WELCOME *Entrapreneurs!*

The community for secure access in a connected world!

aka.ms/dmec

DUTCH MICROSOFT
ENTRA COMMUNITY

nedscaper

03-09-2024

Agenda

18.00 Welcome by **Nedscaper**

18.05 - 18.15 What's new in MS Entra by **Jan Bakker**

18.15 - 19.15 **Jorge de Almeida Pinto** - So You Travelled Back In Time. Reconnecting Mismatching Core Identity Stores!

19.15 - 19.30 **Break**

19.30 - 20.30 **Eric Woodruff -** UnOAuthorized: A discovered path to privilege elevation to Global Administrator.

20.30 Drinks

Thanks to our sponsor!

DUTCH MICROSOFT
ENTRA COMMUNITY

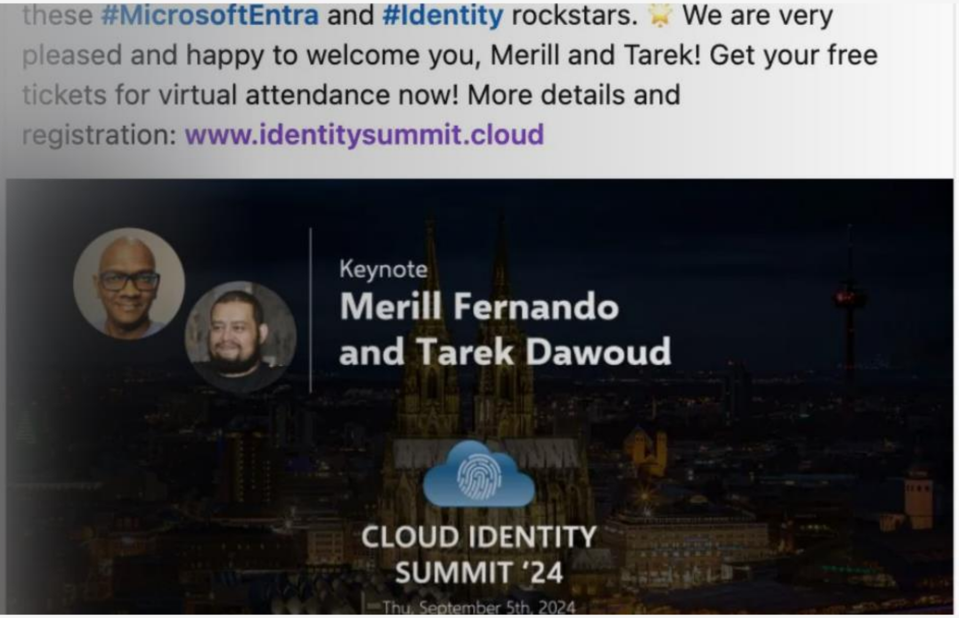
What’s new in Entra?

nedscaper

Entra 🆔 News #60 → This week in Microsoft Entra

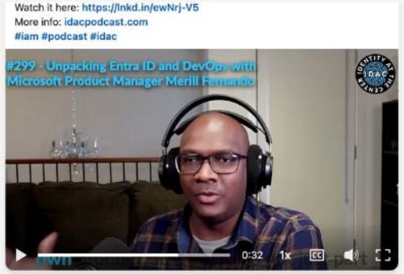
Learn about Microsoft switching from SailPoint to Entra ID Governance 😎, upcoming breaking changes 🤷, Kerberos SSO to on-prem AD in macOS 🍎 💻, changes to the Sync account role and more!

READ THE LATEST



these #MicrosoftEntra and #Identity rockstars. 🌟 We are very pleased and happy to welcome you, Merill and Tarek! Get your free tickets for virtual attendance now! More details and registration: www.identitysummit.cloud

Latest Top Discussions



Watch it here: https://lnkd.in/ewNrj-V5
More info: idacpodcast.com
#iam #podcast #idac

#299 - Unpacking Entra ID and DevOps with Microsoft Product Manager Merill Fernando
IDAC
0:32
1x

Entra 🆔 News #59 → This week in Microsoft Entra

🚀 From securing 🛡️ your Azure deploymen...

AUG 25 • MERILL FERNANDO AND

Merill Fernando (He/Him) • You
Product Manager @ Microsoft 👉 Sign up to Entra.News my wee...
2d • Edited •

⏰ Folks, quick update on the Microsoft MFA enforcement on admin portals.

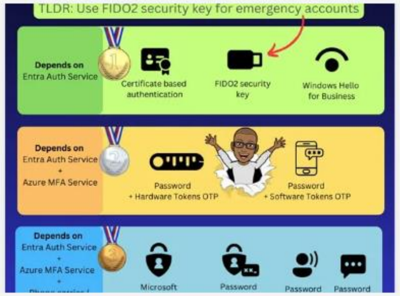
...see more

Enable MFA for your Microsoft admins before 15 Oct 2024!
Multi-factor authentication will be required to sign into these admin portals...

Entra 🆔 News #58 → This week in Microsoft Entra

🎉 Face Check goes GA, 🎓 new Entra Suite...

AUG 18 • JOSHUA FERNANDO AND



TLDR: Use FIDO2 security key for emergency accounts
Depends on Entra Auth Service
Certificate based authentication
FIDO2 security key
Windows Hello for Business
Depends on Entra Auth Service + Azure MFA Service
Password + Hardware Tokens OTP
Password + Software Tokens OTP
Depends on Entra Auth Service + Azure MFA Service
Microsoft
Password
Password
Password

Entra 🆔 News #57 → This week in Microsoft Entra

Learn about bulk provisioning FIDO2 security...

AUG 11 • MERILL FERNANDO

Entra.News - Your weekly dose of Microsoft Entra

Entra.News is a weekly newsletter of the latest Microsoft Entra related news, blog posts & videos from Microsoft, MVPs and infosec experts, curated by Merill & Joshua Fernando. To feature your content on Entra.News tag with #entra or mail hey@entra.news

Type your email... Subscribe

Quick Links

YouTube - @merillx

Microsoft Entra Suite

Microsoft Entra Private Access
Zero Trust Network Access

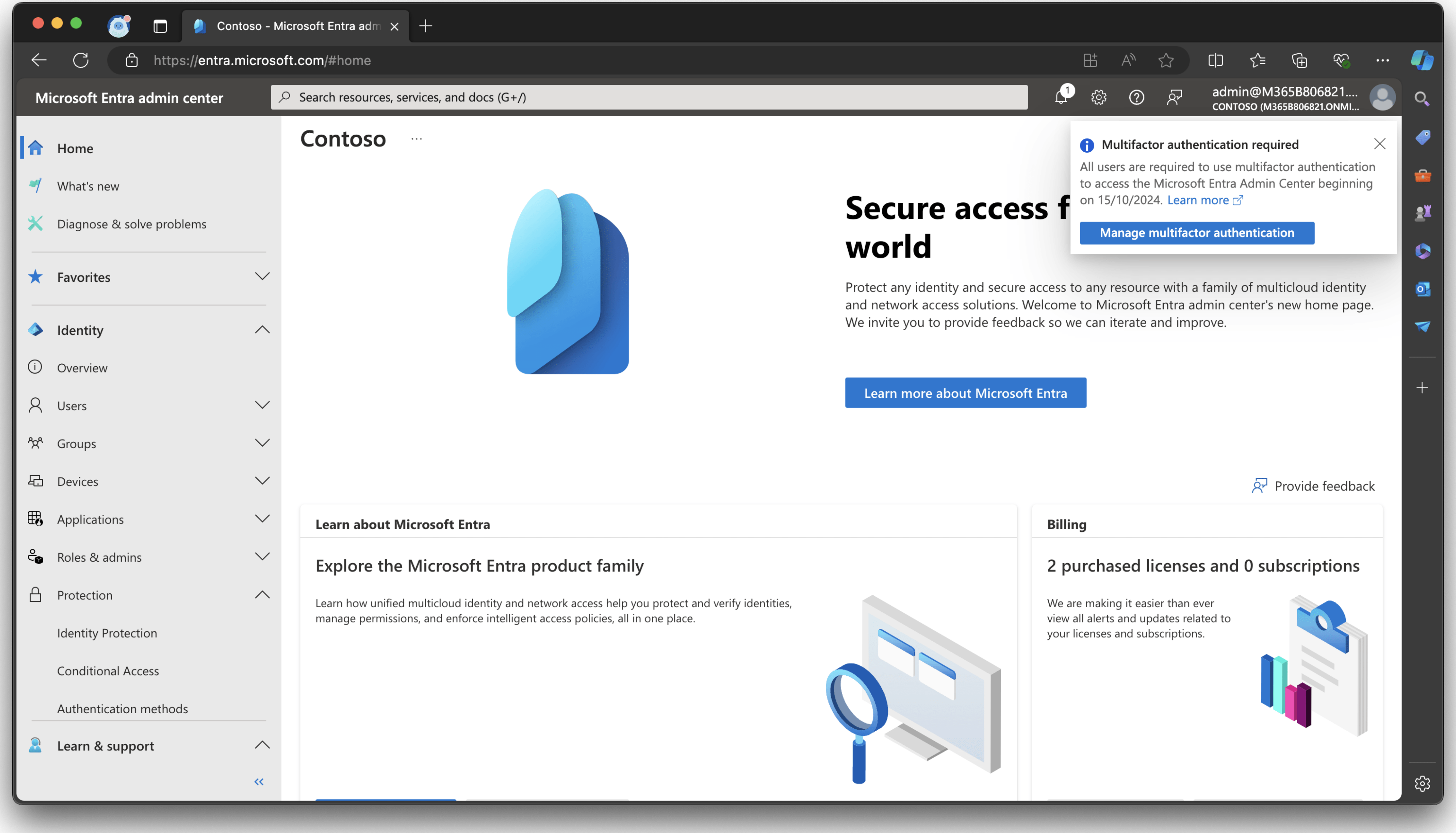
Microsoft Entra Internet Access
Secure Web Gateway

Microsoft Entra ID Governance
Identity Governance and Administration

Microsoft Entra ID Protection
Identity Protection

Microsoft Entra Verified ID (Premium capabilities)
Identity Verification

$12.00
user/month


Contoso - Microsoft Entra adm
https://entra.microsoft.com/#home
Microsoft Entra admin center
Search resources, services, and docs (G+/)
admin@M365B806821....
CONTOSO (M365B806821.ONMI...
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Roles & admins
Protection
Identity Protection
Conditional Access
Authentication methods
Learn & support
Contoso
Learn more about Microsoft Entra
Manage multifactor authentication
Provide feedback

Multifactor authentication required

All users are required to use multifactor authentication to access the Microsoft Entra Admin Center beginning on 15/10/2024. Learn more

Secure access f
world

Protect any identity and secure access to any resource with a family of multicloud identity and network access solutions. Welcome to Microsoft Entra admin center's new home page. We invite you to provide feedback so we can iterate and improve.

Learn about Microsoft Entra

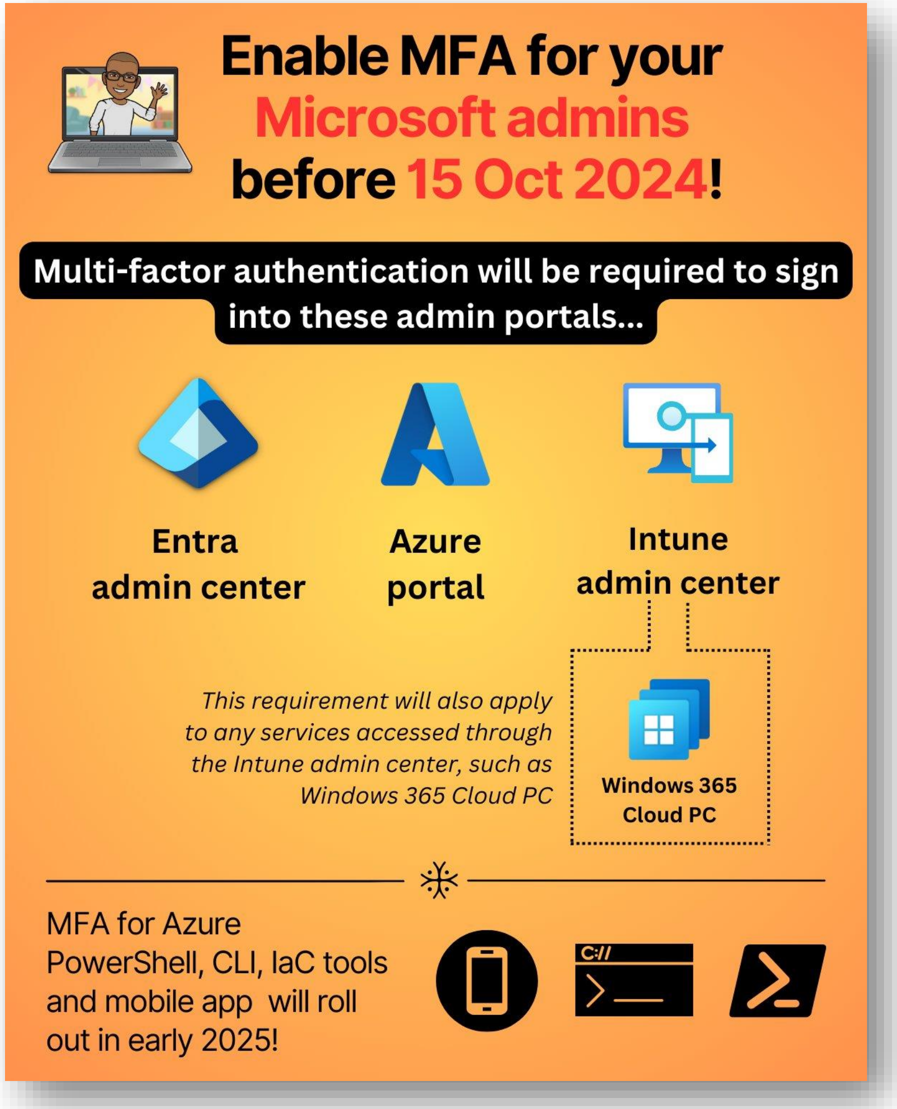
Explore the Microsoft Entra product family

Learn how unified multicloud identity and network access help you protect and verify identities, manage permissions, and enforce intelligent access policies, all in one place.

Billing

2 purchased licenses and 0 subscriptions

We are making it easier than ever view all alerts and updates related to your licenses and subscriptions.



Enable MFA for your Microsoft admins before 15 Oct 2024!

Multi-factor authentication will be required to sign into these admin portals...

Entra admin center

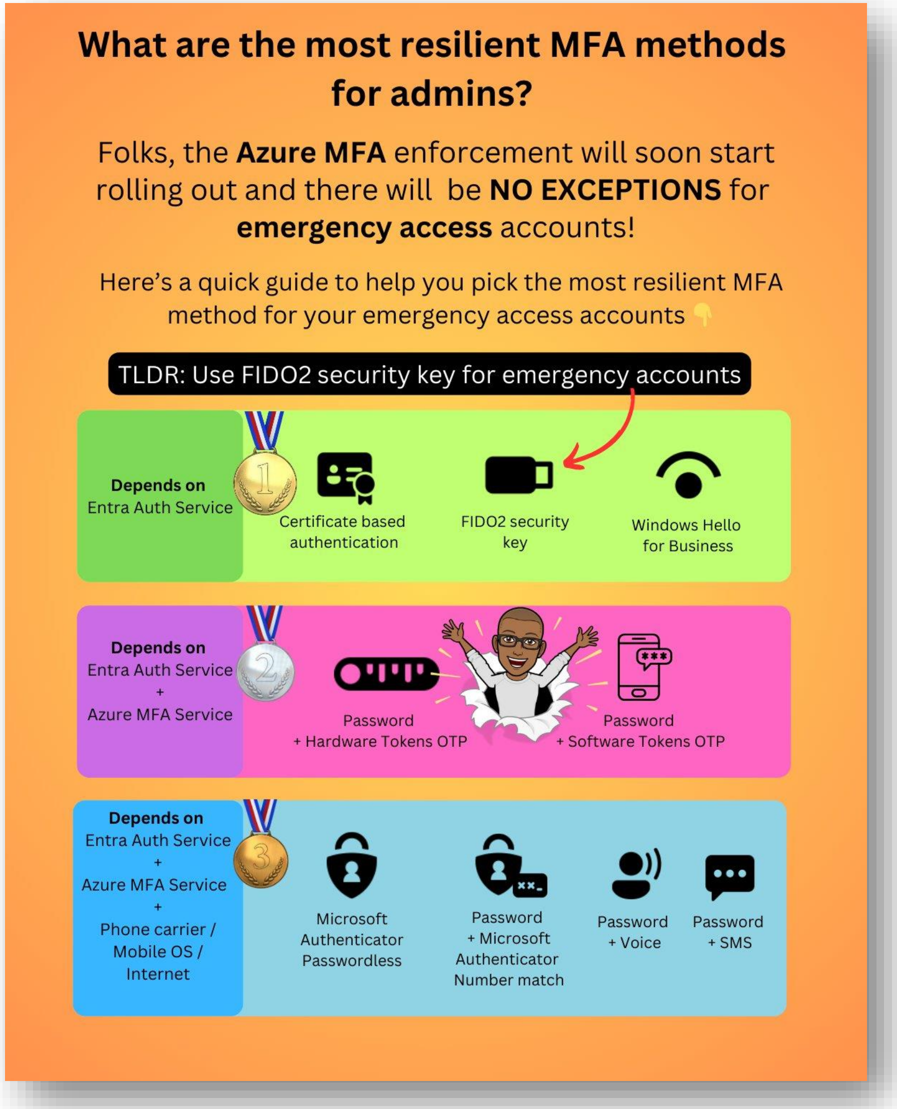
Azure portal

Intune admin center

This requirement will also apply to any services accessed through the Intune admin center, such as Windows 365 Cloud PC

Windows 365 Cloud PC

MFA for Azure PowerShell, CLI, IaC tools and mobile app will roll out in early 2025!



What are the most resilient MFA methods for admins?

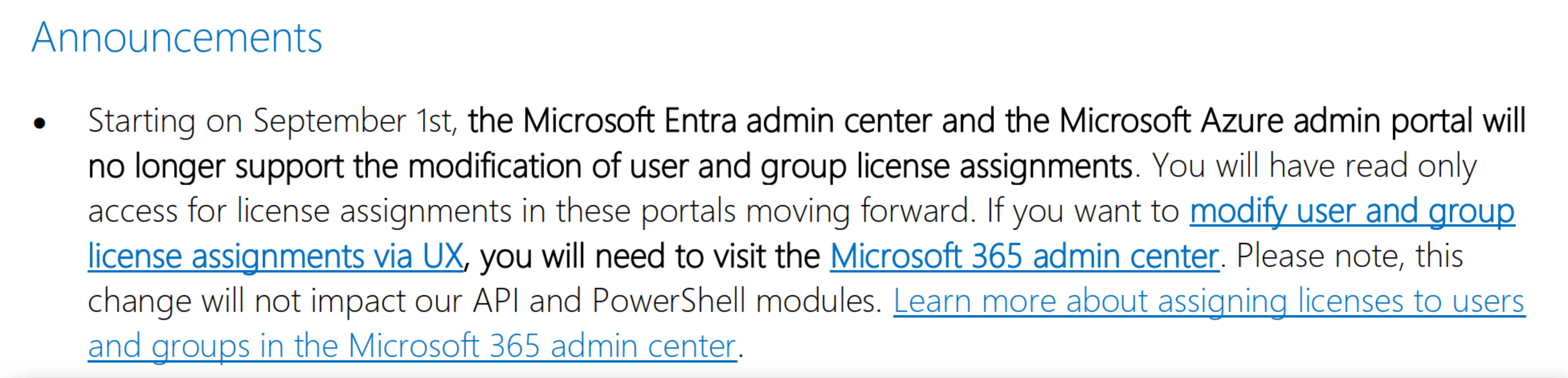
Folks, the **Azure MFA** enforcement will soon start rolling out and there will be **NO EXCEPTIONS** for **emergency access** accounts!

Here's a quick guide to help you pick the most resilient MFA method for your emergency access accounts 👇

TLDR: Use FIDO2 security key for emergency accounts

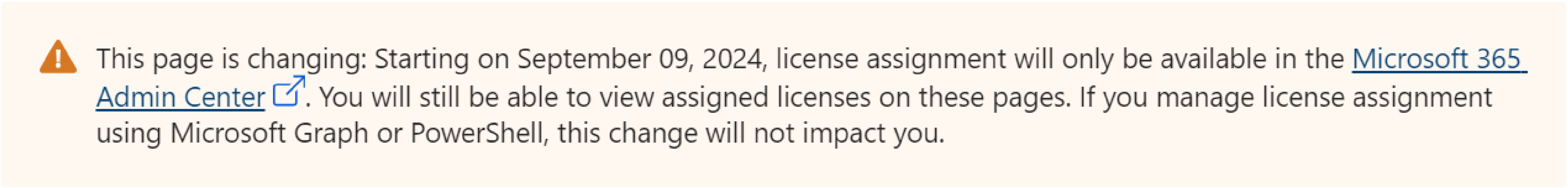
Depends on Entra Auth Service	1	Certificate based authentication FIDO2 security key Windows Hello for Business
Depends on Entra Auth Service + Azure MFA Service	2	Password + Hardware Tokens OTP Password + Software Tokens OTP
Depends on Entra Auth Service + Azure MFA Service + Phone carrier / Mobile OS / Internet	3	Microsoft Authenticator Passwordless Password + Microsoft Authenticator Number match Password + Voice Password + SMS

Group license assignments

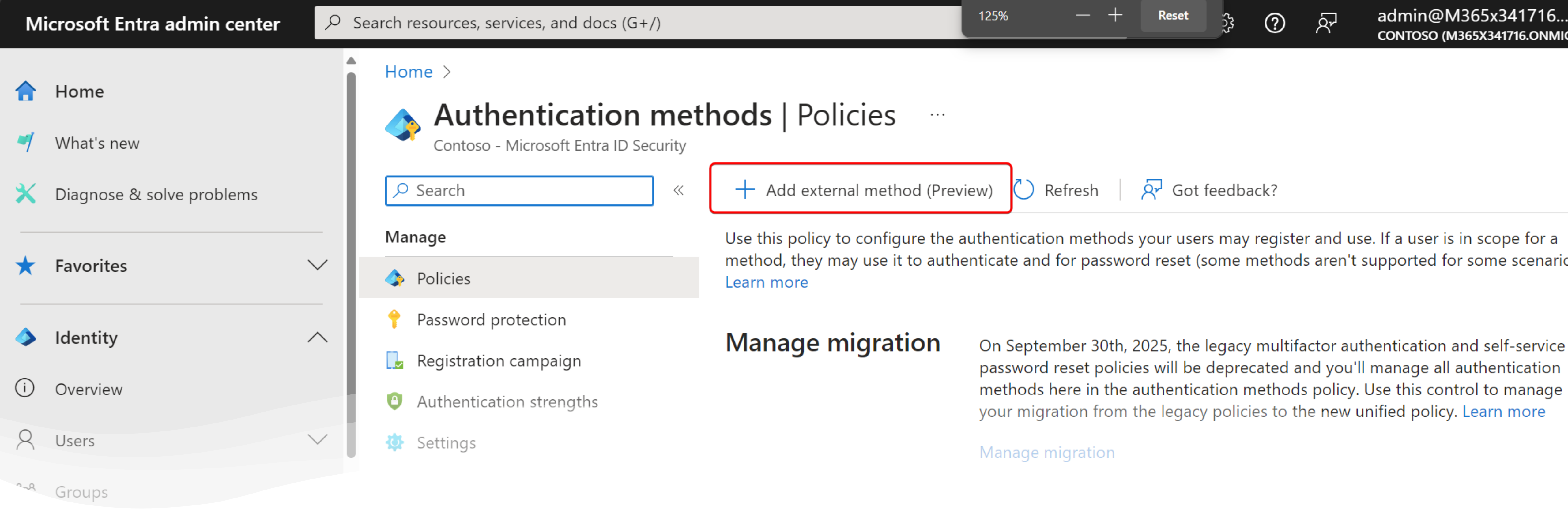


Announcements

- Starting on September 1st, **the Microsoft Entra admin center and the Microsoft Azure admin portal will no longer support the modification of user and group license assignments**. You will have read only access for license assignments in these portals moving forward. If you want to **modify user and group license assignments via UX**, **you will need to visit the Microsoft 365 admin center**. Please note, this change will not impact our API and PowerShell modules. Learn more about assigning licenses to users and groups in the Microsoft 365 admin center.



⚠ This page is changing: Starting on September 09, 2024, license assignment will only be available in the Microsoft 365 Admin Center. You will still be able to view assigned licenses on these pages. If you manage license assignment using Microsoft Graph or PowerShell, this change will not impact you.



Authentication methods | Policies

Contoso - Microsoft Entra ID Security

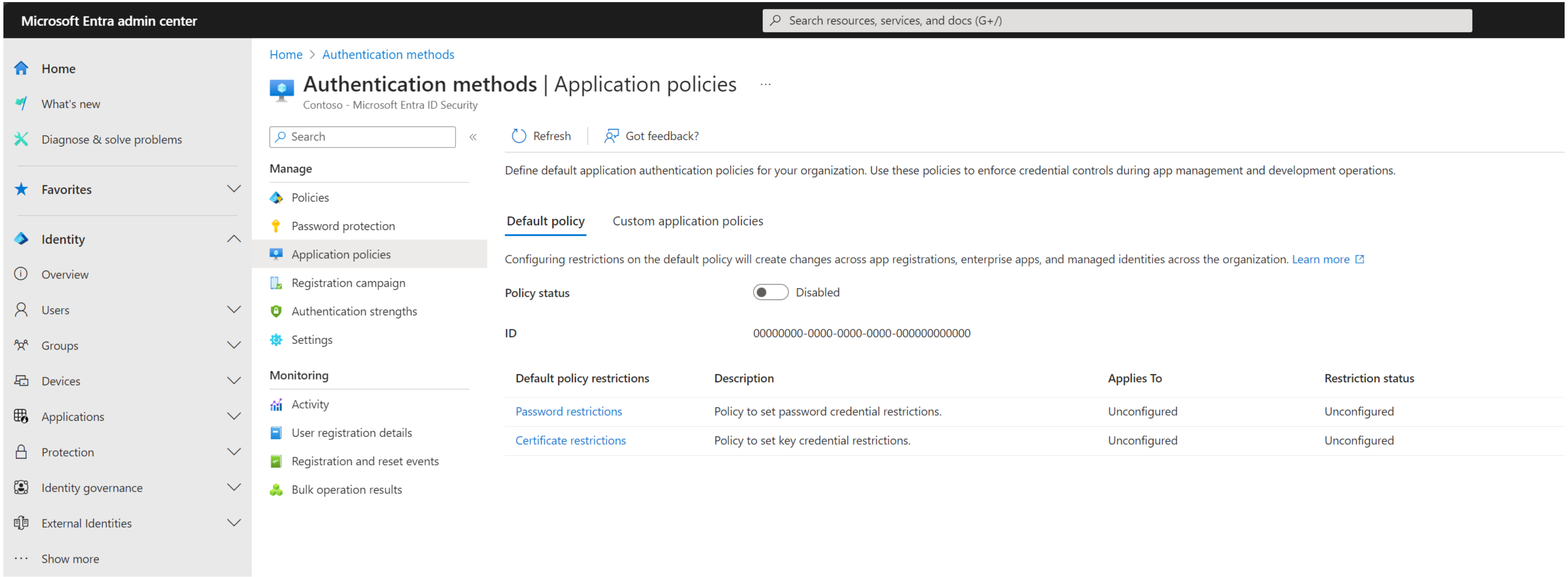
Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenario Learn more

Manage migration

On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy. Learn more

Multifactor authentication external method provider reference (Preview)

Application policies – Added to UX



Authentication methods | Application policies

Contoso - Microsoft Entra ID Security

Define default application authentication policies for your organization. Use these policies to enforce credential controls during app management and development operations.

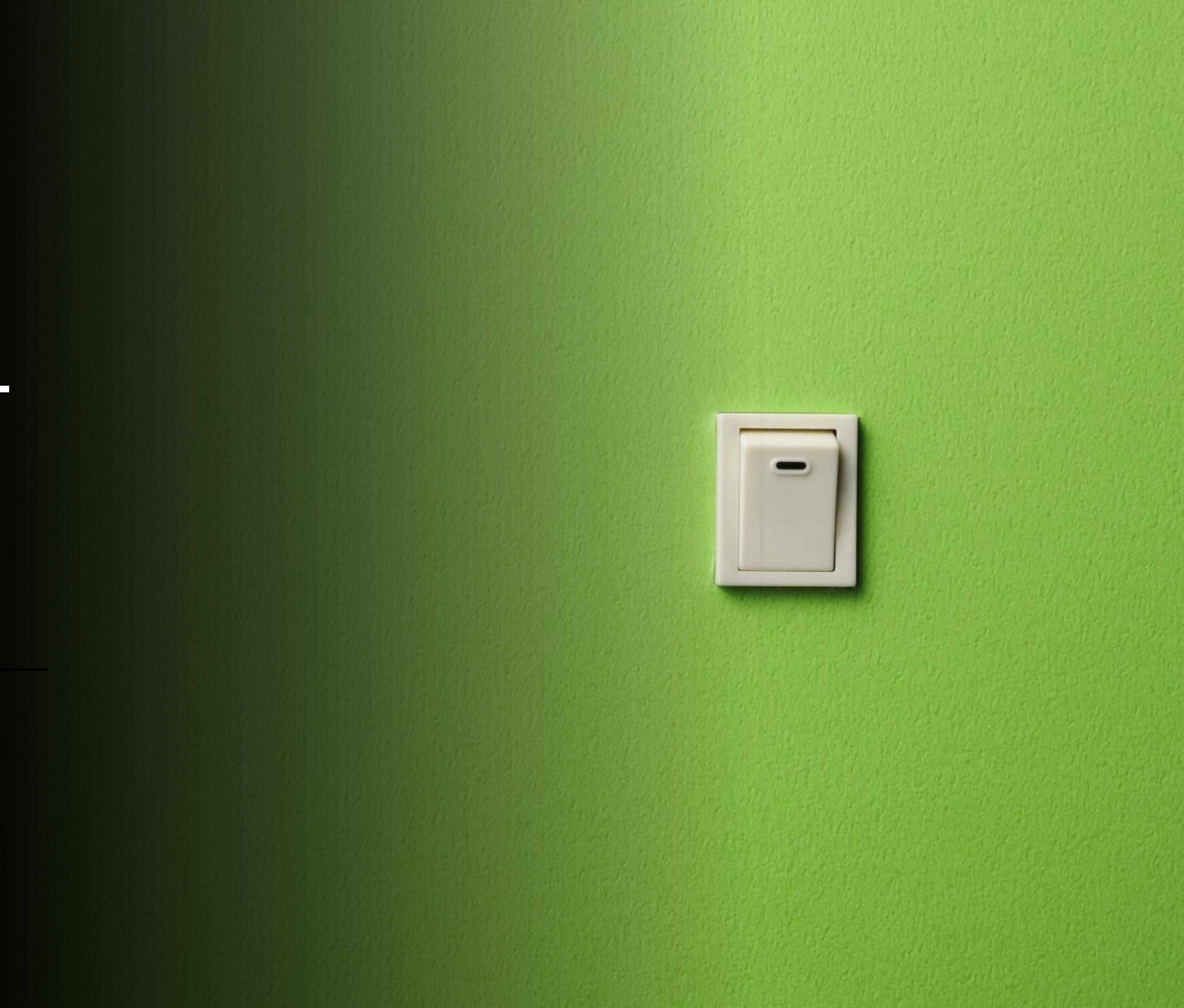
Configuring restrictions on the default policy will create changes across app registrations, enterprise apps, and managed identities across the organization. Learn more

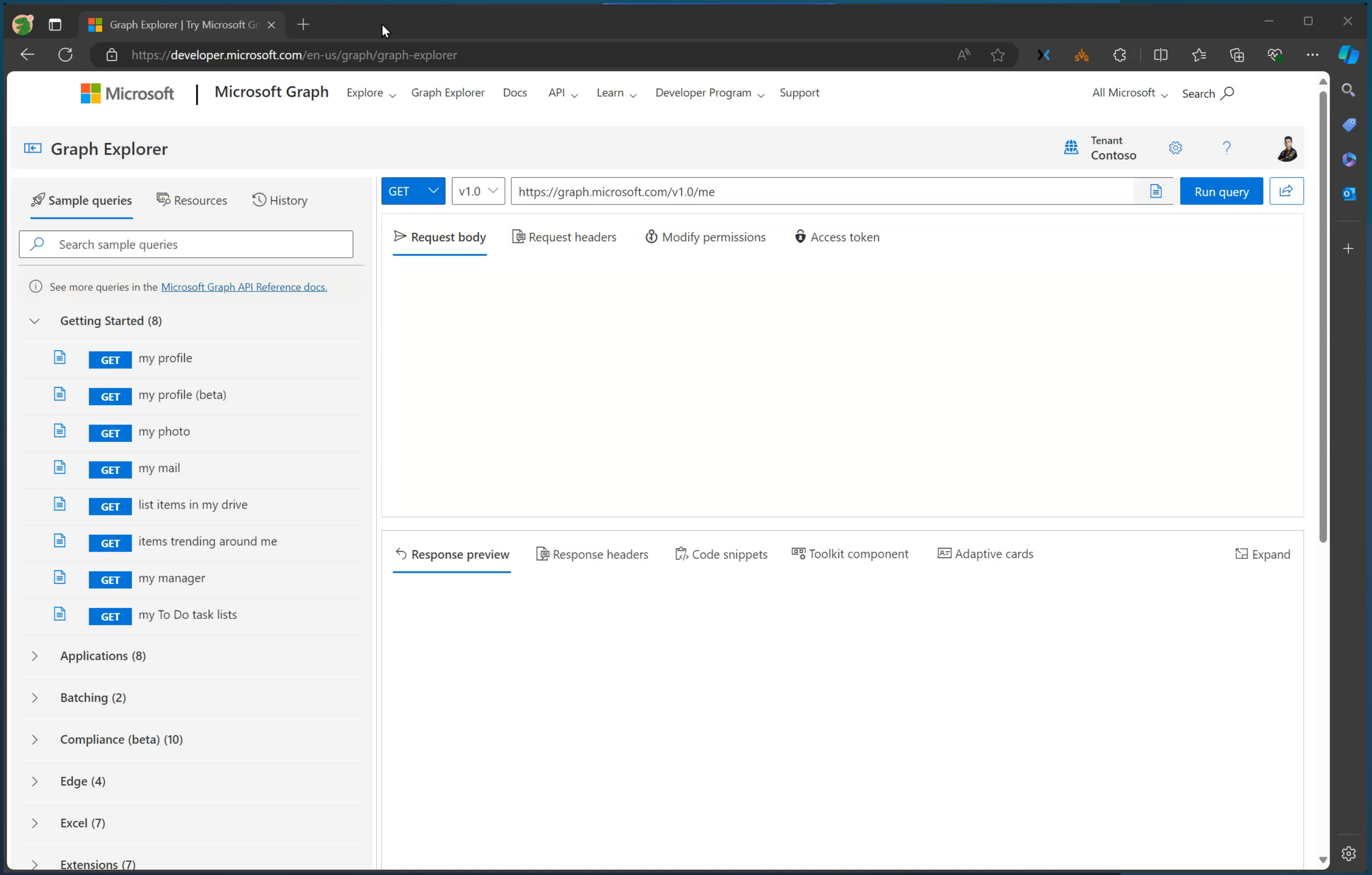
Policy status: Disabled

ID: 00000000-0000-0000-0000-000000000000

Default policy restrictions	Description	Applies To	Restriction status
Password restrictions	Policy to set password credential restrictions.	Unconfigured	Unconfigured
Certificate restrictions	Policy to set key credential restrictions.	Unconfigured	Unconfigured

Per user MFA – Graph API support





https://graph.microsoft.com/v1.0/me

See more queries in the Microsoft Graph API Reference docs.

Getting Started (8)

GET my profile

GET my profile (beta)

GET my photo

GET my mail

GET list items in my drive

GET items trending around me

GET my manager

GET my To Do task lists

Applications (8)

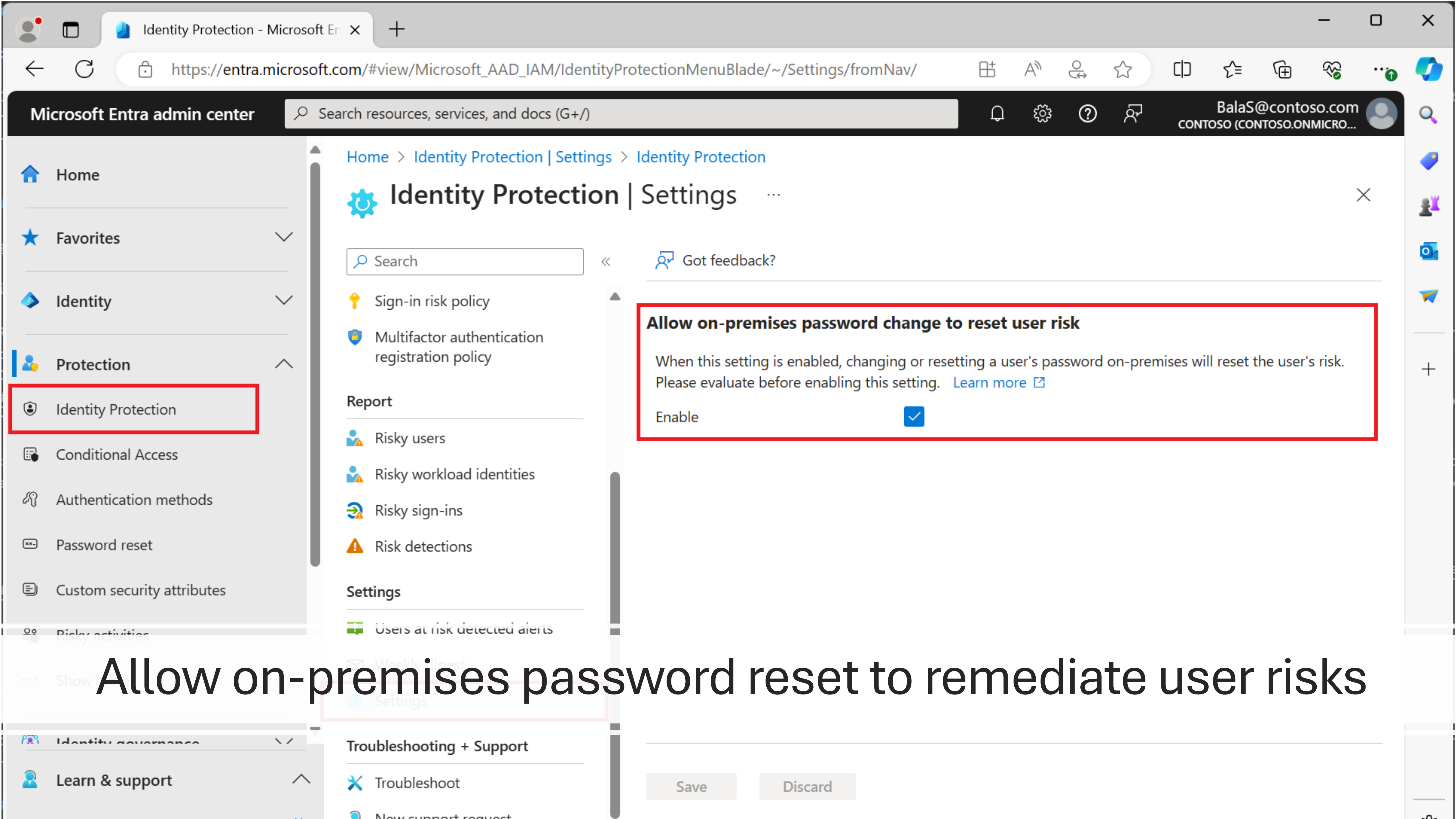
Batching (2)

Compliance (beta) (10)

Edge (4)

Excel (7)

Extensions (7)



Identity Protection - Microsoft Er

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/IdentityProtectionMenuBlade/~/Settings/fromNav/

Microsoft Entra admin center

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

BalaS@contoso.com
CONTOSO (CONTOSO.ONMICRO...

Home > Identity Protection | Settings > Identity Protection

Identity Protection | Settings

Got feedback?

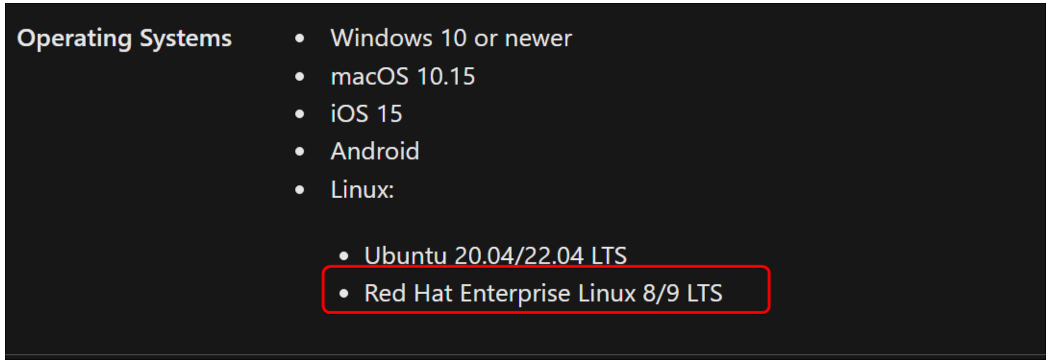
Allow on-premises password change to reset user risk

When this setting is enabled, changing or resetting a user's password on-premises will reset the user's risk. Please evaluate before enabling this setting. Learn more

Enable ☑

Allow on-premises password reset to remediate user risks

GA - Device based conditional access to M365/Azure resources on Red Hat Enterprise Linux

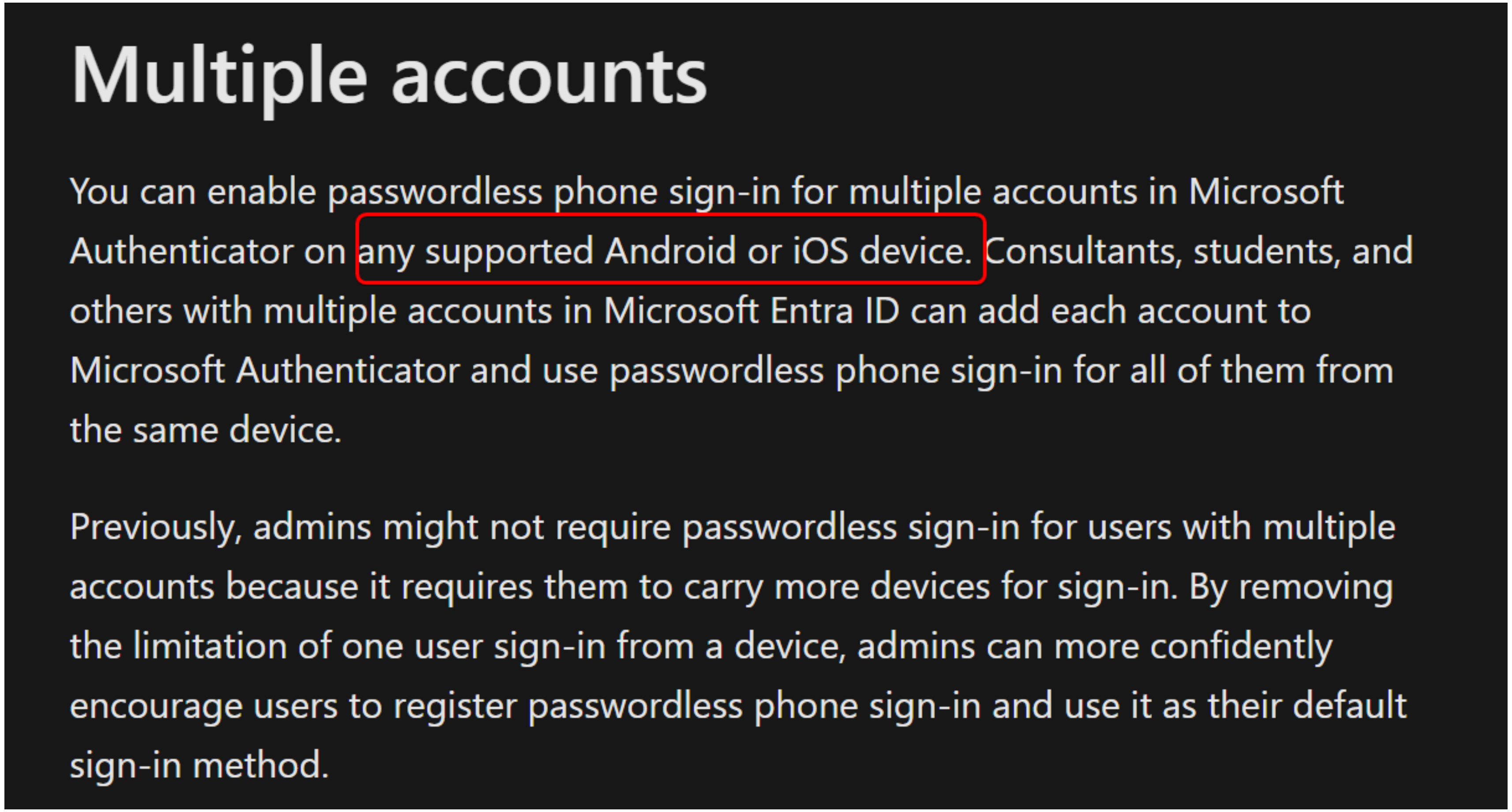


Operating Systems

- Windows 10 or newer
- macOS 10.15
- iOS 15
- Android
- Linux:
  - Ubuntu 20.04/22.04 LTS
  - Red Hat Enterprise Linux 8/9 LTS

- Entra ID registration & enrollment
- Single Sign On via Edge
- Intune Compliance policies
- Custom policies (using bash scripts)
- Support for RPM packages

Passwordless Phone Sign-in | Support for multiple accounts on Android

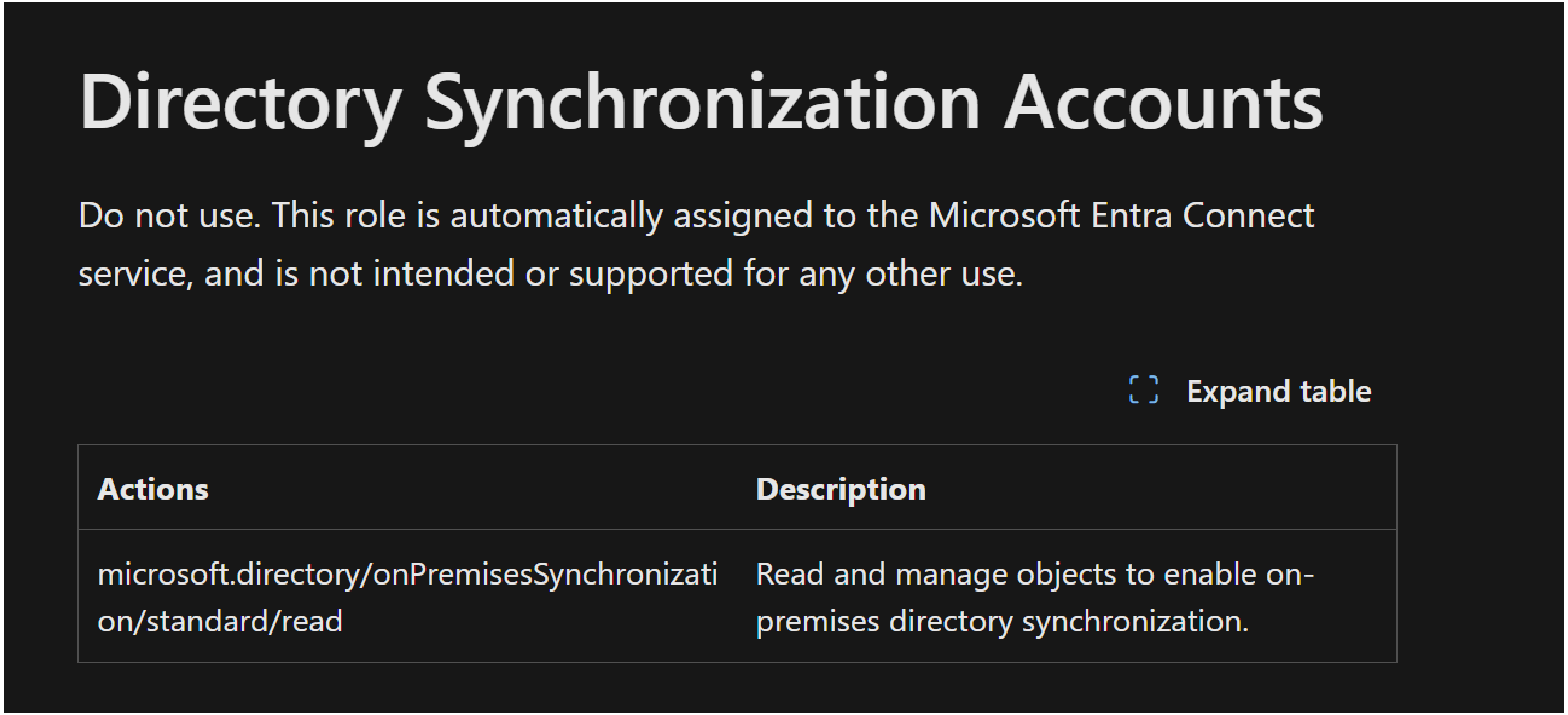


Multiple accounts

You can enable passwordless phone sign-in for multiple accounts in Microsoft Authenticator on any supported Android or iOS device. Consultants, students, and others with multiple accounts in Microsoft Entra ID can add each account to Microsoft Authenticator and use passwordless phone sign-in for all of them from the same device.

Previously, admins might not require passwordless sign-in for users with multiple accounts because it requires them to carry more devices for sign-in. By removing the limitation of one user sign-in from a device, admins can more confidently encourage users to register passwordless phone sign-in and use it as their default sign-in method.

Removed unused permissions from the privileged "Directory Synchronization Accounts" role.

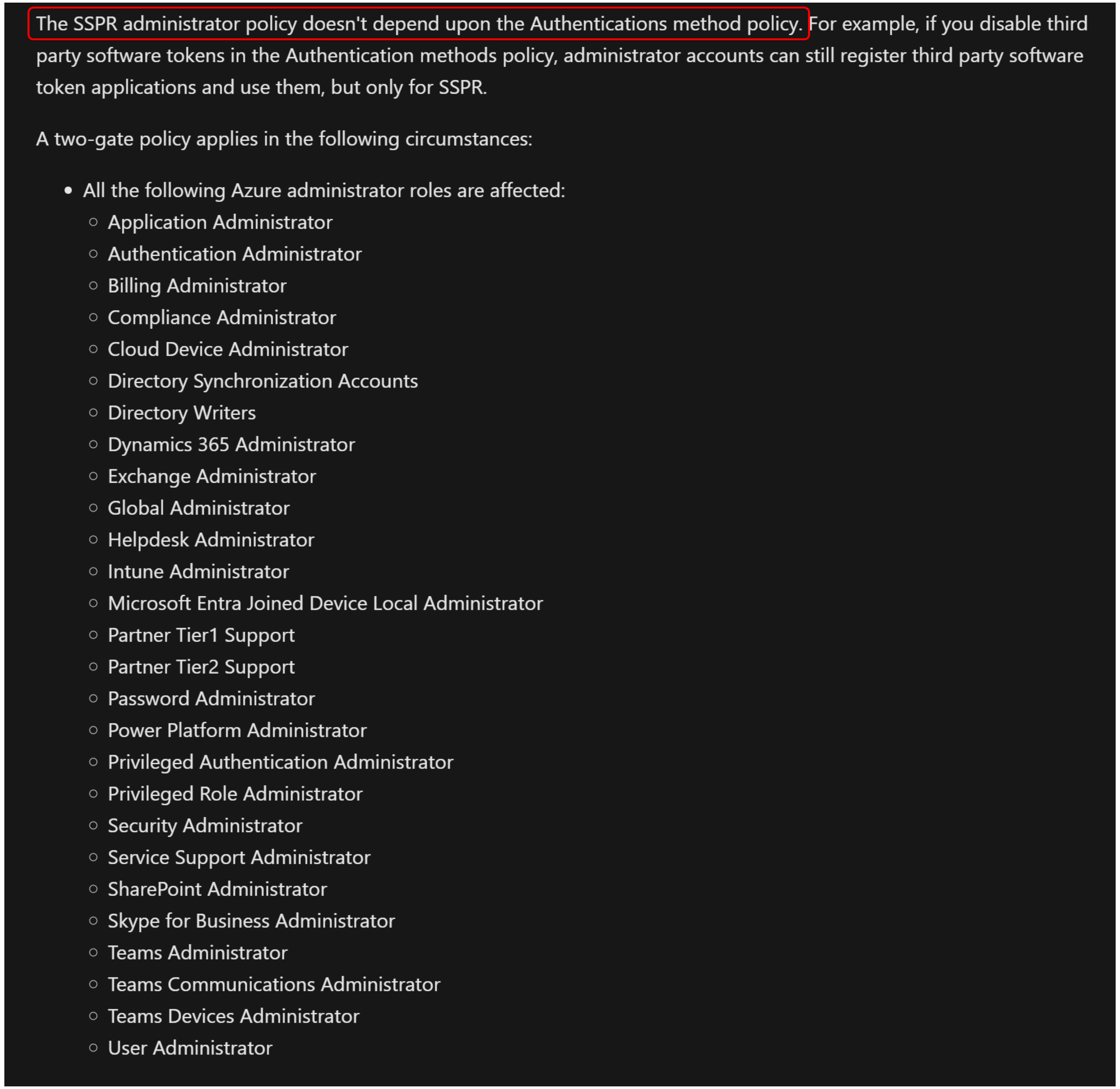


Directory Synchronization Accounts

Do not use. This role is automatically assigned to the Microsoft Entra Connect service, and is not intended or supported for any other use.

Actions	Description
microsoft.directory/onPremisesSynchronization/standard/read	Read and manage objects to enable on-premises directory synchronization.

SSPR for admins (role expansion)

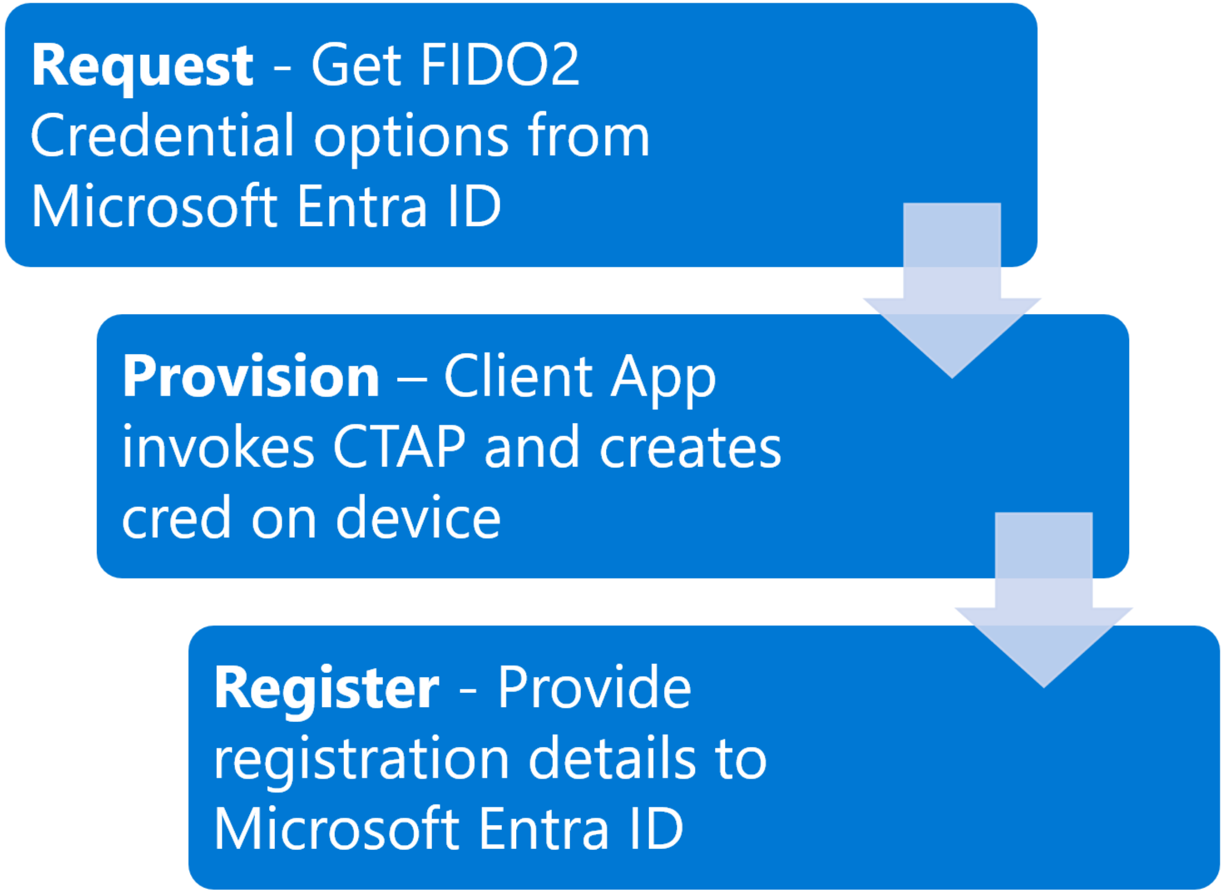


The SSPR administrator policy doesn't depend upon the Authentications method policy. For example, if you disable third party software tokens in the Authentication methods policy, administrator accounts can still register third party software token applications and use them, but only for SSPR.

A two-gate policy applies in the following circumstances:

- All the following Azure administrator roles are affected:
  - Application Administrator
  - Authentication Administrator
  - Billing Administrator
  - Compliance Administrator
  - Cloud Device Administrator
  - Directory Synchronization Accounts
  - Directory Writers
  - Dynamics 365 Administrator
  - Exchange Administrator
  - Global Administrator
  - Helpdesk Administrator
  - Intune Administrator
  - Microsoft Entra Joined Device Local Administrator
  - Partner Tier1 Support
  - Partner Tier2 Support
  - Password Administrator
  - Power Platform Administrator
  - Privileged Authentication Administrator
  - Privileged Role Administrator
  - Security Administrator
  - Service Support Administrator
  - SharePoint Administrator
  - Skype for Business Administrator
  - Teams Administrator
  - Teams Communications Administrator
  - Teams Devices Administrator
  - User Administrator

Provision FIDO2 security keys using Microsoft Graph API (preview)



Request - Get FIDO2 Credential options from Microsoft Entra ID

Provision – Client App invokes CTAP and creates cred on device

Register - Provide registration details to Microsoft Entra ID

evilginxpro

The phishing framework for red team companies

Stress test the company security against phishing to convince your clients or employers to apply more secure sign-in authentication solutions.

AiTM detection by Identity Protection

The Microsoft Security Research team uses Microsoft 365 Defender to capture the identified risk and raises the user to High risk.