Adelaide Microsoft IT Pro Community

July Meetup

Zero Trust at the Edge

Managing Local Admin Access in Intune-Connected Devices

Brett Moffett

Chief Nerd / Director
at System@tech Solutions

Thursday, July 16, 2026
12:00 PM to 2:00 PM ACST
Microsoft Adelaide Office
Level 12, Aurora Building, 147 Pirie Street, Adelaide

Proudly Sponsored By:

SYSTEMATECH
IT CONSULTING

The Problem

Local administrator access remains one of the most exploited attack vectors in modern organisations.

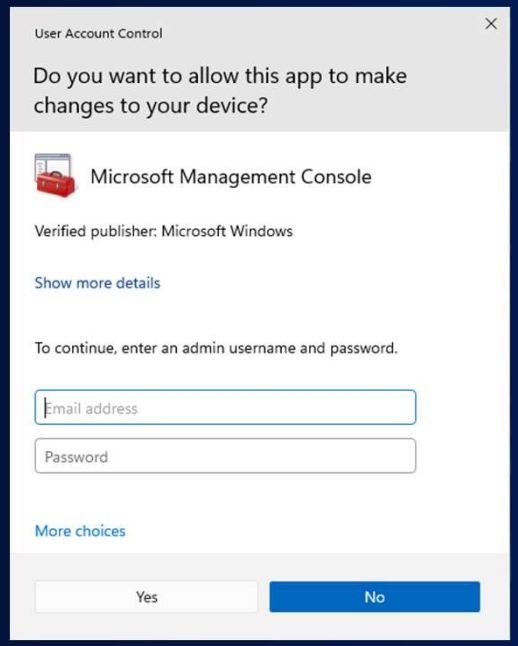
The Problem


User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: Windows Live
Verified publisher: Microsoft Corporation
File origin: Downloaded from the Internet
To continue, type an administrator password, and then click Yes.
User name
Password
Domain: Microsoft
Show details
Yes
No

The Problem


User Account Control
Do you want to allow this app to make changes to your device?
Windows Security
Verified publisher: Microsoft Windows
Show more details
Yes
No

The Problem


User Account Control
Do you want to allow this app to make changes to your device?
Microsoft Management Console
Verified publisher: Microsoft Windows
Show more details
To continue, enter an admin username and password.
Email address
Password
More choices
Yes
No

The Solution(s)

Make Every User a Local Admin

The Solution(s)

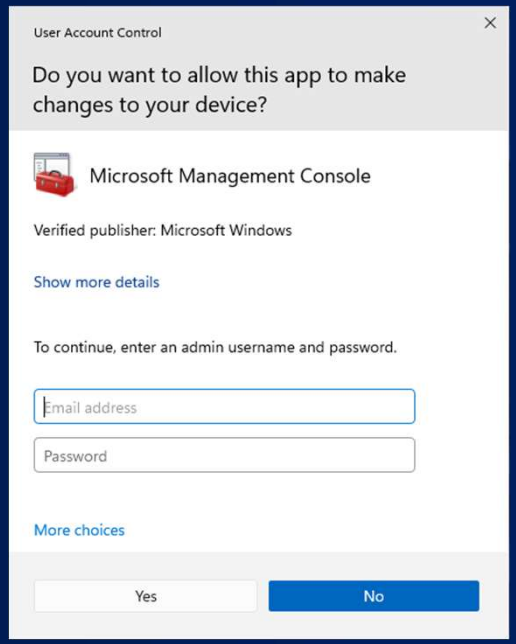
Unique Local Admin Accounts For Each PC

The Solution(s)

Unique Local Admin Accounts For Each PC

The Solution(s)

Separate Named Admin Accounts



The Solution(s)

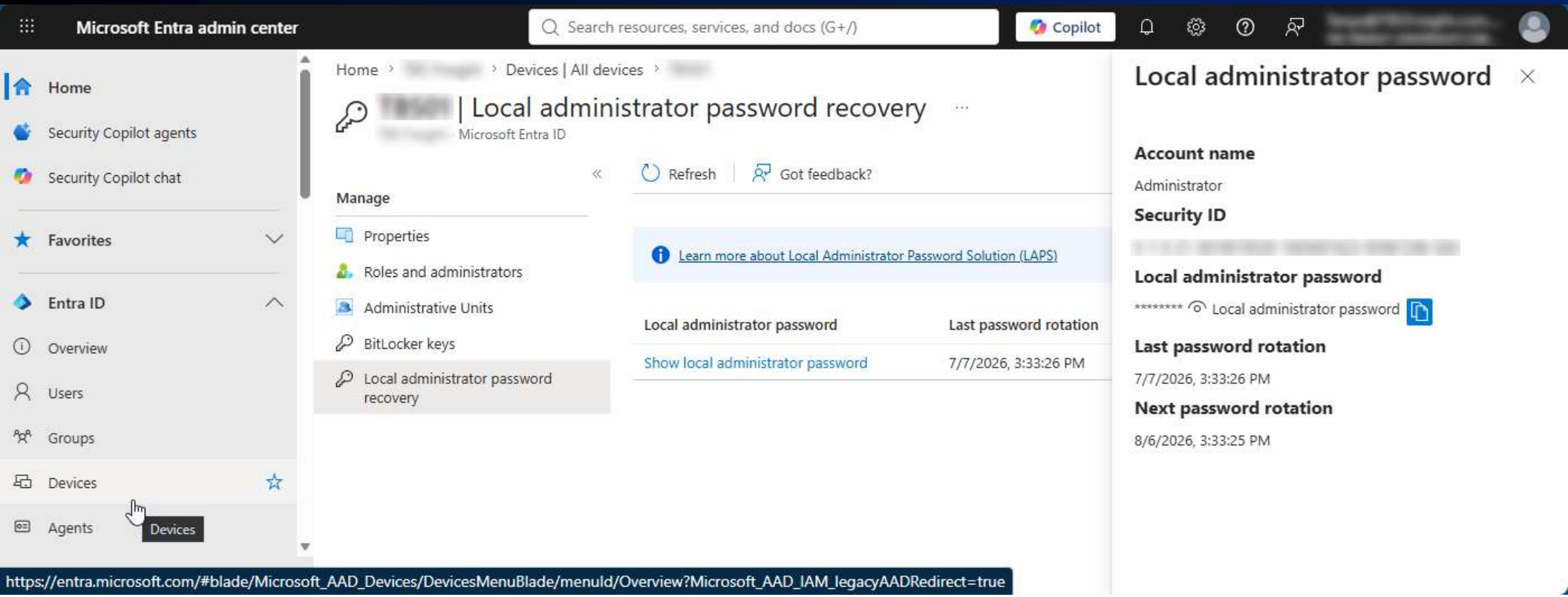
LAPS

Local Admin Password Solution

- Every device gets its own local admin password, not a shared one.
- Passwords rotate automatically on a policy-defined schedule.
- Secrets are stored and retrieved securely through Entra ID.
- Removes the single shared "god password" that once existed fleet-wide.

The Solution(s)

LAPS



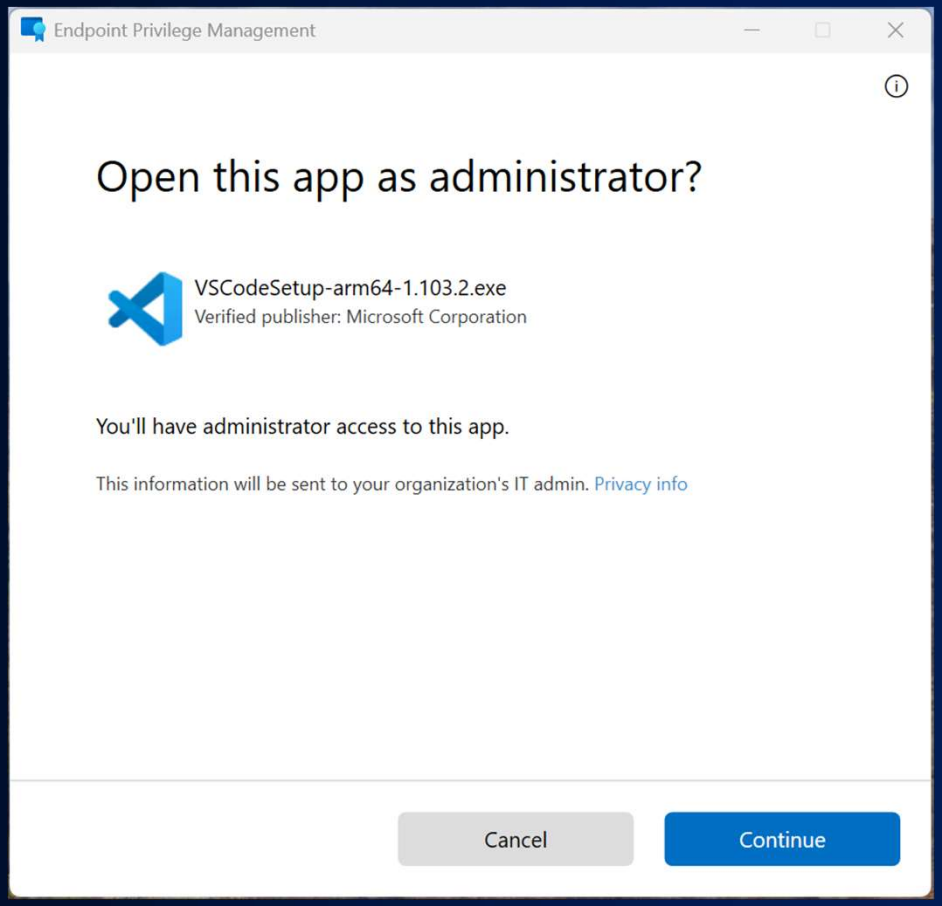
The Solution(s)

EPM

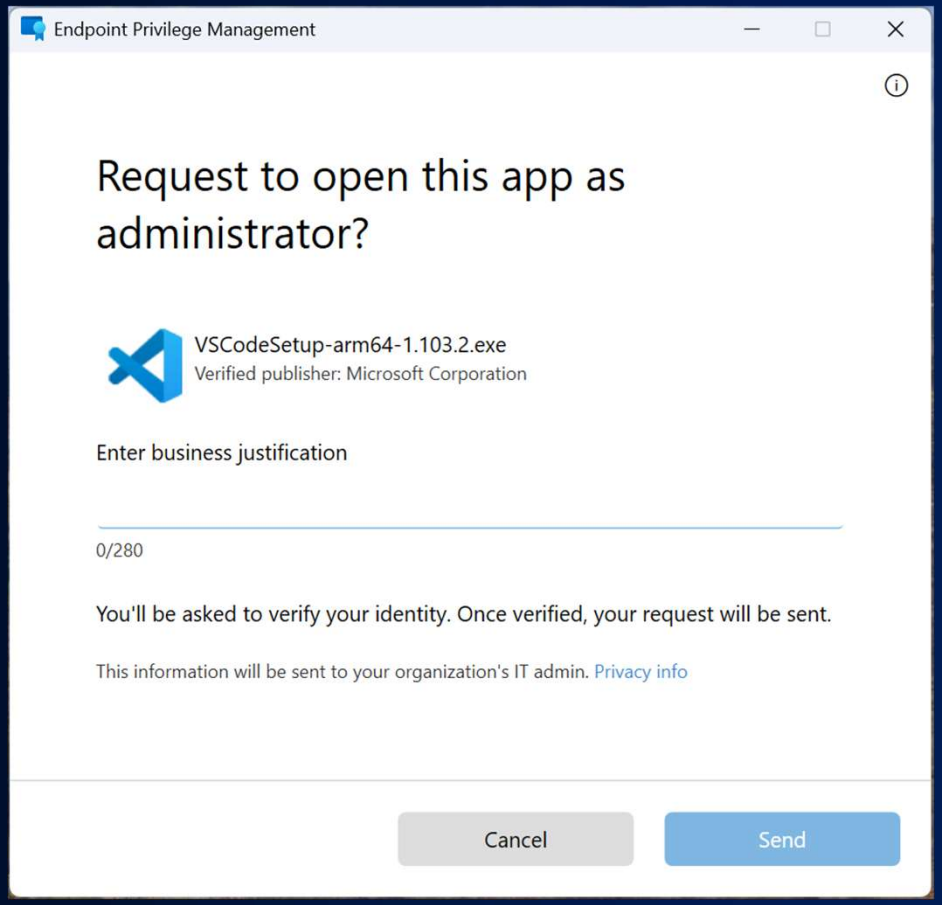
Intune Endpoint Privilege Management

- Provides controlled elevation of applications, scripts, and installers
- Supports least-privilege and Zero Trust
- Delivers auditing and reporting of elevation activity
- Does require Intune Plan 2

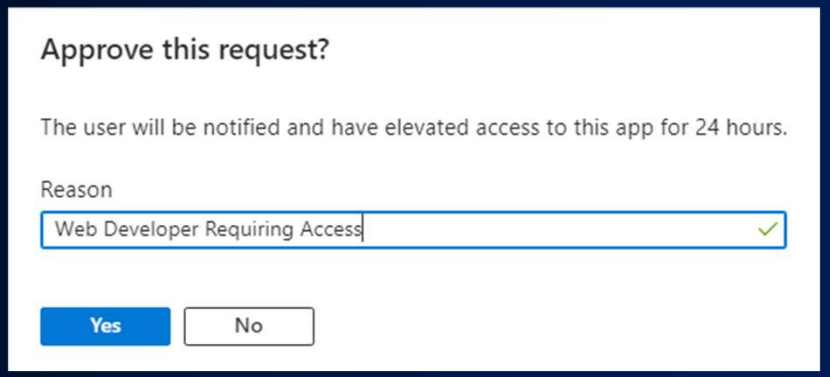
EPM

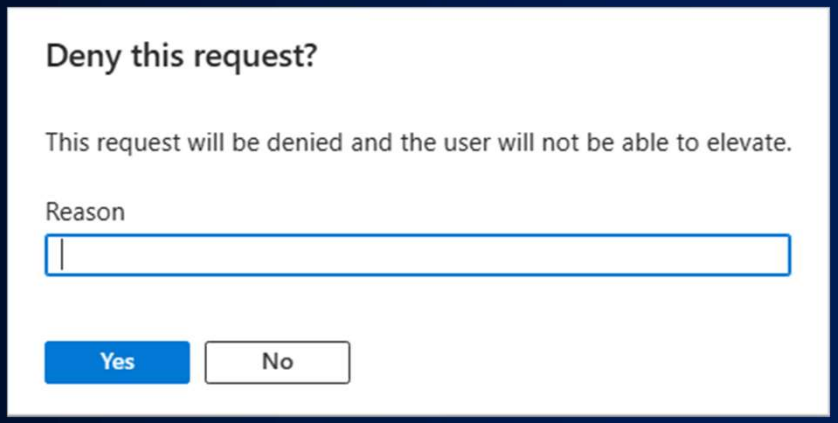

Endpoint Privilege Management
Open this app as administrator?
VSCodeSetup-arm64-1.103.2.exe
Verified publisher: Microsoft Corporation
You'll have administrator access to this app.
This information will be sent to your organization's IT admin. Privacy info
Cancel
Continue

EPM

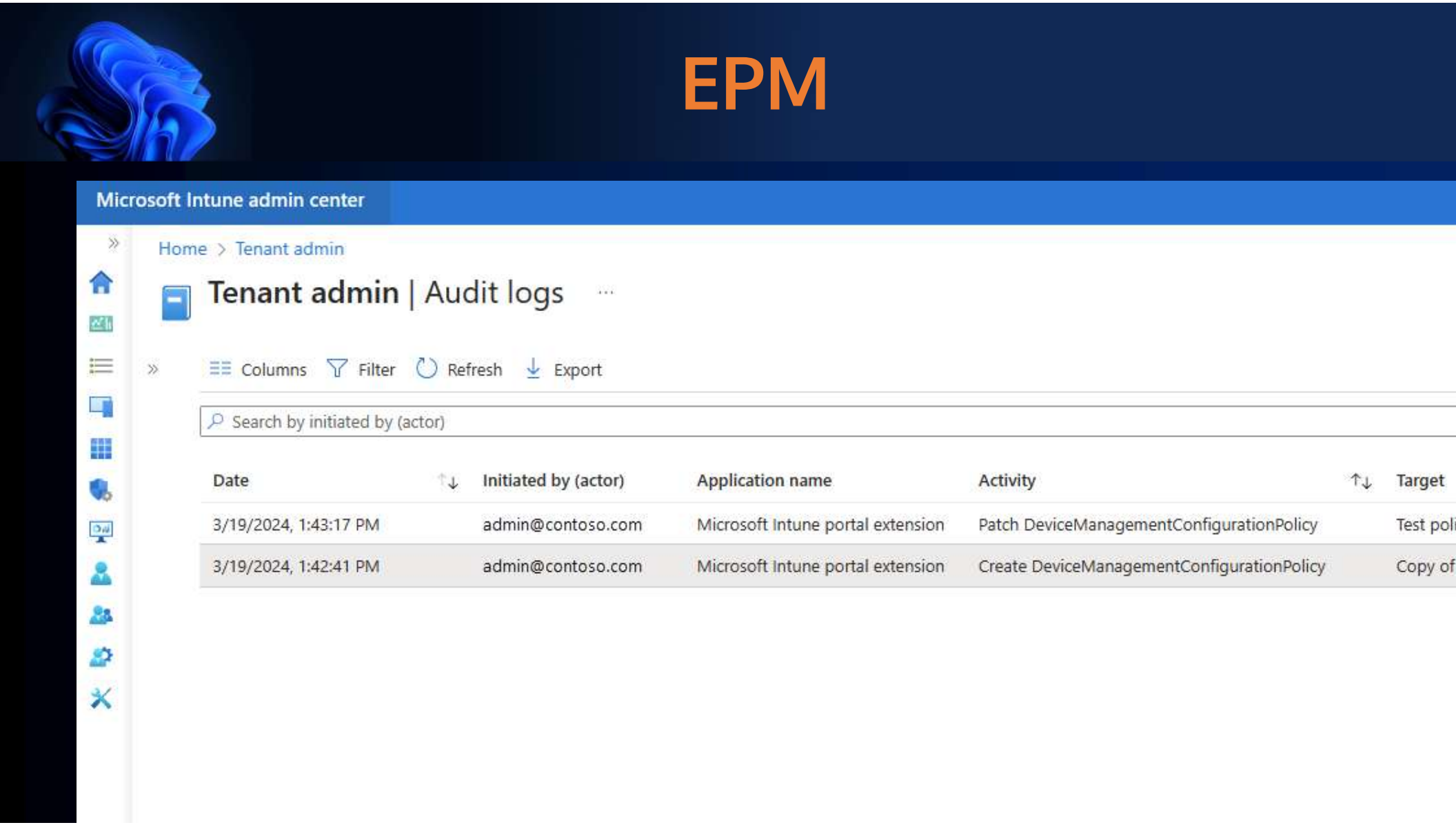

Endpoint Privilege Management
Request to open this app as administrator?
VSCodeSetup-arm64-1.103.2.exe
Verified publisher: Microsoft Corporation
Enter business justification
0/280
You'll be asked to verify your identity. Once verified, your request will be sent.
This information will be sent to your organization's IT admin. Privacy info
Cancel
Send

EPM

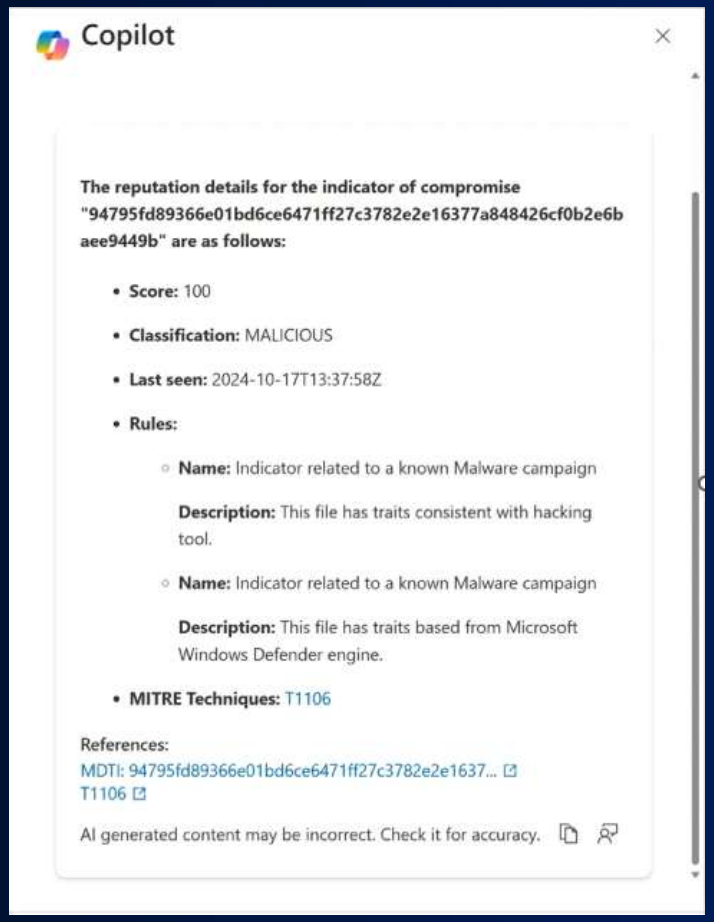

Approve this request?
The user will be notified and have elevated access to this app for 24 hours.
Reason
Web Developer Requiring Access
Yes
No


Deny this request?
This request will be denied and the user will not be able to elevate.
Reason
Yes
No

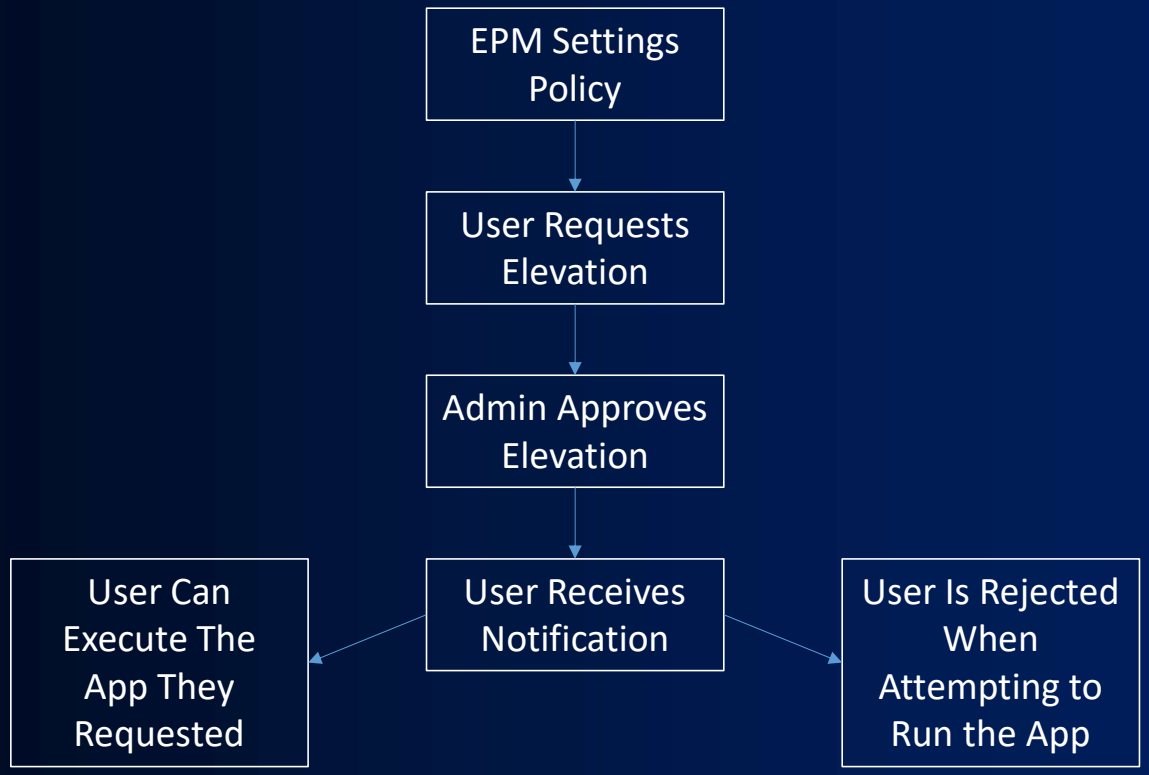
EPM


Microsoft Intune admin center
Home > Tenant admin
Tenant admin | Audit logs
Columns
Filter
Refresh
Export
Search by initiated by (actor)
Date
Initiated by (actor)
Application name
Activity
Target
3/19/2024, 1:43:17 PM
admin@contoso.com
Microsoft Intune portal extension
Patch DeviceManagementConfigurationPolicy
Test poli
3/19/2024, 1:42:41 PM
admin@contoso.com
Microsoft Intune portal extension
Create DeviceManagementConfigurationPolicy
Copy of

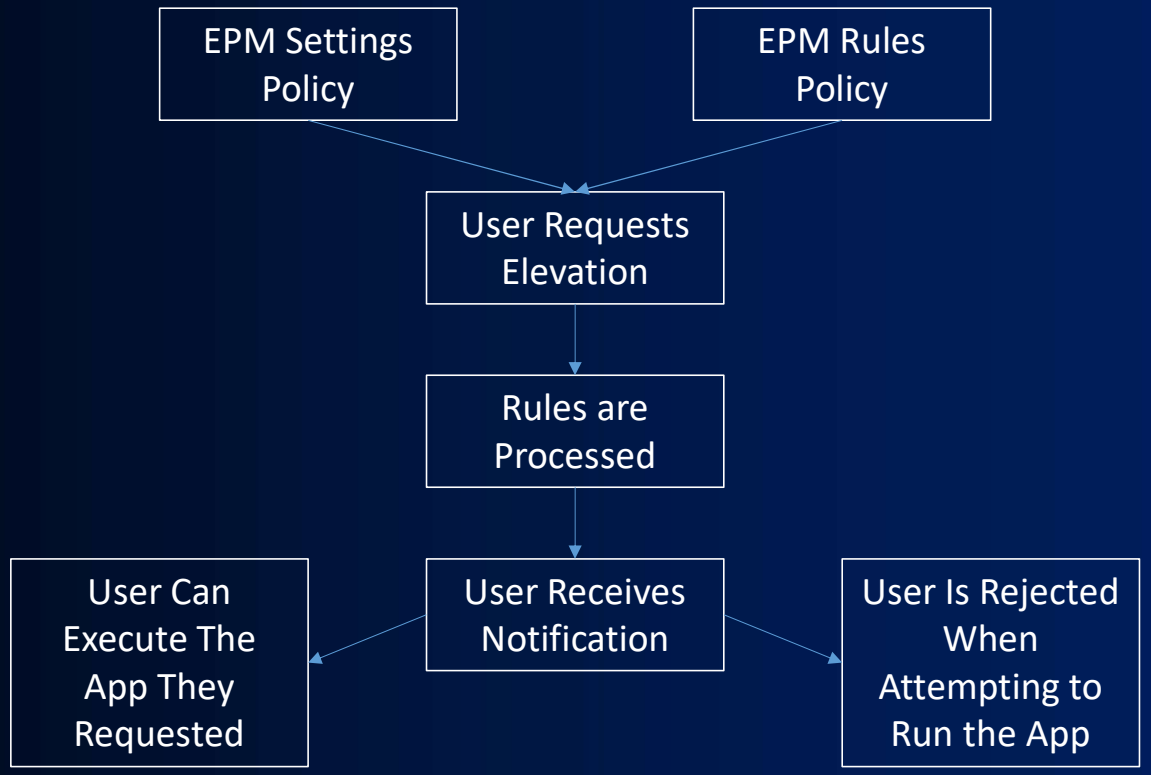
Security Copilot



EPM Setup


EPM Settings Policy
User Requests Elevation
Admin Approves Elevation
User Receives Notification
User Can Execute The App They Requested
User Is Rejected When Attempting to Run the App

EPM Setup


EPM Settings Policy
EPM Rules Policy
User Requests Elevation
Rules are Processed
User Receives Notification
User Can Execute The App They Requested
User Is Rejected When Attempting to Run the App

The Solution(s)

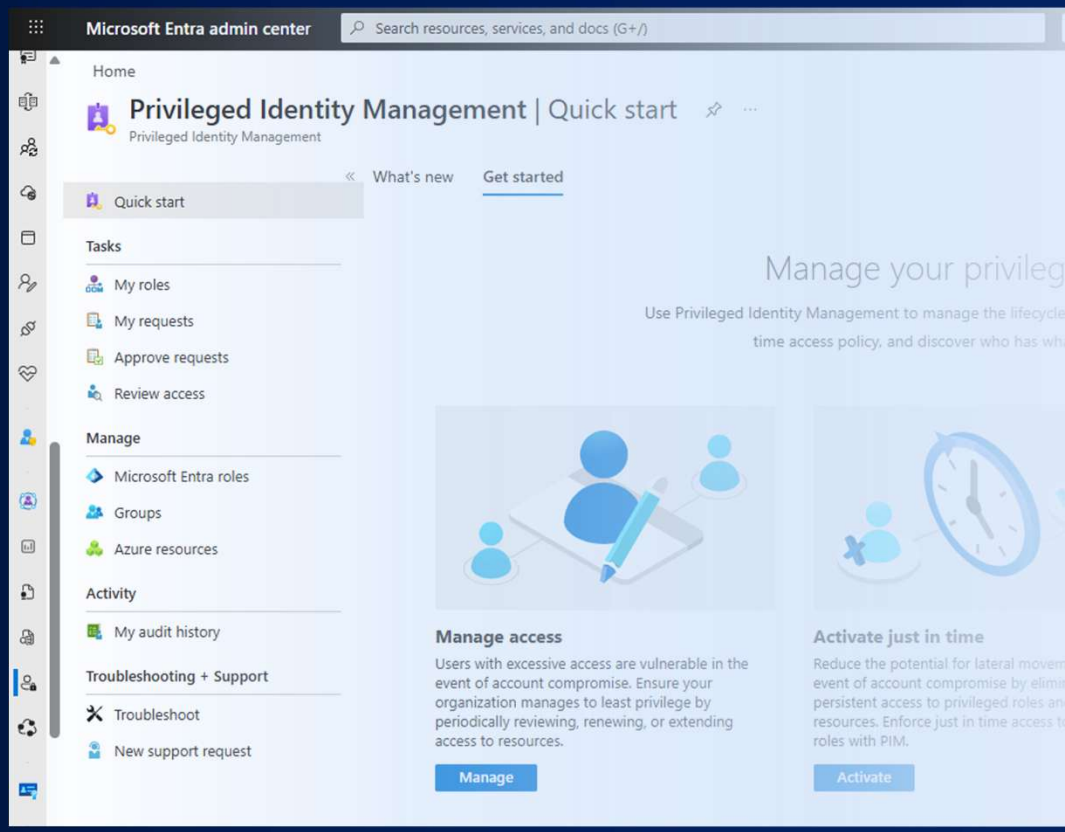
PIM

Privilege Identity Management

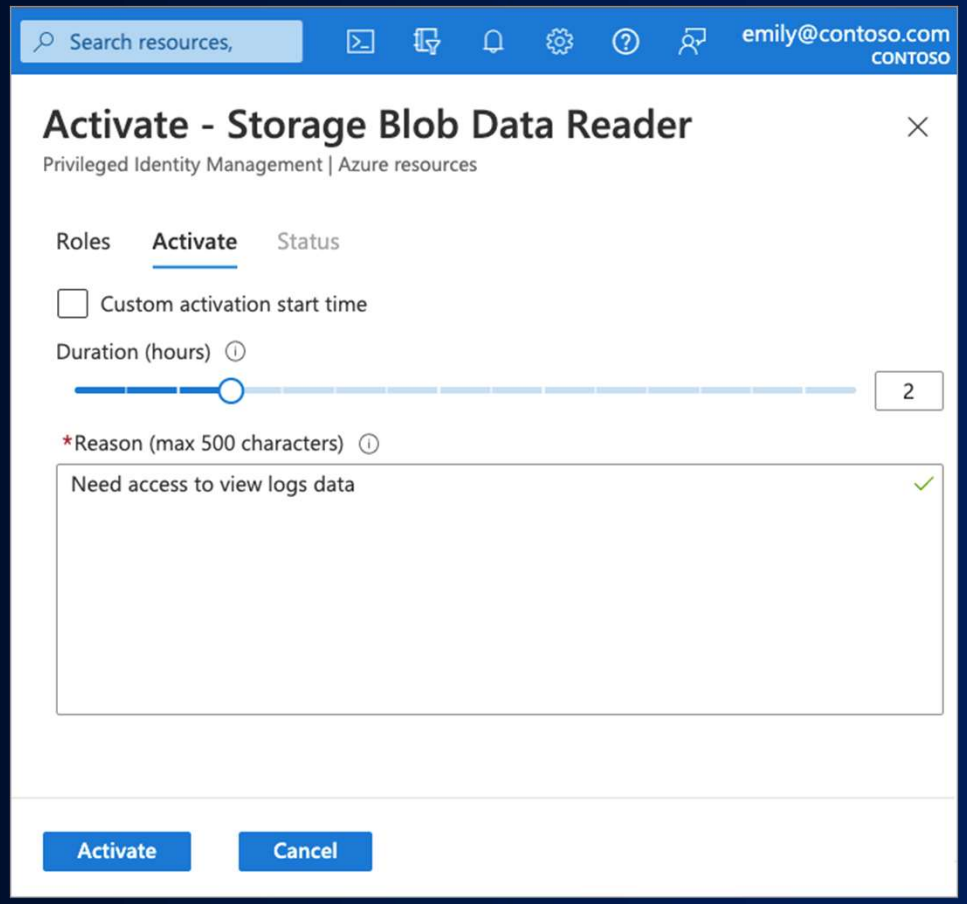
- Provides elevation of rights or roles for a given period. Just In Time (JIT) admin rights
- Supports least-privilege and Zero Trust
- Delivers auditing and reporting of elevation activity
- Does require Entra ID Plan 2

PIM

- No More GA members
- True Role Base Access Control
- Time Based RBAC
- Can Require Approval
- Integration with ITSM Tools

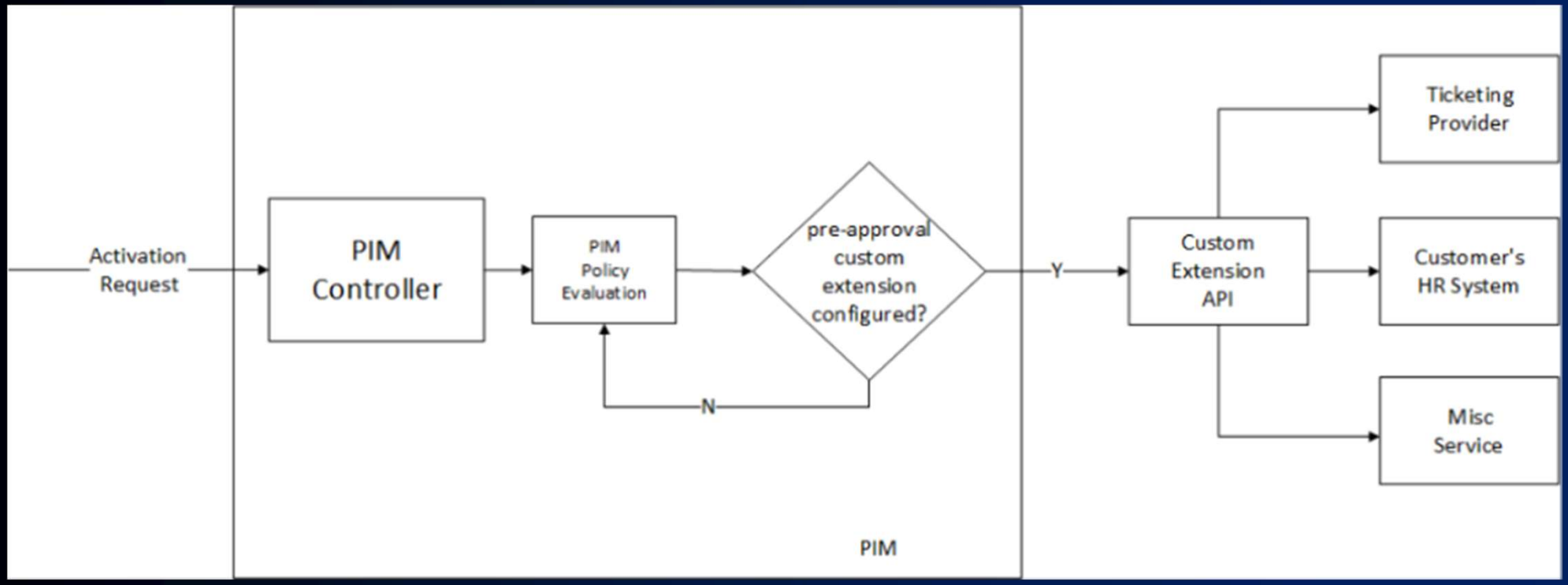


PIM


Search resources,
emily@contoso.com
CONTOSO
Activate - Storage Blob Data Reader
Privileged Identity Management | Azure resources
Roles
Activate
Status
Custom activation start time
Duration (hours)
2
*Reason (max 500 characters)
Need access to view logs data
Activate
Cancel

PIM

Custom Extensions



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

Adelaide Microsoft IT Pro Community

Systematech.com.au

@Moff25

Systematech.com.au

Linkedin.com/in/brettmoffett/