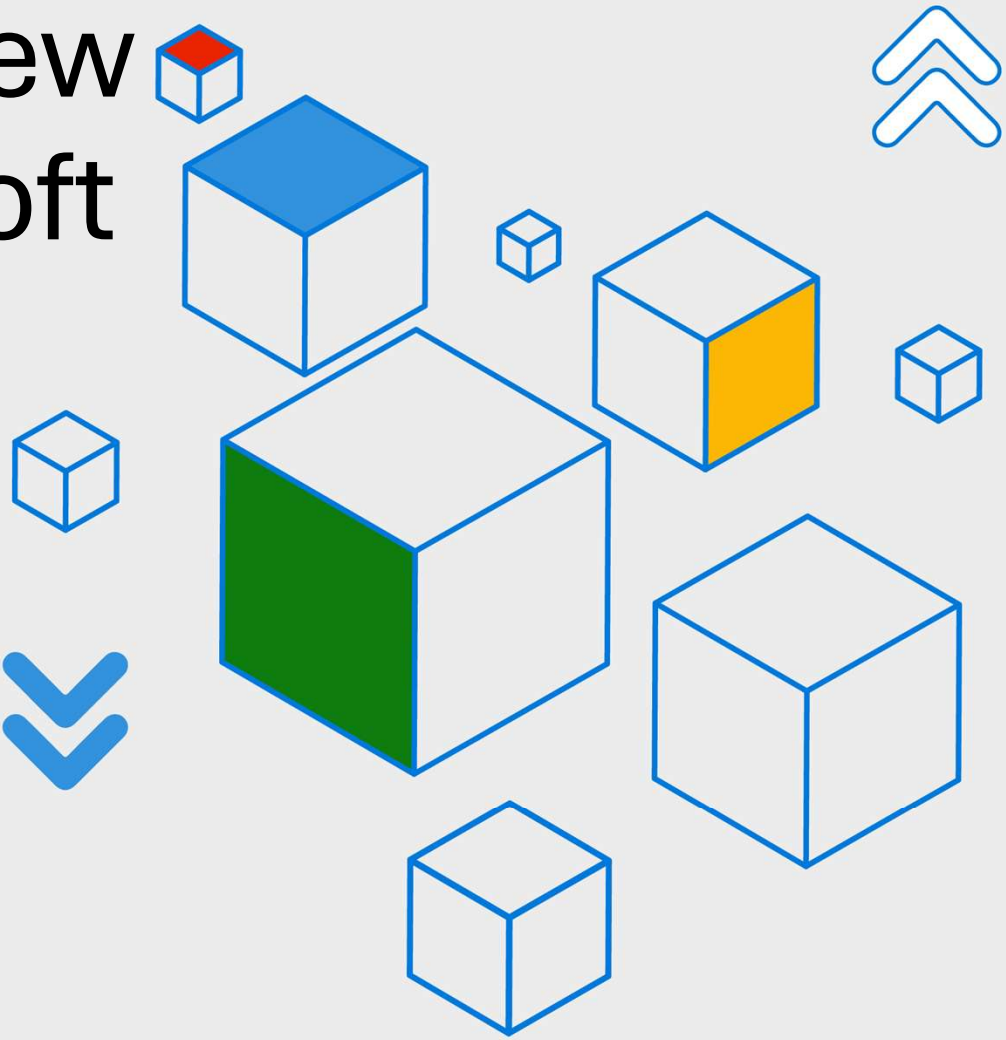
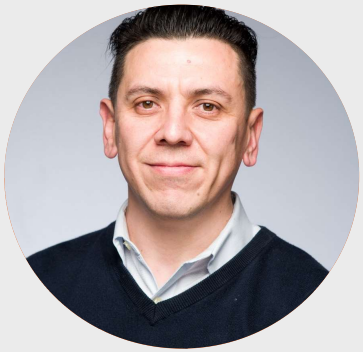
What's New in Microsoft Entra ID August 2023



Grace Picking

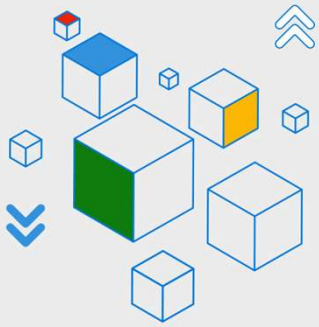


Jorge Lopez

425Show

425Show

Azure AD is being renamed to Microsoft Entra ID



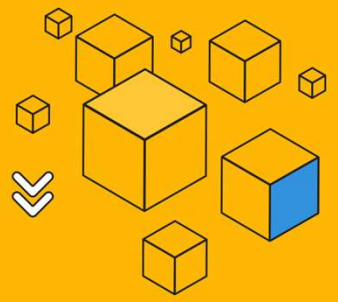
Overview : We are excited to inform you that Azure AD, which has been part of the Microsoft Entra product family since 2022, is becoming Microsoft Entra ID!

- **Microsoft Entra ID** (formerly Azure AD)
- **Microsoft Entra ID Protection**
- (formerly Identity Protection)
- **Microsoft Entra ID Governance** (formerly Identity Governance)
- **Microsoft Entra Workload ID** (formerly Workload Identities)
- **Microsoft Entra External ID** (formerly External Identities. Special note: Azure AD B2C will remain as is.)

425Show

Microsoft Entra ID Governance

The following governance features went GA and are part of the Microsoft Entra ID Governance SKU



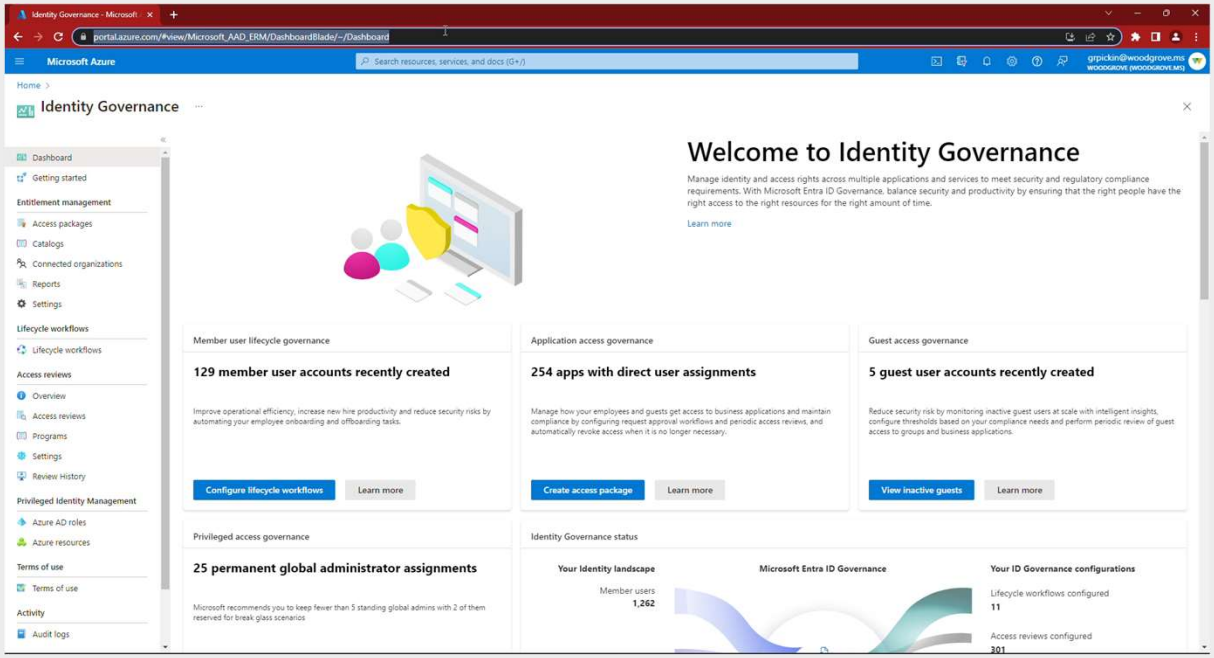
Identity Governance dashboard	Discovers usage information about various Identity Governance & Administration (IGA) features configured in your tenant. It then gives you an at-a-glance view of your current state of Identity Governance, with actionable buttons and quickly accessible links to documentation.
Lifecycle workflows (LCW)	Enables you to use custom workflows to automate identity lifecycle management tasks for your Microsoft Entra ID users by managing your joiner, mover, and leaver lifecycle processes. With LCW, you can leverage Microsoft Entra ID to confidently deploy workflows to configure out-of-the-box actions to onboard and offboard your employees.
Access reviews for inactive users	Allows admins to review and address stale accounts that haven't been active for a specified period. Admins can set a specific duration to determine inactive accounts which were not used for either interactive or non-interactive sign-in activities. As part of the review process, stale accounts can automatically be removed.
Access reviews: Machine Learning (ML) based recommendation on User-to-Group Affiliation	Provides ML-based recommendations to the reviewers of an access review, making the review experience easier and more accurate. This recommendation leverages a scoring mechanism and compares users' relative affiliation with other users in the group, based on the organization's reporting structure. Users who are very distant from other users in the group have low affiliation and our system then provides a Deny recommendation.
Entitlement management custom extensions to Logic Apps	Extends the access lifecycle with specific processes and business logic when access is requested or about to expire. You can create tickets for manual access provisioning in disconnected systems, send custom notifications, automate additional access-related configuration in your business apps, or integrate complex governance, risk, and compliance (GRC) checks for more advanced scenarios.
Require Microsoft Entra Verified ID from specific issuer for entitlement management	As an access package manager, you can require that requestors present a verified ID containing credentials from a trusted issuer. Approvers can then quickly view if a user's verifiable credentials were valid at the time that the user presented their credentials and submitted the access package request.
Assigning access automatically with no requests required	Enables you to automate processes for access lifecycle management by assigning access to users based on their attributes coming from your HR system or other systems, without the need of access requests or administrative interaction.

425Show

Identity Governance dashboard

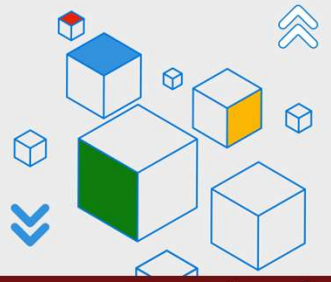
Stage : GA **Product family :** Microsoft Entra ID Governance

Overview : Discovers usage information about various Identity Governance & Administration (IGA) features configured in your tenant. It then gives you an at-a-glance view of your current state of Identity Governance, with actionable buttons and quickly accessible links to documentation.



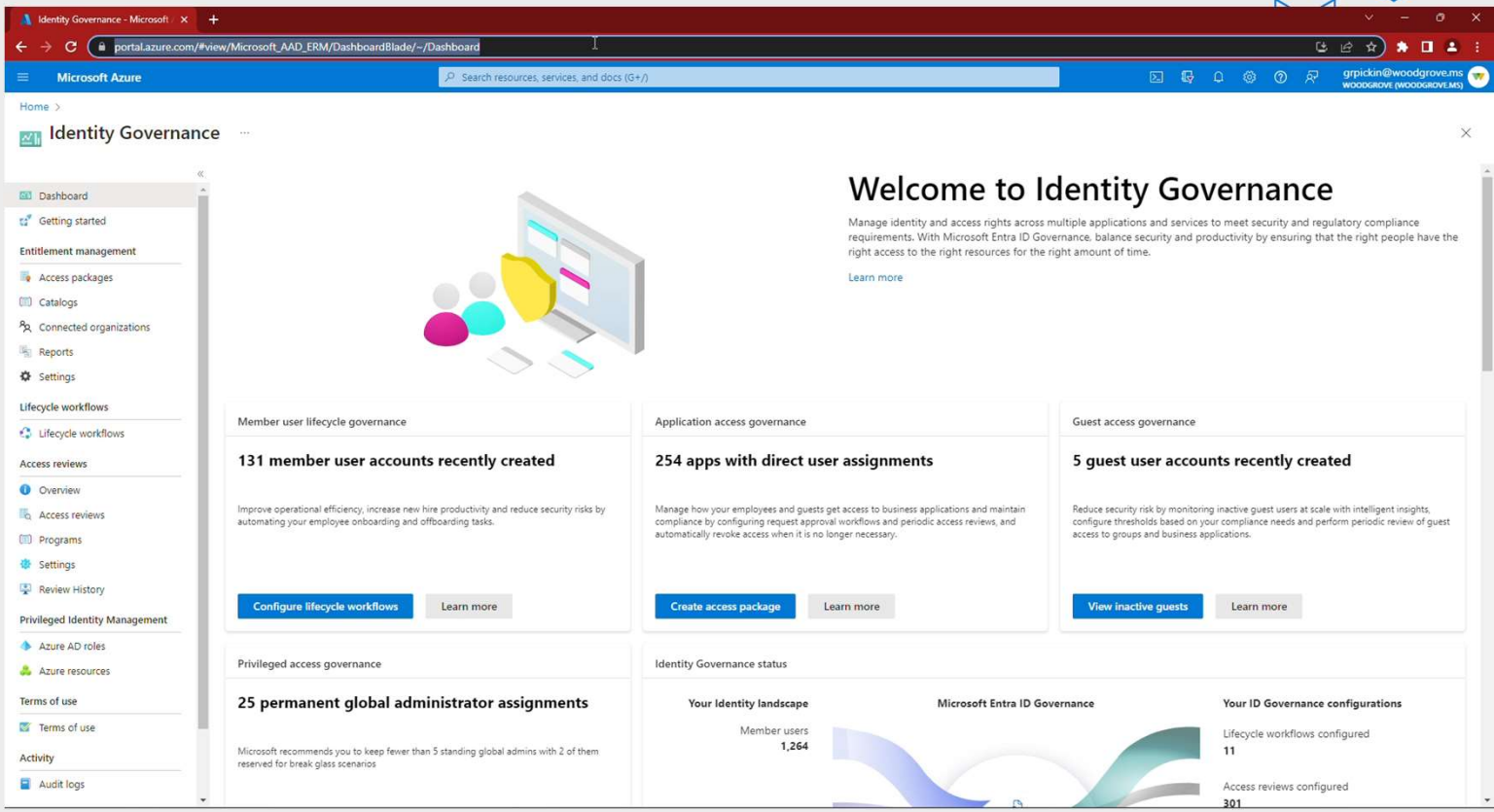
425Show

Lifecycle workflows (LCW)



Stage : GA **Product family :** Microsoft Entra ID Governance

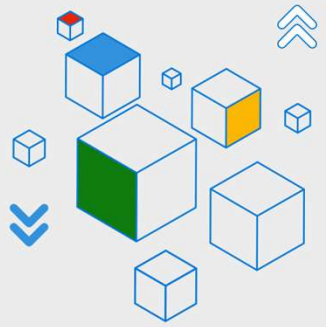
Overview : Enables you to use custom workflows to automate identity lifecycle management tasks for your Microsoft Entra ID users by managing your joiner, mover, and leaver lifecycle processes. With LCW, you can leverage Microsoft Entra ID to confidently deploy workflows to configure out-of-the-box actions to onboard and offboard your employees.



https://aka.ms/425show/EntraIDG/Overview

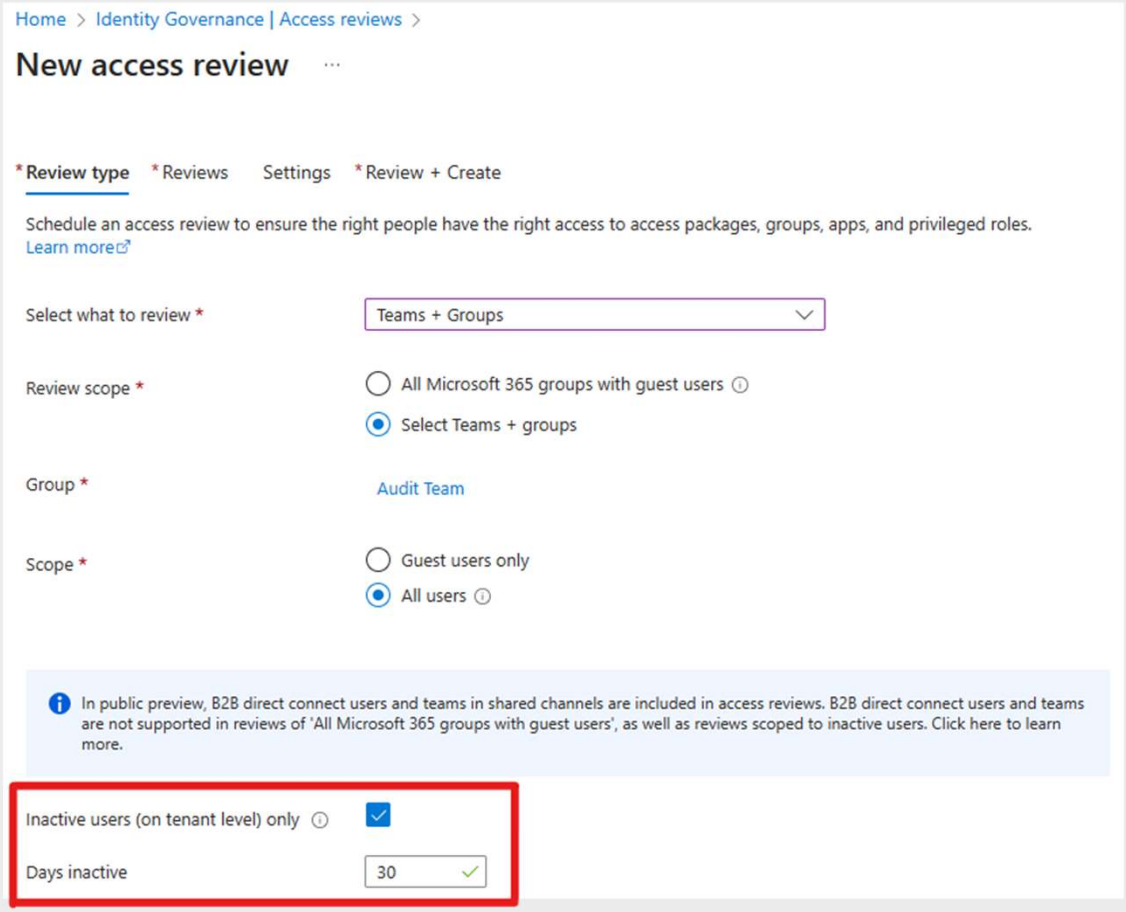
425Show

Access reviews for inactive users



Stage : GA **Product family :** Microsoft Entra ID Governance

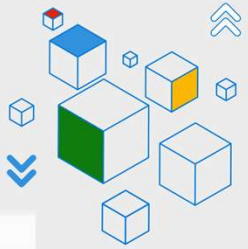
Overview : Allows admins to review and address stale accounts that haven't been active for a specified period. Admins can set a specific duration to determine inactive accounts which were not used for either interactive or non-interactive sign-in activities. As part of the review process, stale accounts can automatically be removed.



https://aka.ms/425show/EntraIDG/Overview

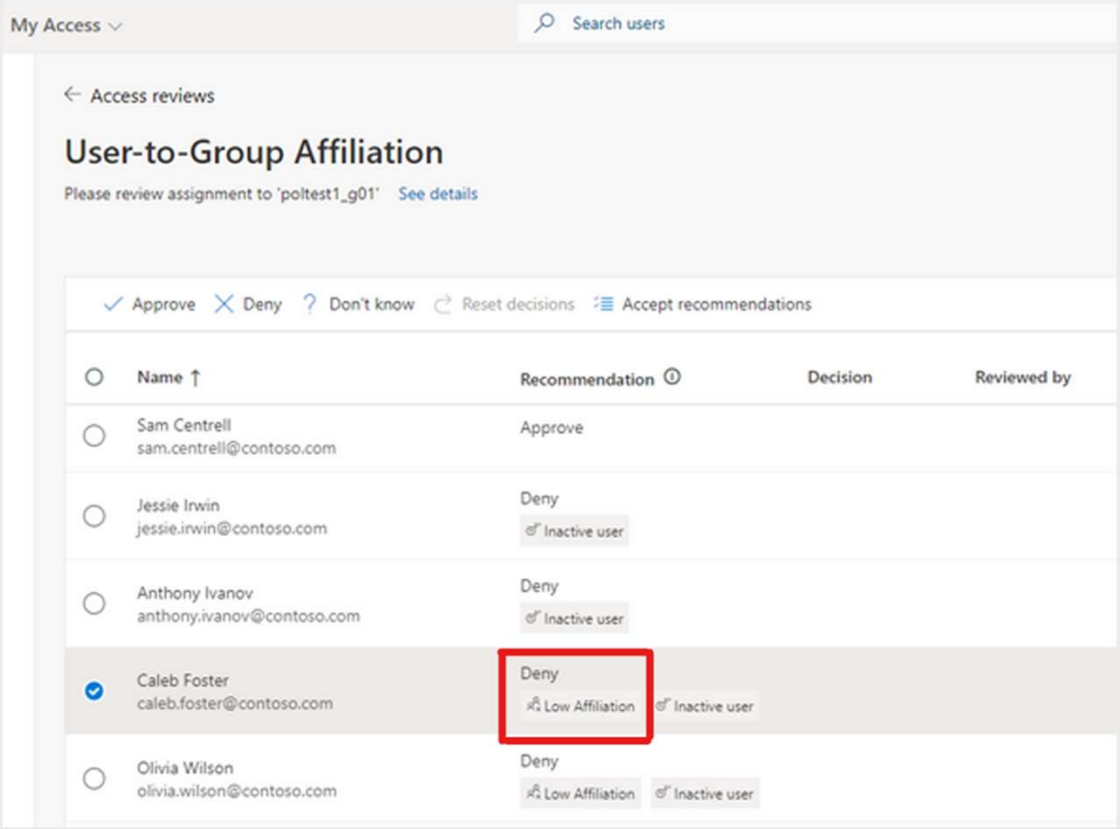
425Show

Access reviews: Machine Learning (ML) based recommendation on User-to-Group Affiliation



Stage : GA **Product family :** Microsoft Entra ID Governance

Overview Provides ML-based recommendations to the reviewers of an access review, making the review experience easier and more accurate. This recommendation leverages a scoring mechanism and compares users' relative affiliation with other users in the group, based on the organization's reporting structure. Users who are very distant from other users in the group have low affiliation and our system then provides a Deny recommendation.



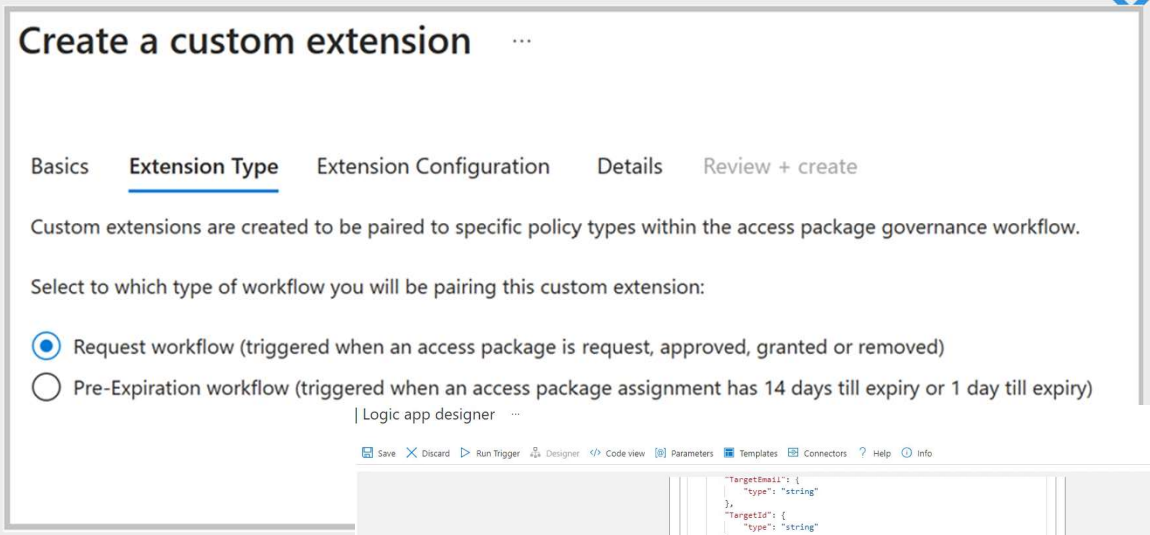
https://aka.ms/425show/EntraIDG/Overview

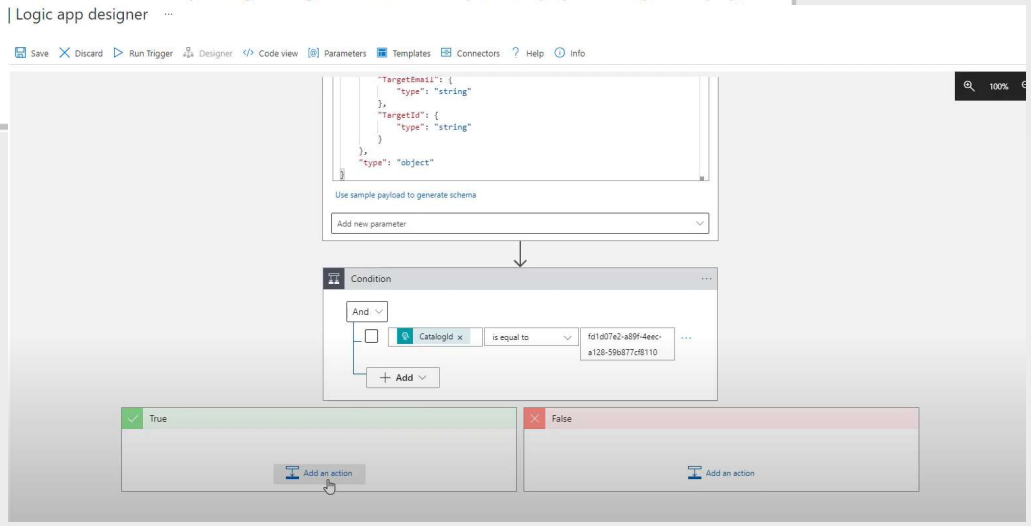
425Show

Entitlement management custom extensions to Logic Apps

Stage : GA **Product family :** Microsoft Entra ID Governance

Overview : Extends the access lifecycle with specific processes and business logic when access is requested or about to expire. You can create tickets for manual access provisioning in disconnected systems, send custom notifications, automate additional access-related configuration in your business apps, or integrate complex governance, risk, and compliance (GRC) checks for more advanced scenarios.

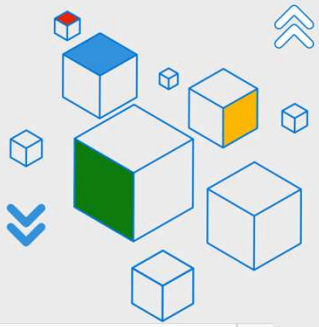




https://aka.ms/425show/EntraIDG/Overview

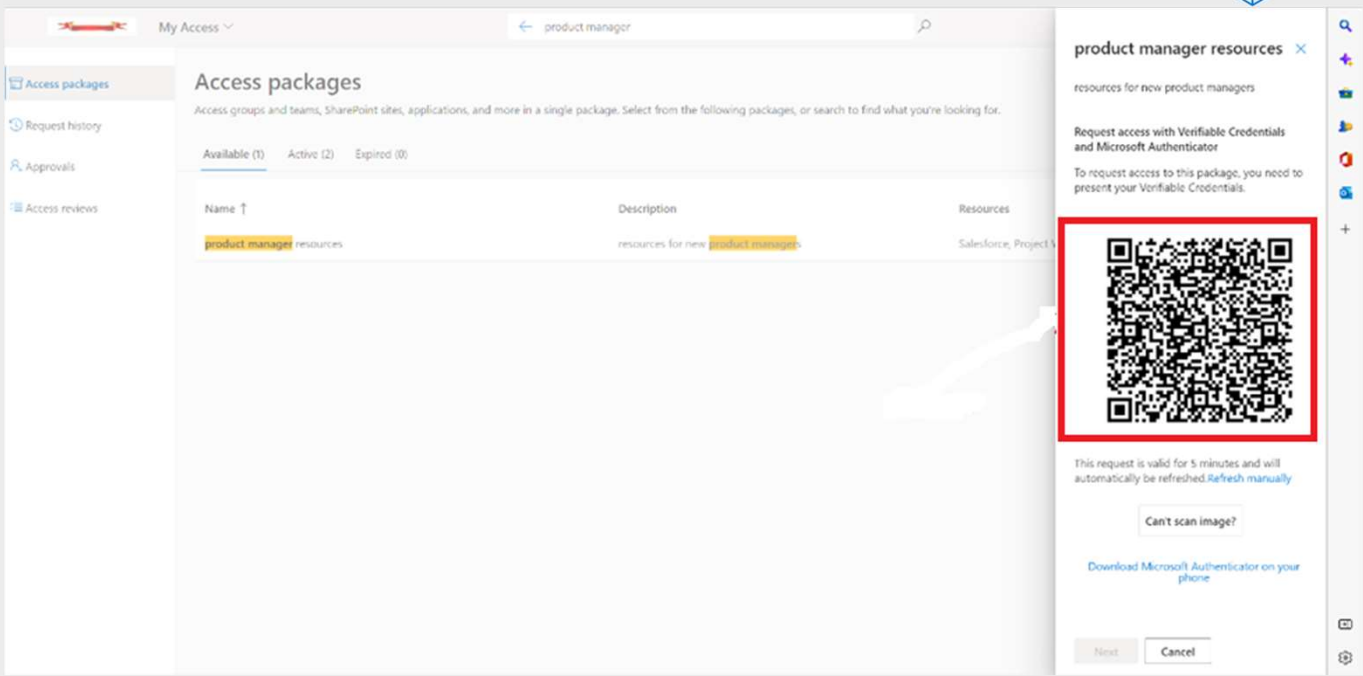
425Show

Require Microsoft Entra Verified ID from specific issuer for entitlement management



Stage : GA **Product family :** Microsoft Entra ID Governance

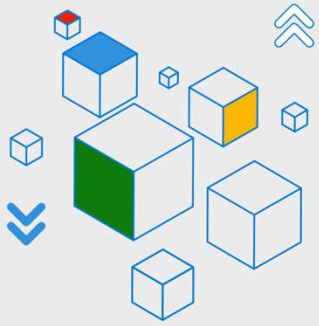
Overview : As an access package manager, you can require that requestors present a verified ID containing credentials from a trusted issuer. Approvers can then quickly view if a user's verifiable credentials were valid at the time that the user presented their credentials and submitted the access package request.



https://aka.ms/425show/EntraIDG/Overview

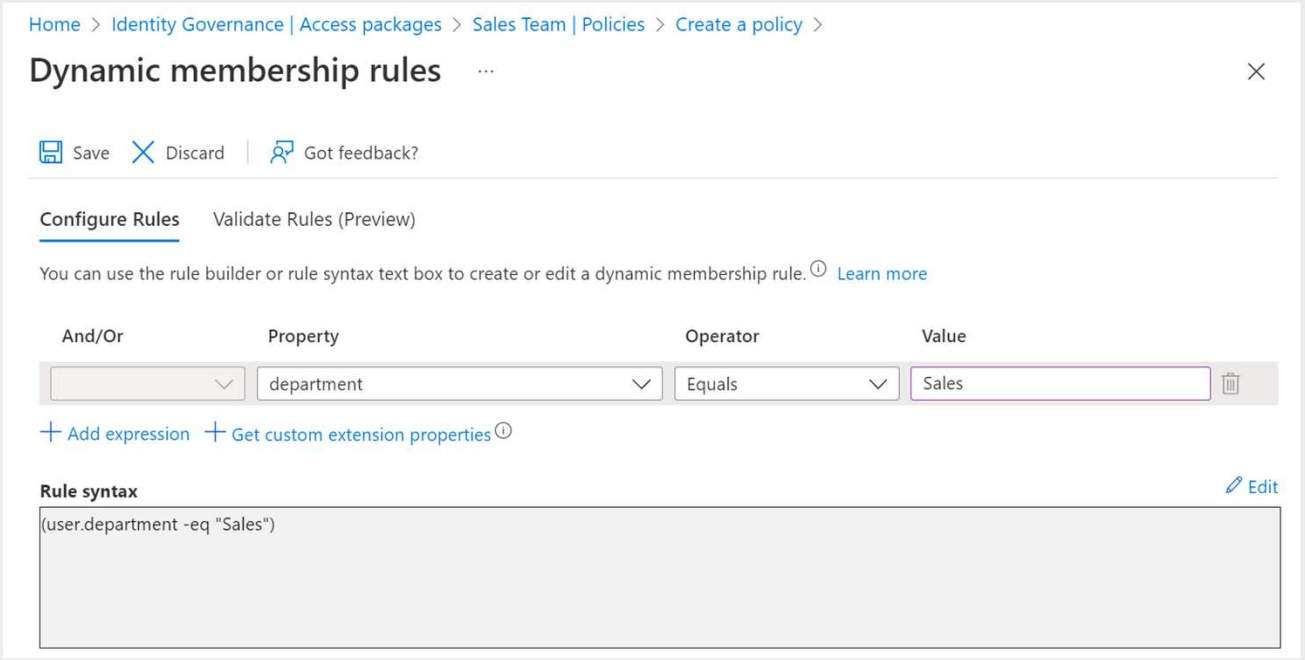
425Show

Assigning access automatically with no requests required



Stage : GA **Product family :** Microsoft Entra ID Governance

Overview : Enables you to automate processes for access lifecycle management by assigning access to users based on their attributes coming from your HR system or other systems, without the need of access requests or administrative interaction.



https://aka.ms/425show/EntraIDG/Overview

425Show

Enhanced company branding for sign-in experiences

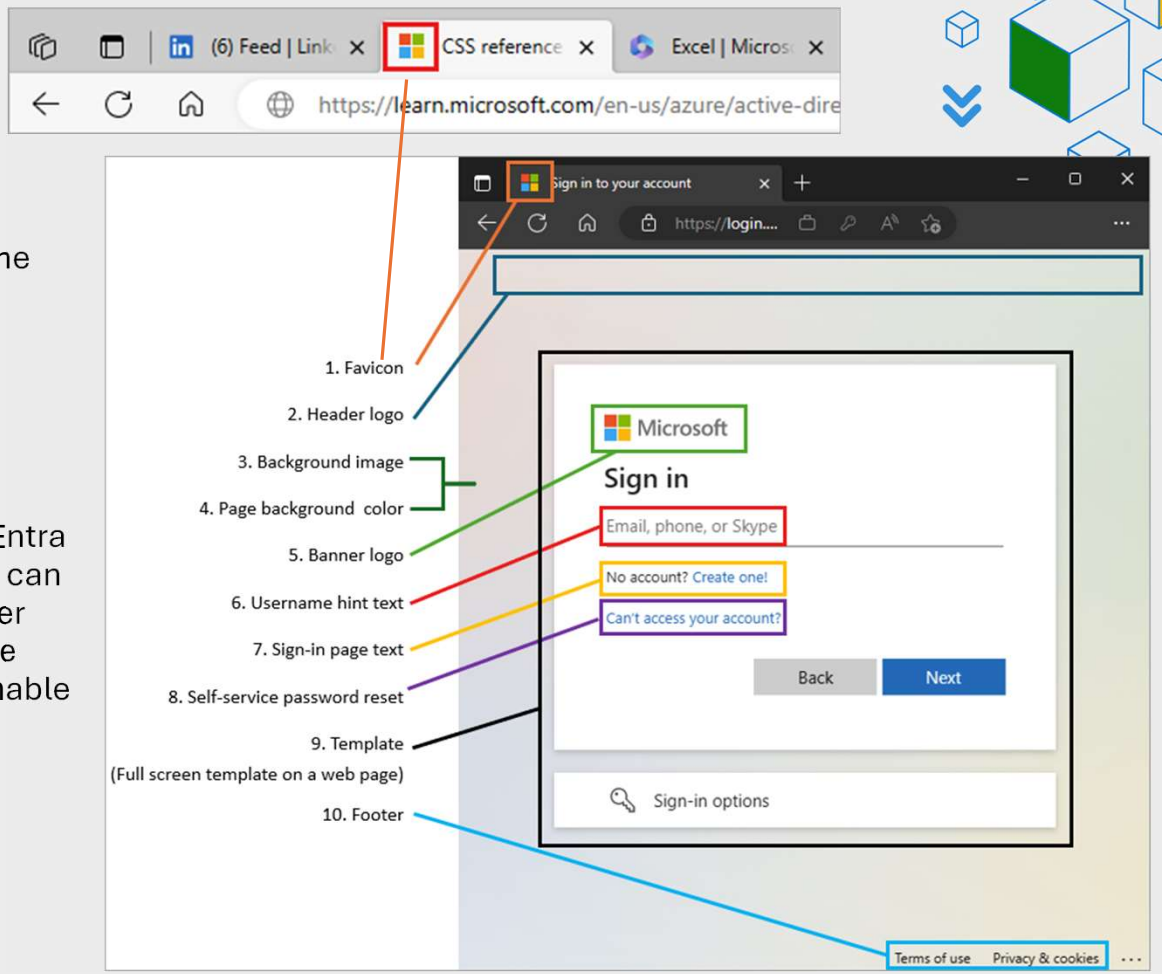
Stage : GA

Product family : Microsoft Entra ID

License : Adding custom branding requires one of the following licenses:

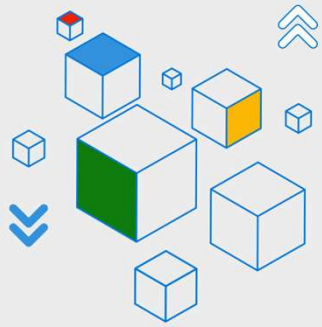
- Azure AD Premium 1
- Azure AD Premium 2
- Office 365 (for Office apps)

Create a custom look and feel for users' Microsoft Entra ID and Microsoft 365 sign-in experiences. Now, you can customize self-service password reset (SSPR), footer hyperlinks, and the browser icon. Also, you can style sign-in experiences by applying custom CSS and enable a header and footer by using one of the pre-defined templates.



425Show

Authentication methods reporting API



Stage : GA

Product family : Microsoft Entra ID

/Internet Access /Private Access

License : An Azure AD Premium P1 or P2 license is required to access usage and insights. Azure AD Multi-Factor Authentication and self-service password reset (SSPR)

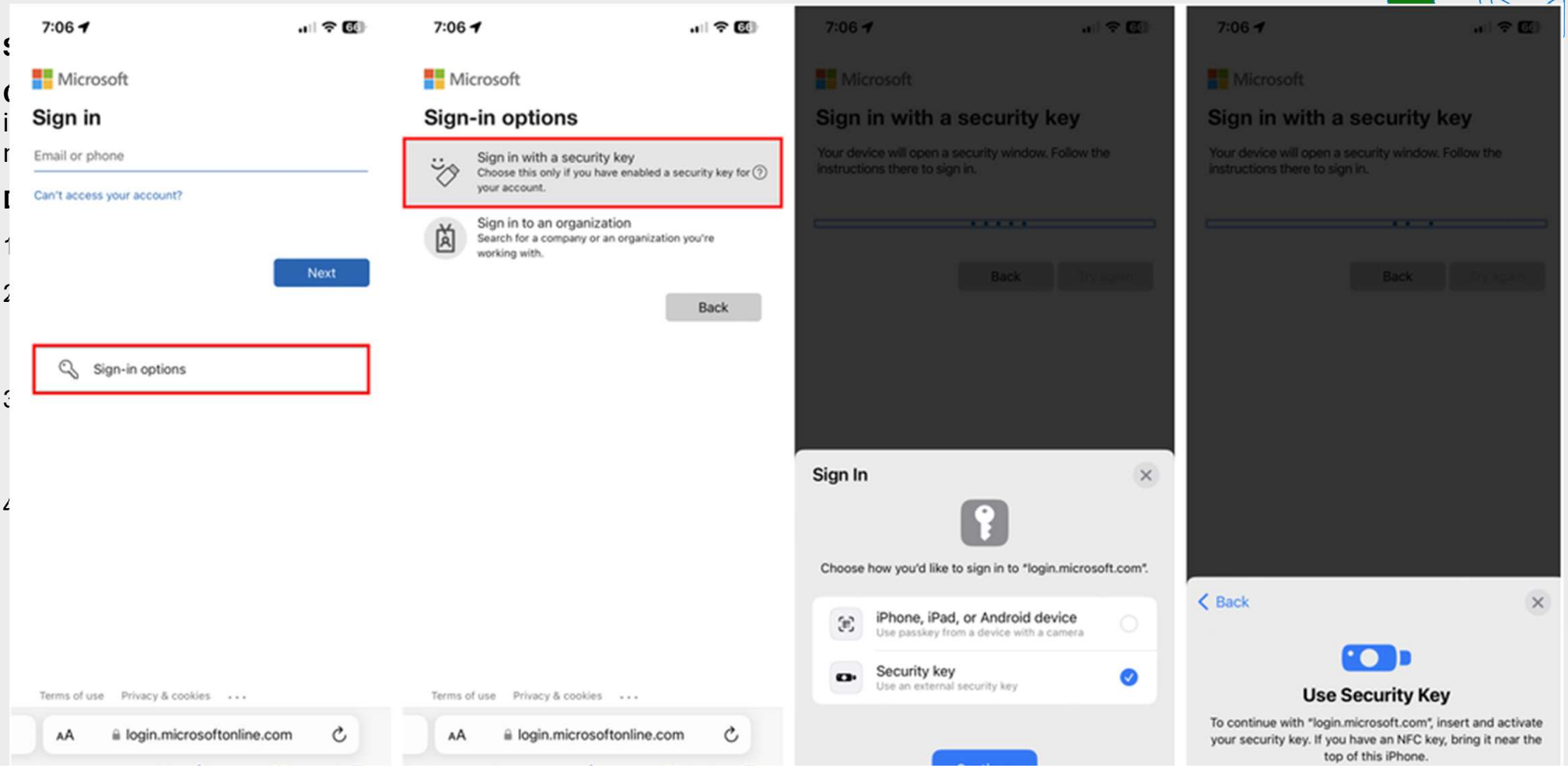
Overview : The new authentication methods activity dashboard enables admins to monitor authentication method registration and usage across their organization. This reporting capability provides your organization with the means to understand what methods are being registered and how they're being used.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "@odata.context":
"https://graph.microsoft.com/v1.0/$metadata#reports/authenticationMethods/userRegistratio
s",
  "value": [
    {
      "id": "86462606-fde0-4fc4-9e0c-a20eb73e54c6",
      "userPrincipalName": "AlexW@Contoso.com",
      "userDisplayName": "Alex Wilber",
      "isAdmin": false,
      "isSsprRegistered": false,
      "isSsprEnabled": false,
      "isSsprCapable": false,
      "isMfaRegistered": true,
```

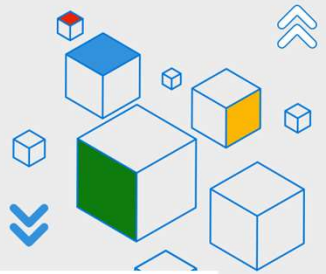
425Show

FIDO2 support on iOS and macOS browsers



425Show

Entitlement management support in Conditional Access (CA)

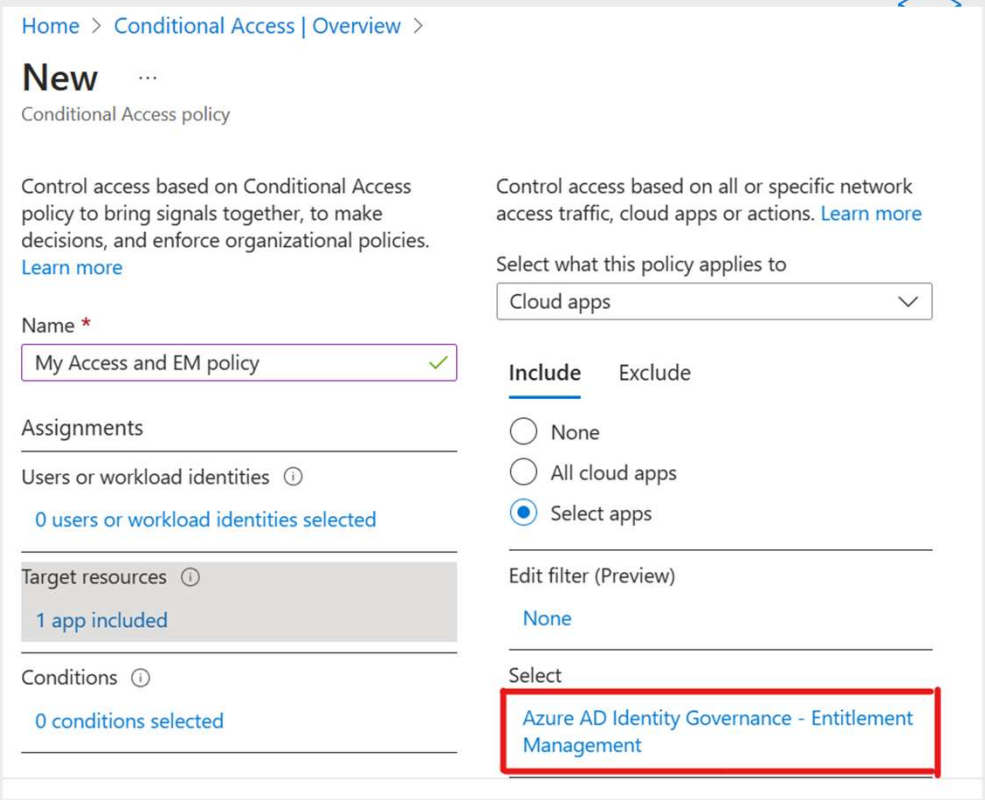


Stage : GA

Product family : Microsoft Entra ID Governance

License : Microsoft Entra ID Governance, You can set up a trial of Microsoft Entra ID Governance at https://aka.ms/EntraIDGovTrial.

Overview : Enables you to include or exclude entitlement management in CA policies, better setting up your organization for self-service onboarding and CA policy exception management scenarios. The Entitlement Management service is now targetable in the conditional access policy for inclusion or exclusion of applications. By enabling the inclusion or exclusion of Entitlement Management and/or My Access in conditional access policies, your organization is better set up for self-service onboarding and conditional access policy exception management scenarios.



425Show

Recommendation to migrate ADAL apps to MSAL

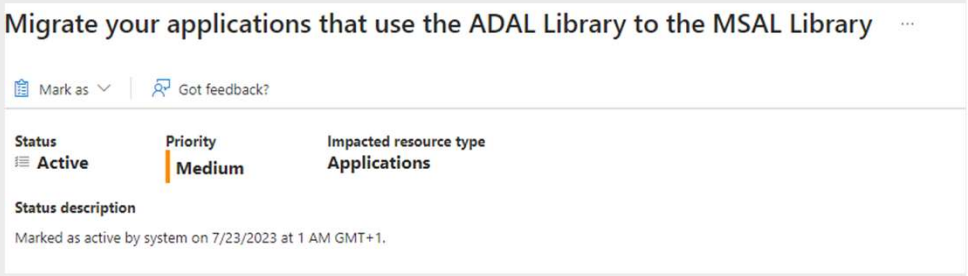
Stage : GA

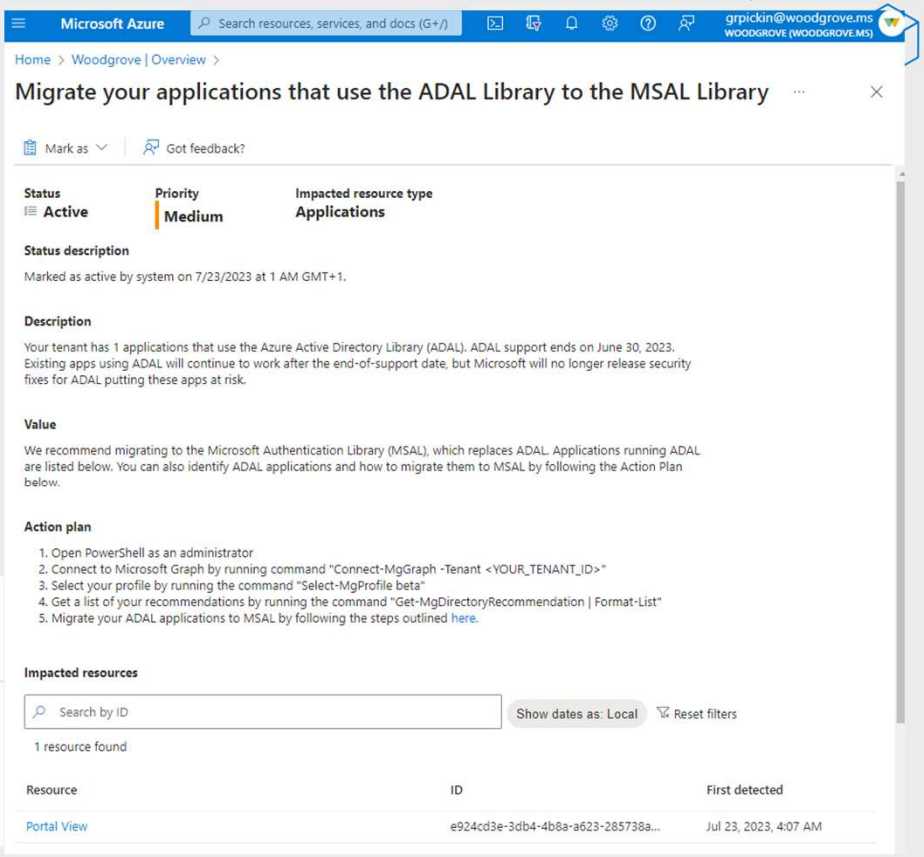
Product family : Microsoft Entra ID

Overview : With Azure Active Directory Authentication Library (ADAL) having been retired on June 30th, this recommendation helps you identify apps using the legacy ADAL via the Azure portal, Microsoft Graph API and PowerShell.

Deployment Steps:

The first step to migrating your apps from ADAL to MSAL is to identify all applications in your tenant that are currently using ADAL. You can identify your apps in the Azure portal or programmatically.





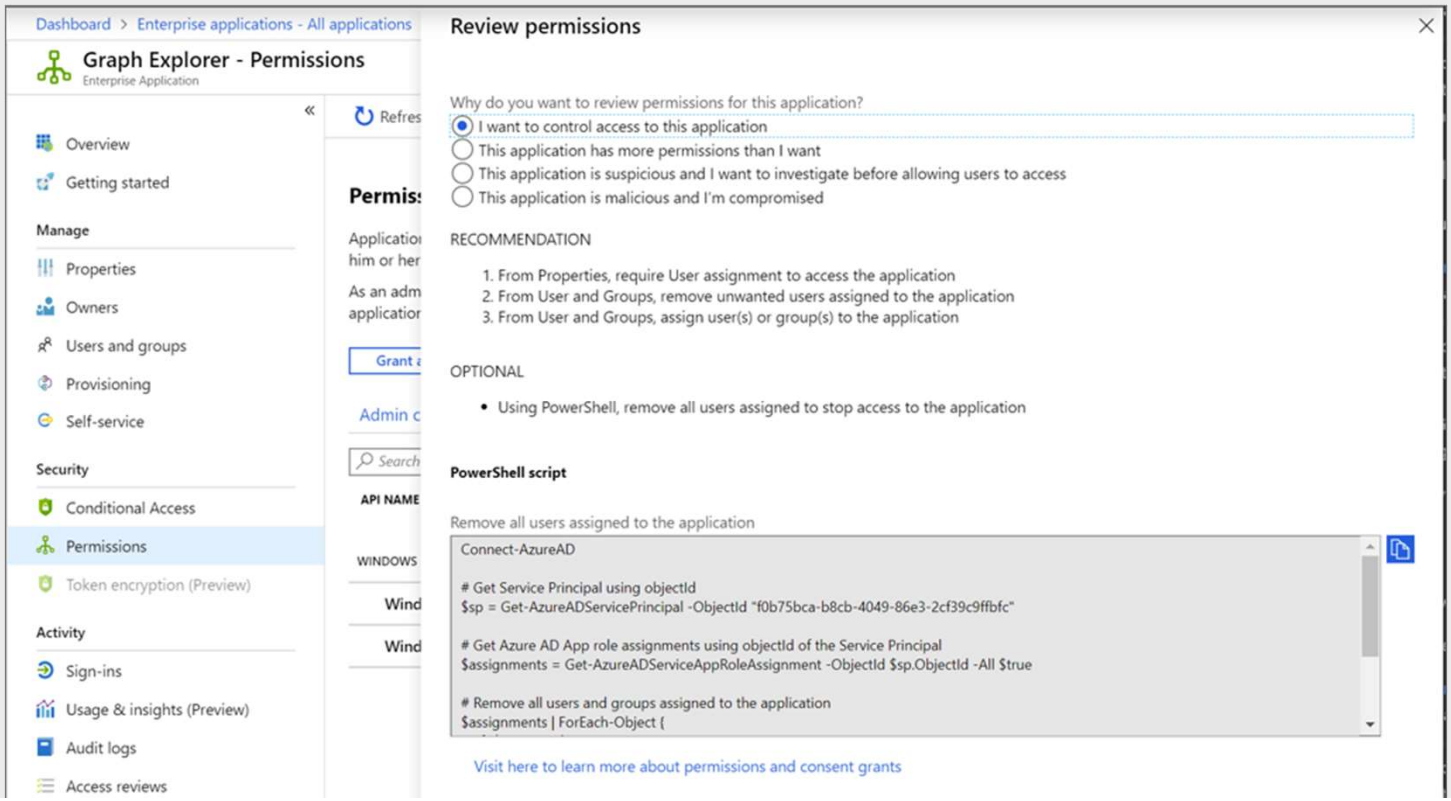
425Show

Revoke previously granted tenant-wide permissions

Stage : GA

Product family : Microsoft Entra ID

Overview : Enables you to revoke an application's permissions that have been granted for the entire organization through admin consent.



425Show

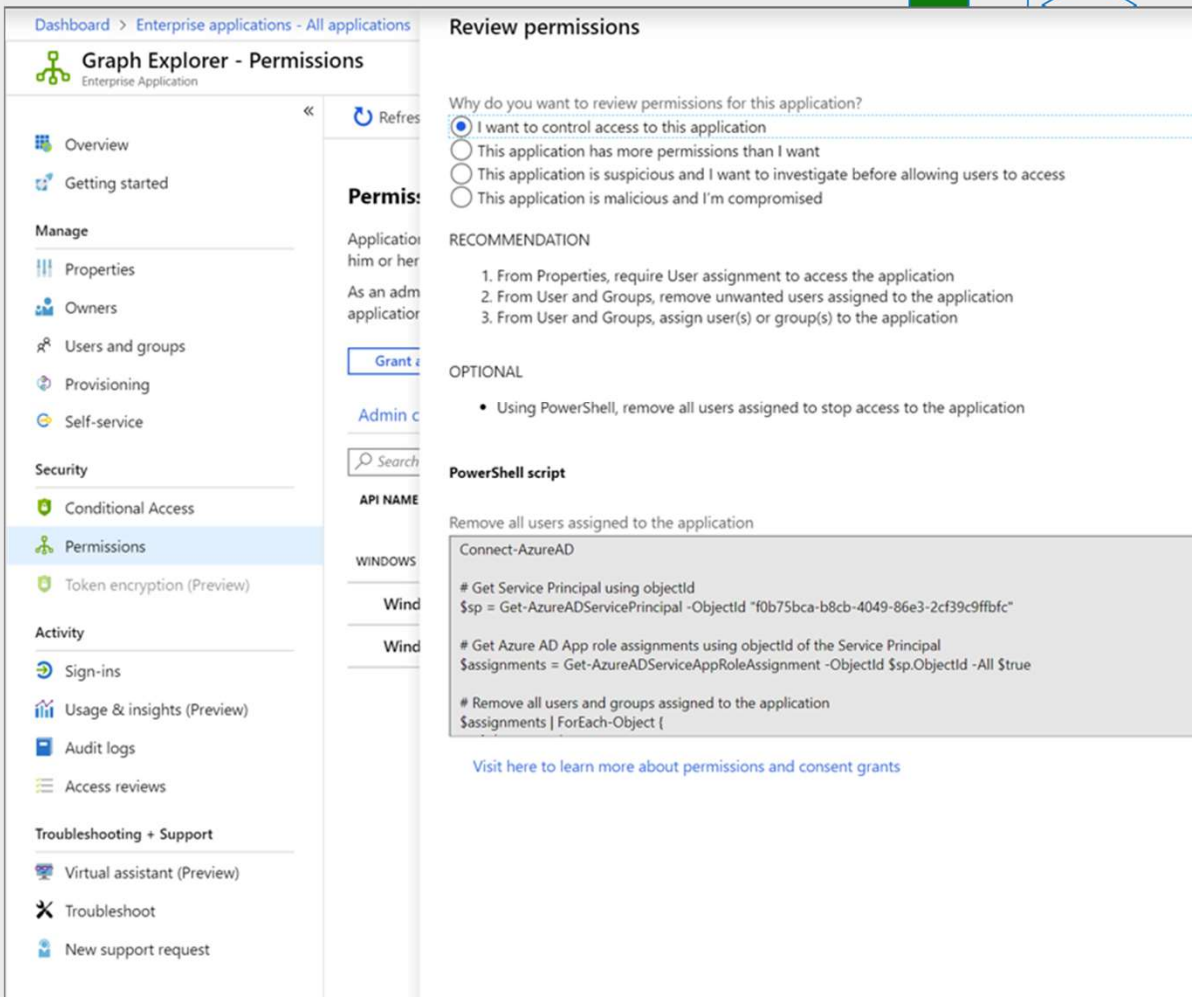
Revoke previously granted tenant-wide permissions

To revoke an application's permissions that have been granted for the entire organization:

1. Sign in to the Azure portal using one of the roles listed in the prerequisites section.
2. Select Azure Active Directory, and then select Enterprise applications.
3. Select the application that you want to restrict access to.
4. Select Permissions.
5. The permissions listed in the Admin consent tab apply to your entire organization. Choose the permission you would like to remove, select the ... control for that permission, and then choose Revoke permission.

To review an application's permissions:

1. Sign in to the Azure portal using one of the roles listed in the prerequisites section.
2. Select Azure Active Directory, and then select Enterprise applications.
3. Select the application that you want to restrict access to.
4. Select Permissions. In the command bar, select Review permissions. Screenshot of the review permissions window.
5. Give a reason for why you want to review permissions for the application by selecting any of the options listed after the question, Why do you want to review permissions for this application?



425Show

Microsoft Entra ID Protection: Unfamiliar sign-in properties

Stage : GA

Product family : Microsoft Entra ID Protection

License : Azure AD Premium P2

Overview : The Unfamiliar sign-in properties detection shows which properties are unfamiliar in the Additional Info field in the Risk detection report details.

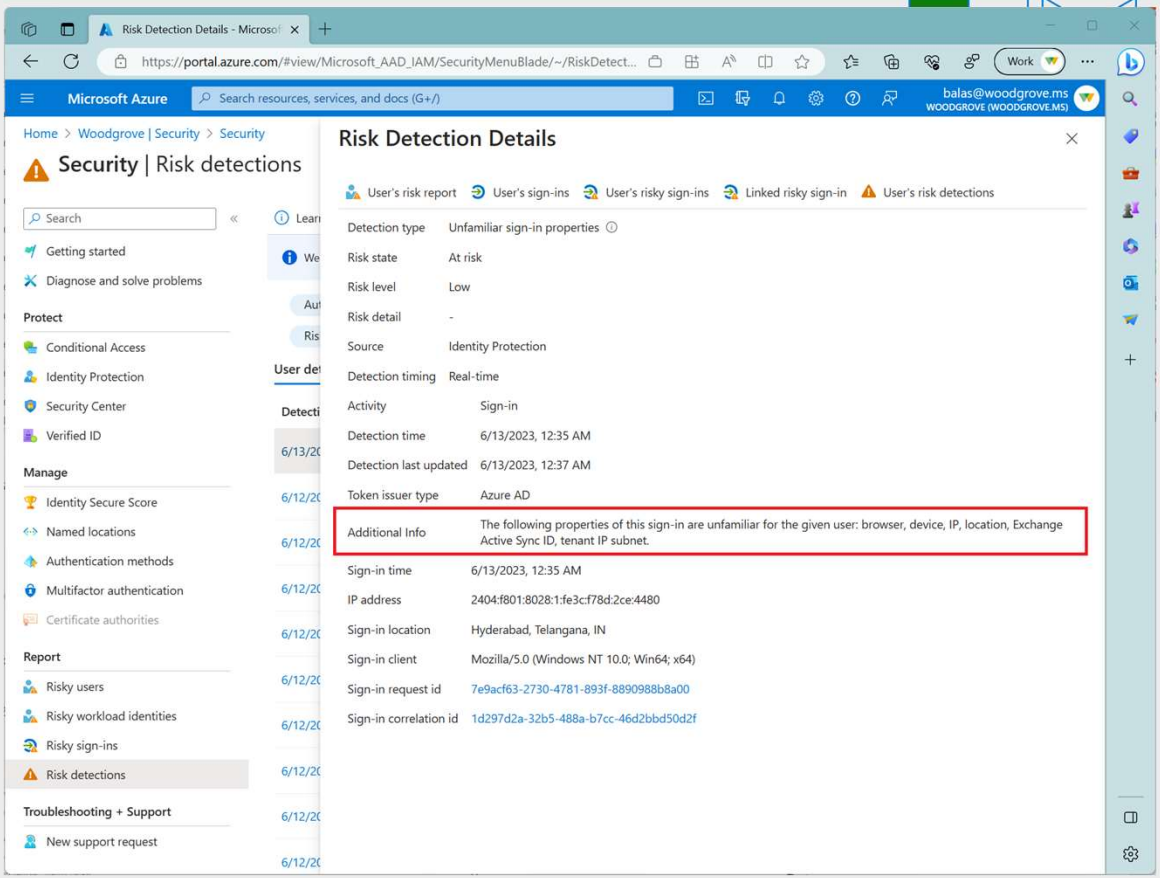
Deployment Steps:

Step 1: Review existing reports

Step 2: Plan for Conditional Access risk policies

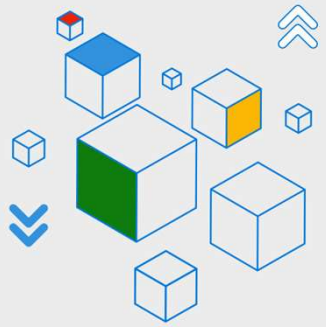
Step 3: Configure your policies

Step 4: Monitoring and continuous operational need



425Show

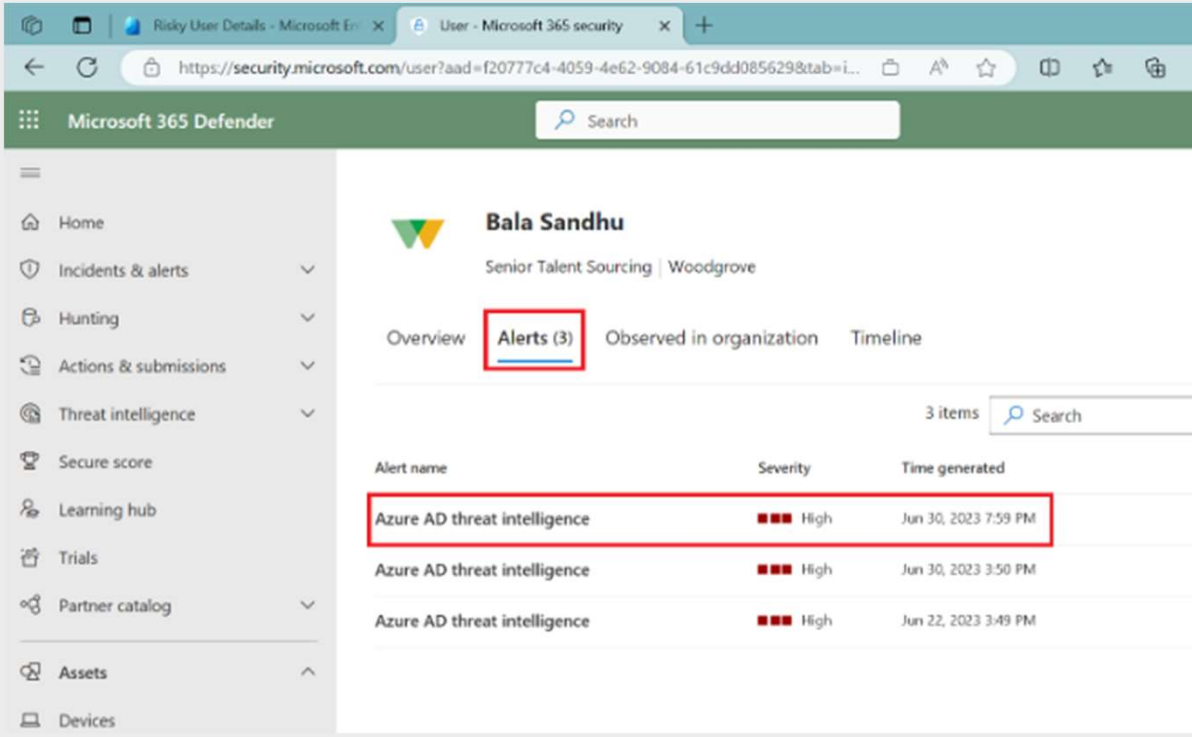
Integration of Microsoft Entra ID Protection with Microsoft 365 Defender



Stage : GA

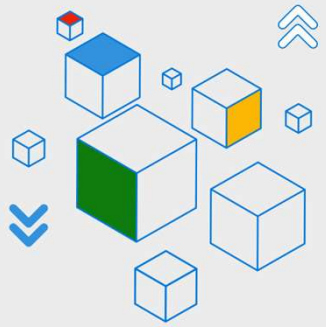
Product family : Microsoft Entra ID Protection

Overview : Microsoft Entra ID Protection alerts are correlated into related incidents along with alerts from the other security domains and can be reviewed directly in Microsoft 365 Defender for a holistic view of an end-to-end attack. Organizations who have deployed Microsoft 365 Defender and Microsoft Defender for Identity gain extra value from Identity Protection signals. This value comes in the form of enhanced correlation with other data from other parts of the organization and extra automated investigation and response.



425Show

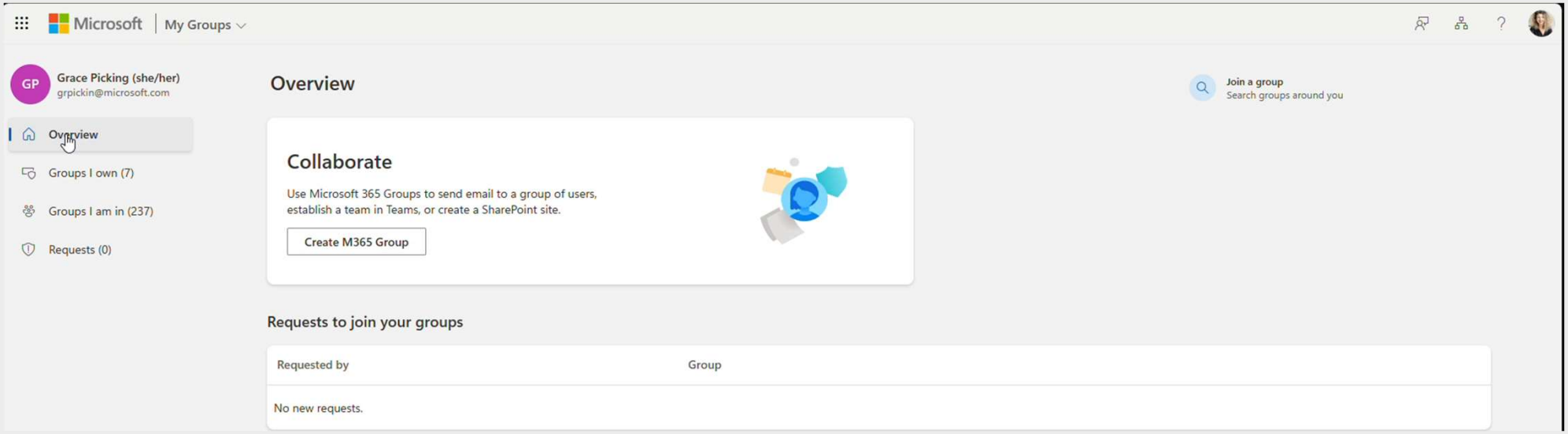
New My Groups experience



Stage : GA

Overview : My Groups is an end-user group management experience that empowers admins to delegate group management to end users so they can manage their group membership and group lifecycle by themselves. The new My Groups experience improves navigation for end users, addresses limitations My Groups has today, and aligns with other end user experiences.

https://myaccount.microsoft.com/groups/



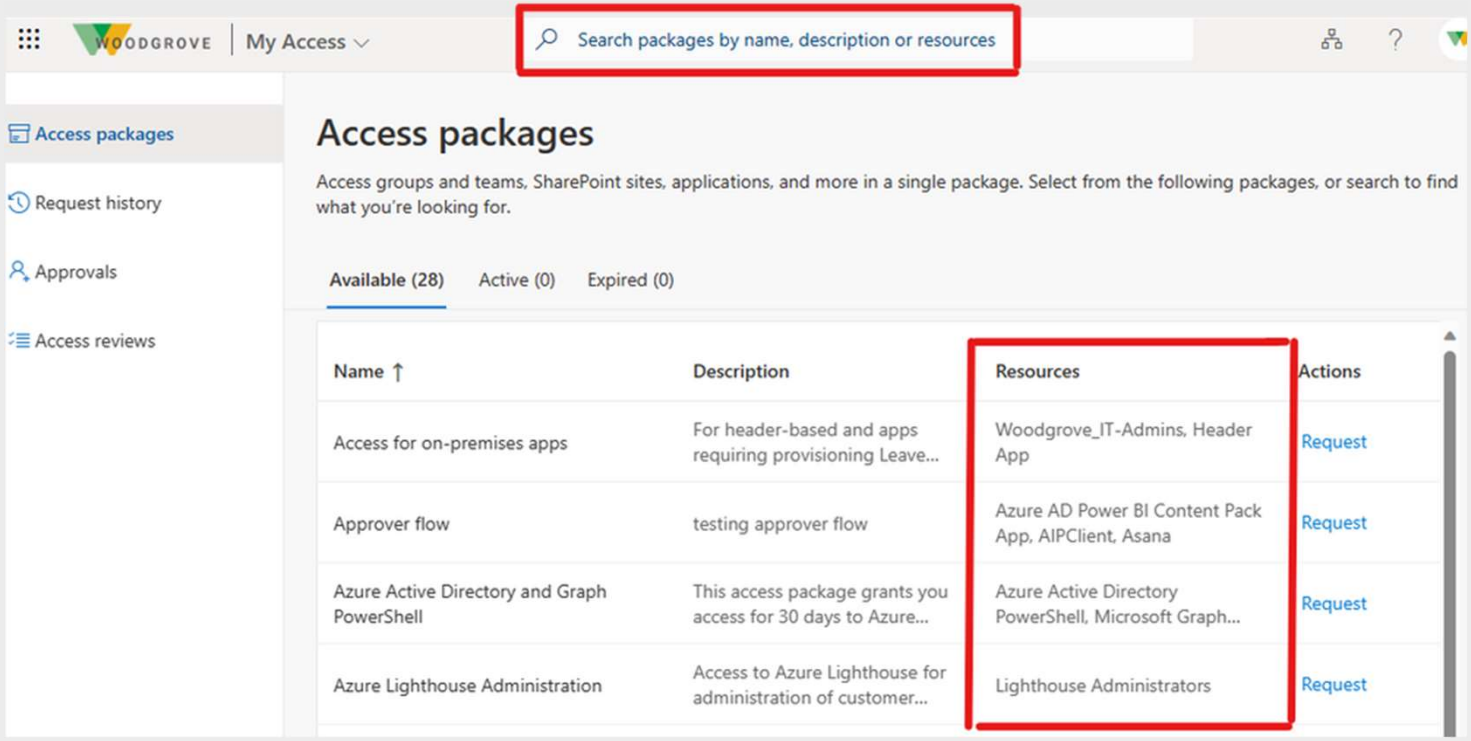
425Show

New search experience in My Access

Stage : GA

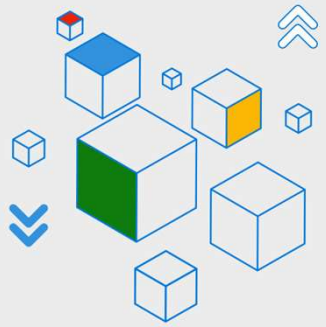
Product family : Microsoft Entra ID Governance

Overview : Enables search of access packages based on keywords in access package names, descriptions, or resource names.



425Show

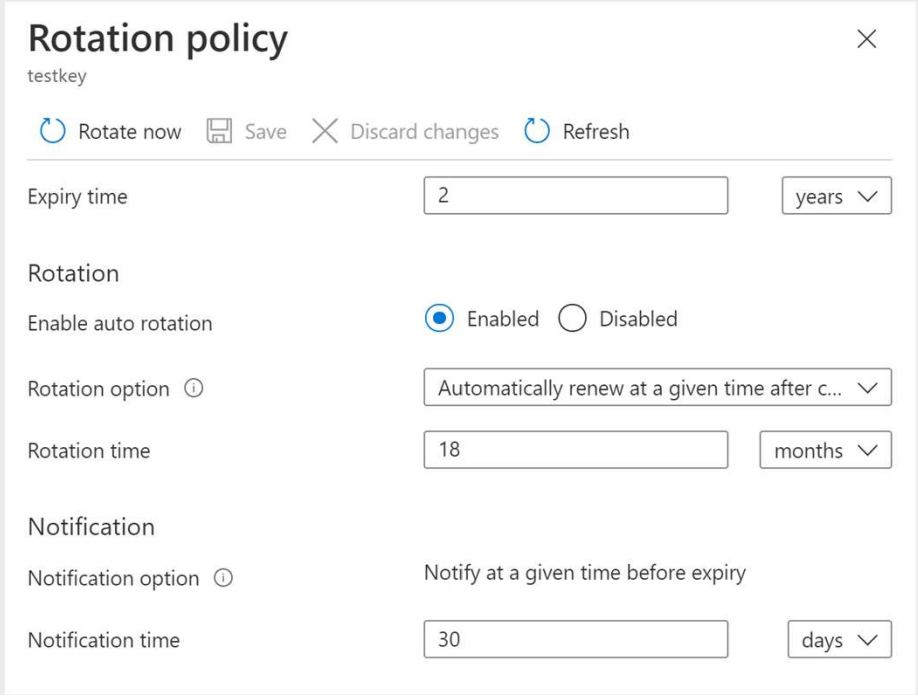
Azure Key Vault: configure key rotation policy governance



Stage : GA

License : There's an additional cost per scheduled key rotation.

Overview : Using the Azure Policy service you can govern the key lifecycle and ensure that all cryptographic software and Hardware Security Module (HSM) keys within your Azure Key Vault are configured to undergo regular rotation, adhering to your organization's specific security standards.



425Show

Microsoft Entra Internet Access

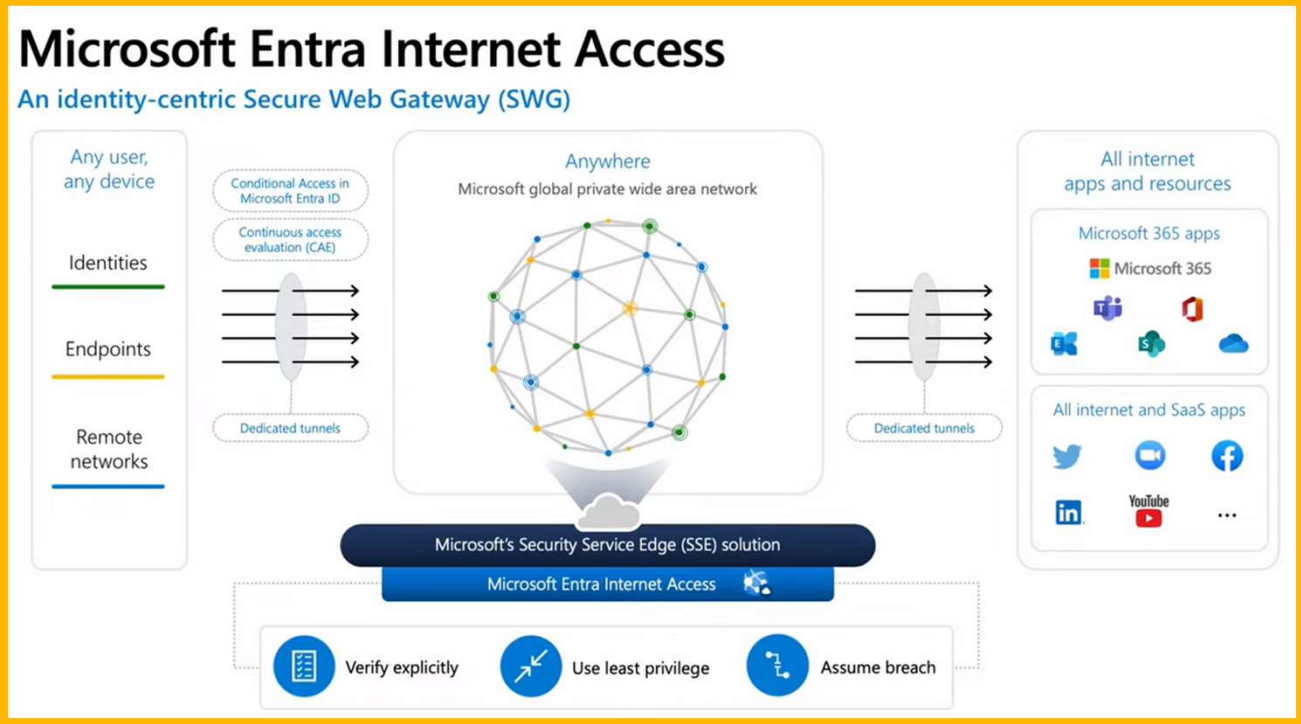
Stage : Public Preview

Product family : Microsoft Entra Internet Access

License :

Overview : This identity-centric Secure Web Gateway (SWG) protects access to Microsoft 365 apps and enables best-in-class security and visibility, along with faster and more seamless access to Microsoft 365 apps. You can also leverage the extended Conditional Access capabilities and protect your organization against data exfiltration and token theft. Also, you gain detailed insights into your network traffic, including the original user source IP.

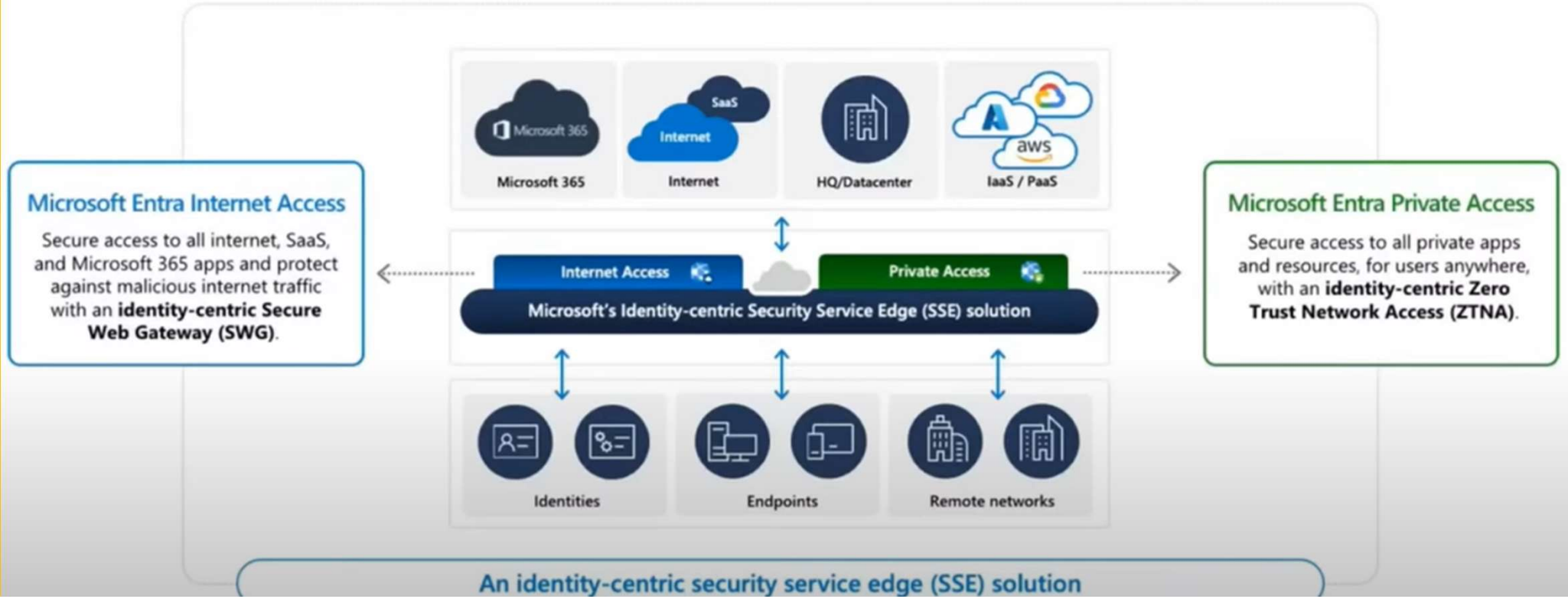
Stakeholders to engage: Networks, SecOps, helpdesk & end user compute



425Show

Microsoft Entra Private Access

Microsoft's Identity-centric SSE solution



425Show

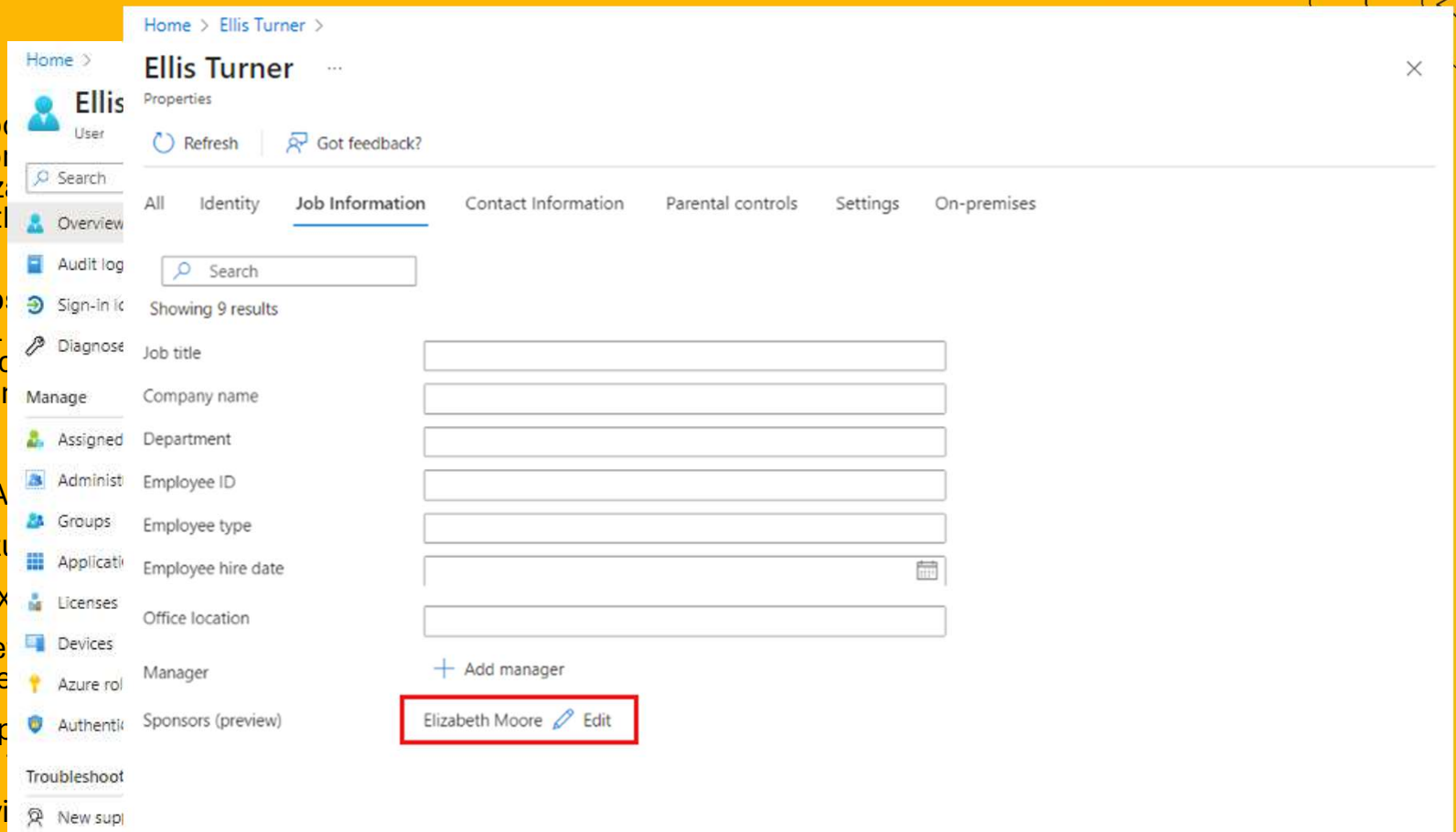
Sponsors field for B2B users

Stage : Preview

Overview : The Spo
refers to the perso
user to the organiz
track who invited t
accountability.

Deployment Step
to have the Global
administrator direc
User Administrator

1. Sign in to the A
2. Navigate to Azu
3. Select Invite ex
4. Entered the de
   Next: Propertie
5. You can add sp
   the Properties
6. Select the Revi
   process.



425Show

Mobile Application Management (MAM) for Windows using Microsoft Edge

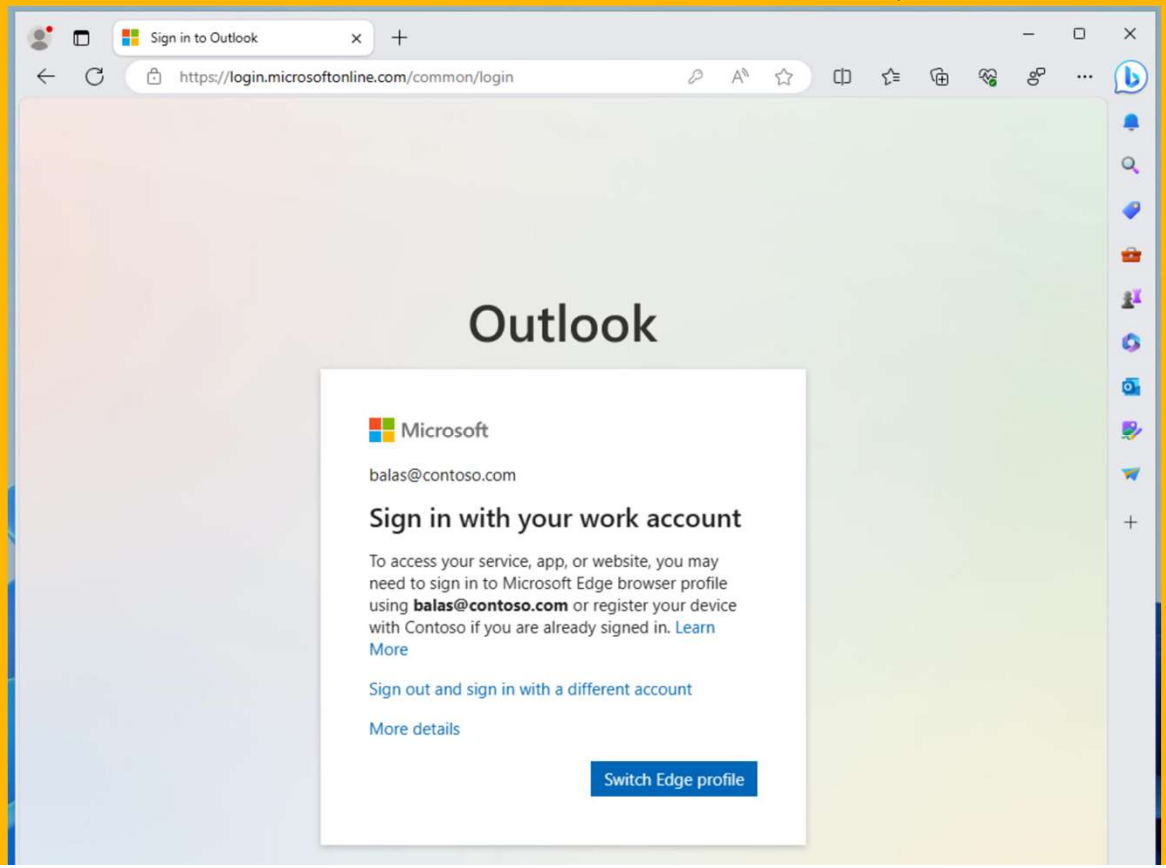
Stage : Preview

Product family : Microsoft Entra ID

Overview : Windows MAM extends MAM application configuration and protection capabilities to Edge on Windows including admin experience, policy lifecycle management, client for applications, and Windows Defender health checks. MAM is enforced via CA before allowing resource access on Windows which ensures only MAM protected Edge can access CA-protected resources.

Deployment Steps:

Customers interested in the public preview will need to opt-in using the MAM for Windows Public Preview Sign Up Form.



425Show

Strictly enforce location policies using continuous access evaluation (CAE)

Stage : Preview

Product family : Microsoft Entra ID

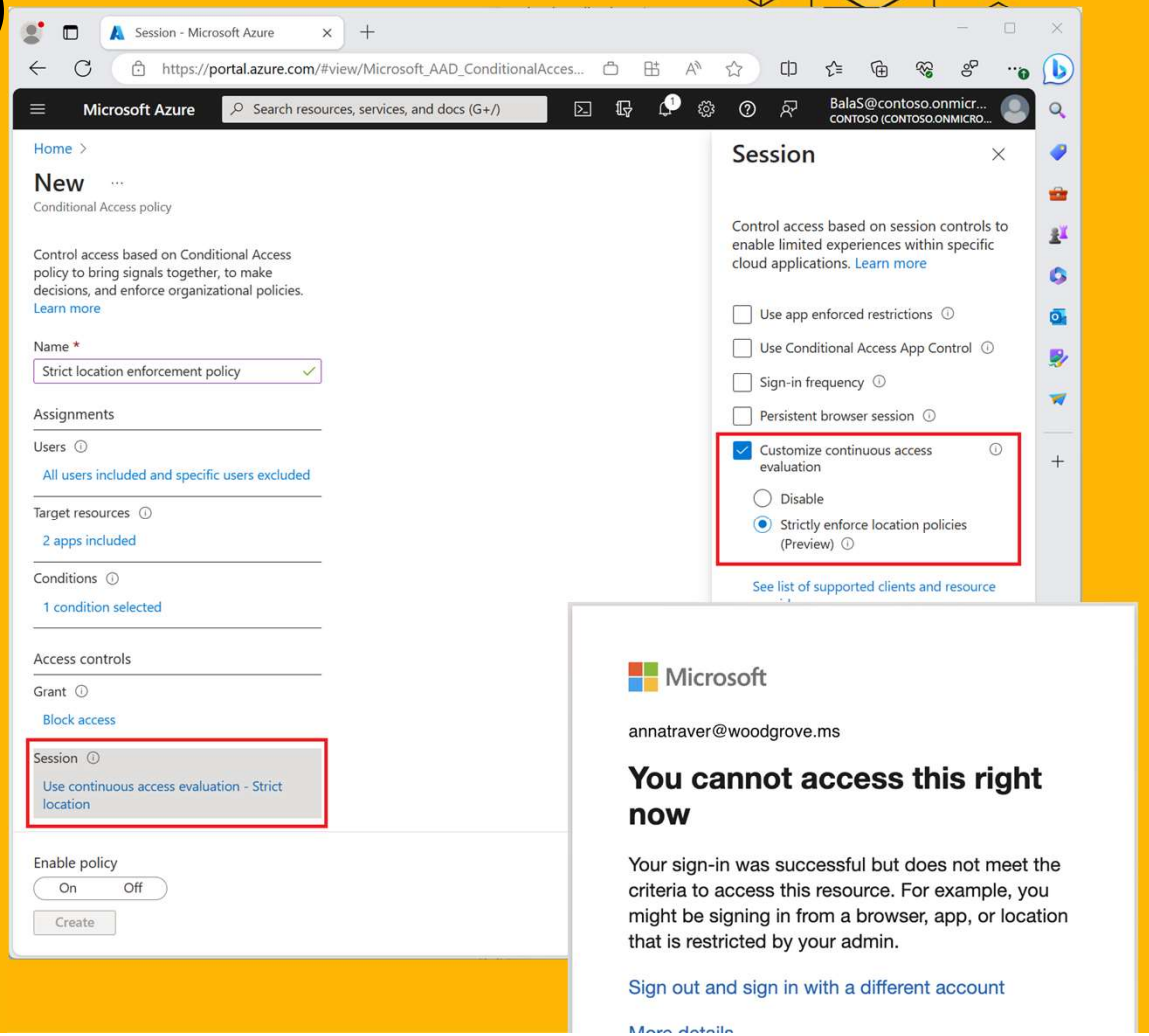
Overview : Allows tenant admins to investigate IP addresses, seen by resource providers, to utilize CAE to promptly invalidate tokens that violate location policies.

Step 1 - Configure a Conditional Access location base policy for your target users

Step 2 - Test policy on a small subset of users

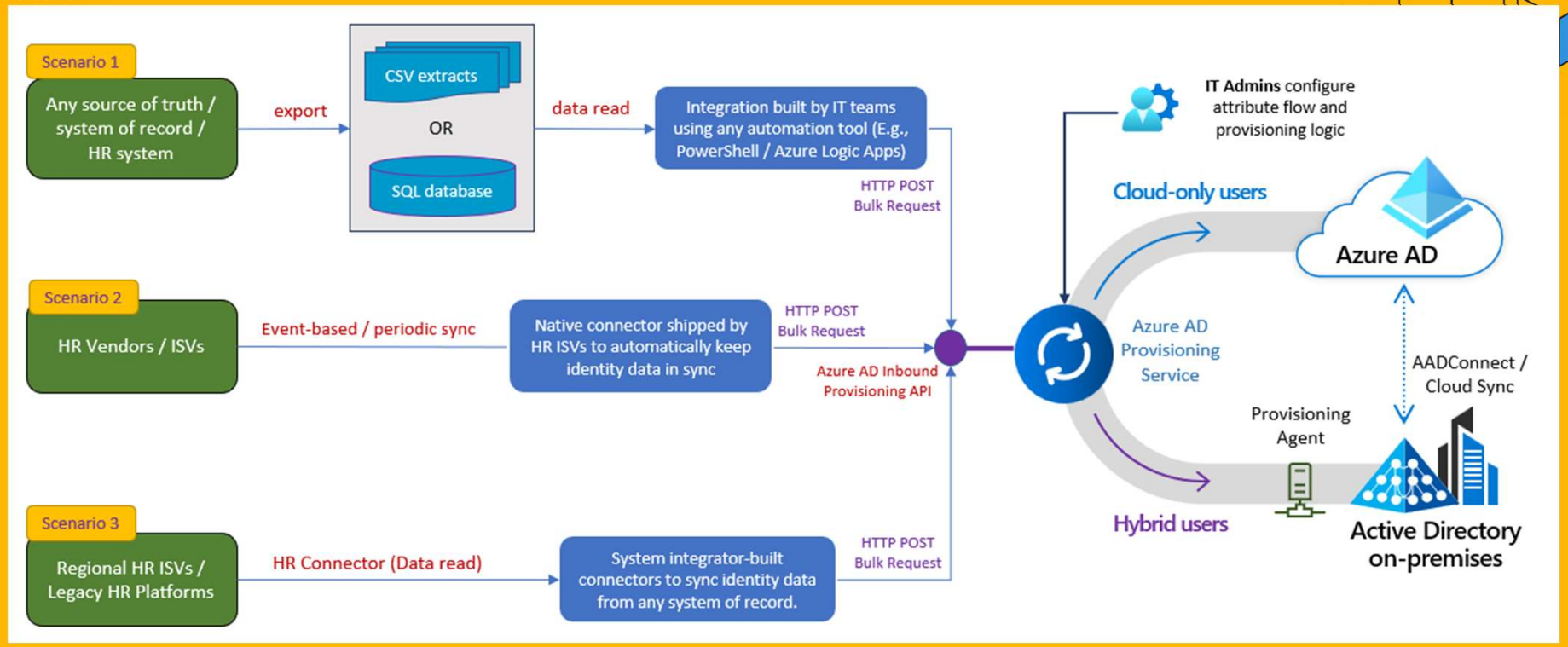
Step 3 - Use the CAE Workbook to Identify IP addresses that should be added to your named locations

Step 4 - Continue deployment - Repeat steps 2 and 3 with expanding groups of users until Strictly Enforce Location Policies are applied across your target user base. Roll out carefully to avoid impacting user experience.



425Show

API-driven inbound provisioning



Stage : Preview **Product family :** Microsoft Entra ID

Overview : Enables you to use any automation tool of your choice to retrieve workforce data from any system of record for provisioning into Microsoft Entra ID and connected on-premises Active Directory domains. IT admins have full control on how the data is processed and transformed with attribute mappings. Once the workforce data is available in Microsoft Entra ID, IT admins can configure appropriate joiner-mover-leaver business processes using Microsoft Entra ID Governance Lifecycle Workflows.

425Show

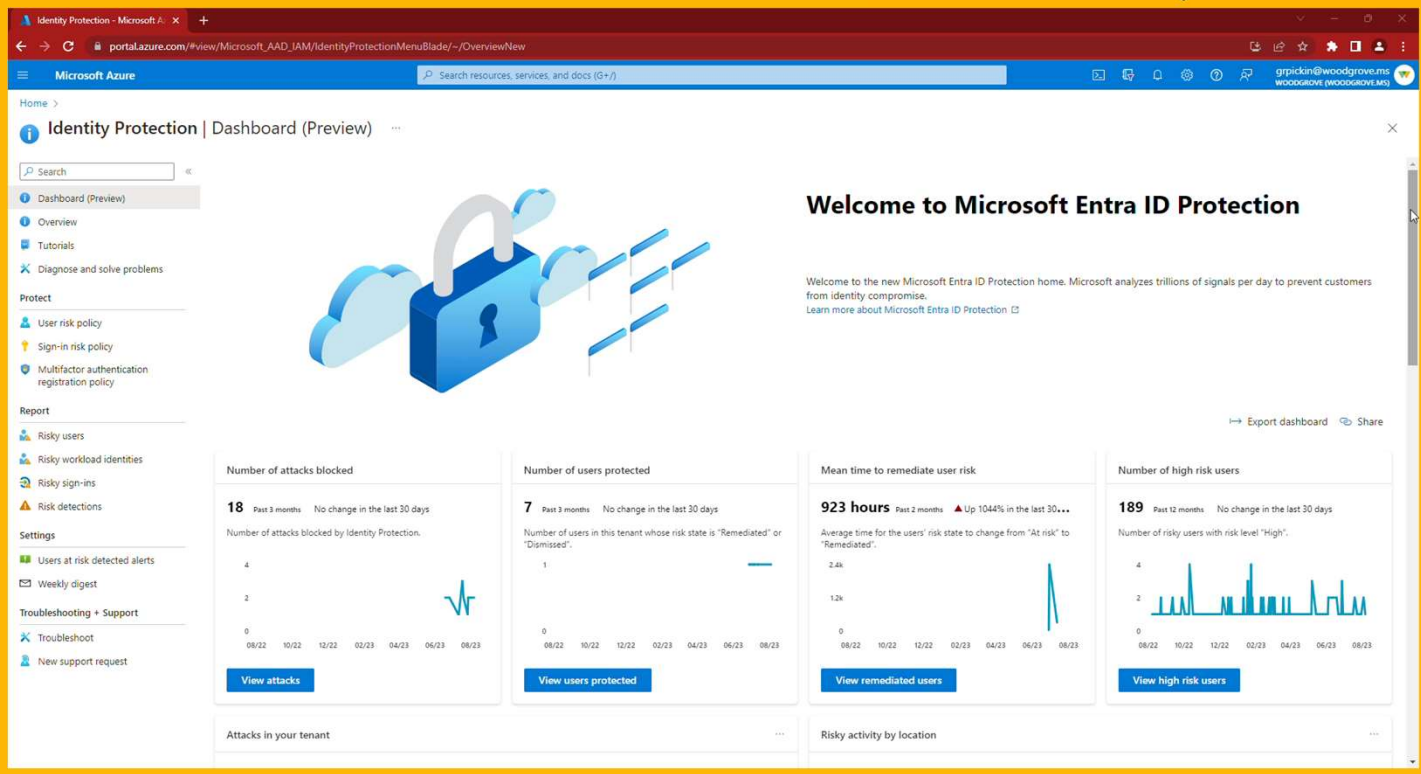
Microsoft Entra ID Protection: new landing page

Stage : Preview

Product family : Microsoft Entra ID Governance

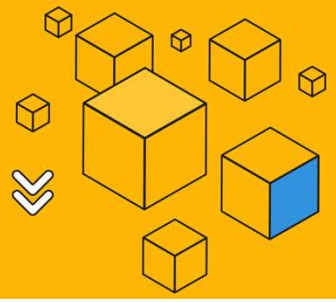
License : Microsoft Entra ID Governance

Overview : The brand-new Microsoft Entra ID Protection dashboard is designed as a central hub to empower IT admins and SOC teams with rich insights and actionable recommendations tailored to your tenant. By providing a deeper view into the security posture of your organization, the dashboard enables you to implement effective protections accordingly.



425Show

Microsoft Entra ID Governance: Sponsors as approvers in entitlement management

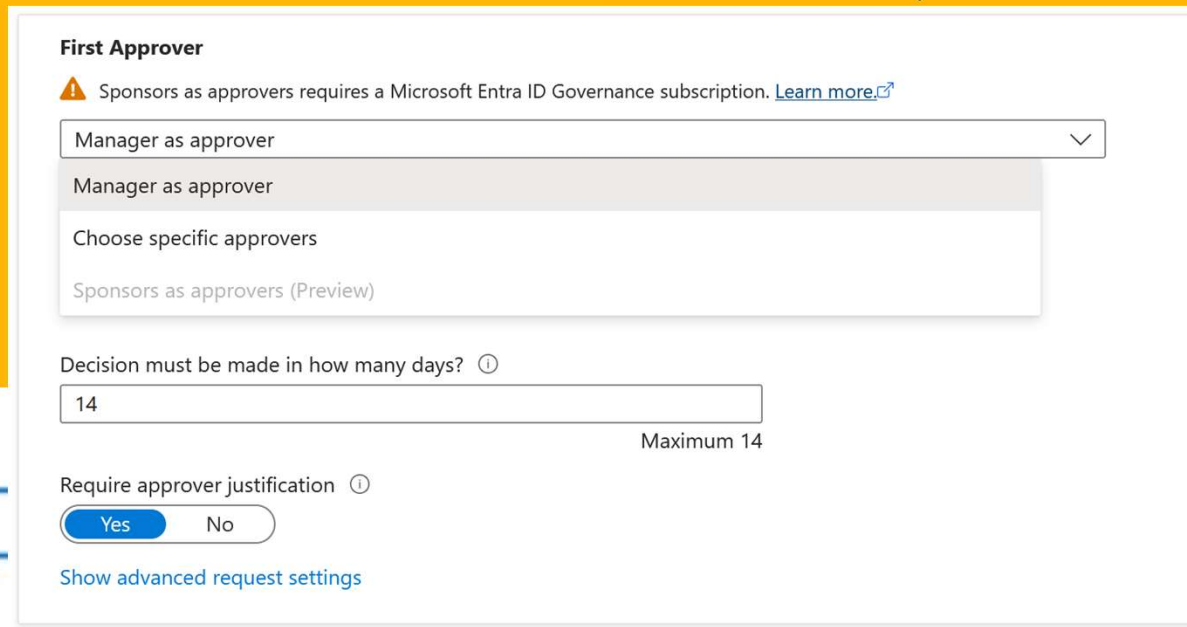


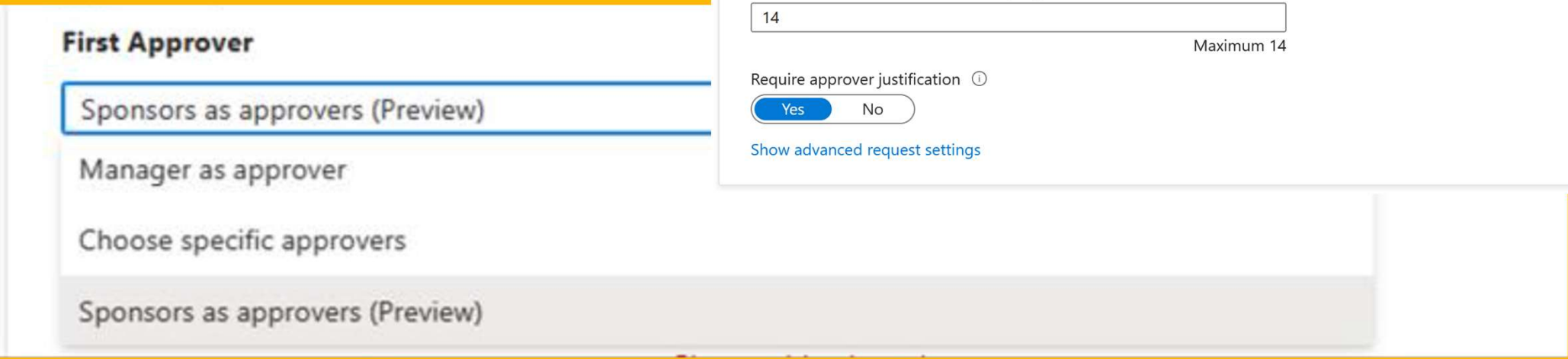
Stage : Preview

Product family : Microsoft Entra ID Governance

License : Microsoft Entra ID Governance

Overview : Sponsors for guest users can be approvers for access packages which were requested by a guest user.





425Show

Microsoft Entra ID Governance: manage guest user lifecycle

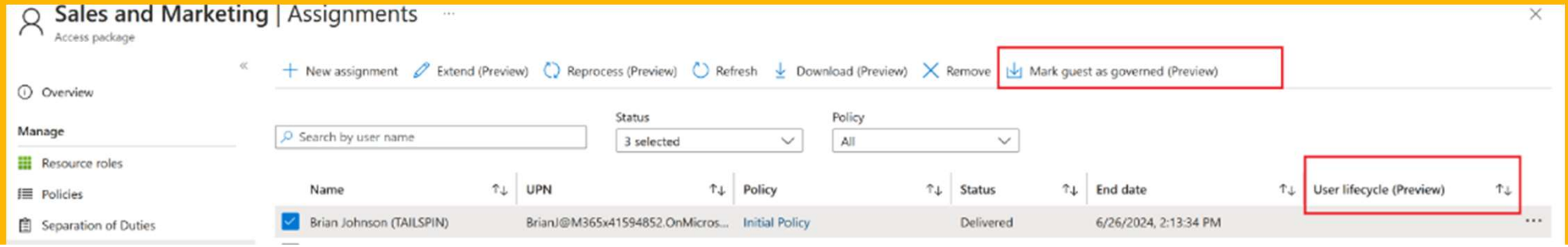
Stage : Preview

Product family : Microsoft Entra ID Governance

Overview : Entitlement management (ELM) allows you to govern the state of a guest user's lifecycle. When a guest user is set as Governed, based on ELM tenant settings, their account will be deleted or disabled in specified days after their last access package assignment expires.

Deployment Steps:

1. In the Azure portal, select Azure Active Directory and then select Identity Governance.
2. In the left menu, select Access packages and then open the access package.
3. In the left menu, select Assignments.
4. On the assignments screen, select the user you want to manage the lifecycle for, and then select Mark guest as governed (Preview).
5. Select save.



425Show

Microsoft Entra ID Governance: inactive guest insights

Stage : Preview **Product family :** Microsoft Entra ID Governance **License :** Microsoft Entra ID Governance

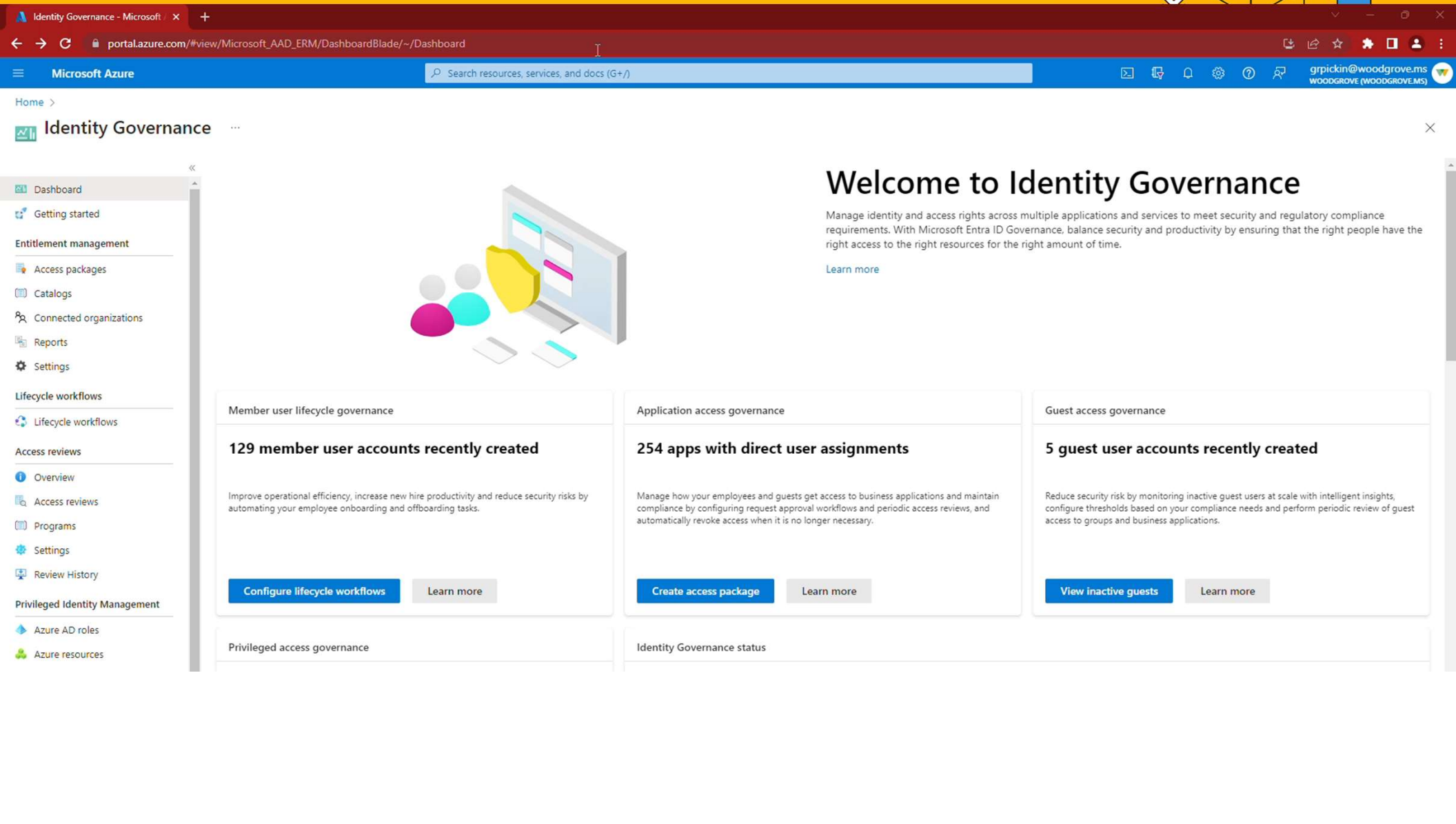
Overview : Allows you to monitor guest accounts at scale with intelligent insights into inactive guest users in your organization. You can customize the inactivity threshold depending on your organization's needs, narrow down the scope of guest users you want to monitor and identify the guest users that may be inactive.

Deployment Steps:

1. Sign in to the Azure portal and open the Identity Governance page.
2. Access the inactive guest account report by navigating to "Guest access governance" card and click on "View inactive guests"
3. You will see the inactive guest report which will provide insights about inactive guest users based on 90 days of inactivity. The threshold is set to 90 days by default but can be configured using "Edit inactivity threshold" based on your organization's needs.
4. The following insights are provided as part of this report:
   - Guest account overview (total guests and inactive guests with further categorization of guests who have never signed in or signed in at least once)
   - Guest inactivity distribution (Percentage distribution of guest users based on days since last sign in)
   - Guest inactivity overview (Guest inactivity guidance to configure inactivity threshold)
   - Guest accounts summary (A tabular view with details of all guest accounts with insights into their activity state. The Activity state could be active or inactive based on the configured inactivity threshold)
5. The inactive days are calculated based on last sign in date if the user has signed in atleast once. For users who have never signed in, the inactive days are calculated based on creation date.

425Show

Microsoft Entra ID Governance: inactive guest insights



Thank you for tuning in!

Don’t forget to tune in again for the September updates on

6th September 2023

Grace Picking

Jorge Lopez

425Show