



Identity Master Class

February 24th, 2026

09:00 – 16:00



THANK YOU TO OUR AMAZING SPONSORS !



Identity Master Class - The Team

- Merill Fernando
 - Principal Product Manager, Microsoft
- Thomas Naunheim
 - Microsoft MVP | Cyber Security Architect @glueckkanja AG
- Klaus Bierschenk
 - Microsoft MVP for Security | Director Consulting Expert @CGI Germany
- Pim Jacobs
 - Microsoft MVP & Technology Lead Security @InSpark
- Jan Vidar Elven
 - Senior Architect @ Evidi, MVP Security



Agenda

- 09:00 – Start and Welcome – User Lifecycle
 - User Lifecycle Story
 - Entra ID Governance – Lifecycle Workflows
 - Lab Break 1
- 10:30 – Snacks / Fruit / Coffee
- 10:45 – Governance & Identity Security
 - Entra ID Governance - Access Management
 - Lab Break 2
 - Securing Identities
 - Privileged User Lifecycle Story
 - Lab Break 3
 - Securing Privileged Access
- 12:00 – Lunch

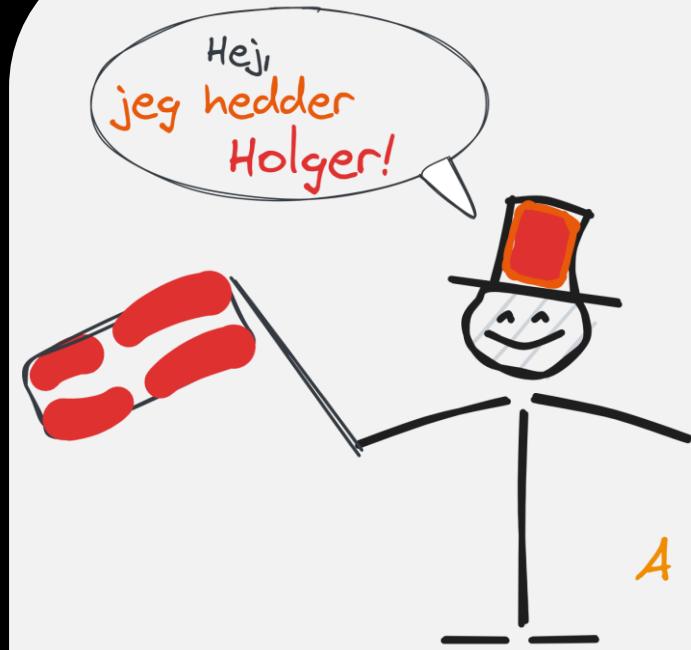
Agenda (cont.)

- 12:45 – Agent ID
 - Securing agentic AI using Microsoft Entra Agent ID
 - Lab break 4
- 14:15 – Cake / Snacks / Fruit / Coffee
- 14:45 – Maintaining, Security Exposure & Monitoring
 - Monitoring, Maintaining, Disaster Recovery
 - Optimize Identity Security Exposure
 - Lab break 5
 - Interactive closure and QA with audience



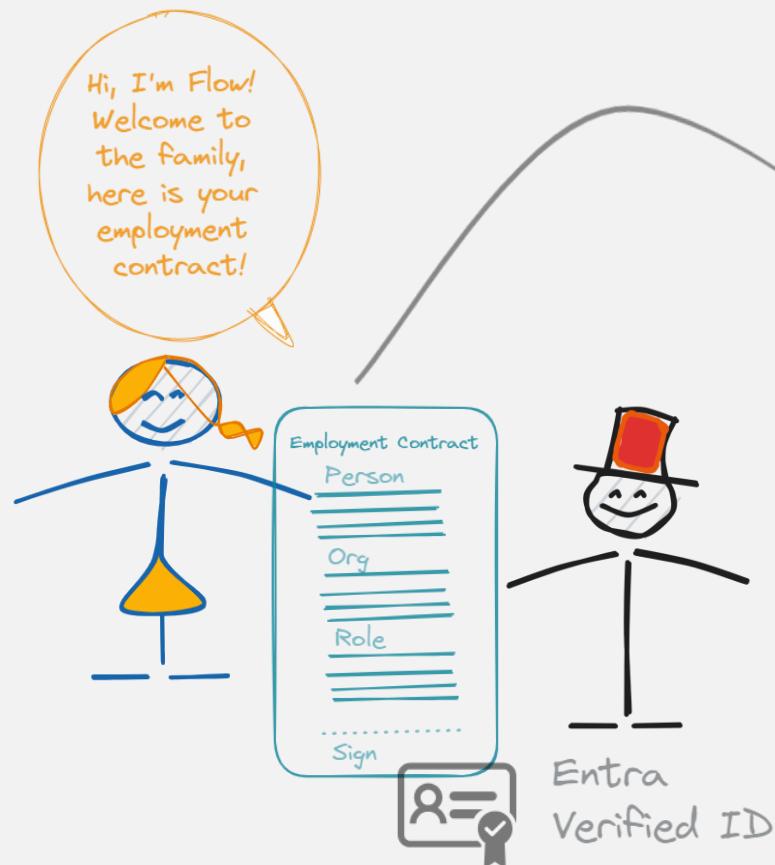
Entra ID Inbound Provisioning & Lifecycle Workflows





Mød Holger Danske!

A new recent hire to the Elven organization!



Entra ID Inbound Provisioning

Create
Read
Update
Disable

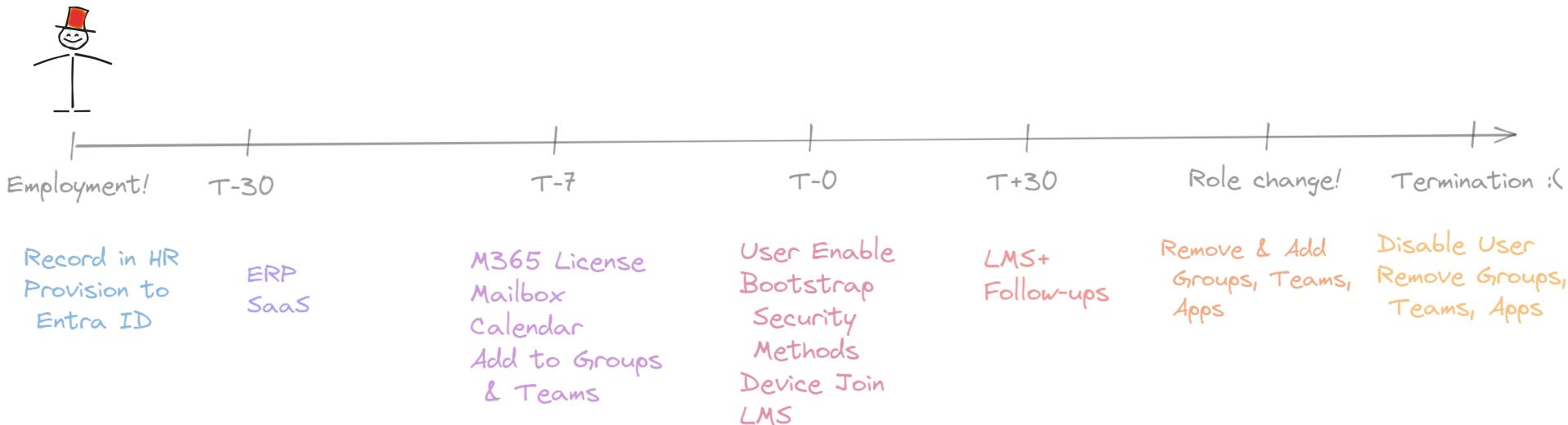
employeeHireDate
employeeLeaveDateTime

Manage Access

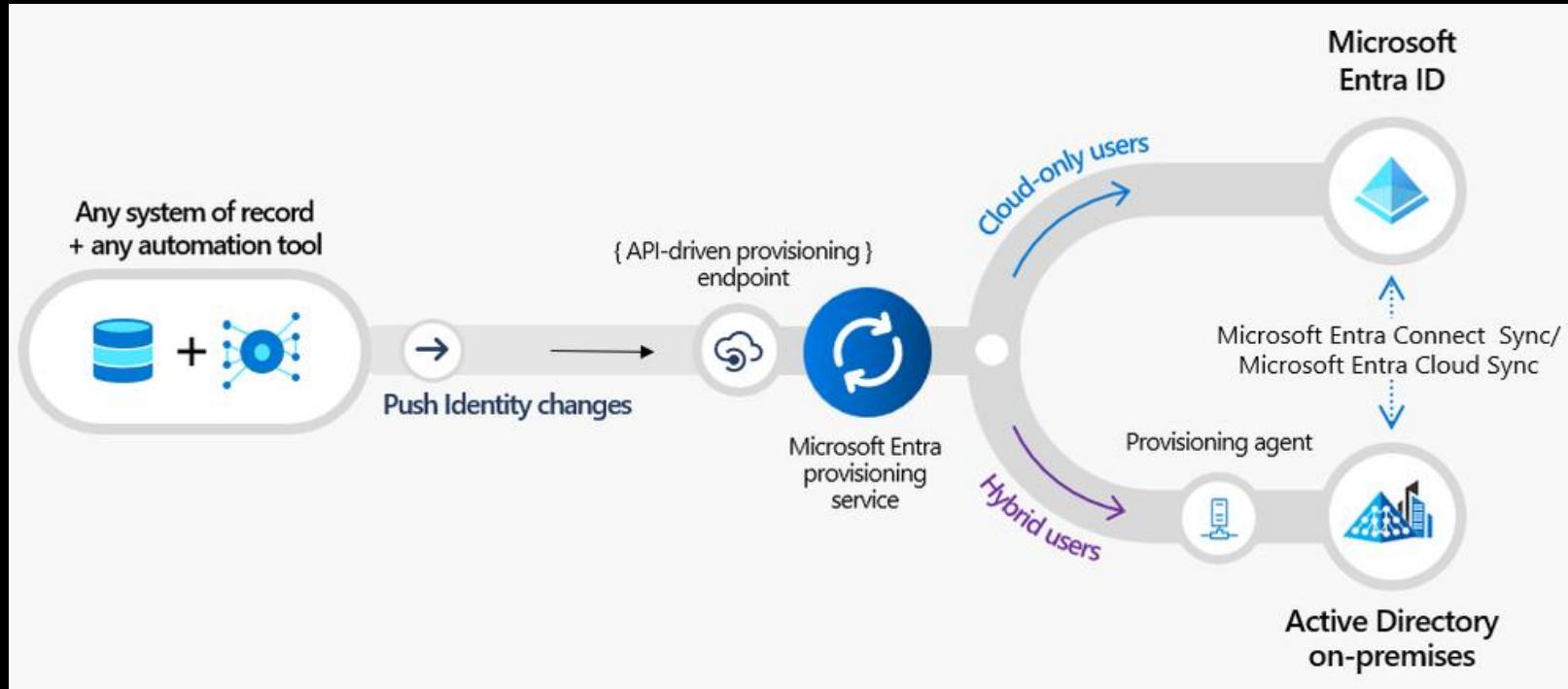


Entra ID Identity Governance

Identity & Access Lifecycle



Entra ID Provisioning API



Connect Sync vs. Cloud Sync

Entra Connect Sync:

- Do you know MIIS, ILM or FIM, MIM?
- Sync Srv Dates back to the early 2000s
- 20 years of Metadirectory Experience
- Sync Service is very robust like a Swiss Army Knife ...
- Large on-premises infrastructure footprint
- Management, Connect Server, SQL

Entra Cloud Sync:

- GA since 2021
- Modern Architecture, Cloud based
- Lightweight On-Premises Agents
- Not the entire feature set but
- also major improvements over Entra Connect Sync
- Is this right for you?
Use the comparison tool in EAC



Connect Sync vs. Cloud Sync

(My) top features from
Cloud Sync:

- Disconnected Forest Option
- On-Premises agent failover
- Cloud Management in EAC
- Group Writeback

Thinking about migration?

- Comparison Tool (EAC) helpful
- Both technologies can run in parallel
- Strategy considerations
- Where is your source of authority?

API-drive Provisioning log details X

displayname

Steps	Troubleshooting & Recommendations	Modified Properties	Summary
Property name	Old value	New value	
country		DK	
companyName		Elven	
department		ELDK 2026	
employeeHireDate		2026-02-24T06:00:00.000000+00:00	
employeeType		Demo	
employeeOrgData.costCenter		ELDK	Source system
employeeOrgData.division		Experts Live Denmark	API
givenName		Holger	
jobTitle		Consultant	API
mail		holger.danske@@M365x91871532.onmicrosoft.com	
mobile		+47 00000000	API
physicalDeliveryOfficeName		Denmark	
preferredLanguage	en-US	dk-DK	
surname		Danske	API

Delete

Entra ID Governance

01

Identity Lifecycle Management

Inbound Provisioning,
Lifecycle Workflows

03

Outbound provisioning

Provisioning and access to
3rd party applications

02

Access Lifecycle Management

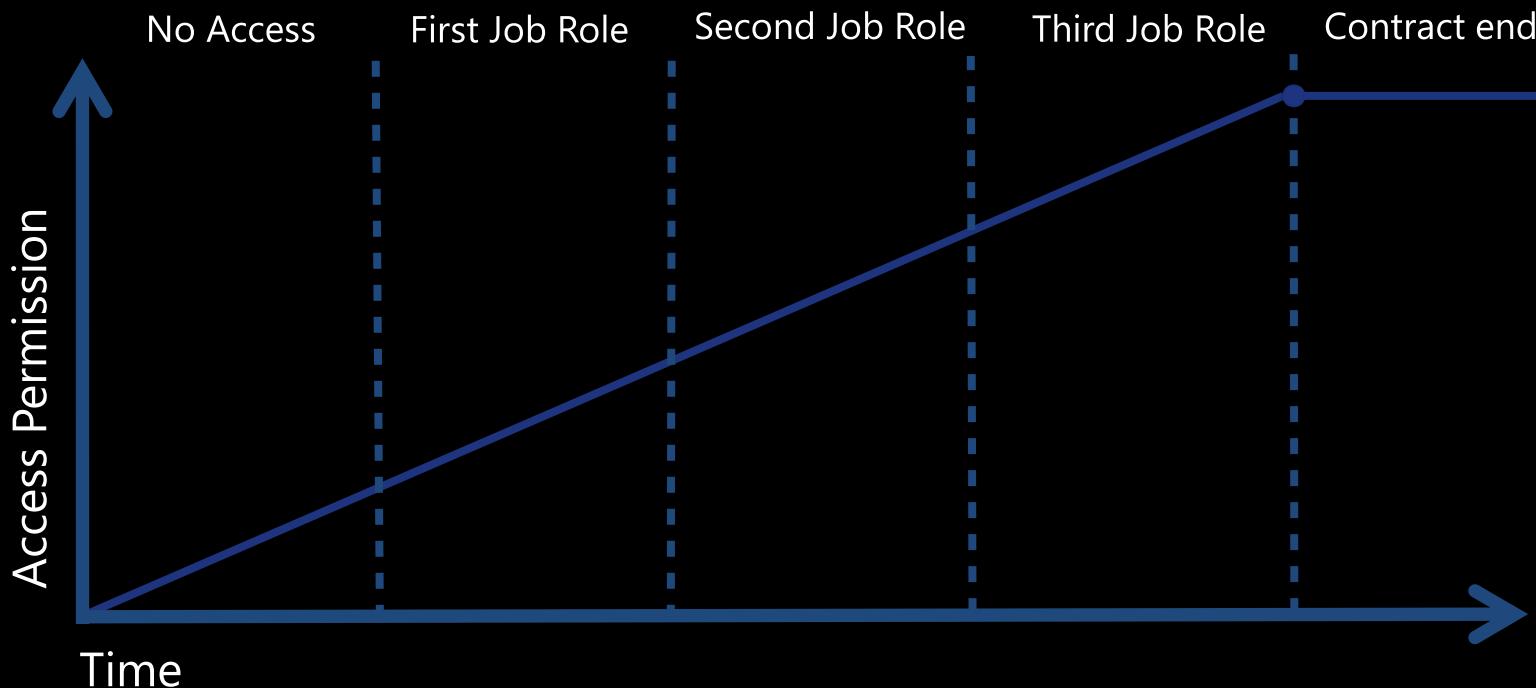
Lifecycle Mover Workflows,
Access Packages,
Access Reviews

04

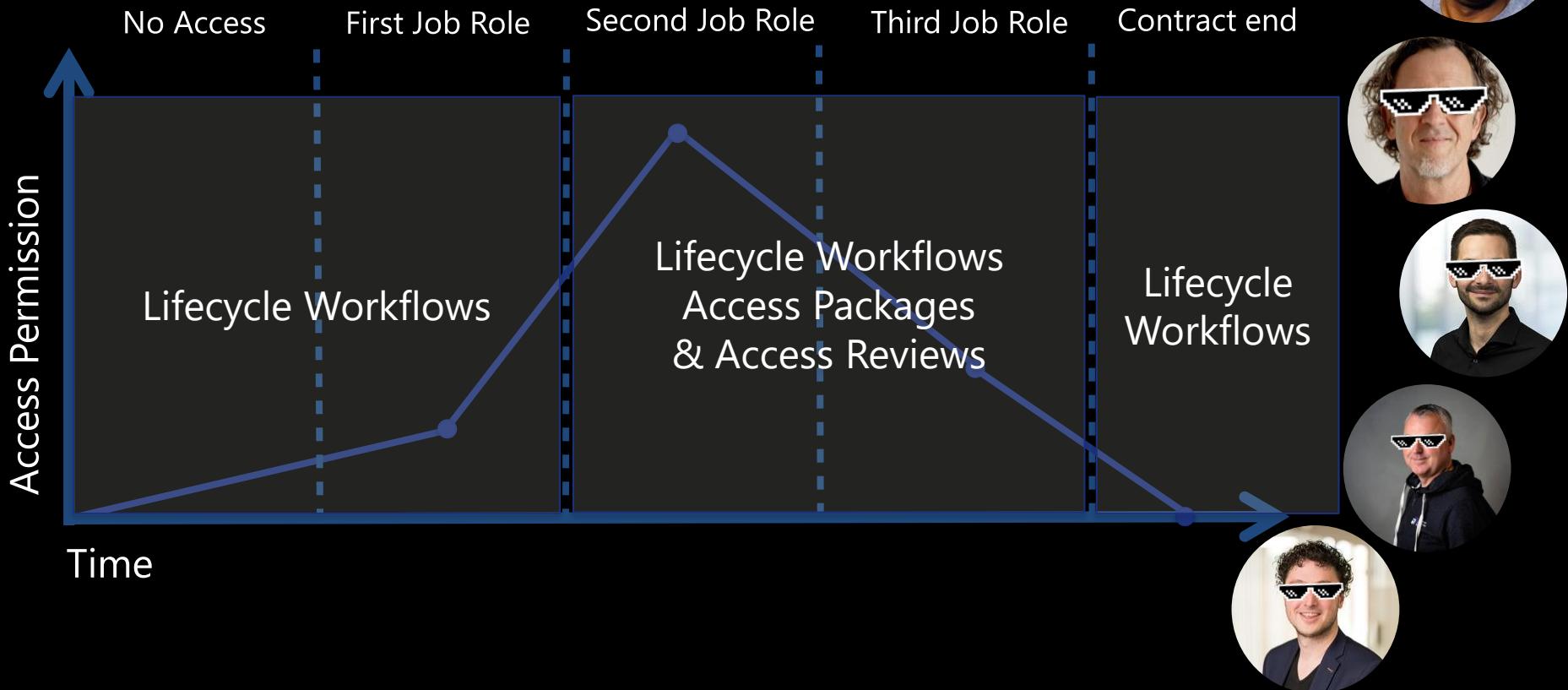
Least Privileged Access

Just in time just enough
access

Historic Access Lifecycle Management

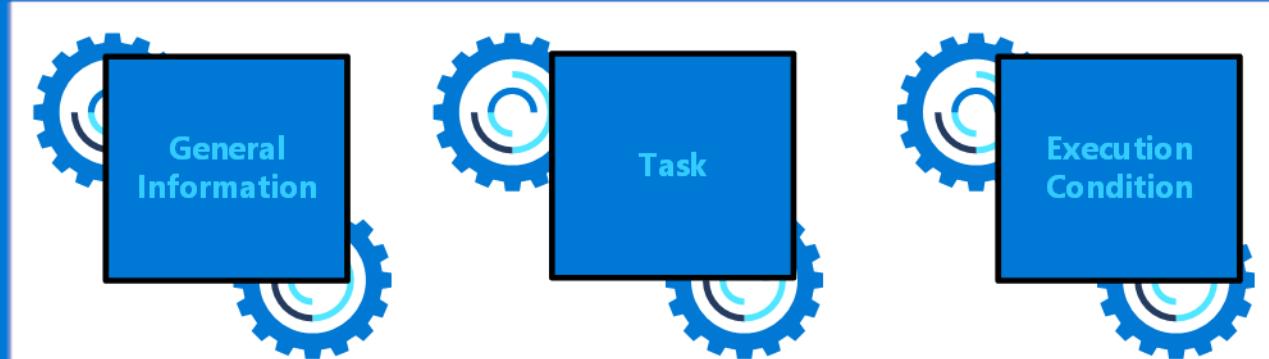


Modern Access Lifecycle Management



Understanding Lifecycle Workflows

Lifecycle workflows



Automated Joiner, Mover & Leaver

Lifecycle Workflows facts

Custom import to Active Directory Must be in the format "yyyyMMddHHmmss.fZ"

On-premises AD string attribute

eeHireDate and eeLeaveDate

Task name * ① Send Welcome Email to end user

Task description Send welcome email to new hire

Configure

The user's email address automatically populated from the mail attribute on the user's profile.

To recipient * ① [User mail attribute]

CC recipients ① 0 Users selected

Configure

i The user's account info will automatically be retrieved from the user's profile.

User account * ① [User ID]

Enable on-premises account ①

Email language translation ① Dynamic based on recipient (Default)

Runs each 3 hours

Interval is customizable (1-24)

Max 100 Workflows per tenant

25 per tasks per workflow

Preferred Language

Email customizations (Logo, Domain & Text)

Built-in native tasks for Microsoft Entra

Option to continue workflow on error

Native hybrid integration for enable, disable and delete

EmployeeHireDate

EmployeeLeaveDateTime

Latest Lifecycle Workflows updates



Reprocess failed users and workflows in Lifecycle Workflows



Visibility of sensitivity labels on group tasks in Lifecycle Workflows



Trigger workflows for inactive employees and guests in Lifecycle Workflows



Agent identity sponsor lifecycle support in Lifecycle Workflows



Delegated Workflow Management with AUs in Lifecycle Workflows



Expanded attribute support in Lifecycle Workflows attribute changes trigger (like CSA)



Basic HTML support in Lifecycle Workflow



Entra ID Governance guest billing meter enforcement



Custom task extensions

Lifecycle workflows



Logic Apps

Custom Extension examples



Setting the out of office for the user and hiding user from address list



Converting the mailbox to shared



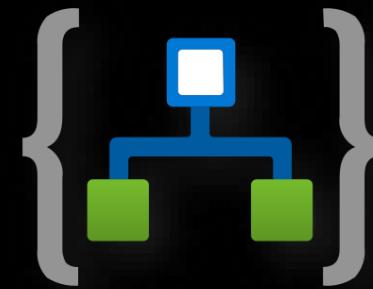
Wiping Intune managed devices (MAM/MDM)



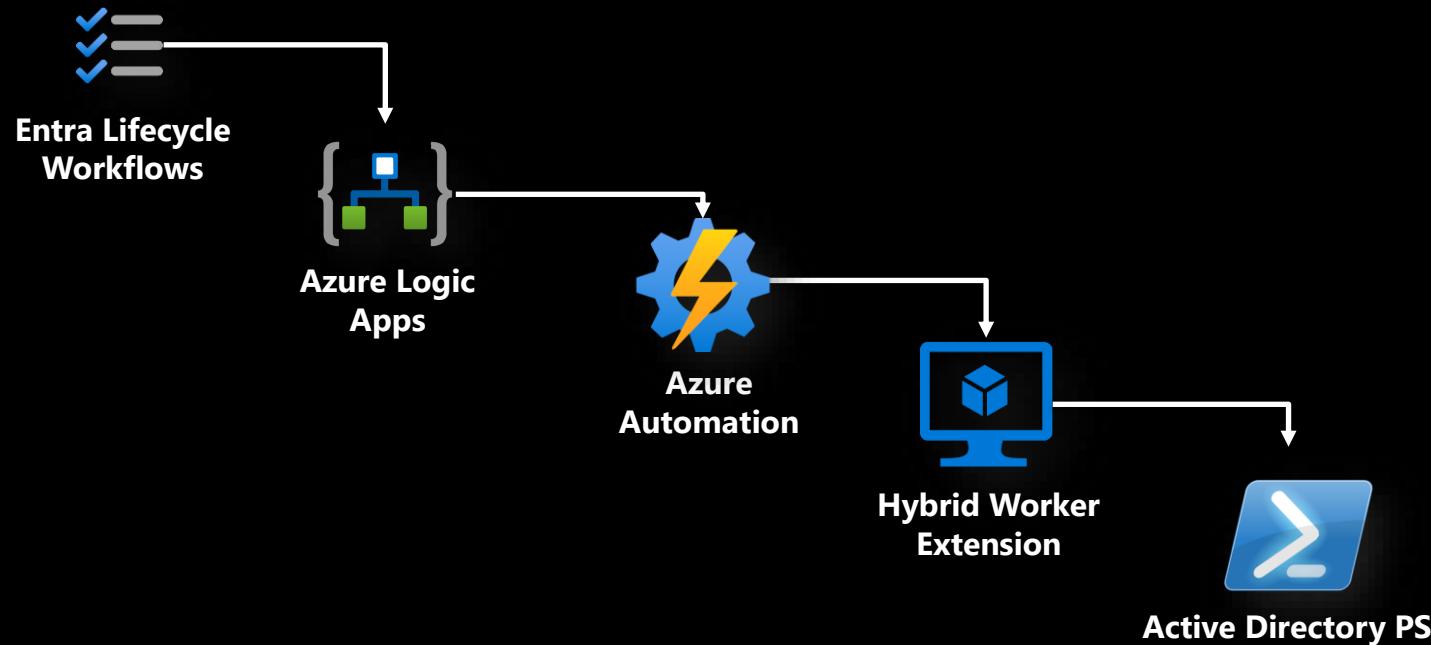
Disabling admin / test accounts associated to user account



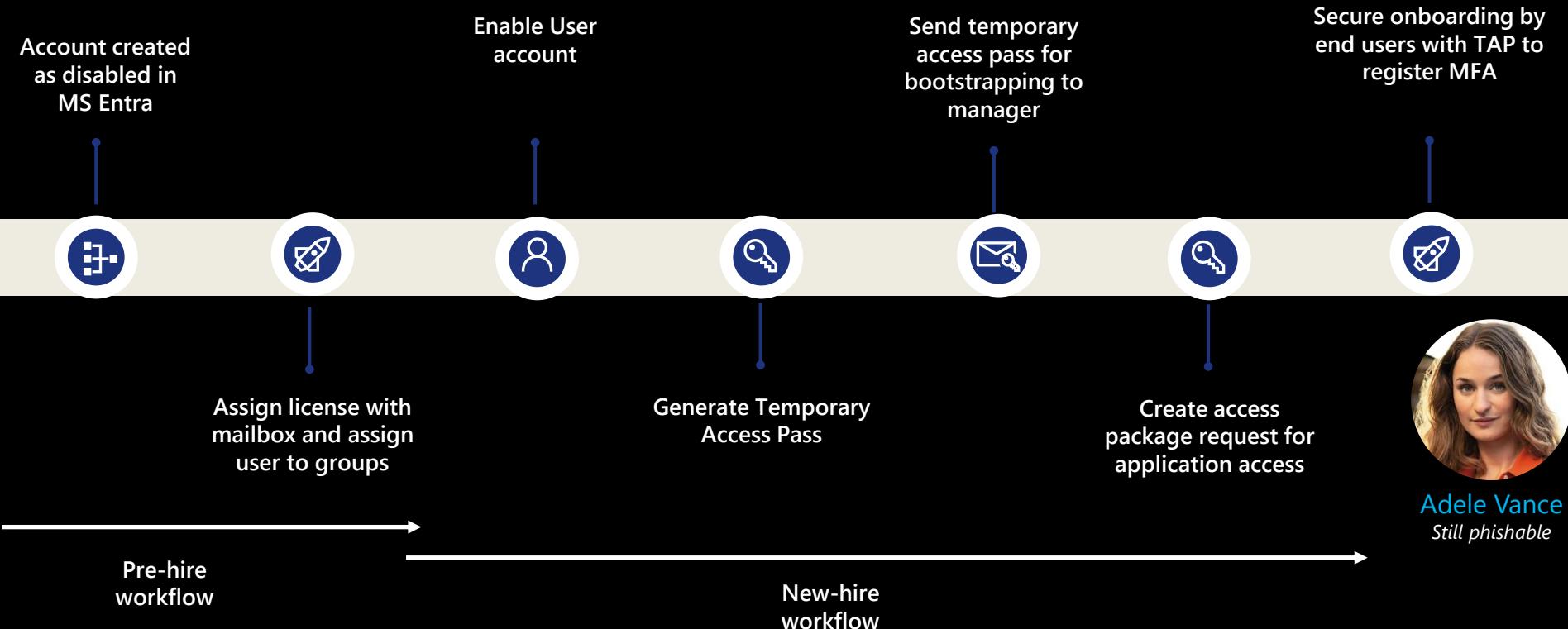
Deleting admin / test accounts associated to user account



Executing tasks on Active Directory?



Onboarding example





D E M O

LAB 1: Inbound Provisioning API & Lifecycle Workflows

<https://aka.ms/eldk26>





Entra ID Governance Access Management



Entra ID Governance

01

Identity Lifecycle Management

Inbound Provisioning,
Lifecycle Workflows

03

Outbound provisioning

Provisioning and access to
3rd party applications

02

Access Lifecycle Management

Lifecycle Mover Workflows,
Access Packages,
Access Reviews

04

Least Privileged Access

Just in time just enough
access

Understanding Access Packages



- Teams
- Groups
- Applications
- SharePoint sites
- Entra Roles
- API Permissions

Access Package + Approval



- Periodic reviews
- Self-review
- Recommendations

Access Review

Policies

Who can request?

- Members and/or guests

Assignments

- Admin assignment (manual)
- On demand (user can request)
- Dynamic assignment (attribute based)



Catalogs

Group resources for:

- Delegation to key users in your org
- Governance (visibility and protection for guests)

Custom Extensions for:

- Pre-expiration workflow
- Request workflow

Note: Moving access packages between catalogs isn't possible!



Separation of Duties



Deny access based on:

- Current group membership
- Incompatible Access Packages

Examples:

- Update rings (Fast vs. Slow ring)
- License groups

Custom Extensions

Create a custom extension ...

Basics Extension Type Extension Configuration Details Review + create

Custom extensions are created to be paired to specific policy types within the access package governance workflow.

Select to which type of workflow you will be pairing this custom extension:

- Request workflow (triggered when an access package is request, approved, granted or removed)
- Pre-Expiration workflow (triggered when an access package assignment has 14 days till expiry or 1 day till expiry)

- Pre-Expiration workflow (triggered when an access package assignment has 14 days till expiry or 1 day till expiry)
- Request workflow (triggered when an access package is request, approved, granted or removed)



Created in Catalog



Linked to a logic app



Use app authorization for security



Request Workflow type
(Created, Approved, Granted or removed)

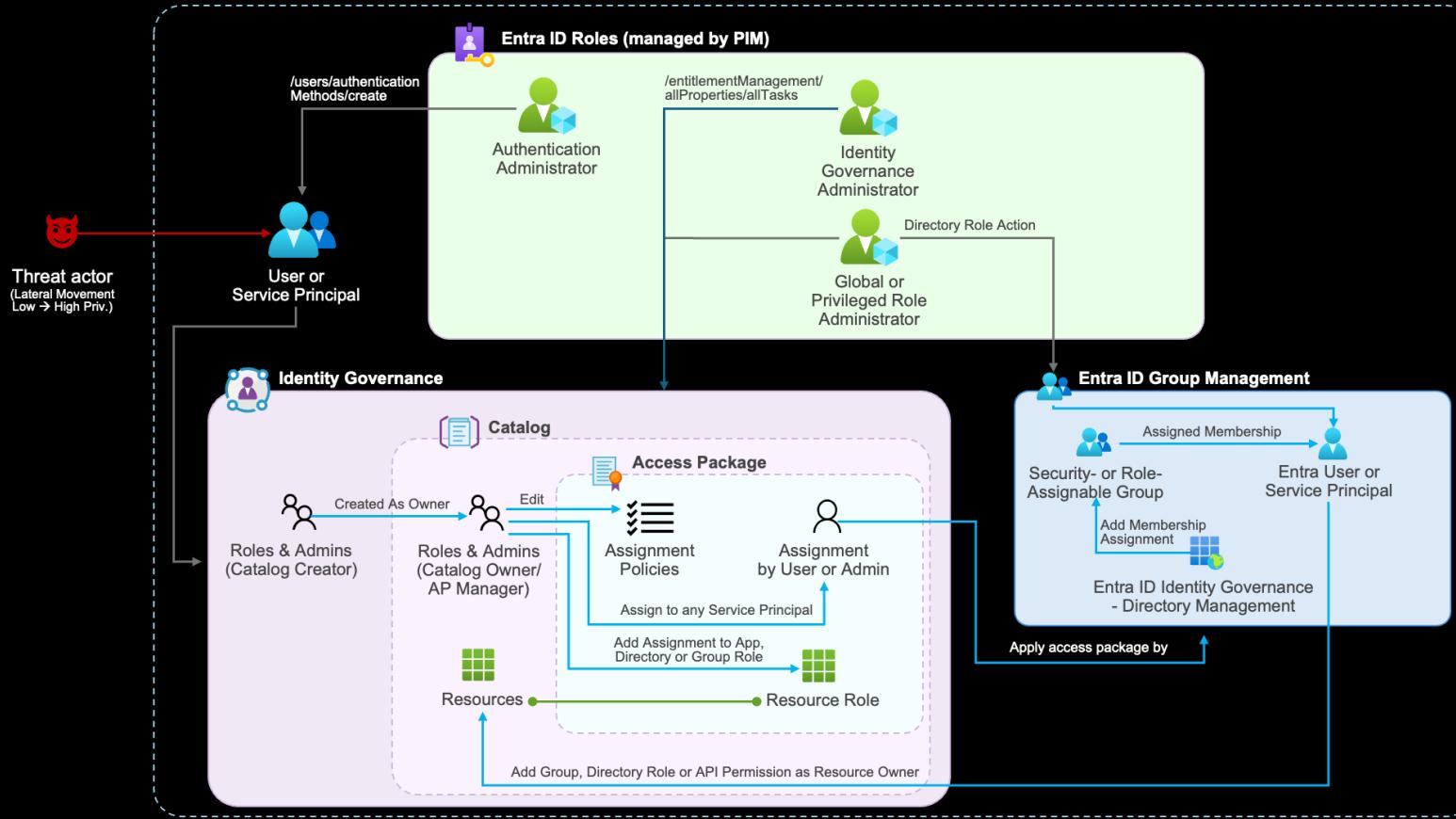


Pre-Expiration Workflow
(1 or 14 days)



Fire and Forget or Fire and Wait

ELM Delegation and Attack Paths



ELM Settings for Hardening

Home > Identity Governance

Identity Governance | Preview Features

Save Cancel

Home > Identity Governance

Identity Governance | Control c

Entitlement management

- Dashboard
- Getting started
- Diagnose and solve problems

Access packages

- Catalogs
- Connected organizations
- Reports
- Control configurations
- Preview Features
- Roles and administrators (Preview)

Risk-based approval (Preview)

Configure approval settings for risky users.

Require approval for users with insider risk level (Preview) ⓘ

Require approval for users with ID protection risk (Preview) ⓘ

When enabled, users with insider risk level will need additional access package approval. [Customize](#)

When enabled, users with Entra ID Protection risk level will need additional access package approval. [Customize](#)



D E M O

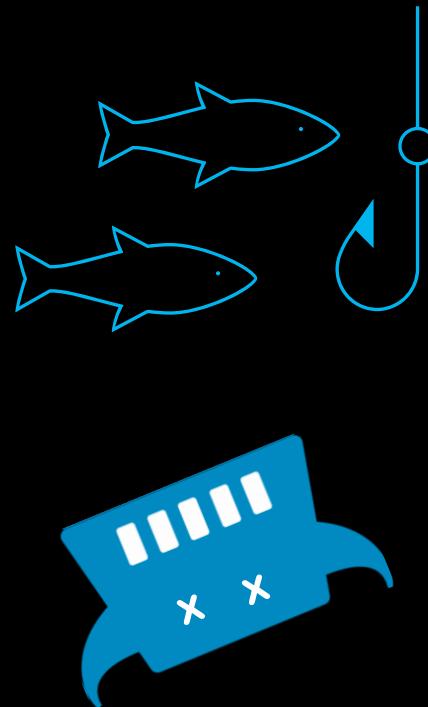
LAB 2: Access Management – Entra ID Governance

<https://aka.ms/eldk26>





Phishing Resistant





How passkeys work (Registration)

Authenticator



PIN or
Biometrics

RP ID Priv Pub

Contoso.com



Client

I want to create a new passkey for
user A

Sure, here's a challenge

Here's the public key and the origin
challenge

I've linked the public key to **user A**.
See you next time!

Relying Party



User Pub

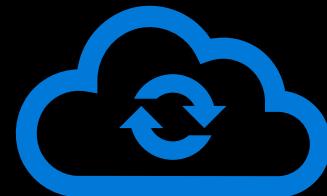
User A



Device-bound or Synced Passkeys

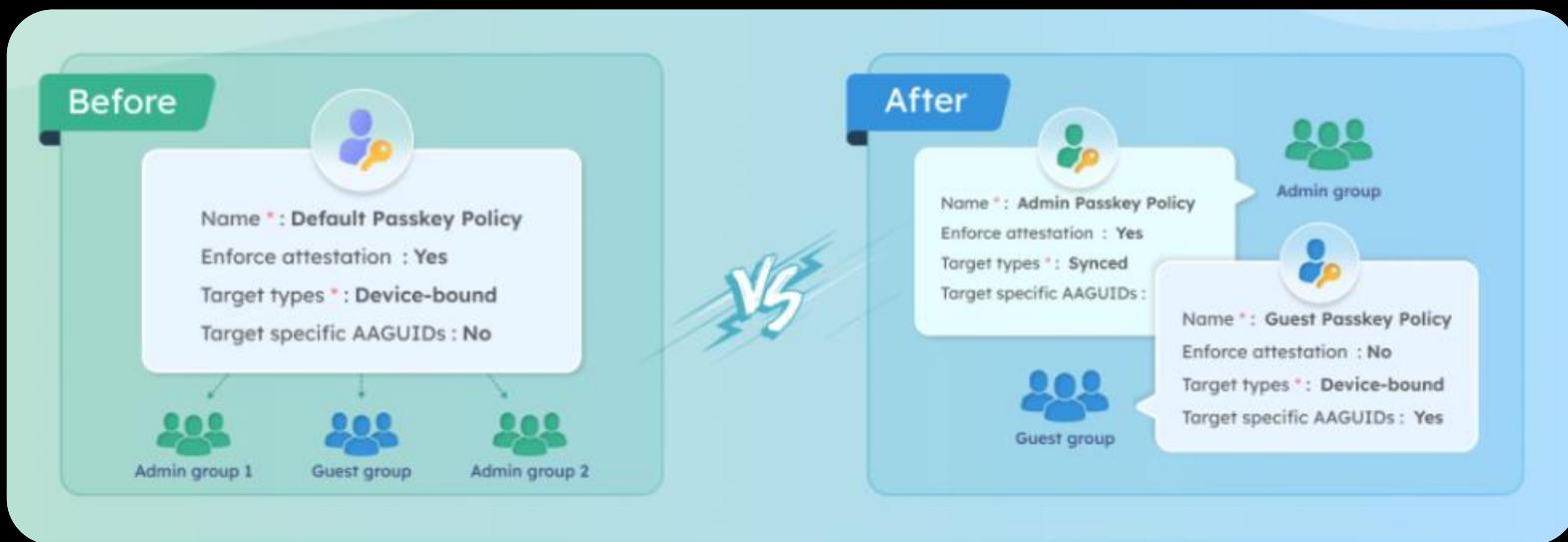


Device-bound passkeys



Synced passkeys

Passkey Profiles



Steps to enable Passkeys in Microsoft Entra ID

- 

Gather list of AAGUIDs of current passkeys (security keys) in Microsoft Entra
- 

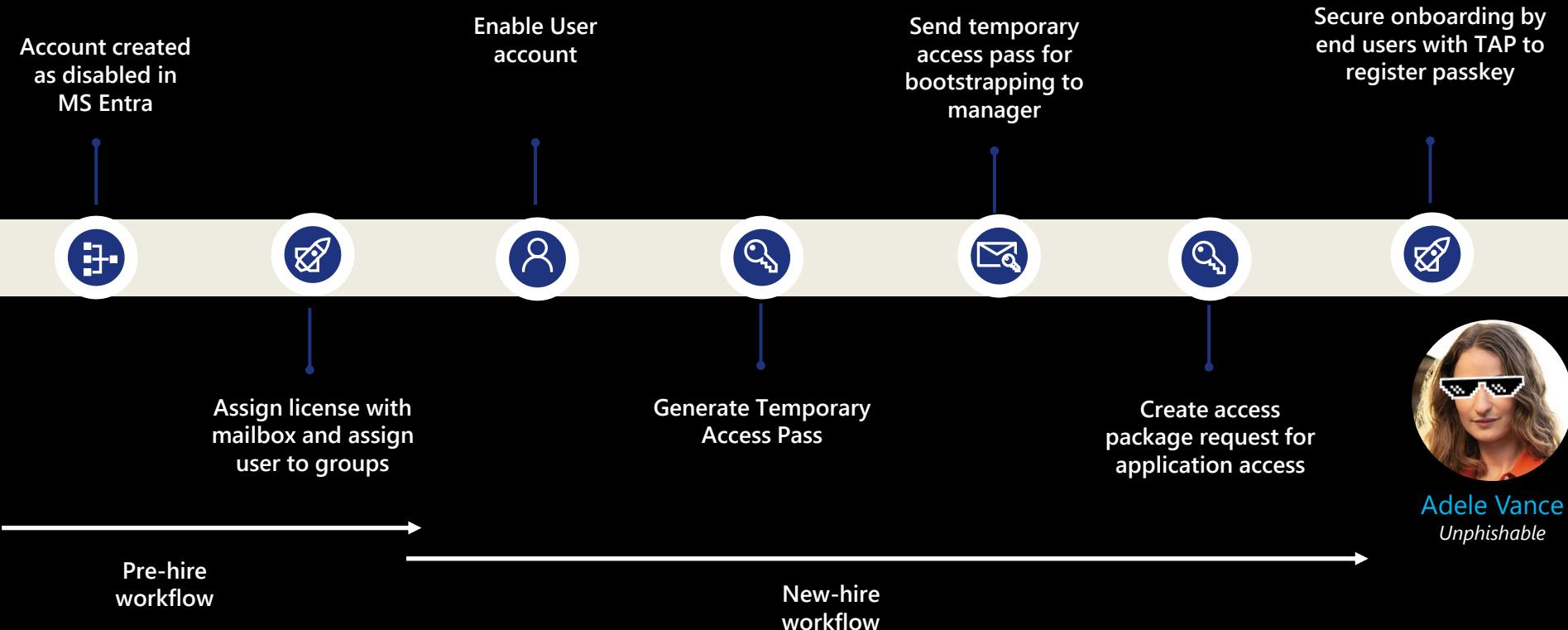
Determine scope for Passkey enrollment
- 

Enable Passkeys Authentication Method in Microsoft Entra
- 

Configure passkey profiles (example: device-bound for admin, synced for regular users)
- 

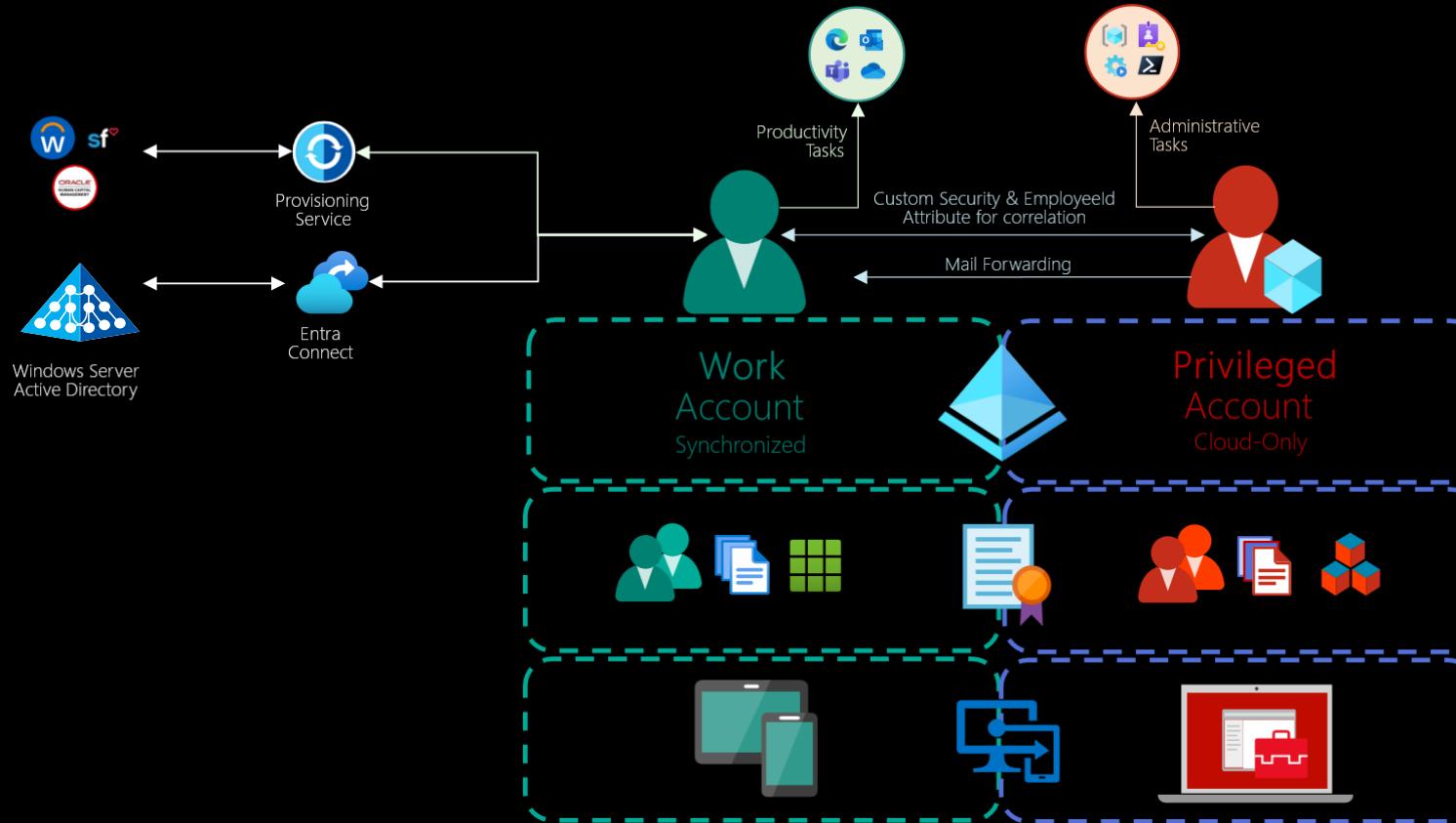
Provide adoption materials to end users!

Onboarding example

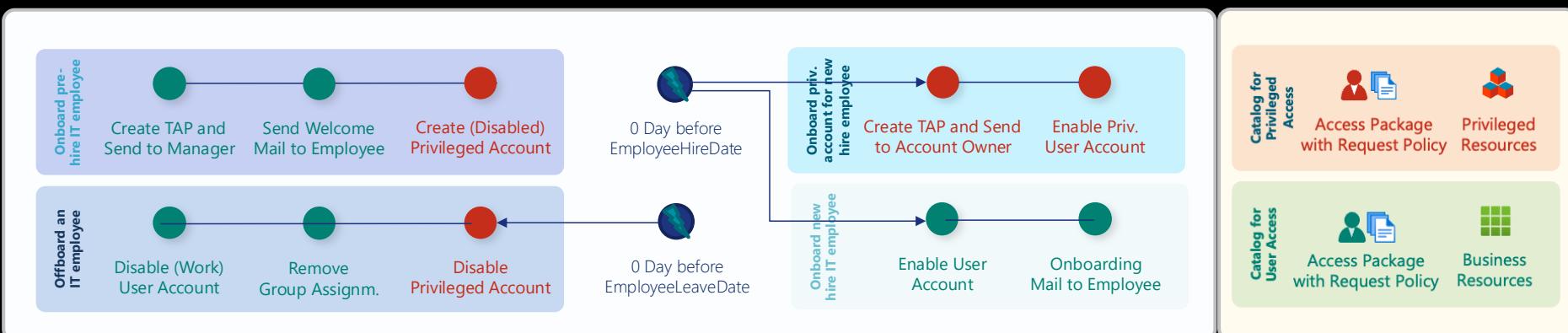
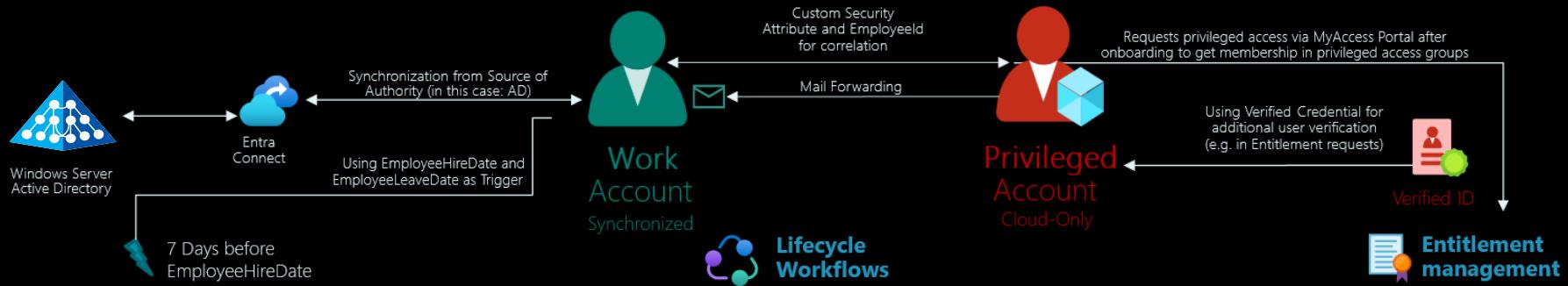


Privileged User Lifecycle Story

Work and Privileged Account Separation



Privileged Account Lifecycle Workflow



Options for Privileged Account Provisioning



Lifecycle Workflows and Custom Logic App

Advantage: Direct automation and linkage to the lifecycle of the "work account".

Disadvantage: Requires a filter/condition; requires an Entra ID Governance P2 license.



Access Package and Custom Extension (Logic App)

Advantage: Flexibility and process control for the provisioning of admin accounts.

Disadvantage: A request is required; the offboarding trigger must be implemented separately.

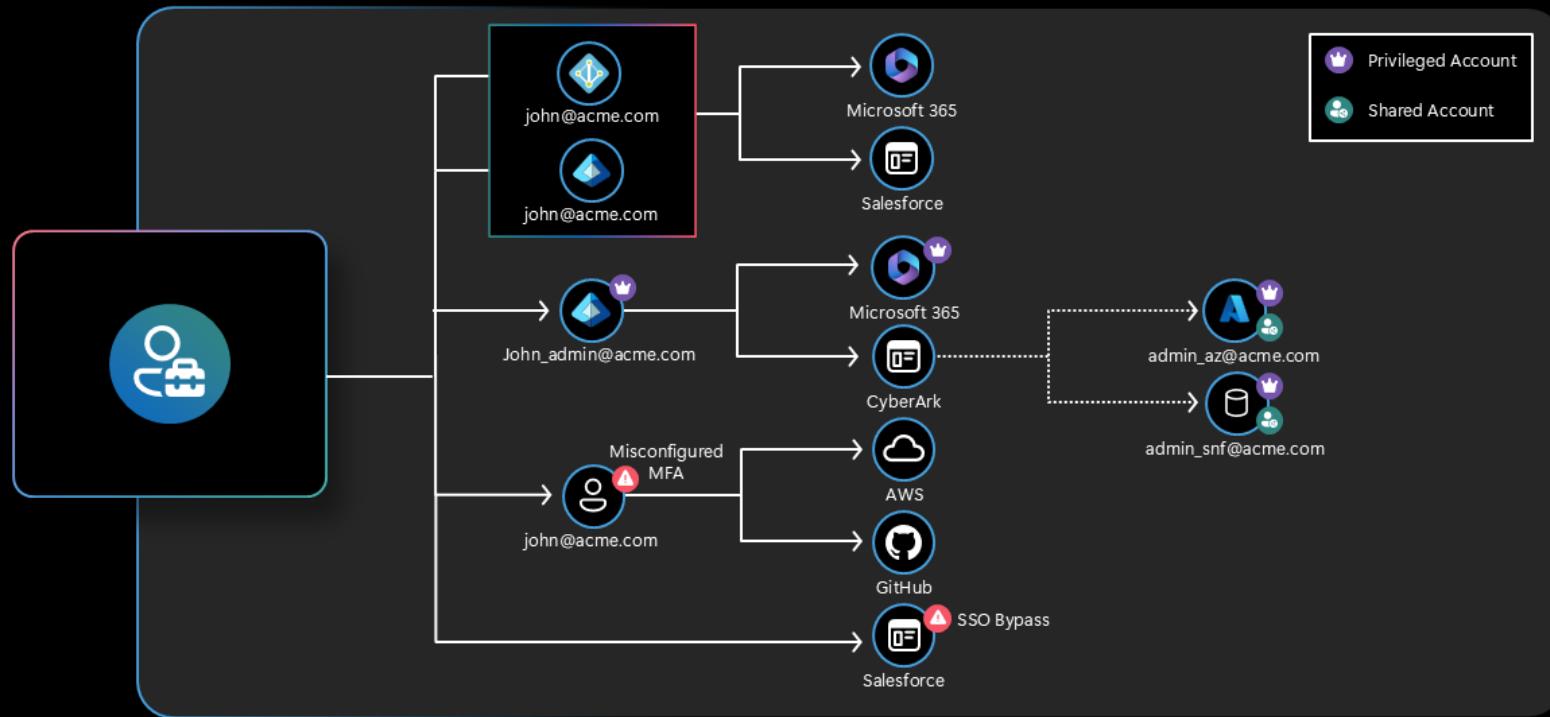


API-driven inbound provisioning with **Logic App, PowerShell or other low-code client**

Advantage: High flexibility, a fully featured sync process with direct data source integration

Disadvantage: Effort required for customization and integration of the API client.

Linked Identities in Defender XDR





D E M O

LAB 3: Privileged Accounts

<https://aka.ms/eldk26>



Securing Privileged Access

Golden Rules for Privileged IAM



Separation of User Accounts

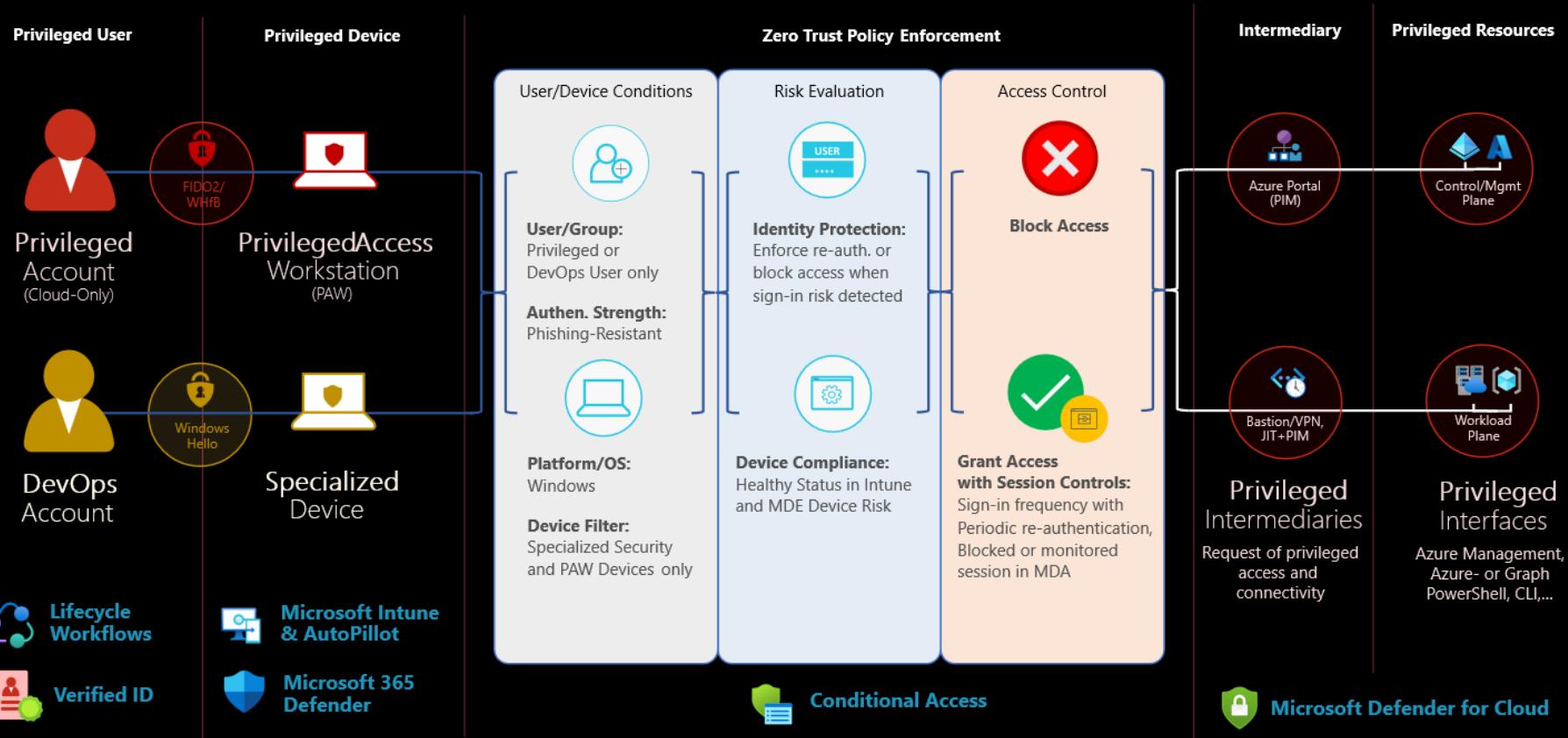
Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.



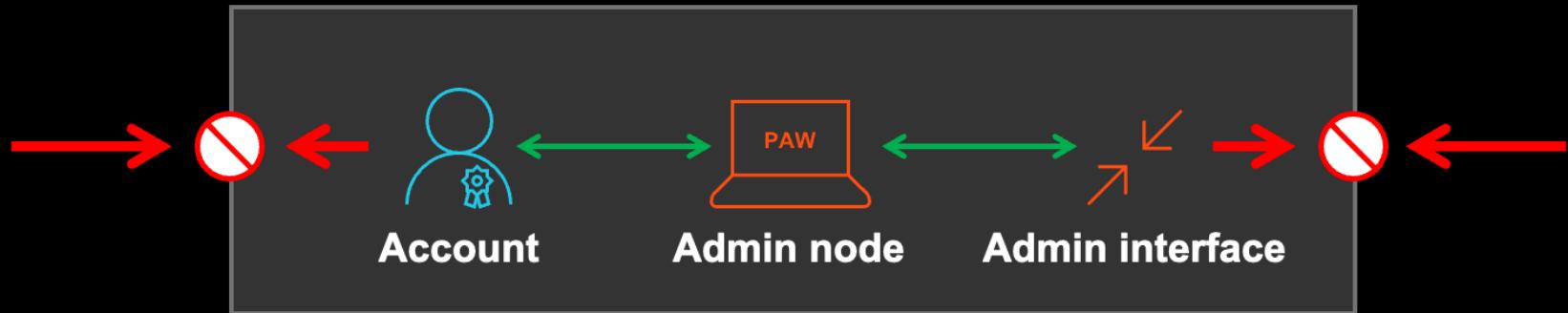
Strong Security Policies

Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.

Strong CA Policies for Privileged Users



Foundation of Privileged Endpoints



Comparison of Virtualized vs. Physical PAW

Criteria

 **Security Model**

 **Usability**

 **Deployment**

 **Cost Strategy**

 **Connectivity**

 **Maintenance**

 **Ideal Use Case**

Physical PAW (Hardware)

Hardware Isolation: Zero reliance on host OS integrity; physical separation protects against host-level malware.

Low: Requires carrying two distinct physical laptops

Dependencies: Procurement, shipping (days/weeks)

CAPEX High: Expensive bespoke hardware, shipping, and replacement costs.

Hybrid/Offline: Can work offline for local AD/Datacenter admin tasks.

High Touch: Firmware updates, battery swelling, physical repairs require swaps.

IAM Platform, Zero Trust and Privilege Access Management, PKI-Infrastructure

Virtual "PAW" (Windows 365)

Logical Isolation: Relies on the security of the hosting device, vulnerable if the access point is compromised.

High: Access secure admin desktop from standard productivity device.

Instant: Automated provisioning via Intune/Windows 365 portal (minutes/hours).

OPEX Predictable: Fixed monthly license per admin; uses existing physical hardware.

Online Only: Requires stable internet; unusable without connectivity.

Zero Touch: Microsoft manages backend; "Reprovision" feature resets environment instantly.

Azure Platform (exclude Control Plane or Root Scope) and Workloads

Golden Rules for Privileged IAM



Separation of User Accounts

Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.



Strong Security Policies

Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.



Restricted Delegation

Use “Restricted Management Administrative Units” and/or role-assignable groups to limit access to privileged objects.



Tiered Administration

Create a clear classification of sensitive roles and their scopes to segment administrative access areas.

Quiz: Who wants to be Control Plane?



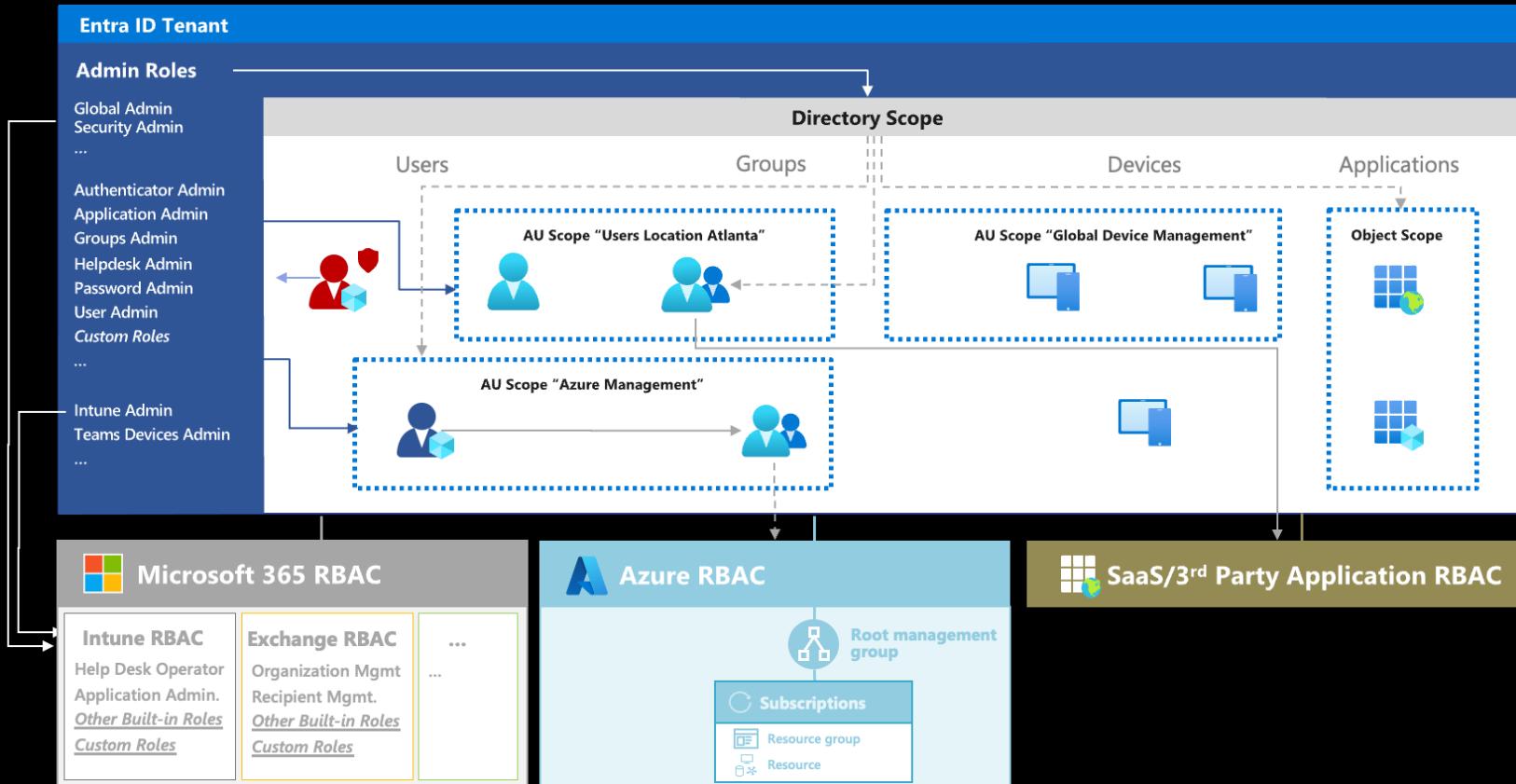
WHICH OF THESE DIRECTORY ROLES ARE TIER0?



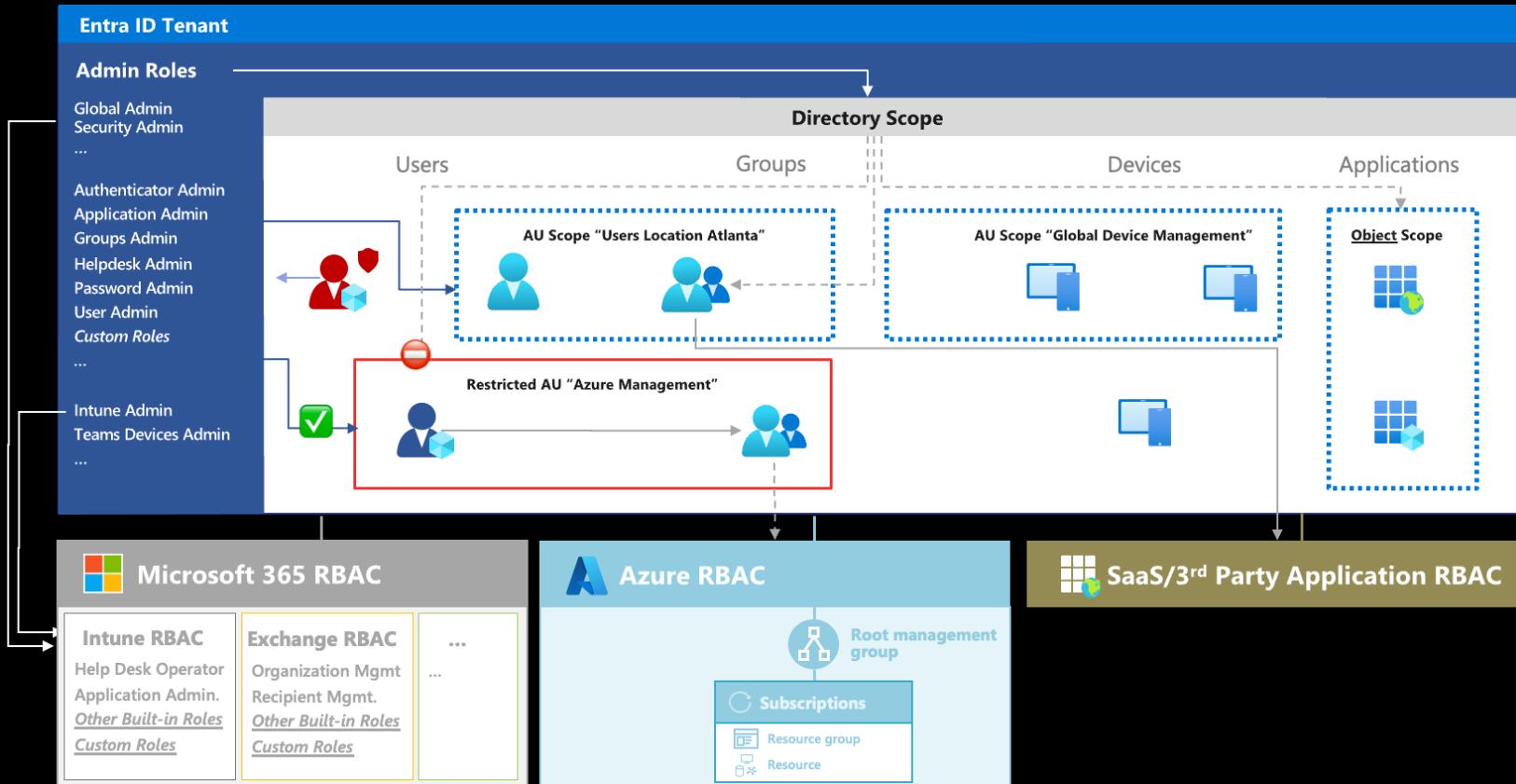
"It Depends"

- A. Authenticator Administrator
- B. Cloud Application Administrator
- C. Groups Administrator
- D. User Administrator

Delegation on Directory or AU-Level scope



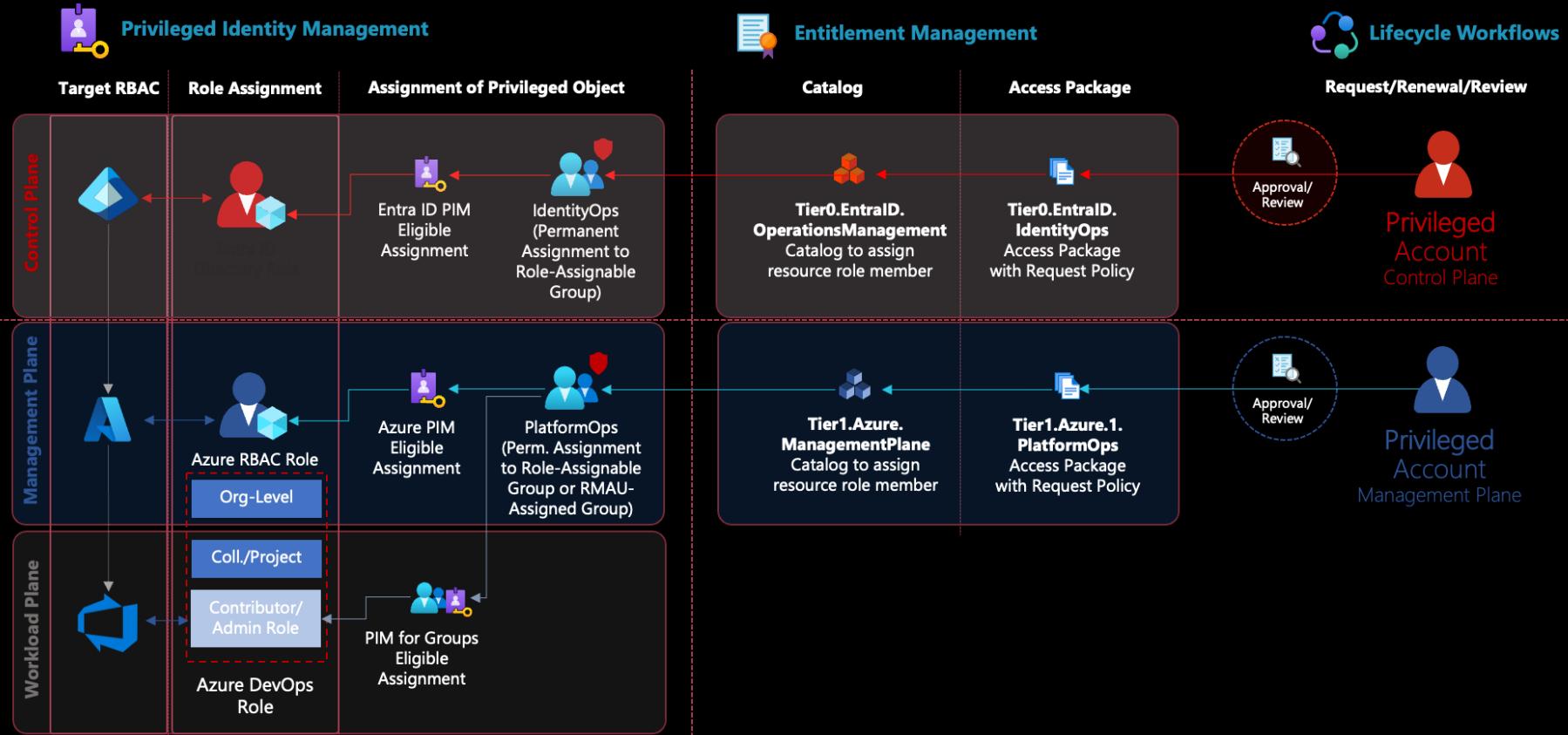
Delegation on Directory or AU-Level scope



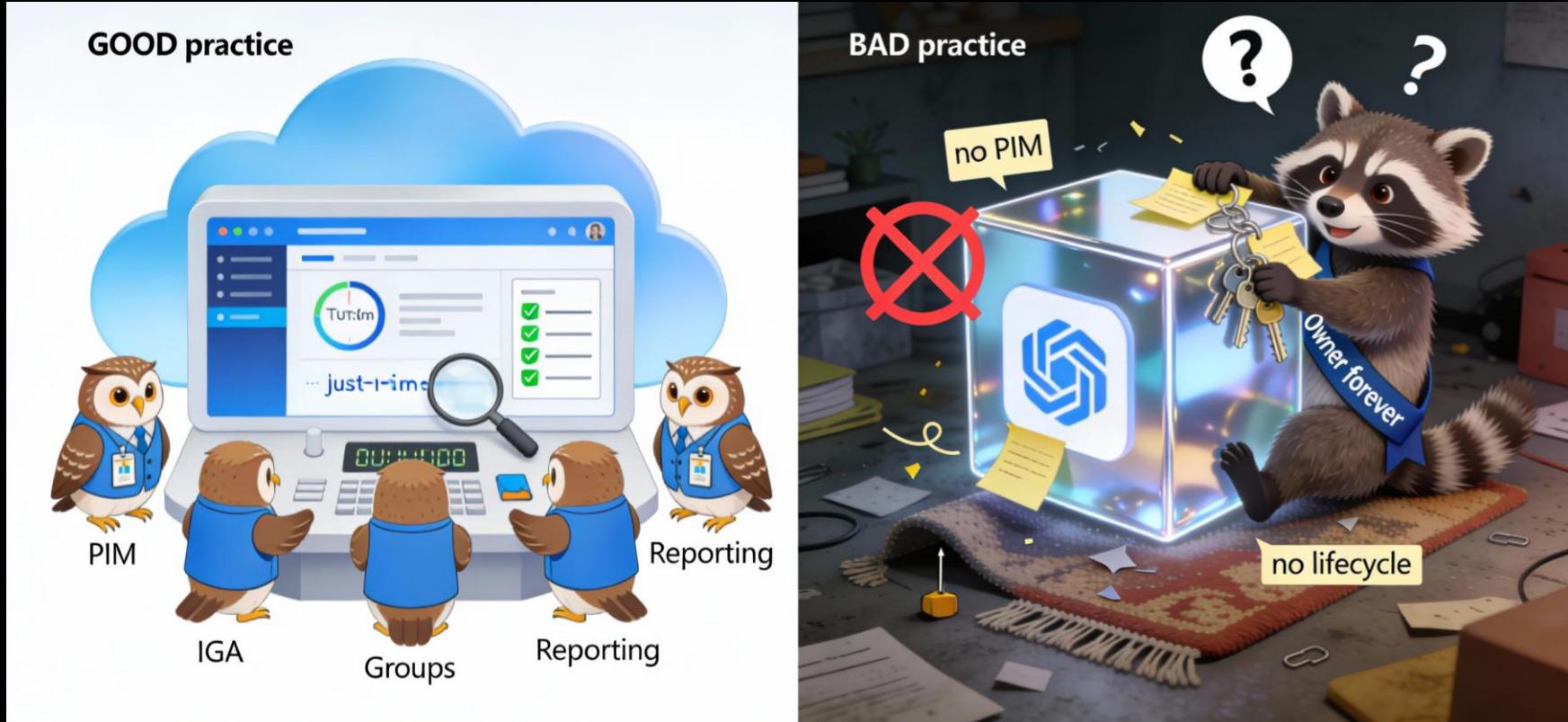
Types of Groups and Protection Capabilities

	Restricted Management by High-Privileged Roles	Restriction applies to group members	Support for Identity Governance	Preferred use case/scenario
Security Group without PIM	✗ No restriction on directory-scoped roles or object owners	✗ No restriction	✓ Assignment by Access Packages	Assignments to "User Access" when avoiding directory-level delegations

Delegation of Control/Management Plane



Delegation by Roles vs. Ownership



Role Actions by Condition "IsOwner"

```
"microsoft.directory/applications/appRoles/update",
"microsoft.directory/applications/credentials/update",
"microsoft.directory/applications/delete",
"microsoft.directory/applications/owners/update",
"microsoft.directory/applications/permissions/update",
"microsoft.directory/deletedItems.applications/delete",
"microsoft.directory/deletedItems.applications/restore",
"microsoft.directory/deletedItems.groups/restore",
"microsoft.directory/devices/disable",
"microsoft.directory/groupsAssignableToRoles/allProperties/update",
"microsoft.directory/groupsAssignableToRoles/delete",
"microsoft.directory/groupsAssignableToRoles/restore",
"microsoft.directory/groups/delete",
"microsoft.directory/groups/groupType/update",
"microsoft.directory/groups/members/update",
"microsoft.directory/groups/owners/update",
"microsoft.directory/groups/restore",
"microsoft.directory/policies/basic/update",
"microsoft.directory/policies/delete",
"microsoft.directory/policies/owners/update",
"microsoft.directory/servicePrincipals/appRoleAssignedTo/update",
"microsoft.directory/servicePrincipals/basic/update",
"microsoft.directory/servicePrincipals/credentials/update",
"microsoft.directory/servicePrincipals/delete",
"microsoft.directory/servicePrincipals/owners/update",
"microsoft.directory/servicePrincipals/permissions/update",
..."
```

Golden Rules for Privileged IAM



Separation of User Accounts

Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.



Strong Security Policies

Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.



Restricted Delegation

Use “Restricted Management Administrative Units” and/or role-assignable groups to limit access to privileged objects.



Tiered Administration

Create a clear classification of sensitive roles and their scopes to segment administrative access areas.



Review and Monitoring

Regularly review assigned, eligible, and active permissions to detect anomalies, outdated permissions, or misuse.

PIM Alerts

Microsoft Entra admin center Search resources, services, and docs (G+/-) Copilot thomas@cloud-architek... CLOUDLAB (CLOUD-ARCHITEK...)

Home > Browse > Identity Governance | Microsoft Entra roles > Privileged Identity Management > CloudLab | Alerts >

Alert settings

Privileged Identity Management | Microsoft Entra roles

Alert

- The organization doesn't have Azure AD Premium P2
- Roles don't require multi-factor authentication for activation
- Eligible administrators aren't activating their privileged role
- Roles are being assigned outside of Privileged Identity Management
- Roles are being activated too frequently
- There are too many global administrators
- Potential stale accounts in a privileged role

Microsoft Entra admin center Search resources, services, and docs (G+/-) Copilot thomas@cloud-architek... CLOUDLAB (CLOUD-ARCHITEK...)

... > Privileged Identity Management > CloudLab | Alerts >

Alert detail - Eligible administrators aren't activating their privileged role

Privileged Identity Management | Microsoft Entra roles

Fix Dismiss

Why am I getting this?
4 user(s) haven't activated their privileged roles in the past 30 days
[Learn more about this alert](#)

How do I fix this?
Review the users in the list and remove them from privileged roles they do not need.

Can I prevent this? (Recommended)
-Assign privileged roles to users that have a business justification. -Schedule regular access reviews to verify that users still need their access.

Name	User Principal Name	Role Name	Last Activation On	Status
Thomas Naunheim	thomas@cloud-architekt.net	Cloud Application Administrator		
Thomas Naunheim	thomas@cloud-architekt.net	Cloud Application Administrator		
Thomas Naunheim	thomas@cloud-architekt.net	Hybrid Identity Administrator	1/9/2024, 6:39:53 AM	
Adele Vance	adeley_c4a8ando.net#EXT#@clou...	Attack Payload Author		
admMOB1	admMOB1@lab.cloud-architekt.net	Attack Payload Author		
Thomas Naunheim	thomas@cloud-architekt.net	AI Administrator		
Montgomery Scott	scotty@corp.cloud-architekt.net	Cloud Application Secret Manager	12/16/2025, 7:29:05 AM	

KQL function for Privileged Access Hunting

UnifiedIdentityInfoXDR

TimeGenerated ▾	AccountObjectId ▾	AccountDisplayName ▾	AccountStatus ▾	Type ▾	CriticalityLevel ▾	CriticalAssetDetails ▾	Classification ▾	AssignedAzureRoles ▾
AccountDisplayName	admThom0-B2C							
AccountStatus	Enabled							
Type	User							
CriticalityLevel	0							
› CriticalAssetDetails	[{"CriticalityLevel": "0", "RuleName": "B2C Resources"}]							
Classification	ControlPlane							
› AssignedEntraRoles	[{"RoleDefinitionName": "Cloud Application Administrator", "RoleAssignmentType": "Indirect", "PimAssignmentType": "Eligible", "PimAssignmentExpiration": "NoExpiration", "Classification": "ControlPlane", "RolesPrivileged": true}]							
› 0	{"RoleDefinitionName": "Cloud Application Administrator", "RoleAssignmentType": "Indirect", "PimAssignmentType": "Eligible", "PimAssignmentExpiration": "NoExpiration", "Classification": "ControlPlane", "RolesPrivileged": true}							
RoleDefinitionName	Cloud Application Administrator							
RoleAssignmentType	Indirect							
PimAssignmentType	Eligible							
PimAssignmentExpiration	NoExpiration							
Classification	ControlPlane							
RolesPrivileged	true							
RoleCategories	identity							
› RolePermissions	[{"AuthorizedResourceAction": "microsoft.directory/adminConsentRequestPolicy/allProperties/allTasks", "Category": "Application and Workload Identity", "EAMTierLevelName": "ControlPlane", "EAMTierLevelTagValue": null}]							

KQL function for Privileged Access Hunting

Run query Last 30 days Save Share link Create summary rule Create detection rule

Query

```
10 UnifiedIdentityInfoXdr()
11 | extend ParsedRoles = parse_json(AssignedEntraRoles)
12 | mv-expand Role = ParsedRoles
13 | mv-expand Permission = Role.RolePermissions
14 | where Permission.AuthorizedResourceAction has 'microsoft.directory/conditionalAccessPolicies/basic/update'
15 | where RiskLevel != "None" and RiskStatus == "AtRisk"
16 | summarize MatchingRoles = make_list(Role) by AccountObjectId, AccountUpn, RiskStatus, RiskLevel, RiskLevelDetails
```

Getting started Results Query history

Export Show empty columns 1 item Search 00:05.682 Low Chart type Full screen

Filters: Add filter

AccountObjectId	AccountUpn	RiskStatus	RiskLevel	RiskLevelDetails	MatchingRoles
0e1e6c34-9d5c-4	thomas@cloud-architekt.net	AtRisk	Medium	None	[{"RoleDefinitionName": "Security Administrator", "RoleAssignmentType": "Direct", "PimAssignmentType": "Active", "PimAssignmentExpiration": "NoExpiration", "Classification": "ControlPlane", "Ro..."}]
AccountObjectId	0e1e6c34-9d5c-4b24-bba6-aafb0995a6e0				
AccountUpn	thomas@cloud-architekt.net				
RiskStatus	AtRisk				
RiskLevel	Medium				
RiskLevelDetails	None				
MatchingRoles	0				[{"RoleDefinitionName": "Security Administrator", "RoleAssignmentType": "Direct", "PimAssignmentType": "Active", "PimAssignmentExpiration": "NoExpiration", "Classification": "ControlPlane", "Ro..."}]

Golden Rules for Privileged IAM



Separation of User Accounts

Ensure that administrative (privileged) accounts are separated from standard user accounts to prevent the risk of compromise, for example, through internet and email access.



Strong Security Policies

Enforce phishing-resistant authentication, device compliance, and filtering to allow access to privileged interfaces only from authorized endpoints.



Restricted Delegation

Use “Restricted Management Administrative Units” and/or role-assignable groups to limit access to privileged objects.



Tiered Administration

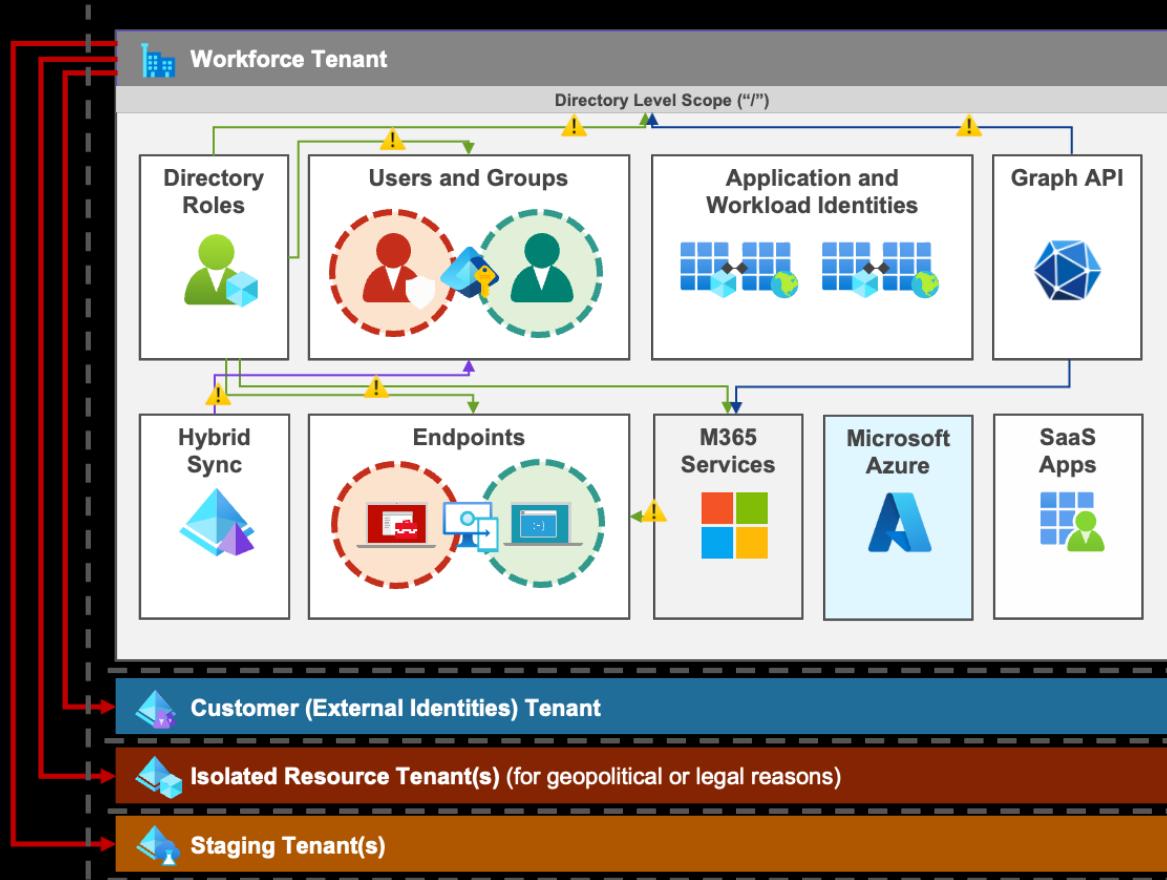
Create a clear classification of sensitive roles and their scopes to segment administrative access areas.



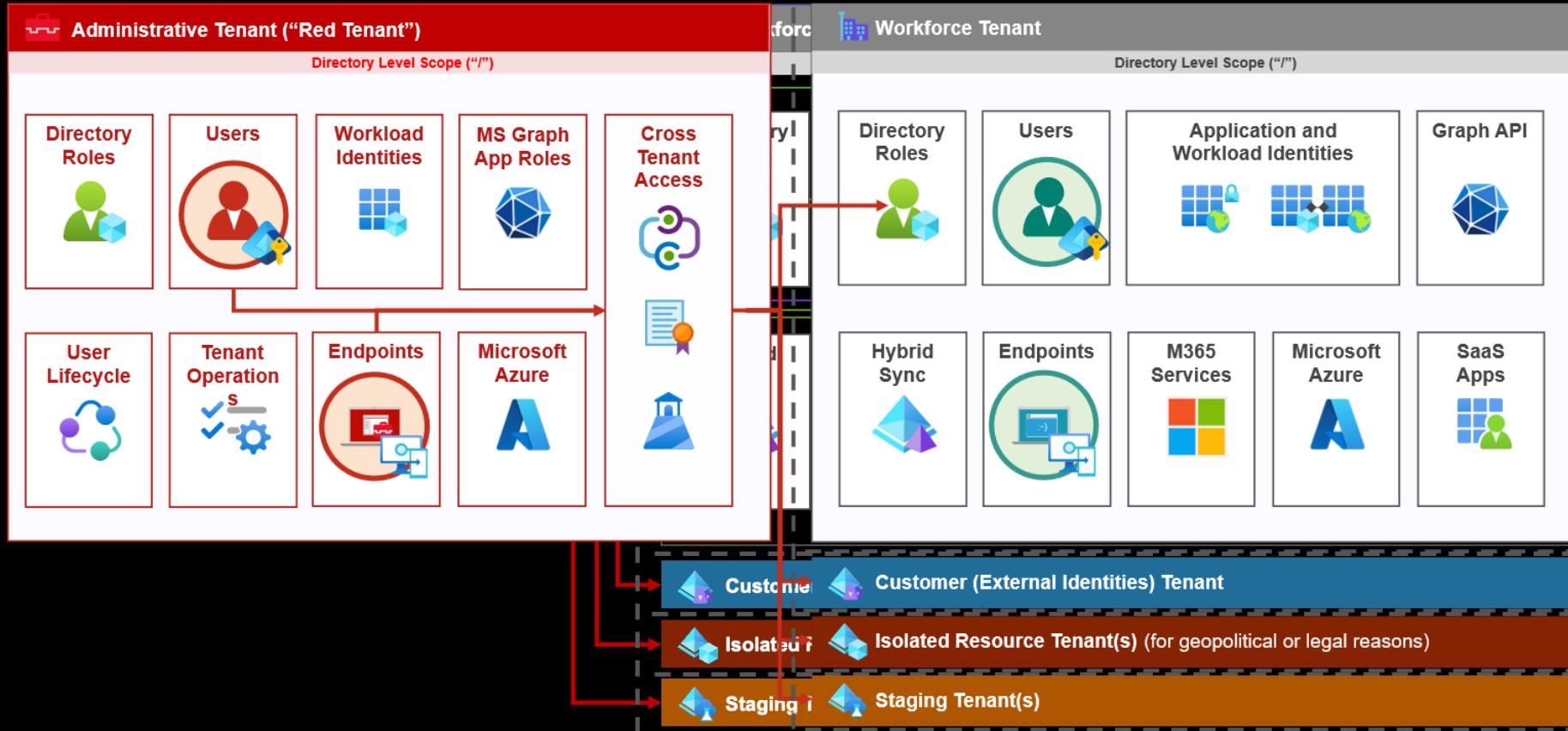
Review and Monitoring

Regularly review assigned, eligible, and active permissions to detect anomalies, outdated permissions, or misuse.

Intra-Tenant Isolation



Inter-Tenant Isolation with Red Tenant





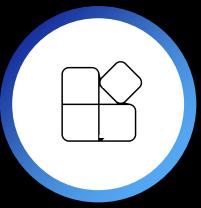
Securing agentic AI using Microsoft Entra Agent ID



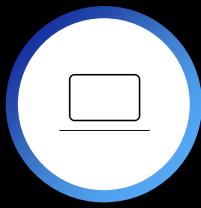
Agents are a new type of identity



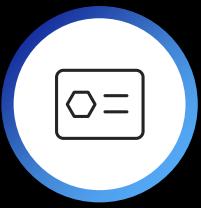
User



App



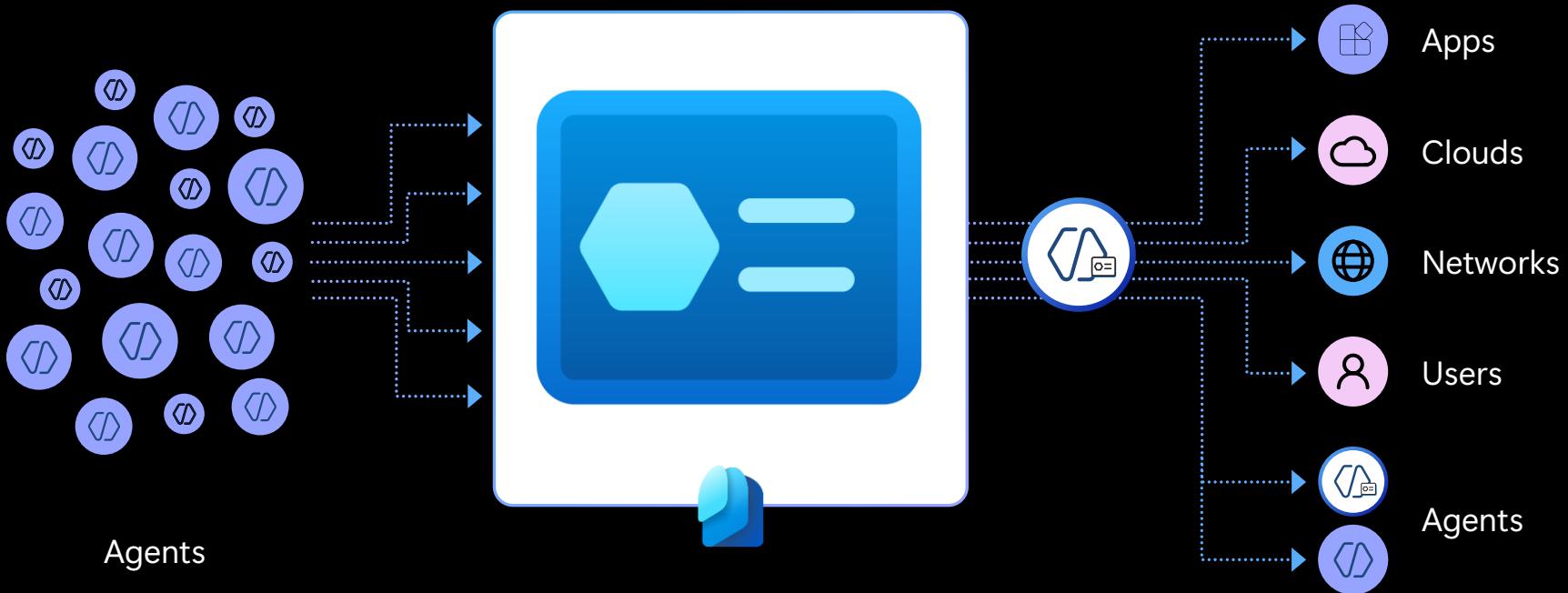
Device



Agent

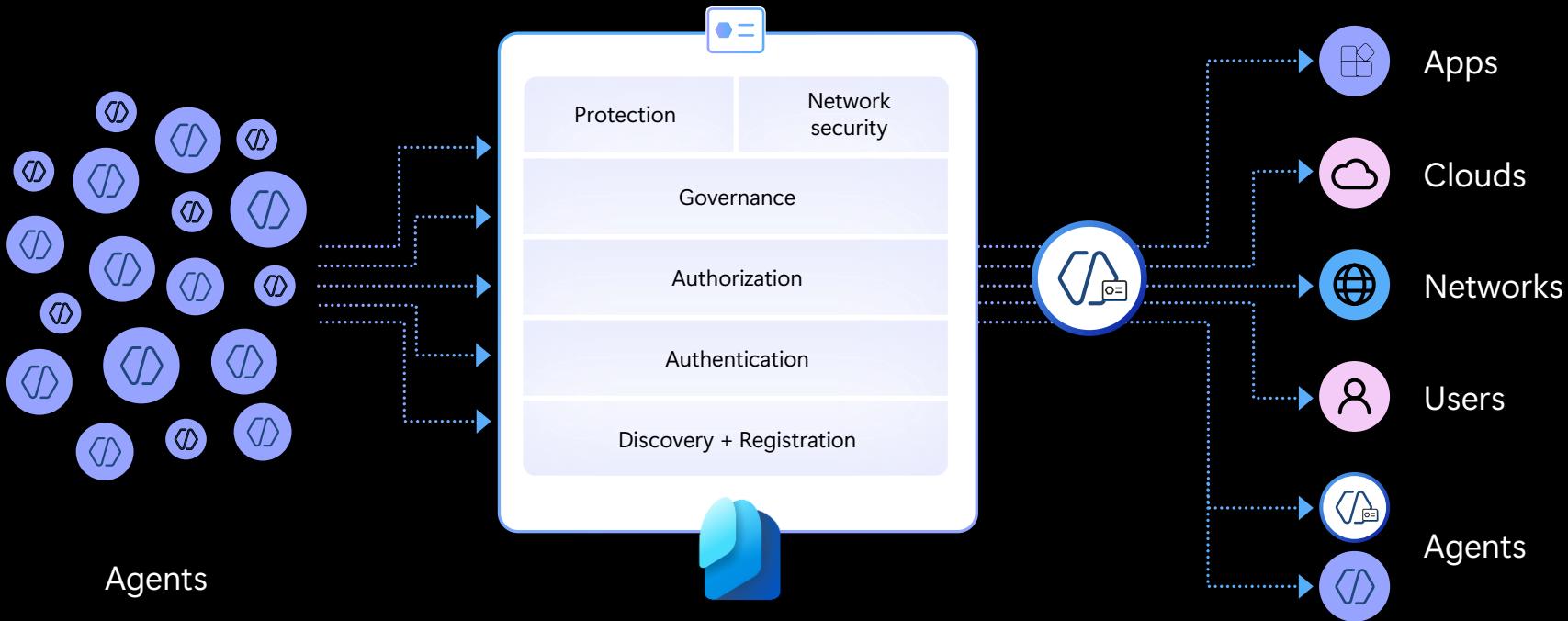
Microsoft Entra Agent ID

Secure access for AI agents - just as you do for employees - with enterprise-grade access management, protection, and governance of agent identities.



Microsoft Entra Agent ID

Secure access for AI agents - just as you do for employees - with enterprise-grade access management, protection, and governance of agent identities.



Public Preview

Microsoft Entra Agent ID

Secure access for AI agents

Register and
manage agents

Govern agent
identities and
lifecycle

Protect agent
access to resources

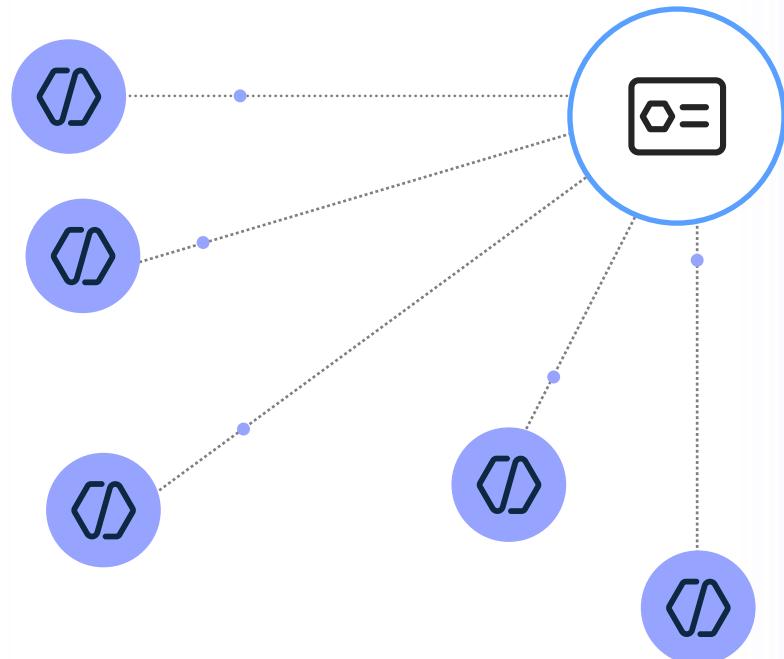
aka.ms/EntraAgentID



Register and manage agents

Get a complete inventory of your agent fleet and ensure agents are created with a built-in identity.

- Gain visibility into agents in your environment.
- Ensure that new agents have an agent ID built-in.
- Empower developers to build enterprise-ready agents.



[Register](#)[Govern](#)[Protect](#)

Unify agents in a registry

Discover and bring all agents
under management with
IT-defined guardrails using
agent collections.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Home, Entra agents, Favorites, and Agent ID. Under Agent ID, 'Agent registry' is selected. The main area is titled 'Agent ID | Agent registry' and shows a list of 6,053 items. The columns in the table are Name, Registry ID, Platform, Has Agent ID, and Source ID. Each row contains a small icon, the agent name, its unique ID, the platform it runs on, whether it has an agent ID (indicated by a red or green dot), and the source ID. There are also 'View more' links for some rows.

Name	Registry ID	Platform	Has Agent ID	Source ID
Image Recognition Agent	jpjg5qtp-hr5o-lq9s-me2r-le4l2n4p6...	PixelNova AI	No	default_05beb02-87cc-48e1-b4ab-7...
Inventory Management Agent	58b744c1-e3b9-4205-8016-dbc9194...	Adatum	No	ab9c6ad5-9da3-4610-bd2f-7db8de2c...
Procurement & logistics	microsoftCopilotStudio_05beb02-87...	Copilot Studio	Yes	default_bd1aeccb-6e88-41aa-90ab-e3...
Content Generation Agent	10314218-d541-48aa-a2c:e62e2ea6...	BrightMind Systems	No	default_b0e5327b-403b-49dd-9720-c...
HR Actions	microsoftAzureFoundry_088beb02-87...	Microsoft Foundry	Yes	783beb02-87cc-48e1-b4ab-784888ed...
Deal advisor	microsoftCopilotStudio_05beb02-87...	Copilot Studio	Yes	default_982beb02-87cc-48e1-b4ab-78...
Conditional Access Optimization Agent	bcecf3a5-8a8b-4b6b-87b5-bace1fb5...	Security Copilot	Yes	376bee-0f8-4345-982b-6e3bcea65...
Manus	0a52a0fb-5b3b-4ebc-b231-5cc98f7b...	Manus AI	Yes	95deb0cd-6d3d-441d-9ace-5b1c5be3...
HR self-service	microsoftCopilotStudio_05beb02-87...	Copilot Studio	Yes	default_675ref02-87cc-48e1-b4ab-784...
Finance optimizer	microsoftCopilotStudio_05beb02-87...	Copilot Studio	Yes	default_426117dc-2180-4057-9939-ae...
Zava Assist	microsoftAzureFoundry_088beb02-87...	Microsoft Foundry	Yes	29000fd4-b521-480b-8125-79293609...
Sales Forecasting Agent	84e24f35-bf19-4e39-b700-bbae2cc6...	FutureCast Labs	No	default_05beb02-87cc-48e1-b4ab-7...
Genspark Super	41d8d132-7546-4b9c-8589-f2a5d16...	Genspark	Yes	d6f078d6-feeb-4dd3-933d-e87573bc...
Test HR 123	microsoftCopilotStudio_05beb02-87...	Copilot Studio	Yes	default_05beb02-87cc-48e1-b4ab-78...

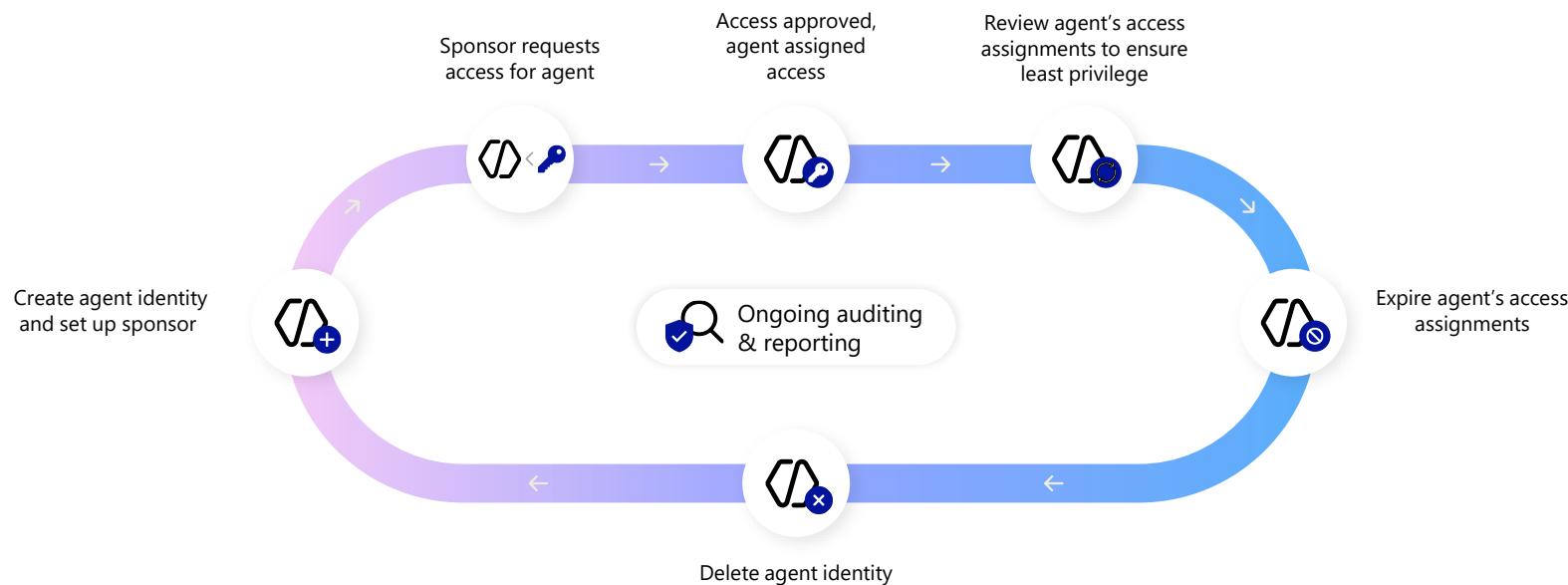
[Register](#)[Govern](#)[Protect](#)

Govern agent identities and lifecycle

Keep your agent fleet under control with lifecycle management and pre-defined guardrails.

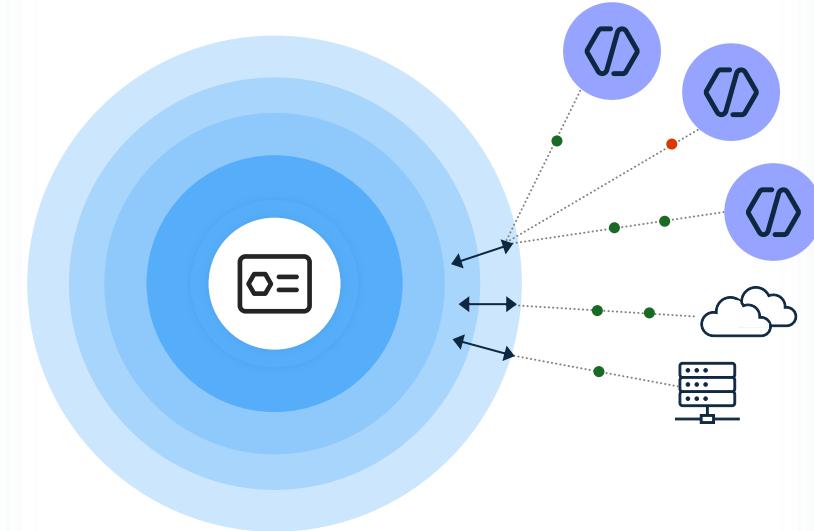


Automate agent identity lifecycle workflows



Protect agent access to resources

Reduce risk of breaches and prevent malicious agent access to resources.





Register

Govern

Protect

Apply Conditional Access for agents

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Agents, Favorites, and several sections under Entra ID such as Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access (which is selected), Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, External identities, Cross-federation synchronization, Entra Connect, Domain names, Custom branding, Mobility, and Monitoring & health.

In the center, a modal window titled "New Conditional Access policy" is open. It contains the following fields:

- Name:** Allow only approved agents to access resources.
- What does this policy apply to?** Set to "Agents (Preview)".
- Assignments:** Set to "All agent identities (Preview)".
- Target resources:** Set to "All resources (formerly All cloud apps)".
- Conditions:** 0 conditions selected.
- Access controls:** Set to "Grant".

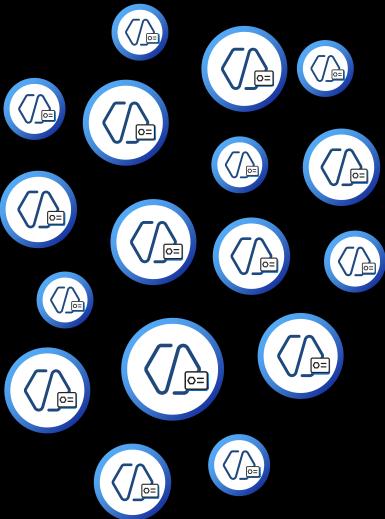
At the bottom of the modal, there is an "Enable policy" section with a "Report issue" dropdown set to "On" and a "Create" button.

To the right of the modal, a "Edit filter" sidebar is visible, showing the filter configuration:

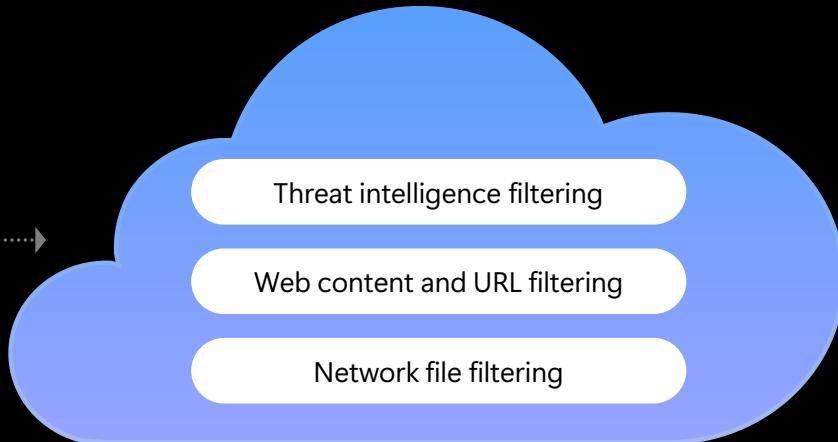
Configure	Attribute	Operator	Value
And/Or	AgentAttributes_AgentStatus	Equal	Approved

Below this, the rule syntax is shown as: `CustomSecurityIdentityAndAgentAttributes_AgentStatus == "Approved"`.

Safeguard agents with network controls



Microsoft Copilot
Studio agents

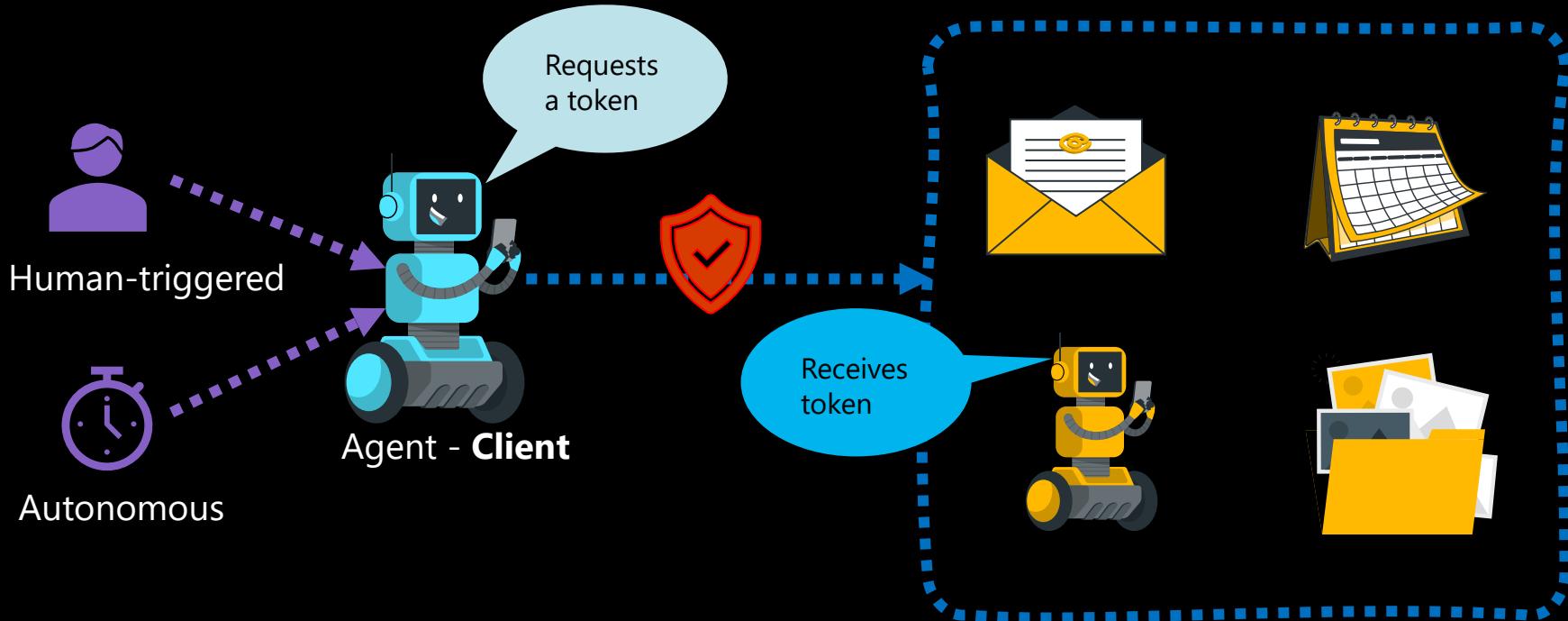


Protect agent access to resources



Agent Flows

Agent interaction patterns



■ **Client** an entity that access resources (with a security token)

■ **Resource** a service or system being accessed for the data

Resources

Agent Flows

Interactive Agent

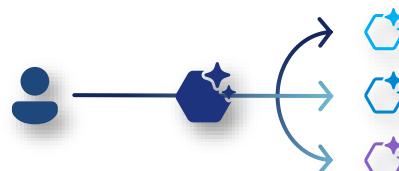
Single, specific, defined, repetitive tasks
"Summarize this email."



Acts on-demand on user's behalf

Autonomous Agent

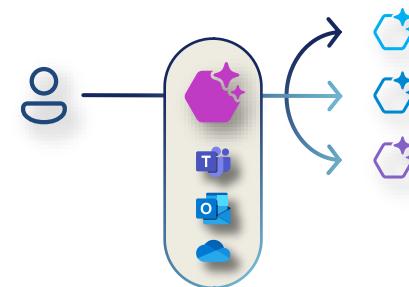
Complex, goal-oriented
Creates plans to achieve outcomes



Coordinates actions on user's behalf
and on user's schedule

Digital Colleague

Learning-driven
Emulates human decision making



Provisioned its own access and resources;
achieves goals on own behalf and schedule

On behalf of flow

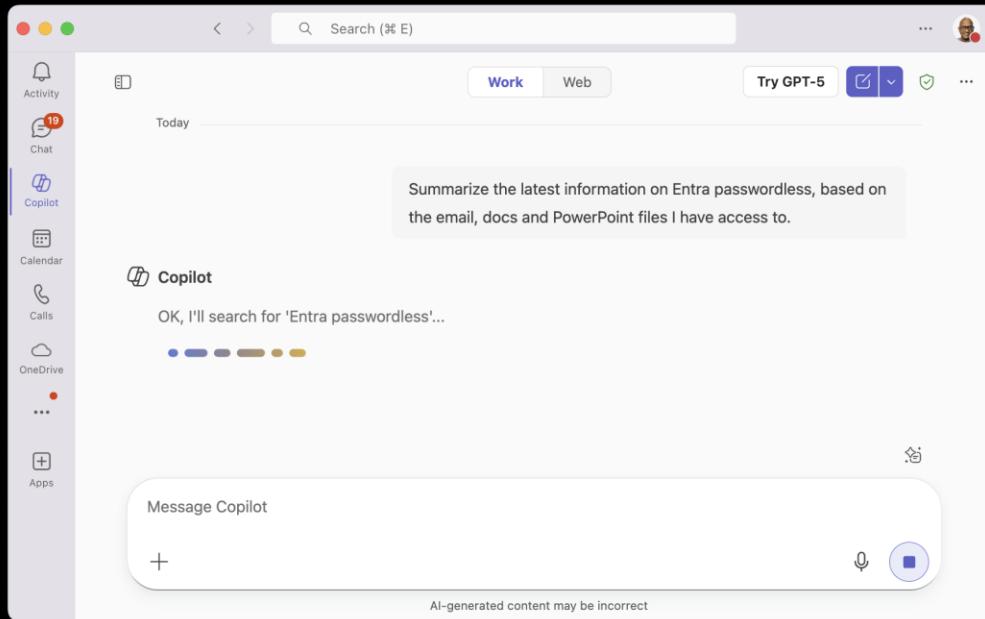
Autonomous App Flow

Agentic User Flow

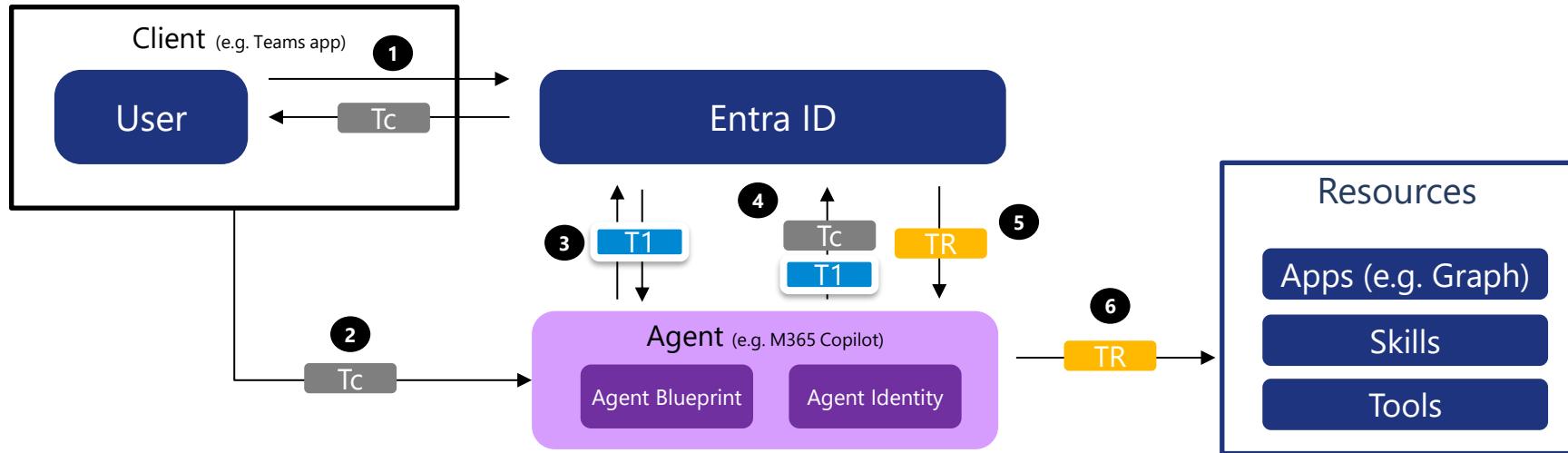
On behalf of flow - summary

Agent Identity operates on behalf of regular user

In the example below, M365 copilot Agent uses signed-in user's identity to make graph API calls on behalf of the user



On behalf of flow - diagram



1. User authenticates with the Client and obtains a User Access Token (**Tc**)
2. Client sends the User Access Token (**Tc**) to the Agent Blueprint to act on behalf of the user
3. Agent Blueprint requests a FIC Exchange Token (**T1**) from Entra ID using MSI, Entra ID returns the **T1** to Agent
4. Agent Identity sends an OBO token exchange request to Entra ID, including both **T1** and the User Access Token (**TC**)
 - $T_1.\text{Aud} == \text{AgentIdentity.ParentApp} == \text{Agent Blueprint}$
 - $T_C.\text{Aud} == \text{Agent Blueprint}$
5. Entra ID issues a Resource Access Token (**TR**) to the Agent Identity after validating both **T1** and **TC**
 - $T_1.\text{Aud} == \text{AgentIdentity.ParentApp} == \text{Agent Blueprint}$
 - $T_C.\text{Aud} == \text{Agent Blueprint}$
6. Agent Identity accesses the Resource using the Resource Access Token (**TR**)

Autonomous App flow - summary

The screenshot shows the Microsoft Entra admin center interface. On the left, the 'Condition Access Optimization Agent (Preview)' page is displayed. A red box highlights the 'Trigger' section, which says 'This agent runs every 24 hours.' An arrow points from this section to a yellow callout box at the bottom left that reads: 'Agent has its own identity and permissions and can run autonomously'. On the right, a modal window titled 'Add 15 users to policy' is open, showing a list of suggestions and a table of users added yesterday. Another red box highlights the 'Users' table, which lists several users with their names, email addresses, and dates added.

Microsoft Entra admin center

Home > Conditional Access | Agents >

Condition Access Optimization Agent (Preview)

Agent is available

The agent is next scheduled to run February 19, 2025 at 12:32 PM. ...

Trigger

This agent runs every 24 hours.

Recent suggestions

Suggestion Time generated

- Add 15 users to CA 3: MFA for Engineering New 12:43 PM, 2/1/2025
- Add 2 users to Device Compliance New 12:43 PM, 2/1/2025

Recent activity

Name Time

- Generated 2 suggestions for policy updates. 12:43 PM, 2/1/2025
- Analyzed out of scope identities against policy best practices 12:40 PM, 2/1/2025
- Checked new users against Conditional Access policies 12:36 PM, 2/1/2025
- Scanned for applications added in the last 24 hours 12:34 PM, 2/1/2025

Add 15 users to policy

Condition Access Optimization Agent suggestion

15 new users need to be added to policy

The Condition Access Optimization Agent recommends that 15 new users be added to the policy CA 3: MFA for Engineering, which will require users to satisfy MFA controls before accessing resources targeted in the policy.

Factors: These users are not in scope of any Conditional Access policies and were added to the Contoso tenant by Lauren Baker on 1/31/25 at 1:56 PM.

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

Review policy changes

Download updated policy JSON

Actions taken

Data analysis performed on new Users/Applications added to your tenant over the past 24 hrs (from 1/30/25 12:32:02PM – 1/31/25 12:32:02PM).

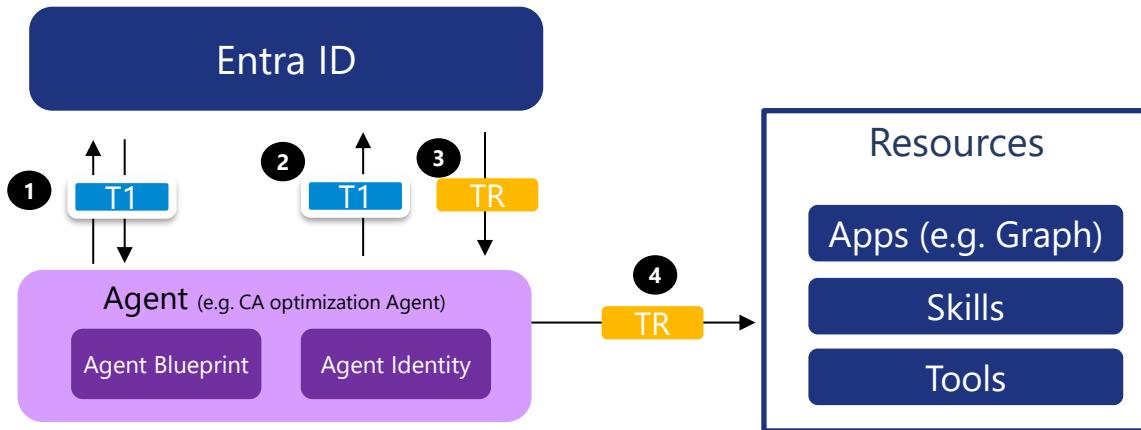
Users

15 users were added to your tenant yesterday and are not in scope of any Conditional Access policy.

User name	Email address	Date/time added
Samuel Thompson	s.thompson@contoso.com	11:07:29 AM, 5/20/25
Tiffany Li	tli@contoso.com	11:07:29 AM, 5/20/25
Leah George	leahg@contoso.com	1:56 PM, 5/20/25
Bethany Savely	bsavely@contoso.com	1:56 PM, 5/20/25
Emilie Wing	ewing@contoso.com	1:56 PM, 5/20/25

Agent has its own identity and permissions and can run autonomously

Autonomous App flow



1. Agent Blueprint requests a FIC Exchange Token (T1) from Entra ID using MSI, Entra ID returns the T1 to Agent
2. Agent Identity sends an OBO token exchange request to Entra ID, including T1
3. Entra ID issues a Resource Access Token (TR) to the Agent Identity after validating T1
 - $T_1.\text{Aud} == \text{AgentIdentity.ParentApp} == \text{Agent Blueprint}$
4. Agent Identity accesses the Resource using the Resource Access Token (TR).

Agentic user flow - summary

Anyा Sharma
CEO
Office of the CEO

Kenji Tanaka
CEO
Executive Office

Maria Rodriguez
Chief Technology Officer
Engineering HQ

People reporting to Maria Rodriguez (11)

AI Agent 1
Senior AI Research Scientist

AI Agent 2
Lead AI Solutions Architect

David Chen
VP of Product

Sarah Lee
Chief Data Officer

Michael O'Connell
VP of Infrastructure

Emily Davis
VP of Design

James Wilson
VP of Operations

Jessica Kim
Senior Executive Assistant

Robert Brown
VP of Engineering

Thomas Garcia
Chief Information Security Officer

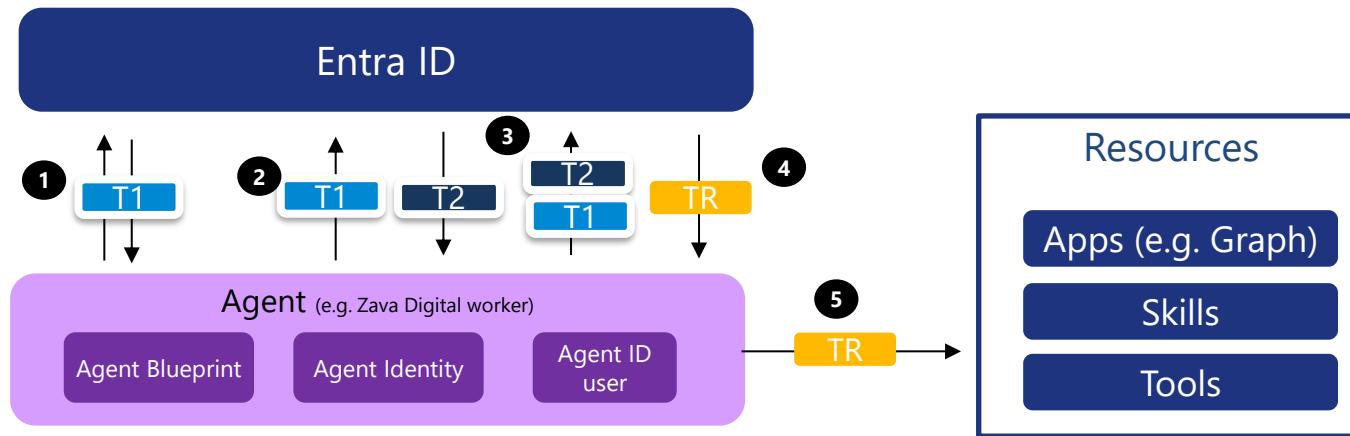
Linda Martinez
VP of AI Strategy

Autonomous human-like agent that can use Teams, Outlook and other applications just like a real person.

The agent's identity is in HR and other systems.

The Agent user has delegate permission to Graph and other resources.

Agentic user flow



1. Agent Blueprint requests a FIC Exchange Token (T1, for Agent Identity impersonation) from Entra ID using MSI, Entra ID returns the T1 to Agent
2. Agent Identity requests a FIC Exchange Token (T2, for Agent ID user impersonation) using T1, Entra ID returns the T2 to Agent Identity
 - Entra ID validates `T1.Aud == AgentIdentity.ParentApp == Agent Blueprint`
3. Agent Identity sends an OBO token exchange request to Entra ID, including both T1 and T2
 - Entra ID validates `T2.Aud == Agent ID User.ParentApp == Agent Identity`
4. Entra ID issues a Resource Access Token (TR) to the Agent Identity after validating both T1 and T2
5. Agent ID user accesses the Resource using the Resource Access Token (TR).

Agent ID – Building Blocks

Agent ID - Deconstructed



Agent ID Administrator

1.01



Agent Blueprint App
(app registration)

1.02



Agent Blueprint
Service Principal



Agent Blueprint MS Graph token
(e.g. via client credentials or MI)

2



Autonomous Agent Identity
(Service Principal)



Agent ID Administrator

3.01

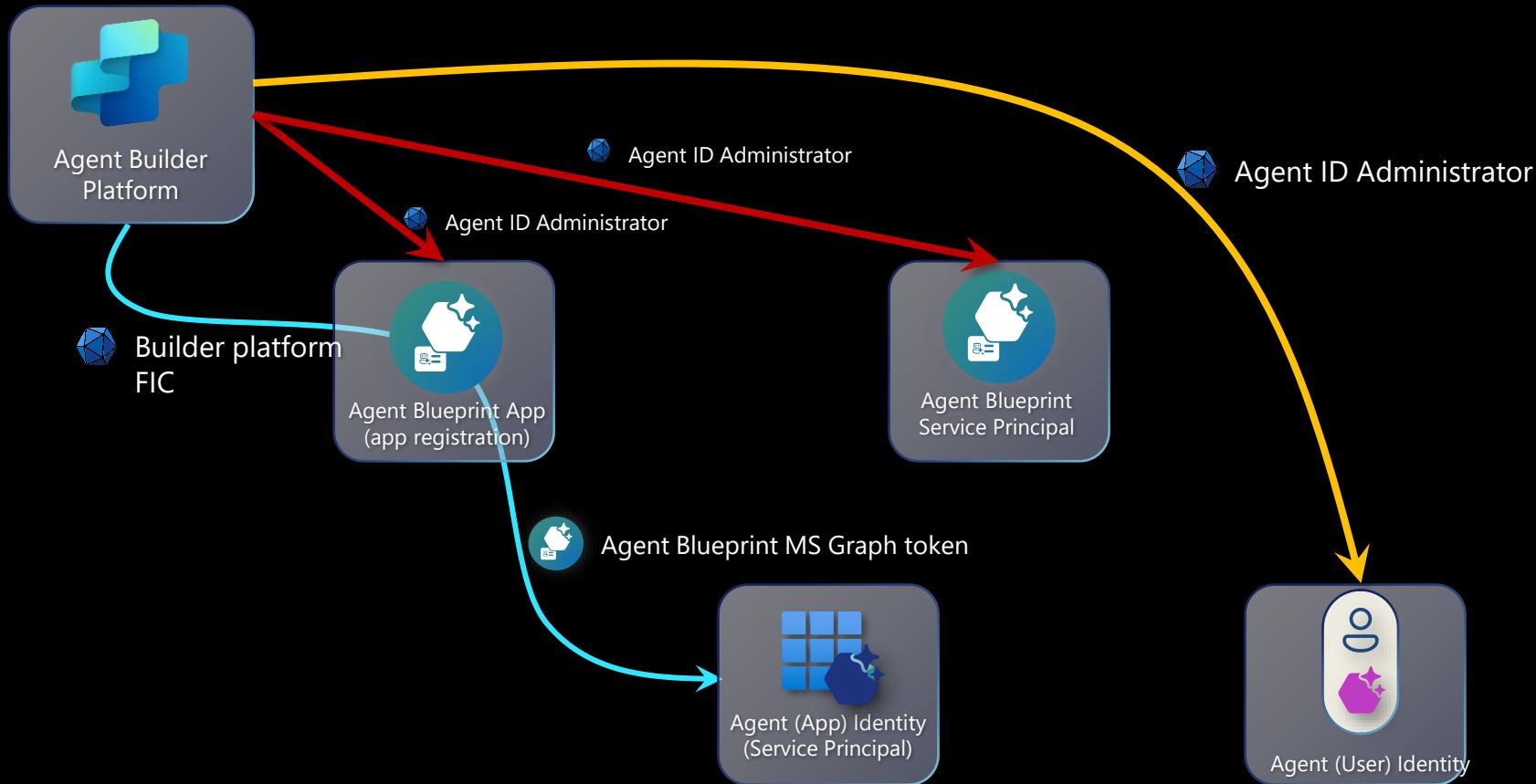


Agent (User) Identity

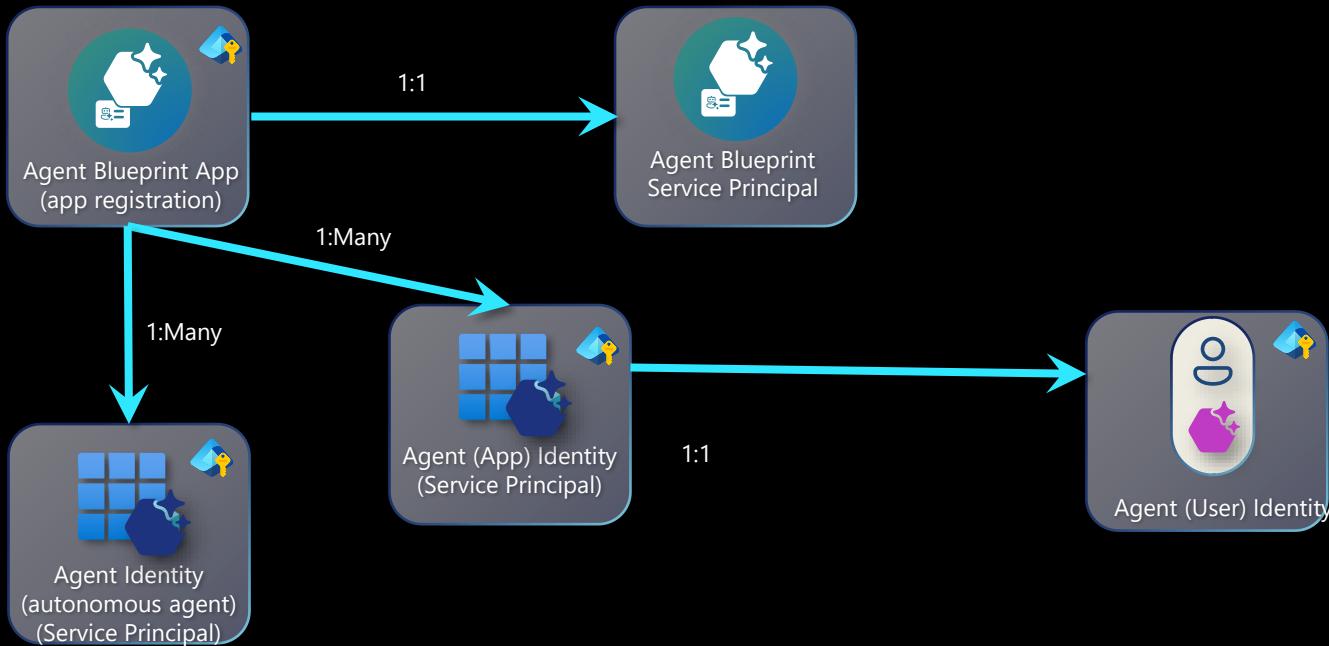
3.02

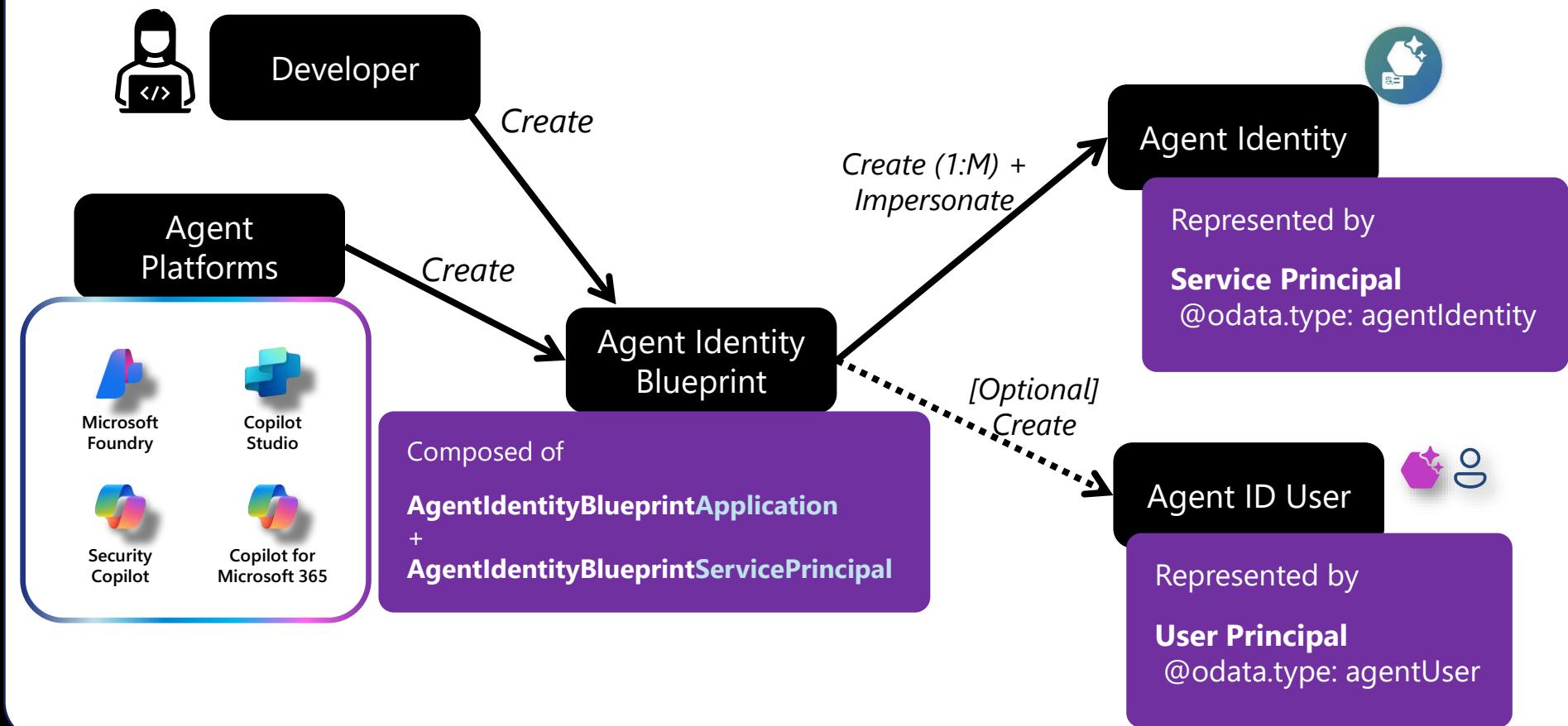
+ OAuth2PermissionGrants

Artifacts creation



Artifacts relationships





Permissions for agent IDs

Option 1

Each agent ID will request the permissions that the agent needs when needed.

Users or admins can grant consent

Each agent needs the permission request/grant experience

Option 2

Agents inherit some or all of the permissions granted to the blueprint

Admin grants consent for all users in the tenant

Add inheritable permissions to the blueprint

If not granted, can not be inherited

Option 3

Use both option 1 and option 2

```
beta/applications/microsoft.graph.agentIdentityBlueprint/  
<blueprintID>/inheritablePermissions
```



← a-kyle@wrytercorp.onmicrosoft.com

Step 2 of 2

Allow agents created from this blueprint to access data?



Bob Agent
unverified

- This agent blueprint was not published by Microsoft.
- If this agent blueprint looks suspicious, [report it here](#).

By giving permission, **all Bob Agent agents** can:

- › Read your mail
- › Sign you in and read your profile
- › Send mail as you
- › Maintain access to data you have given it access to

Accepting these permissions means that you allow this agent blueprint to use your data as specified in their [terms of service](#) and [privacy policy](#). You can change these permissions at <http://myapps.microsoft.com>. [Show details](#).

Deny

Allow

High Privilege Access (HPA) Permissions



Entra prevents HPA permissions from being granted to agents.

Neither users nor admins can grant consent to these permissions

Entra's goal is to move toward fine-grained, task-specific access so agents can perform critical operations safely with minimal risk.

Example of Application HPA permissions

AgentIdentity.Create
AgentIdentityBlueprint.Create
Application.ReadWrite.All
Directory.ReadWrite.All
RoleManagement.ReadWrite.All
User.ReadWrite.All

Example Delegated HPA permissions

Directory.AccessAsUser.All

Directory.ReadWrite.All

User.ReadWrite.All

<https://aka.ms/agentid-blocked-perms>

Where do agent identity blueprints come from?

Microsoft products

Copilot Studio, Microsoft AI Foundry, [Agent 365](#)

When you create your agent on a Microsoft agent platform you don't need the details

Microsoft Graph APIs

PowerShell (<https://github.com/AzureAD/MSIdentityTools>)

Any app that can call Microsoft Graph (<https://github.com/azure-Samples/ms-identity-agent-identities>)

Microsoft Entra ID consent experience

Multi-tenant blueprint

Create the Agent identity blueprint principal in the tenant



a-kyle@wrytercorp.onmicrosoft.com

Step 1 of 2

Add this agent blueprint to your organization?



Bob Agent
unverified

This adds the agent blueprint to your organization and **allows it to create agent accounts**. These accounts will be visible in [MyAgents](#).

[Learn more about agents, access, and permissions.](#)

This agent blueprint was not published by Microsoft. If it looks suspicious, [report it here](#).

Adding this agent blueprint means you accept its [terms of service](#) and [privacy policy](#).

No

Yes

Create an agent identity blueprint

Need AgentIdentityBlueprint.Create permission (admin consent only)

Need an Agent ID Administrator or Agent ID Developer role

Alternatively, an app with AgentIdentityBlueprint.Create as an app permission

Can create 250 agent identity blueprints

Required to provide an owner or a sponsor. Sponsor preferred.

Limits

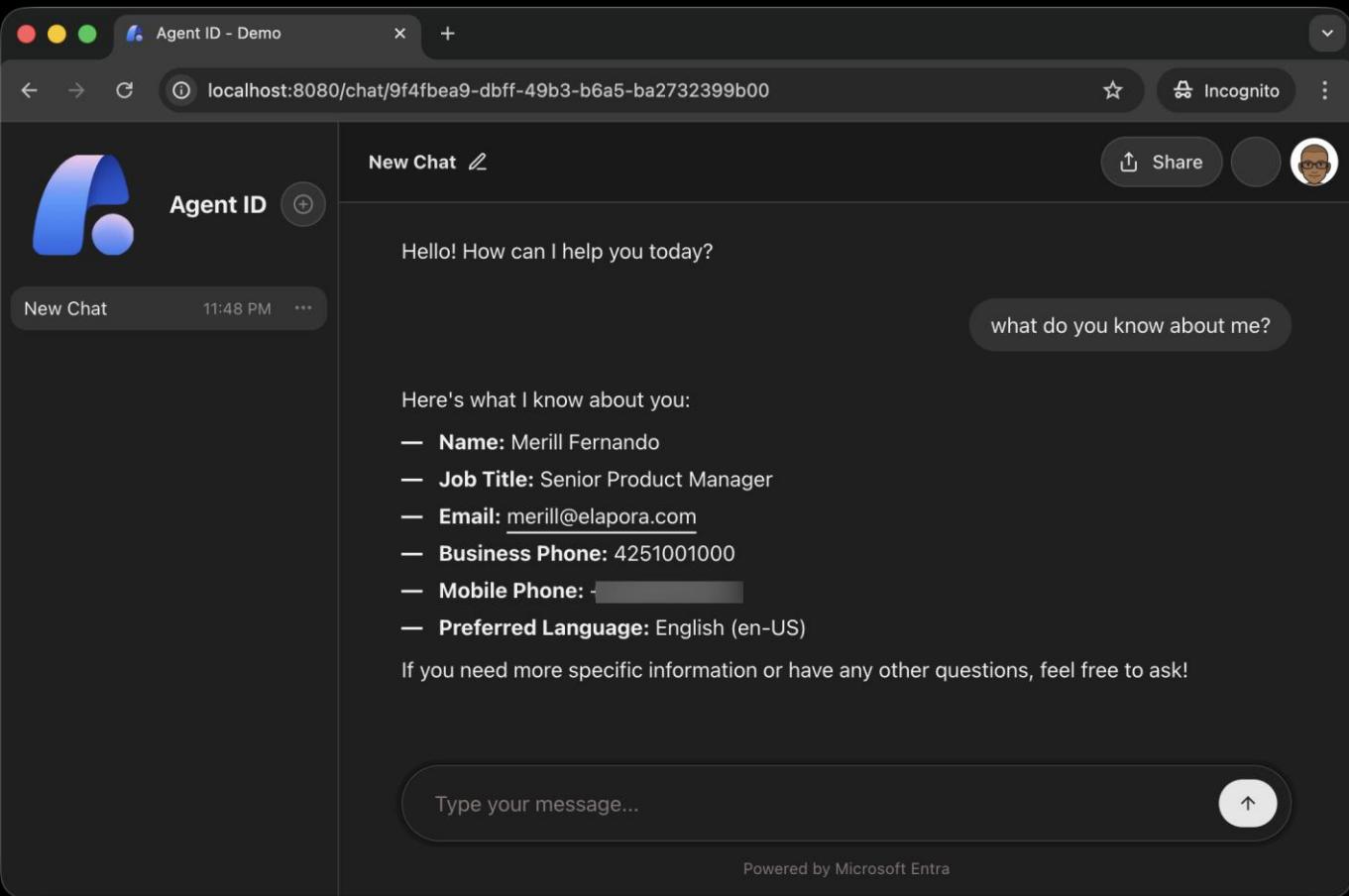
Apps using app-only permissions can create 250 Blueprints per tenant

250 Agent IDs per blueprint

Deleted agents count until hard deleted

Overall tenant limits apply

Agent ID Lab Overview

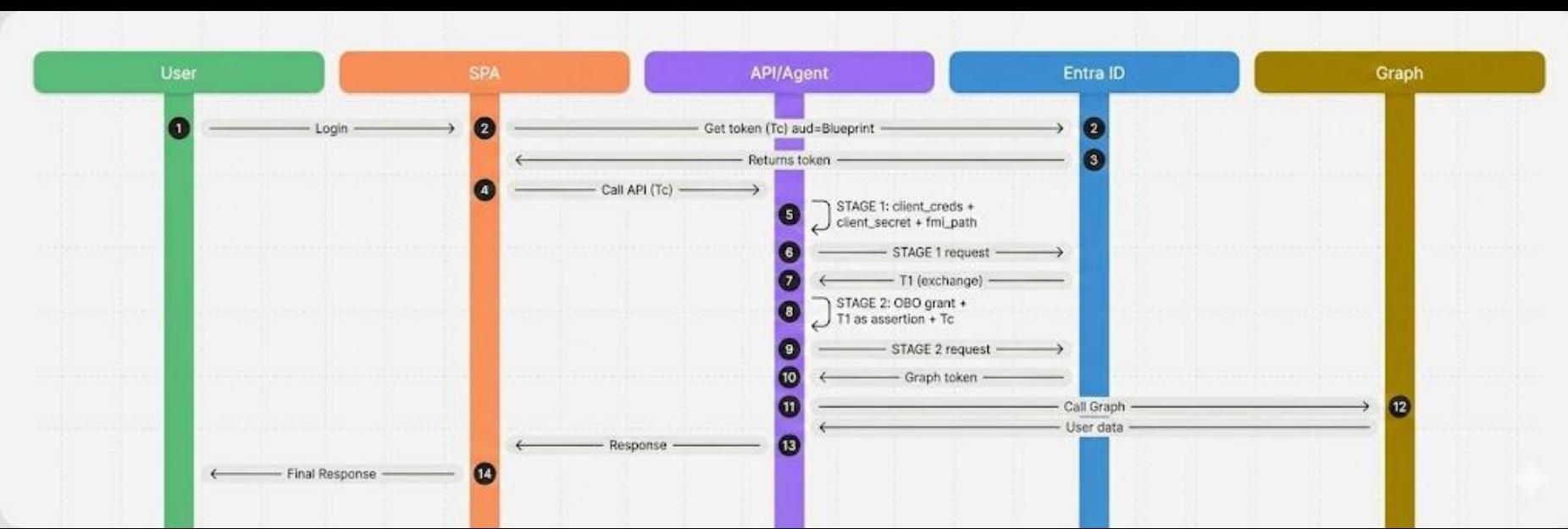


The screenshot shows a web-based chat interface titled "Agent ID - Demo". The URL in the address bar is "localhost:8080/chat/9f4fbea9-dbff-49b3-b6a5-ba2732399b00". The interface has a dark theme. On the left, there's a sidebar with a blue "A" logo, a "New Chat" button, the time "11:48 PM", and a three-dot menu. The main area starts with a "New Chat" button and a "New Chat" link. Below that, a message from the AI says "Hello! How can I help you today?". A user message "what do you know about me?" follows. The AI then responds with a list of details:

- **Name:** Merill Fernando
- **Job Title:** Senior Product Manager
- **Email:** merill@elapora.com
- **Business Phone:** 4251001000
- **Mobile Phone:** [REDACTED]
- **Preferred Language:** English (en-US)

At the bottom, a message box says "If you need more specific information or have any other questions, feel free to ask!" and contains a placeholder "Type your message...". A "Powered by Microsoft Entra" footer is at the bottom right.

Agent ID – Lab Overview



```
MSIdentityTools @ merill-macbook
/Applications/.../MSIdentityTools >▶ main > 0.132s
>
```

D E M O

LAB 4: Creating a custom agent with Agent ID

<https://aka.ms/eldk26>





Monitoring, Maintaining, Disaster Recovery



Backup Restore

Entra object restore – reality check

Object type	Soft delete	Restore?
User object	✓	🗑️ 30d Recycle Bin
Security group	✓	🚫 No restore
M365 group	✓	🗑️ 30d Recycle Bin
Device object	X	🚫 No restore
Enterprise Application	✓	🔄 Multi-Tenant 🔄 Single-Tenant
App Registration	✓	🗑️ Recycle Bin
Administrative Unit	✓	🔄 Deleted Item
Conditional Access	✓	🔄 Deleted Item

```

1  {
2    "id": "049fab0d-a309-43b9-a3f9-e2f25aa9caf8",
3    "templateId": null,
4    "displayName": "CA003-Global-BaseProtection-AllApps-AnyPlatform-MFA",
5    "createdDateTime": "2022-07-05T17:05:36.8206457Z",
6    "modifiedDateTime": "2025-07-31T19:38:28.5262738Z",
7    "state": "enabled",
8    "deletedDateTime": null,
9    "partialEnablementStrategy": null,
10   "sessionControls": null,
11   "conditions": [
12     "userRiskLevels": [],
13     "signInRiskLevels": [],
14     "clientAppTypes": [ ...
15   ],
16     "platforms": null,
17     "locations": null,
18     "times": null,
19     "deviceStates": null,
20     "devices": null,
21     "clientApplications": null,
22     "applications": { ...
23   },
24     "users": {
25       "includeUsers": [ ...
26         1.
27         "excludeUsers": [
28           "08a644d4-6533-4931-9158-edee7db7ffffa",
29           "349c5270-e777-4727-b655-43f99f454dc2"
30         ],
31         "includeGroups": [],
32         "excludeGroups": [
33           "af7e030f-84e5-4edd-827f-8c7a7a1d14be"
34         ],
35         "includeRoles": []
36       }
37     }
38   }
39 }
40
41
42
43
44

```

Hard deleted? And now what?

- ❖ No support recovery option after hard delete
- ❖ Object must be recreated
- ❖ Object becomes a new ID
- ❖ Previous JSON export required (EntraExporter)
- ❖ Example article on rebuilding a hard-deleted Administrative Unit. Additional read:



<https://nothingbutcloud.net/2025-08-30-DeletedEntraObjects/>



To make sure it never comes down to a restore ...

- ❖ Protect sensitive Groups with „PIM Protected Groups“
-> possible, but should you?
- ❖ AU – Restricted Management (GA since June 2025)
- ❖ Protected Actions for hard deletions (GA since January 2025)
- Smart Alerting for important Resources
Example implementation. Additional read:



<https://nothingbutcloud.net/2025-12-16-ZeroTrust-Monitoring>

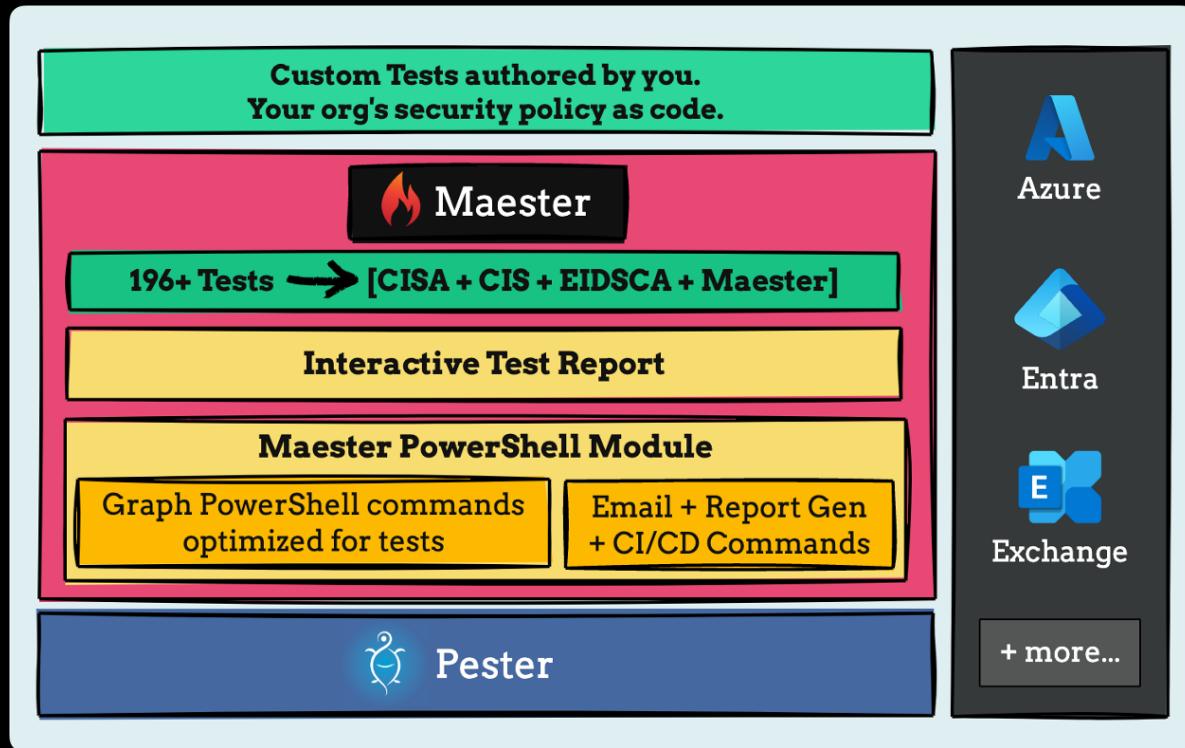
Demo ...





Optimize Identity Security Exposure

Overview of Maester Framework



Tenant Hardening of Default Settings

Dashboard > Security | Authentication methods >

Dashboard > CloudLab | Enterprise applications > Enterprise applications | User settings >

CloudLab | User settings

Groups | General

Self Service Group Management

Owners can manage group membership requests in My Groups Yes No

Restrict user ability to access groups features in My Groups. Group and User Admin will have read-only access when the value of this setting is 'Yes'. Yes No

In June 2024, this setting will restrict users' ability to view and edit security groups in My Groups. It will no longer restrict access to My Groups. [Learn more](#).

Security Groups

Users can create security groups in Azure portals, API or PowerShell Yes No

Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell Yes No

Authorization Policy (Microsoft Graph API)

```
GET "https://graph.microsoft.com/beta/authorizationPolicy"
```

```
"@odata.context":  
"https://graph.microsoft.com/beta/$metadata#policies/authorizationPolicy",  
  
"value": [  
  {  
    "displayName": "Authorization Policy",  
    "id": "authorizationPolicy",  
    "allowInvitesFrom": "adminsAndGuestInviters",  
    "allowedToSignUpEmailBasedSubscriptions": true,  
    "allowedToUseSSPR": true,  
    "defaultUserRolePermissions": {  
      "allowedToCreateApps": true,  
      "allowedToCreateSecurityGroups": true,  
      "allowedToCreateTenants": false,  
      "allowedToReadBitlockerKeysForOwnedDevice": true,  
      "allowedToReadOtherUsers": true  
    }  
  }  
]
```

Authorization Check (EIDSCA)

```
"Name": "allowedToCreateApps",
"DisplayName": "Default User Role Permissions - Allowed to create Apps",
"CheckId": "EIDSCA.AP10",

"SkipCondition": "",
"SkipReason": "",

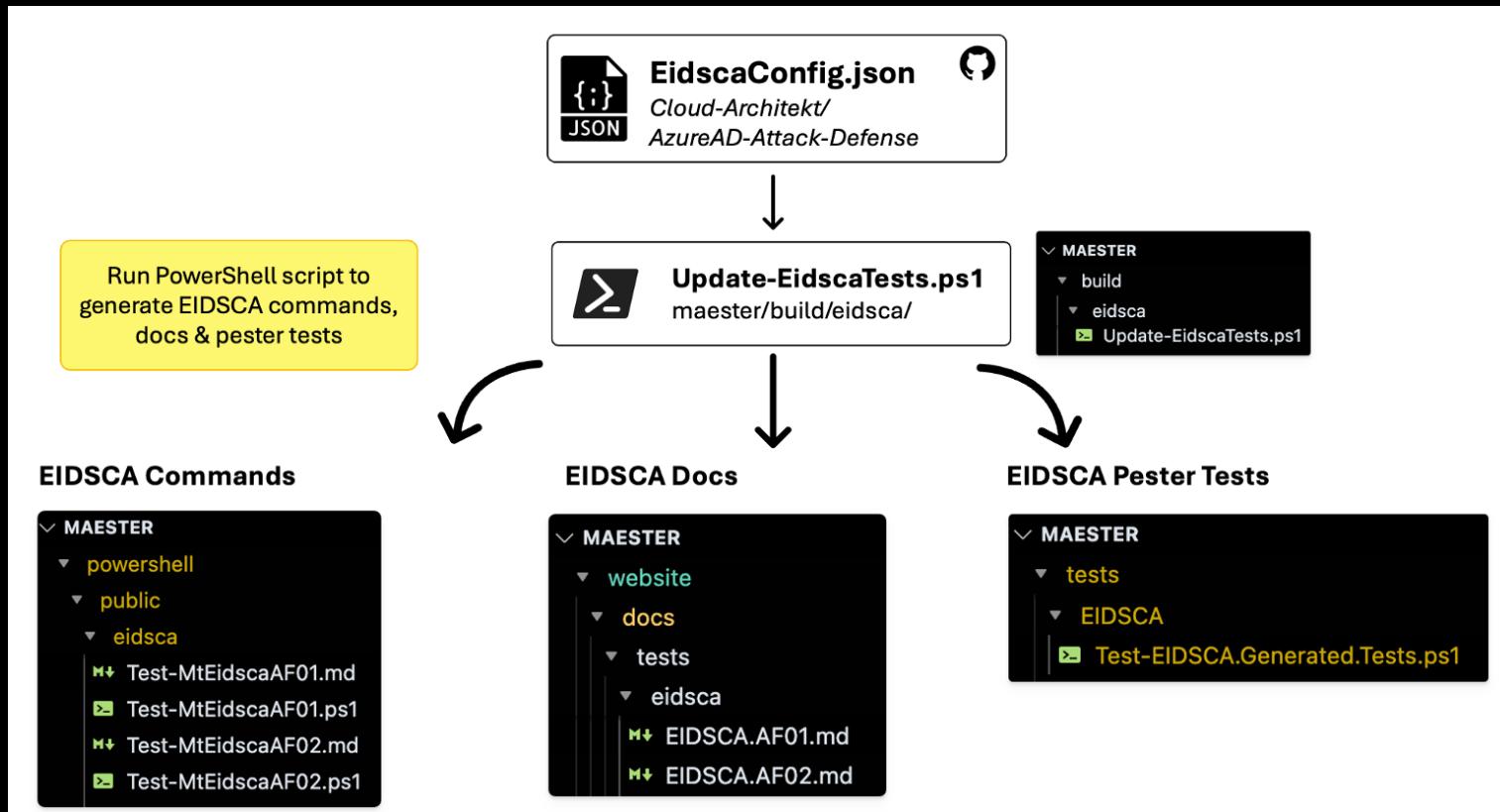
"CurrentValue": "defaultUserRolePermissions.allowedToCreateApps",
"DefaultValue": "true",
"RecommendedValue": "false",

"Recommendation": "CISA SCuBA 2.6: Only Administrators SHALL Be Allowed To Register 3rd Apps",
"Severity": "High",

"MitreTactic": ["TA0001 - Initial Access", ...],
"MitreTechnique": ["T1566.002", ...],
"MitreMitigation": ["M1017", ...], 

"PortalDeepLink": "https://entra.microsoft.com/.../UserManagementMenuBlade/~/UserSettings",
"Description": "Controls if non-admin users may register custom-developed applications (...)",
"HowToFix": "Microsoft Graph PowerShell: Update-MgPolicyAuthorizationPolicy (...)"
```

EIDSCA Checks in Maester



Exposure Management

Exposure Management Overview

**Unified Threat
Management**
(XDR/SIEM)

Detect

Response

**Unified Exposure
Management**
(XSPM)

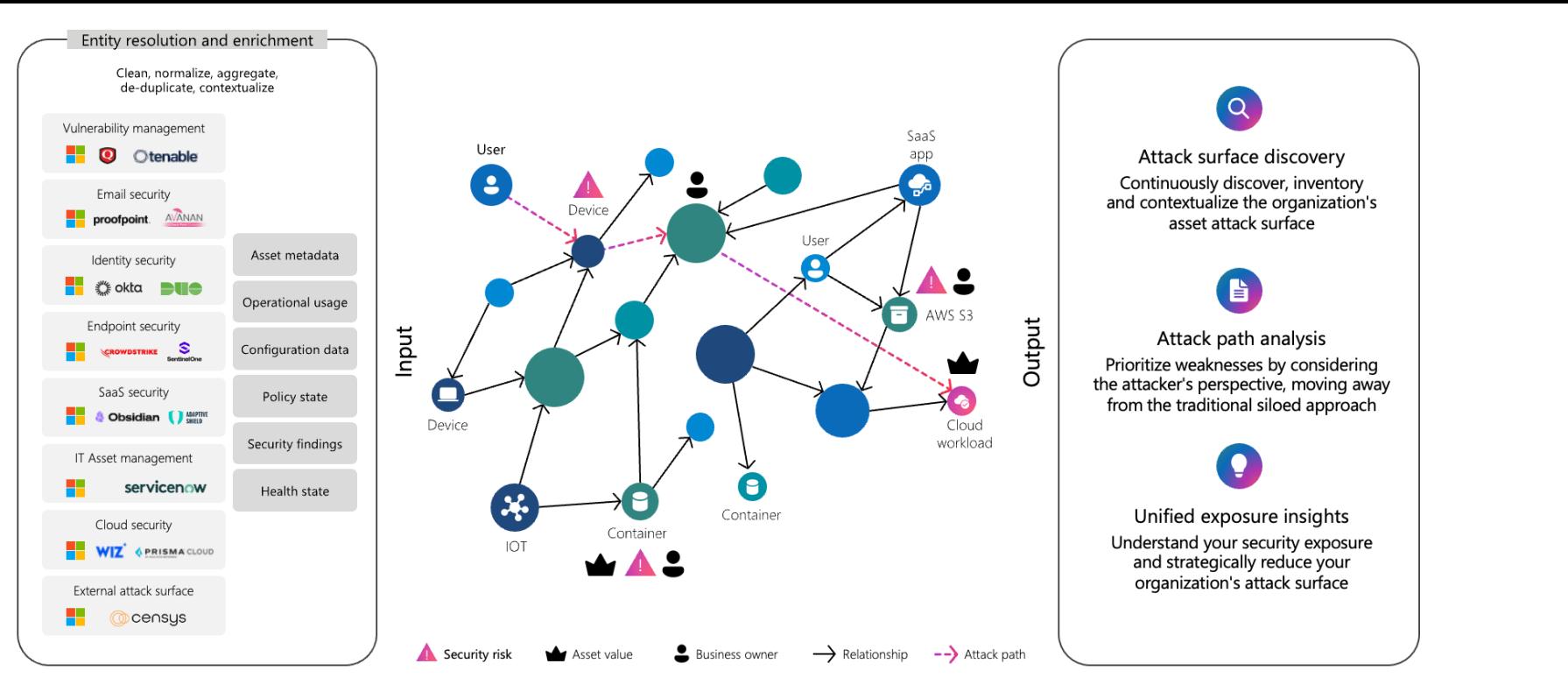
Identify

Protect



Holistic pre- and post-breach view and data

Exposure Management Overview



Source "[Proactive security with continuous exposure management](#)" (Microsoft Ignite)

Attack paths - Microsoft Defender | Attack paths - Microsoft Defender | Map - Microsoft Defender X +

https://security.microsoft.com/security-graph?nodeIds=%5B"8fc95387211d4fcf81cb02dfbc6c3a72"%2C"4133eb7cfef9c42cda6f1c152fa1ee124"%2C"0e447a7d9dc433797d19b21a0d75663"%2C"a7d1a307d9394032a5a79bf... A ⭐ 🌐 📁 ...

Zava Microsoft Defender Search Michael Mukasine MM

Map

Scope filter : Off ⓘ

Search

Export Search

Key ↑ Value ↓

- containsSensitiv...
- containsSensitiv... Sensitivity
- criticalityLevel.c... Critical
- criticalityLevel.r... Critical
- criticalityLevel.r... Databases with Sensitive Data
- criticalityLevel.r... Internet facing
- criticalityLevel.r... criticalResource
- criticalityLevel.t... CriticalityLevel
- environmentNa... Azure
- exposedToInter... 76.182.132.142
- exposedToInter... InternetExposure
- hierarchyIdentif... 34d58fcf-b44c-4c75-b18d-37a49e3018c9
- hierarchyType subscriptionid
- nativeEnvironm... eastus2
- tags.type TagsData

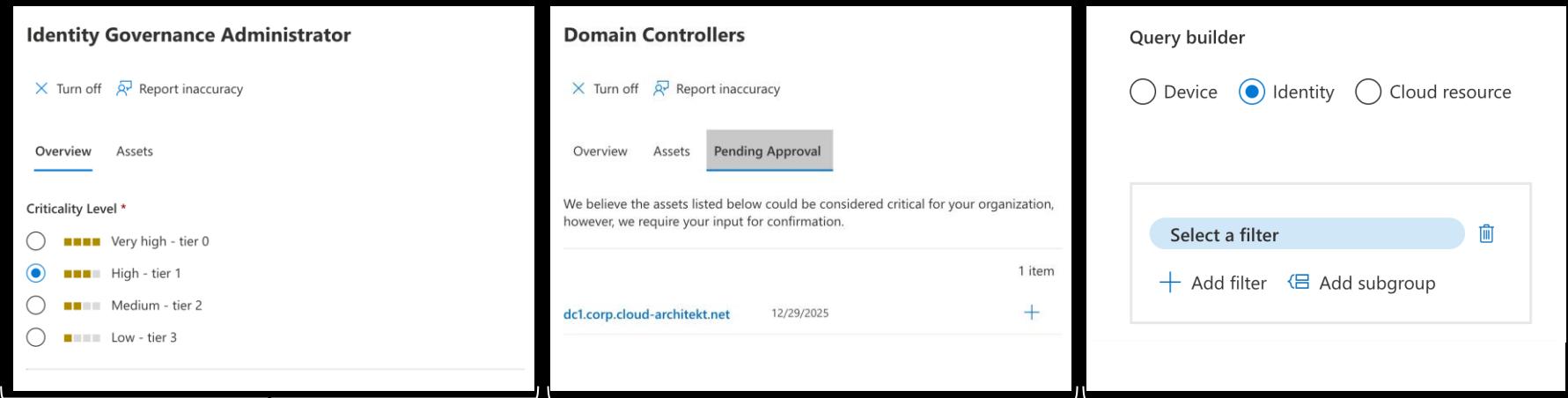
Layers

Discovery Source ⓘ

+

-

Critical Asset Management



The image displays three side-by-side screenshots of a critical asset management application interface.

- Identity Governance Administrator:** Shows a navigation bar with "Identity Governance Administrator". Below it are two buttons: "Turn off" and "Report inaccuracy". Underneath are tabs for "Overview" (selected) and "Assets". A section titled "Criticality Level *" contains five radio buttons with corresponding color swatches:
 - Very high - tier 0 (light blue)
 - High - tier 1 (dark blue, selected)
 - Medium - tier 2 (light gray)
 - Low - tier 3 (white)
- Domain Controllers:** Shows a navigation bar with "Domain Controllers". Below it are three buttons: "Turn off", "Report inaccuracy", and "Pending Approval" (selected). Underneath are tabs for "Overview", "Assets" (selected), and "Pending Approval". A message states: "We believe the assets listed below could be considered critical for your organization, however, we require your input for confirmation." Below this is a table with one item:

Asset	Date
dc1.corp.cloud-architekt.net	12/29/2025
- Query builder:** Shows a navigation bar with "Query builder". Below it are three radio buttons: "Device" (white), "Identity" (dark blue, selected), and "Cloud resource" (white). A section titled "Select a filter" contains two buttons: "Add filter" and "Add subgroup".

Review Criticality Level
Tier != Tier

Check Pending
Approvals

No custom classification
for Groups and
Non-Human Identities



D E M O

LAB 5: Maester and Identity Security Posture

<https://aka.ms/eldk26>



Maester @ merill-macbook



/

... / Maester

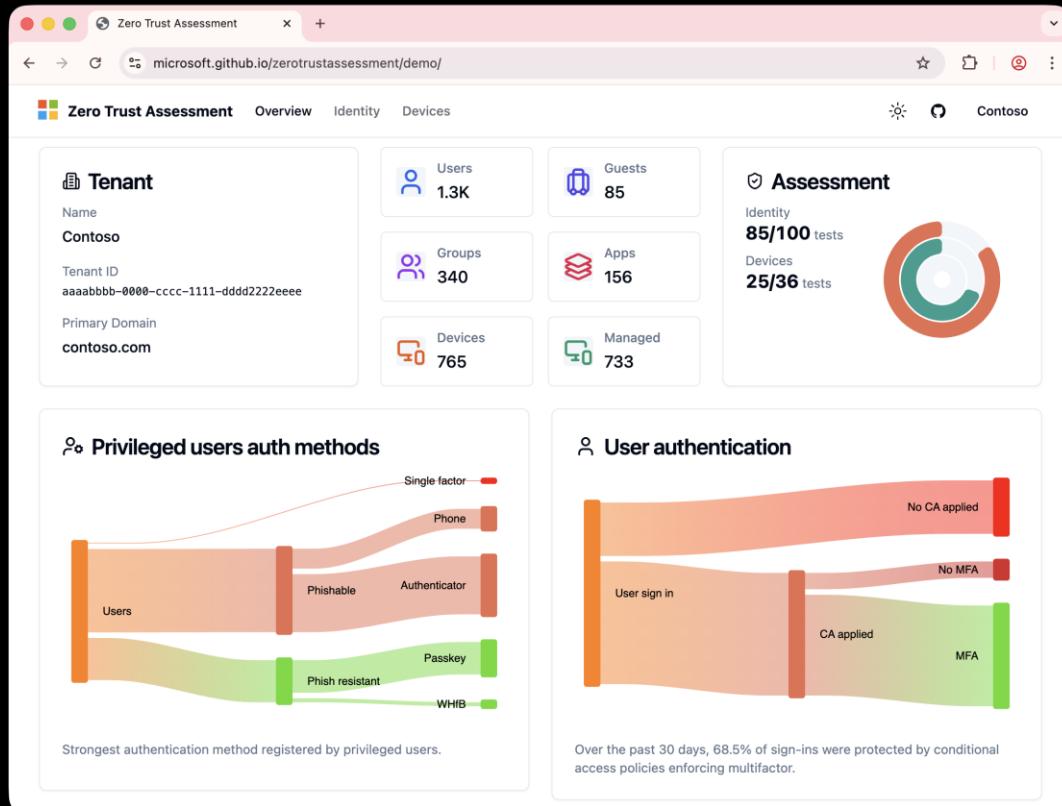
0.047s



Zero Trust Assessment

- PowerShell module that you install on your desktop
- Run an intensive scan against your tenant to generate a report with recommendations

```
Install-Module ZeroTrustAssessment  
Connect-ZtAssessment  
Invoke-ZtAssessment -Path C:\Report
```



Zero Trust Assessment

The screenshot shows a browser window with two tabs open. The left tab is a GitHub raw file containing a JSON configuration for a Zero Trust Assessment. The right tab is the Microsoft Zero Trust Assessment tool interface.

GitHub Raw File Content:

```

---
title: Inactive applications don't have highly privileged built-in roles
ms.author: barclayn
author: barclayn
manager: pwongera
ms.service: entra-id
ms.topic: include
ms.date: 02/03/2025
ms.custom: Identity-Secure-Recomm
# sfipillar: Protect engineering
# category: Application management
# risklevel: High
# userimpact: Low
# implementationcost: Low
---
Attackers might exploit valid but because they're legitimate applications by manipulating the inactive application access later.

**Remediation action**
- [Disable inactive privileged service principals]
- Investigate if the application has legitimate use cases
- [If service principal doesn't have highly privileged built-in roles, delete it]
  
```

Zero Trust Assessment Tool Interface:

- Test Result:** Failed. Found 1 inactive applications with privileged Entra built-in roles.
- Apps with privileged Entra built-in roles:**

Name	Role	Assignment	App owner	Last sign in
AppRolePimAutomationTestParentAcc19Feb22	Application Administrator	Permanent	tenant	
- What was checked:**

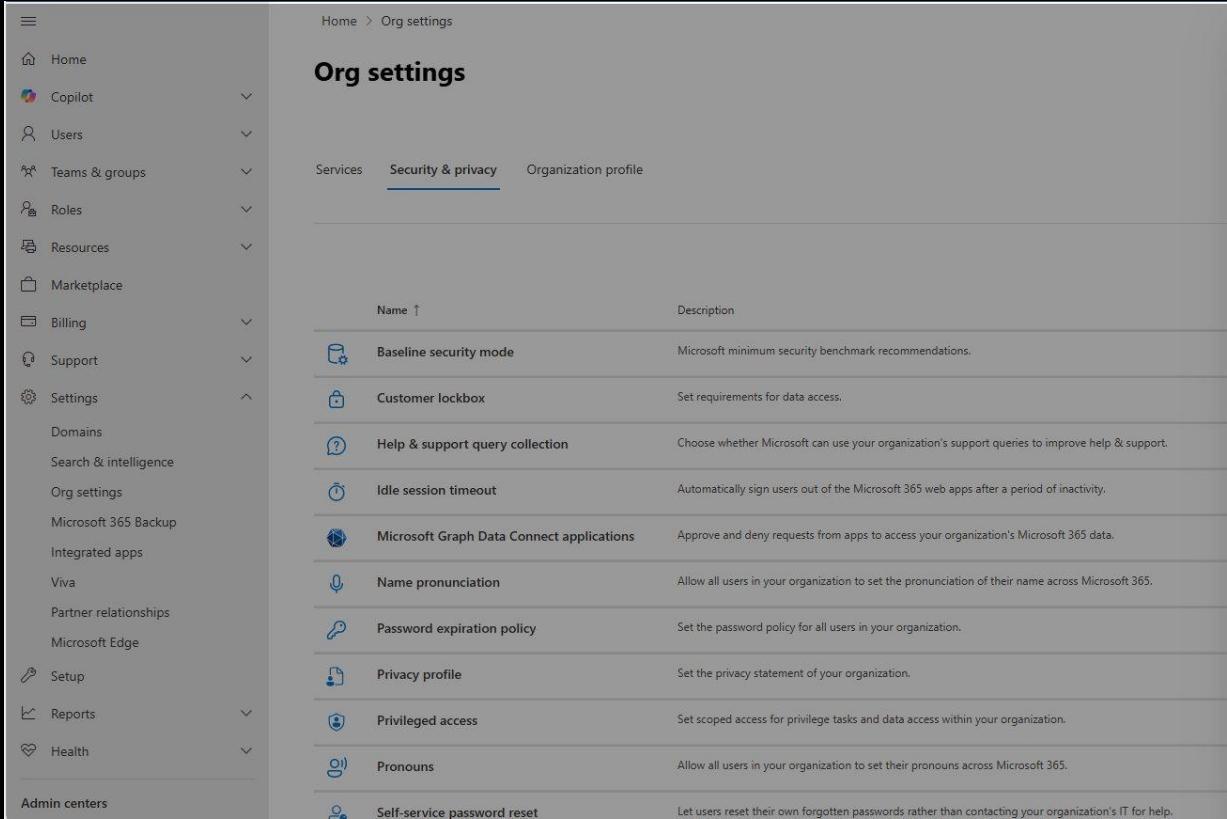
Attackers might exploit valid but inactive applications that still have elevated privileges. These applications can be used to gain initial access without raising alarm because they're legitimate applications. From there, attackers can use the application privileges to plan or execute other attacks. Attackers might also maintain access by manipulating the inactive application, such as by adding credentials. This persistence ensures that even if their primary access method is detected, they can regain access later.
- Remediation action:**
 - [Disable inactive privileged service principals](#)
 - [Investigate if the application has legitimate use cases. If so, \[analyze if a OAuth2 permission is a better fit\]\(#\)](#)
 - [If service principal doesn't have legitimate use cases, delete it](#)

App registrations use safe redirect URIs

OAuth applications configured with URLs that include wildcards, or URL shorteners increase the attack surface for threat actors. Insecure redirect URLs (reply URLs) might allow adversaries to manipulate authentication requests, hijack authorization codes, and intercept tokens by directing users to attacker-controlled endpoints. Wildcard entries expand the risk by permitting unintended domains to process

Baseline Security Mode

Adoption of strong secure-by-default settings and eliminating vulnerabilities caused by legacy configurations



The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with various options like Home, Copilot, Users, Teams & groups, Roles, Resources, Marketplace, Billing, Support, Settings, Domains, Search & intelligence, Org settings, Microsoft 365 Backup, Integrated apps, Viva, Partner relationships, Microsoft Edge, Setup, Reports, Health, and Admin centers. The main area is titled "Org settings" and has tabs for Services, Security & privacy (which is selected), and Organization profile. Below these tabs is a table with columns for Name and Description. The table lists several items, including "Baseline security mode" (selected), "Customer lockbox", "Help & support query collection", "Idle session timeout", "Microsoft Graph Data Connect applications", "Name pronunciation", "Password expiration policy", "Privacy profile", "Privileged access", "Pronouns", and "Self-service password reset". To the right of the table, there's a modal window titled "Baseline security mode" with the following content:

Baseline security mode

Reduce your attack surface and harden your organization from malicious attacks. We recommend that you apply all default policies immediately.

To apply policies individually, select Manage all policies.

[Learn more about baseline security mode](#)

Automatically apply default policies

Microsoft will apply all default policies that are recommended because they usually have little impact for organizations.

[View default policies \(7\)](#)

Generate reports and consent to view sensitive data for remaining policies

This will initiate the generation of impact reports for the remaining policies. Baseline security mode impact reports contain end-user identifiable information (EUUI) and some require tenant-level audit logs for Word, Excel, PowerPoint and OneNote. If you want to view impact reports, you must consent to view this data.

[View remaining policies \(11\)](#)

Save **Manage all policies**

Baseline security mode

Manage these policies to reduce your attack surface and harden your Microsoft 365 organization from malicious attacks. Each policy is recommended to reach the minimum security benchmark.

[Learn about baseline security mode and why it's important](#)

Report settings

Progress to meet standard

94%

Your progress Standard benchmark You have applied 17 out of 18 recommendations

Recommended setting automation

Microsoft recommended setting adjustments as of
Tue Nov 11 2025

Filters: Category: [all](#) Workload: [all](#) Status: [all](#) Reset all filters

Setting recommendation

Status

Service

Authentication (12)

Require phishing-resistant authentication for admins

In review

Entra ID

Block legacy authentication

Meets standard

Entra ID

Block new password credentials in apps

Meets standard

Entra ID

Turn on restricted management user consent settings

Meets standard

Entra ID

Block access to Exchange Web Services

Meets standard

Exchange

Block basic authentication prompts

Meets standard

Microsoft 365 apps

Block files from opening with insecure protocols

Meets standard

Microsoft 365 apps

Block files from opening with FPRPC protocol

Meets standard

Microsoft 365 apps

Block legacy browser authentication connections to SharePoint

Meets standard

SharePoint

Block IDCRL protocol connections to SharePoint

Meets standard

SharePoint



Unified Tenant Configuration Management

Unified Tenant Configuration Management



Configuration-as-Code platform for all Microsoft Clouds



Supports configurations for 7 of the major M365 Workloads



Works for organizations with 1 or 1,000+ tenants

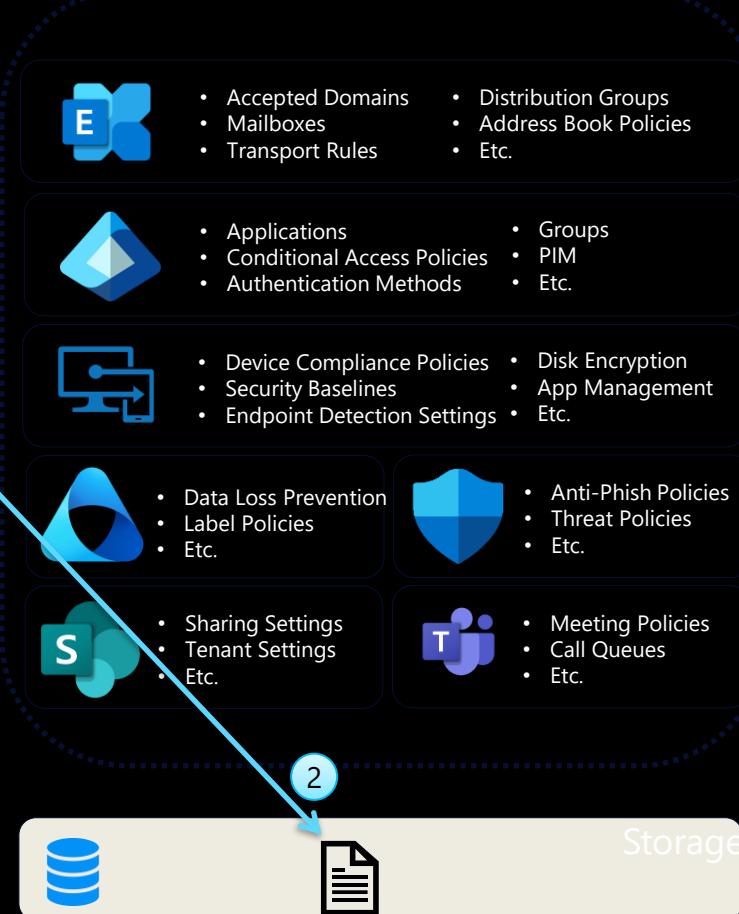




1. Requests a Snapshot for components (e.g. EXO Transport Rules, Purview Label Policies and Teams Call Queues)
2. XTA stores the extracted configuration in the tenant's internal storage.
3. User retrieves the extracted configuration baseline and stores it back in his environment (e.g., Azure DevOps source control)



Storage



Step 1: Configure Service Principal and create Snapshot Job

The screenshot shows a Microsoft PowerShell terminal window with the following details:

- Title Bar:** Shows the file name "UTCM-Demo.ps1" and a tab count of "4".
- Search Bar:** Contains a search icon and the word "Search".
- Toolbar:** Includes icons for back, forward, refresh, and other navigation functions.
- Code Area:** Displays a PowerShell script with line numbers from 1 to 190. The script performs several steps:
 - Region 1: Defines resources to include in the snapshot.
 - Region 2: Adds a service principal for UTCM and assigns permissions.
 - Region 3: Connects to Microsoft Graph with required scopes.
 - Region 4: Creates a snapshot of Conditional Access policy configurations via Microsoft Graph PowerShell SDK.
 - Region 5: Waits for the snapshot job to complete before proceeding.
 - Region 6: Invokes a PowerShell command to get the configuration snapshot job.
 - Region 7: Gets the configuration snapshot that was just created.
 - Region 8: Sets up a configuration monitor with the snapshot data.
 - Region 9: Waits for necessary time based on frequency to get monitoring results.
 - Region 10: Gets the monitoring results from the configuration monitor.
 - Region 11: Analyzes the monitoring results for any drifts in Conditional Access policies.
- Status Bar:** Shows "PROBLEMS 33", "AZURE 17", "SPELL CHECKER 17", "PORTS", "OUTPUT", "DEBUG CONSOLE", and "TERMINAL".
- Terminal Tab:** Shows "PS /Users/thomas>".
- Bottom Status:** Displays "Ln 53, Col 65" and "Spaces: 4" along with other terminal status indicators.



A FEW
MOMENTS LATER



The screenshot shows a Microsoft Visual Studio Code (VS Code) window with the following details:

- Title Bar:** Waiting for completion of Snapshot job
- File Explorer:** Shows a file named "UTCM-Demo.ps1" with 4 tabs open.
- Code Editor:** Displays PowerShell script code for creating a Conditional Access policy snapshot. The code includes regions for defining resources, adding service principals, connecting to Microsoft Graph, creating a snapshot, and setting up a configuration monitor.
- Right Panel:** A "Task List" sidebar with 9 items, including "Define resources to include in the snapshot", "Create a service principal", "Create a PowerShell SDK", etc.
- Bottom Navigation:** Includes tabs for PROBLEMS, AZURE, SPELL CHECKER, PORTS, OUTPUT, DEBUG CONSOLE, and TERMINAL.
- Bottom Status Bar:** Shows the current terminal session is PS /Users:thomas>, status indicators (0 errors, 16 warnings, 17 info), and a message: "Failed to initiate Application Insights extension. Check the console for more details or reload the extension to try again".
- Bottom Right:** Includes status information: Ln 116, Col 1 (125 selected), Spaces: 4, UTF-8, LF, and icons for PowerShell and terminal.

```
1 > #region 1. Define resources to include in the snapshot-
2
3 #endregion
4
5 > #region 2. Add service principal for UTCM and assign permissions-
6
7 #endregion
8
9 > #region 3. Connect to Microsoft Graph with the required scopes-
10
11 #endregion
12
13 #region 4. Create a snapshot of Conditional Access policy configurations via Microsoft Graph PowerShell SDK
14 $SnapshotDisplayName = "Entra CAP Baseline"
15
16 $Uri = "beta/admin/configurationManagement/configurationSnapshots/createSnapshot"
17 $Body = @{
18     displayName = $SnapshotDisplayName
19     description = "Baseline for your configured Conditional Access policies"
20     resources   = @( "$($ResourcesToInclude)" )
21 }
22
23 $CreatedSnapshot = Invoke-MgGraphRequest -Uri $Uri -Method POST -Body $Body
24 $CreatedSnapshot
25 #endregion
26
27 # Wait until the snapshot job is completed before proceeding to the next steps.
28 Invoke-MgGraphRequest -Method GET -Uri "beta/admin/configurationManagement/configurationSnapshotJobs/$(($CreatedSnapshot.id))"
29
30 > #region 5. Get the configuration snapshot that was just created-
31
32 #endregion
33
34 > #region 6. Set up a configuration monitor with the snapshot data-
35
36 #endregion
37
38
```

Name	Value
@odata.context	https://graph.microsoft.com/beta/\$metadata#admin/configurationManagement/configurationSnapshotJobs/\$entity
id	413726dd-188b-480e-9542-caaf14a81c9a
resources	{microsoft.entra.conditionalAccessPolicy}
resourceLocation	
description	Baseline for your configured Conditional Access policies
completedDateTime	01.01.0001 00:00:00
tenantId	19e61dac-ecff-427a-94c0-df49ff2f2331
createdDateTime	12.02.2026 20:27:11
status	running
displayName	Entra CAP Baseline
createdBy	{[user, System.Collections.Hashtable], [application, System.Collections.Hashtable]}



A FEW
MOMENTS LATER



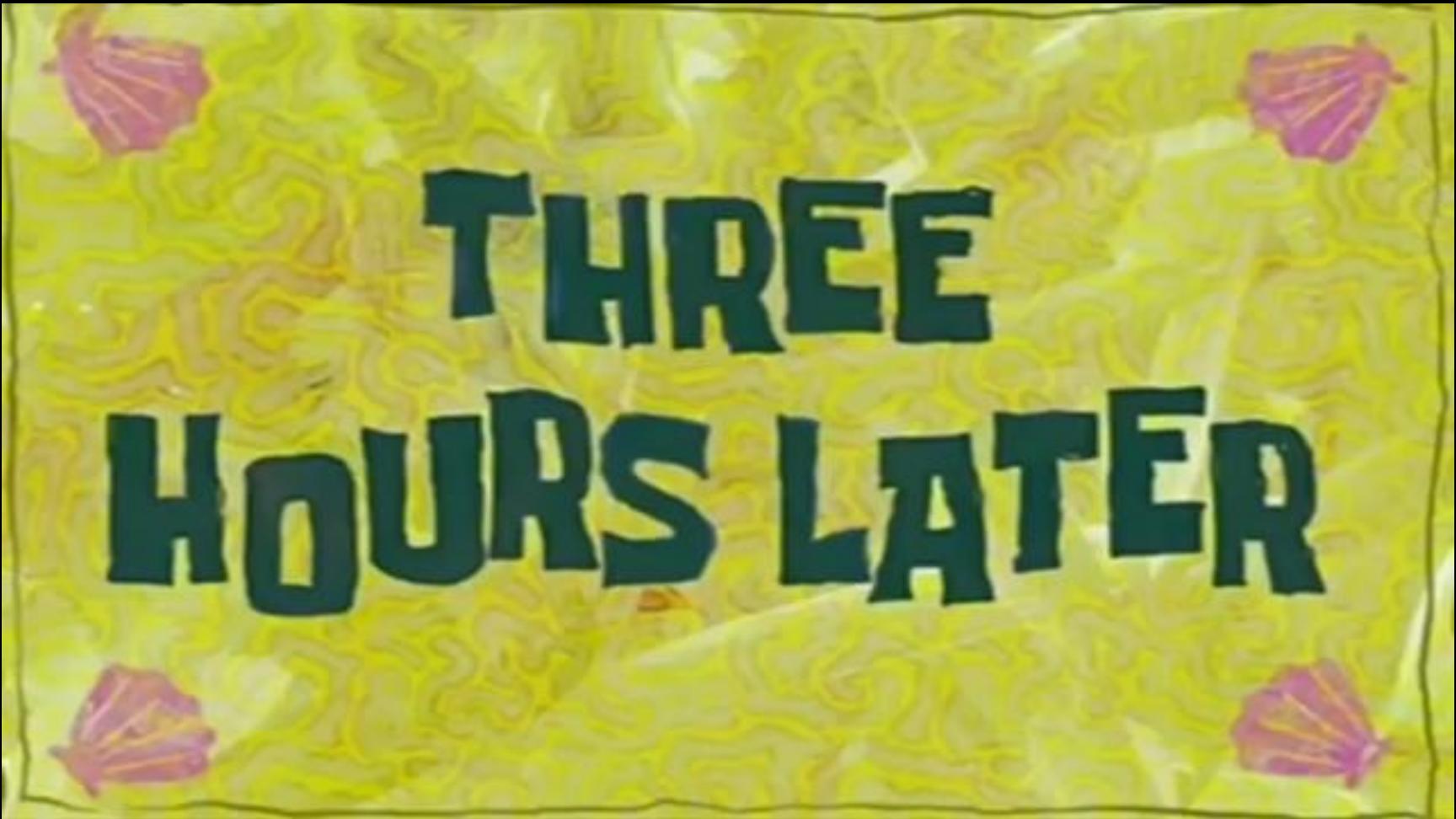
Configure Monitoring of selected resources from Snapshot

The screenshot shows a Microsoft Visual Studio Code (VS Code) window with the following details:

- Title Bar:** Shows the file name "UTCM-Demo.ps1" and a tab count of "4".
- Search Bar:** Contains a search icon and the word "Search".
- Code Editor:** Displays a PowerShell script. The code is color-coded, with syntax highlighting for variables, functions, and comments.
- Right Margin:** A vertical toolbar with numbered steps: 1. Define resources to include in the snapshot, 2. Create a service principal, 3. Create a PowerShell SDK, 4. Get the last created configuration snapshot, 5. Set up a configuration monitor with the snapshot data, 6. Get the configuration monitor, 7. Analyze the monitor data.
- Bottom Navigation:** Includes tabs for PROBLEMS (33), AZURE, SPELL CHECKER (17), PORTS, OUTPUT, DEBUG CONSOLE, and TERMINAL.
- Bottom Status Bar:** Shows the current path as "PS /Users:thomas> []", status indicators (0 errors, 16 warnings, 17 info), and the message "Failed to initiate Application Insights extension. Check the console for more details or reload the extension to try again". It also displays the line number (Ln 115), column (Col 1), and character count (124 selected), along with file format (Spaces: 4), encoding (UTF-8), line separator (LF), and terminal type (PowerShell).

```
1 > #region 1. Define resources to include in the snapshot-
2 51 #endregion
3 52
4 53 > #region 2. Add service principal for UTCM and assign permissions-
5 95 #endregion
6 96
7 97 > #region 3. Connect to Microsoft Graph with the required scopes-
8 99 #endregion
9 100
101 #region 4. Create a snapshot of Conditional Access policy configurations via Microsoft Graph PowerShell SDK
102 $SnapshotDisplayName = "Entra CAP Baseline"
103
104 $Uri = "beta/admin/configurationManagement/configurationSnapshots/createSnapshot"
105 $Body = @{
106     displayName = $SnapshotDisplayName
107     description = "Baseline for your configured Conditional Access policies"
108     resources   = @( "$(ResourcesToInclude)" )
109 }
110 $CreatedSnapshot = Invoke-MgGraphRequest -Uri $Uri -Method POST -Body $Body
111 $CreatedSnapshot
112 #endregion
113
114 # Wait until the snapshot job is completed before proceeding to the next steps.
115 [Invoke-MgGraphRequest -Method GET -Uri "beta/admin/configurationManagement/configurationSnapshotJobs/$(CreatedSnapshot.id)"]
116
117 > #region 5. Get the configuration snapshot that was just created-
118 #endregion
119
120 #region 6. Set up a configuration monitor with the snapshot data-
121 #endregion
122
123
```

Name	Value
@odata.context	https://graph.microsoft.com/beta/\$metadata#admin/configurationManagement/configurationSnapshotJobs/\$entity
id	413726fd-188b-480e-9542-caaf14a81c9a
resources	{microsoft.entra.conditionalAccessPolicy}
resourceLocation	https://graph.microsoft.com/beta/admin/configurationManagement/configurationSnapshots('dc37a8de-bba2-4ddb-82ca-04e1f49fca5a')
description	Baseline for your configured Conditional Access policies
completedDateTime	12.02.2026 20:30:34
tenantId	19e61dac-eccf-427a-94c0-df49ff2f2331
createdAt	12.02.2026 20:27:11
status	partiallySuccessful
displayName	Entra CAP Baseline
createdBy	{user, System.Collections.Hashtable}, [application, System.Collections.Hashtable]



**THREE
HOURS LATER**



Initial run of configuration monitor

The screenshot shows a Microsoft Visual Studio Code interface with a PowerShell script named `UTCM-Demo.ps1`. The script is numbered from 53 to 190. A context menu is open at the top right, listing nine steps related to configuration monitoring. The terminal below shows the execution of the script, specifically the command `$MonitorJob = Invoke-MgGraphRequest -Method GET -Uri $Uri -OutputType PSObject | Select -Expand Value`, which retrieves a configuration monitor object.

```
> UTCM-Demo.ps1 4 x
Users > thomas > Library > CloudStorage > OneDrive-Personal > Community > Workshops > Identity Security - ELDE > > UTCM-Demo.ps1 > abc #region 6. Set up a configuration monitor with the snapshot data
53 > #region 2. Add service principal for UTCM and assign permissions-
95 #endregion
96
97 > #region 3. Connect to Microsoft Graph with the required scopes-
99 #endregion
100
101 > #region 4. Create a snapshot of Conditional Access policy configurations via Microsoft Graph PowerShell SDK-
112 #endregion
113
114 # Wait until the snapshot job is completed before proceeding to the next steps.
115 Invoke-MgGraphRequest -Method GET -Uri "beta/admin/configurationManagement/configurationSnapshotJobs/$(CreatedSnapshot.id)"
116
117 > #region 5. Get the configuration snapshot that was just created-
144 #endregion
145
146 > #region 6. Set up a configuration monitor with the snapshot data-
161 #endregion
162
163 #region 7. Retrieve the configuration monitor details
164 $filter = "displayName eq '$MonitorDisplayName'"
165 $Uri = "beta/admin/configurationManagement/configurationMonitors/?$filter=$filter"
166 $MonitorJob = Invoke-MgGraphRequest -Method GET -Uri $Uri -OutputType PSObject | Select -Expand Value
167 #endregion
168
169 > #region 8. Get the monitoring results from the configuration monitor-
173 #endregion
174
175 # Wait for necessary time based on the frequency set for the monitor to get the monitoring results before proceeding to analyze the results for any drifts in the Conditional Access policies.
176
177 > #region 9. Analyze the monitoring results for any drifts in the Conditional Access policies-
190 #endregion

PROBLEMS 38 AZURE SPELL CHECKER 17 PORTS OUTPUT DEBUG CONSOLE TERMINAL
PS /Users/thomas> $MonitorJob
description : Monitor critical CA
tenantId : 19e61dac-ecff-427a-94c0-df49ff2f2331
status : active
monitorRunFrequencyInHours : 6
mode : monitorOnly
createdDateTime : 12.02.2026 20:32:47
lastModifiedDateTime : 12.02.2026 20:32:47
runAsUTCMServicePrincipal : True
inactivationReason :
createdBy : @{user=; application=}
runningOnBehalfOf : @{user=; application=}
lastModifiedBy : @{user=; application=}
parameters : 
```

PS /Users/thomas>

0 16 17 Failed to initiate Application Insights extension. Check the console for more details or reload the extension to try again.

Ln 146, Col 65 Spaces: 4 UTF-8 LF () PowerShell



Home > Conditional Access | Policies

Admin 4: Require phishing-resistant MFA for all high-privilege roles

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Admin 4: Require phishing-resistant MFA fo...

Assignments

Users, agents or workload identities ⓘ

Specific users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Control access based on who the policy will apply to, such as users and groups, agents, workload identities, directory roles, or external guests. [Learn more](#)

What does this policy apply to?

Users and groups

Include Exclude

Select the users and groups to exempt from the policy

- Guest or external users ⓘ
- Directory roles ⓘ
- Users and groups

Select excluded users and groups

3 users



Adele Vance
AdeleV@c4a8ando.com

...

Home > Conditional Access | Policies

Red Tenant - Require FIDO2 security keys

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Red Tenant - Require FIDO2 security keys

Assignments

Users, agents or workload identities ⓘ

Specific users included

Target resources ⓘ

All resources (formerly 'All cloud apps')

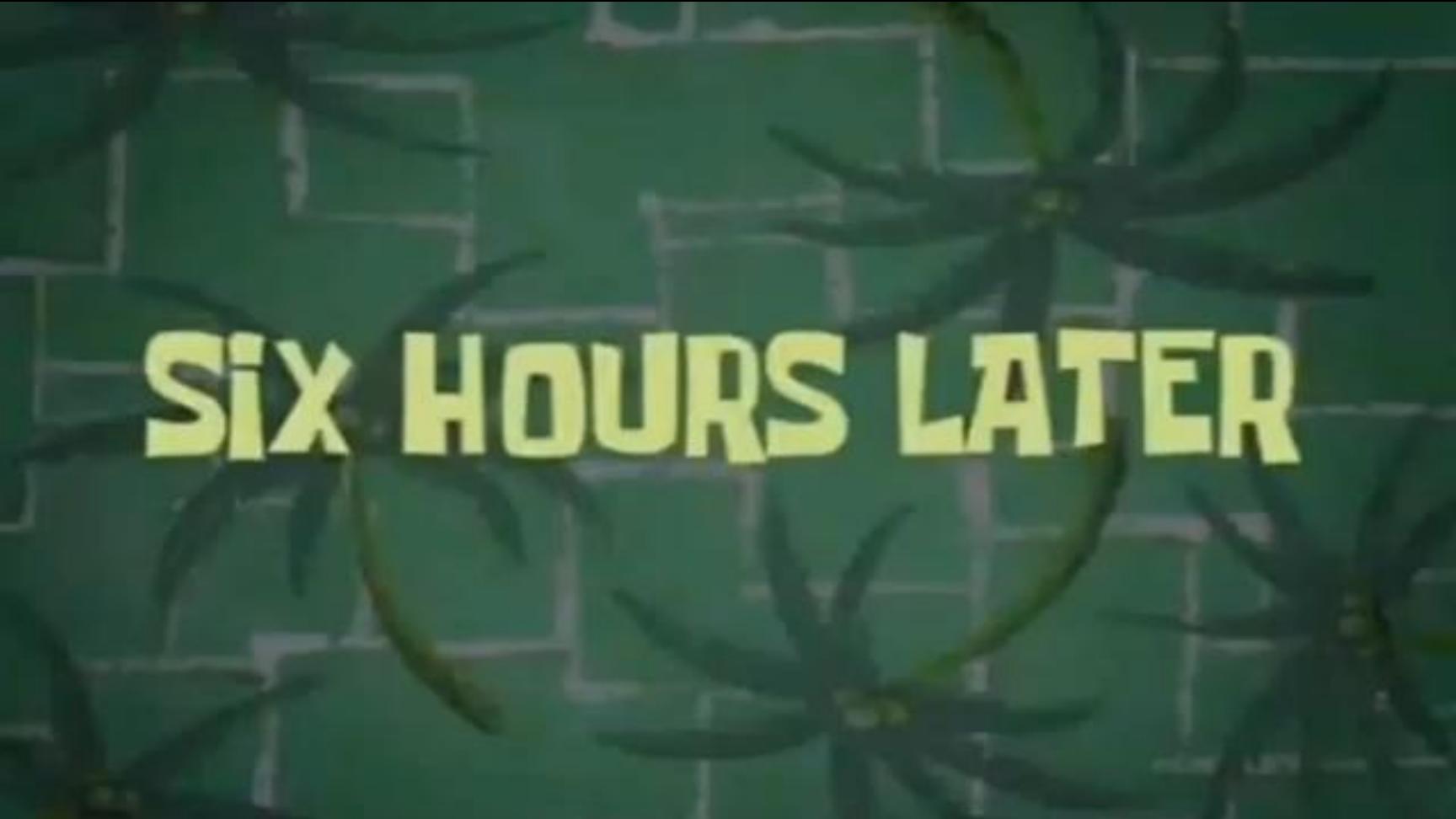
Network NEW ⓘ

Not configured

Enable policy

Report-only On Off

Save



SIX HOURS LATER



The screenshot shows a Microsoft Visual Studio Code (VS Code) window with the following details:

- Title Bar:** Shows the file name "UTCM-Demo.ps1" and line number "4".
- Code Editor:** Displays PowerShell script code. The script performs several steps:
 - #region 6: Sets up a configuration monitor with snapshot data.
 - #region 7: Retrieves configuration monitor details.
 - #region 8: Gets monitoring results from the configuration monitor. It uses a filter (\$Filter = "monitorId eq '\$(\$MonitorJob[0].id)'") and sends a GET request to the Microsoft Graph API endpoint \$Uri = "/beta/admin/configurationManagement/configurationMonitoringResults?\$.filter=\$Filter". The results are stored in \$MonitorResults.
 - #region 9: Analyzes monitoring results for drifts in Conditional Access policies. It waits for a specified frequency before proceeding.
- Right Panel:** Shows a list of 9 steps:
 - Define a variable
 - Get the configuration monitor
 - Create a PowerShell object
 - Get the last created
 - Get the last modified
 - Get the last updated
 - Get the last modified date
 - Get the last updated date
 - Analyze the results
- Bottom Navigation Bar:** Includes tabs for PROBLEMS, AZURE, SPELL CHECKER, PORTS, OUTPUT, DEBUG CONSOLE, and TERMINAL. The TERMINAL tab is active.
- Terminal:** Shows the PowerShell command PS /Users/thomas> \$monitorResults[1] followed by its output, which includes fields like tenantId, runInitiationDateTime, runCompletionDateTime, runStatus, driftsCount, driftsFixed, and runType.
- Status Bar:** Shows the status "Ln 169, Col 1 (326 selected) Spaces: 4 UTF-8 LF () PowerShell" and icons for Application Insights, GitHub, and other extensions.

Summary & QA

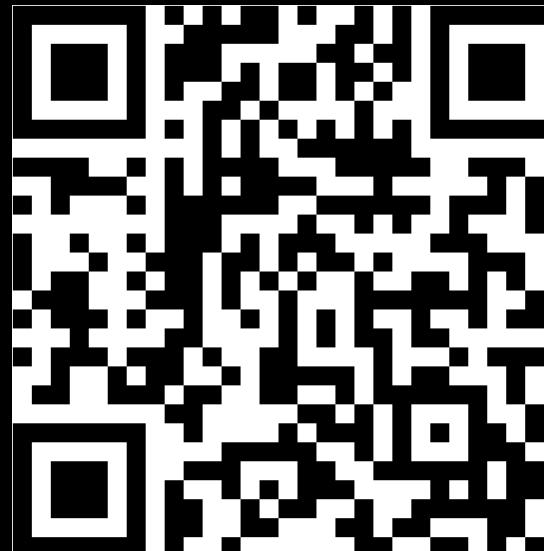


Session Feedback – THANK YOU ☺

Please evaluate this session using QR Code during next 30 min

- or -

Make your session feedback on your way out of the room



<https://smiley.link/DJWTGBTN>