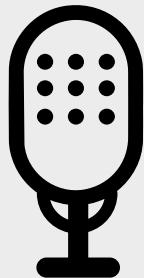
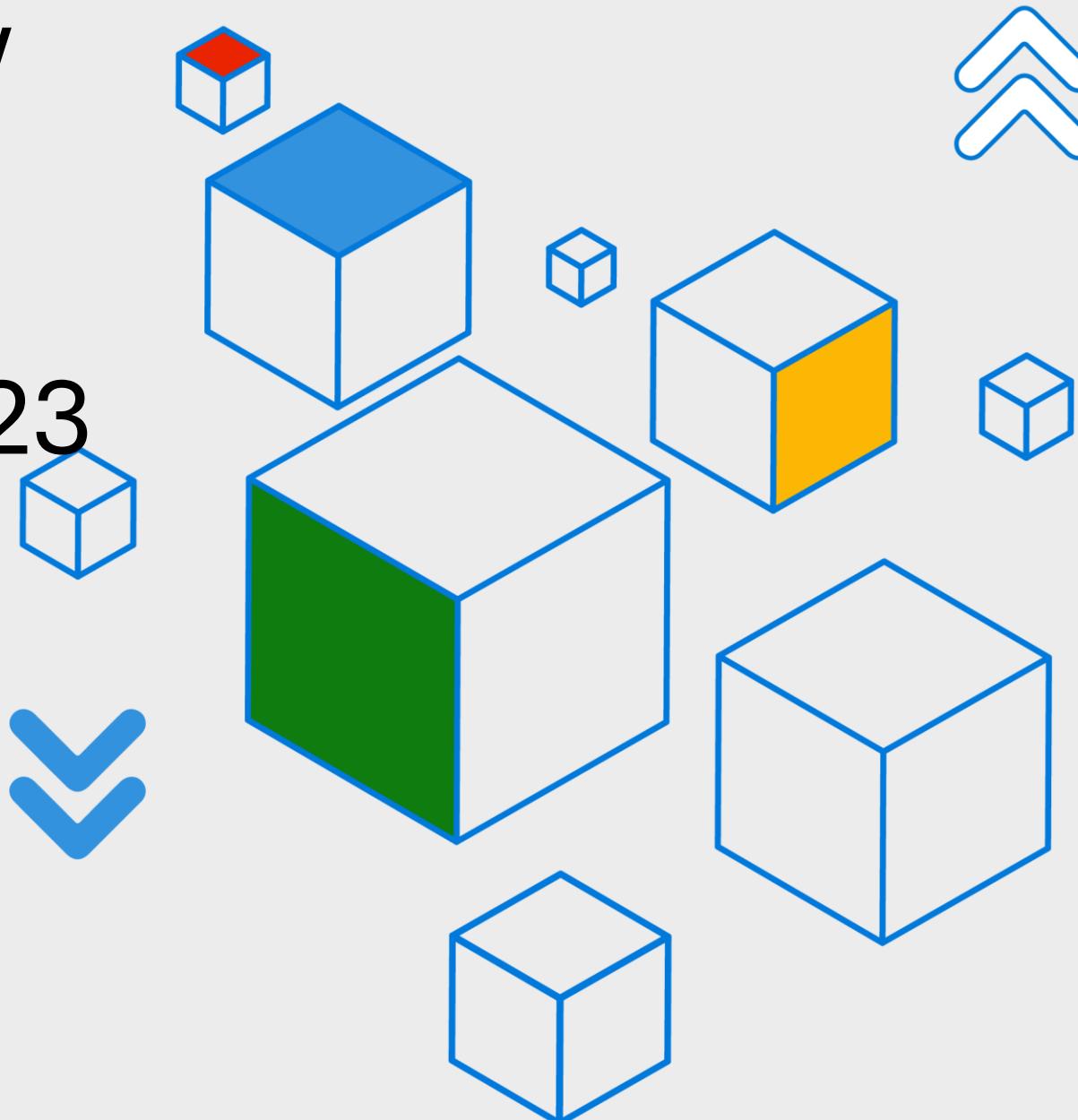


What's New in Microsoft Entra ID

October 2023



425Show



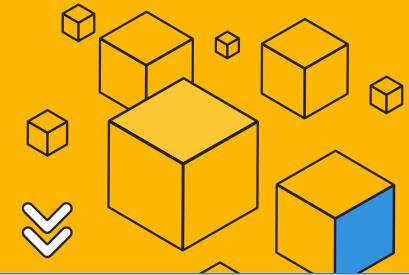
Grace Picking



Jorge Lopez



Privileged Roles and permissions in Entra ID



Stage : Public Preview

Product family : Microsoft
Entra ID

Overview : Allow you to identify which custom and built-in roles, permissions and role assignments are privileged using the Microsoft Entra admin center, PowerShell, or Graph API. Also provide guidance for best practices for using privileged roles.

Home > Default Directory | Roles and administrators >

Roles and administrators | All roles

Default Directory - Azure Active Directory

+ New custom role | Delete custom role | Download assignments | Refresh | Preview features | Got feedback?

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

⚠ There are currently 16 privileged role assignments. It is recommended to not exceed 10.

ⓘ Your Role: Global Administrator and 2 other roles

Administrative roles

Administrative roles are used for granting access for privileged actions in Azure AD. We recommend using these built-in roles for delegating access to manage application configuration permissions without granting access to manage other parts of Azure AD not related to application configuration. [Learn more](#).

Learn more about Azure AD role-based access control

Search by name or description | Add filters

Role	Description	Privileged	Assign...	Type
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	0	Built-in
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	1	Built-in
Attack Payload Author	Can create attack payloads that an administrator can initiate later.		0	Built-in
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.		0	Built-in
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Azure AD objects.		6	Built-in
Attribute Assignment Reader	Read custom security attribute keys and values for supported Azure AD objects.		1	Built-in
Attribute Definition Administrator	Define and manage the definition of custom security attributes.		3	Built-in



Delegate Azure role assignments with attribute-based access control (ABAC) conditions



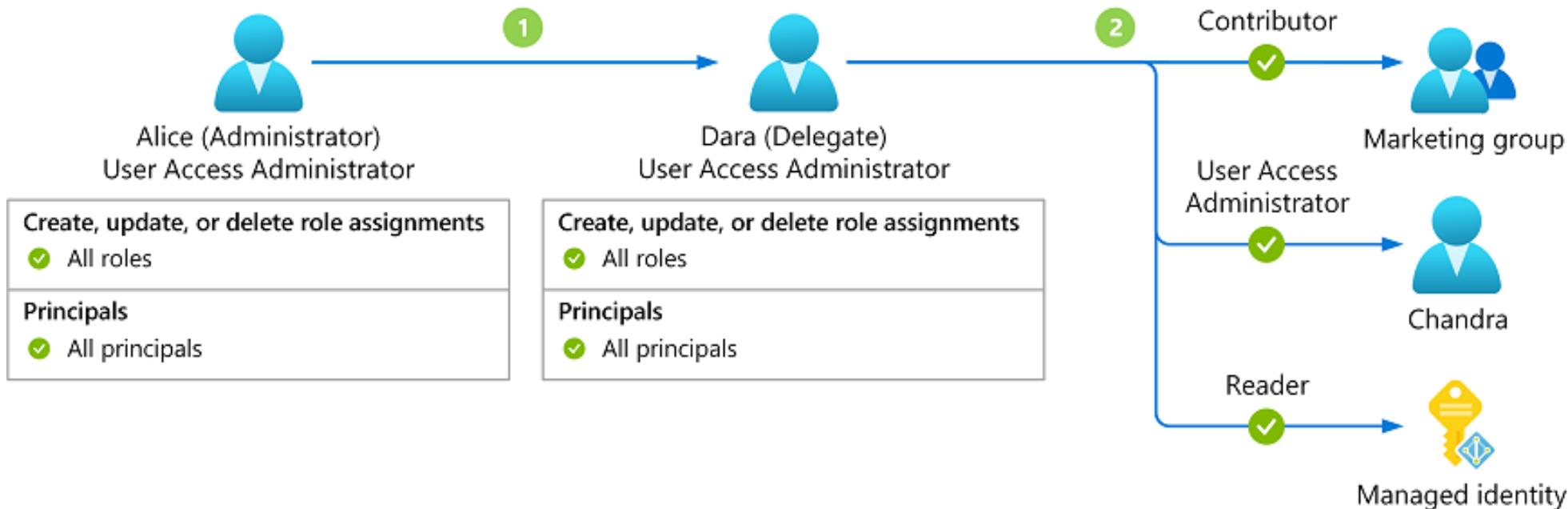
Stage : Public Preview

Product family : Microsoft Entra ID

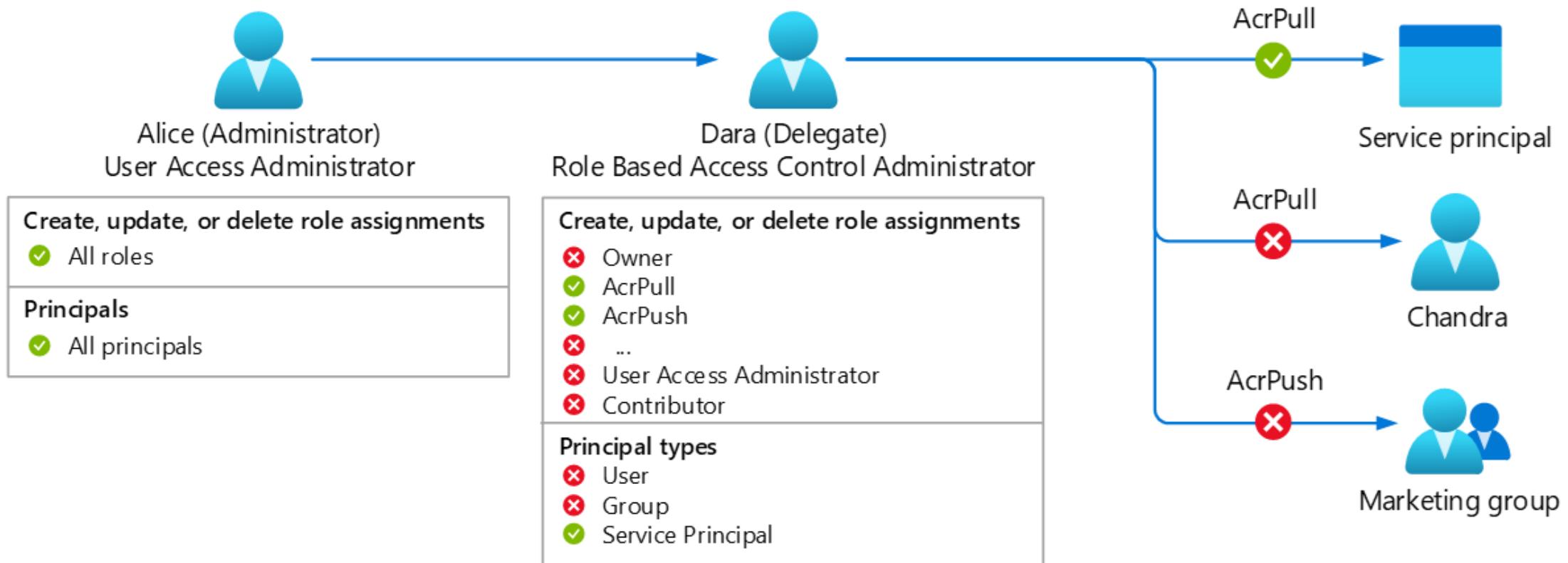
Overview : This feature enables cloud administrators to grant the ability to assign Azure roles while adding restrictions on the roles they can assign and who they can assign roles to. For example, allow an admin to create Azure role assignments for VM Contributor and Reader role only.

[Aka.ms/425show/AzureABACPreview](https://aka.ms/425show/AzureABACPreview)

How customers delegate role assignments

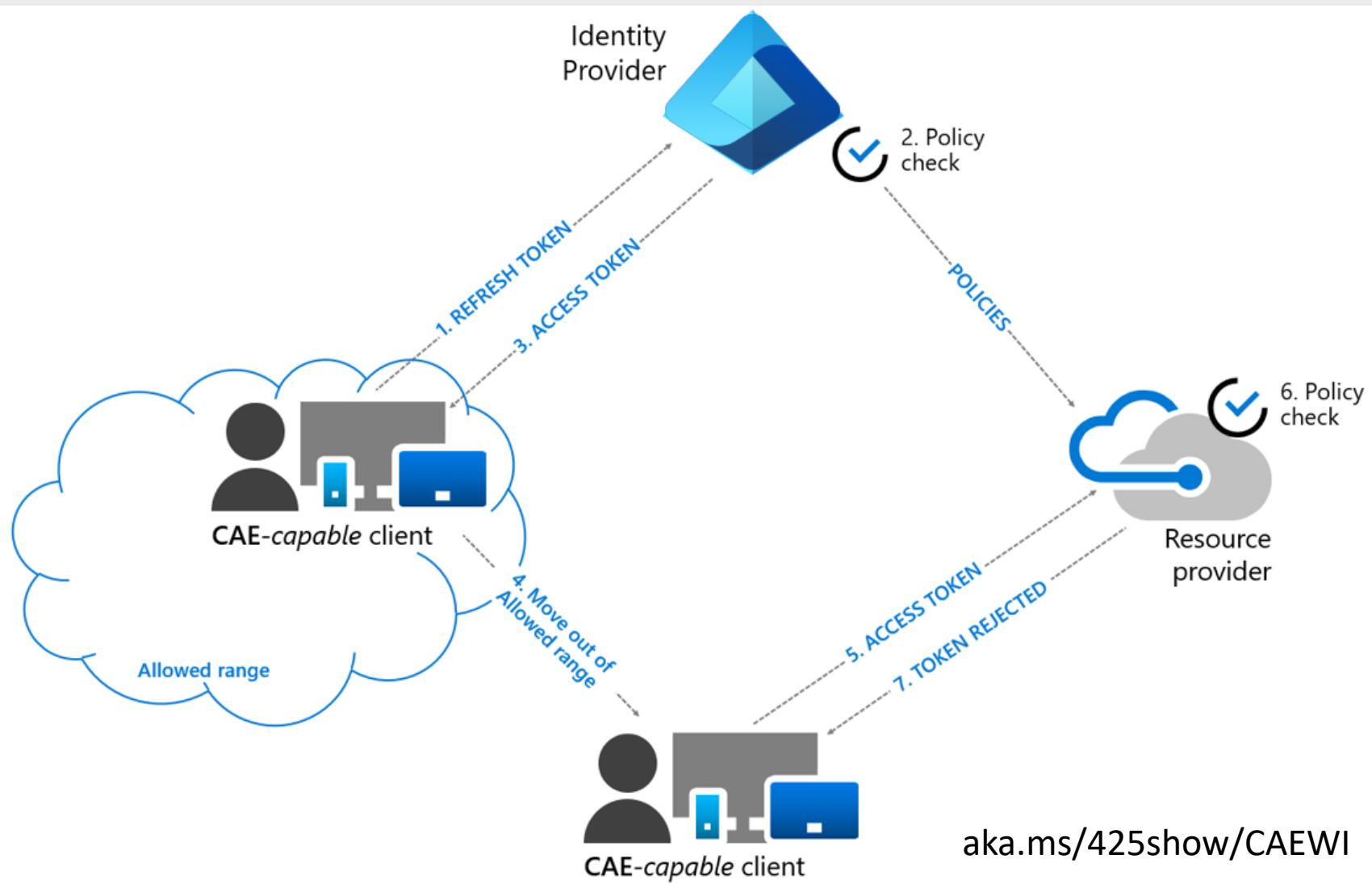
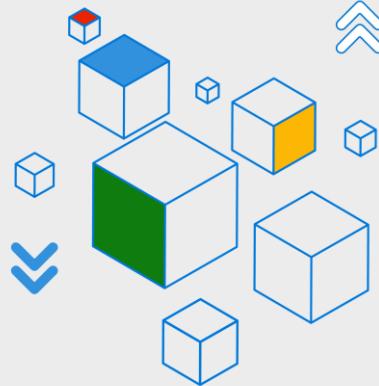


How you can delegate azure role assignments using conditions





Continuous access evaluation (CAE) for workload identities



Stage : GA

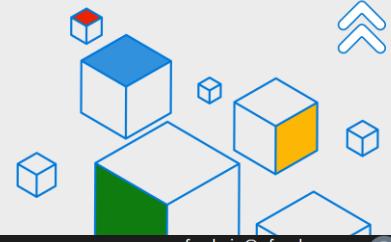
Product family : Microsoft Entra Workload ID

Overview : Enables real-time enforcement of Conditional Access location and risk policies along with instant enforcement of token revocation events for workload identities. We support the revocation events for disabling and deleting service principals, and detect a high service principal risk leveraging Azure AD Identity Protection



425Show

Application Instance lock for workload identities



Stage : GA Product
family : Microsoft
Entra workload ID

Overview : Allows app developers to protect their multi-tenant apps from having critical properties tampered by attackers

Microsoft Entra admin center Search resources, services, and docs (G+)

Home > App registrations > Roles Demo - MultiTenant

Roles Demo - MultiTenant | Authentication

Search Got feedback? ID tokens (used for implicit and hybrid flows)

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (JORLOPLABS only)
 Accounts in any organizational directory (Any Microsoft Entra ID t Help me decide...

Due to temporary differences in supported functionality, we don't recommend accounts for an existing registration. If you need to enable personal accounts, contact support. Learn more about these restrictions.

Starting November 9th, 2020 end users will no longer be able to grant permissions to apps without verified publishers. Add MPN ID to verify publisher

Advanced settings
Allow public client flows ⓘ
Enable the following mobile and desktop flows:

- App collects plaintext password (Resource Owner Password Cre
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flo

App instance property lock ⓘ
Configure the application instance modification lock. [Learn more](#)

App instance property lock

Roles Demo - MultiTenant

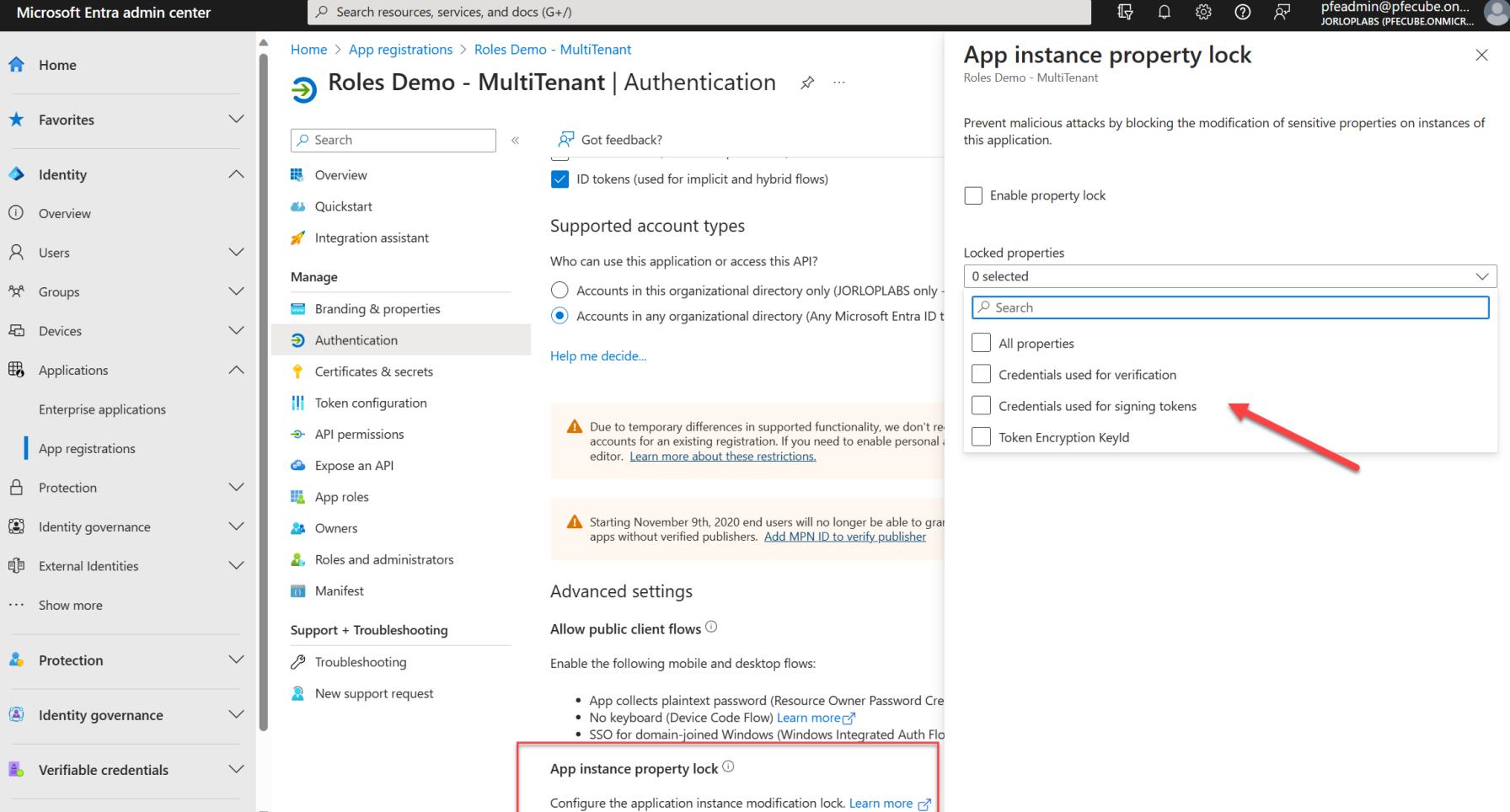
Prevent malicious attacks by blocking the modification of sensitive properties on instances of this application.

Enable property lock

Locked properties
0 selected

Search

All properties
 Credentials used for verification
 Credentials used for signing tokens
 Token Encryption KeyId



Aka.ms/425show/SPLockConfiguration



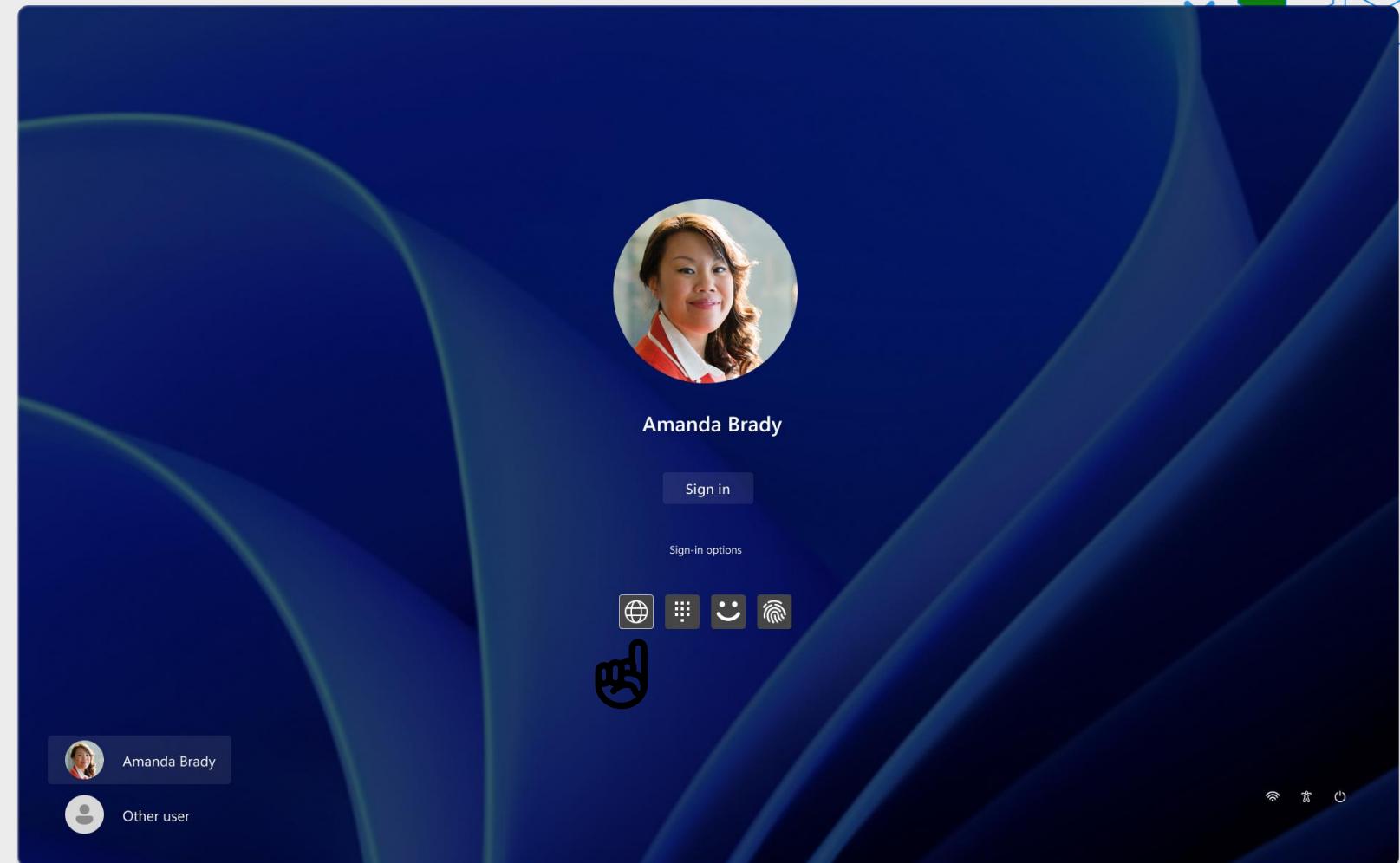
425Show

Web sign in on Windows



Stage : GA Product family :
Microsoft Entra ID

Overview: A new Web Sign-In experience has been released as part of the September update for Windows 11. This update significantly enhances security, reliability, performance, and the overall end-to-end user experience. It also expands the range of supported scenarios

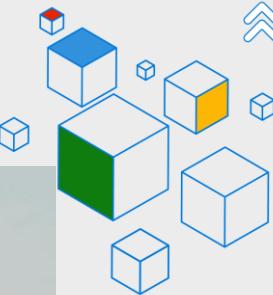


aka.ms/425show/W11WebSignIn



425Show

Web sign in on Windows



4:39

Wednesday, August 2



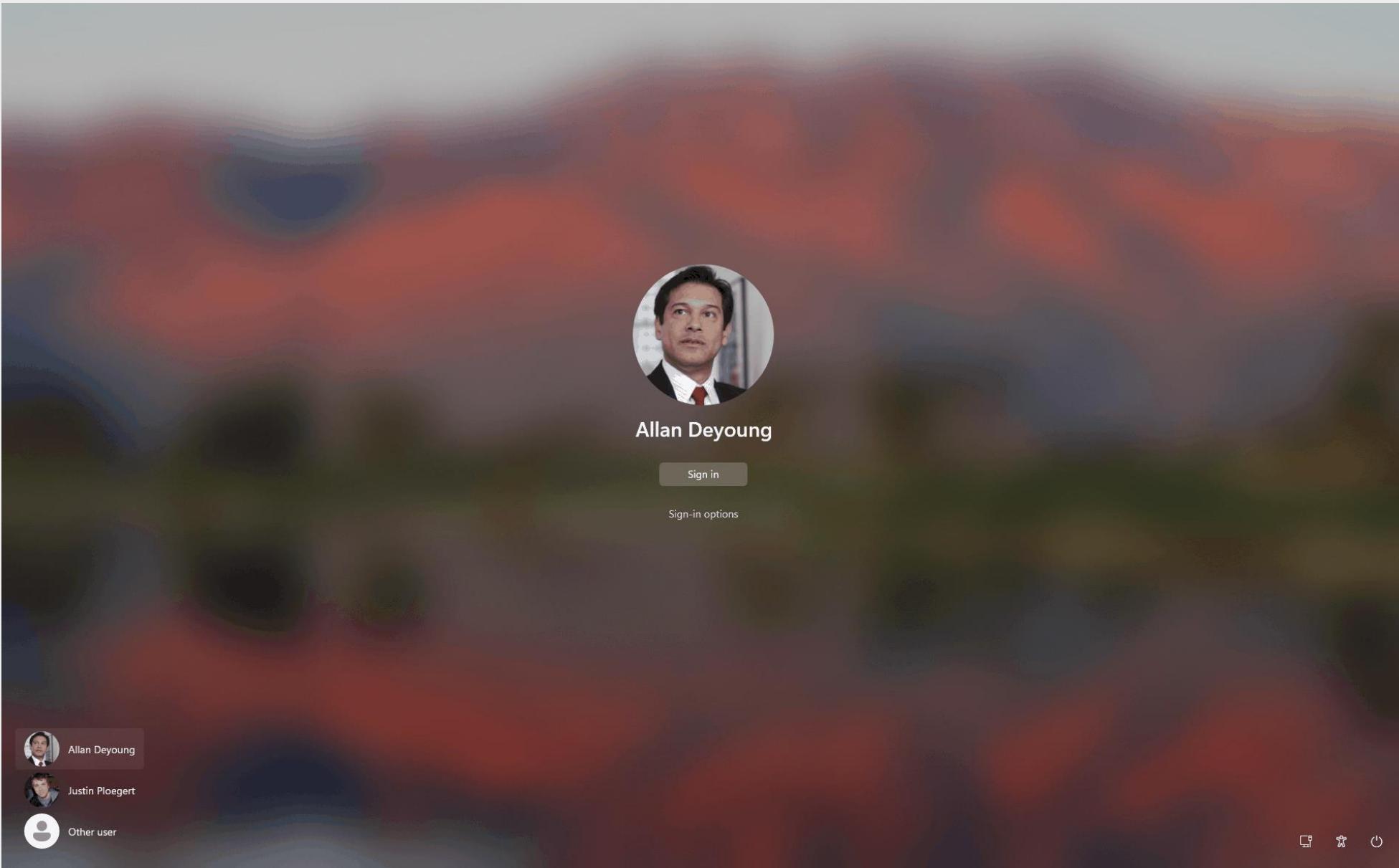
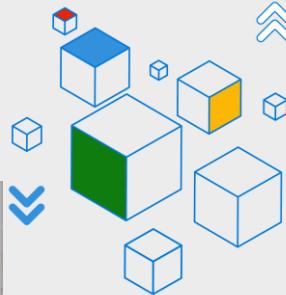
Activate Windows
Go to Settings to activate Windows.





425Show

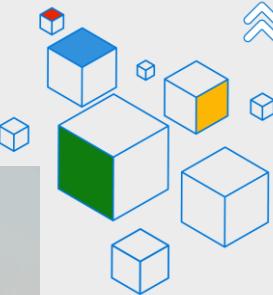
Web sign in on Windows





425Show

Web sign in on Windows



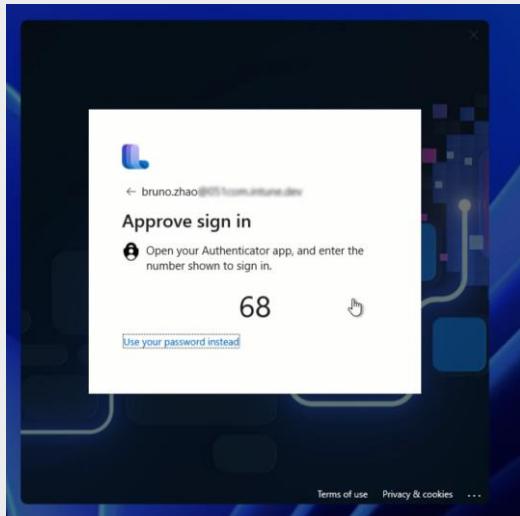
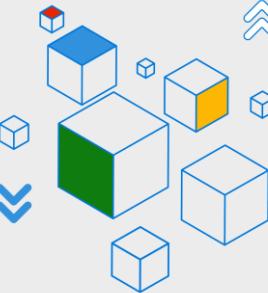
3:06

Wednesday, August 2

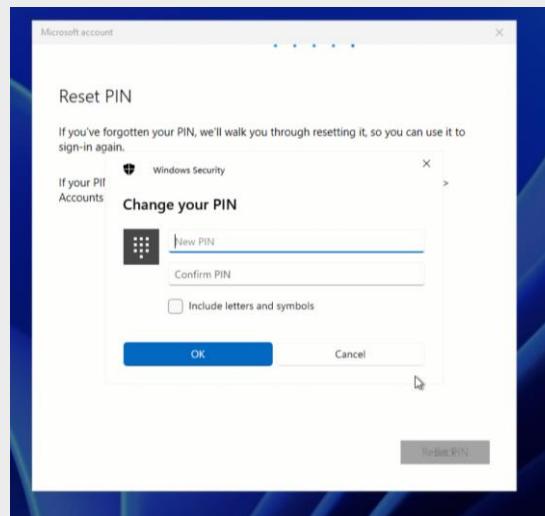


Web sign in on Windows - Scenarios

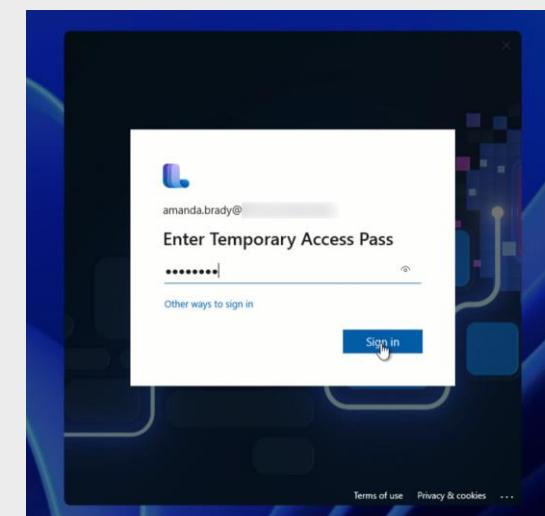
Available with the September release of Windows 11 (23H2)



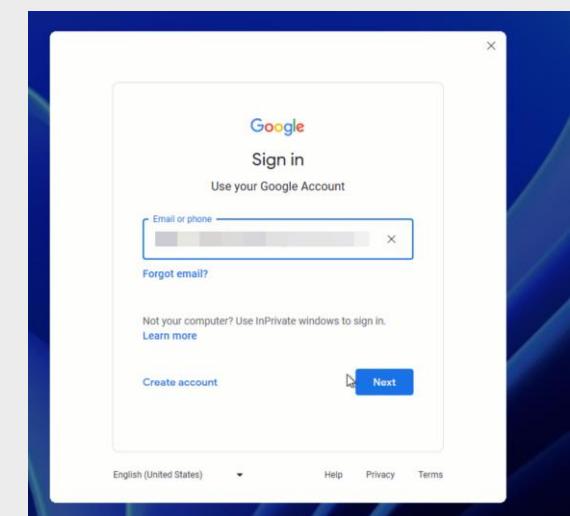
Passwordless sign-in



Windows Hello for
Business PIN
reset



Temporary Access
Pass (TAP)



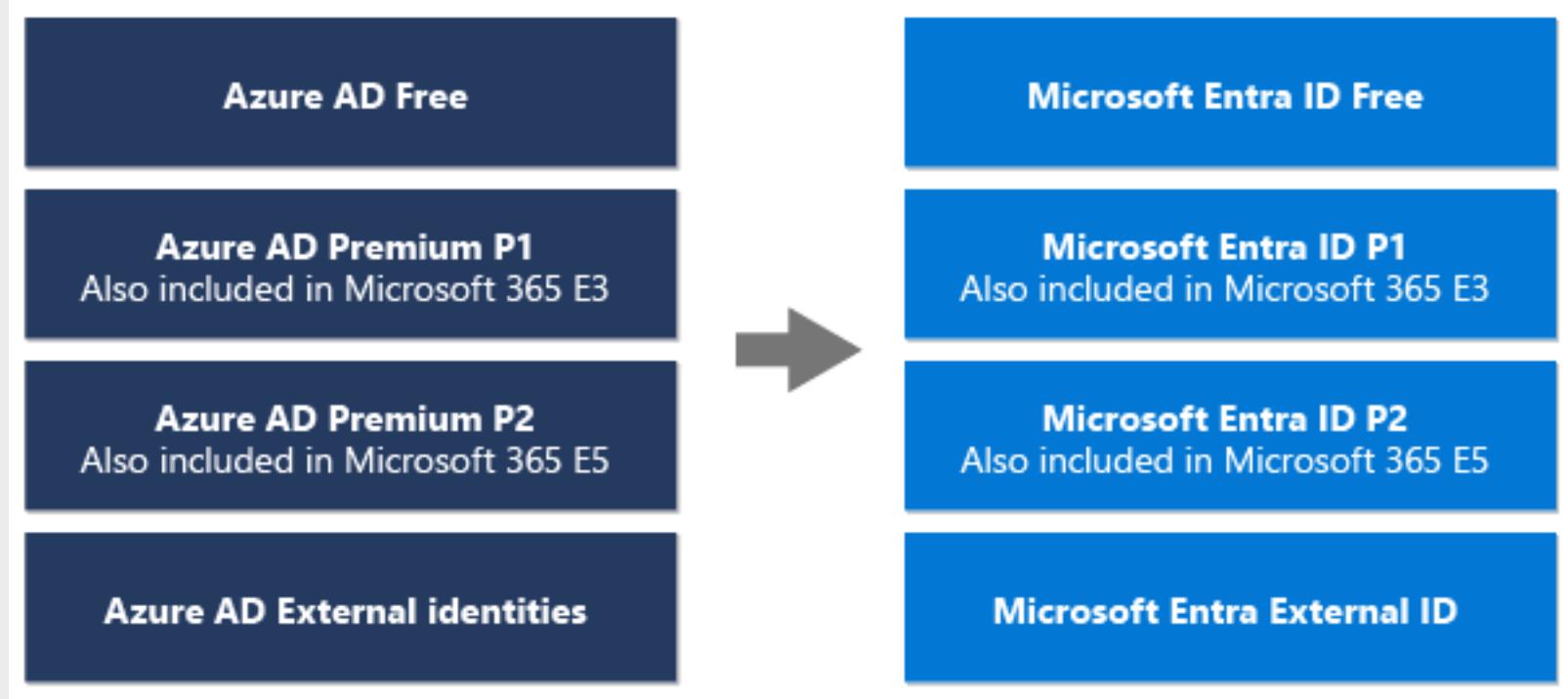
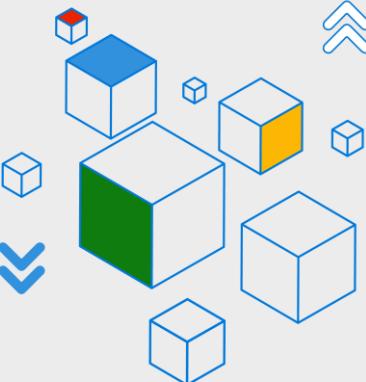
Sign in with a
federated identity



Announcements

<https://aka.ms/AADRebrandFAQ>

<https://aka.ms/howtorenameAzureAD>



July 11
Announce

August 15
Changes begin

October 1
SKU rename
November 15
Microsoft Ignite



Unifying the identity and network access portfolio with the Microsoft Entra product family name

Why change the Azure AD name?

1

Growing set of Identity and Access capabilities that customers are looking to consolidate and unify – IAM, CIAM, IGA, DID, CIEM, SSE, ...

2

Offerings go beyond Azure and Active Directory to protect multi-cloud and hybrid environments, based on Zero Trust principles

3

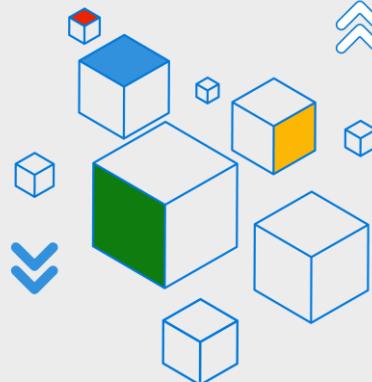
Simplify naming and licensing for customers with one identity product family name, as part of the end-to-end Microsoft security portfolio



425Show

Announcements

<https://admin.microsoft.com/Adminportal>



Over the next two months, two changes to the registration campaign (aka Nudge) feature in Microsoft Entra ID are rolling out (MC650420)

Home > Message center



Message center

Each message gives you a high-level overview of a planned change and how it may affect your users, and links out to more detailed information to help you prepare. [Learn more about managing changes](#)

Inbox Archive

Add to favorites Archive Mark as unread Share

Filters: Service Tag Message state Status for your org Platform

<input checked="" type="checkbox"/> Message title		Service	Last updated	Act by
(Updated) Changes to the registration campaign feature in ...		Microsoft Entra	19 Sept 2023	

(Updated) Changes to the registration campaign feature in Microsoft Entra (previously Azure Active Directory)

MC650420 · Published 20 Jul 2023 · Last updated 19 Sept 2023

Archive Share Copy link Mark as unread

Service & monthly active users

Microsoft Entra

Tag

MAJOR UPDATE ADMIN IMPACT NEW FEATURE USER IMPACT

Message Summary

Updated September 18, 2023: Deployment will begin September 25th and will run to October 20th. These dates replace the dates mentioned in the email "We're enabling a stronger form of multifactor authentication beginning September 15, 2023" that you might have received. We apologize for the inconvenience.

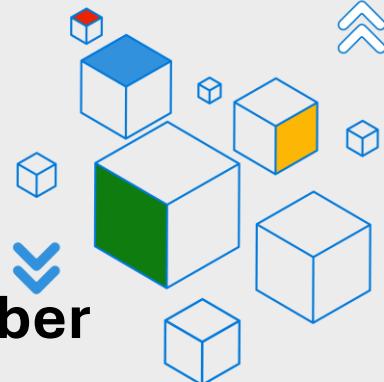
Publicly switched telephone networks (PSTN) such as SMS and voice authentication are the weakest forms of MFA. To help your users move away from these less secure MFA methods we are introducing changes to the [Microsoft managed](#) state of the [registration campaign \(aka Nudge\)](#) feature in Microsoft Entra (previously Azure Active Directory).

When this will happen:



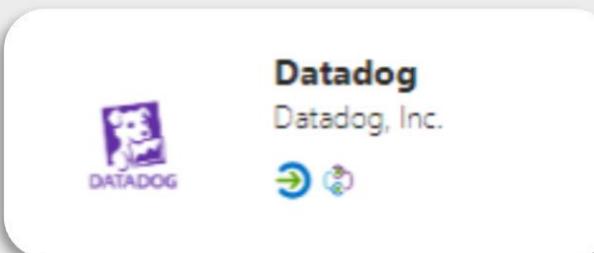
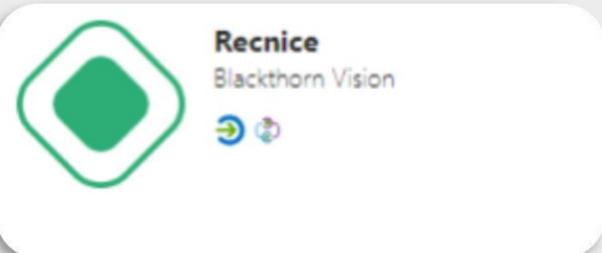
425Show

Did you know?



New applications added to the Microsoft Entra ID app gallery in September 2023 supporting user provisioning.

We've added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:



Microsoft Ignite 2023

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

In Seattle: November 14–17, 2023 PT

Online dates: November 15–16, 2023 PT

Discover the best of what's next in technology, problem-solve with experts, and make global connections to empower yourself to lead your organization.



Register now

Join online from anywhere
November 15–16, 2023 PT

Connect with the global community online from wherever you are while learning from keynotes, breakout sessions, and taking part in live discussions at no cost.

[Register now >](#)

Sold out

In-person Seattle event
November 14–17, 2023 PT

Join us for live, in-person keynotes, participate in interactive labs and demos, learn directly from Microsoft engineers and partners, and catch up with peers while making new connections.

Thank you for
tuning in!

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



425Show



Grace Picking



Jorge Lopez