

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:



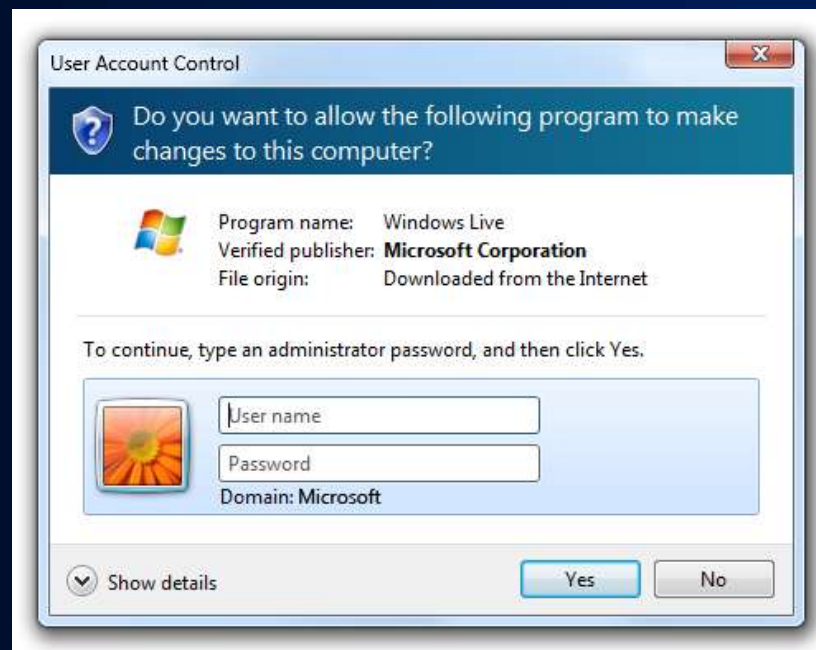


The Problem

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



The Problem





The Problem





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.

[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**

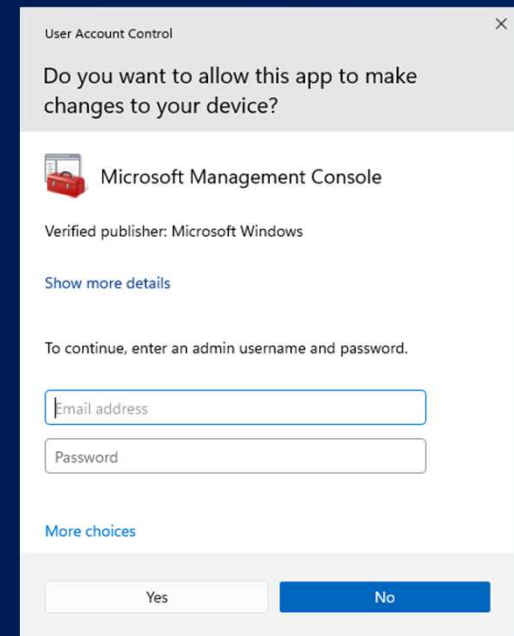


bitwarden
Password Manager



The Solution(s)

Separate Named Admin Accounts





The Solution(s)

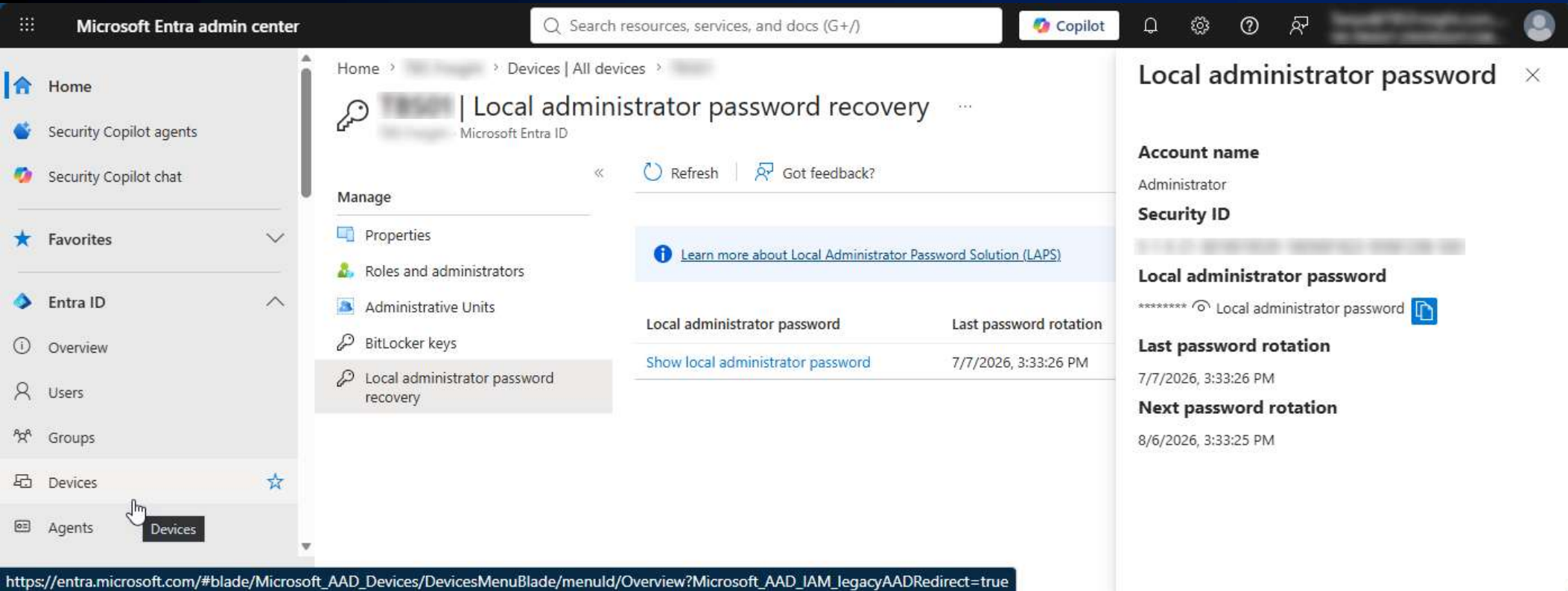
LAPS

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 screenshot displays the Microsoft Entra admin center interface. The left sidebar contains navigation links: Home, Security Copilot agents, Security Copilot chat, Favorites, Entra ID, Overview, Users, Groups, Devices, and Agents. The main content area shows the 'Local administrator password recovery' page for a specific device. The page includes a 'Manage' section with links to Properties, Roles and administrators, Administrative Units, BitLocker keys, and Local administrator password recovery. A table displays the 'Local administrator password' and its 'Last password rotation' date and time. A right-hand pane provides details for the 'Local administrator password', including the account name, security ID, and the next password rotation date.

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

Home > Devices | All devices >

Local administrator password recovery

Microsoft Entra ID

« Refresh Got feedback?

Manage

- Properties
- Roles and administrators
- Administrative Units
- BitLocker keys
- Local administrator password recovery

Local administrator password	Last password rotation
Show local administrator password	7/7/2026, 3:33:26 PM

[Learn more about Local Administrator Password Solution \(LAPS\)](#)

Local administrator password

Administrator

Security ID

***** Local administrator password

Last password rotation

7/7/2026, 3:33:26 PM

Next password rotation

8/6/2026, 3:33:25 PM

https://entra.microsoft.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/menuld/Overview?Microsoft_AAD_IAM_legacyAADRedirect=true



The Solution(s)

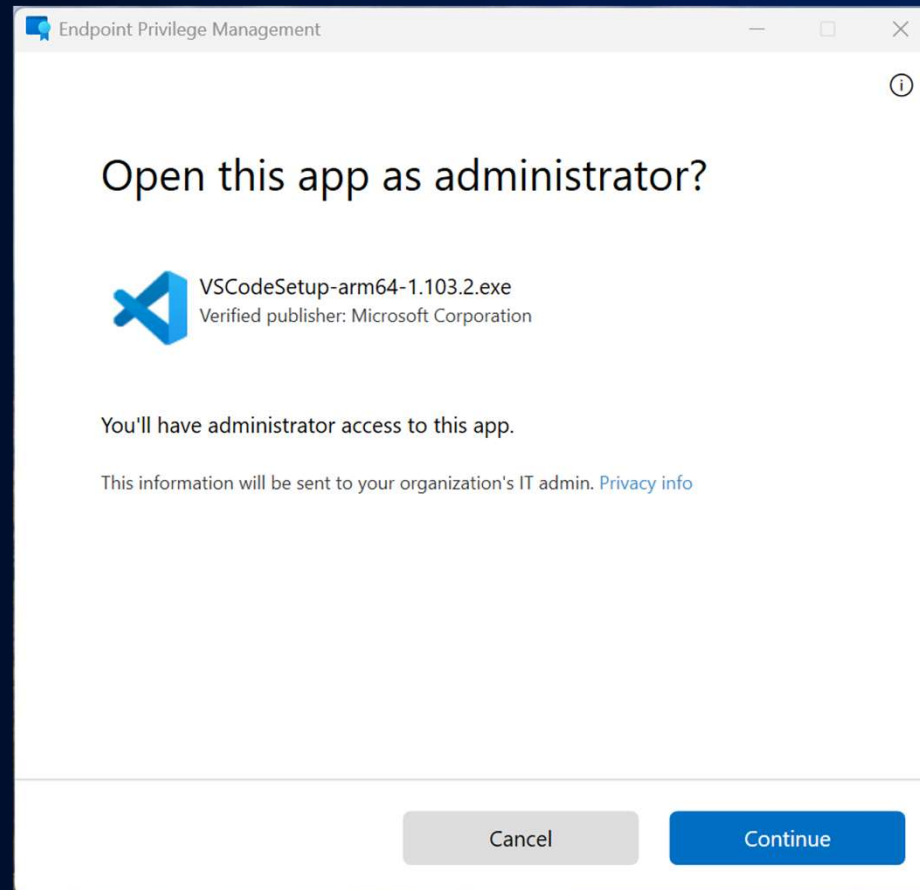
EPM

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





EPM

Endpoint Privilege Management

Request to open this app as administrator?



VSCoSetup-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 pol
3/19/2024, 1:42:41 PM	admin@contoso.com	Microsoft Intune portal extension	Create DeviceManagementConfigurationPolicy	Copy of



Security Copilot

 Copilot ✕

The reputation details for the indicator of compromise
"94795fd89366e01bd6ce6471ff27c3782e2e16377a848426cf0b2e6b
aee9449b" are as follows:

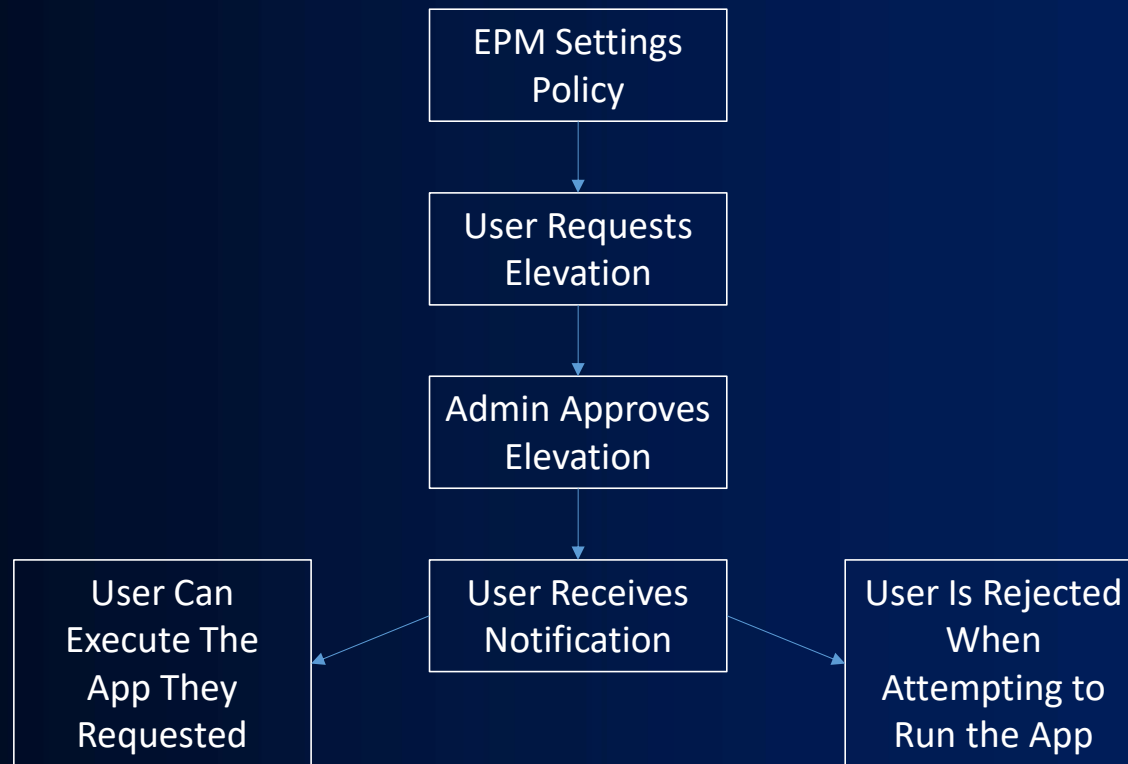
- **Score:** 100
- **Classification:** MALICIOUS
- **Last seen:** 2024-10-17T13:37:58Z
- **Rules:**
 - **Name:** Indicator related to a known Malware campaign
Description: This file has traits consistent with hacking tool.
 - **Name:** Indicator related to a known Malware campaign
Description: This file has traits based from Microsoft Windows Defender engine.
- **MITRE Techniques:** [T1106](#)

References:
[MDTI: 94795fd89366e01bd6ce6471ff27c3782e2e1637...](#) 
[T1106](#) 

AI generated content may be incorrect. Check it for accuracy.  

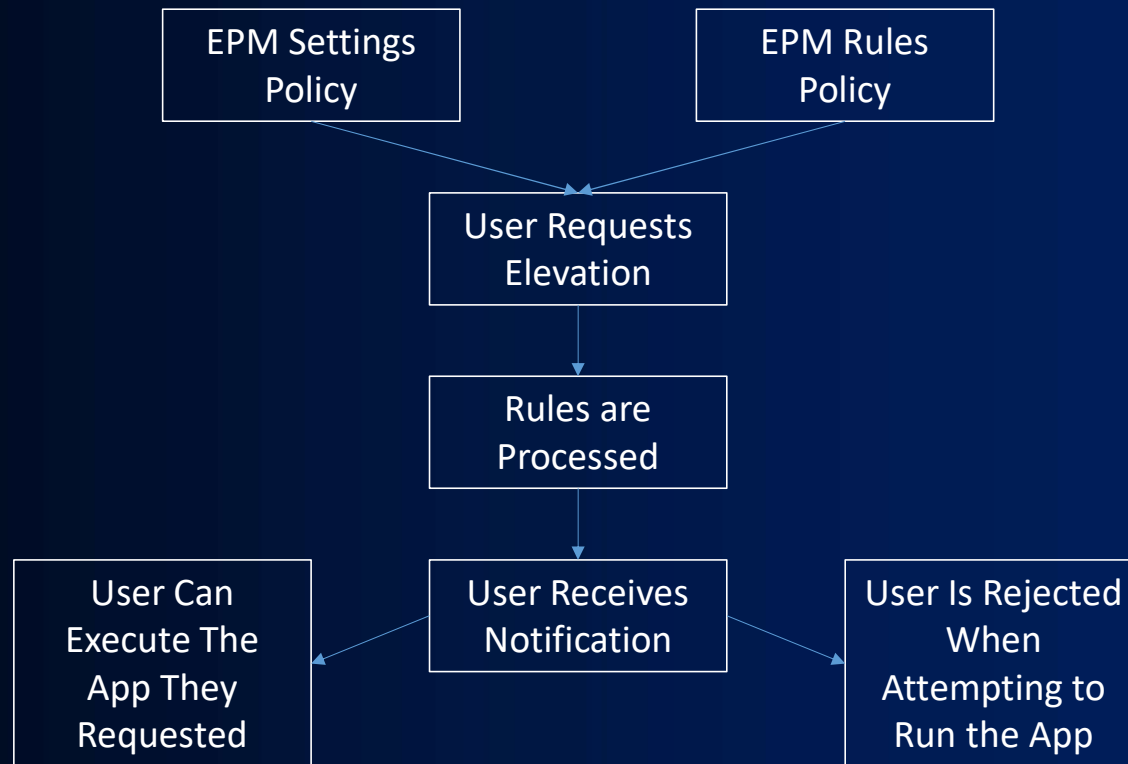


EPM Setup





EPM Setup





The Solution(s)

PIM

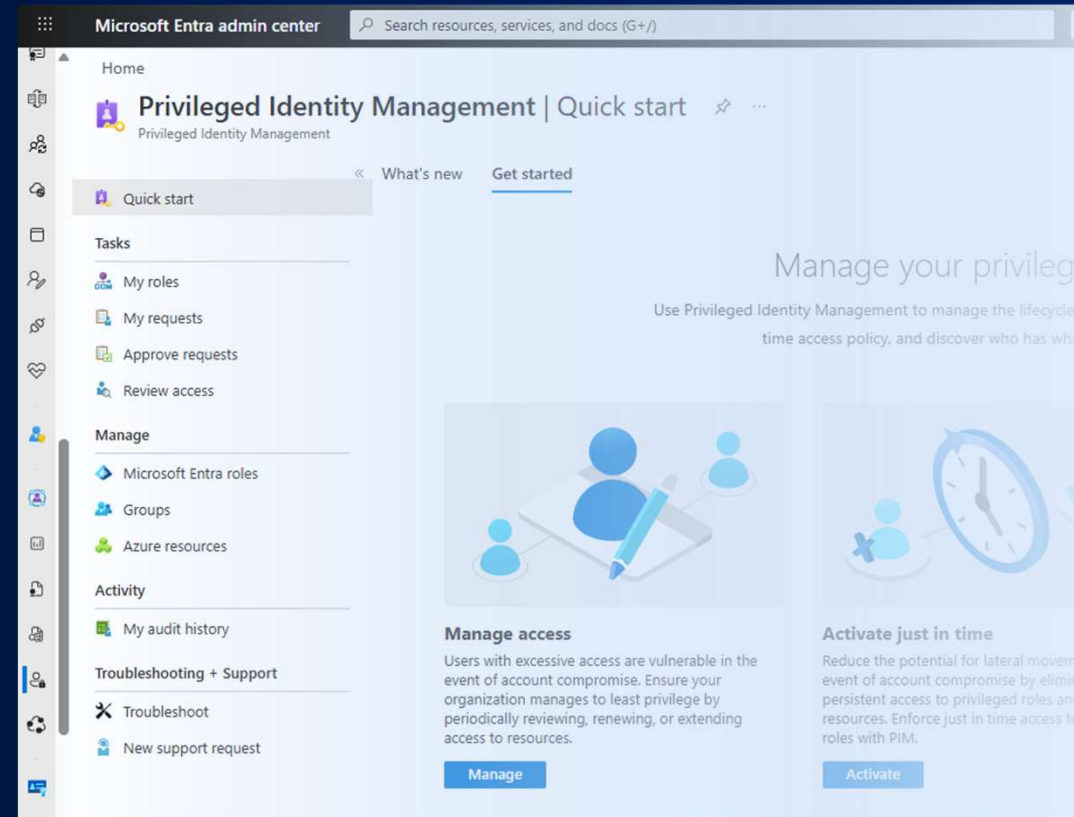
Privilege Identity Management

- 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 ✓

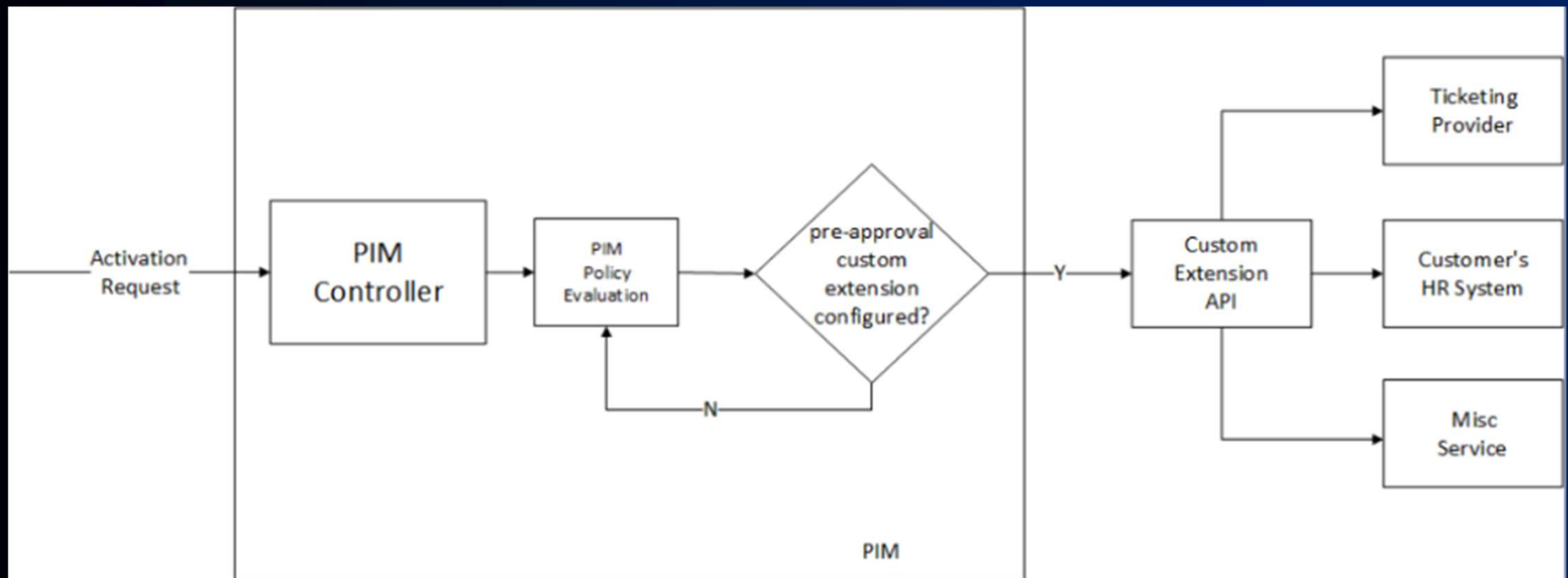
Activate

Cancel



PIM

Custom Extensions



Adelaide Microsoft IT Pro Community

Systematech.com.au

@Moff25



Systematech.com.au

[Linkedin.com/in/brettmoffett/](https://www.linkedin.com/in/brettmoffett/)

