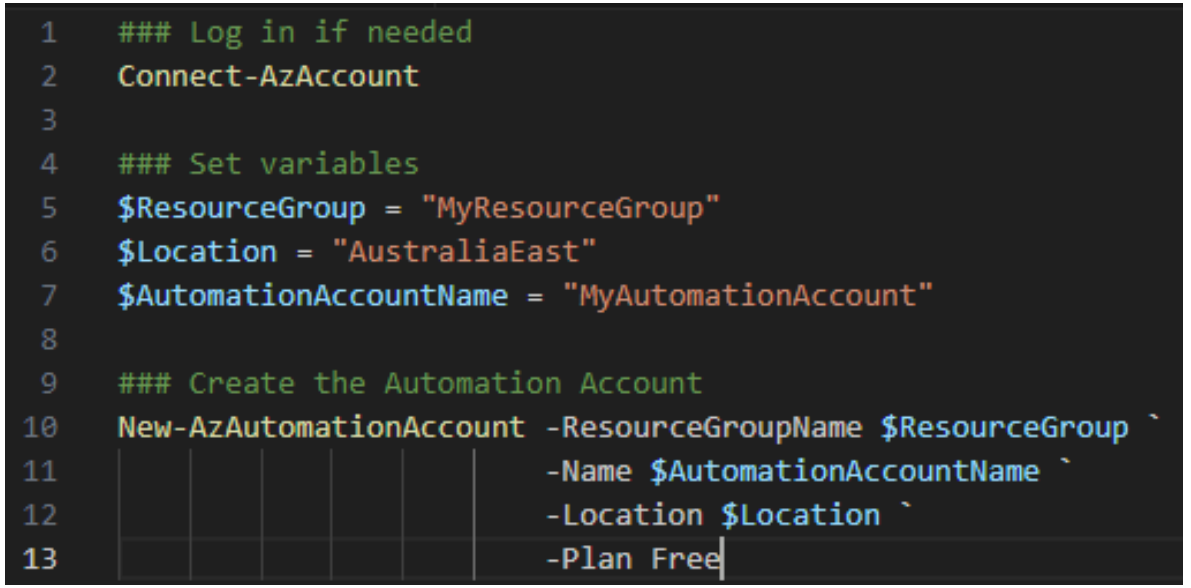
1. Azure Portal (GUI)
    1. Go to https://portal.azure.com
    2. In the search bar, type and select Resource groups.
    3. Click + Create.
    4. Fill in:
        - Subscription
        - Resource group name
        - Region (where the resources will be deployed)
    5. Click Review + Create > Create.
2. PowerShell →

```powershell
### Log in if needed
Connect-AzAccount

### Create a new resource group
New-AzResourceGroup -Name "MyResourceGroup" -Location "AustraliaEast"
```

2. Create an Azure Automation Account

Azure Automation Accounts can also be created via the Azure Portal (GUI) or PowerShell.

1. Go to the Azure Portal.
    1. Search for "Automation Accounts" in the top search bar and select it.
    2. Click + Create.
    3. Fill in the required fields:
        - Subscription
        - Resource Group (you can create a new one here if needed)
        - Automation Account Name
        - Region
        - Optionally enable System-assigned managed identity
    4. Click Review + create, then click Create.
2. PowerShell →



```powershell
### Log in if needed
Connect-AzAccount

### Set variables
$ResourceGroup = "MyResourceGroup"
$Location = "AustraliaEast"
$AutomationAccountName = "MyAutomationAccount"

### Create the Automation Account
New-AzAutomationAccount -ResourceGroupName $ResourceGroup `
                        -Name $AutomationAccountName `
                        -Location $Location `
                        -Plan Free
```

3. Grant the Service Principal correct permissions

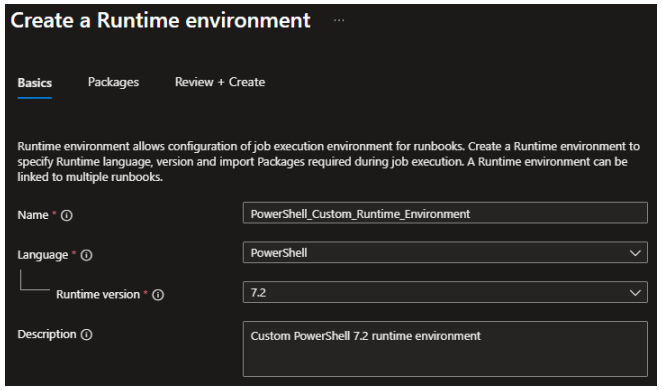
There are two ways of granting permissions to the Service Principal

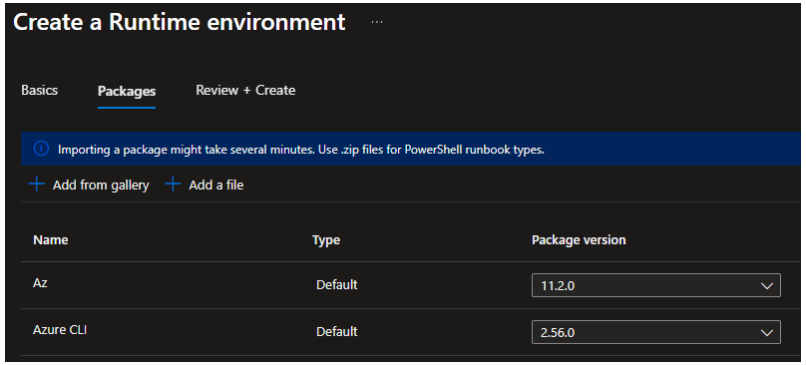
1. Assigning an Entra ID role via the portal
    1. Go to Microsoft Entra ID > Roles and administrators.
    2. In the search bar, type the name of a role (e.g., "Groups Administrator").
    3. Click the role, then go to Assignments.
    4. Search for your Automation Account listed as a Managed Identity.
2. Using PowerShell to enable individual permissions

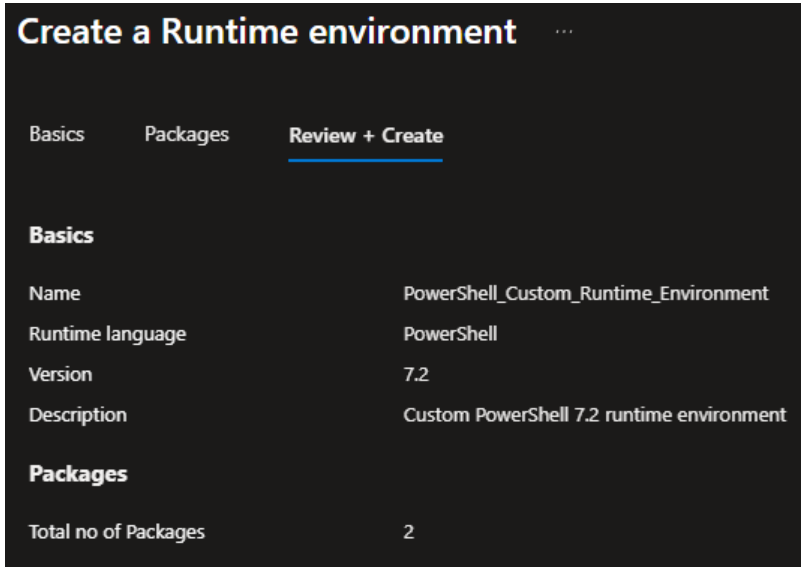
```powershell
### Connect to MS Graph
Connect-MgGraph -Scopes "Directory.ReadWrite.All", "AppRoleAssignment.ReadWrite.All"

### List Required Permissions for Entra
$EntraPermissions = @(
    "Directory.ReadWrite.All"
    "Group.ReadWrite.All"
    "User.ReadWrite.All"
)

### List Required Permissions for Exchange
$ExchangePermissions = @(
    "Exchange.ManageAsApp"
)

### Get the MS Graph Service Principal
$EntraGraphApp = Get-MgServicePrincipal -Filter "AppId eq '00000003-0000-0000-c000-000000000000'"

### Get the MS Exchange Service Principal
$ExchangeGraphApp = Get-MgServicePrincipal -Filter "AppId eq '00000002-0000-0ff1-ce00-000000000000'"

### Get the Automation Account Service Principal ID
$SPID = (Get-MgServicePrincipal -Filter "displayName eq 'aaacuitinfosecautomation'").id

### Get the MS Entra Graph and Exchange Role IDs, then combine into a single array
[array]$EntraRoles = $EntraGraphApp.AppRoles | Where-Object {$EntraPermissions -contains $_.Value}
[array]$ExchangeRoles = $ExchangeGraphApp.AppRoles | Where-Object {$ExchangePermissions -contains $_.Value}
$Roles = $EntraRoles + $ExchangeRoles

### Assign each permission
foreach($Role in $Roles){
    $AppRoleAssignment = @{
        "PrincipalId" = $SPID
        "ResourceId" =  if ($EntraRoles.Id -contains $Role.Id) {$EntraGraphApp.Id}
                        elseif($ExchangeRoles.Id -contains $Role.Id) {$ExchangeGraphApp.Id}
                        else {""}
        "AppRoleId" =   $Role.Id
    }

    ### Assign the Graph permission
    New-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $SPID -BodyParameter $AppRoleAssignment
}
```

4. Configure Runtime Environments

- Runtime environments can be found in Azure Automation under Process Automation → Runtime Environments
- With the current Runtime Environments(preview) there are system-generated runtime environments for PowerShell versions 5.1, 7.1 and 7.2 with commonly used modules. However, you can't make any changes.
- If you need modules not included in the above, you can create a custom runtime environment.



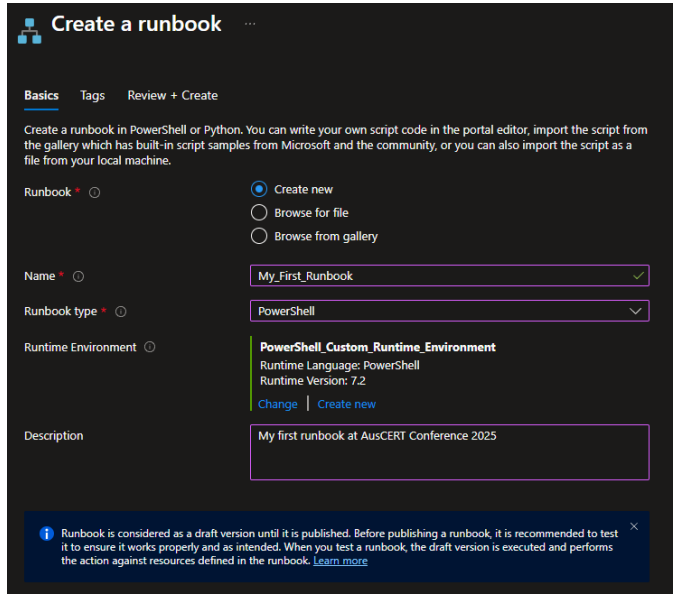


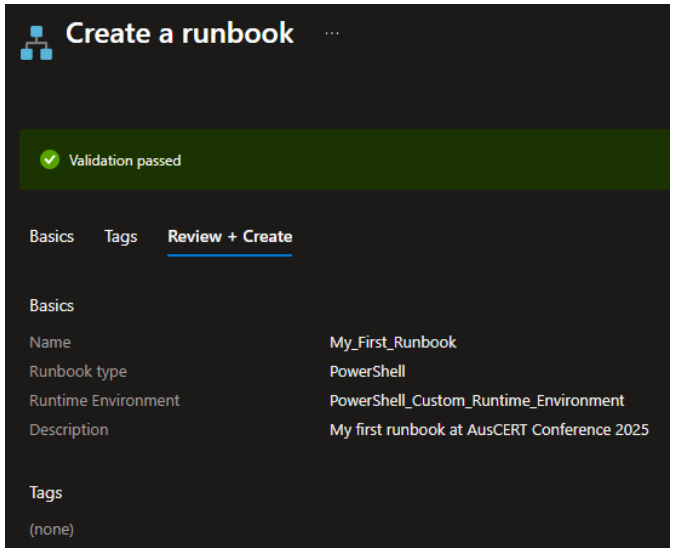


5. Create the Runbook

- Runbooks can be found in Azure Automation under Process Automation → Runbooks
- Here we can see existing runbooks or create a new one using the custom runtime environment just created.
- Once the runbook is created, we can now add our code. Remember to connect to Microsoft Graph using the Managed Identity.

```
### CONNECT TO MICROSOFT GRAPH WITH MANAGED IDENTITY ###
Connect-MgGraph -Identity
```





6. Set a schedule for the Runbook

1. Azure Portal (GUI)
    1. From your Automation account, on the left-hand pane select Schedules under Shared Resources.
    2. On the Schedules page, select Add a schedule.
    3. On the New schedule page, enter a name and optionally enter a description for the new schedule.
    4. Select whether the schedule runs once or on a reoccurring schedule by selecting Once or Recurring.
        1. If you select Week, the days of the week are presented for you to choose from.
        2. If you select Month, you're given different options. For the Monthly occurrences option, select either Month days or Week days.
    5. When you're finished, select Create.
2. PowerShell
    1. Depending on the frequency there are multiple scripts/commands to use. Microsoft list them here: [Manage schedules in Azure Automation | Microsoft Learn]

Azure Automation - key points to note

- Cost [1]
  - Job run time – 500 minutes free per month, then $0.004/minute ($0.24/hour)
  - Watchers – 744 hours free per month, then $0.004/hour
- Limits and Quotas [2]
  - Maximum runtime allowed per runbook – three hours
  - Maximum amount of memory given to a sandbox – 400 MB
  - Maximum runbook parameters – 50
  - Maximum number of runbooks per Automation account - 800

(1) Pricing - Automation | Microsoft Azure

(2) Azure Automation subscription limits and quotas | Microsoft Learn

Examples

SOA – EOP - Phishing simulation

- SOA – an introduction - what it is, what you get
- Do you do EOP? - settings you should consider
- Tips & Tricks for Phishing simulations

Microsoft's Security Optimization Assessment

These assessments and controls are part of Microsoft's proactive offerings to enhance security and compliance – Talk to your MS rep!

Microsoft 365 Foundations - Workload Security Assessment:

- Exchange Online
- SharePoint Online
- Microsoft Teams
- Power Apps admin
- Microsoft Graph Authentication

SOA cont.

Security Optimization Assessment for Microsoft Defender:

- DMARC Reporting
- MFA Report
- SharePoint Audit Logging
- Calendar Publishing Information
- Dataverse Auditing
- Delegates and Forwarding Rules
- Inactive Users Report
- M365 Role Report
- Mailbox OWA Storage Provider

SOA powershell collection script

- Runs as a privileged user
- Output is a bunch of JSON & Excel files
- You can read them (useful for dumping configuration & block/allow lists)
- .. but, if you have MS Maintenance hours?

Engage with your Microsoft Rep to produce a nice report and remediation activities!

- 4 day engagement
- O365 Findings report
- O365 Remediation planning
- O365 Knowledge transfer

https://github.com/o365soa

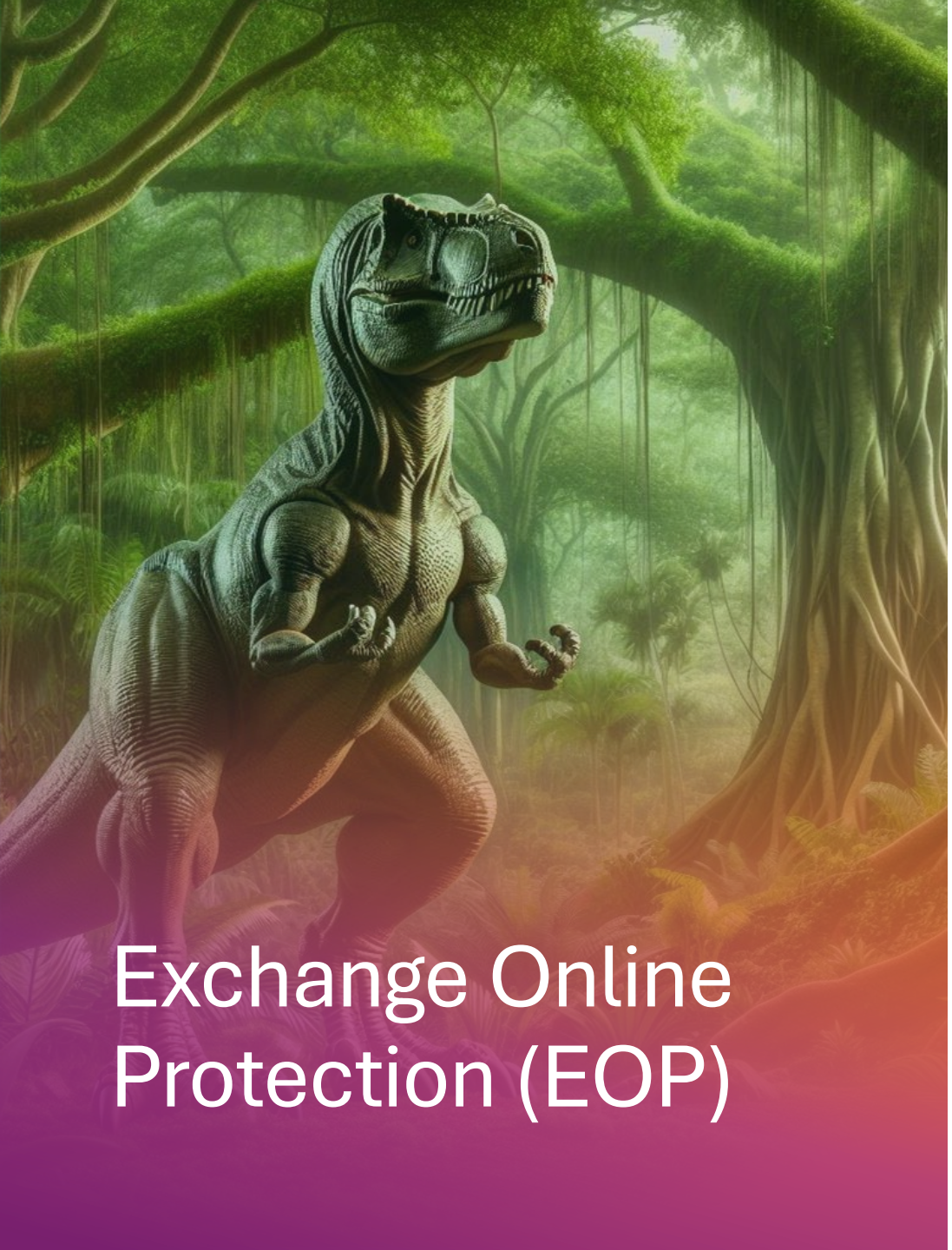
Remediation Planning Playbook example

	A	B	C	D	E	F	G	I	L	M	N
1	ID	Name	Function	Percent Pass	Qty. Pass	Qty. Fail	Qty. Total	Result	Cost	User Impact	Recommendation
2	SOA-100	Implement Sender Policy Framework (SPF)	Protect	20	4	16	20	Fail	Low	Low	Strongly Recommended
3	SOA-101	Enable mailbox auditing for all mailboxes	Respond	27	255	672	927	Fail	Low	Low	Strongly Recommended
4	SOA-102	All Global Administrators should have MFA	Protect	70	7	3	10	Fail	Low	Low	Strongly Recommended
5	SOA-103	Sender Policy Framework should be configured to hard fail	Protect	0	0	20	20	Fail	Low	Low	Strongly Recommended
6	SOA-105	Implement Domain-based Message Reporting and Conformance (DMARC) reporting	Detect	0	0	20	20	Fail	Moderate	Low	Strongly Recommended
7	SOA-106	Develop or improve end-user security training program	Protect	0	0	1	1	Fail	Moderate	Low	Strongly Recommended
8	SOA-107	Implement DMARC policy action	Protect	0	0	20	20	Fail	Low	Low	Strongly Recommended
9	SOA-108	Configure DKIM signing for custom domains	Protect	0	0	20	20	Fail	Low	Low	Strongly Recommended
10	SOA-109	The number of Global Administrators should be reduced	Protect	50	5	5	10	Fail	Low	Moderate	Recommended

Detailed Findings Report example

Implement Domain-based Message Reporting and Conformance (DMARC) reporting	
Change strongly recommended	
Control ID	SOA-105
User Impact	Low
Implementation Cost	Low to Moderate (Depending on method)
Threats	Phishing, Spoofing
Description	Email by itself has no mechanisms of detecting and reporting on legitimate or illegitimate use of your email domains when sending to third parties. By implementing a DMARC record, with an aggregate and/or forensic reporting address, third-party email servers have a reporting loop to send information to you about use of your email domains, either legitimately, or illegitimately. The DMARC reports are sent to an email address in an XML format and are not easily read. Using a third-party parsing service, or a parsing script can provide you with easy to use reports. DMARC reports will enable your organisation to further improve your sender authentication records. DMARC reports will show you legitimate uses, e.g., if you are using third parties to send on your behalf but will also show you illegitimate uses. Enhance your Sender Authentication records after setting up DMARC reporting, by either adding or removing support for third-party senders based on the reporting information provided.

Affected Objects	Your organisation has **not implemented DMARC reporting any domain.**
Remediation Change	It is recommended, for the least amount of effort, to utilise a third-party DMARC parsing service. The process of implementing DMARC reporting using a third-party service depends on the service provider, but usually involves the following: • Signing up to the service • Receiving an email address for the service provider • Setting up your DMARC rua addresses to point to the service provider Sometimes, the cost of the third-party service prohibits DMARC reporting. In these cases, there are several parsing scripts available. The Office 365 Security Optimisation Assessment team has provided one example script which can be used for low volume parsing. It is provided without support or warranty, and is available here: https://github.com/o365soa/Scripts/tree/master/DMARC%20Reporting
Remediation Impact	No impact
Cybersecurity Function	Detect
Additional Information	DMARC Official Website https://dmarc.org/ Use DMARC to validate email in Office 365 https://docs.microsoft.com/en-us/office365/SecurityCompliance/use-dmarc-to-validate-email



Exchange Online Protection (EOP)

ACU History:

- Removed messagelabs (Symantec) in 2019 to EOP/ATP
  - Engaged with MS fast track to migrate configuration (block and allow lists)
  - Enabled protection like Impersonation controls, configuration Sanity check etc
  - Knowledge transfer from Microsoft
- Reviewed SOP settings in 2022 – via SOA
- Migrated students into staff tenant – EOY 2022
- Remediation project for SOA findings started in 2023
- Increased Anti-phishing controls in 2024
- Used Phishing simulations for all staff in 2024

EOP settings to consider

First contact safety tip
On

User impersonation safety tip
On

Domain impersonation safety tip
On

Unusual characters safety tip
On

Unauthenticated senders symbol (?) for spoof
On

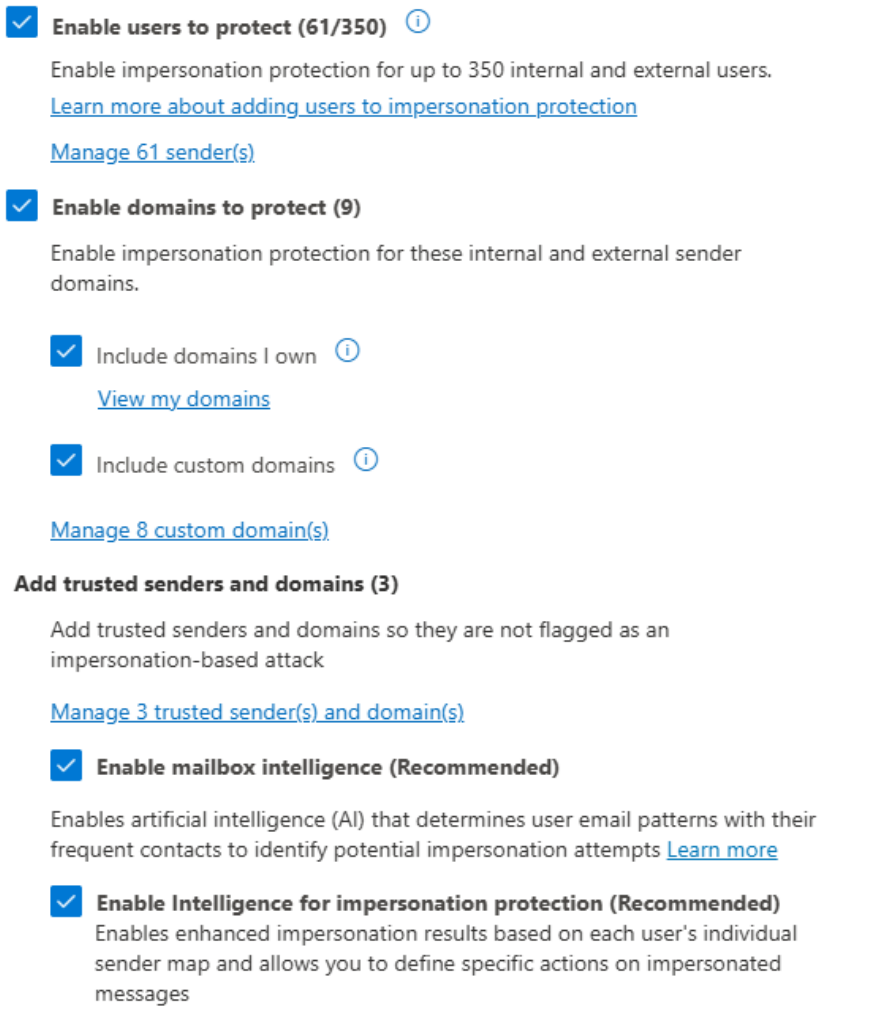
- **Enable** DKIM signing
- **Enable** all header warnings
- Add a “external” email banner – mail flow rule
- Turn up anti-phishing settings to Max (4)
  - Move impersonations and all others to quarantine
  - Enable mailbox intelligence!
- Don’t give users access to quarantine box (personal preference)
  - If you must, consider read only, no release request!
- Stop using mail flow rules to block/allow emails!
  - Tenant Allow/Deny list must be used instead
  - Allow/deny items can be made to expire

Phishing email threshold

4 - Most Aggressive

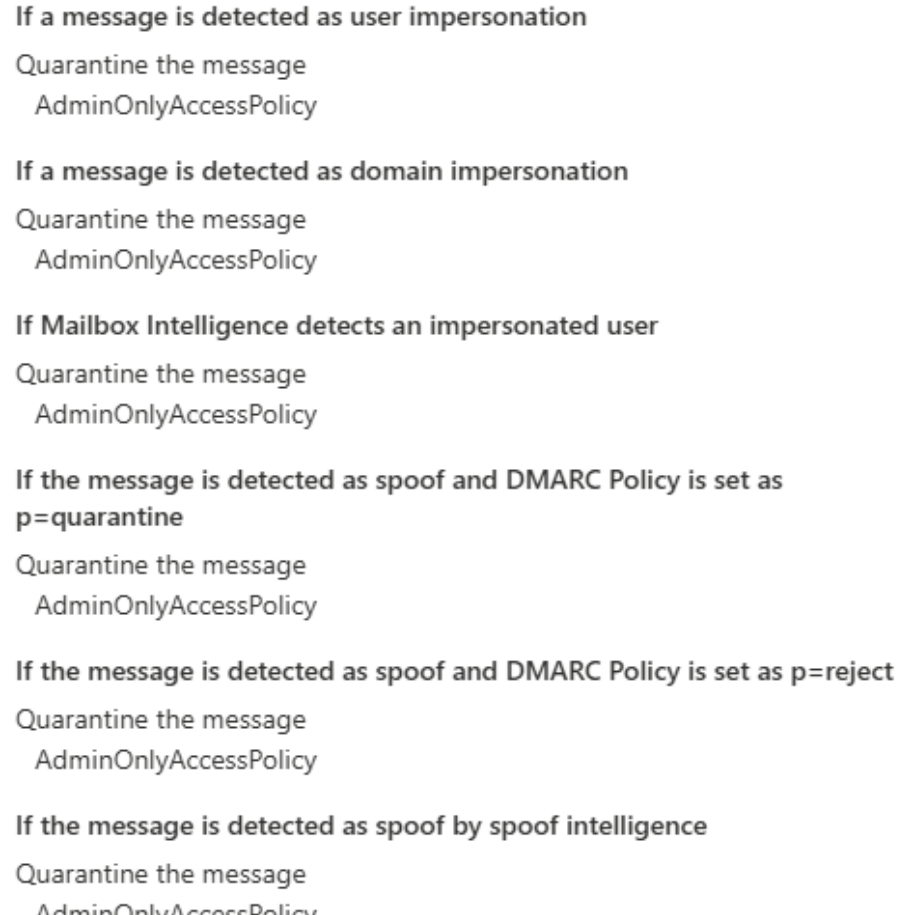
Messages that are identified as phishing with a low, medium, or high degree of confidence are treated as if they were identified with a very high degree of confidence.

EOP tips & tricks



Anti-Phishing settings

- Add VIP’s to Impersonation list (Max 350)
- Review impersonation insights
- Quarantine everything



Phishing simulation tips & tricks

- Don’t use DL’s or groups – export accounts to CSV and import them into the campaign
- Once you start a campaign you can’t stop it!
- You can’t delete delivered emails – will not appear in explorer
- You can’t change a campaign – web sites will be pulled down after the campaign ends
- You can create your own content –email, and landing pages
- Learn HTML (again) or use a WYSIWYG editor
- MS has a lot of pre-built training!
- Test, test, test, then test again
- Lots of reports, richer over time

November driveby - all staff

Completed Processing User Actions Social Engineering . Drive-by URL Delivery Platform : Email

Report Users Details

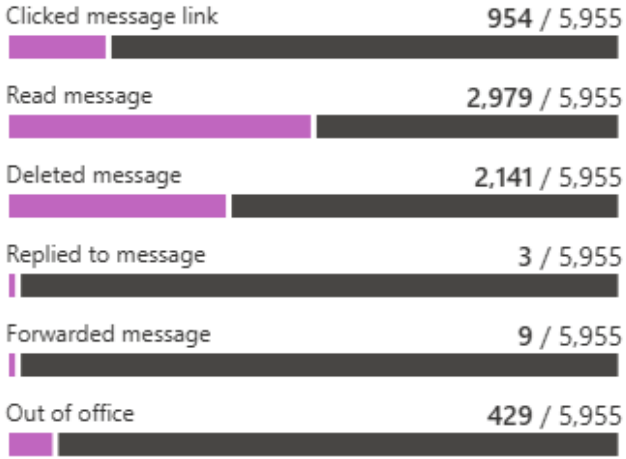
Simulation Impact

16.02% users were compromised & 7.74% users reported

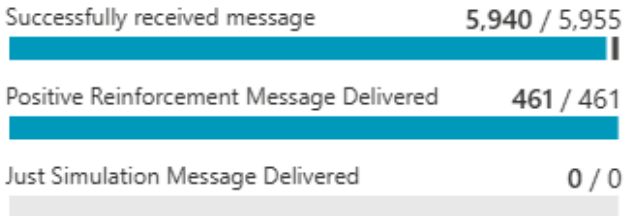
View compromised users

View users who reported

All user activity



Delivery Status



Training completion

Trainings were not part of this simulation

First & Average Instances

First Link Clicked
0h 0m 24s

Avg. Link Clicked
18h 38m 26s

First Message Reported
0h 0m 47s

Avg. Message Reported
8h 19m 11s

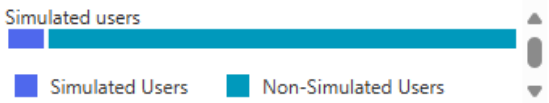
Attack simulation training

Learn more | What's New? | Share

Overview | Simulations | Training | **Reports** | Automations | Content library | Settings

Simulation coverage

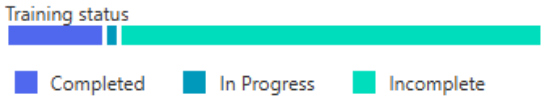
93% users have not experienced the simulation



View simulation coverage report

Training completion

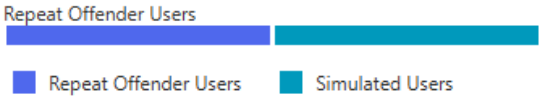
18% users have completed training



View training completion report

Repeat Offenders

119 user(s) are repeat offender



View repeat offender report

Behavior impact on compromise rate

884 users less susceptible to phishing

1% better than predicted rate

View simulations and training efficacy report

Training Efficacy | User Coverage | Training completion | **Repeat offenders**

Repeat Offender Users
119

Simulated users
6607

Export | Refresh

100 items | Search | Customiz

User	Simulation Types	Simulations	Email Address	Latest Repeat Count	Repeat Offences	Last Simulation Name	Last Simulation Result
Mark Laffan	CredentialHarvesting +5 more	test, sec team test, test 1 +17 more	Mark.Laffan@acu.edu.au	7	6	November driveby - all staff	Failed

Download documents here

https://github.com/markslaffan/Auscert2025

War stories and other questions…

And please provide Feedback?

Other useful stuff…

- Take the Security operations self-assessment tool

https://www.microsoft.com/en-au/security/business/threat-protection/security-operations-assessment