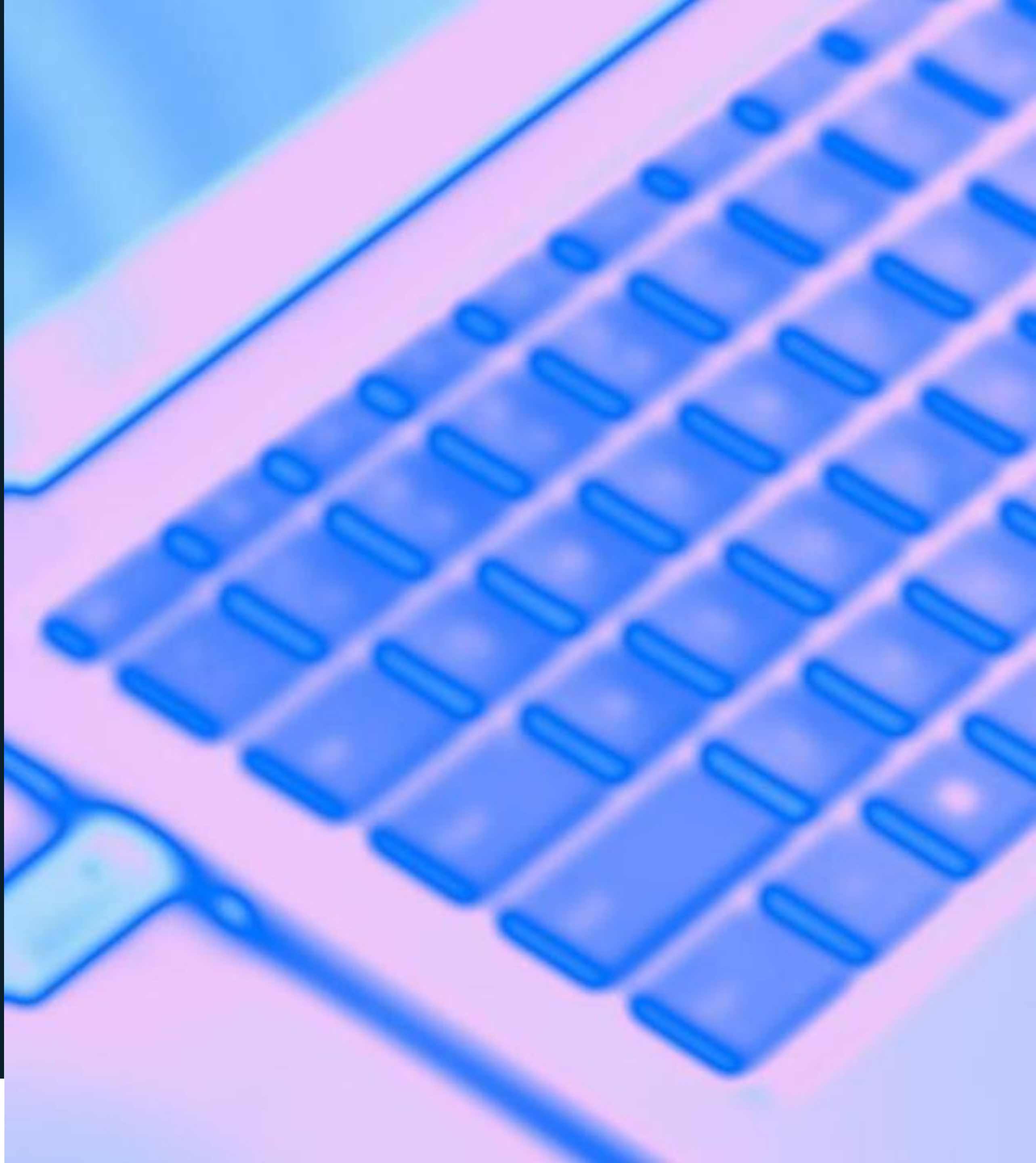
Microsoft Security

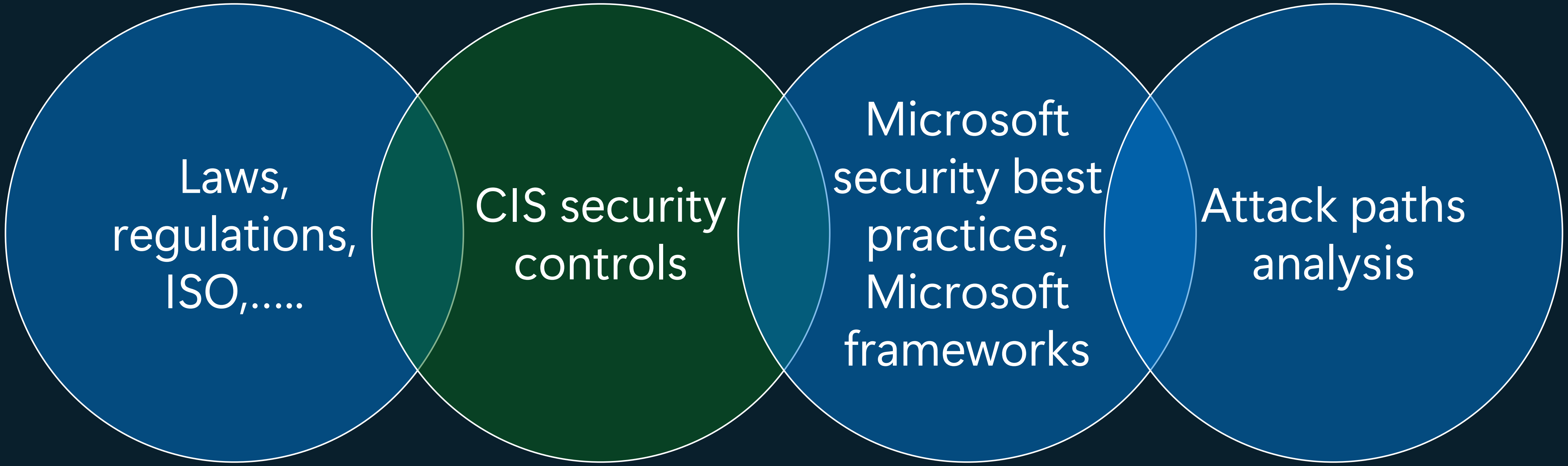
Microsoft Partner Security Day - Identity and email security

Lubomir Osmera (MCT, MCSE, CEH, CND, CEI, CARTP, CAWASP)
GOPAS
Email: lubomir@osmera.tech
https://www.gopas.cz
https://Lubomirosmera.cz
https://www.linkedin.com/in/lubomirosmera
https://hybridcloudprotection.com



ALSO ARROW TD SYNNEX GOPAS Microsoft system4u

Adopt comprehensive cybersecurity control framework



Laws, regulations, ISO,…..

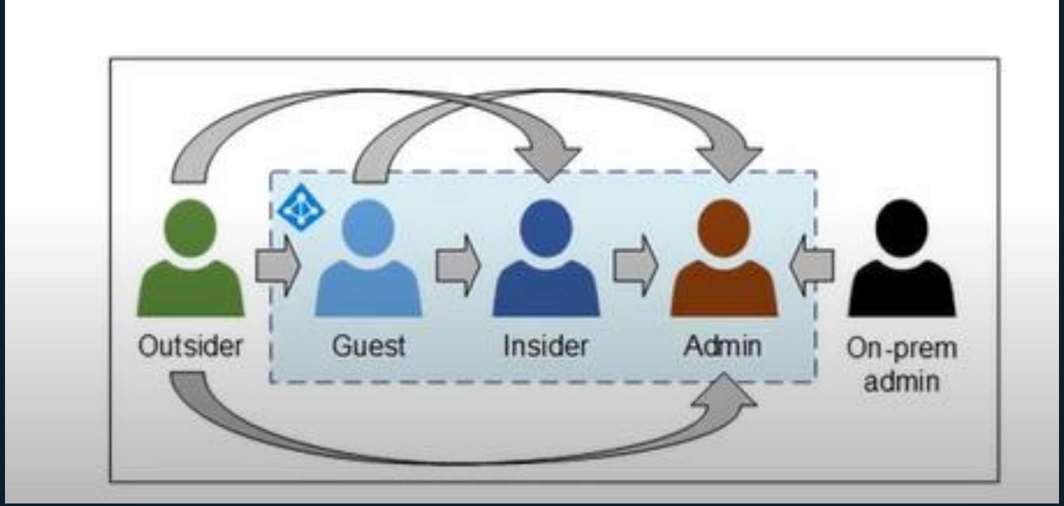
CIS security controls

Microsoft security best practices, Microsoft frameworks

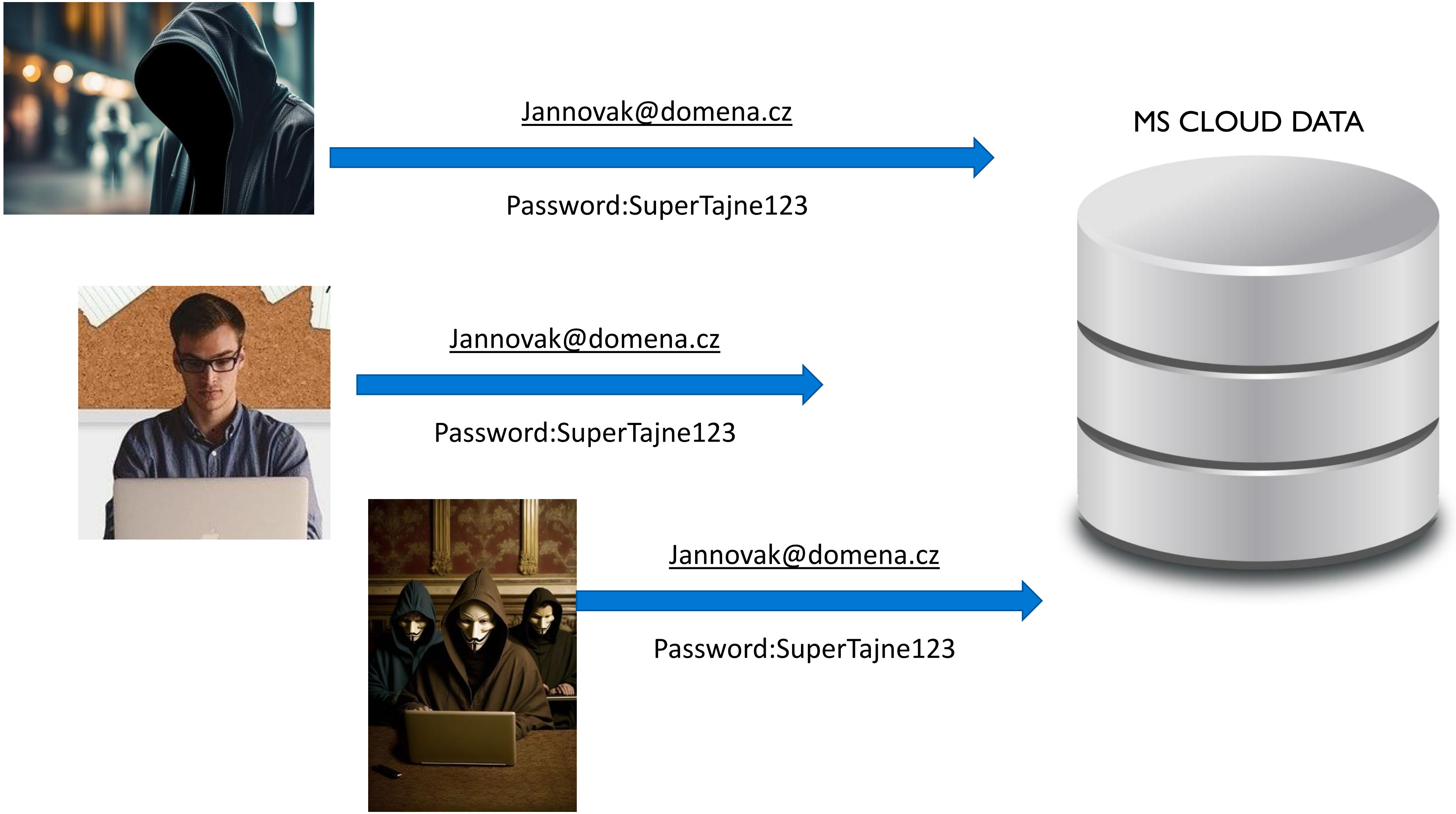
Attack paths analysis

Adopt comprehensive cybersecurity control framework

- https://www.cisecurity.org/cis-benchmarks
- https://learn.microsoft.com/en-us/security/benchmark/azure/overview
- https://microsoft.github.io/Azure-Threat-Research-Matrix/
- https://attack.mitre.org/matrices/enterprise/cloud/officesuite/



https://my.ine.com/Cloud/courses/75c31e17/azure-pentesting



MS CLOUD DATA

Jannovak@domena.cz

Password:SuperTajne123

Jannovak@domena.cz

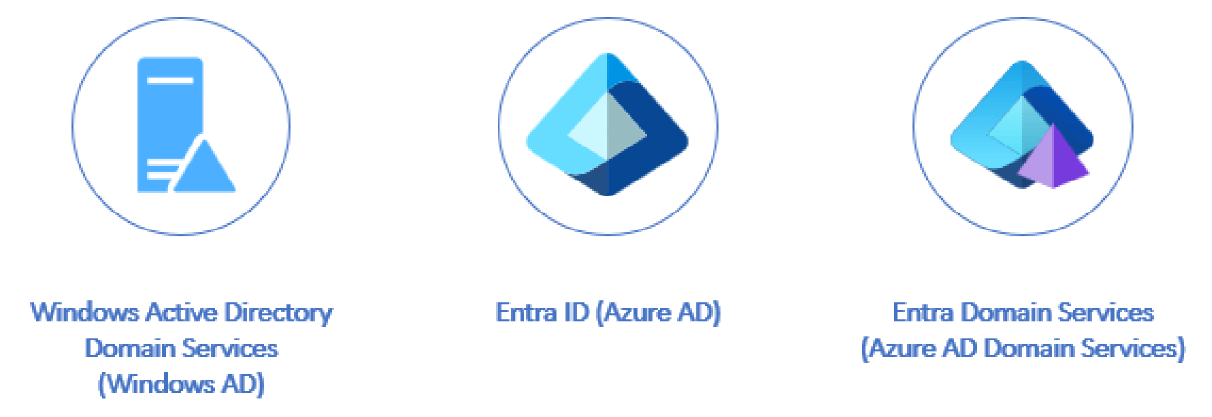
Password:SuperTajne123

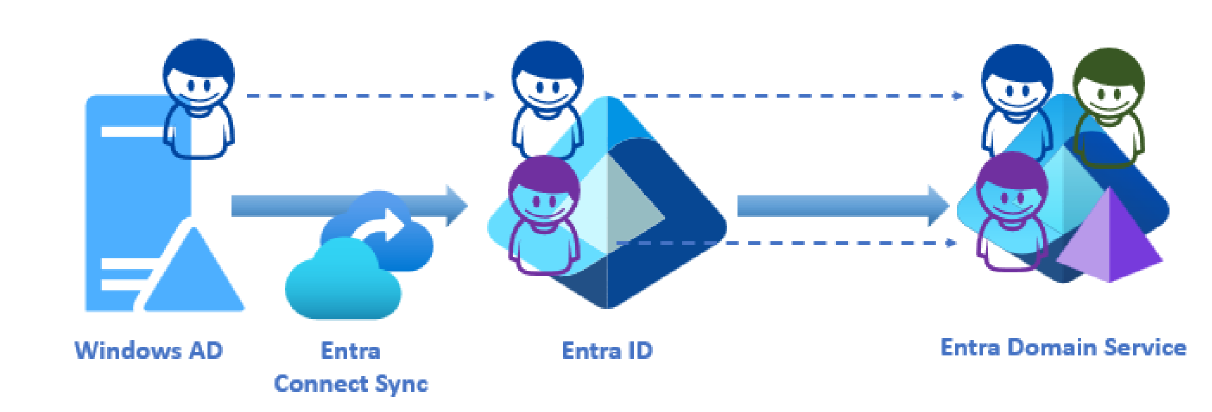
Jannovak@domena.cz

Password:SuperTajne123

Develop an identity management strategy

- Cloud-only
  - Microsoft 365 applications
  - Other Microsoft cloud integrated applications
  - Azure resources
- Hybrid environment
  - Custom onpremises resources
  - Active Directory
  - Legacy applications (NTLM, Kerberos)


Windows Active Directory Domain Services (Windows AD)
Entra ID (Azure AD)
Entra Domain Services (Azure AD Domain Services)

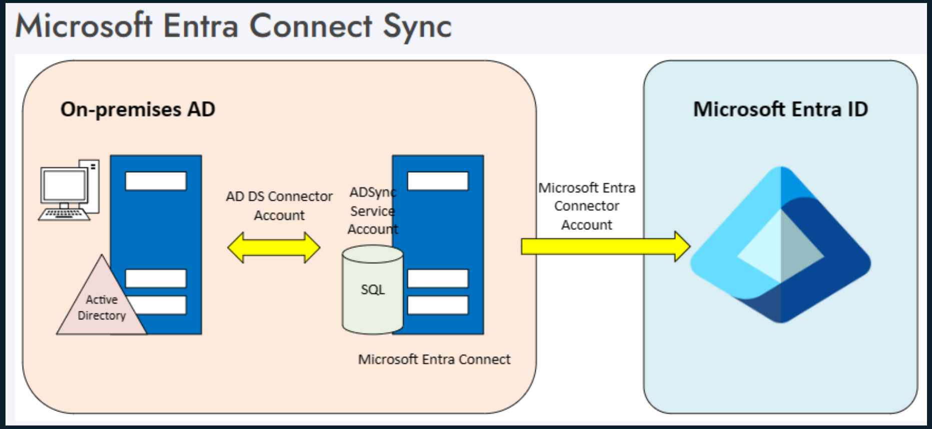


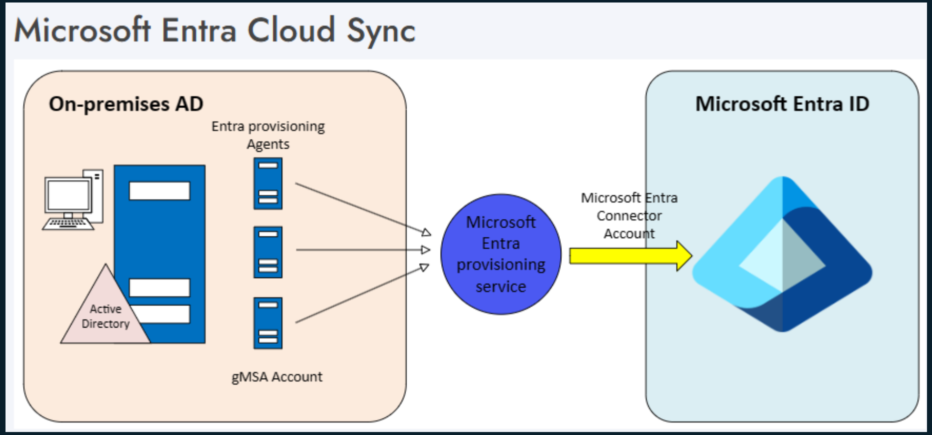
https://www.ciraltos.com/what-is-entra-id-entra-domain-services-and-windows-ad/

Hybrid environment

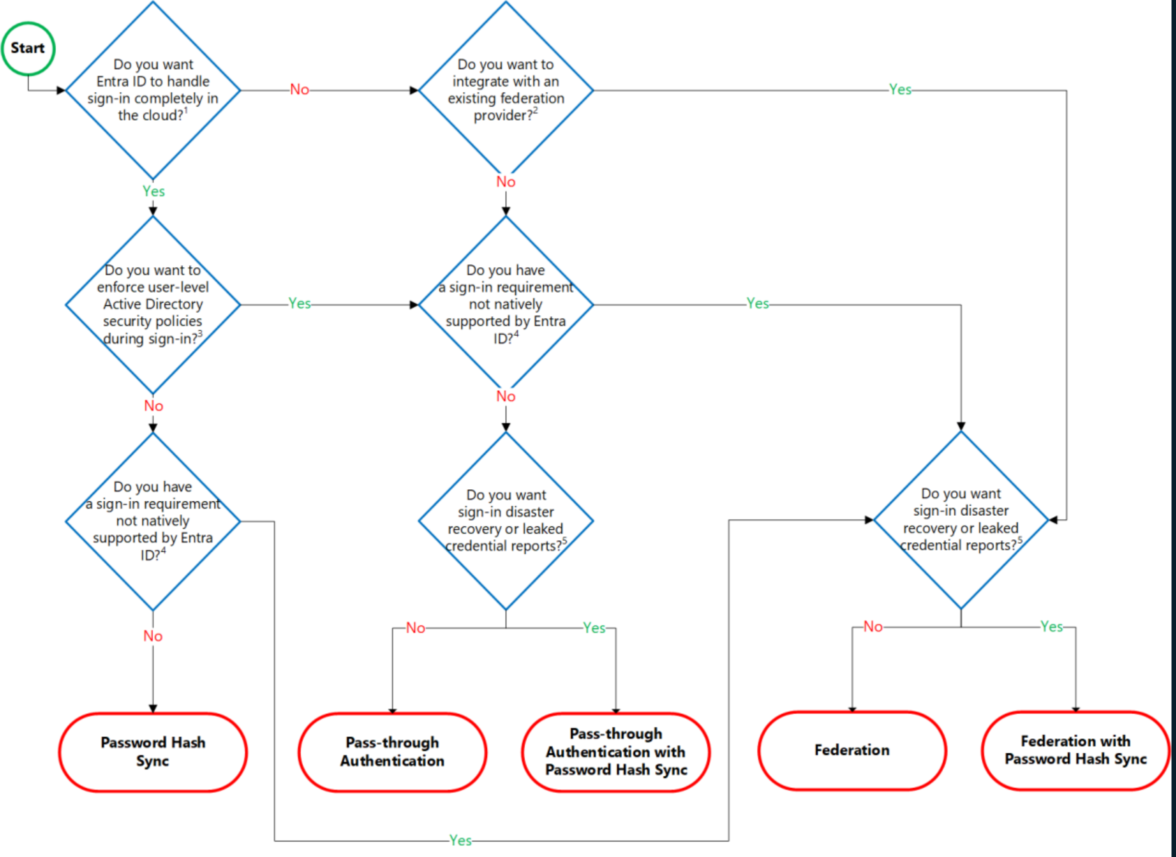
Consider sync scenario, architecture, resources

Objects (users, devices, groups)




Microsoft Entra Cloud Sync
On-premises AD
Entra provisioning Agents
Active Directory
gMSA Account
Microsoft Entra provisioning service
Microsoft Entra Connector Account
Microsoft Entra ID

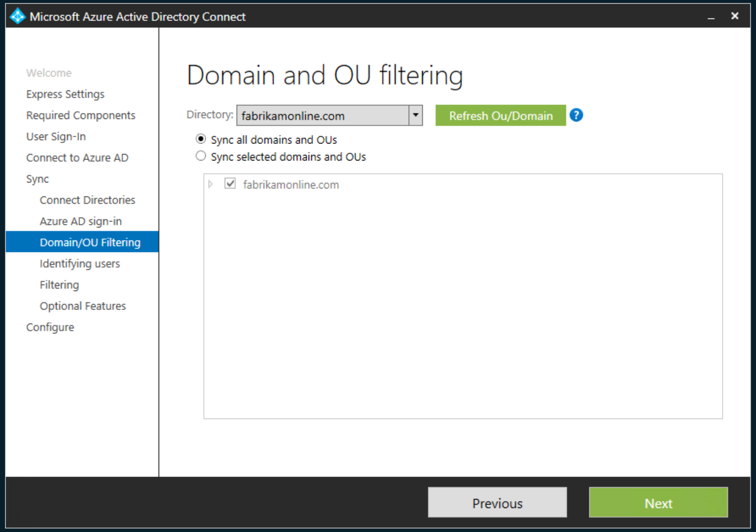
Authentication method:


Start
Do you want Entra ID to handle sign-in completely in the cloud?1
No
Yes
Do you want to integrate with an existing federation provider?2
Yes
No
Do you want to enforce user-level Active Directory security policies during sign-in?3
Yes
No
Do you have a sign-in requirement not natively supported by Entra ID?4
Yes
No
Do you have a sign-in requirement not natively supported by Entra ID?4
No
Yes
Do you want sign-in disaster recovery or leaked credential reports?5
No
Yes
Do you want sign-in disaster recovery or leaked credential reports?5
No
Yes
Password Hash Sync
Pass-through Authentication
Pass-through Authentication with Password Hash Sync
Federation
Federation with Password Hash Sync

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-whatis
https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-install-custom
https://tierzerosecurity.co.nz/2024/05/21/ms-entra-connect-sync-mothods.html
https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync#how-is-microsoft-entra-cloud-sync-different-from-microsoft-entra-connect-sync

Hybrid environment

Sync **only users who consume services** from Microsoft cloud!



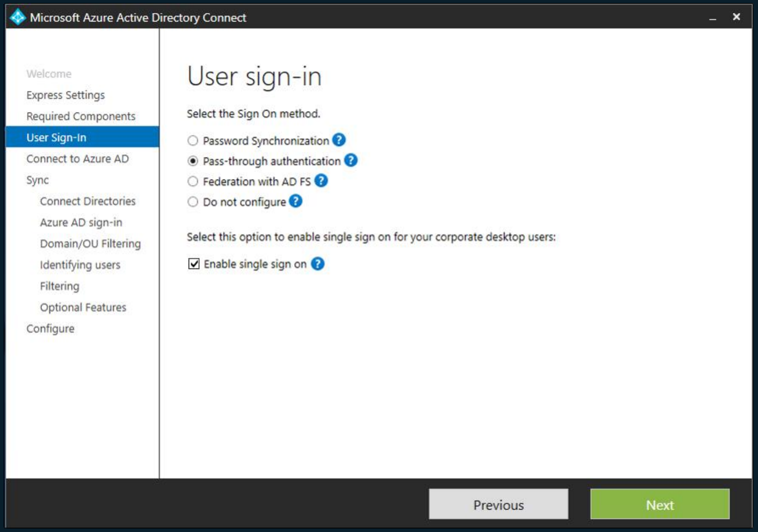
Domain and OU filtering

Directory: fabrikamonline.com

● Sync all domains and OUs
○ Sync selected domains and OUs

☑ fabrikamonline.com

Method, SSO



User sign-in

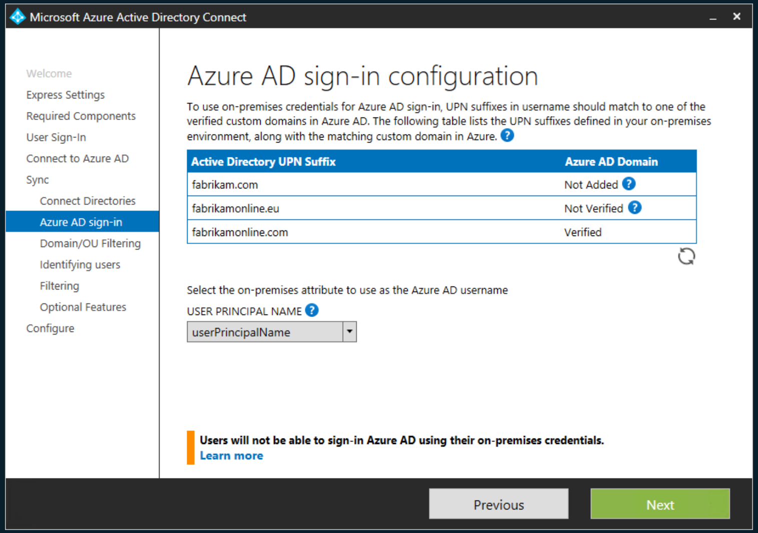
Select the Sign On method.

○ Password Synchronization
● Pass-through authentication
○ Federation with AD FS
○ Do not configure

Select this option to enable single sign on for your corporate desktop users:

☑ Enable single sign on

On-premises attribute for Microsoft Entra ID username



Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes in username should match to one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

Active Directory UPN Suffix	Azure AD Domain
fabrikam.com	Not Added
fabrikamonline.eu	Not Verified
fabrikamonline.com	Verified

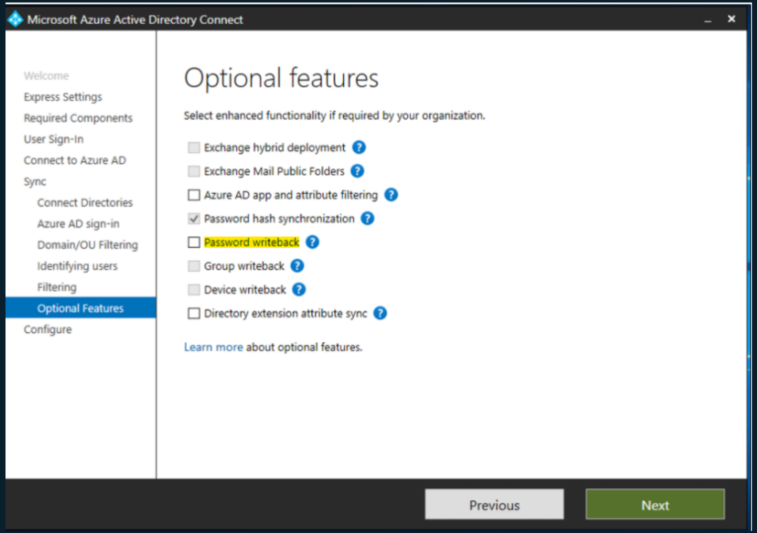
Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME

userPrincipalName

Users will not be able to sign-in Azure AD using their on-premises credentials.
Learn more

Microsoft Entra ID Connect - Password writeback



Optional features

Select enhanced functionality if required by your organization.

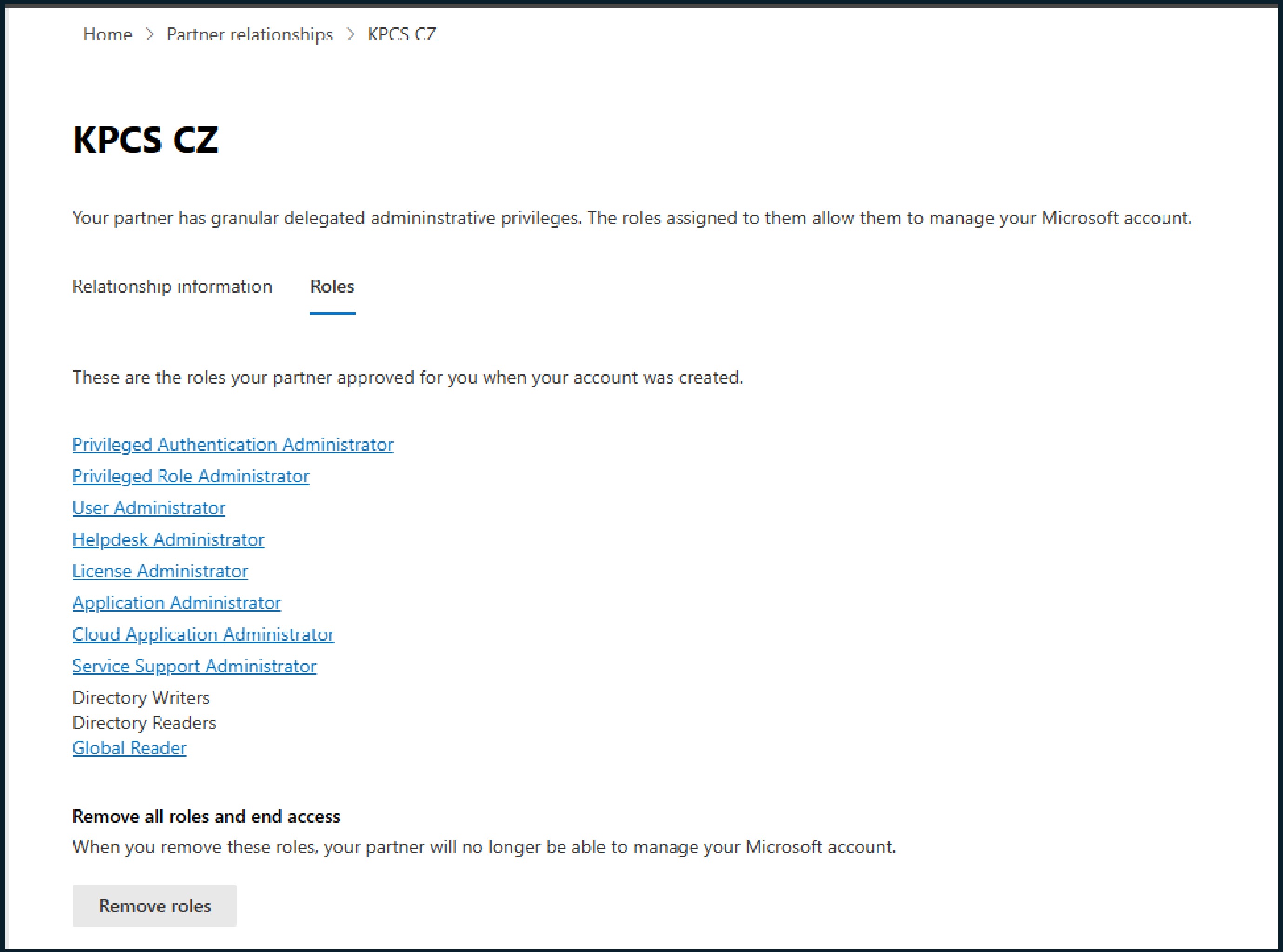
□ Exchange hybrid deployment
□ Exchange Mail Public Folders
□ Azure AD app and attribute filtering
☑ Password hash synchronization
□ Password writeback
□ Group writeback
□ Device writeback
□ Directory extension attribute sync

Learn more about optional features.

Prepare domains

- Which domain you plan to use in cloud?
- Do you have .local or non-routable domain?
- https://learn.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide

GDAP and roles



KPCS CZ

Your partner has granular delegated admininstrative privileges. The roles assigned to them allow them to manage your Microsoft account.

These are the roles your partner approved for you when your account was created.

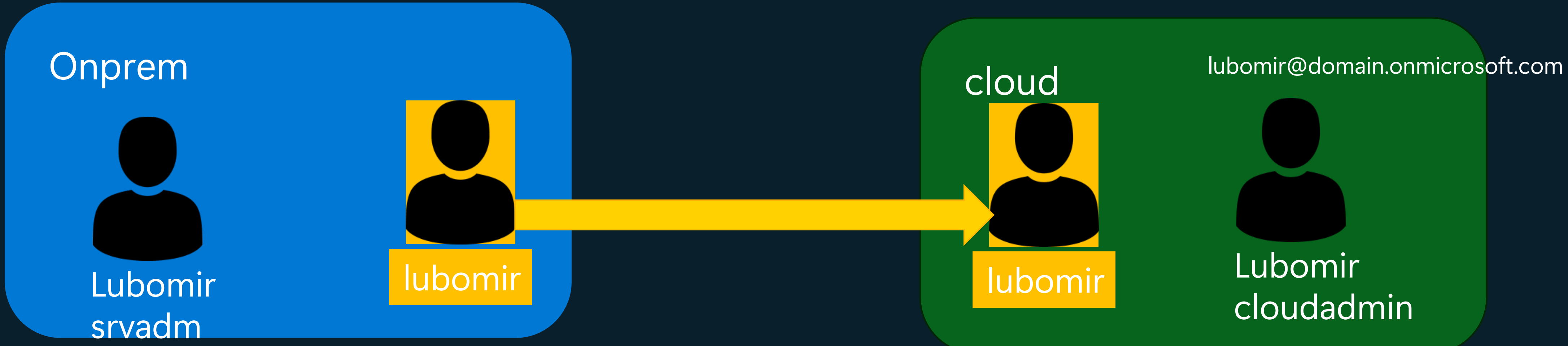
Privileged Authentication Administrator
Privileged Role Administrator
User Administrator
Helpdesk Administrator
License Administrator
Application Administrator
Cloud Application Administrator
Service Support Administrator
Directory Writers
Directory Readers
Global Reader

Remove all roles and end access

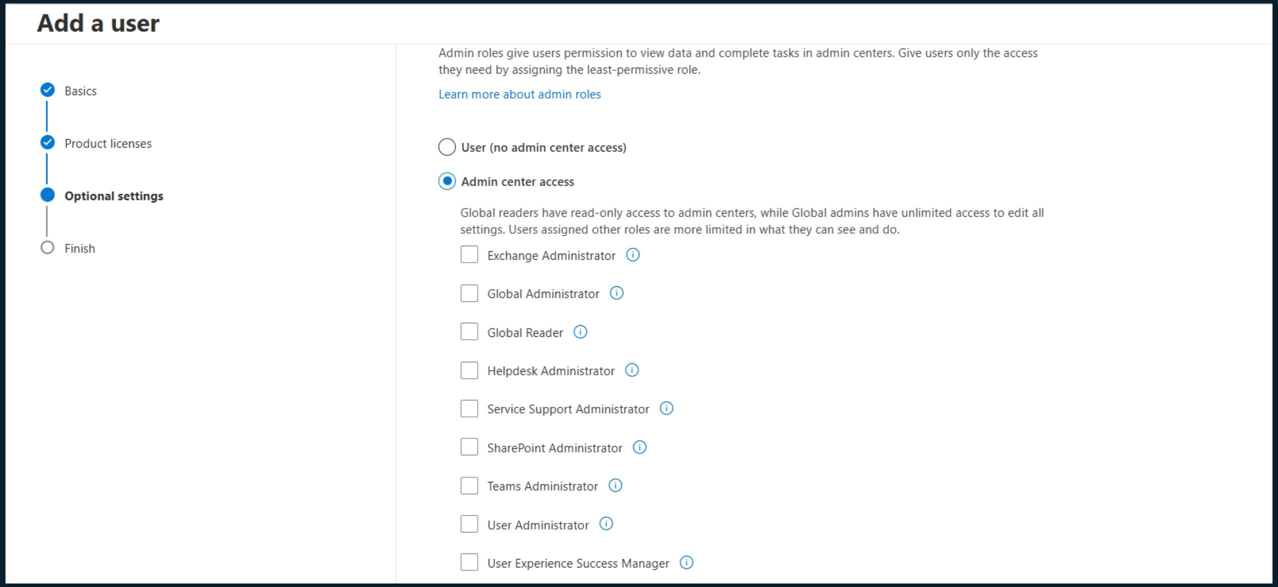
When you remove these roles, your partner will no longer be able to manage your Microsoft account.

Admin accounts

- Least privilege according *individual job function*
- Limit the number of global admins
- Admin accounts: create separate, unlicensed administrative user IDs in the onmicrosoft.com domain.



RBAC, configuration



Add a user

- ✓ Basics
- ✓ Product licenses
- ● **Optional settings**
- ○ Finish

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.

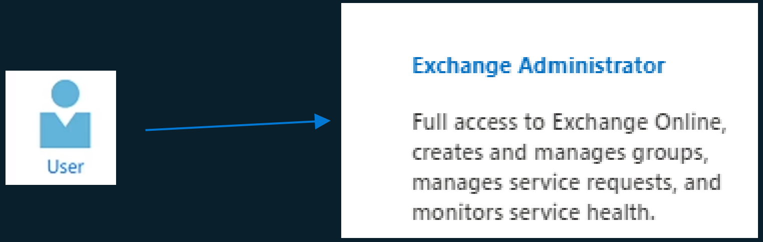
Learn more about admin roles

○ User (no admin center access)

● Admin center access

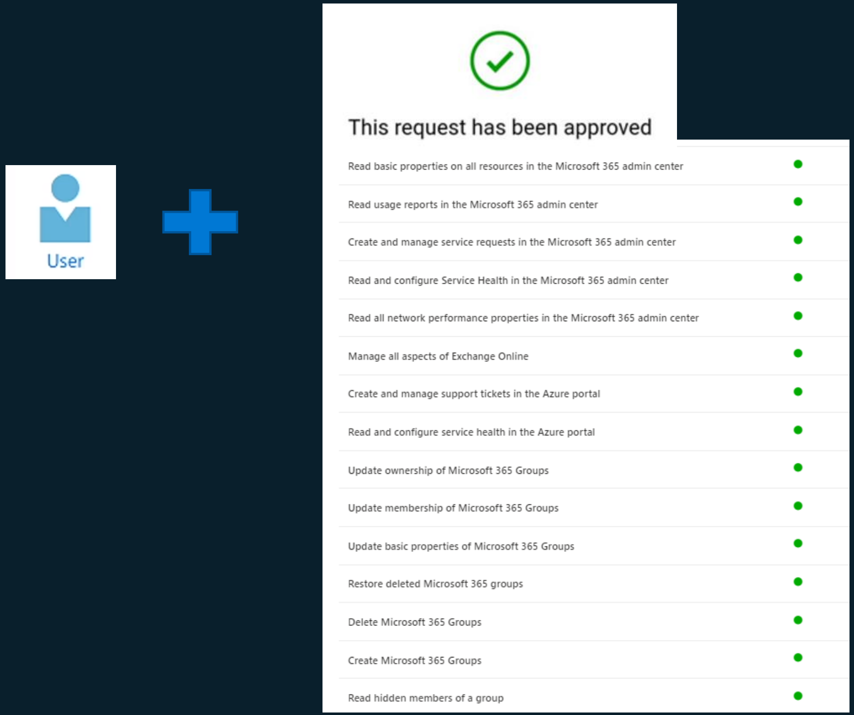
Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

- □ Exchange Administrator ⓘ
- □ Global Administrator ⓘ
- □ Global Reader ⓘ
- □ Helpdesk Administrator ⓘ
- □ Service Support Administrator ⓘ
- □ SharePoint Administrator ⓘ
- □ Teams Administrator ⓘ
- □ User Administrator ⓘ
- □ User Experience Success Manager ⓘ



Exchange Administrator

Full access to Exchange Online, creates and manages groups, manages service requests, and monitors service health.



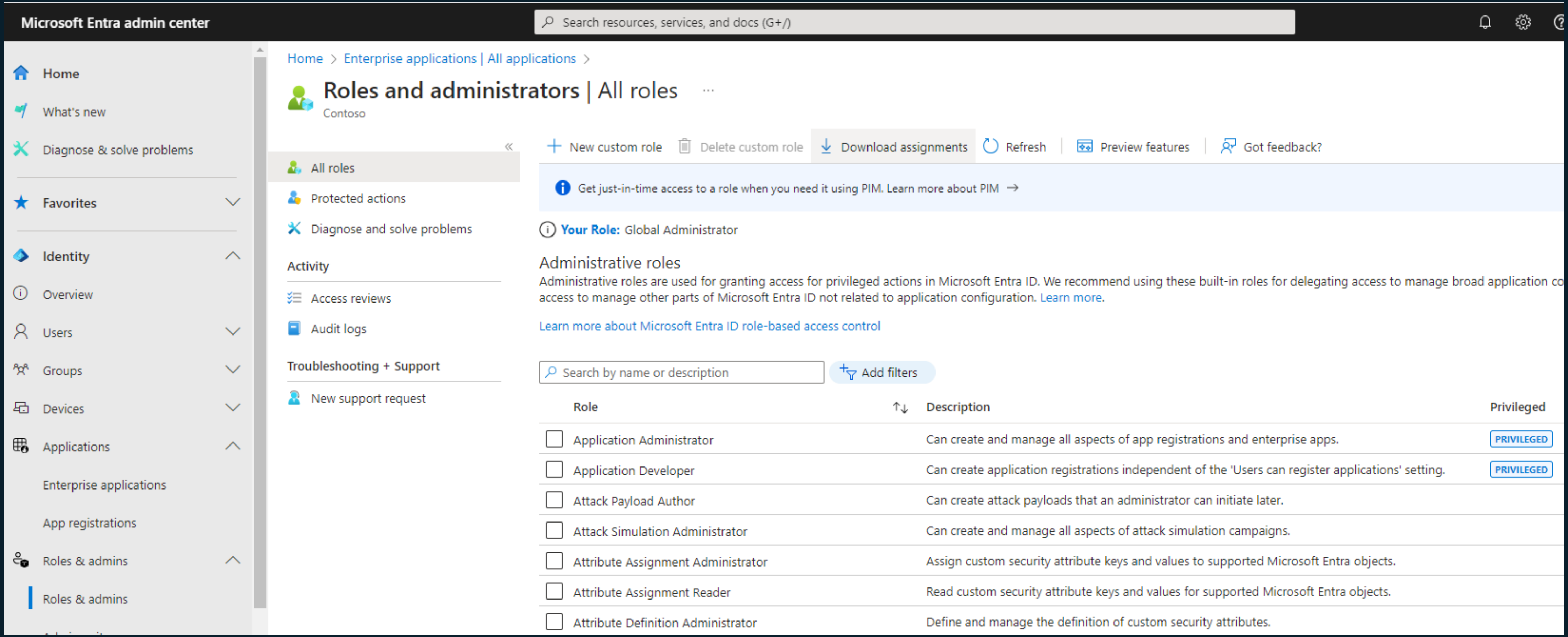
This request has been approved

- Read basic properties on all resources in the Microsoft 365 admin center ●
- Read usage reports in the Microsoft 365 admin center ●
- Create and manage service requests in the Microsoft 365 admin center ●
- Read and configure Service Health in the Microsoft 365 admin center ●
- Read all network performance properties in the Microsoft 365 admin center ●
- Manage all aspects of Exchange Online ●
- Create and manage support tickets in the Azure portal ●
- Read and configure service health in the Azure portal ●
- Update ownership of Microsoft 365 Groups ●
- Update membership of Microsoft 365 Groups ●
- Update basic properties of Microsoft 365 Groups ●
- Restore deleted Microsoft 365 groups ●
- Delete Microsoft 365 Groups ●
- Create Microsoft 365 Groups ●
- Read hidden members of a group ●

RBAC roles

Name	UPN	ROLES
Lubomir Junior ADM	junior_adm@domain.com	User Administrator License Administrator Global Reader
Jan Security ADM	Security_adm@domain.com	Application Administrator Security Administrator Compliance Administrator
Jan Intune ADM	Intune_adm@domain.com	Intune Administrator
Katerina Kratka ADM	kratka_adm@domain.com	Exchange admin Sharepoint admin Teams admin
Lubomir Osmera	Osmera_adm	Global administrator

Download assignment list



Roles and administrators | All roles

Contoso

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

Your Role: Global Administrator

Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application co access to manage other parts of Microsoft Entra ID not related to application configuration. Learn more.

Learn more about Microsoft Entra ID role-based access control

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

Portals

- Cmd.ms
- Msportals.io
- Admin.Microsoft.com
- Portal.azure.com
- Entra.Microsoft.com

Domain registrations

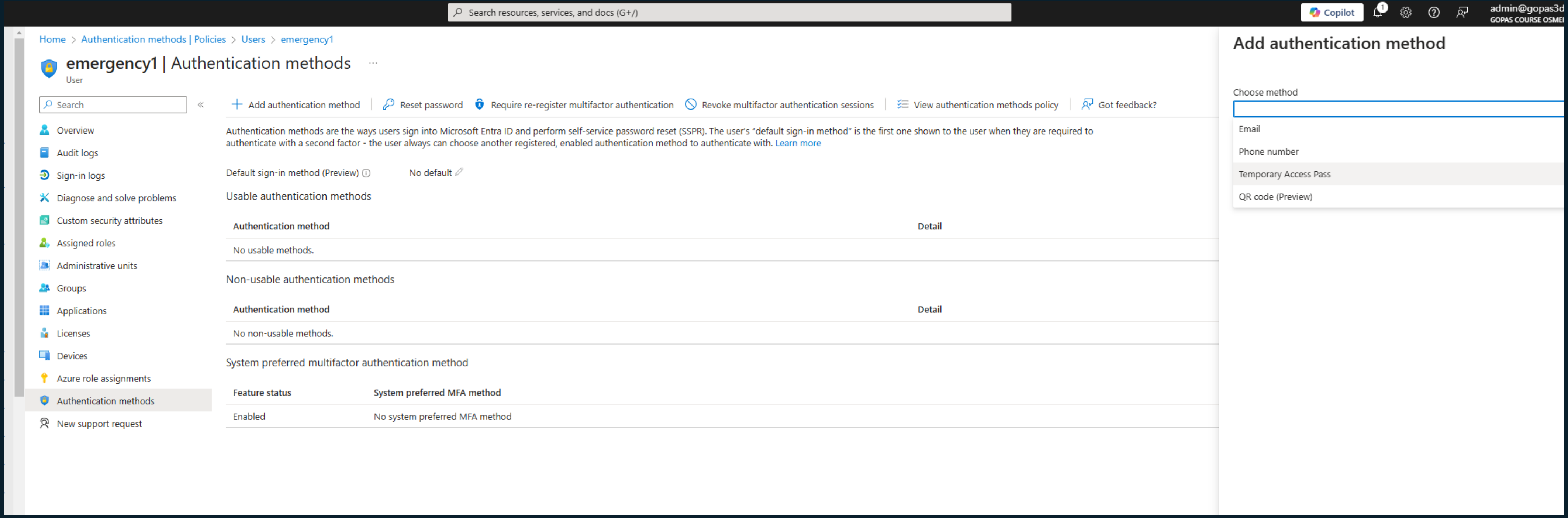
- UPN
- Email addresses
- Devices
- Application (rather custom URL than myapplicion.azurewebsites.net)

Emergency account

- https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access
- demo

demo

- Create account
- Assign global admin   (adminn portal)
- Generate tap
- Register youbico (aka.ms/mfasetup)


Search resources, services, and docs (G+/)
Copilot
admin@gopas3d
GOPAS COURSE OSME
Home > Authentication methods | Policies > Users > emergency1
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request
+ Add authentication method
Reset password
Require re-register multifactor authentication
Revoke multifactor authentication sessions
View authentication methods policy
Got feedback?

emergency1 | Authentication methods

User

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) ⓘ   No default

Usable authentication methods

Authentication method	Detail
No usable methods.	

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	No system preferred MFA method

Add authentication method

Choose method

- Email
- Phone number
- Temporary Access Pass
- QR code (Preview)

Develop a Device Management Strategy

- MAM, MDM for mobile devices (next session)
- Access to applications from company owned vs BYOD devices

NIS 2 IMPLEMENTATION: “

a) zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných obdobných technických aktiv, popřípadě i bezpečnostní opatření spojená s využitím technických aktiv, která povinná osoba nemá ve své správě”

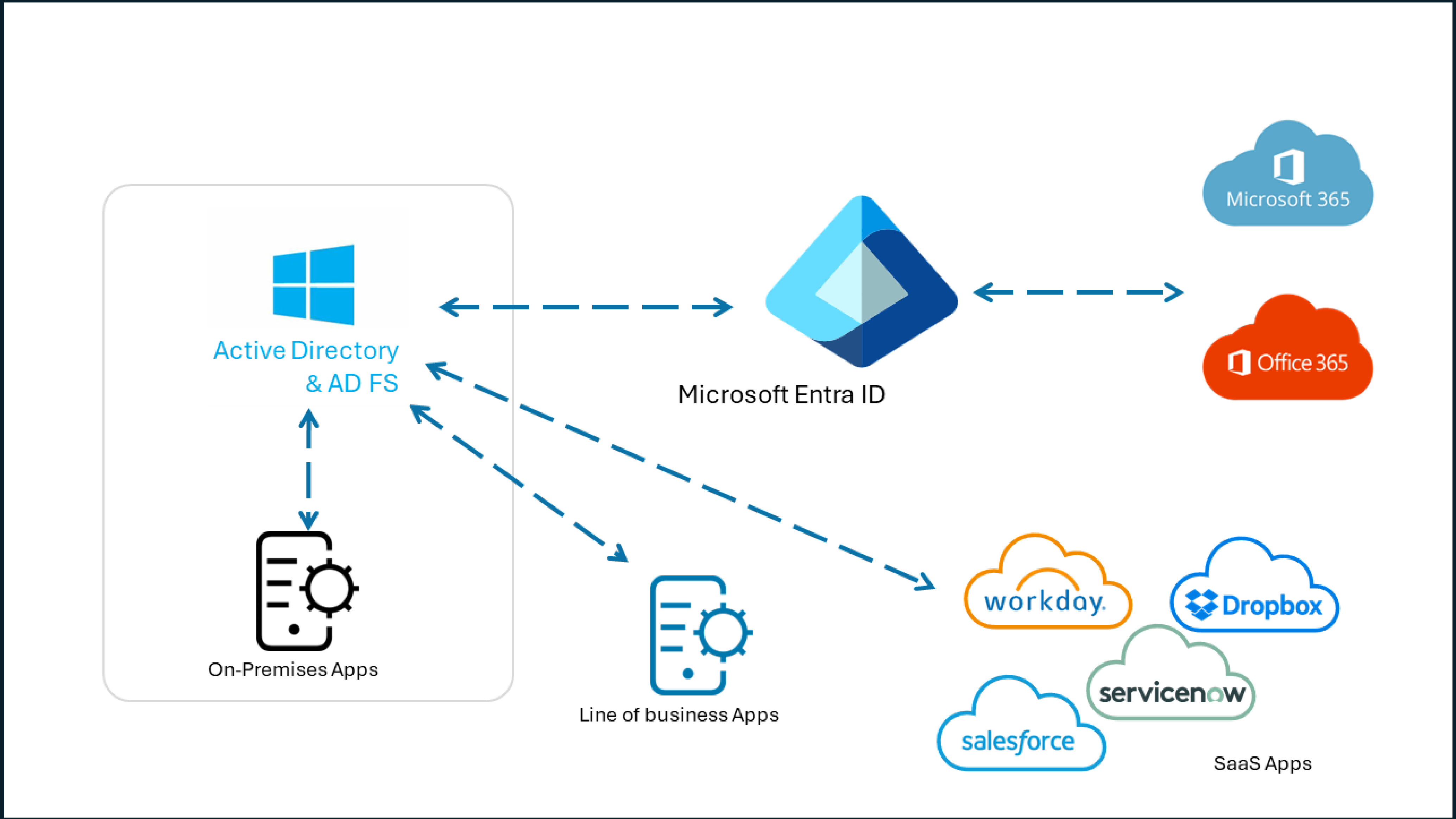
Develop a Licensing Plan

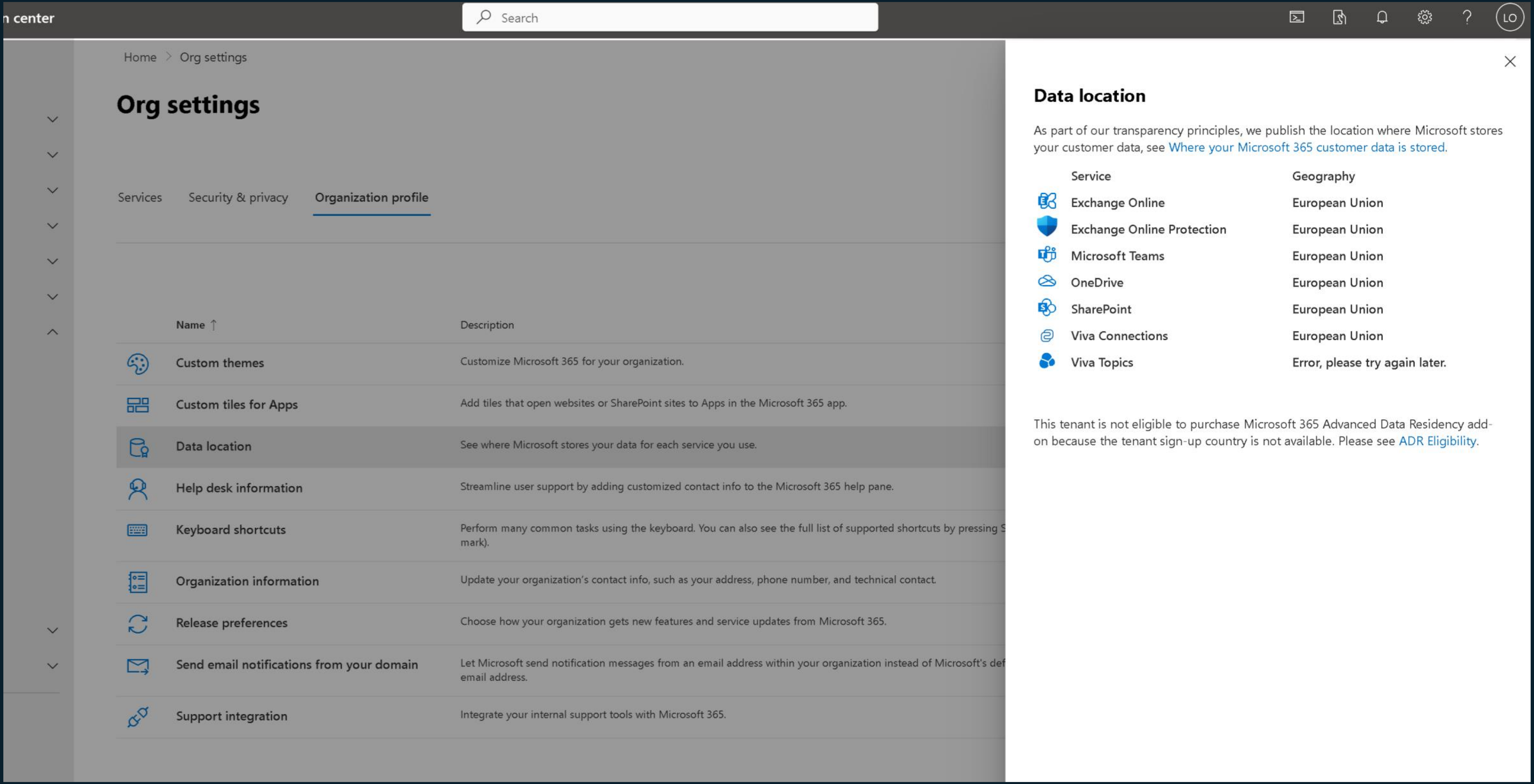
- Business premium contains advanced security components:
  - Defender for Business (endpoint security)
  - Defender for Office 365 (advanced email and office 365 apps security)
  - Entra Premium P1 (advanced identity security)

Microsoft Security

Tenant configuration, identity security

Entra importance and role





Org settings

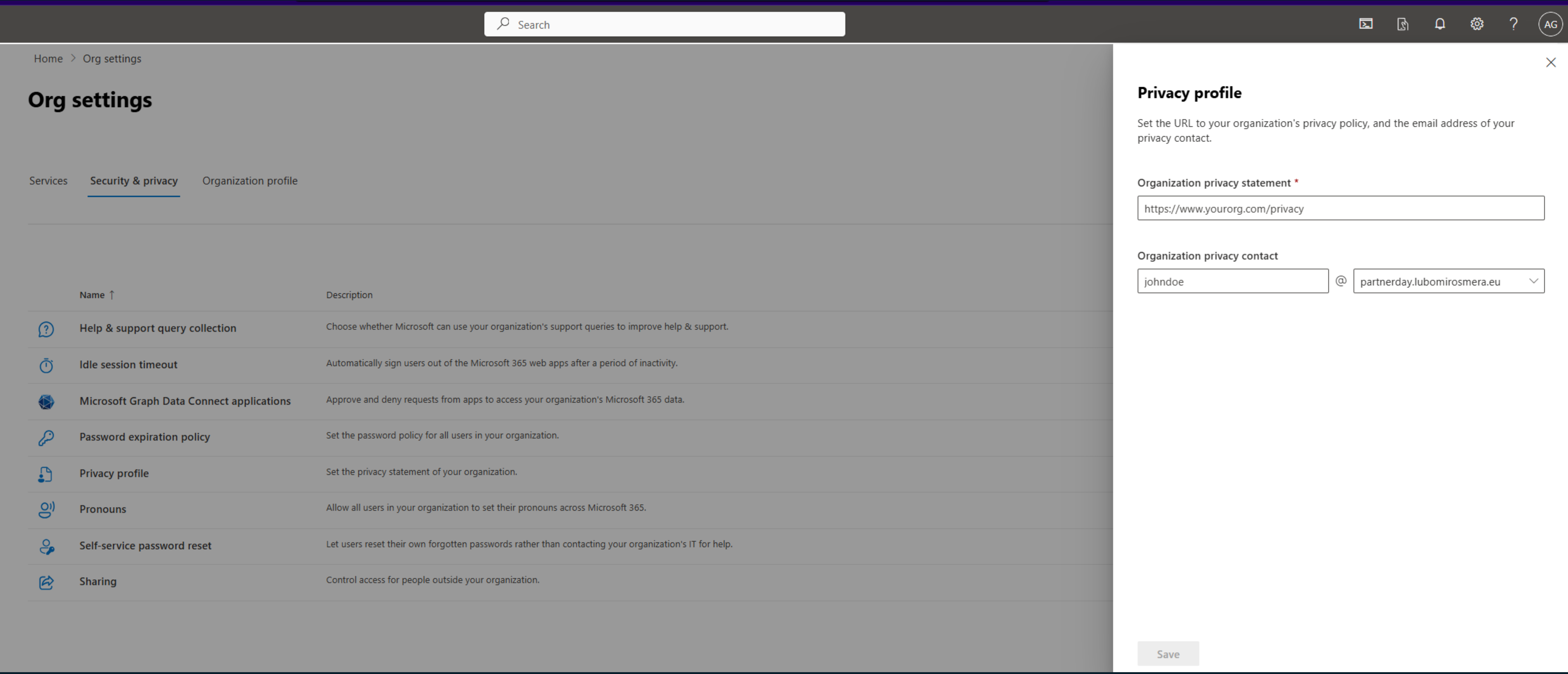
Name ↑	Description
Custom themes	Customize Microsoft 365 for your organization.
Custom tiles for Apps	Add tiles that open websites or SharePoint sites to Apps in the Microsoft 365 app.
Data location	See where Microsoft stores your data for each service you use.
Help desk information	Streamline user support by adding customized contact info to the Microsoft 365 help pane.
Keyboard shortcuts	Perform many common tasks using the keyboard. You can also see the full list of supported shortcuts by pressing S mark).
Organization information	Update your organization's contact info, such as your address, phone number, and technical contact.
Release preferences	Choose how your organization gets new features and service updates from Microsoft 365.
Send email notifications from your domain	Let Microsoft send notification messages from an email address within your organization instead of Microsoft's def email address.
Support integration	Integrate your internal support tools with Microsoft 365.

Data location

As part of our transparency principles, we publish the location where Microsoft stores your customer data, see Where your Microsoft 365 customer data is stored.

Service	Geography
Exchange Online	European Union
Exchange Online Protection	European Union
Microsoft Teams	European Union
OneDrive	European Union
SharePoint	European Union
Viva Connections	European Union
Viva Topics	Error, please try again later.

This tenant is not eligible to purchase Microsoft 365 Advanced Data Residency add-on because the tenant sign-up country is not available. Please see ADR Eligibility.



Org settings

Name ↑	Description
Help & support query collection	Choose whether Microsoft can use your organization's support queries to improve help & support.
Idle session timeout	Automatically sign users out of the Microsoft 365 web apps after a period of inactivity.
Microsoft Graph Data Connect applications	Approve and deny requests from apps to access your organization's Microsoft 365 data.
Password expiration policy	Set the password policy for all users in your organization.
Privacy profile	Set the privacy statement of your organization.
Pronouns	Allow all users in your organization to set their pronouns across Microsoft 365.
Self-service password reset	Let users reset their own forgotten passwords rather than contacting your organization's IT for help.
Sharing	Control access for people outside your organization.

Privacy profile

Set the URL to your organization's privacy policy, and the email address of your privacy contact.

Organization privacy statement *

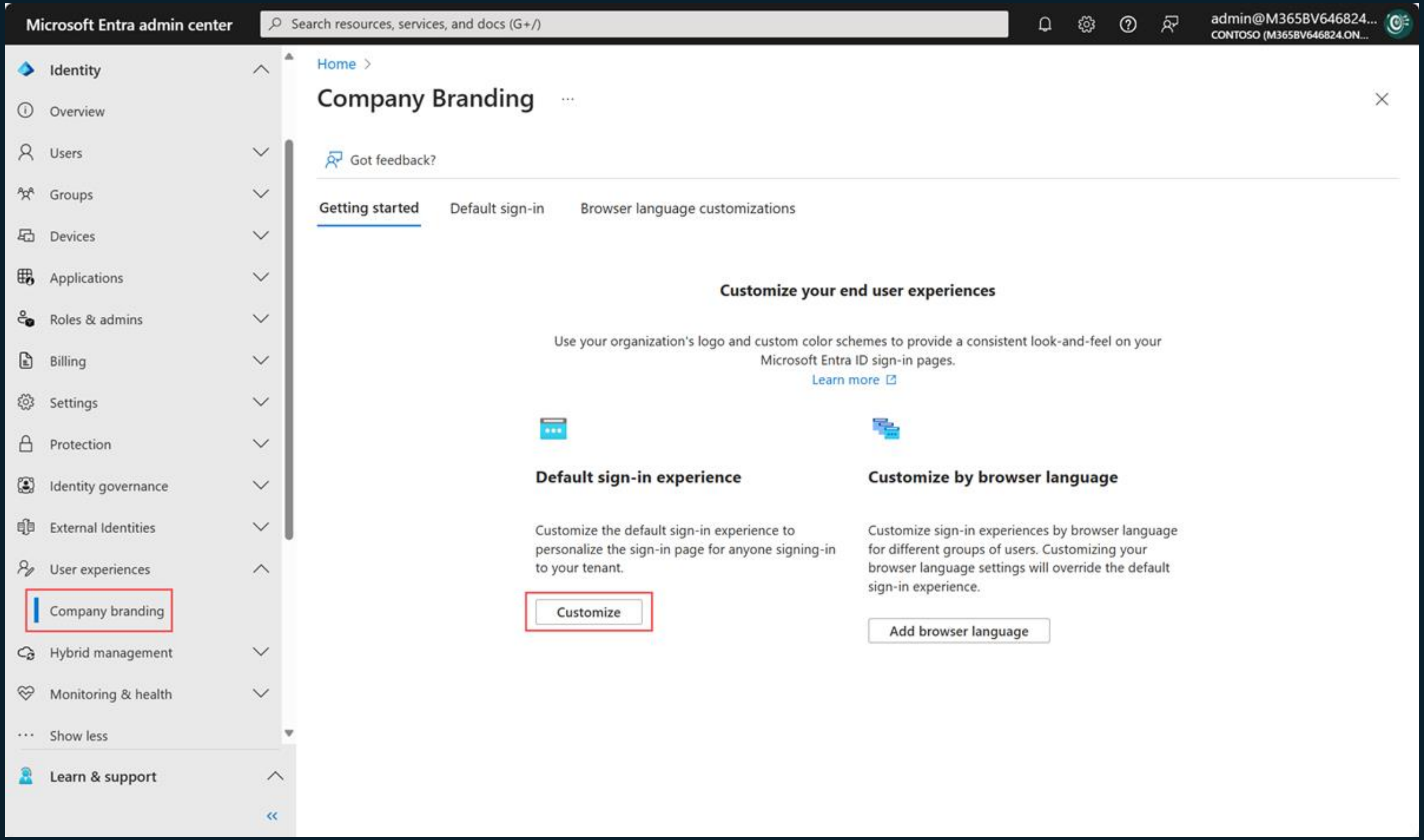
https://www.yourorg.com/privacy

Organization privacy contact

johndoe @ partnerday.lubomirosmera.eu

Company branding

https://learn.microsoft.com/en-us/entra/fundamentals/how-to-customize-branding



Company Branding

Customize your end user experiences

Use your organization's logo and custom color schemes to provide a consistent look-and-feel on your Microsoft Entra ID sign-in pages.
Learn more

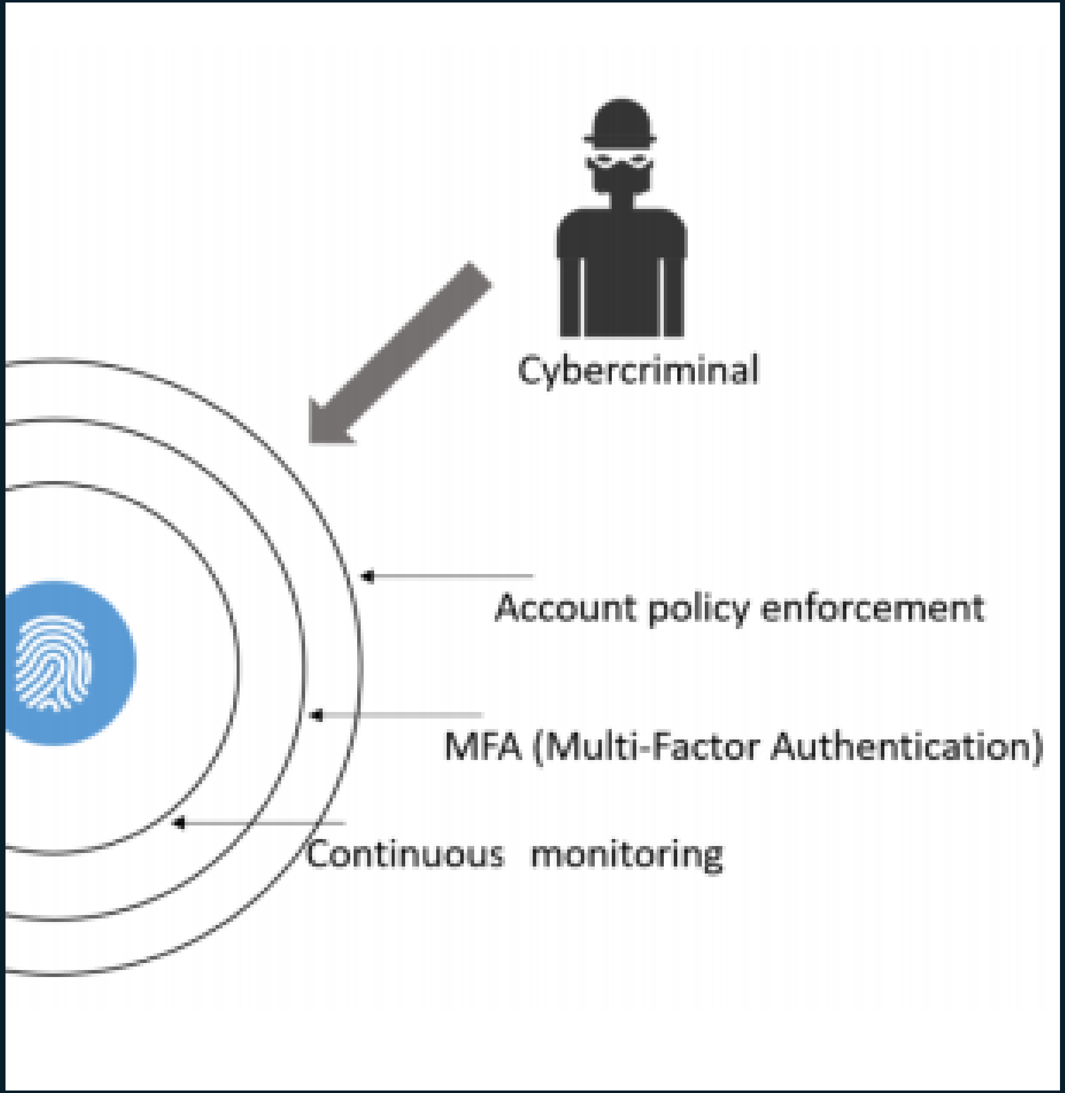
Default sign-in experience

Customize the default sign-in experience to personalize the sign-in page for anyone signing-in to your tenant.

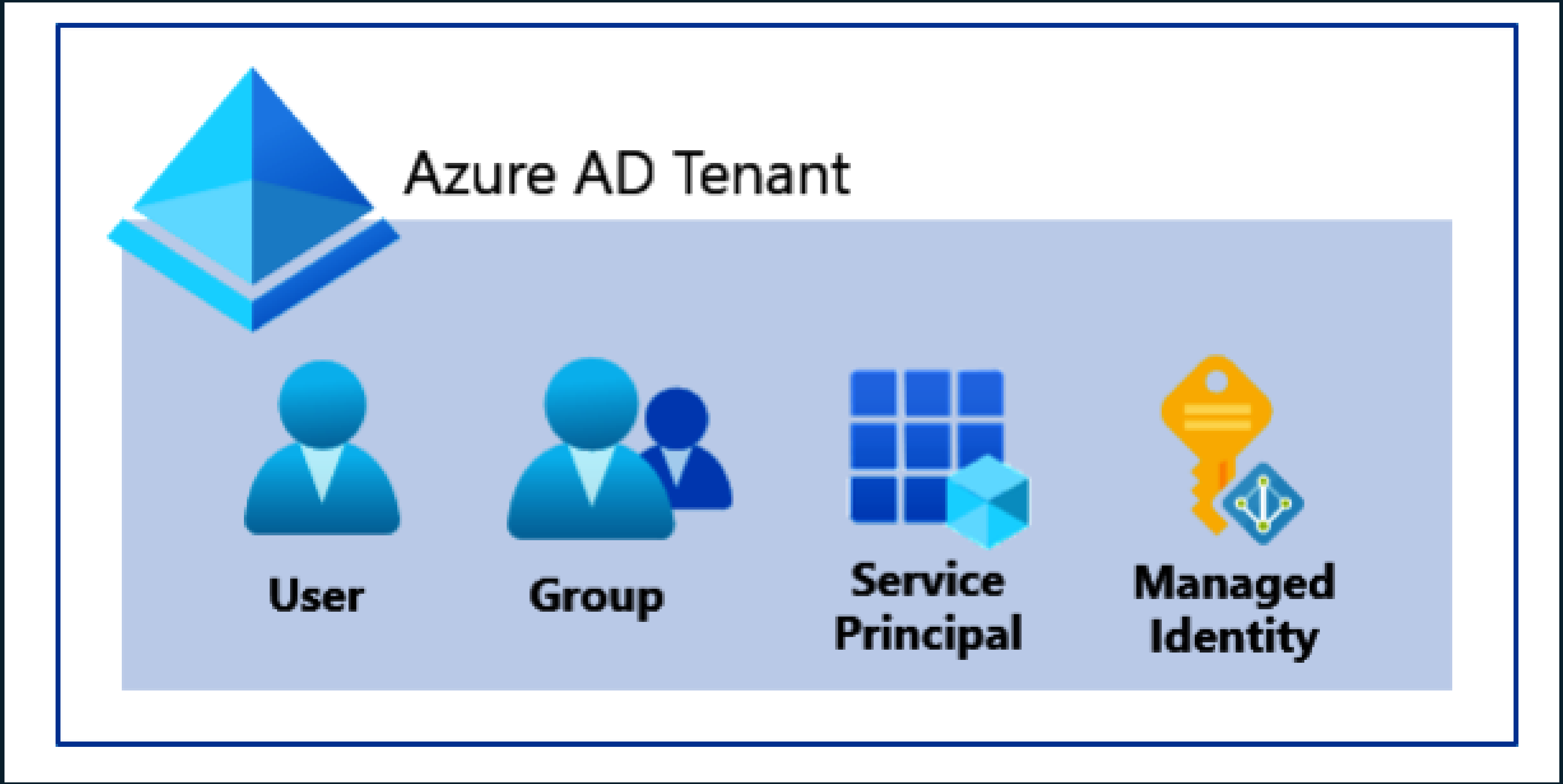
Customize by browser language

Customize sign-in experiences by browser language for different groups of users. Customizing your browser language settings will override the default sign-in experience.

Identity security principle

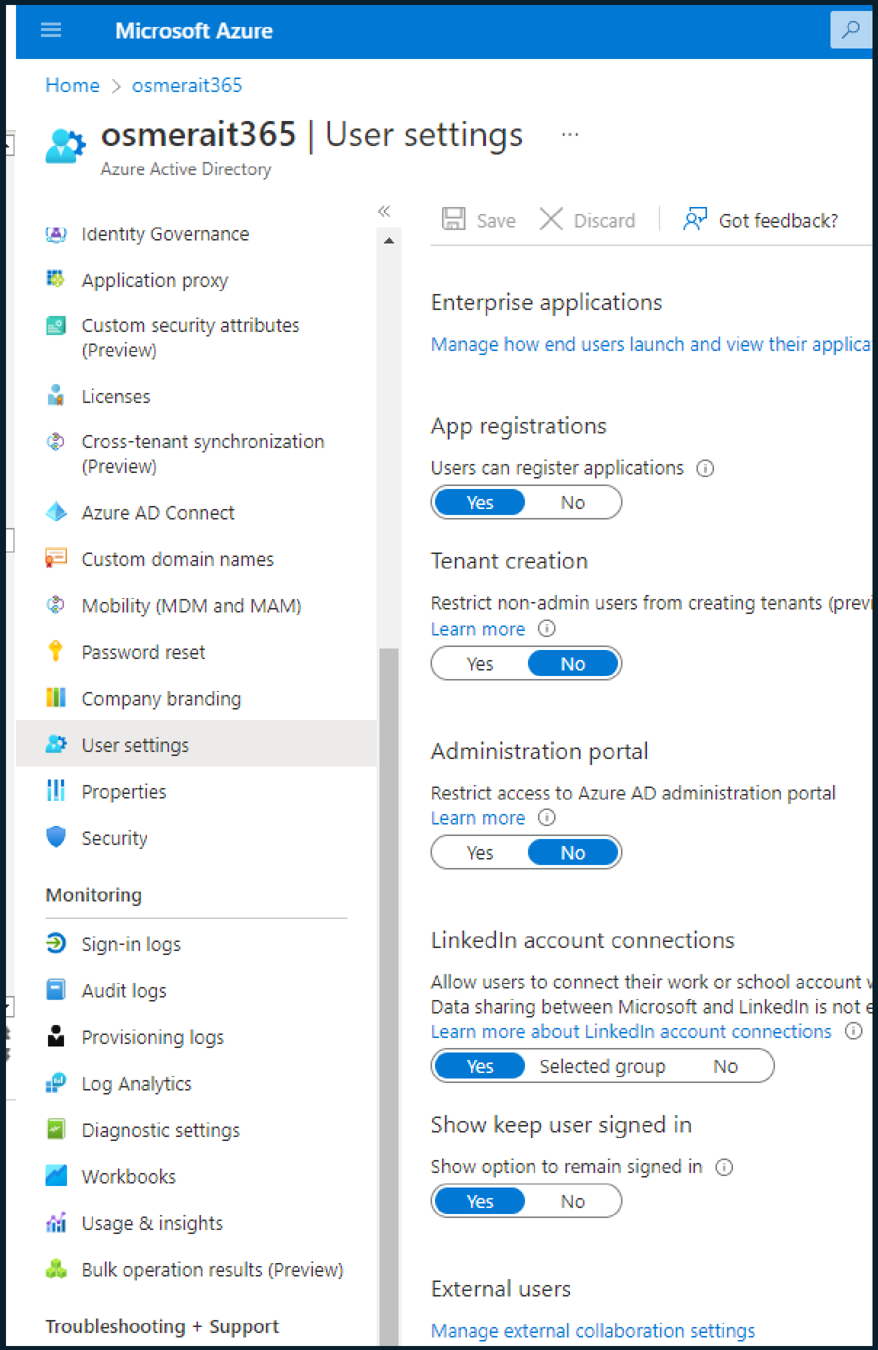


Identity types



Entra ID default configuration

- User settings:
  Users - Microsoft Entra admin center
- External collaboration:
  https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AllowlistPolicyBlade
- Groups:
  Groups - Microsoft Entra admin center
- Devices
  Devices - Microsoft Entra admin center
  - Warning – autopilot: https://learn.microsoft.com/en-us/autopilot/tutorial/user-driven/azure-ad-join-allow-users-to-join



osmerait365 | User settings ...

Azure Active Directory

Enterprise applications

Manage how end users launch and view their applica

App registrations

Users can register applications ⓘ

[✓ Yes] No

Tenant creation

Restrict non-admin users from creating tenants (previ

Learn more ⓘ

Yes [✓ No]

Administration portal

Restrict access to Azure AD administration portal

Learn more ⓘ

Yes [✓ No]

LinkedIn account connections

Allow users to connect their work or school account v

Data sharing between Microsoft and LinkedIn is not e

Learn more about LinkedIn account connections ⓘ

[✓ Yes] Selected group No

Show keep user signed in

Show option to remain signed in ⓘ

[✓ Yes] No

External users

Manage external collaboration settings

Existing Guests - cleaning

- Possible reasons for guest cleaning
  - A guest account is used to review a shared document and is not needed thereafter.
  - External people leave a team (or teams) and their guest account remains in Entra ID.
  - People leave their employer and move on to new challenges. Their guest account is invalid because they can no longer authenticate using the Entra ID instance for the tenant of their old employer.

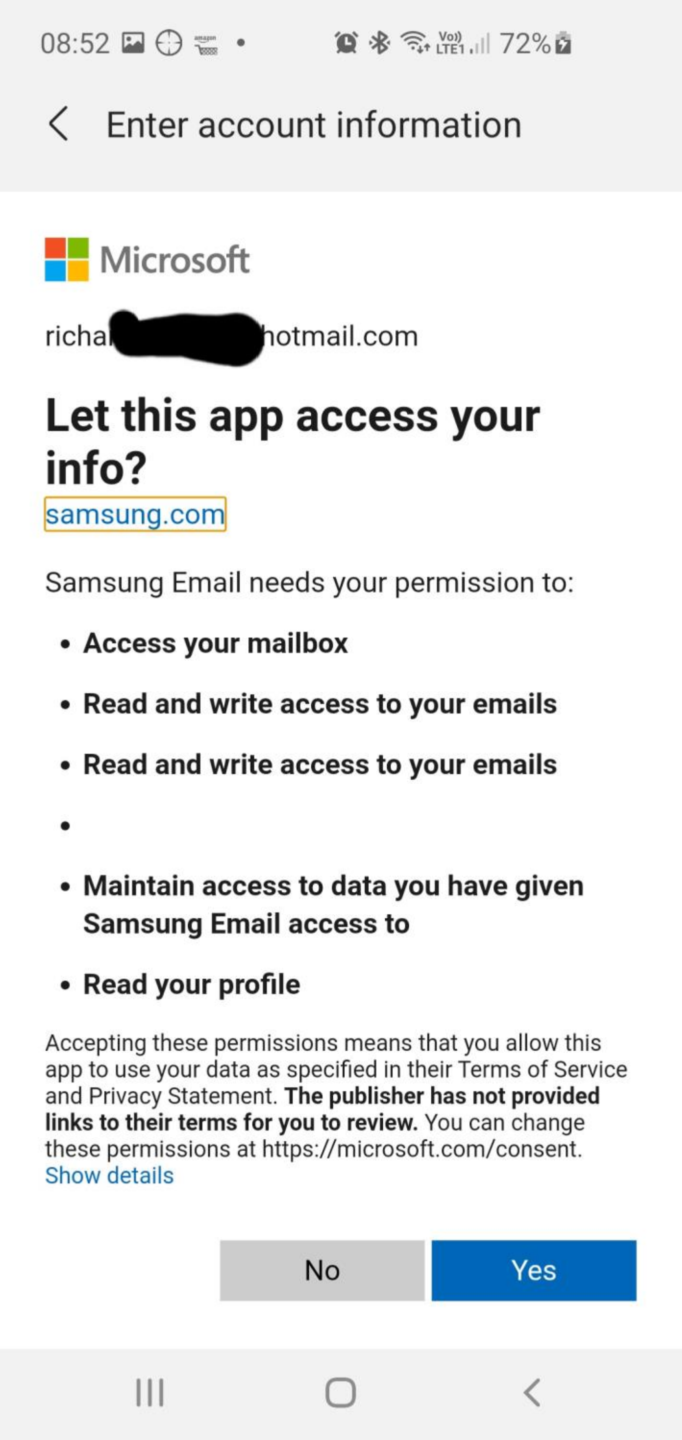
Which cloud application can user use?

When I have Microsoft 365, I have only Microsoft 365 apps – teams, office or?????

Application approve process

https://app.diagrams.net/?src=about

Techcommunity.Microsoft.com



richa[redacted]hotmail.com

Let this app access your info?

samsung.com

Samsung Email needs your permission to:

- **Access your mailbox**
- **Read and write access to your emails**
- **Read and write access to your emails**
-
- **Maintain access to data you have given Samsung Email access to**
- **Read your profile**

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://microsoft.com/consent. Show details

Groups, dynamic groups consideration

- Microsoft 365 groups
- Security groups
- Mail-enabled security groups
- Distribution groups

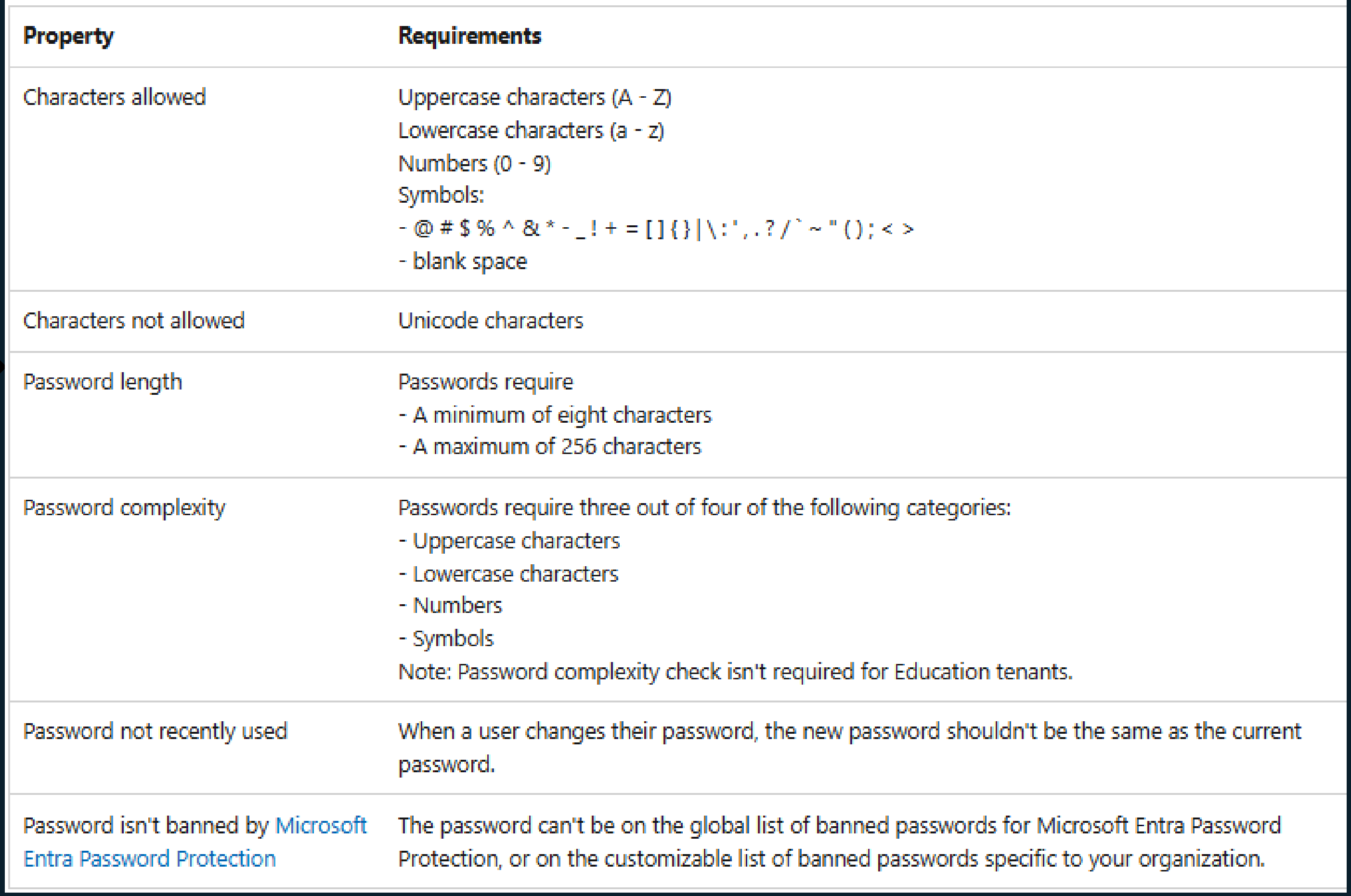
Authentication methods

Passwords in Entra

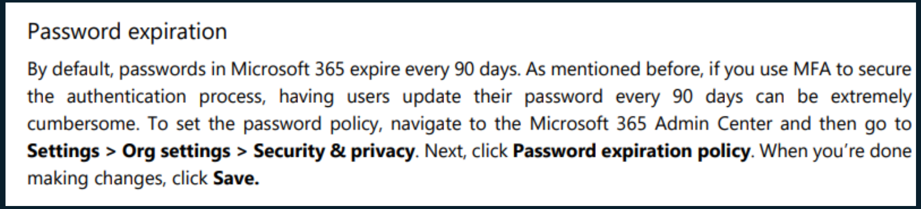
Passwords cannot be disabled…

Cannot be changed

Can be changed

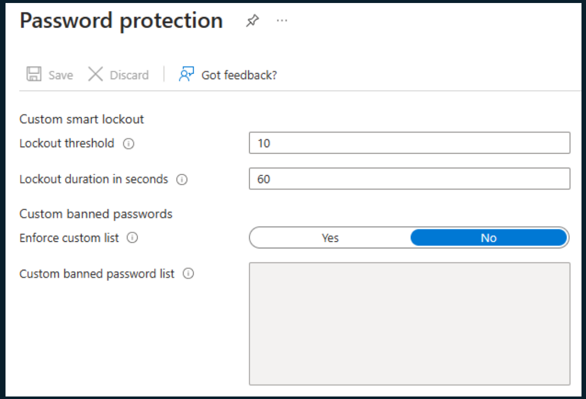


Property	Requirements
Characters allowed	Uppercase characters (A - Z) Lowercase characters (a - z) Numbers (0 - 9) Symbols: - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > - blank space
Characters not allowed	Unicode characters
Password length	Passwords require - A minimum of eight characters - A maximum of 256 characters
Password complexity	Passwords require three out of four of the following categories: - Uppercase characters - Lowercase characters - Numbers - Symbols Note: Password complexity check isn't required for Education tenants.
Password not recently used	When a user changes their password, the new password shouldn't be the same as the current password.
Password isn't banned by Microsoft Entra Password Protection	The password can't be on the global list of banned passwords for Microsoft Entra Password Protection, or on the customizable list of banned passwords specific to your organization.



Password expiration

By default, passwords in Microsoft 365 expire every 90 days. As mentioned before, if you use MFA to secure the authentication process, having users update their password every 90 days can be extremely cumbersome. To set the password policy, navigate to the Microsoft 365 Admin Center and then go to **Settings** > **Org settings** > **Security & privacy**. Next, click **Password expiration policy**. When you're done making changes, click **Save.**



Password protection

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

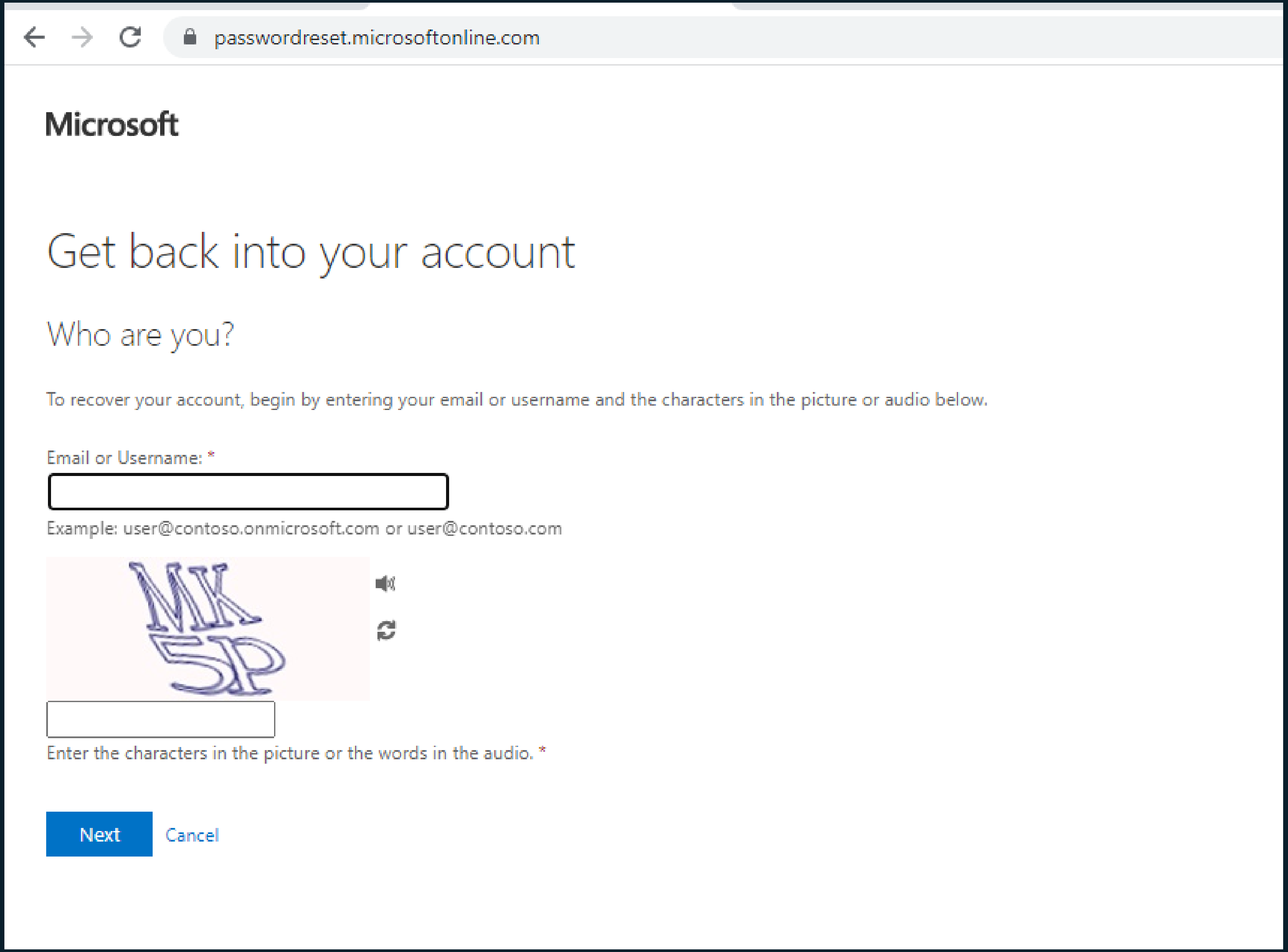
Enforce custom list: ○ Yes ● No

Custom banned password list:

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-combined-policy
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PasswordProtectionBlade
https://admin.microsoft.com/Adminportal/Home#/Settings/SecurityPrivacy/:/Settings/L1/PasswordPolicy

Help desk is not necessary

Configuration link: https://entra.microsoft.com/#view/Microsoft_AAD_IAM/PasswordResetMenuBlade/~/Properties/fromNav/



Get back into your account

Who are you?

To recover your account, begin by entering your email or username and the characters in the picture or audio below.

Email or Username: *

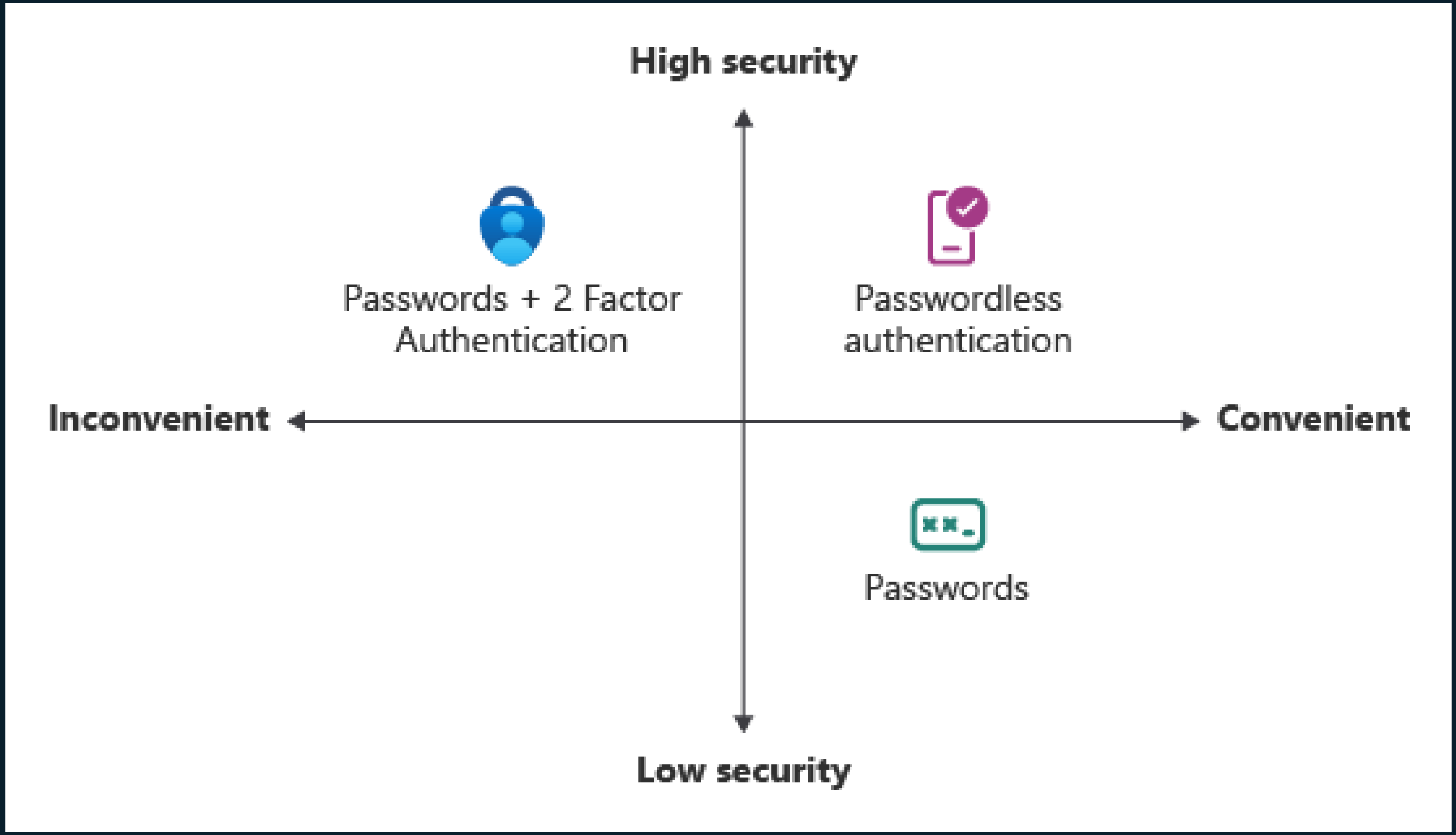
Example: user@contoso.onmicrosoft.com or user@contoso.com

Enter the characters in the picture or the words in the audio. *

DEMO ssprgroupusers

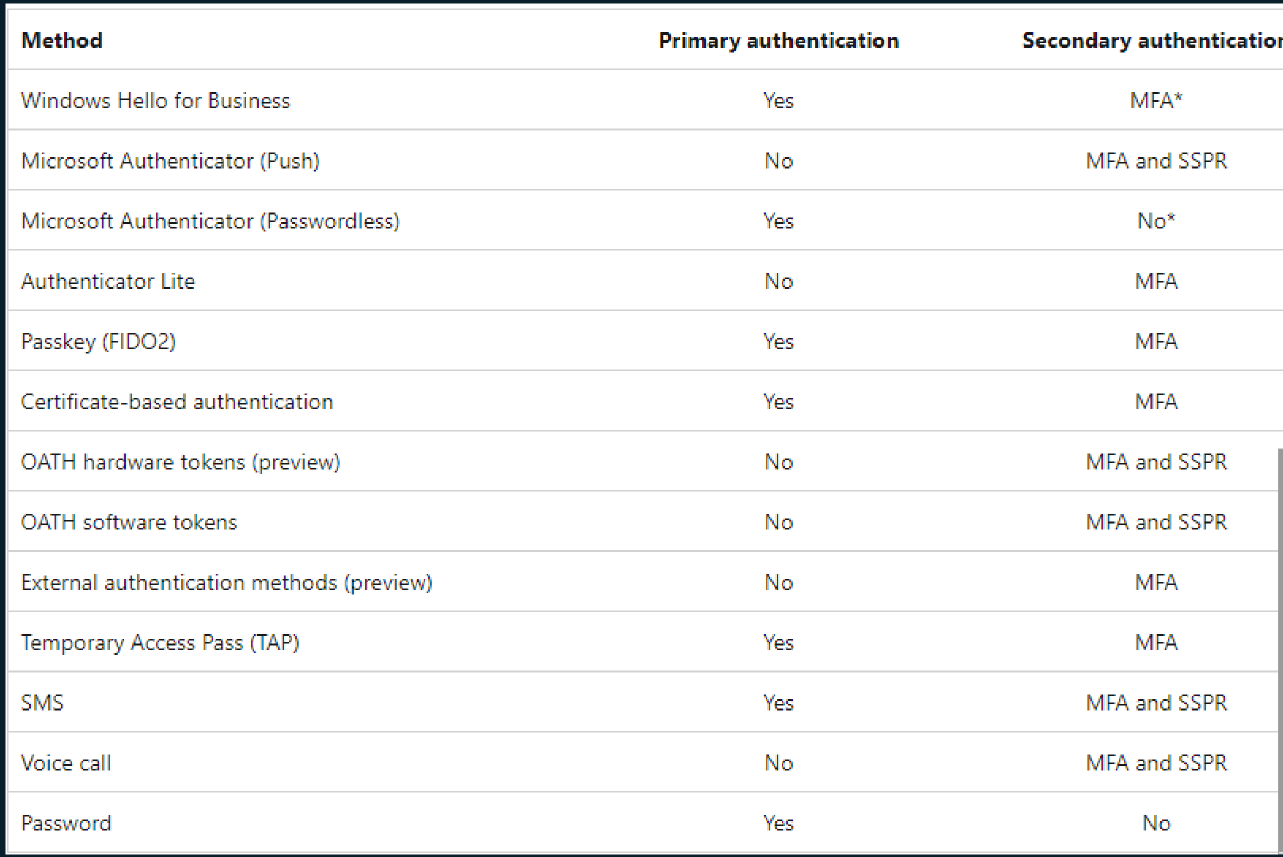
- sspruser2@partnerday.lubomirosmera.eu
- Reg method
- Show sspr

MFA, passwordless

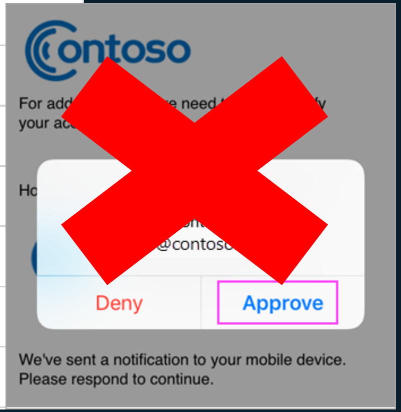


High security
Passwords + 2 Factor Authentication
Passwordless authentication
Inconvenient
Convenient
Passwords
Low security

AUTHENTICATION METHODS



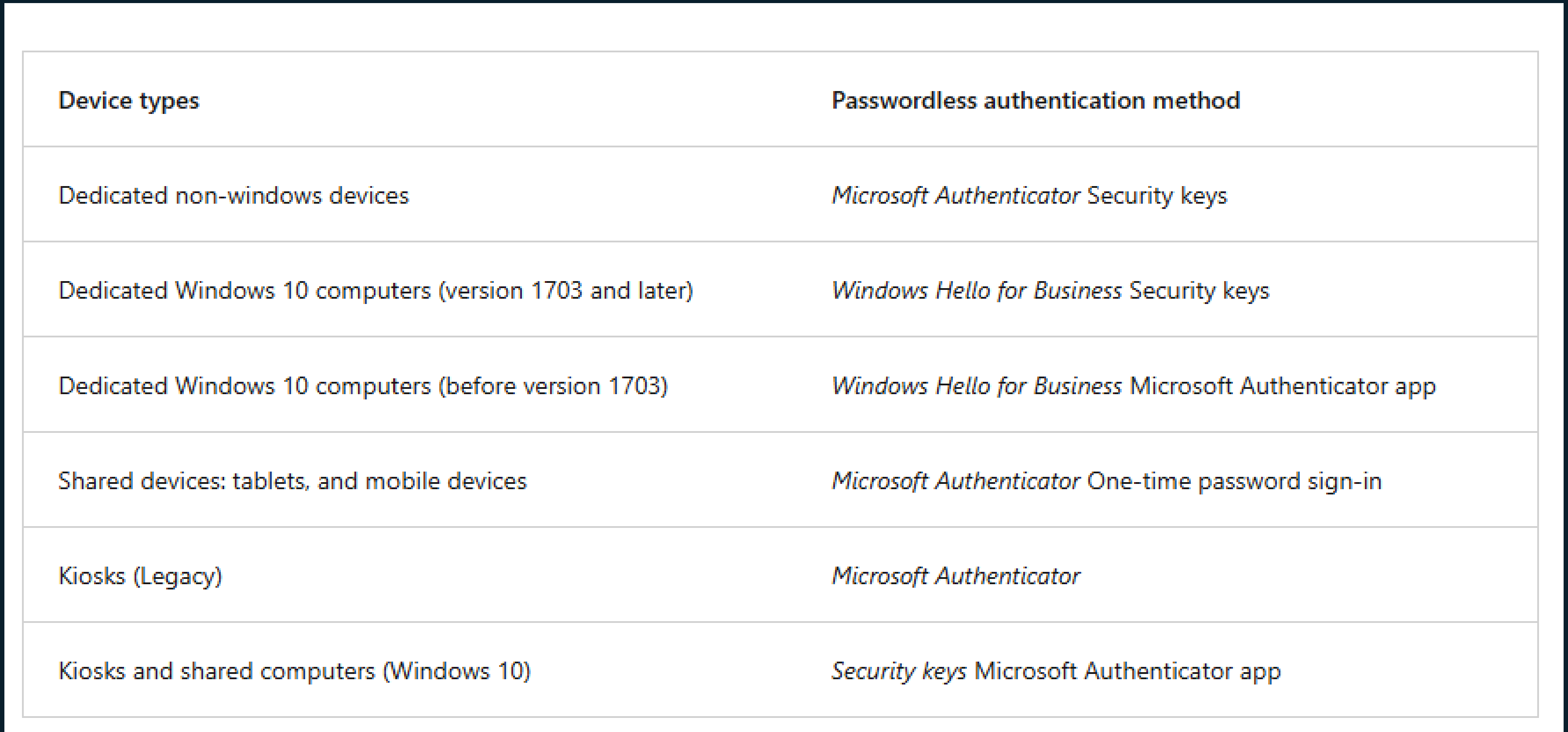
Method	Primary authentication	Secondary authentication
Windows Hello for Business	Yes	MFA*
Microsoft Authenticator (Push)	No	MFA and SSPR
Microsoft Authenticator (Passwordless)	Yes	No*
Authenticator Lite	No	MFA
Passkey (FIDO2)	Yes	MFA
Certificate-based authentication	Yes	MFA
OATH hardware tokens (preview)	No	MFA and SSPR
OATH software tokens	No	MFA and SSPR
External authentication methods (preview)	No	MFA
Temporary Access Pass (TAP)	Yes	MFA
SMS	Yes	MFA and SSPR
Voice call	No	MFA and SSPR
Password	Yes	No



We've sent a notification to your mobile device. Please respond to continue.

https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AdminAuthMethods

Passwordless authentication methods by device types



Device types	Passwordless authentication method
Dedicated non-windows devices	*Microsoft Authenticator* Security keys
Dedicated Windows 10 computers (version 1703 and later)	*Windows Hello for Business* Security keys
Dedicated Windows 10 computers (before version 1703)	*Windows Hello for Business* Microsoft Authenticator app
Shared devices: tablets, and mobile devices	*Microsoft Authenticator* One-time password sign-in
Kiosks (Legacy)	*Microsoft Authenticator*
Kiosks and shared computers (Windows 10)	*Security keys* Microsoft Authenticator app

https://learn.microsoft.com/en-us/training/modules/manage-authentication-microsoft-entra-id/11-passwordless-authentication

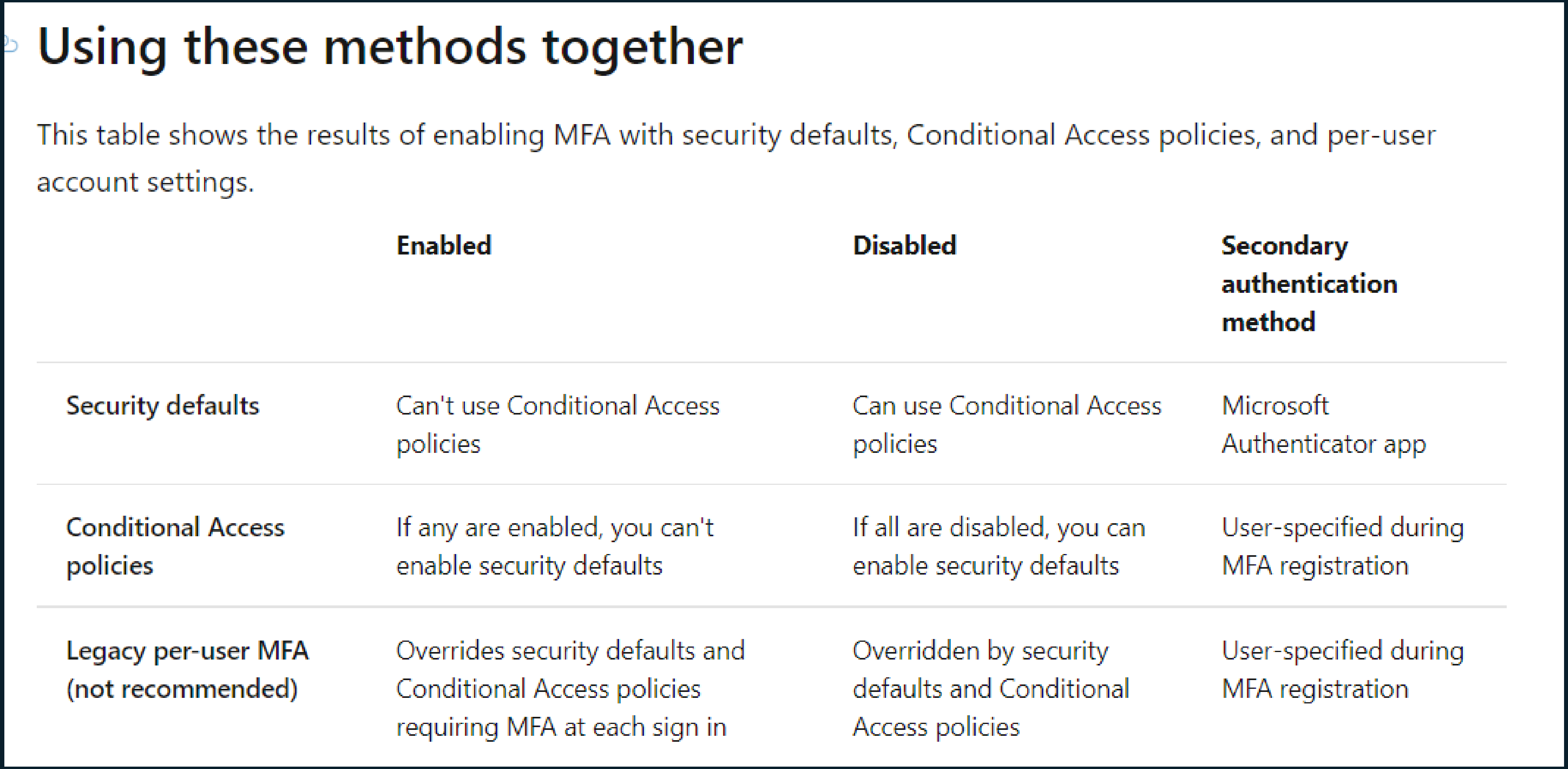
Security defaults?

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Properties

Non-customizable policies for tenant:

- Requiring all users to register for Azure AD Multi-Factor Authentication.
- Requiring administrators to do multifactor authentication.
- Requiring users to do multifactor authentication when necessary.
- Blocking legacy authentication protocols.
- Protecting privileged activities like access to the Azure portal.

MFA deployment strategy



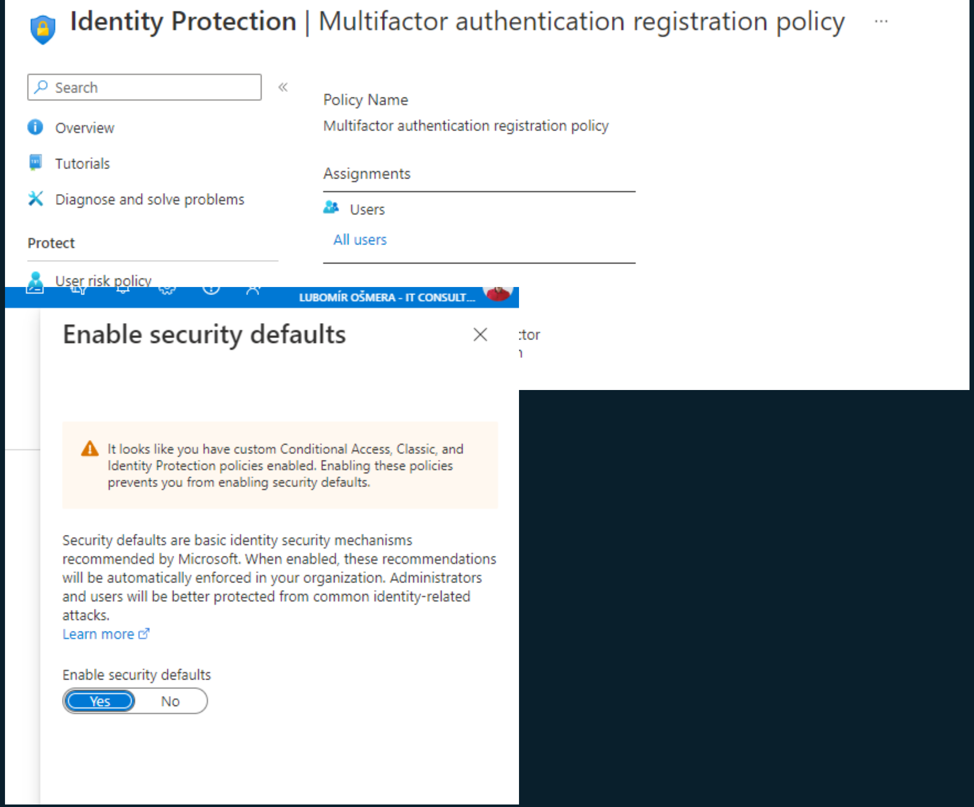
Using these methods together

This table shows the results of enabling MFA with security defaults, Conditional Access policies, and per-user account settings.

	Enabled	Disabled	Secondary authentication method
Security defaults	Can't use Conditional Access policies	Can use Conditional Access policies	Microsoft Authenticator app
Conditional Access policies	If any are enabled, you can't enable security defaults	If all are disabled, you can enable security defaults	User-specified during MFA registration
Legacy per-user MFA (not recommended)	Overrides security defaults and Conditional Access policies requiring MFA at each sign in	Overridden by security defaults and Conditional Access policies	User-specified during MFA registration

User MFA registration – option 1

Enabling security defaults or identity protection registration policy:
User must provide authenticator until 14 days from configuration:



Identity Protection | Multifactor authentication registration policy

Policy Name
Multifactor authentication registration policy

Assignments

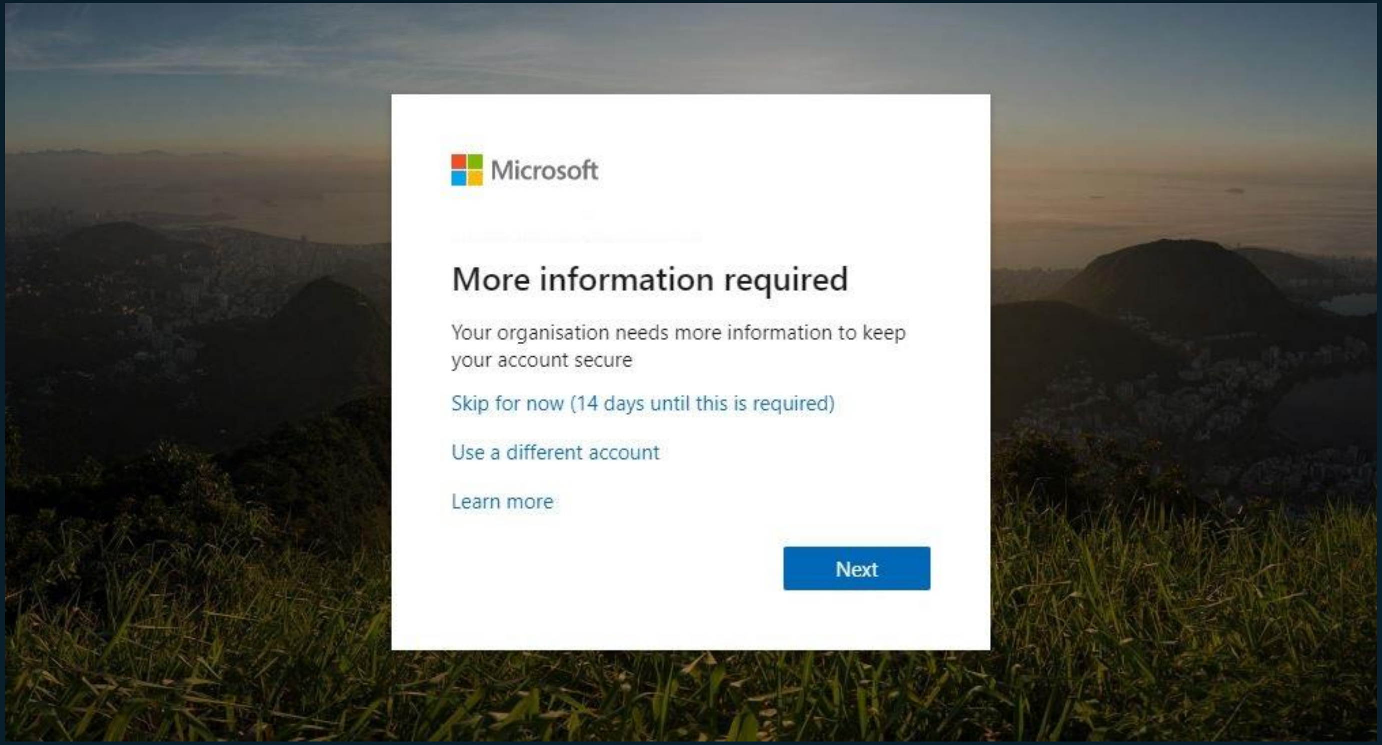
Users
All users

Enable security defaults

It looks like you have custom Conditional Access, Classic, and Identity Protection policies enabled. Enabling these policies prevents you from enabling security defaults.

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.
Learn more

Enable security defaults
[✓ Yes] No



More information required

Your organisation needs more information to keep your account secure

Skip for now (14 days until this is required)

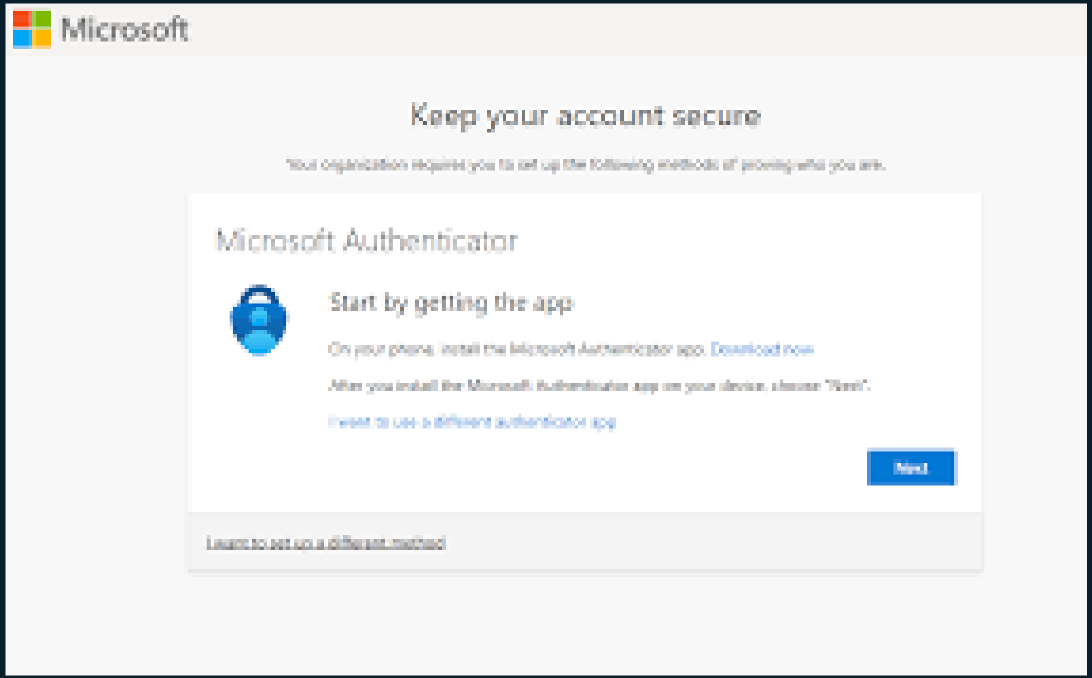
Use a different account

Learn more

Next

User MFA registration – option 2

Manual registration on https://aka.ms/mfasetup



Microsoft

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

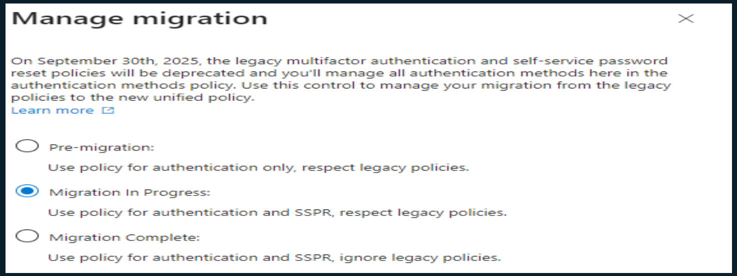
After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Next

I want to set up a different method

Authentication methods configuration



Manage migration

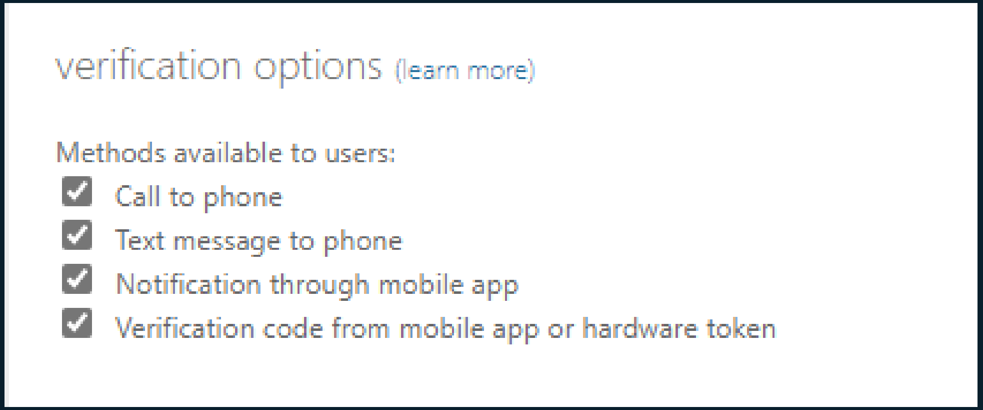
On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy.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

○ Pre-migration:
Use policy for authentication only, respect legacy policies.

● Migration In Progress:
Use policy for authentication and SSPR, respect legacy policies.

○ Migration Complete:
Use policy for authentication and SSPR, ignore legacy policies.

Legacy:
[Multi-factor authentication (windowsazure.com)]

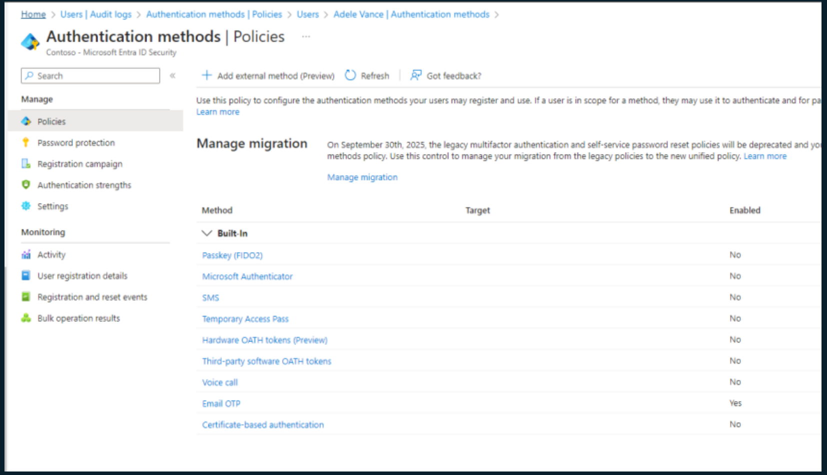


verification options (learn more)

Methods available to users:

- ☑ Call to phone
- ☑ Text message to phone
- ☑ Notification through mobile app
- ☑ Verification code from mobile app or hardware token

Modern:
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AdminAuthMethods/f



Home > Users | Audit logs > Authentication methods | Policies > Users > Adele Vance | Authentication methods >

Authentication methods | Policies

Contoso - Microsoft Entra ID Security

Search
+ Add external method (Preview)
Refresh
Got feedback?
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results

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 pa
Learn more

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

Manage migration

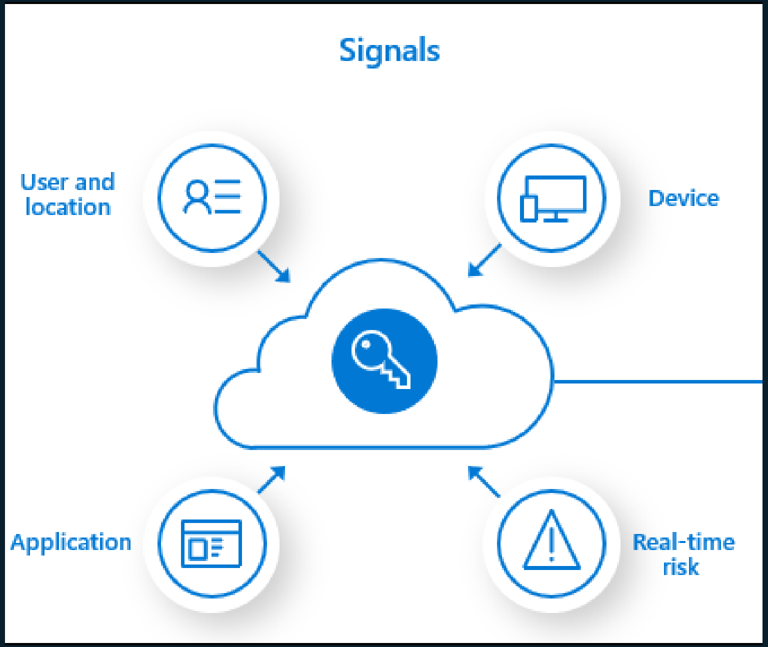
Method	Target	Enabled
Built-In		
Passkey (FIDO2)		No
Microsoft Authenticator		No
SMS		No
Temporary Access Pass		No
Hardware OATH tokens (Preview)		No
Third-party software OATH tokens		No
Voice call		No
Email OTP		Yes
Certificate-based authentication		No

Conditional access

What are default access rules for cloud environments? How can I access?

- Any device
- Any time
- Any location
- Any authentication method

Conditional access



Lokace

- Je v pořádku přihlašování z Číny?
- Je nutno přistupovat pouze z firemních IP adres?
- Pokud nepřistupuji z firemních adres, mám nějaké omezení? (MFA, znepřístupnění, podmínky spravovaných zařízení)

Zařízení

- Je v pořádku připojování z Android, Macu, Linuxu?
- Povolujeme i BYOD?
- Musí zařízení splňovat health check podmínky?

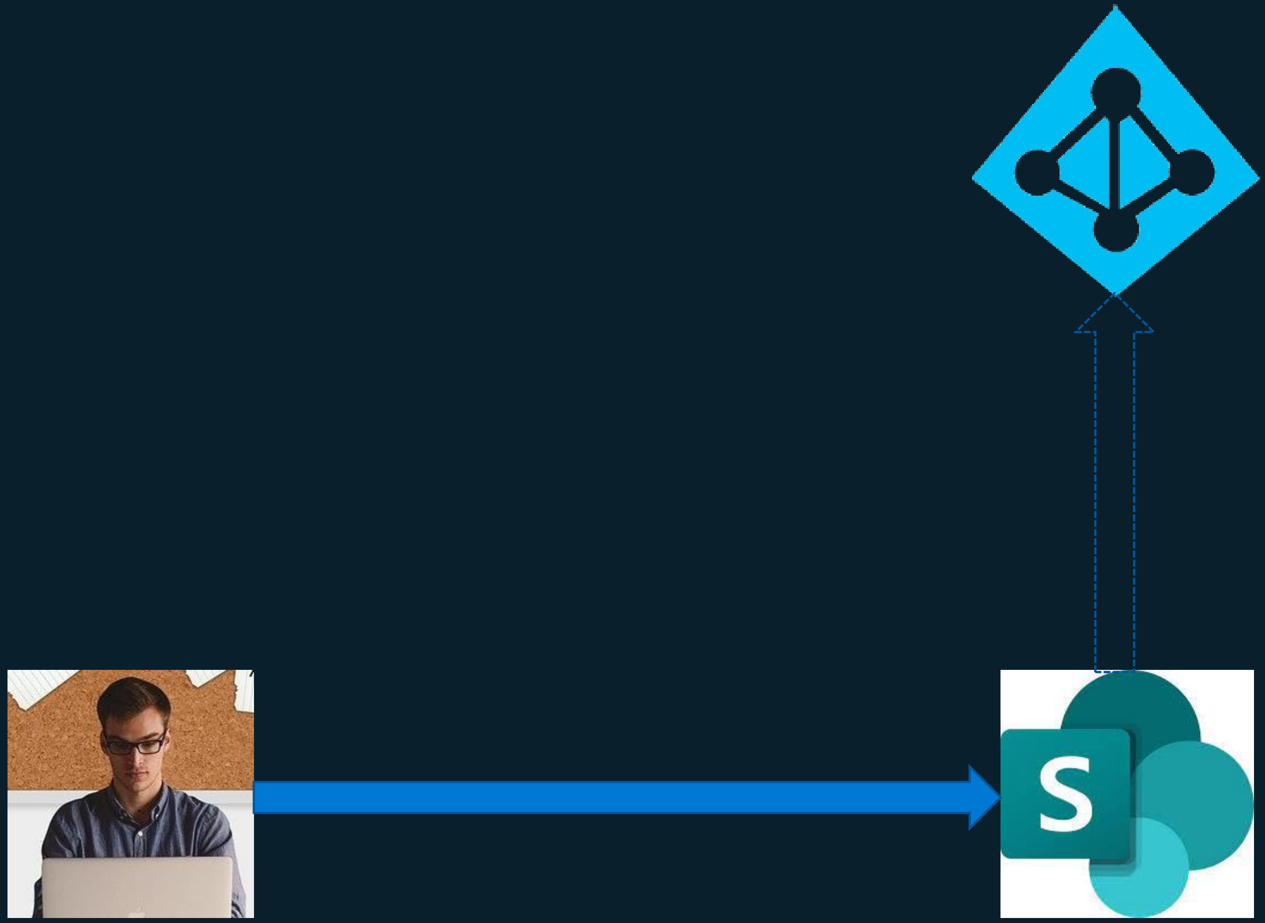
Aplikace

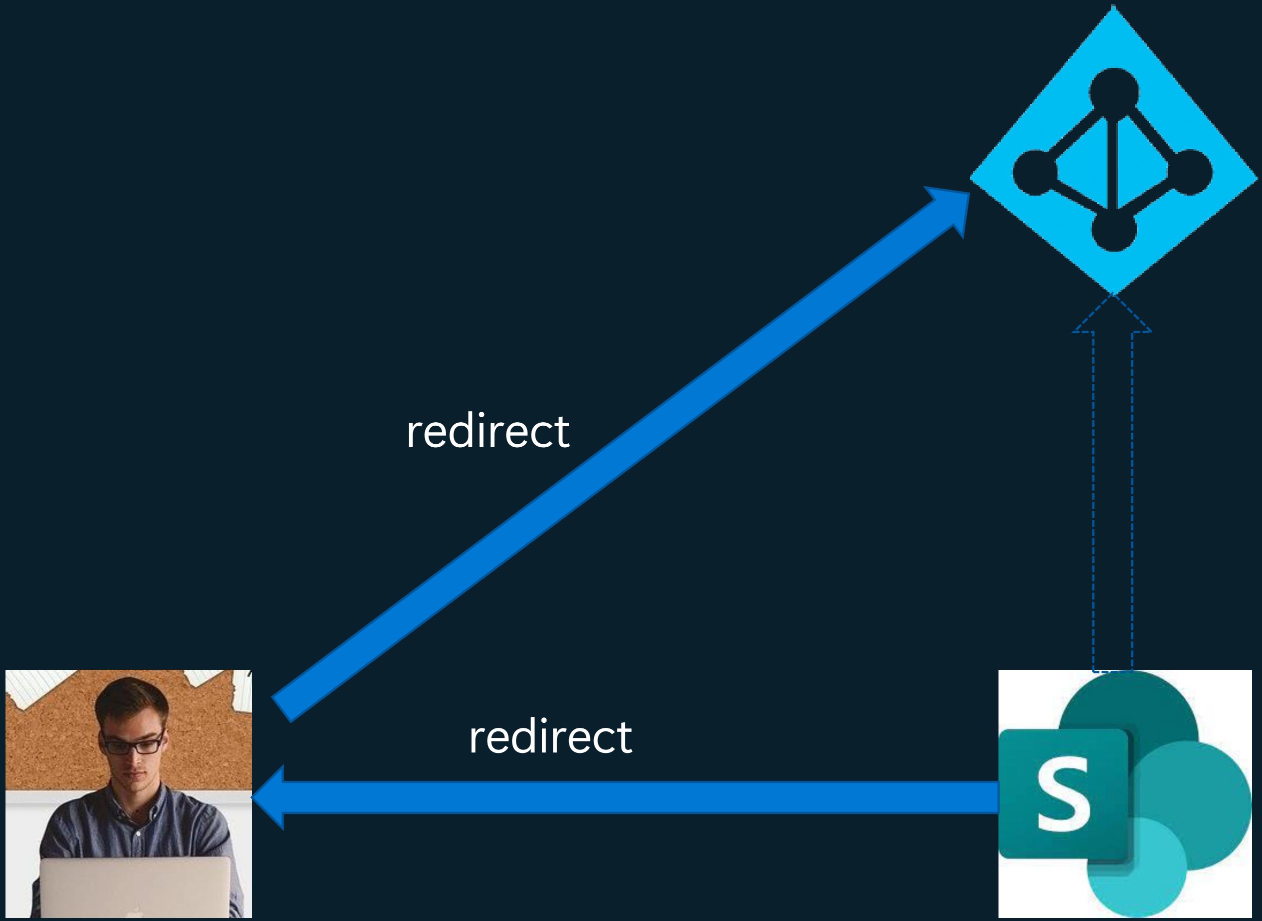
- Povolujeme přístup pouze ze schválených aplikací?
- Podporujeme i legacy aplikace?
- Budeme omezovat přístupy z Browseru? (délka relace, mobily)

Co když je detekce něčeho podezřelého?

- Přístup z anonymní IP, přístup z inikovaného zařízení

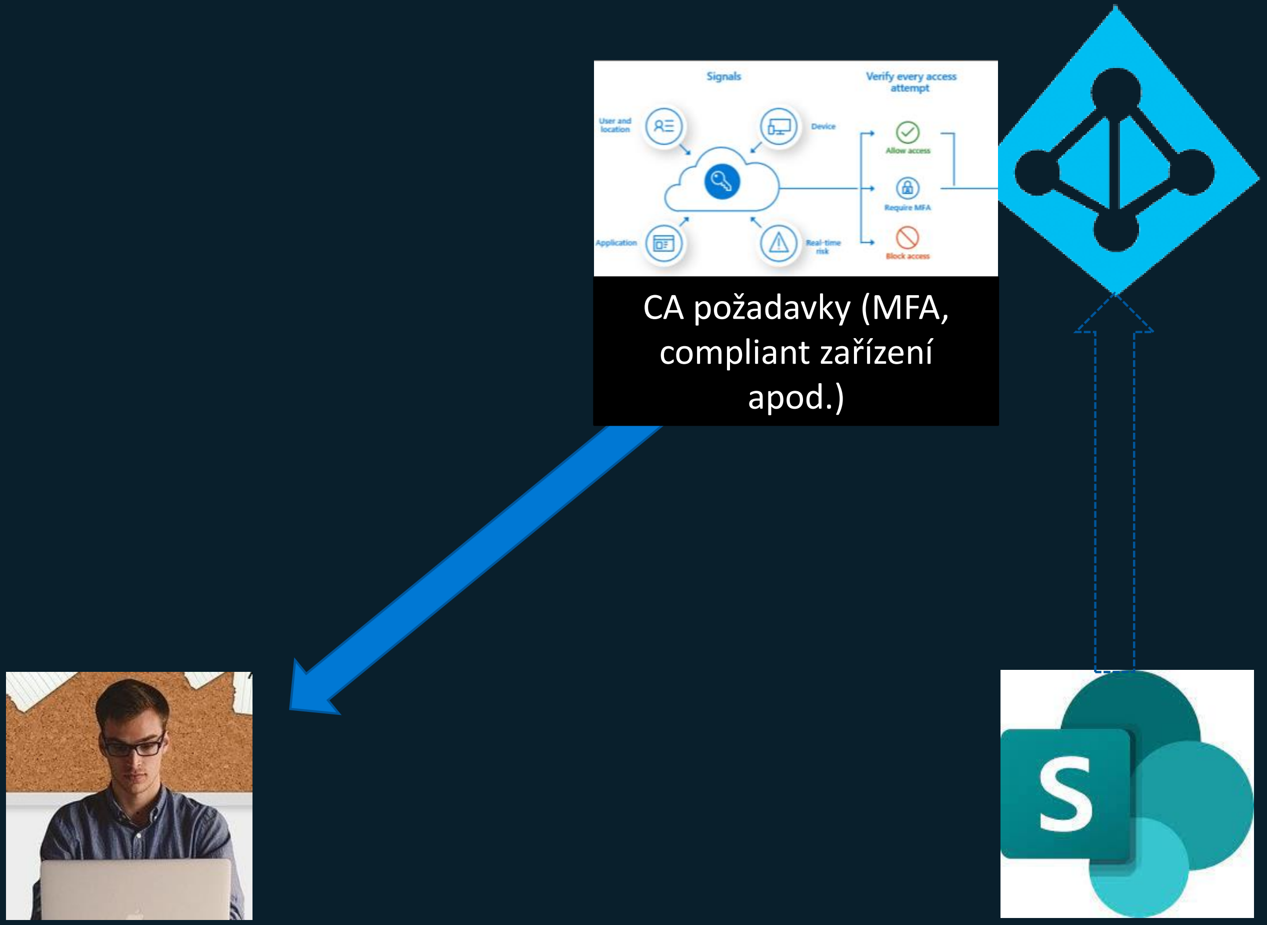
How it works?



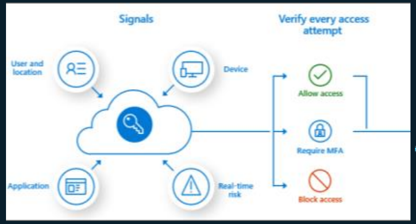


redirect

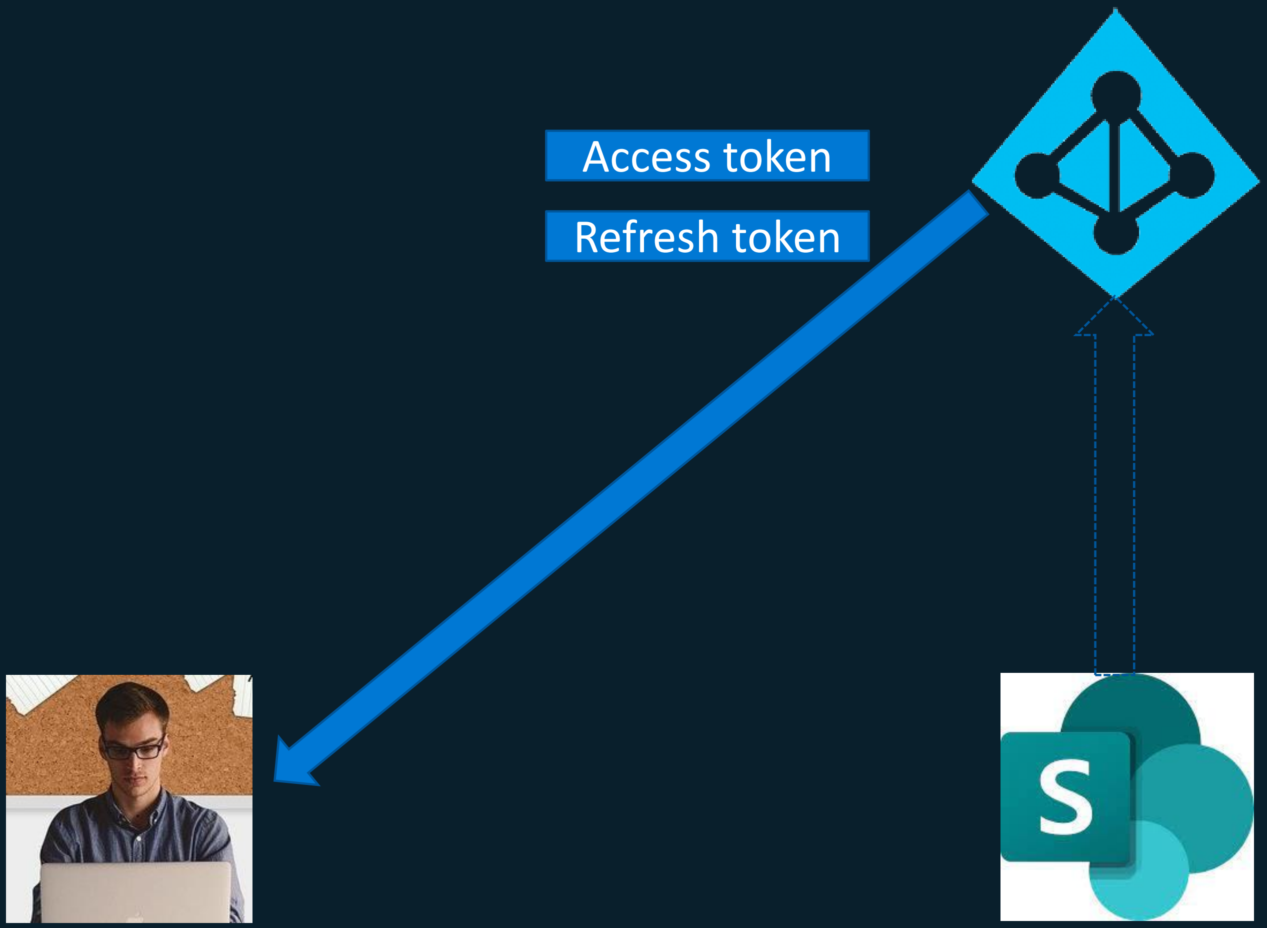
redirect



CA požadavky (MFA, compliant zařízení apod.)

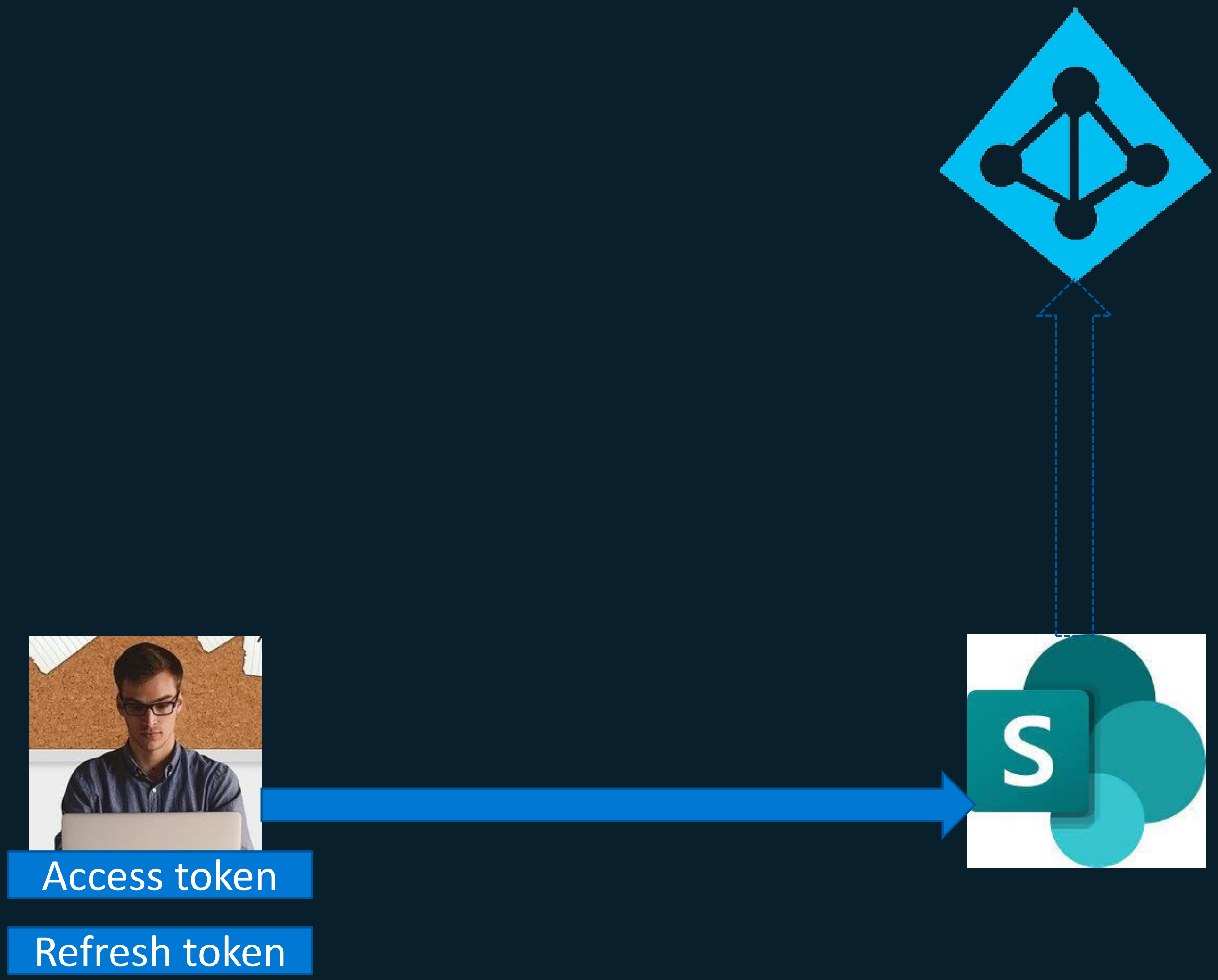


CA požadavky (MFA, compliant zařízení apod.)
splněny



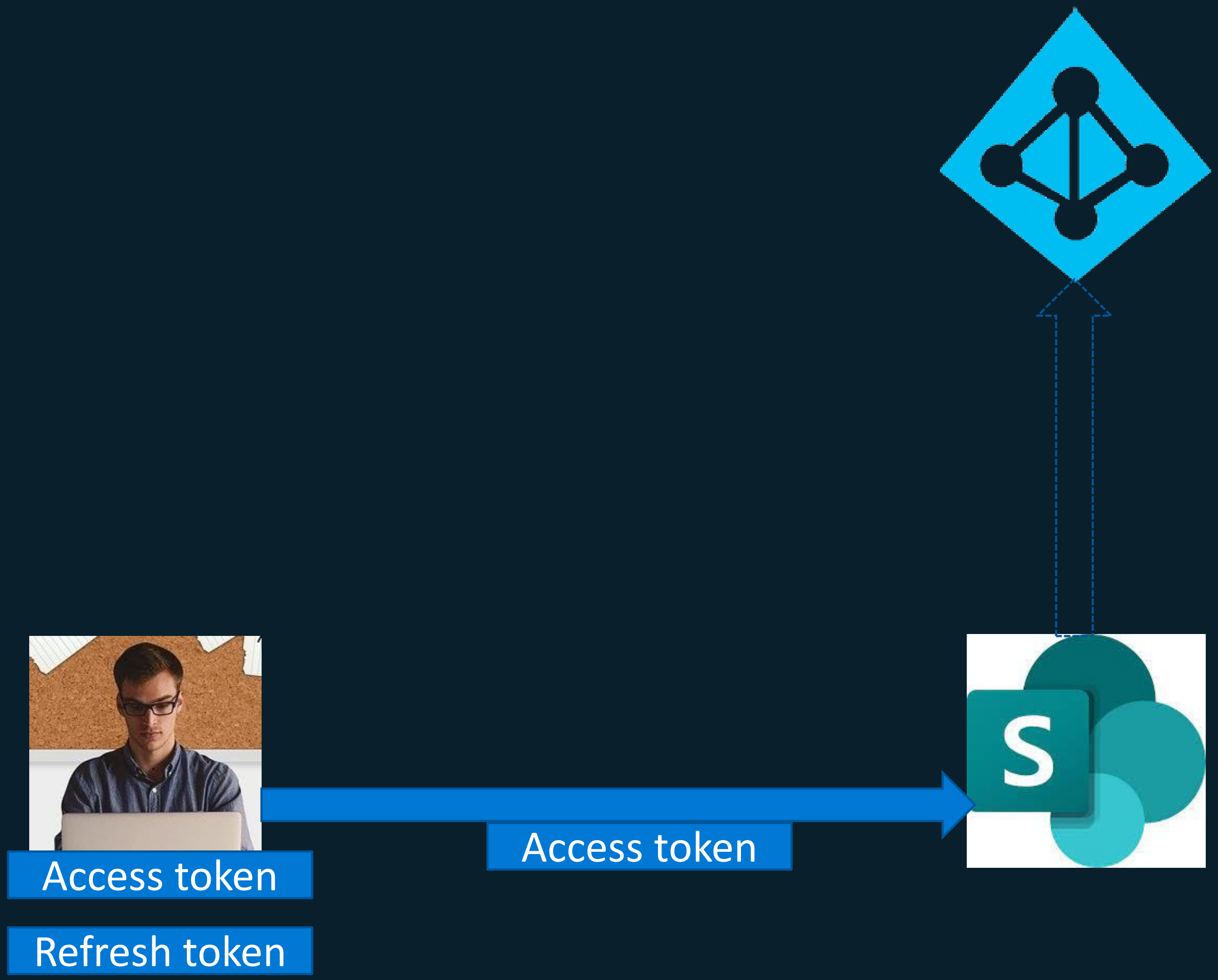
Access token

Refresh token



Access token

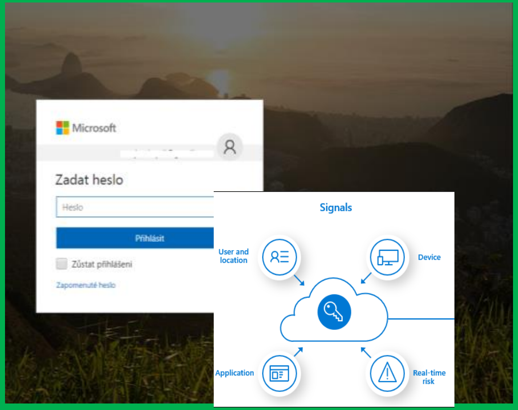
Refresh token



Access token

Refresh token

Access token



Microsoft

[redacted]

Zadat heslo

Heslo

Přihlásit

□ Zůstat přihlášeni

Zapomenuté heslo

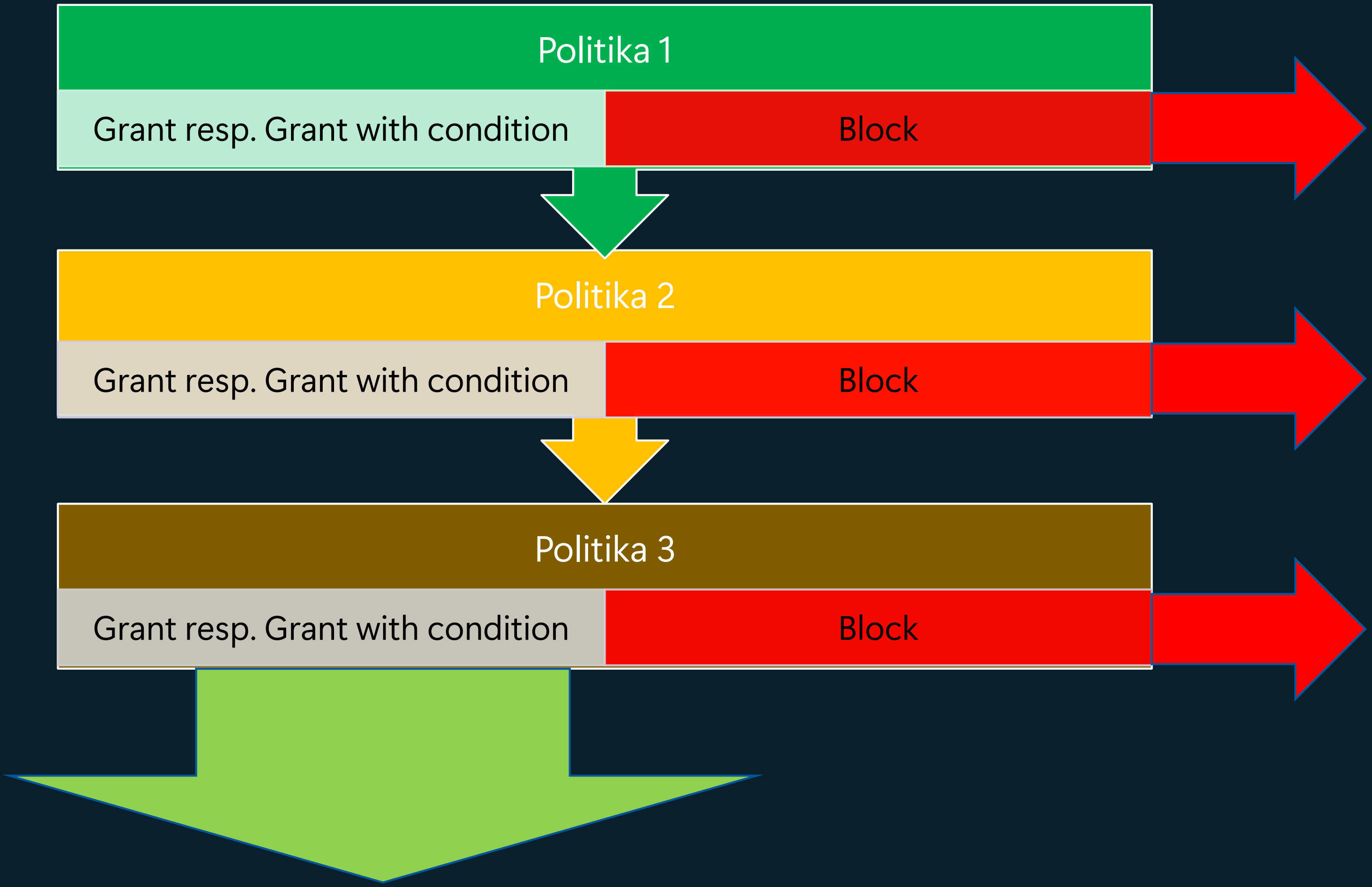
politika1

politika2

politika3

politika4

Evaluation



Politika 1

Grant resp. Grant with condition | Block

Politika 2

Grant resp. Grant with condition | Block

Politika 3

Grant resp. Grant with condition | Block

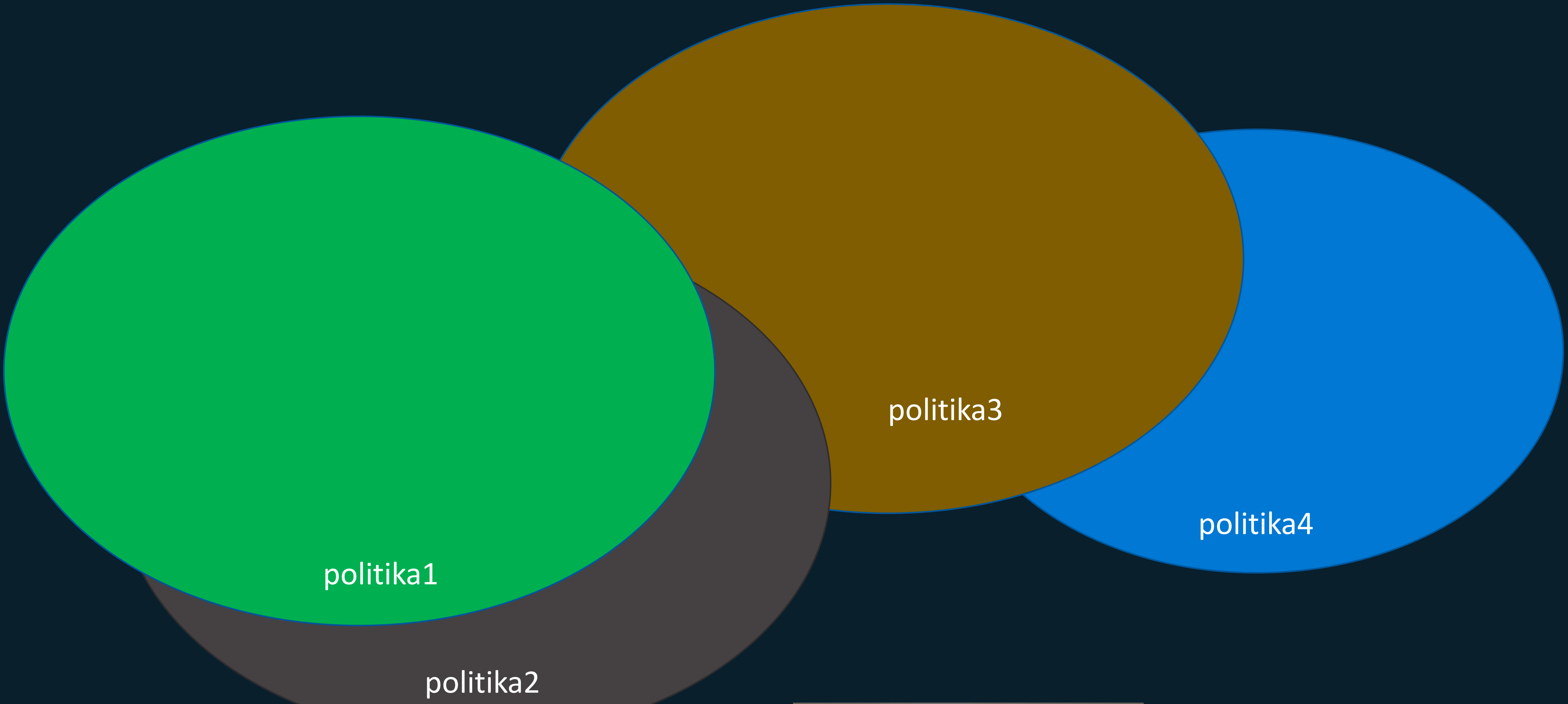
Conditional access policies creation

- Suitable tools – Excel worksheet, onenote, big paper and pens
- Coffee and delicious meal
- Map and design block scenarios – what should be blocked
- Consider also Microsoft prepared templates: https://portal.azure.com/#view/Microsoft_AAD_ConditionalAccess/CaTemplates.ReactView
- Plan a Microsoft Entra Conditional Access deployment - Microsoft Entra ID | Microsoft Learn

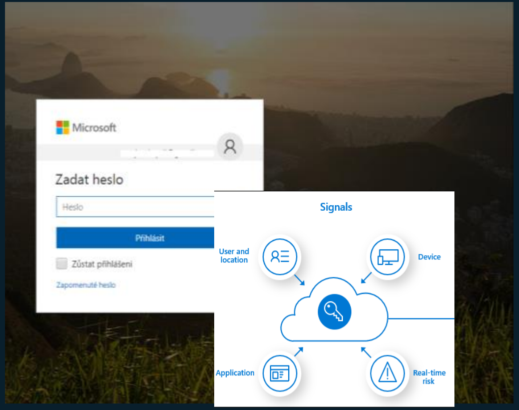
DEMO: CA creation and test

- Block legacy authentication
- Require STRONG authentication for global admins
- Require multifactor authentication for all users, for guests
- Require multifactor authentication for Azure management
- Block access from untrusted location - We consider each other location except your RDP machine as an untrusted
- Secure MFA and self-service password reset registration
- Block any platfrorm except Android, Ios, MACOS and Windows

Important cases



Allow nebo deny????



Microsoft

Zadat heslo

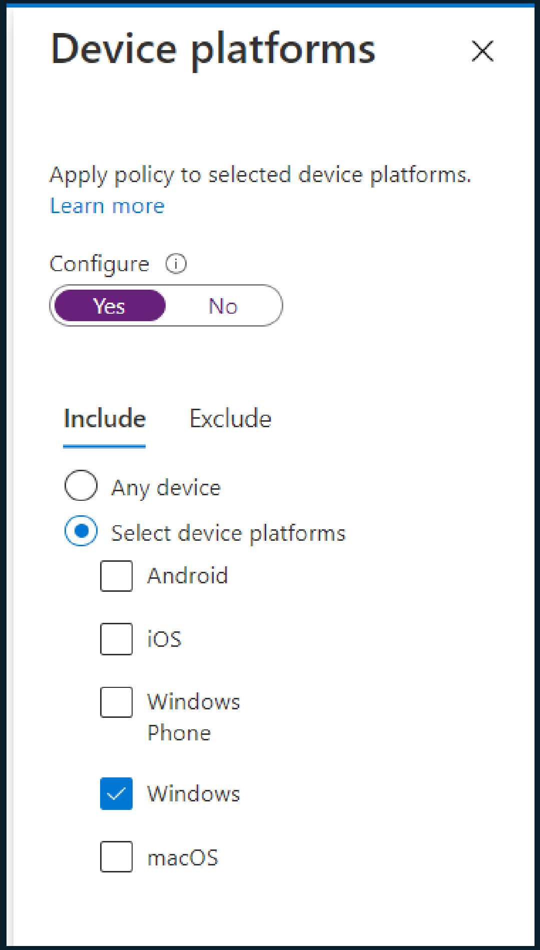
Heslo

Přihlásit

□ Zůstat přihlášeni

Zapomenuté heslo

Forgotten cases



Device platforms ✕

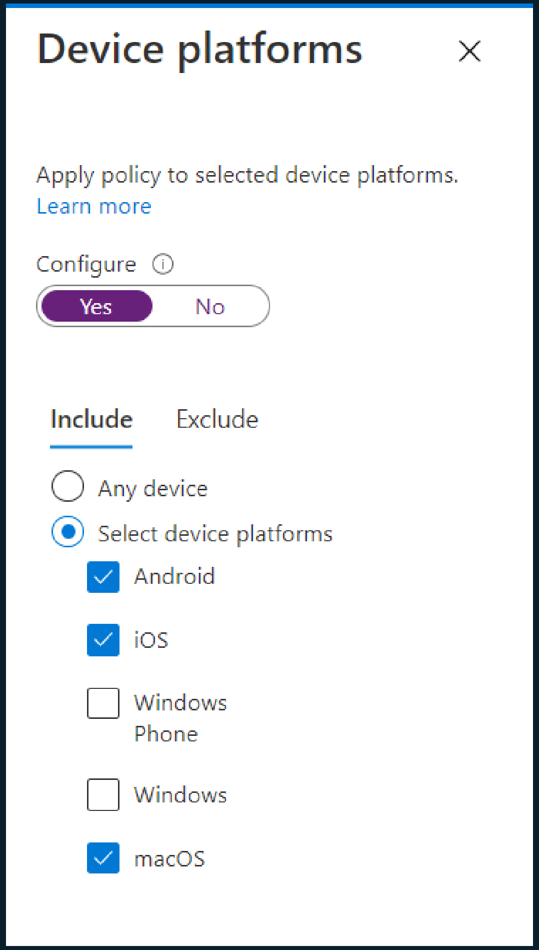
Apply policy to selected device platforms.
Learn more

Configure ⓘ

[✓ Yes] No

Include | Exclude

○ Any device
● Select device platforms
□ Android
□ iOS
□ Windows Phone
☑ Windows
□ macOS



Device platforms ✕

Apply policy to selected device platforms.
Learn more

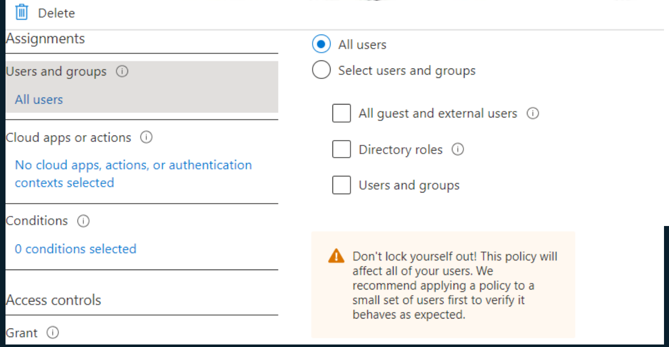
Configure ⓘ

[✓ Yes] No

Include | Exclude

○ Any device
● Select device platforms
☑ Android
☑ iOS
□ Windows Phone
□ Windows
☑ macOS

Attention – don´t forget exceptions



Delete

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

● All users

○ Select users and groups

□ All guest and external users ⓘ

□ Directory roles ⓘ

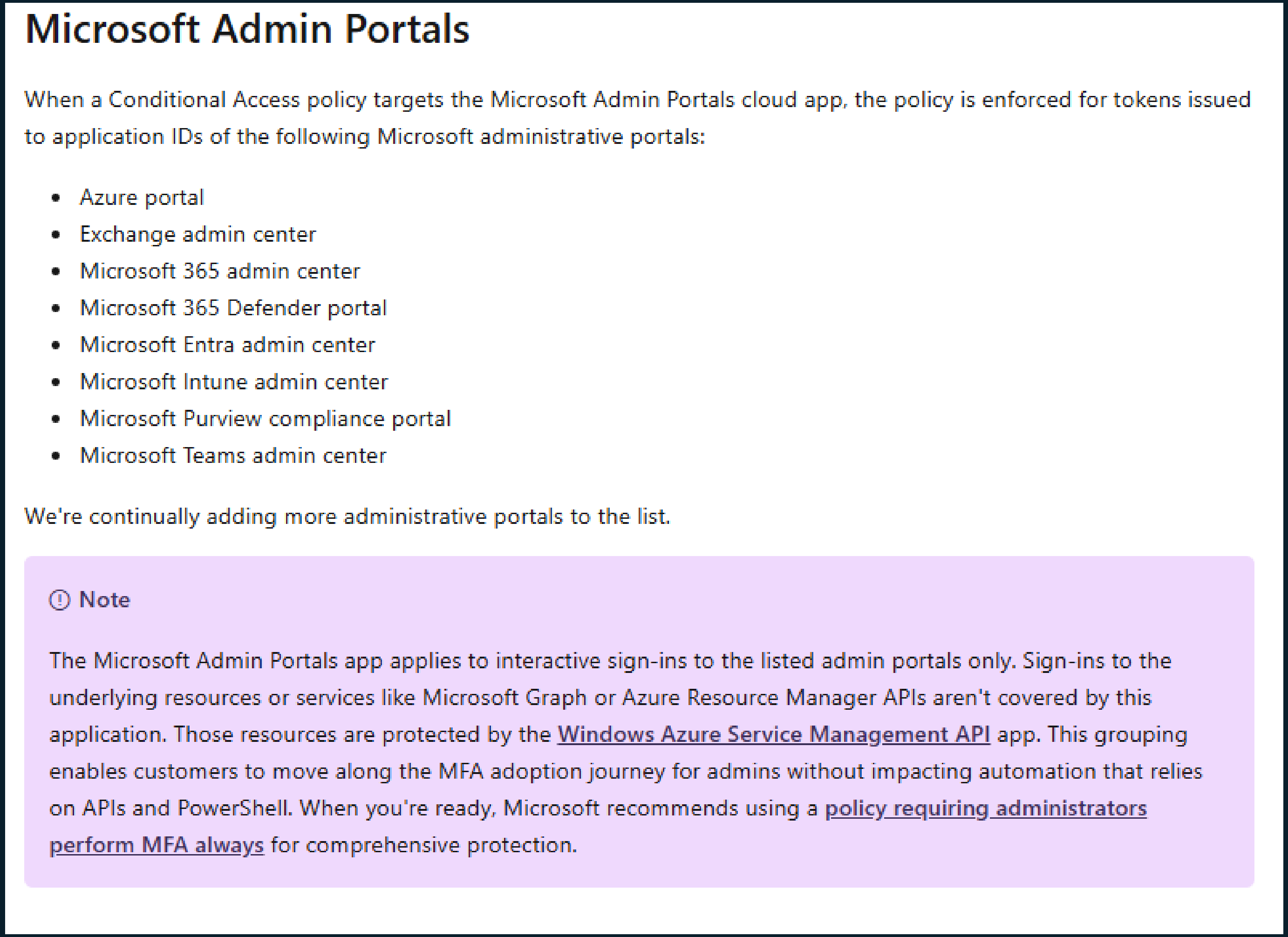
□ Users and groups

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

http://www.podnikani4u.eu/jste-pripraveni-podnikat-aneb-jak-si-pod-sebou-nepodrezat-vetev/d-1056

- Emergency accounts are always in exceptions!!!
- Consider service accounts and external accounts as an exception from specific conditional access policies

Microsoft admin portals term



Microsoft Admin Portals

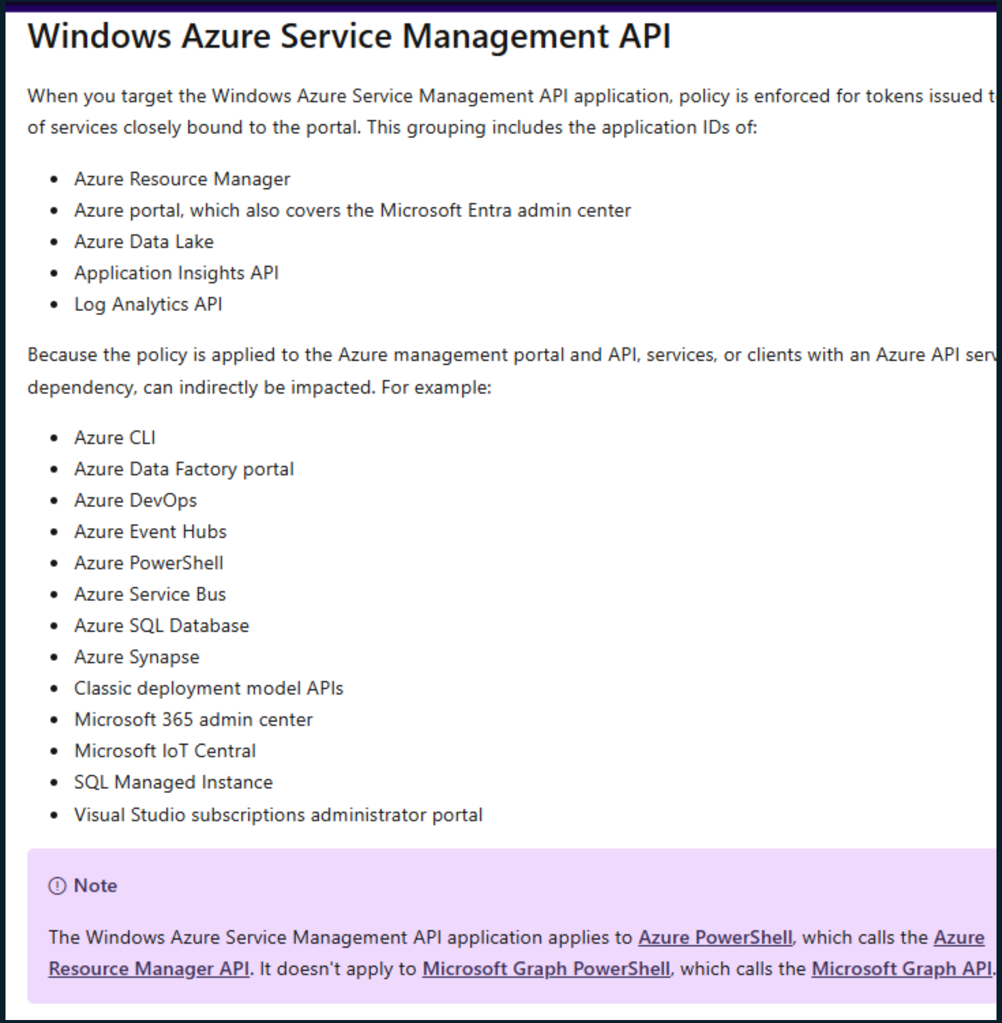
When a Conditional Access policy targets the Microsoft Admin Portals cloud app, the policy is enforced for tokens issued to application IDs of the following Microsoft administrative portals:

- Azure portal
- Exchange admin center
- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Entra admin center
- Microsoft Intune admin center
- Microsoft Purview compliance portal
- Microsoft Teams admin center

We're continually adding more administrative portals to the list.

ⓘ Note

The Microsoft Admin Portals app applies to interactive sign-ins to the listed admin portals only. Sign-ins to the underlying resources or services like Microsoft Graph or Azure Resource Manager APIs aren't covered by this application. Those resources are protected by the Windows Azure Service Management API app. This grouping enables customers to move along the MFA adoption journey for admins without impacting automation that relies on APIs and PowerShell. When you're ready, Microsoft recommends using a policy requiring administrators perform MFA always for comprehensive protection.



Windows Azure Service Management API

When you target the Windows Azure Service Management API application, policy is enforced for tokens issued t of services closely bound to the portal. This grouping includes the application IDs of:

- Azure Resource Manager
- Azure portal, which also covers the Microsoft Entra admin center
- Azure Data Lake
- Application Insights API
- Log Analytics API

Because the policy is applied to the Azure management portal and API, services, or clients with an Azure API serv dependency, can indirectly be impacted. For example:

- Azure CLI
- Azure Data Factory portal
- Azure DevOps
- Azure Event Hubs
- Azure PowerShell
- Azure Service Bus
- Azure SQL Database
- Azure Synapse
- Classic deployment model APIs
- Microsoft 365 admin center
- Microsoft IoT Central
- SQL Managed Instance
- Visual Studio subscriptions administrator portal

ⓘ Note

The Windows Azure Service Management API application applies to Azure PowerShell, which calls the Azure Resource Manager API. It doesn't apply to Microsoft Graph PowerShell, which calls the Microsoft Graph API.

Microsoft Security

What about Entra ID P2?

PIM

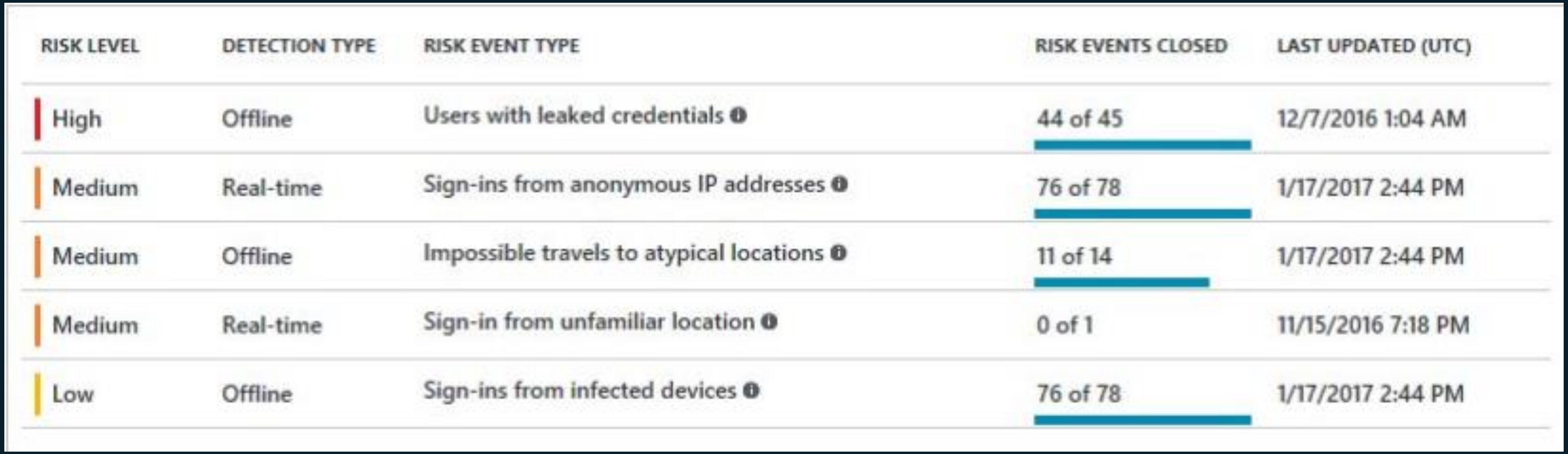
- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit
- Prevents removal of the **last active Global Administrator** role assignment
- Supporting for Azure AD and Azure roles

PIM DESIGN EXAMPLE

Role name	Require MFA	Notification	Require approval	Activation duration
Global Administrator	Yes	Yes	Yes	1 hour
Security Administrator	Yes	Yes	Yes	4 hours
Security Reader	Yes	Yes	No	8 hours
Compliance administrator	Yes	Yes	Yes	4 hours
Exchange administrator	Yes	Yes	Yes	2 hours
SharePoint administrator	Yes	No	No	4 hours
Teams administrator	Yes	No	No	4 hours
User administrator	Yes	Yes	No	2 hours
Global reader	Yes	Yes	No	8 hours
Reports reader	No	No	No	2 hours
Helpdesk administrator	No	No	No	2 hours
Billing administrator	Yes	No	No	2 hours
License administrator	No	No	No	2 hours
Intune administrator	Yes	No	No	4 hours
eDiscovery Manager	Yes	Yes	Yes	2 hours
eDiscovery Administrator	Yes	Yes	Yes	2 hours
Service Support Administrator	-	-	-	Permanently
Message center reader	-	-	-	Permanently
Customer Lockbox access approver	-	-	-	Permanently

DEMO: PIM – global reader for student7

ENTRA ID PROTECTION – AI POWERED IDENTITY PROTECTION



RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials	44 of 45	12/7/2016 1:04 AM
Medium	Real-time	Sign-ins from anonymous IP addresses	76 of 78	1/17/2017 2:44 PM
Medium	Offline	Impossible travels to atypical locations	11 of 14	1/17/2017 2:44 PM
Medium	Real-time	Sign-in from unfamiliar location	0 of 1	11/15/2016 7:18 PM
Low	Offline	Sign-ins from infected devices	76 of 78	1/17/2017 2:44 PM

Image source: https://danielchronlund.com/2019/02/27/top-security-logs-and-reports-in-office-365-and-azure-ad/

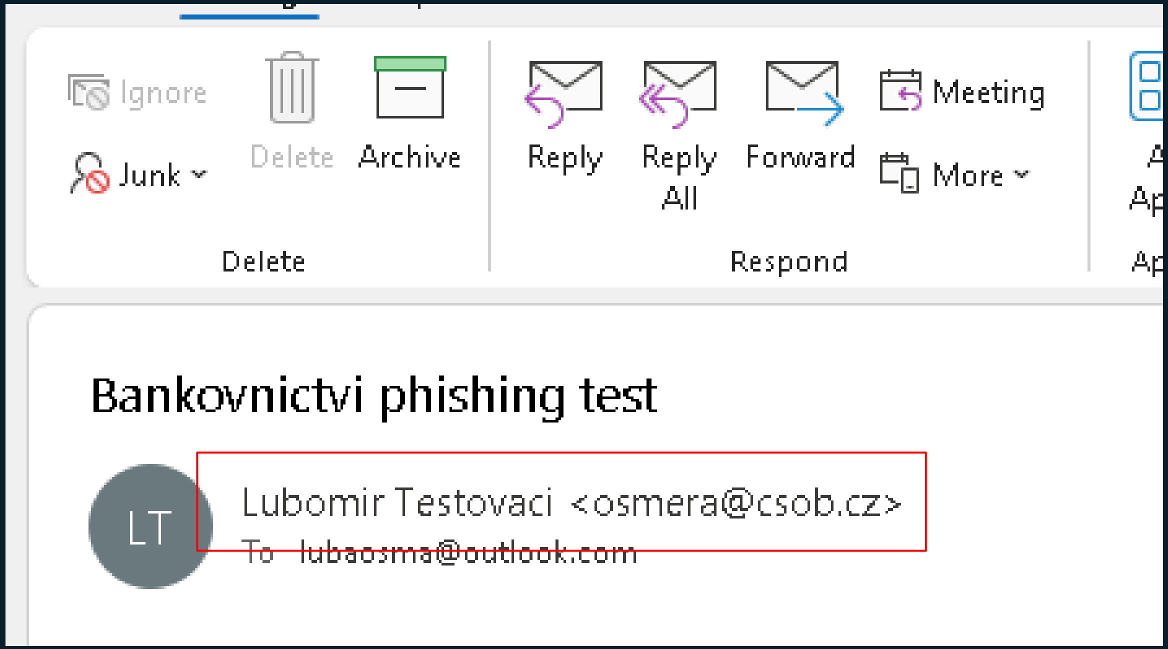
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

Microsoft Security

Office 365 apps security and Defender for Office 365

Addressing issues with phishing and spam should be a top priority for partners…

Basic spoofing demo



Bankovnictvi phishing test

LT Lubomir Testovaci <osmera@csob.cz>

To lubaosma@outlook.com

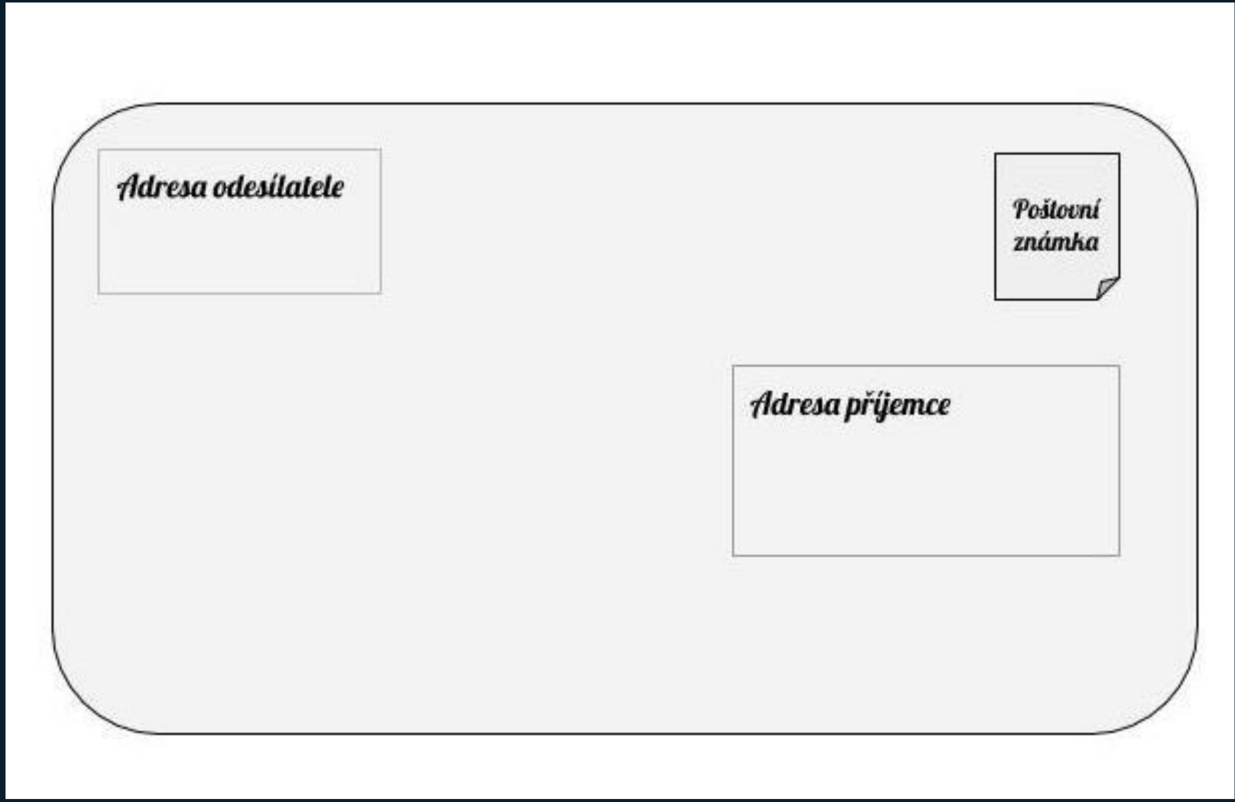
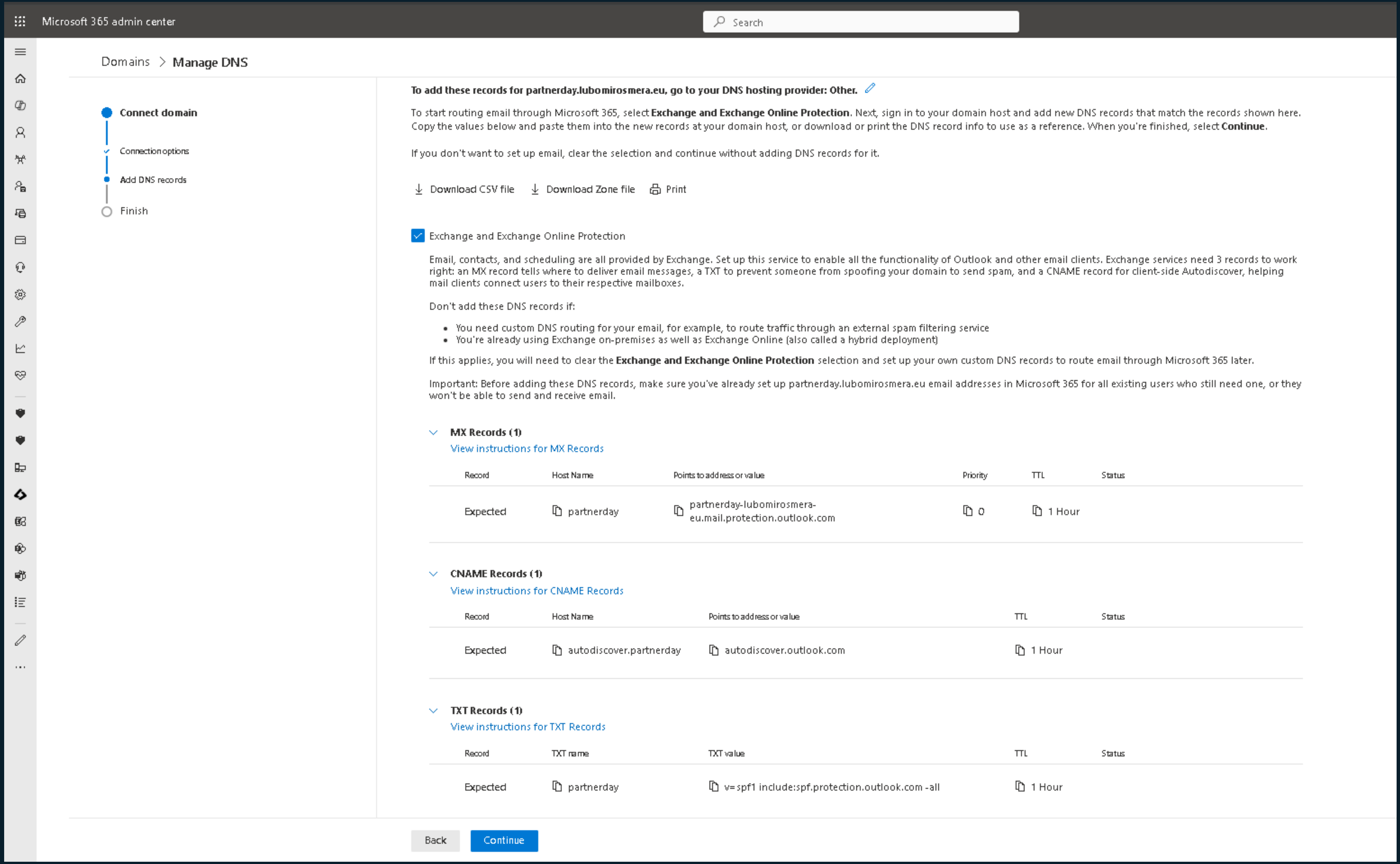


Image source:https://www.chaukiss.cz/blog/jak-spravne-nadepsat-obalku/

DNS records



To add these records for partnerday.lubomirosmera.eu, go to your DNS hosting provider: Other.

To start routing email through Microsoft 365, select **Exchange and Exchange Online Protection**. Next, sign in to your domain host and add new DNS records that match the records shown here. Copy the values below and paste them into the new records at your domain host, or download or print the DNS record info to use as a reference. When you're finished, select **Continue**.

If you don't want to set up email, clear the selection and continue without adding DNS records for it.

☑ Exchange and Exchange Online Protection

Email, contacts, and scheduling are all provided by Exchange. Set up this service to enable all the functionality of Outlook and other email clients. Exchange services need 3 records to work right: an MX record tells where to deliver email messages, a TXT to prevent someone from spoofing your domain to send spam, and a CNAME record for client-side Autodiscover, helping mail clients connect users to their respective mailboxes.

Don't add these DNS records if:

- You need custom DNS routing for your email, for example, to route traffic through an external spam filtering service
- You're already using Exchange on-premises as well as Exchange Online (also called a hybrid deployment)

If this applies, you will need to clear the **Exchange and Exchange Online Protection** selection and set up your own custom DNS records to route email through Microsoft 365 later.

Important: Before adding these DNS records, make sure you've already set up partnerday.lubomirosmera.eu email addresses in Microsoft 365 for all existing users who still need one, or they won't be able to send and receive email.

MX Records (1)

View instructions for MX Records

Record	Host Name	Points to address or value	Priority	TTL	Status
Expected	partnerday	partnerday-lubomirosmera-eu.mail.protection.outlook.com	0	1 Hour	

CNAME Records (1)

View instructions for CNAME Records

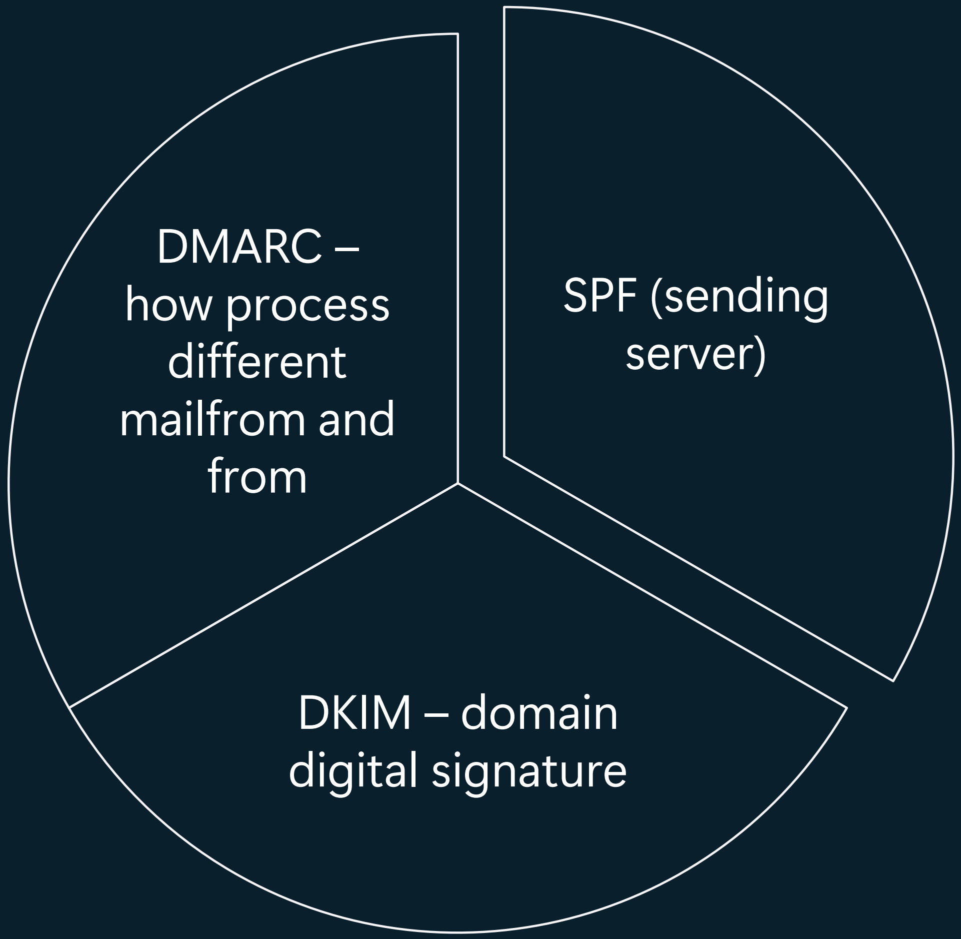
Record	Host Name	Points to address or value	TTL	Status
Expected	autodiscover.partnerday	autodiscover.outlook.com	1 Hour	

TXT Records (1)

View instructions for TXT Records

Record	TXT name	TXT value	TTL	Status
Expected	partnerday	v=spf1 include:spf.protection.outlook.com -all	1 Hour	

Message explicit authentication

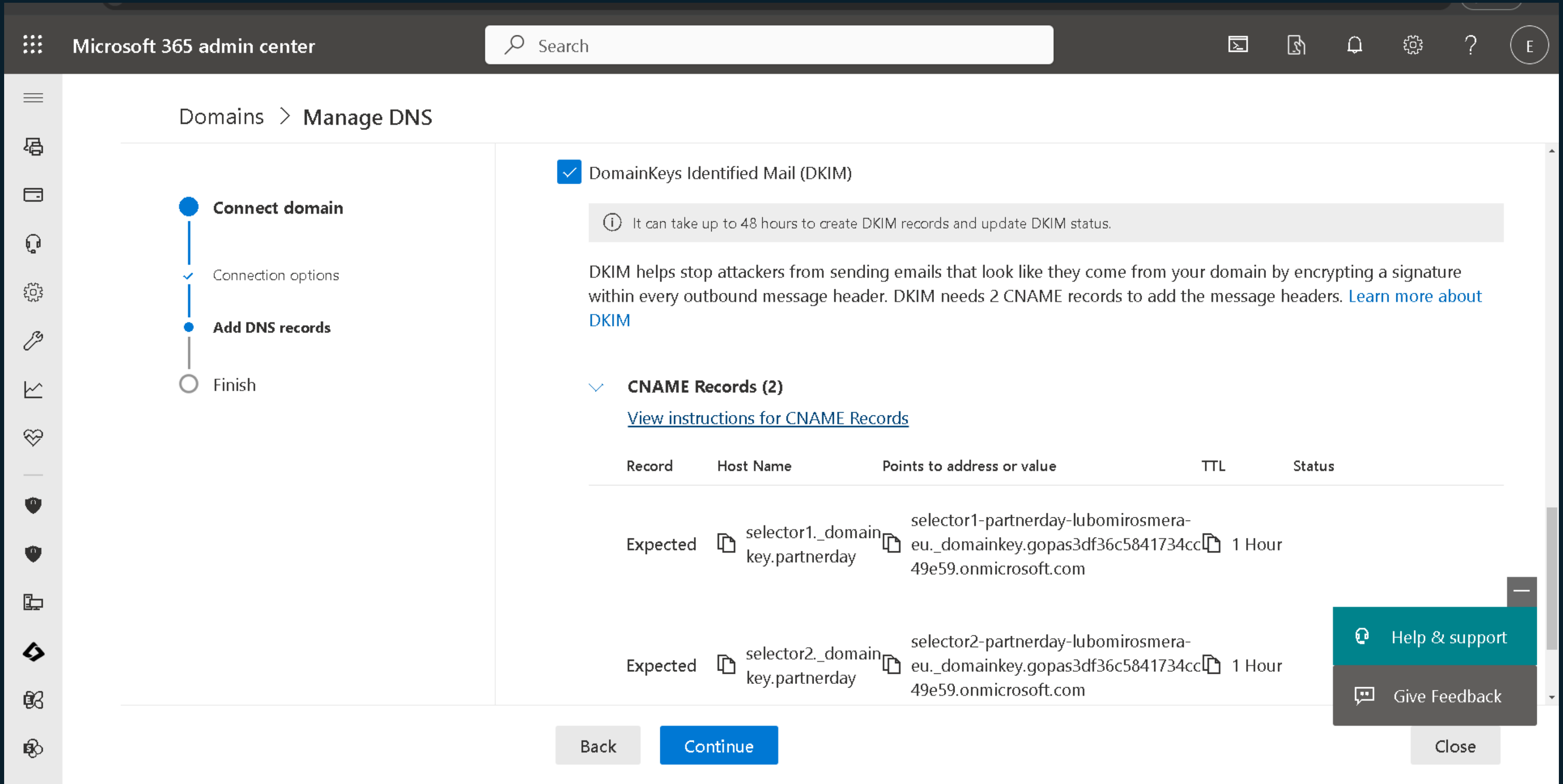


DMARC – how process different mailfrom and from

SPF (sending server)

DKIM – domain digital signature

DKIM DNS records



Domains > Manage DNS

- Connect domain
- ✓ Connection options
- ● Add DNS records
- ○ Finish

☑ DomainKeys Identified Mail (DKIM)

ⓘ It can take up to 48 hours to create DKIM records and update DKIM status.

DKIM helps stop attackers from sending emails that look like they come from your domain by encrypting a signature within every outbound message header. DKIM needs 2 CNAME records to add the message headers. Learn more about DKIM

CNAME Records (2)

View instructions for CNAME Records

Record	Host Name	Points to address or value	TTL	Status
Expected	selector1._domainkey.partnerday	selector1-partnerday-lubomirosmera-eu._domainkey.gopas3df36c5841734cc49e59.onmicrosoft.com	1 Hour	
Expected	selector2._domainkey.partnerday	selector2-partnerday-lubomirosmera-eu._domainkey.gopas3df36c5841734cc49e59.onmicrosoft.com	1 Hour	

Back   Continue   Close

Extend DMARC and SPF protection to other domains not used for email

- enable DMARC and SPF for all domains even if they parked or not currently used for email
- For domains that do not send mail, you can protect them with an SPF record that hard fails all senders. For example, “v=spf1 –all”.

Enable Unified Audit Log

https://purview.microsoft.com/audit/

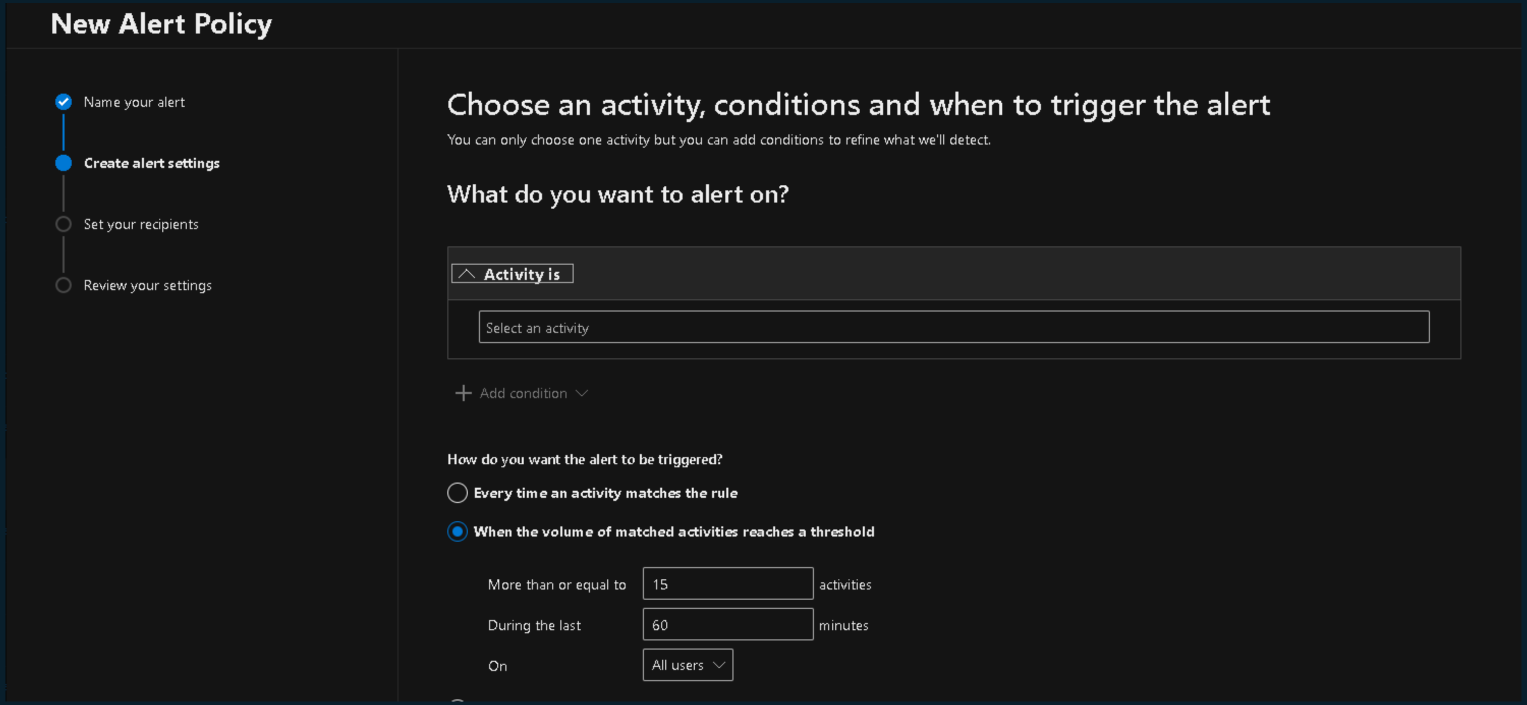
User and admin activity from your organization is recorded in the audit log and automatically retained for 180 days

https://learn.microsoft.com/en-us/purview/audit-log-enable-disable?tabs=microsoft-purview-portal

Enable alert policies

- https://security.microsoft.com/alertpoliciesv2

- How to create custom rules? Based on logs and conditionas - whatever



New Alert Policy

Choose an activity, conditions and when to trigger the alert

You can only choose one activity but you can add conditions to refine what we'll detect.

What do you want to alert on?

Activity is

Select an activity

How do you want the alert to be triggered?

○ Every time an activity matches the rule

● When the volume of matched activities reaches a threshold

More than or equal to 15 activities

During the last 60 minutes

On All users

Email security configuration

- https://security.microsoft.com/threatpolicy

EOP filtering

Microsoft 365 Security for IT Pros (2022-edition) https://m365security.gumroad.com/l/DiRFK

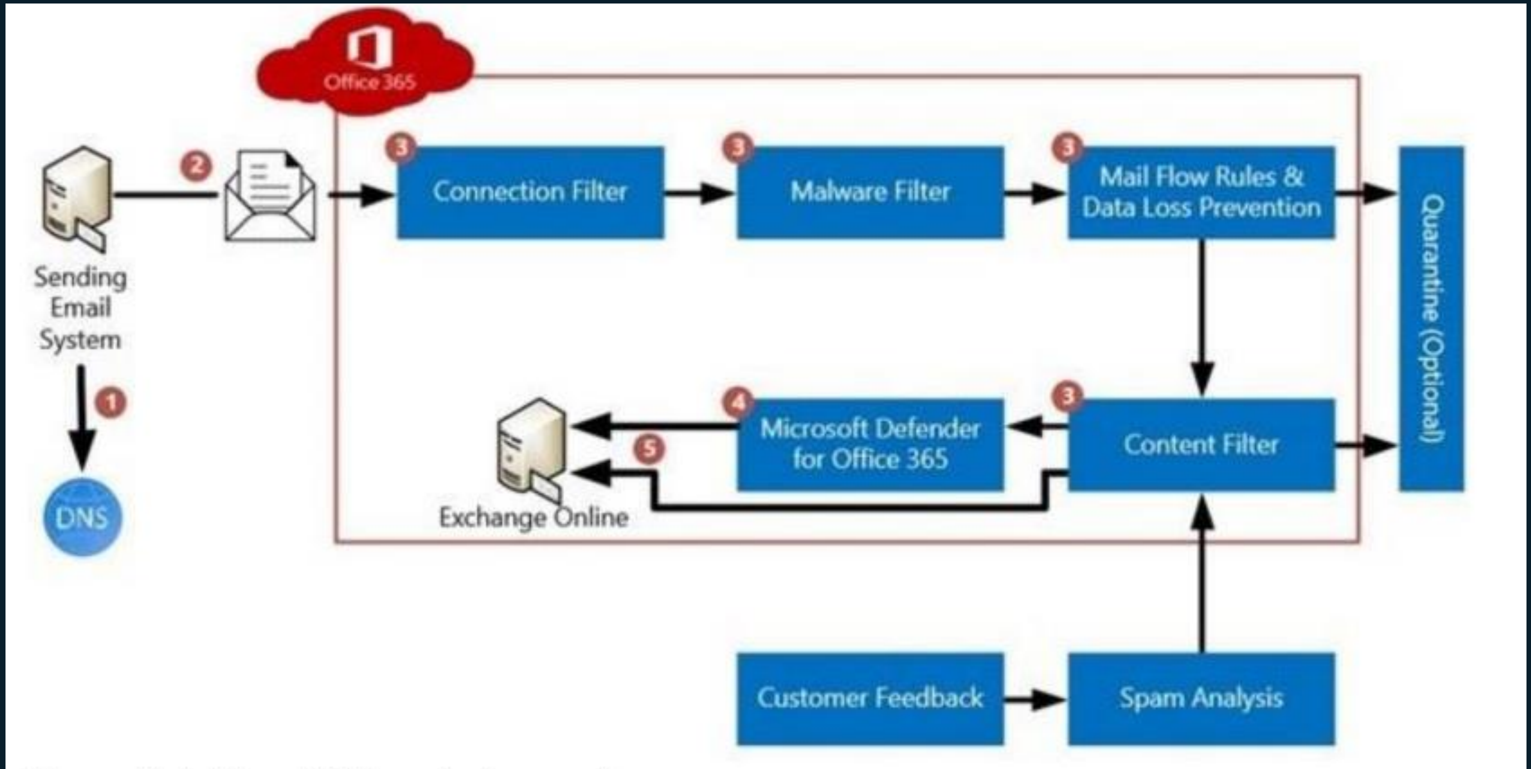


Figure 7-5: How EOP protects email

Block all executable email attachments

- https://www.threatdown.com/blog/emotet-adopts-microsoft-onenote-attachments/
- Encrypted ZIP consideration

Enable preset security policy

EOP

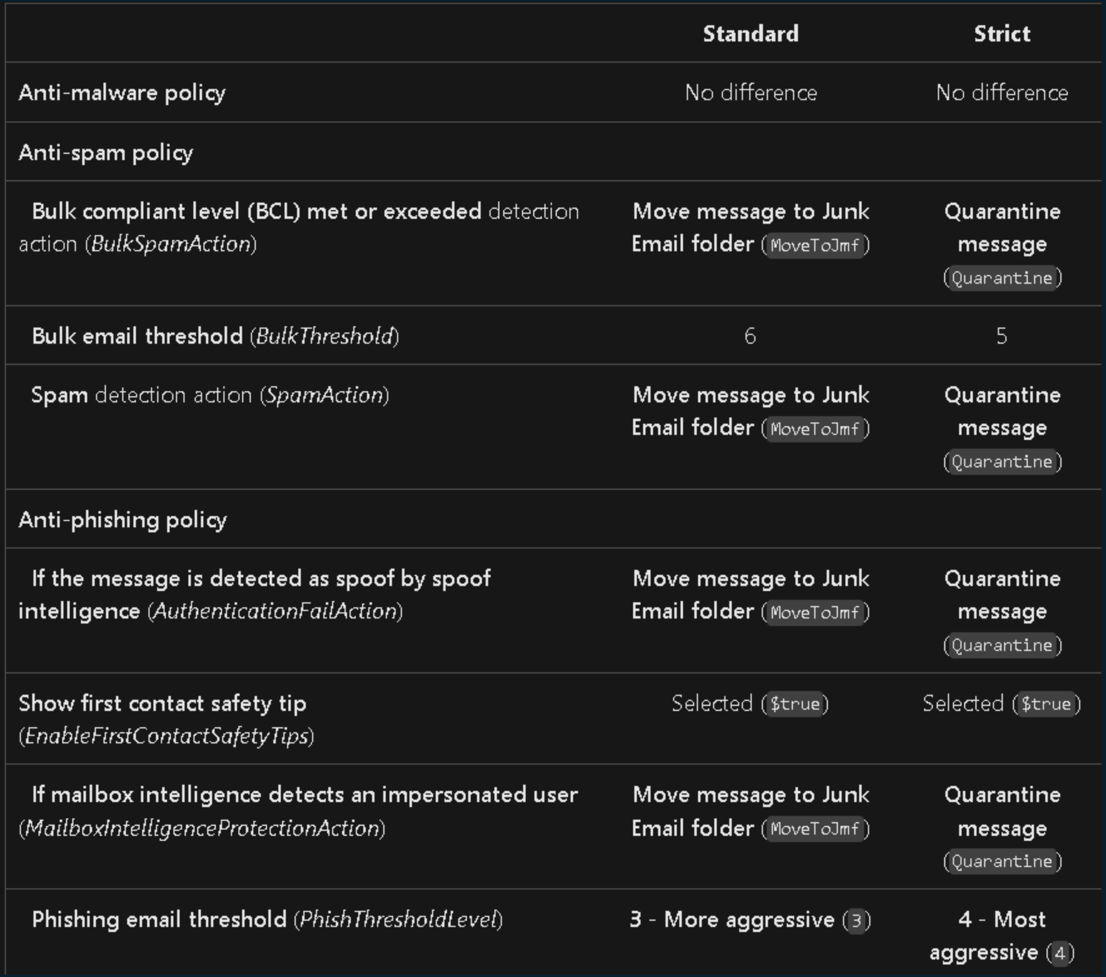
- ANTISPAM
- ANTIMALWARE
- ANTIPHISHING

Defender for Office 365

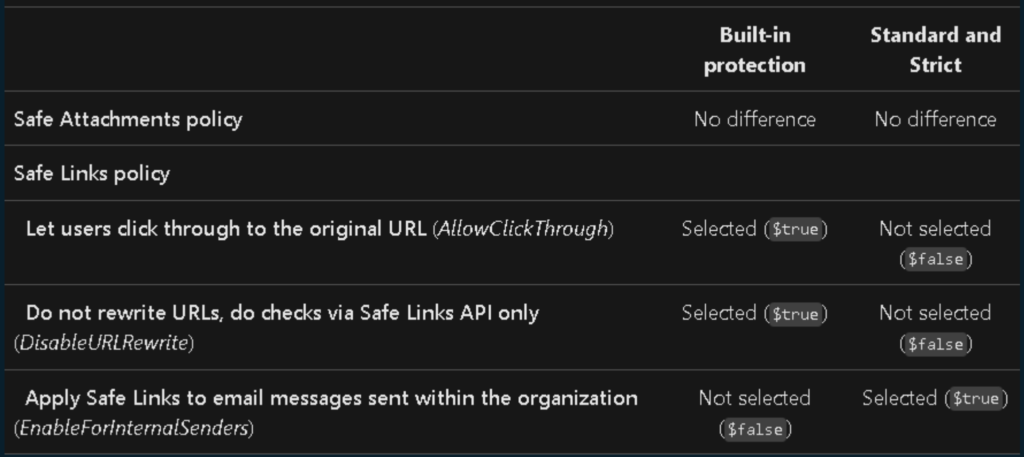
- Advanced Antiphishing
- Safe links

.. Safe Attachments

Standard – for all users, consider strict for sensitive accounts



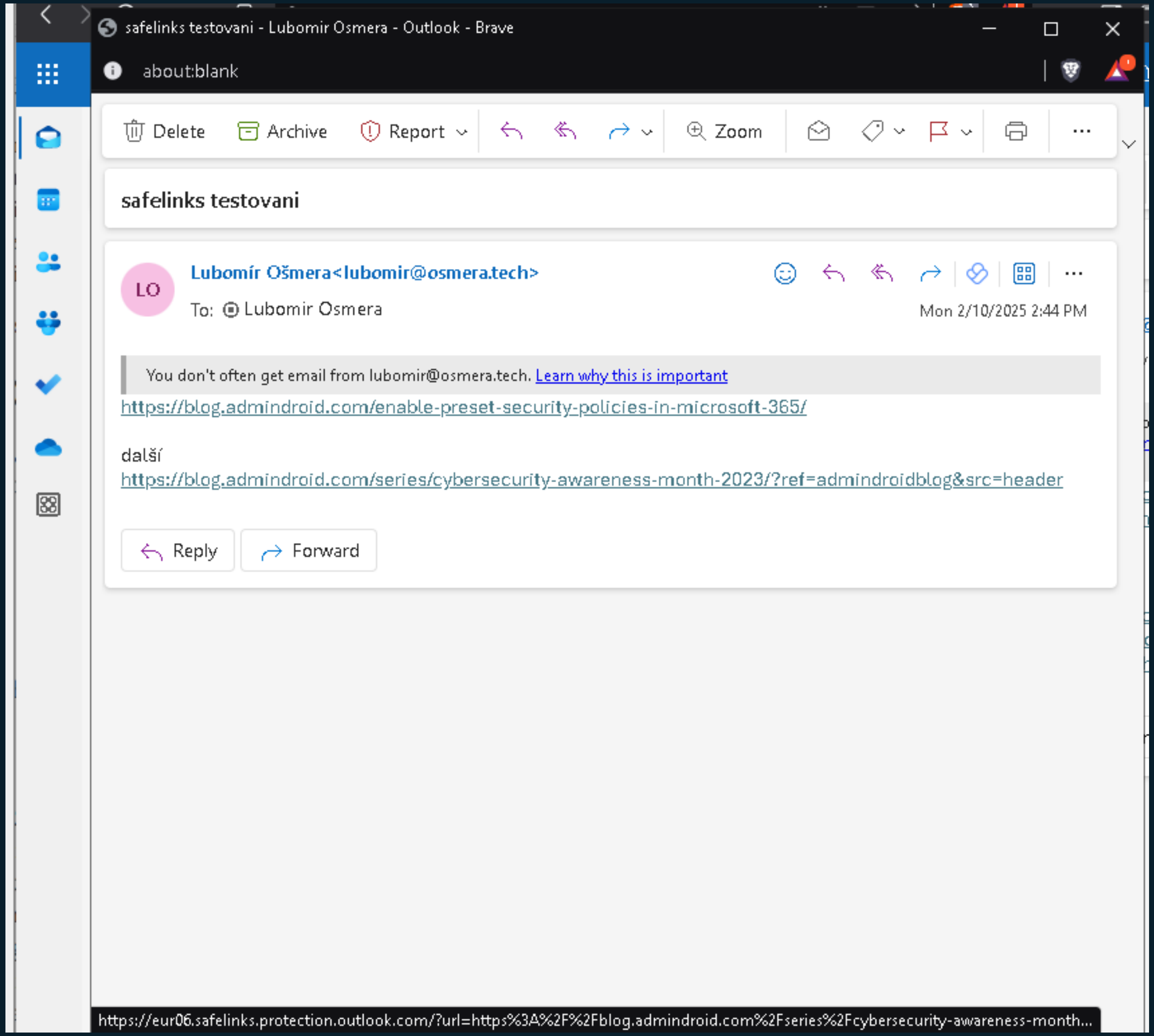
	Standard	Strict
Anti-malware policy	No difference	No difference
Anti-spam policy		
Bulk compliant level (BCL) met or exceeded detection action (*BulkSpamAction*)	Move message to Junk Email folder (`MoveToJmf`)	Quarantine message (`Quarantine`)
Bulk email threshold (*BulkThreshold*)	6	5
Spam detection action (*SpamAction*)	Move message to Junk Email folder (`MoveToJmf`)	Quarantine message (`Quarantine`)
Anti-phishing policy		
If the message is detected as spoof by spoof intelligence (*AuthenticationFailAction*)	Move message to Junk Email folder (`MoveToJmf`)	Quarantine message (`Quarantine`)
Show first contact safety tip (*EnableFirstContactSafetyTips*)	Selected (`$true`)	Selected (`$true`)
If mailbox intelligence detects an impersonated user (*MailboxIntelligenceProtectionAction*)	Move message to Junk Email folder (`MoveToJmf`)	Quarantine message (`Quarantine`)
Phishing email threshold (*PhishThresholdLevel*)	3 - More aggressive (`3`)	4 - Most aggressive (`4`)



	Built-in protection	Standard and Strict
Safe Attachments policy	No difference	No difference
Safe Links policy		
Let users click through to the original URL (*AllowClickThrough*)	Selected (`$true`)	Not selected (`$false`)
Do not rewrite URLs, do checks via Safe Links API only (*DisableURLRewrite*)	Selected (`$true`)	Not selected (`$false`)
Apply Safe Links to email messages sent within the organization (*EnableForInternalSenders*)	Not selected (`$false`)	Selected (`$true`)

https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies?WT.mc_id=%3Fwt.mc_id%3DM365-MVP-33230#order-of-precedence-for-preset-security-policies-and-other-policies

Safe links demo



safelinks testovani - Lubomir Osmera - Outlook - Brave

about:blank

safelinks testovani

Lubomír Ošmera<lubomir@osmera.tech>

To: Lubomir Osmera

Mon 2/10/2025 2:44 PM

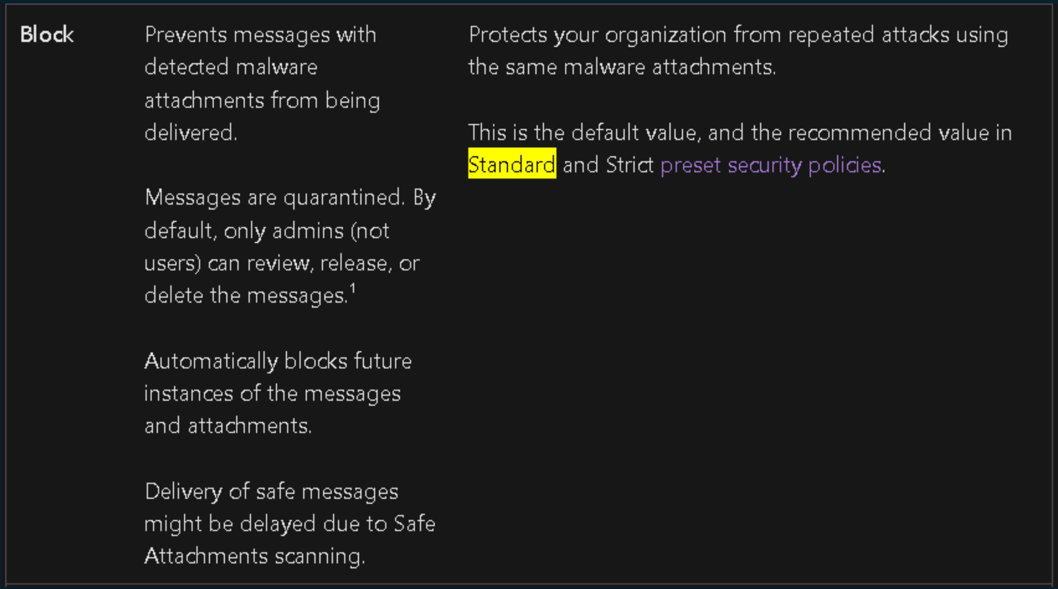
You don't often get email from lubomir@osmera.tech. Learn why this is important

https://blog.admindroid.com/enable-preset-security-policies-in-microsoft-365/

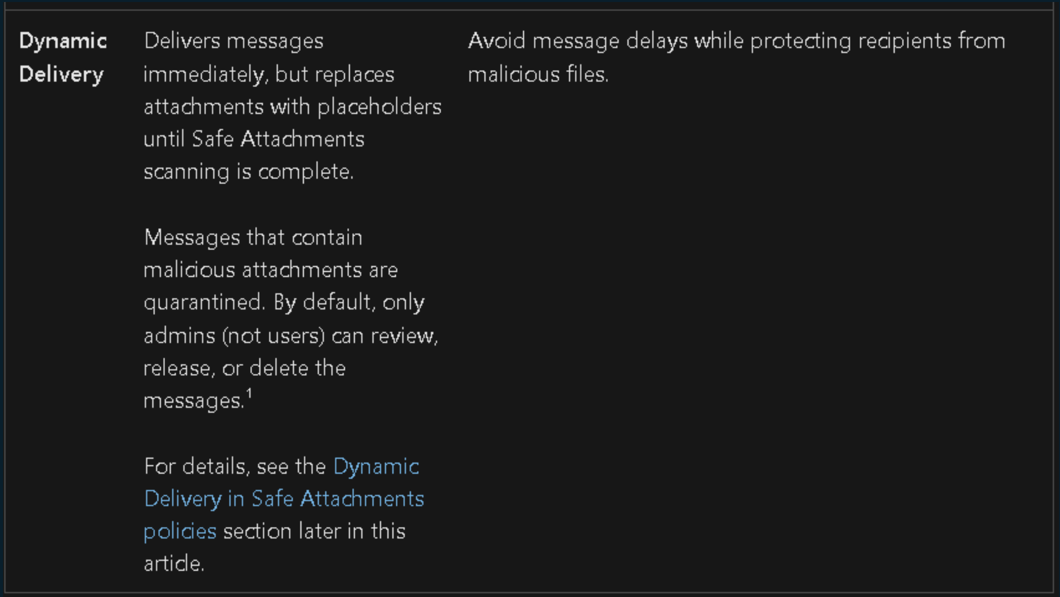
další
https://blog.admindroid.com/series/cybersecurity-awareness-month-2023/?ref=admindroidblog&src=header

https://eur06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fblog.admindroid.com%2Fseries%2Fcybersecurity-awareness-month...

Safe attachments demo

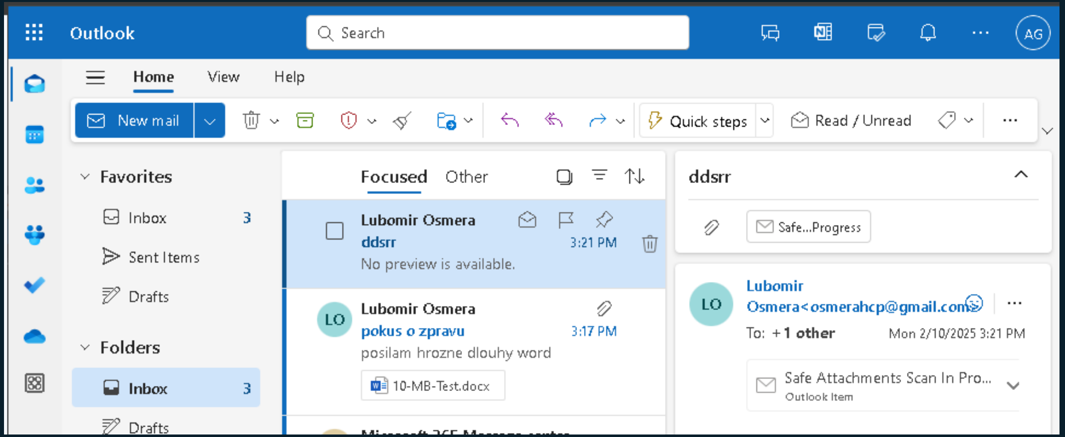


Block	Prevents messages with detected malware attachments from being delivered. Messages are quarantined. By default, only admins (not users) can review, release, or delete the messages.[1] Automatically blocks future instances of the messages and attachments. Delivery of safe messages might be delayed due to Safe Attachments scanning.	Protects your organization from repeated attacks using the same malware attachments. This is the default value, and the recommended value in Standard and Strict preset security policies.



Dynamic Delivery	Delivers messages immediately, but replaces attachments with placeholders until Safe Attachments scanning is complete. Messages that contain malicious attachments are quarantined. By default, only admins (not users) can review, release, or delete the messages.[1] For details, see the Dynamic Delivery in Safe Attachments policies section later in this article.	Avoid message delays while protecting recipients from malicious files.

https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-about



Lubomir Osmera
ddsrr
3:21 PM
No preview is available.

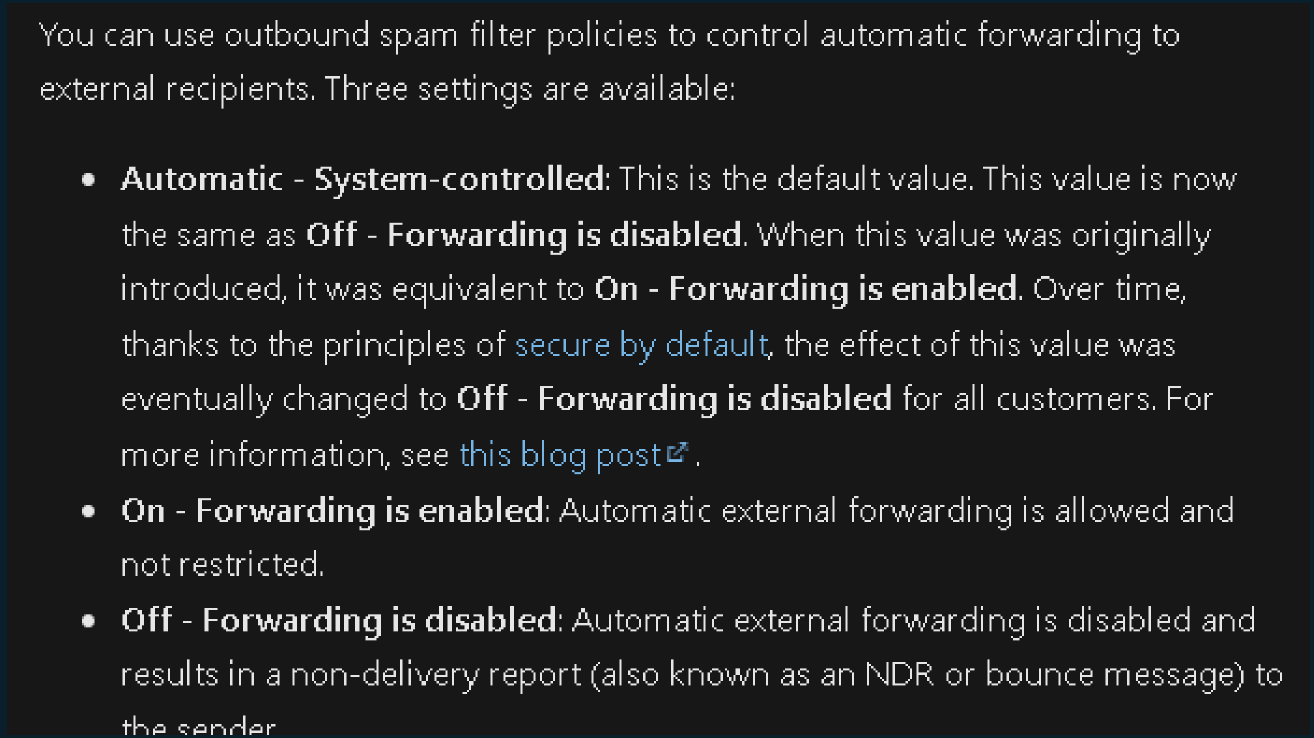
LO
Lubomir Osmera
pokus o zpravu
3:17 PM
posilam hrozne dlouhy word
10-MB-Test.docx

ddsrr
Safe...Progress

LO
Lubomir Osmera<osmerahcp@gmail.com>
To: +1 other
Mon 2/10/2025 3:21 PM

Safe Attachments Scan In Pro...
Outlook Item

Block autoforwarding outside the company



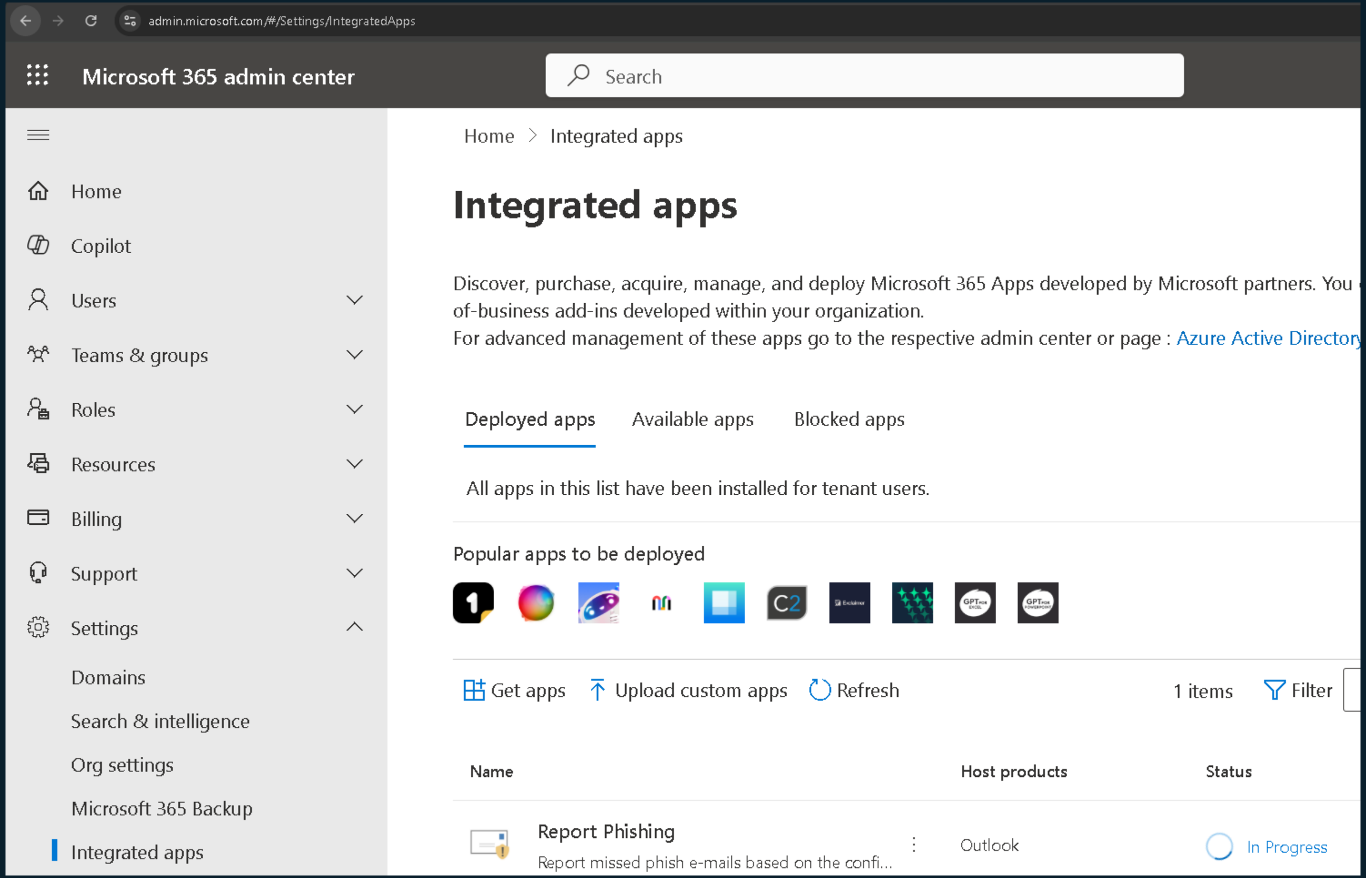
You can use outbound spam filter policies to control automatic forwarding to external recipients. Three settings are available:

- **Automatic - System-controlled**: This is the default value. This value is now the same as **Off - Forwarding is disabled**. When this value was originally introduced, it was equivalent to **On - Forwarding is enabled**. Over time, thanks to the principles of secure by default, the effect of this value was eventually changed to **Off - Forwarding is disabled** for all customers. For more information, see this blog post .
- **On - Forwarding is enabled**: Automatic external forwarding is allowed and not restricted.
- **Off - Forwarding is disabled**: Automatic external forwarding is disabled and results in a non-delivery report (also known as an NDR or bounce message) to the sender

https://security.microsoft.com/antispam

Respond to user Phishing reports

https://admin.microsoft.com/#/Settings/IntegratedApps



admin.microsoft.com/#/Settings/IntegratedApps

Microsoft 365 admin center

Search

Home > Integrated apps

Integrated apps

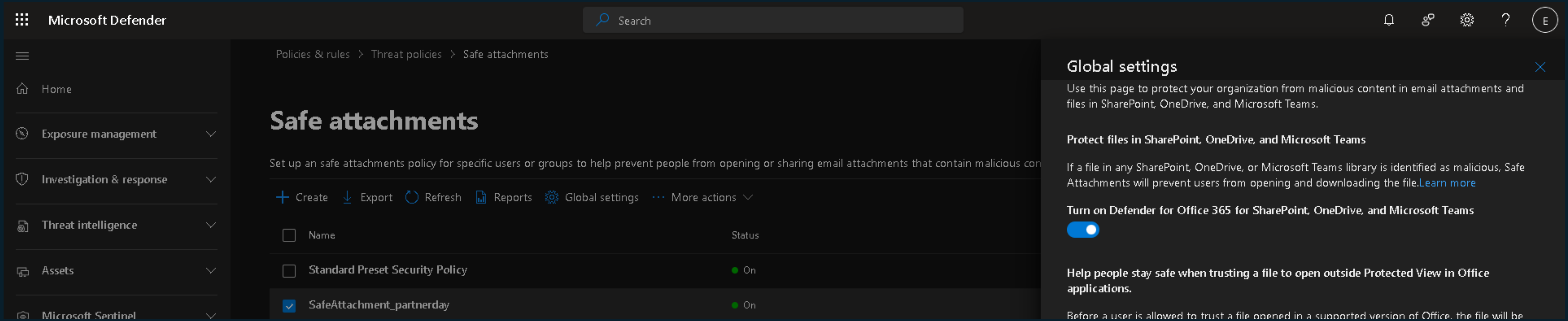
Discover, purchase, acquire, manage, and deploy Microsoft 365 Apps developed by Microsoft partners. You
of-business add-ins developed within your organization.
For advanced management of these apps go to the respective admin center or page : Azure Active Directory

All apps in this list have been installed for tenant users.

Popular apps to be deployed

Name	Host products	Status
Report Phishing Report missed phish e-mails based on the confi...	Outlook	In Progress

Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams



Safe attachments

Set up an safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments that contain malicious con

	Name	Status
□	Standard Preset Security Policy	● On
☑	SafeAttachment_partnerday	● On

Global settings

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.

Protect files in SharePoint, OneDrive, and Microsoft Teams

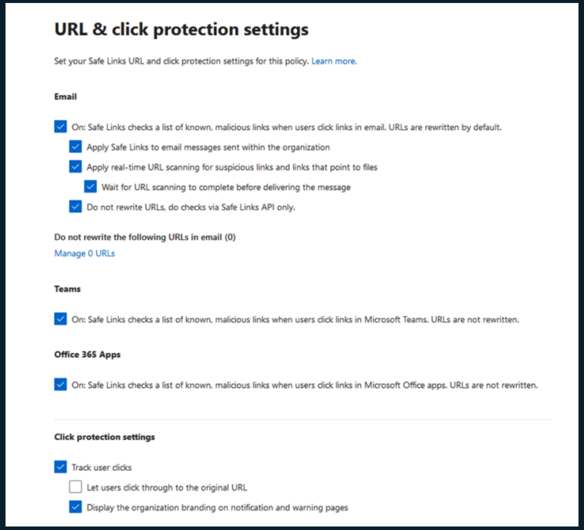
If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, Safe Attachments will prevent users from opening and downloading the file.Learn more

Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams

● On

Help people stay safe when trusting a file to open outside Protected View in Office applications.

Before a user is allowed to trust a file opened in a supported version of Office, the file will be



URL & click protection settings

Set your Safe Links URL and click protection settings for this policy. Learn more.

Email

- ☑ On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.
  - ☑ Apply Safe Links to email messages sent within the organization
  - ☑ Apply real-time URL scanning for suspicious links and links that point to files
    - ☑ Wait for URL scanning to complete before delivering the message
  - ☑ Do not rewrite URLs, do checks via Safe Links API only.

Do not rewrite the following URLs in email (0)

Manage 0 URLs

Teams

☑ On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten.

Office 365 Apps

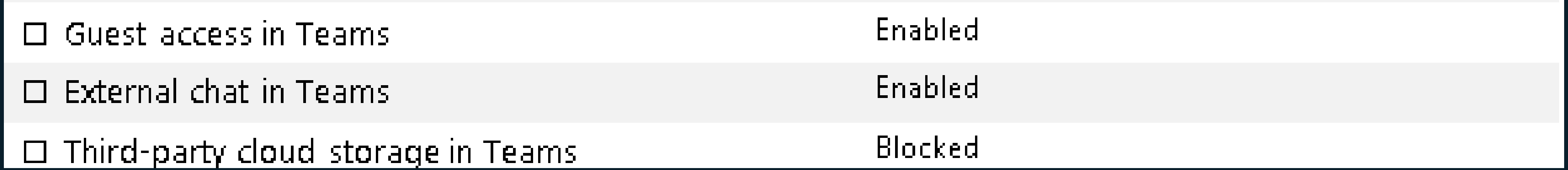
☑ On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten.

Click protection settings

- ☑ Track user clicks
  - □ Let users click through to the original URL
  - ☑ Display the organization branding on notification and warning pages

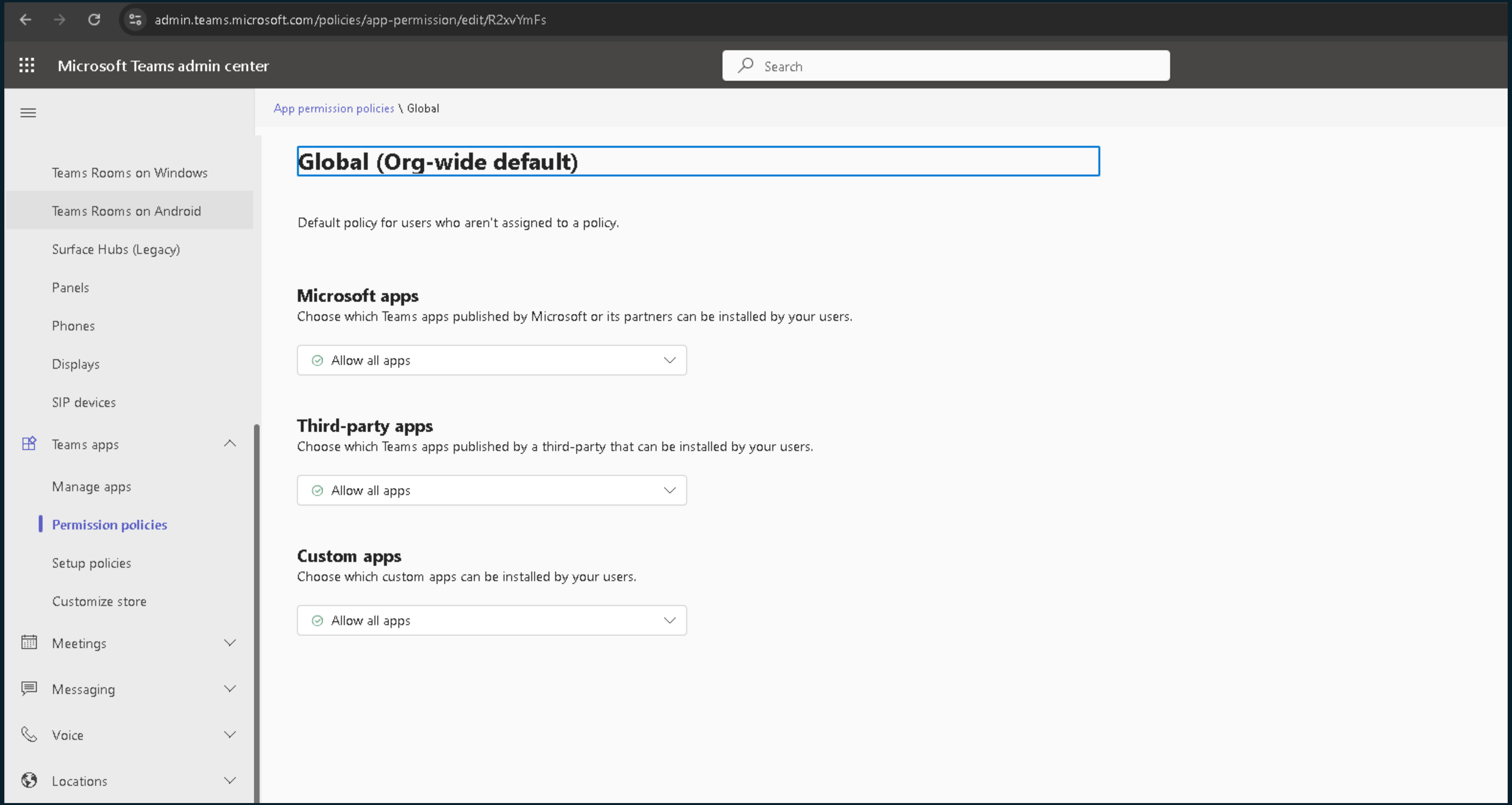
Some Teams security policies

- https://admin.teams.microsoft.com/company-wide-settings/external-communications
- https://admin.teams.microsoft.com/company-wide-settings/guest-configuration
- https://admin.teams.microsoft.com/company-wide-settings/teams-settings



□ Guest access in Teams	Enabled
□ External chat in Teams	Enabled
□ Third-party cloud storage in Teams	Blocked

Disable 3rd party & custom apps in Teams



App permission policies \ Global

Global (Org-wide default)

Default policy for users who aren't assigned to a policy.

Microsoft apps

Choose which Teams apps published by Microsoft or its partners can be installed by your users.

Allow all apps

Third-party apps

Choose which Teams apps published by a third-party that can be installed by your users.

Allow all apps

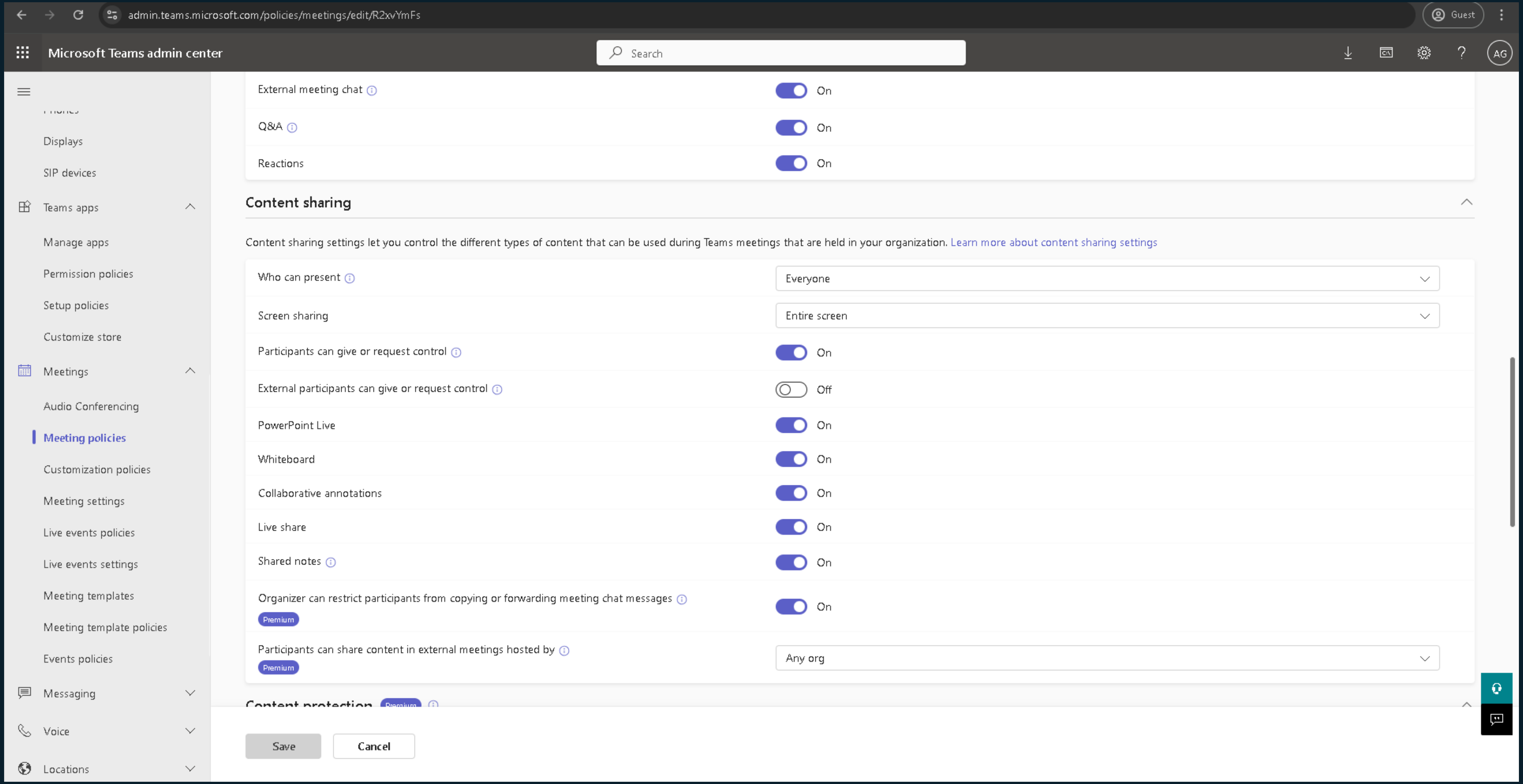
Custom apps

Choose which custom apps can be installed by your users.

Allow all apps

https://admin.teams.microsoft.com/policies/app-permission/

Customize Teams meeting settings



External meeting chat: On

Q&A: On

Reactions: On

Content sharing

Content sharing settings let you control the different types of content that can be used during Teams meetings that are held in your organization. Learn more about content sharing settings

Who can present	Everyone
Screen sharing	Entire screen
Participants can give or request control	On
External participants can give or request control	Off
PowerPoint Live	On
Whiteboard	On
Collaborative annotations	On
Live share	On
Shared notes	On
Organizer can restrict participants from copying or forwarding meeting chat messages (Premium)	On
Participants can share content in external meetings hosted by (Premium)	Any org

Content protection Premium

https://admin.teams.microsoft.com/policies/meetings/edit/R2xvYmFs

Courses and certifications

- Microsoft 365 security - basics
  - SC-900 https://www.gopas.cz/microsoft-365-zaklady-zabezpeceni-spravy-identit-a-souladu_moc-sc-900
- Microsoft 365 identity and access security - advanced
  - SC-300 https://www.gopas.cz/microsoft-365-sprava-uctu-overovani-uzivatelu-a-rizeni-pristupu_moc-sc-300
- Gopas custom courses
  - Microsoft hybrid security:
    - GOC215 https://www.gopas.cz/microsoft-365-bezpecnost-hybridniho-prostredi_goc215
  - Microsoft 365 / Microsoft Azure hacking
    - GOC238 https://www.gopas.cz/microsoft-azure-hacking-a-penetracni-testovani_goc238

Microsoft Security

Microsoft Partner Security Day

Praha, 11. 2. 2025

ALSO ARROW TD SYNNEX GOPAS Microsoft system4u