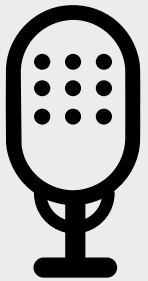
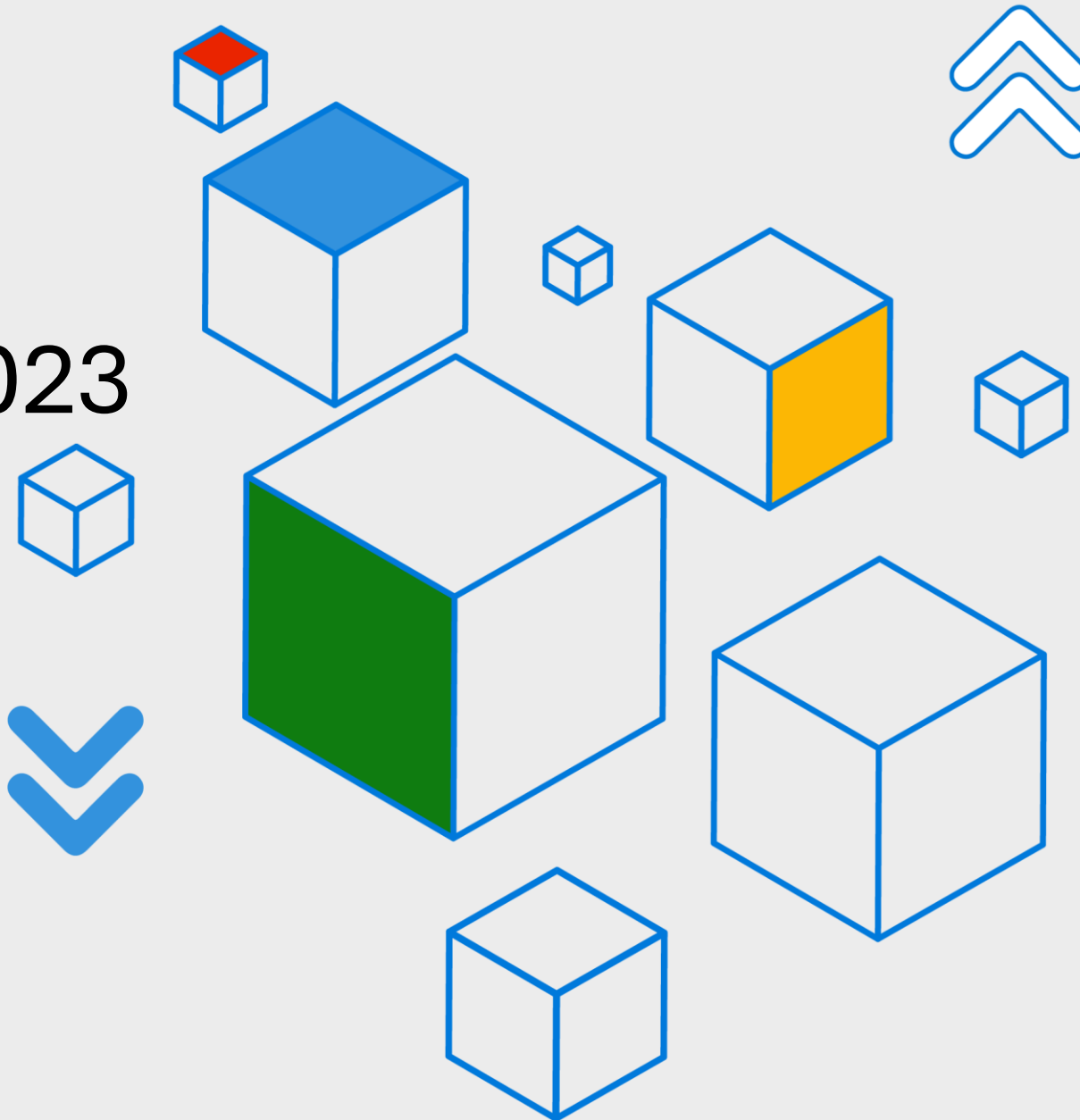


# What's New in Microsoft Entra ID November 2023



425Show



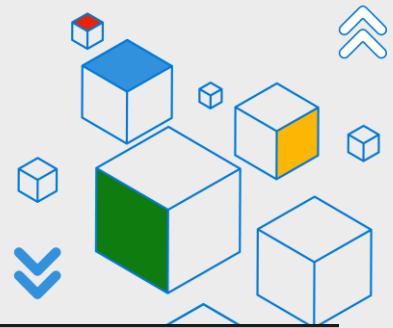
Grace Picking



Jorge Lopez

<https://ignite.microsoft.com/>

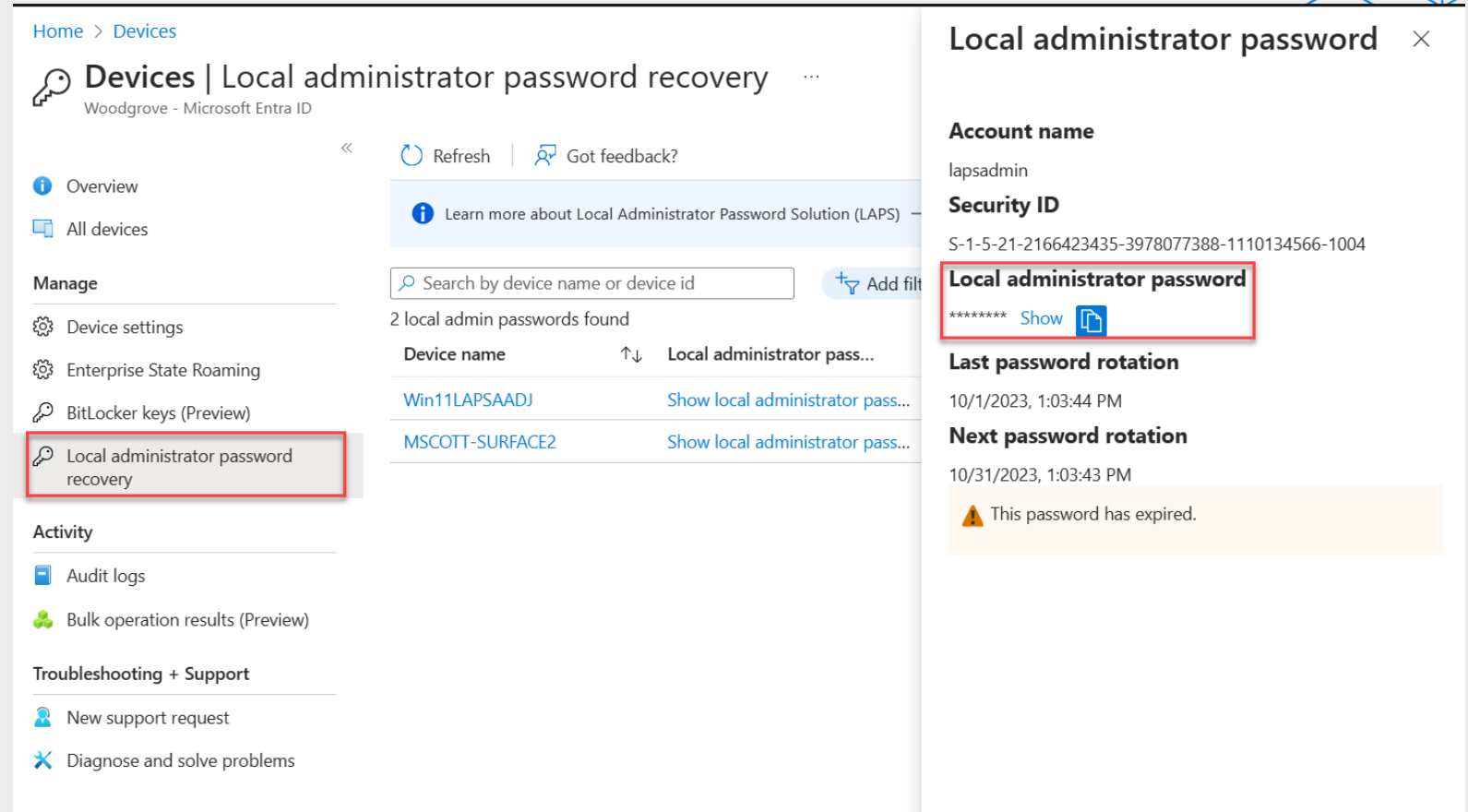
# Windows Local Administrator Password Solution (LAPS) with Microsoft Entra ID and Microsoft Intune



**Stage : GA**

**Product family :**  
Microsoft Entra ID

**Overview :** With Windows LAPS you can automatically manage and back up the password of a local administrator account on your Microsoft Entra ID joined or Hybrid Microsoft Entra ID joined devices.



Home > Devices

**Devices** | Local administrator password recovery ...  
Woodgrove - Microsoft Entra ID

<< Refresh | Got feedback?

Learn more about Local Administrator Password Solution (LAPS)

Search by device name or device id Add filter

2 local admin passwords found

Device name	Local administrator password
Win11LAPSAADJ	Show local administrator password
MSCOTT-SURFACE2	Show local administrator password

**Local administrator password**

**Account name**  
lapsadmin

**Security ID**  
S-1-5-21-2166423435-3978077388-1110134566-1004

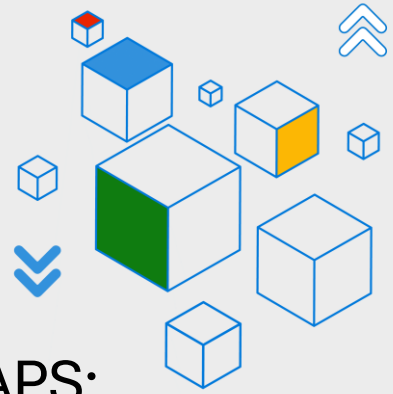
**Local administrator password**  
\*\*\*\*\* Show

**Last password rotation**  
10/1/2023, 1:03:44 PM

**Next password rotation**  
10/31/2023, 1:03:43 PM

⚠ This password has expired.

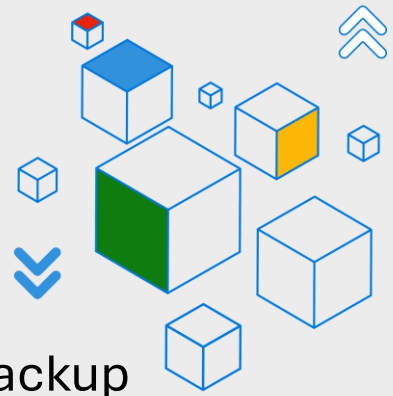
# Windows LAPS - What, Why and How



- Recommended security measure:
  - Defends against Pass the Hash (PtH) and lateral traversal attacks.
  - Manages and securely stores randomized passwords for a local admin account.
- Critical blocker for Microsoft Entra joined devices:
  - Out of box LAPS installer available on download center does not support Microsoft Entra joined devices.
- Windows LAPS:
  - Built into Windows 10, 11 and Windows Server 2019 and 2022 – April 2023 security path.
- Microsoft Entra ID:
  - Entra joined and hybrid joined devices.
- Device Management
  - MDM support with Microsoft Intune and 3P MDM.
  - GPO support for hybrid joined devices.
  - Single local admin account can be managed.

<https://aka.ms/425show/LAPS>

# Windows LAPS – Cloud scenarios



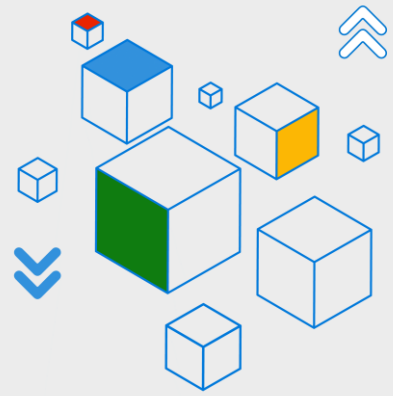
- **Turn on Windows LAPS** using a tenant-wide policy and a client-side policy to backup local administrator password to Microsoft Entra ID.
- **Configure client-side policies** via Microsoft Intune portal for local administrator password management to set account name, password age, length, complexity, manual password reset and so on.
- **Recover stored passwords** via Microsoft Entra/Microsoft Intune portal or Microsoft Graph API/PSH.
- **Enumerate all LAPS-enabled devices** via Microsoft Entra portal or Microsoft Graph API/PSH.
- **Create Microsoft Entra ID role-based access control (RBAC) policies** with custom roles and administrative units for authorization of password recovery.
- **View audit logs** via Microsoft Entra portal or Microsoft Graph API/PSH to monitor password update and retrieval events.
- **Configure Conditional Access policies** on directory roles that have the authorization of password recovery.

<https://aka.ms/425Show/LAPSGetStarted>



425Show

# Windows LAPS - Settings



## Policies

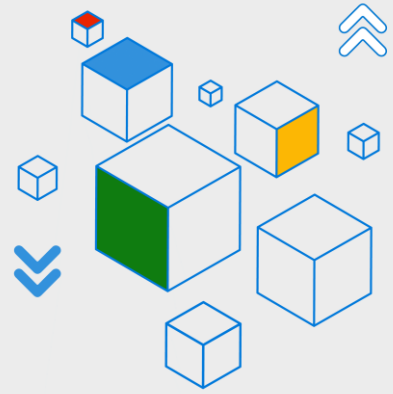
- BackupDirectory
  - Default = Disabled. Entra ID = 1, AD (on-prem domain joined) = 2.
- AdministratorAccountName
  - Default = Administrator (by SID), or other local account name specified.
- PasswordAgeDays (1-365)
  - Default = 30 days. Minimum 7 days for Entra ID.
- PostAuthenticationActions (PAA)
  - Default = 3. 1=Reset pwd. 3=Reset pwd & logoff. 5=Reset pwd & reboot.
- PostAuthenticationResetDelay (0-24 hrs)
  - Default = 24 hrs. 0 disables any PAA.
- PasswordLength (8-64 characters)
  - Default = 14.
- PasswordComplexity
  - Default = 4. 1=Large letters. 2=Large+small letters. 3=2+numbers. 4=3+special characters.

## Actions

- ResetPassword
  - Manual reset of local admin password for a single device.
- ResetPasswordStatus
  - Execution status of last reset password action.

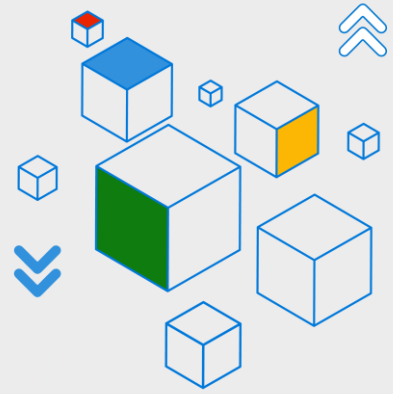
<https://aka.ms/425show/LAPSIntunePolicies>

# Windows LAPS - Licensing



- Windows license (Pro, OEM, etc - Enterprise Or E3 not required).
- Microsoft Intune license (if managing device using Intune).
- Microsoft Entra ID license:
  - Free for baseline features (enabling LAPS, storing encrypted password, password retrieval, audit logs).
  - Premium when you use capabilities like Conditional Access (require MFA when recovering password), Custom Roles (for anyone outside of built in roles to recover password) and Administrative Units (who is allowed to retrieve password on which set of devices).

# Windows LAPS - Roadmap

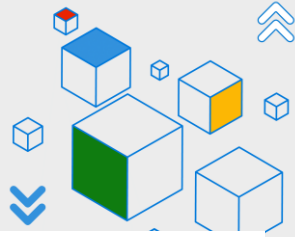


- Account creation/management.
- Enabling LAPS managed account during Windows safe boot.
- Auditing local admin account authentication in Microsoft Entra ID.
- JIT based self-service password recovery.
- Enhanced reporting.



425Show

# Conditional Access templates



**Stage : GA**

**Product family :**  
Microsoft Entra ID

**Overview:** Pre-defined set of conditions and controls that provide a convenient method to deploy new policies aligned with Microsoft recommendations.

Create new policy from templates ...

Select a template    Review + Create

Search

**Secure foundation**    Zero Trust    Remote work    Protect administrator    Emerging threats    All

- ☒ **Require multifactor authentication for admins**  
Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.  
[Learn more](#)
- ☐ **Securing security info registration**  
Secure when and how users register for Azure AD multifactor authentication and self-service password reset.  
[Learn more](#)
- ☐ **Block legacy authentication**  
Block legacy authentication endpoints that can be used to bypass multifactor authentication.  
[Learn more](#)
- ☐ **Require multifactor authentication for all users**  
Require multifactor authentication for all user accounts to reduce risk of compromise.  
[Learn more](#)
- ☐ **Require multifactor authentication for Azure management**  
Require multifactor authentication to protect privileged access to Azure management.  
[Learn more](#)
- ☐ **Require compliant or hybrid Azure AD joined device or multifactor authentication for all users**  
Protect access to company resources by requiring users to use a managed device or perform multifactor authentication.  
[Learn more](#)

View    Download JSON file

<https://aka.ms/ConditionalAccessTemplateDocs>

<https://aka.ms/425show/CAtemplates>

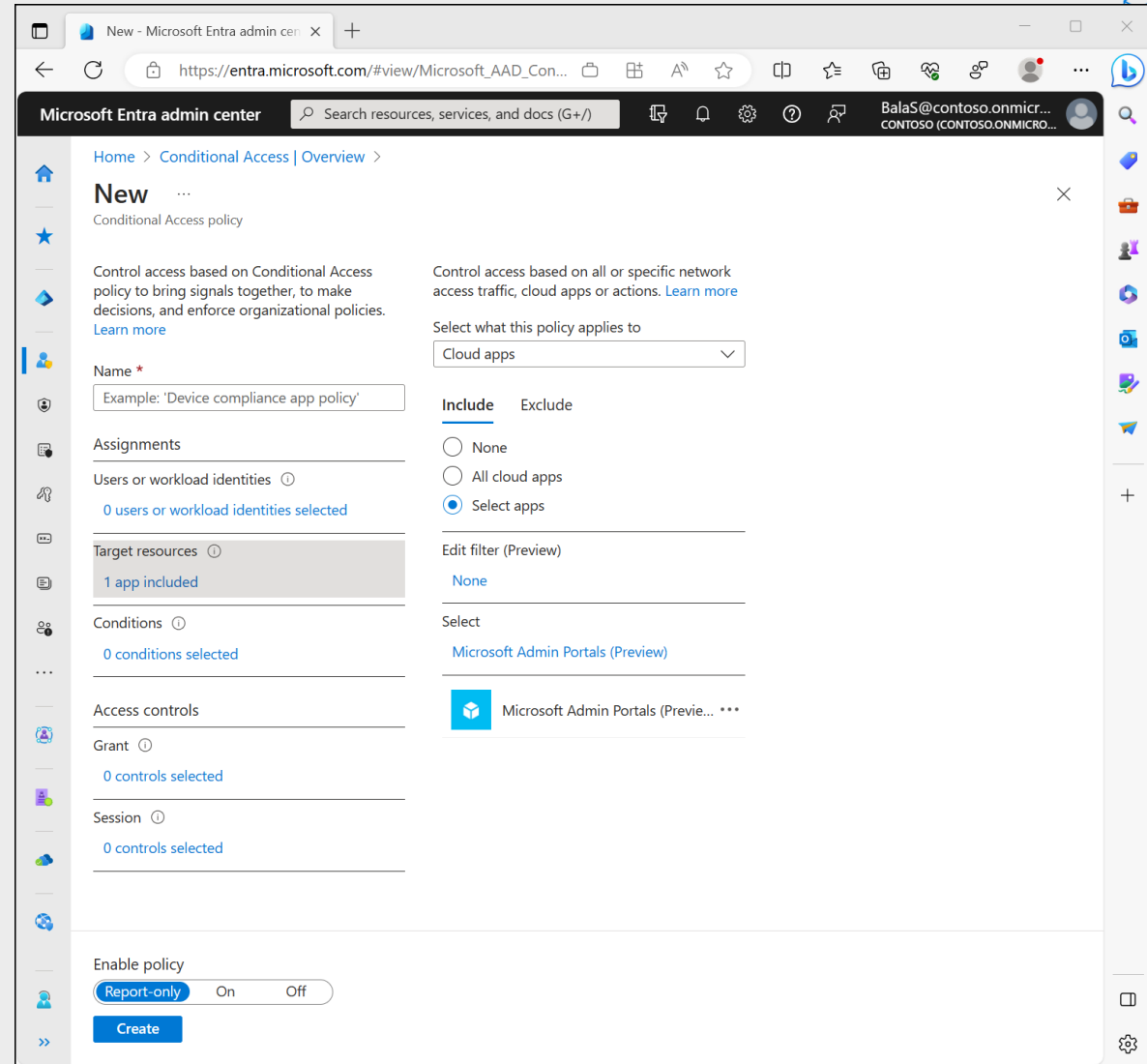


# Support for Microsoft admin portals in Conditional Access

Stage : GA

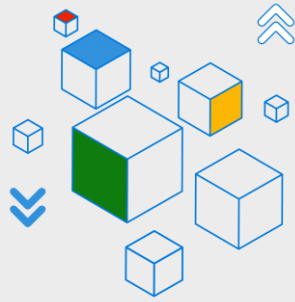
Product family : Microsoft Entra ID

**Overview:** When a CA policy targets the Microsoft admin portals cloud app, the policy is enforced for the Azure portal, the Exchange admin center, Microsoft 365 admin center, Microsoft 365 Defender portal, Microsoft Entra admin center, Microsoft Intune admin center, and the Microsoft Purview compliance portal



<https://aka.ms/425show/CAadminportals>

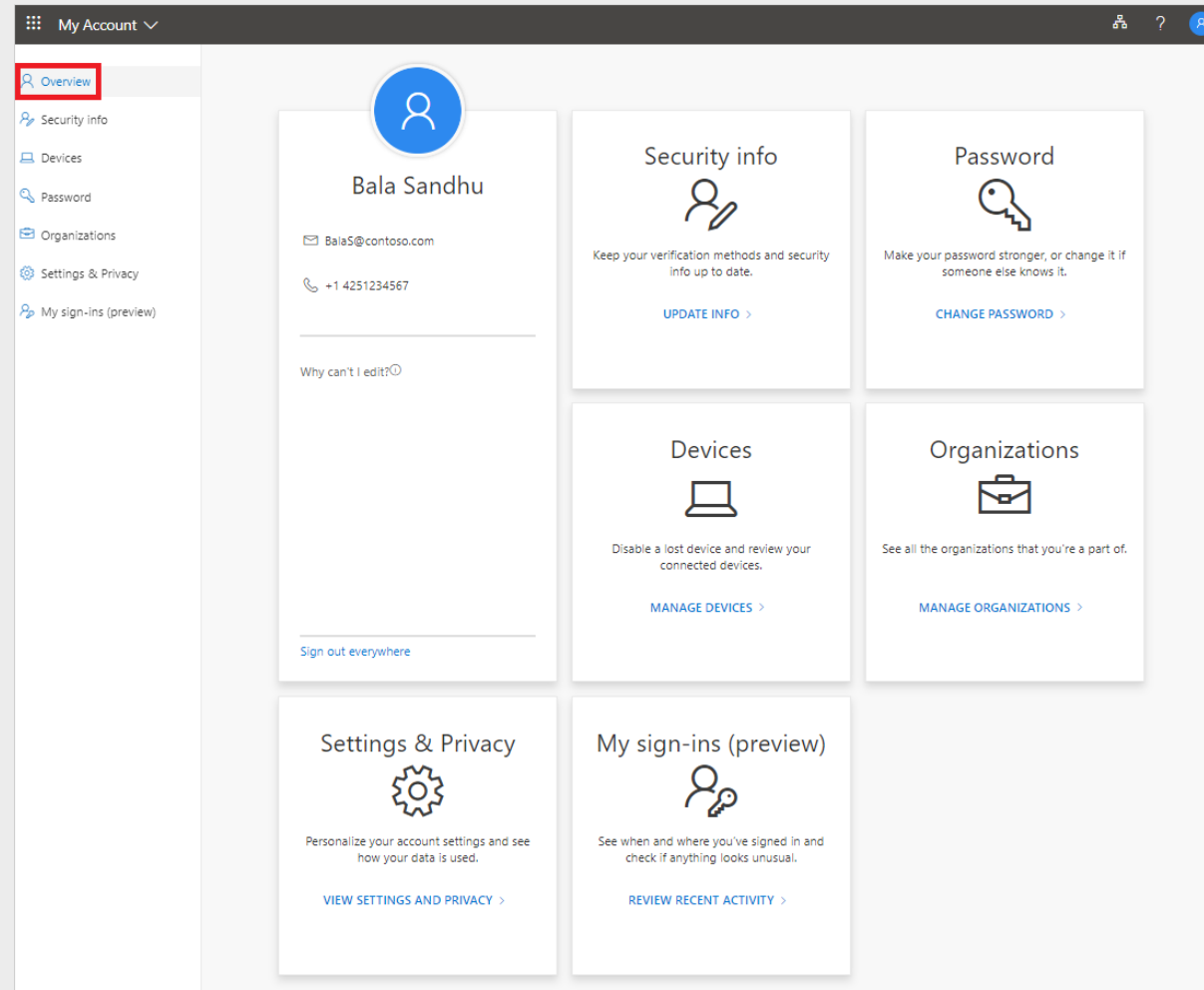
# My Account is targetable by Conditional Access



**Stage : GA**

**Product family :**  
Microsoft Entra ID

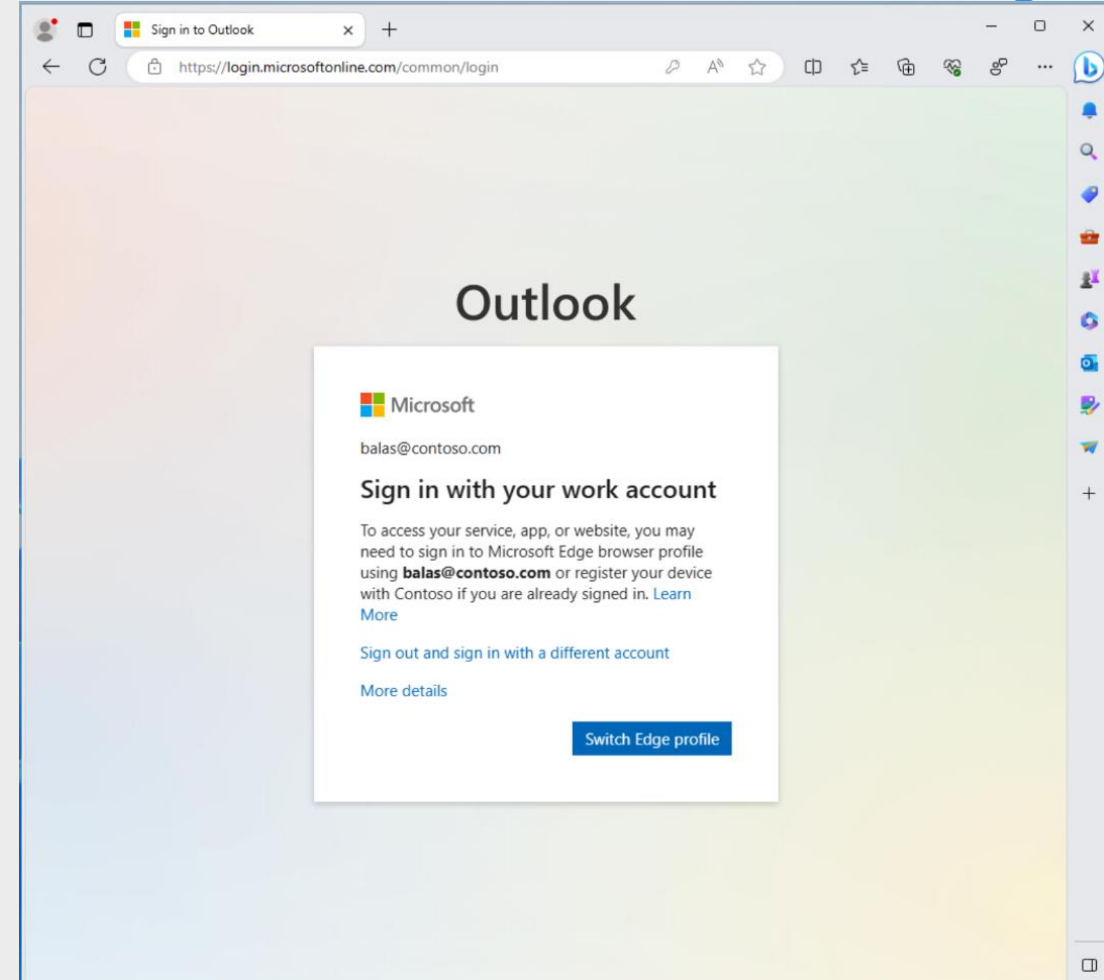
**Overview:**  
Enables admins  
to target My  
Account in CA  
policies.



# Mobile Application Management (MAM) for Windows using Microsoft Edge

**Stage : GA**

**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 protected resources.

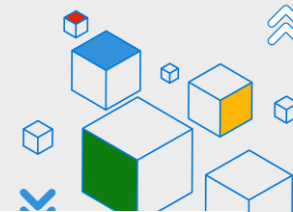


<https://aka.ms/425show/MAMPolicies>



425Show

# Delegated user management using custom roles



Stage : GA

Product family : Microsoft Entra ID

**Overview:** To grant fine-grained access admins can use user management permissions in custom role definitions in Microsoft Entra ID.

Home > Roles and administrators | All roles >

## New custom role

All roles

Got feedback?

Basics Permissions Review + create

Add permissions for this custom role. Currently, permissions for Application registrations and Enterprise applications are supported in custom roles. [Learn more](#)

Search by permission name or description

<input type="checkbox"/> Permission	↑↓ Description	↑↓ Privileged
<input type="checkbox"/> microsoft.directory/applicationPolicies/allProperties/read	Read all properties (including privileged properties) on application policies	
<input type="checkbox"/> microsoft.directory/applicationPolicies/allProperties/update	Update all properties (including privileged properties) on application policies	
<input type="checkbox"/> microsoft.directory/applicationPolicies/basic/update	Update standard properties of application policies	
<input type="checkbox"/> microsoft.directory/applicationPolicies/create	Create application policies	
<input type="checkbox"/> microsoft.directory/applicationPolicies/createAsOwner	Create application policies, and creator is added as the first owner	
<input type="checkbox"/> microsoft.directory/applicationPolicies/delete	Delete application policies	
<input type="checkbox"/> microsoft.directory/applicationPolicies/owners/read	Read owners on application policies	
<input type="checkbox"/> microsoft.directory/applicationPolicies/owners/update	Update the owner property of application policies	
<input type="checkbox"/> microsoft.directory/applicationPolicies/policyAppliedTo/read	Read application policies applied to objects list	
<input type="checkbox"/> microsoft.directory/applicationPolicies/standard/read	Read standard properties of application policies	
<input type="checkbox"/> microsoft.directory/applications.myOrganization/allProperties/read	Read all properties (including privileged properties) on single-directory applications	
<input type="checkbox"/> microsoft.directory/applications.myOrganization/allProperties/update	Update all properties (including privileged properties) on single-directory applications	PRIVILEGED
<input type="checkbox"/> microsoft.directory/applications.myOrganization/audience/update	Update audience on single-directory applications	
<input type="checkbox"/> microsoft.directory/applications.myOrganization/authentication/update	Update authentication on single-directory applications	
<input type="checkbox"/> microsoft.directory/applications.myOrganization/basic/update	Update basic properties on single-directory applications	
<input type="checkbox"/> microsoft.directory/applications.myOrganization/credentials/update	Update credentials on single-directory applications	PRIVILEGED

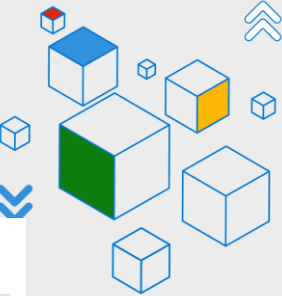
<https://aka.ms/425show/UserCustomRoles>

# Send the group name in the SAML token for SaaS applications

**Stage : GA**

**Product family : Microsoft Entra ID**

**Overview:** Enables admins to send the group name of a user in the SAML token of an application. This feature also adds support to send the group display name for cloud-only groups assigned to an application in addition to the existing capability to use the group object ID in the claim.



**User Attributes & Claims**

+ Add new claim + Add a group claim Columns

**Required claim**

Claim name	Value	
Unique User Identifier (Name ID)	user.mail	...

**Additional claims**

Claim name	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	...

**Group Claims**

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None

☐ All groups

☒ Security groups

☐ Directory roles

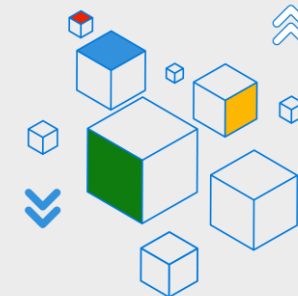
☐ Groups assigned to the application

<https://aka.ms/425show/EntraIDGroupClaims>



425Show

# Claims customization UX for OIDC Enterprise apps



Stage : GA

Product family : Microsoft Entra ID

**Overview:** Brings all existing investments we made for SAML claims to OIDC apps in the Microsoft Entra portal, including group filtering, group RegEx, and claims transformations. With this capability admins can now configure claims for OIDC apps on the Microsoft Entra portal in the same way that they are configured for SAML apps.

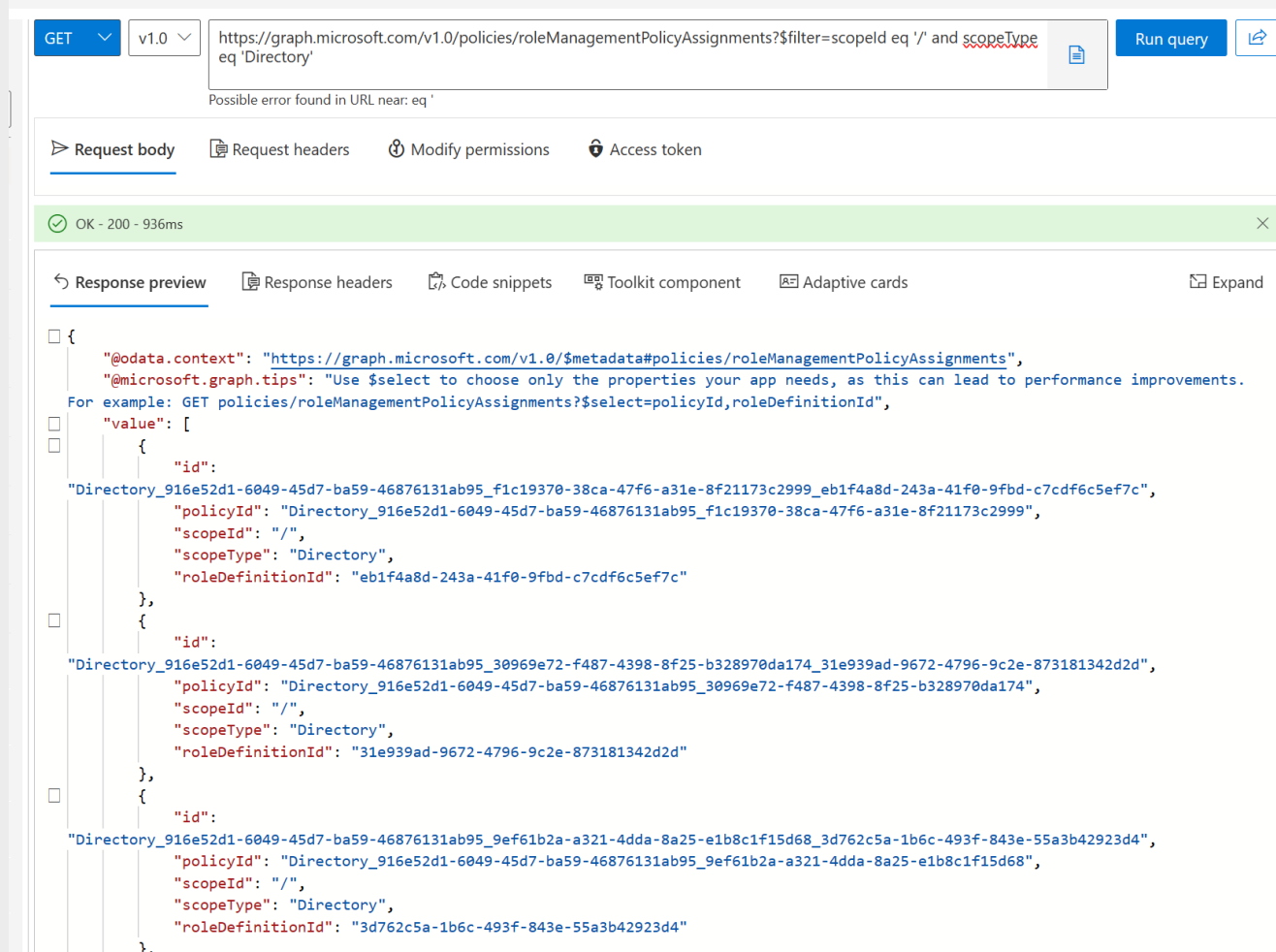
<https://aka.ms/425show/OIDCApplsClaimsUX>

# Microsoft Entra Privileged Identity Management (PIM) for Groups API

Stage : GA

Product family : Microsoft Entra ID

**Overview:** Allows admins to manage all aspects of PIM for Groups through the API: manage membership/ownership assignments, request activation, approve membership/ownership activation requests, and manage PIM policies (also known as role settings).

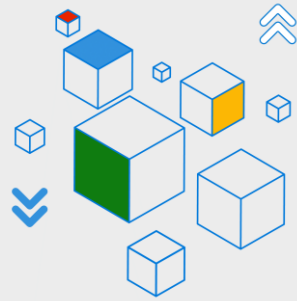


<https://aka.ms/425show/PIMforGroupsAPI>





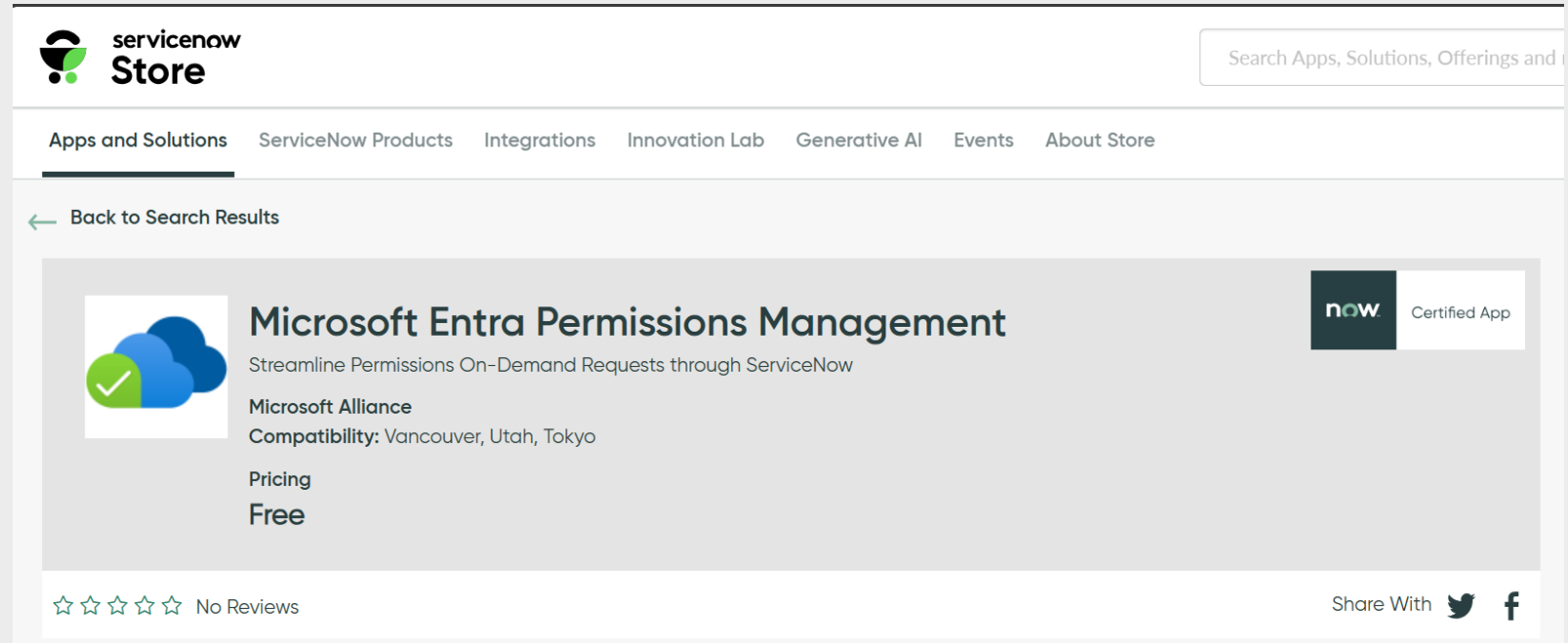
# ServiceNow app for Microsoft Entra Permissions Management available in ServiceNow store



**Stage : GA**

**Product family :** Microsoft  
Entra Permissions  
Management

**Overview:** Enables admins to request time-bound, on-demand permissions for multi-cloud environments (Azure, AWS, GCP) through the ServiceNow portal.







# Updated All Devices list

Stage : GA

Product family : Microsoft Entra ID

Overview: Provides new capabilities to better manage your organizations' devices, including more filtering options, infinite scrolling, or column reordering

Home > Devices

Devices | All devices

JORLOPLABS - Microsoft Entra ID

Overview

All devices

Manage

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Local administrator password recovery

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

Diagnose and solve problems

Download devices

Refresh

Manage view

Enable

Disable

Delete

Azure Active Directory is becoming Microsoft Entra ID.

Search by name or device ID or object ID

Add filters

24 devices found

<input type="checkbox"/>	Name ↑	Enabled	OS
<input type="checkbox"/>		Yes	iOS
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows
<input type="checkbox"/>		Yes	Windows

Add filters

Filter

Enabled

Enabled

Compliant

Join type

Activity

OS

Device Type

MDM

Autopilot

Extension attributes

Administrative unit

Owner

Apply

Cancel

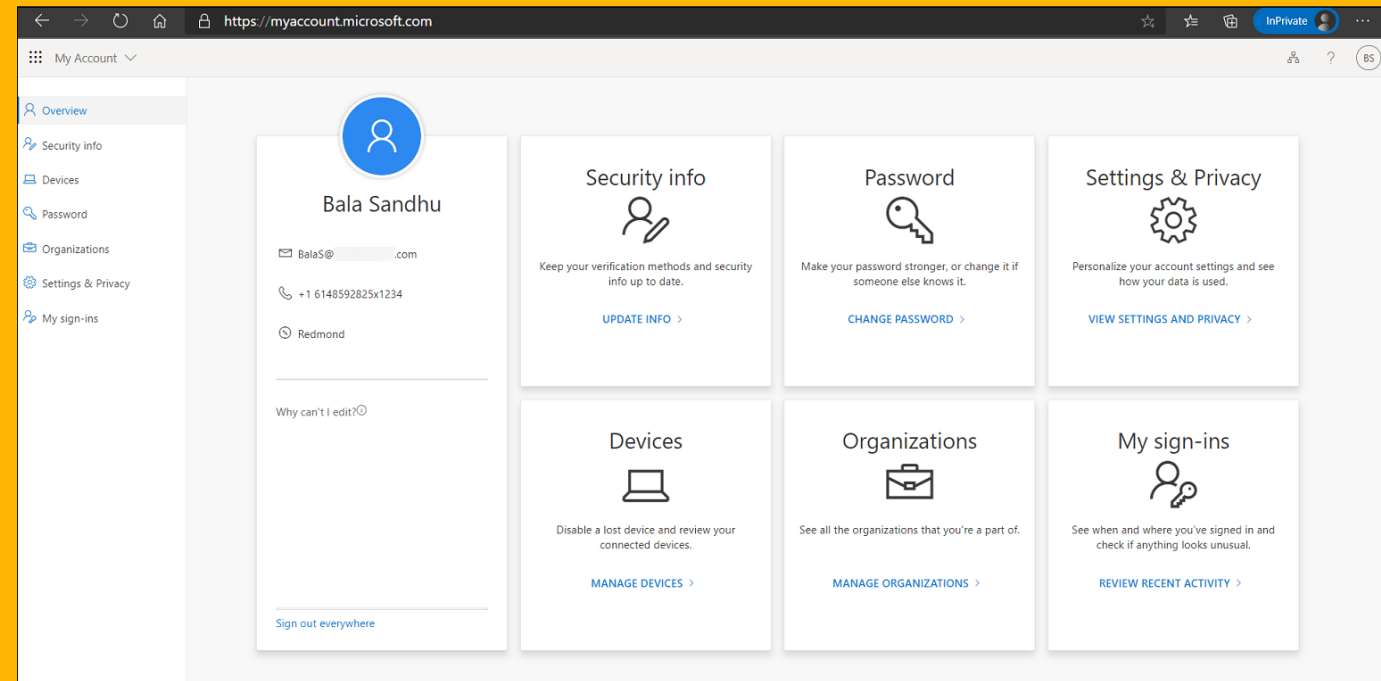
# Managing and changing passwords in My Security Info



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** Administrators can use CA registration policies with authentication strengths targeting My Security Info to control the end user experience for changing passwords. Based on the CA policy, users can change their password by entering their existing password, or if they authenticate with MFA and satisfy the CA policy, can change the password without entering the existing password.





425Show

# Trusted certificate authorities in App management policy



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** Enables admins to restrict the use of certificates in apps and service principals to only certain trusted certificate authorities. Admins can create a trusted certificate authority store which holds a collection of authorities wherein each chain of trust is defined by their intermediate and root authority link. This collection in the store is later referenced in the App management default tenant policy allowing admins to limit all applications in their tenant to use the same certificate authority or create custom policies which serve as exceptions to the default policy for specific scenarios.

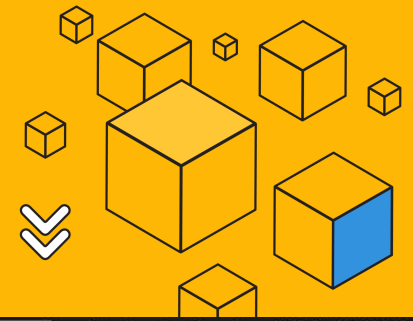
PATCH <https://graph.microsoft.com/v1.0/policies/defaultAppManagementPolicy>

```
{
  "id": "d015220e-9789-4e8e-bbcc-270fe419229d",
  "description": "Lorem ipsum",
  "displayName": "Credential management policy",
  "isEnabled": true,
  "applicationRestrictions": {
    "passwordCredentials": [
      {
        "restrictionType": "passwordLifetime",
        "maxLifetime": "P14D",
        "restrictForAppsCreatedAfterDateTime": "2020-01-01T07:00:00Z"
      }
    ],
    "keyCredentials": [
      {
        "restrictionType": "certificateLifetime",
        "restrictForAppsCreatedAfterDateTime": "2020-01-01T10:37:00Z",
        "maxLifetime": "P90D"
      },
      {
        "restrictionType": "trustedCertificateAuthority",
        "certificateBasedApplicationConfigurationIds": [
          "eec5ba11-2fc0-4113-83a2-ed986ed13743"
        ],
        "restrictForAppsCreatedAfterDateTime": "2019-10-19T10:37:00Z"
      }
    ]
  }
}
```



425Show

# Microsoft Graph activity logs



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** The MicrosoftGraphActivityLogs provide admins full visibility into all HTTP requests accessing the tenant's resources through the Microsoft Graph API. These logs can be used to find activity from compromised accounts, identify anomalous behavior, or investigate application activity.

The screenshot displays the Microsoft Entra admin center interface. The left sidebar shows the navigation menu with categories like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, and Monitoring & health. The main content area is titled 'Logs' and shows a query editor for 'Woodgrove-LogA...'. The query is as follows:

```
1 MicrosoftGraphActivityLogs
2 | where TimeGenerated > ago(1h)
3 | where ResponseStatusCode == 401 or ResponseStatusCode == 403
4 | project AppId, UserId, ServicePrincipalId, ResponseStatusCode, RequestUri,
   RequestMethod
5 | limit 1000
6
```

The query results are displayed in a table with the following columns: AppId, UserId, ResponseStatusCode, RequestUri, and RequestMethod. The results show four entries, all with a ResponseStatusCode of 403 and a RequestMethod of GET.

AppId	UserId	ResponseStatusCode	RequestUri	RequestMethod
> 4813382a-8fa7-425e-ab75...	83999d1-8aad-491a-b276-b81...	403	https://graph.microsoft.com/v1...	GET
> 4813382a-8fa7-425e-ab75...	83999d1-8aad-491a-b276-b81...	403	https://graph.microsoft.com/v1...	GET
> 4813382a-8fa7-425e-ab75...	83999d1-8aad-491a-b276-b81...	403	https://graph.microsoft.com/v1...	GET
> 4813382a-8fa7-425e-ab75...	83999d1-8aad-491a-b276-b81...	403	https://graph.microsoft.com/v1...	GET



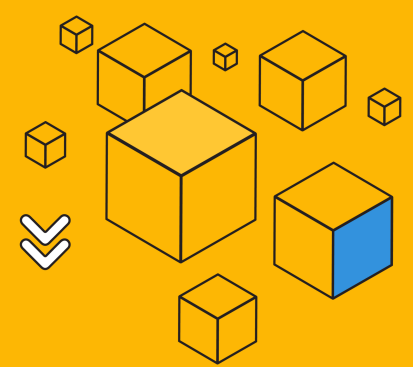
425Show

# My Access overview page

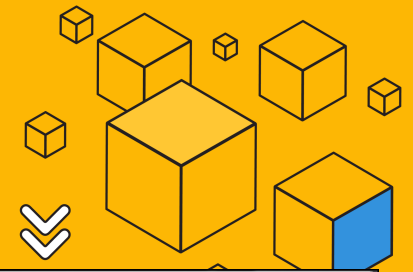
**Stage :** Public Preview

**Product family :** Microsoft Entra ID

**Overview :** The new overview page in the My Access portal shows end users key tasks that need their attention such as pending requests and reviews. Admins can enable/disable the overview page preview from the Microsoft Entra portal by navigating to Entitlement management > Settings > Opt-in Preview Features and locating the My Access overview page in the table.



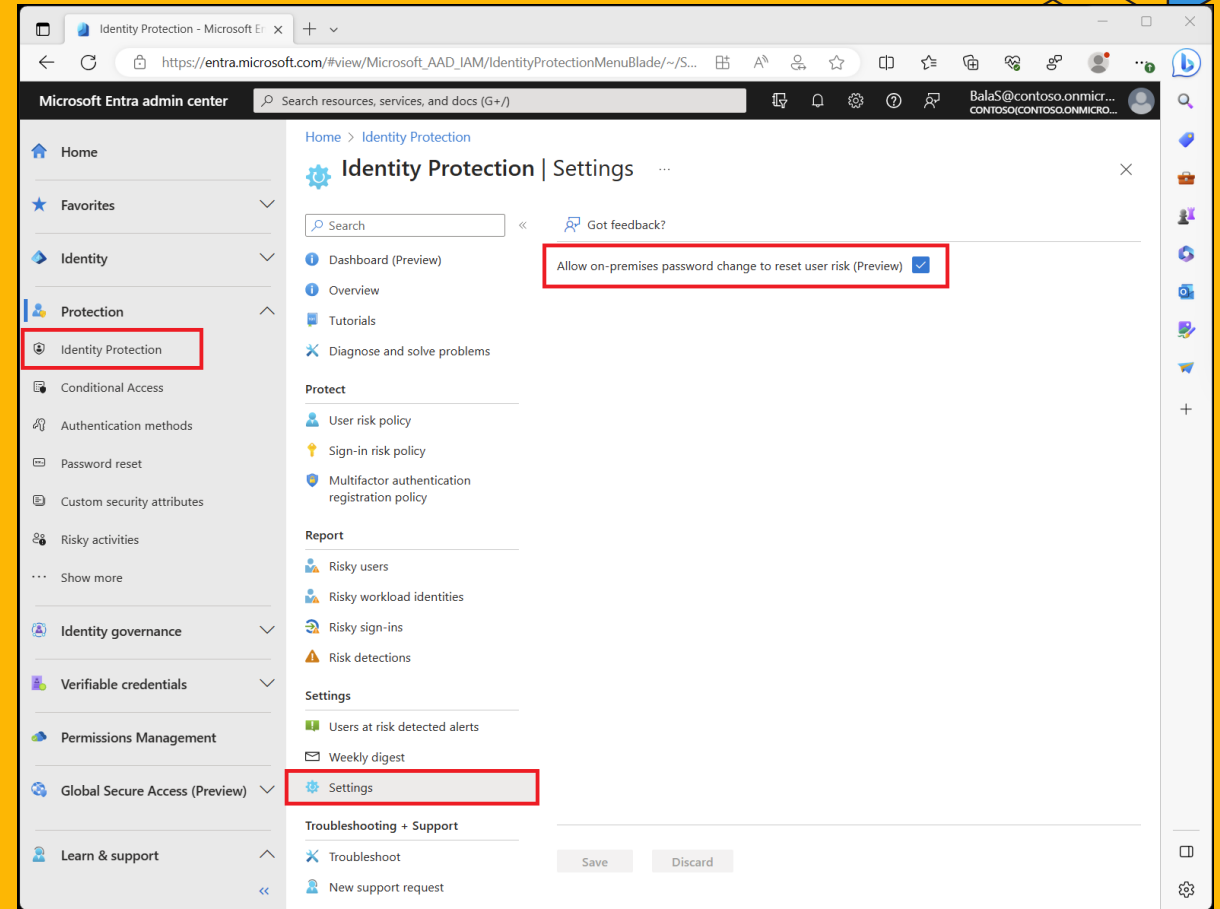
# ID Protection: remediate user risk through on-premises password reset



**Stage :** Public Preview

**Product family :** Microsoft Entra ID

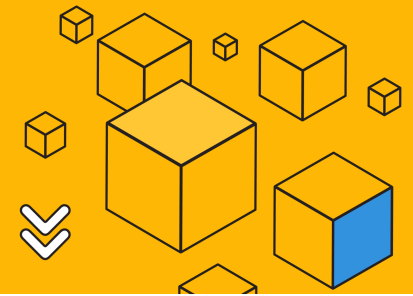
**Overview:** By enabling the new setting called Allow on-premises password change to reset user risk you can remediate risky users through on-premises password resets and deploy user risk policies for automatic user risk remediation to respond to user risks efficiently and protect your organization.





425Show

# Microsoft Entra Verified ID: Quick setup



**Stage :** Public Preview

**Product family :** Microsoft Entra Verified ID

**Overview:** Now with a single click admins can enable Microsoft Entra Verified ID to issue Verified Employee credentials to employees so they can prove the company they work for across the internet. Such credentials can then be used for enabling granular attribute based cross-tenant entitlements using Governance, while reducing approval fatigue, automate revocation and improve compliance posture.

The screenshot shows the 'Verified ID | Get started' page within the Azure Active Directory interface. On the left is a navigation pane with links to Home, Azure Active Directory, Permissions Management, Verified ID, Get started (selected), Overview, Credentials, and Organization settings. The main content area has a breadcrumb 'Home > Verified ID >' and a title 'Verified ID | Get started'. Below this is a welcome message: 'Welcome to Microsoft Entra Verified ID' followed by 'Create and issue custom credentials or pre-configured ones that allow you to verify information online with little to no custom code written.' There are two main sections: 'Quick and easy Verified ID setup' with a 'Get started' button, and 'Control apps access with Verified ID' with a 'Learn more' button. At the bottom, there is a 'Give feedback' link and a note about manual setup with a 'here' link.

Home > Verified ID >

## Verified ID | Get started

Azure Active Directory

### Welcome to Microsoft Entra Verified ID

Create and issue custom credentials or pre-configured ones that allow you to verify information online with little to no custom code written.

#### Quick and easy Verified ID setup

Unlock verifiable workplace credentials. It only takes a click and will be ready for use instantly.

[Get started](#)

#### Control apps access with Verified ID

Add a verified ID to your Access package or request it to secure access to high value packages.

[Learn more](#)

If you wish to use manual setup of Verified ID, you can do so [here](#)

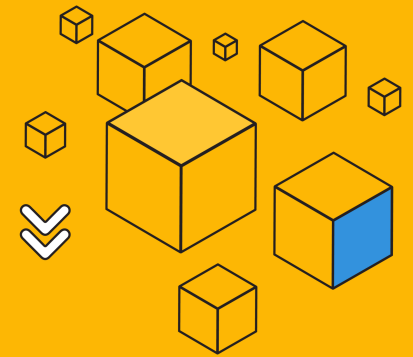
[Give feedback](#)

[Help us improve the landing page](#)





# Microsoft Entra Permissions Management: Okta integration



**Stage :** Public Preview

**Product family :** Microsoft Entra Permissions Management

**Overview:** Allows security admins to integrate with Okta during or after the AWS account onboarding. This feature allows Microsoft Entra Permissions Management to read AWS permission assignments to users via Okta groups and to provide more accurate analytics, effectively calculate permissions granted and as a result a precise permissions creep index.

### Configure identity provider (IdP) (Public Preview)

Configuring Identity Provider is an optional step.

By configuring Identity Provider information, Permissions Management can read user and role access configured at Identity Provider. Admins can see the augmented view of assigned permissions to the identities.

None

Select this option if you do not want any integration

AWS IAM Identity Center

Allow Permissions Management to read user and role access configured at AWS IAM Identity Center




Okta

Allow Permissions Management to read user and role access configured at Okta

#### Okta Integration

Download the Okta Credentials template to create AWS secret for Okta Credentials

#### Download Okta Credentials Template



Launch Okta Credentials Template

Secret ARN\*

secret-arn



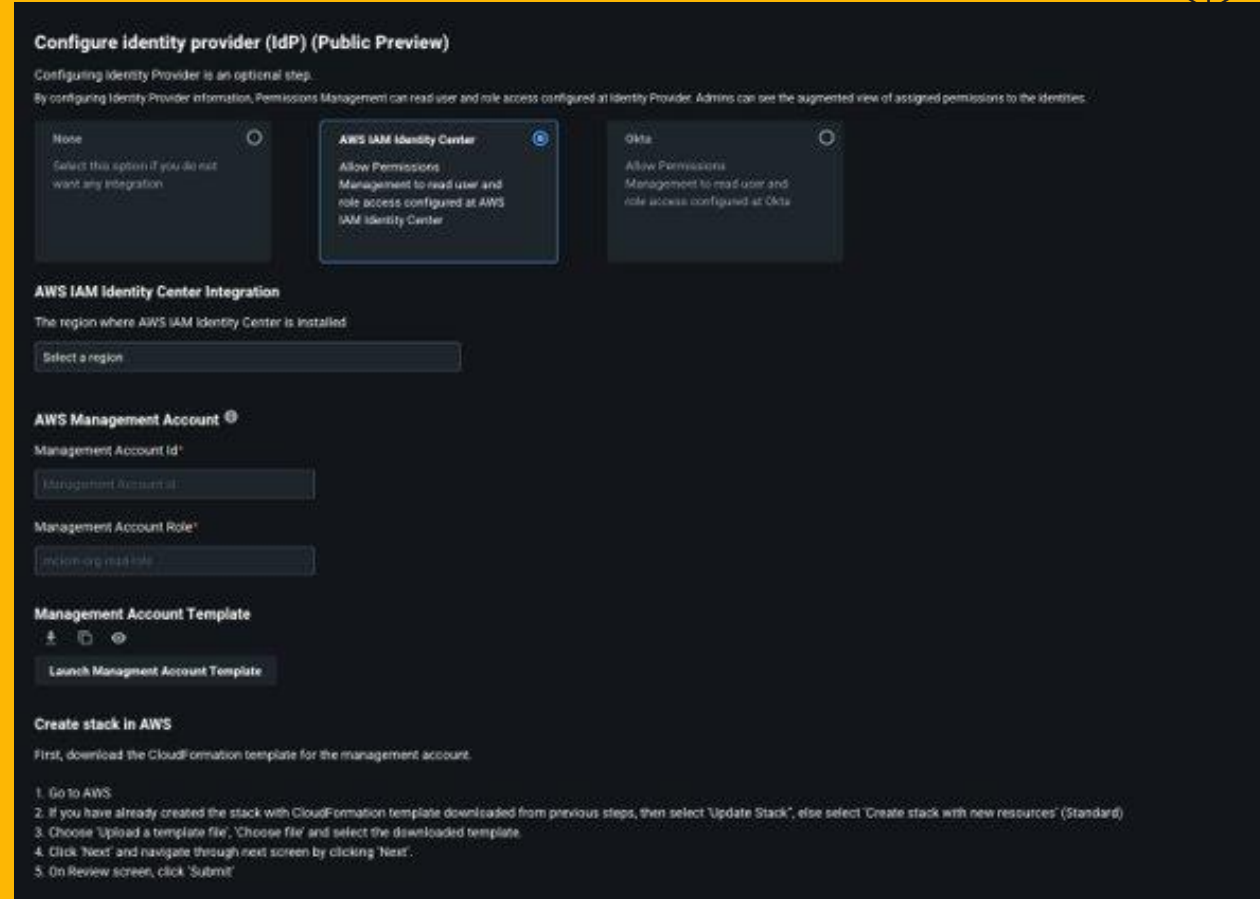
# Microsoft Entra Permissions Management: AWS IAM Identity Center integration



**Stage :** Public Preview

**Product family :** Microsoft Entra Permissions Management

**Overview:** Allows an admin to get the full view of permissions assigned to identities via AWS IAM Identity Center. By running the cloud formation template in an AWS environment, the admin allows Microsoft Entra Permissions Management to read user and role access configuration data from the management account. After a successful configuration, Microsoft Entra Permissions Management can read the data to calculate the permissions



**Configure identity provider (IdP) (Public Preview)**

Configuring Identity Provider is an optional step.  
By configuring Identity Provider information, Permissions Management can read user and role access configured at Identity Provider. Admins can see the augmented view of assigned permissions to the identities.

**None** ☐ Select this option if you do not want any integration.

**AWS IAM Identity Center** ☒ Allow Permissions Management to read user and role access configured at AWS IAM Identity Center.

**Okta** ☐ Allow Permissions Management to read user and role access configured at Okta.

**AWS IAM Identity Center Integration**

The region where AWS IAM Identity Center is installed

Select a region

**AWS Management Account** ⓘ

Management Account Id\*

Management Account Role\*

Management Account Template

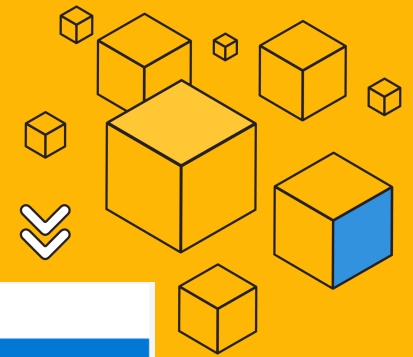
Launch Management Account Template

**Create stack in AWS**

First, download the CloudFormation template for the management account.

1. Go to AWS.
2. If you have already created the stack with CloudFormation template downloaded from previous steps, then select 'Update Stack', else select 'Create stack with new resources' (Standard).
3. Choose 'Upload a template file', 'Choose file' and select the downloaded template.
4. Click 'Next' and navigate through next screen by clicking 'Next'.
5. On Review screen, click 'Submit'.

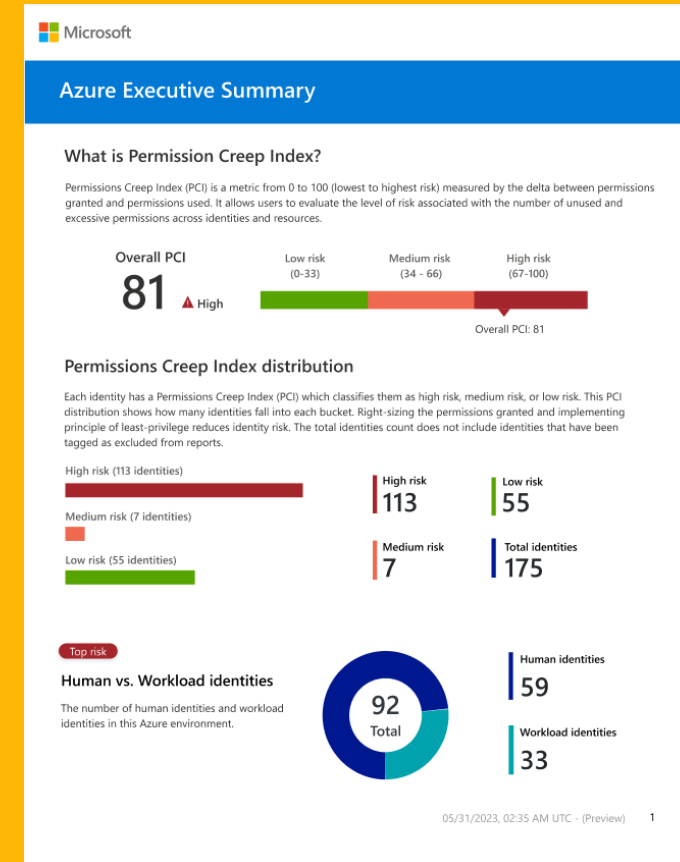
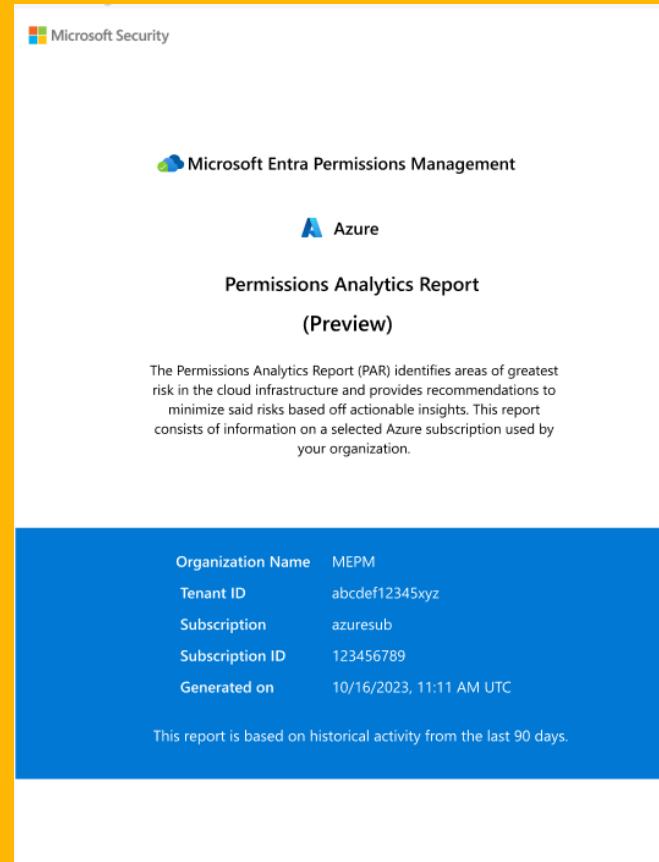
# Microsoft Entra Permissions Management: Permissions Analytics Report (PAR) PDF



**Stage :** Public Preview

**Product family :** Microsoft Entra Permissions Management

**Overview:** The PAR lists findings across identities and resources in Microsoft Entra Permissions Management and can be directly viewed in the UI, downloaded in an Excel format, and exported as a PDF. The report is available for all supported cloud environments: AWS, Microsoft Azure, and GCP, and can be downloaded for up to 10 authorization systems with one click.



# Thank you for tuning in!

Don't forget to tune in again for the October updates in November!



## 425Show



Grace Picking



Jorge Lopez