



# Key Security Controls in Microsoft 365

# About Me

Brian Greidanus

[bgreidan@telasasecurity.com](mailto:bgreidan@telasasecurity.com)

- 25 years of security and compliance experience delivering consulting and managed services to enterprises, governments, and education.
- Current focus:
  - Strategic and technical consulting
  - Cloud security architecture and assessment

# Presentation Outline

- Current Threat Landscape for Microsoft 365
- Key Security Controls in Entra ID
- General M365 Security Controls
- Key Security Controls in Exchange Online
- Key Security Controls in SharePoint Online
- Key Security Controls in Microsoft Teams
- Key Security Controls in Microsoft Copilot



# Current Threat Landscape for Microsoft 365

## Section Outline

- Recent Incident Walkthrough
- Modern Phishing Attacks and Attacks Against MFA

# Recent Incident Walkthrough

# Story of a Disclosed Incident

- Beginning in late November 2023, a threat actor used a password spray attack to compromise a legacy non-production test Microsoft Entra ID tenant account and gain a foothold (guessable password, no MFA was in place).
- Attacker was able to use OAUTH application to pivot from the test tenant to the production corporate environment.
- Corporate email accounts were accessed, including members of senior leadership team and employees in cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents.

# What went wrong?

Quite a bit!!

Two areas where we can infer insecure practices by victim:

- Area 1 – Insecure practices in the test tenant
- Area 2 – Insecure practices in the boundary between test and production

Following slides are our understanding of what exactly happened.



# Insecure Practices in Test Tenant

## Insecure practices in Test Tenant

- Stale test tenant – tenant likely should have been decommissioned
- No MFA
- Guessable passwords
- No/unmonitored user risk detection
- No/ineffective Entra ID Conditional Access Policies
- No Privileged Identity Management for highly privileged account
- Highly privileged legacy OAUTH application
- Tenant appears to not have been monitored at all

# Insecure practices at Test/Production boundary

Insecure practices at test/production boundary:

- Test tenant application with permissions to access production
- Test application granted highly privileged roles in production environment
- No monitoring or auditing of cross-tenant permissions or activities
- Ineffective detection of new admin account creation
- Ineffective detection of application consent grant
- Ineffective detection of new Service Principal creation

# Who Was This Victim?

Anyone know the victim in this attack?

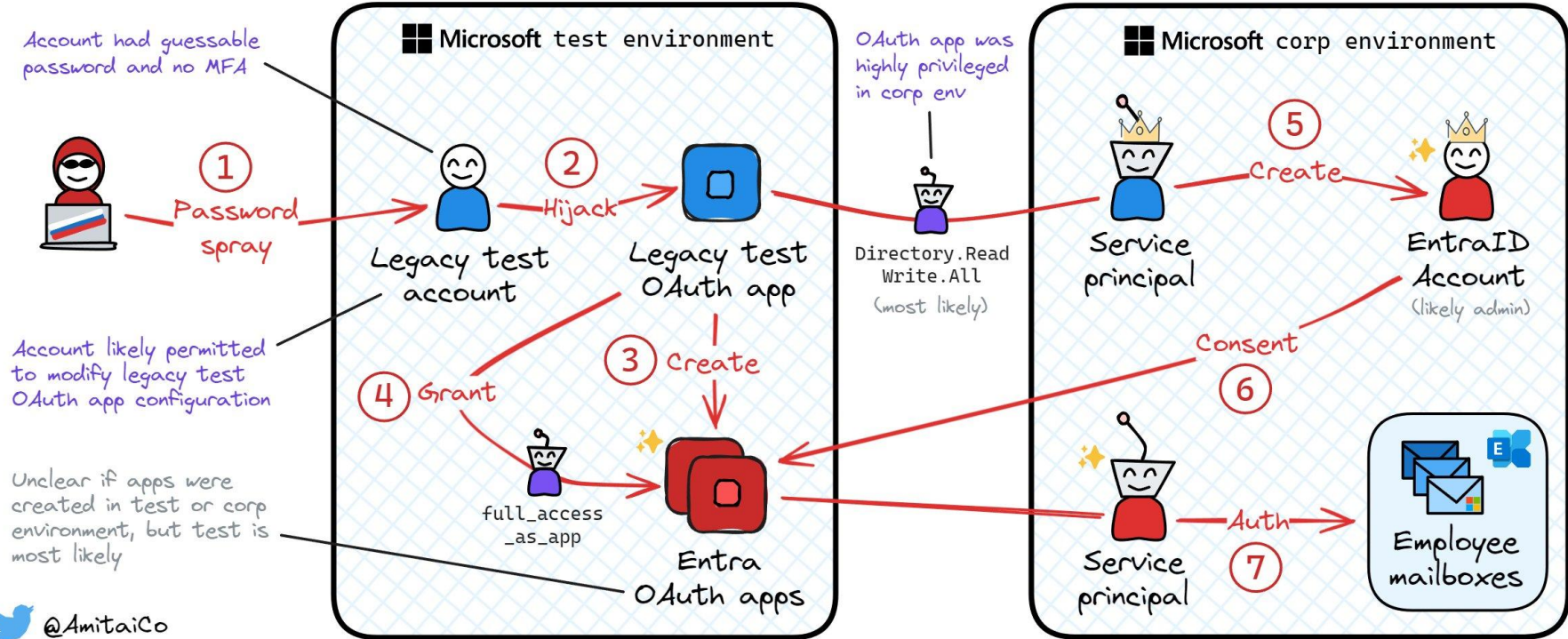
- Victim was Microsoft!

# Microsoft Breach

- <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/>
- Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium.
- Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold.
- Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents.

# Visualization of the Attack (from X user @AmitaiCo)

## ❄️ Midnight Blizzard Exchange Online Exfiltration Campaign (estimated attack flow)



# Today's Presentation

- In today's presentation we will discuss many Microsoft Entra ID and M365 controls that Microsoft did not implement properly, which led to this compromise.
- Effective security in Microsoft Entra ID and M365 environments consists of layers of detection across different services and applications.

# Modern Phishing and Cloud Token Theft

# Device Code Phishing – Device Code Authentication

- Device code authentication uses a numeric or alphanumeric code to authenticate an account from an input-constrained device that can't perform interactive authentication on its own (e.g., smart TVs, other smart devices) and must authenticate on another device to sign-in.
- Device code tokens are an industry standard and do not reflect an attack unique to Microsoft.

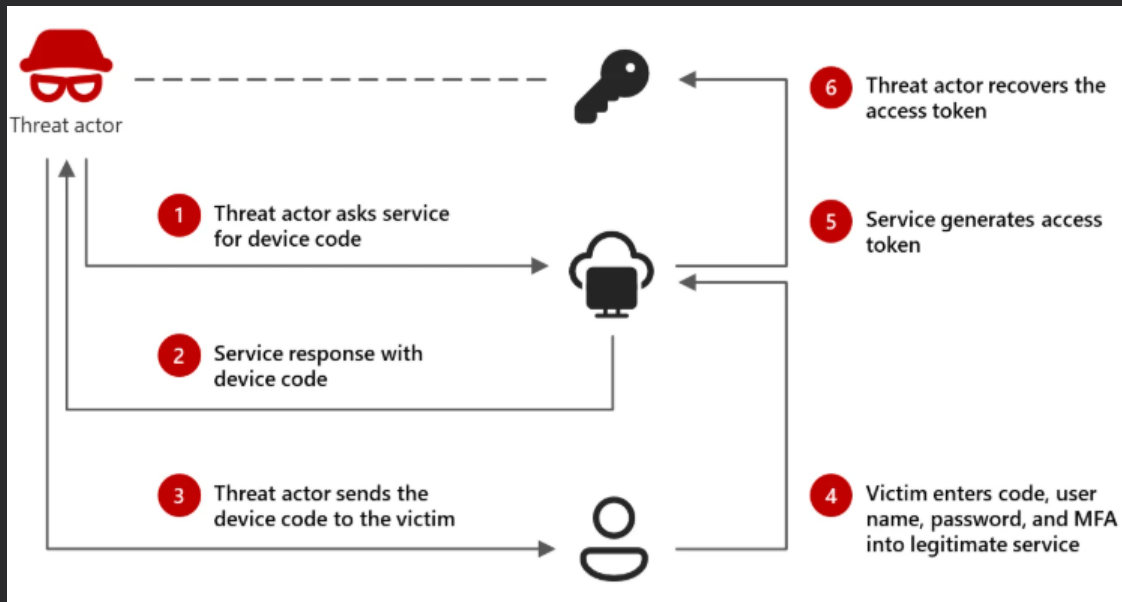




# Device Code Phishing Campaign – Attack Flow

In device code phishing, a threat actor generates a legitimate device code request and tricks the target into entering it into a legitimate sign-in page.

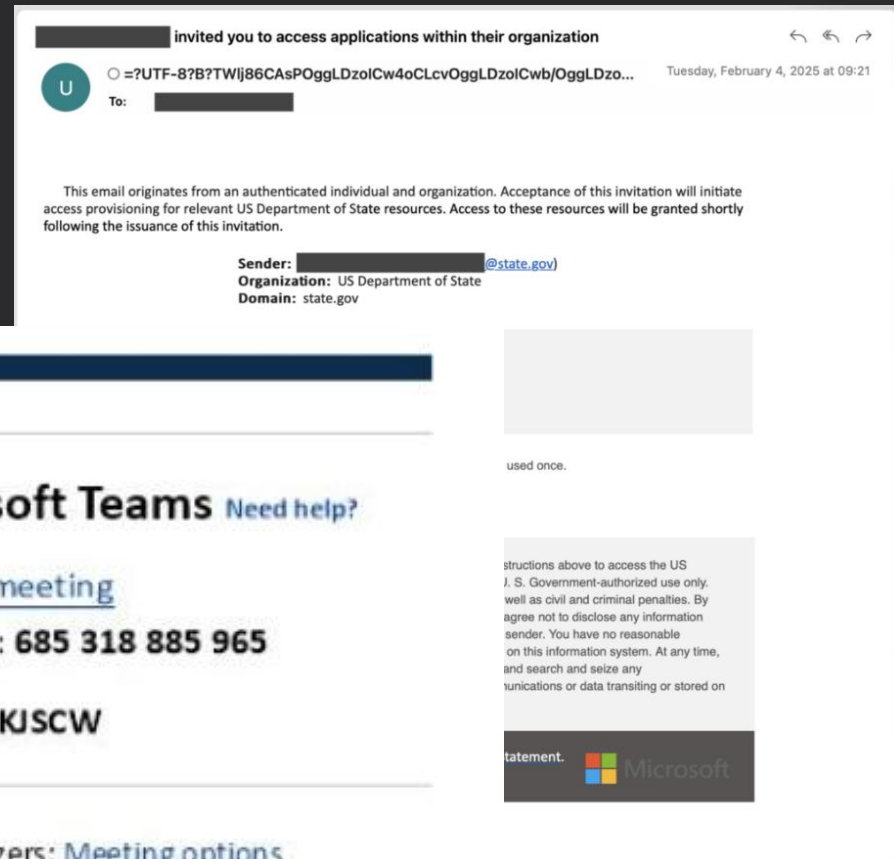
This grants the actor access and enables them to capture valid authentication tokens and use the tokens to access the target's accounts and data.



# Device Code Phishing Campaign – Phishing Component

Potential victims are targeted using third-party messaging services including WhatsApp, Signal, and Teams, to develop rapport before sending invitations to online events or meetings via phishing emails.

Victim is tricked into entering device code that the threat actor included as the ID for the fake Teams meeting invitation.



# Teams-based Attacks

<https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/>

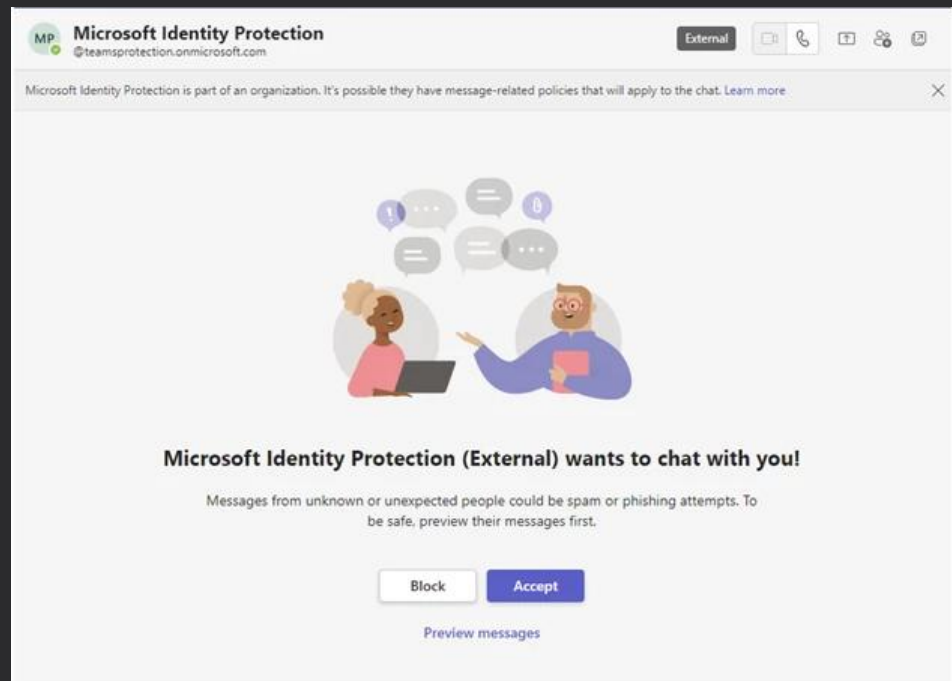
- Actors use Microsoft 365 tenants owned by small businesses they have compromised to host and launch their social engineering attack.
- Bad actor renames the compromised tenant, adds a new onmicrosoft.com subdomain, then sends messages from new subdomain.

# Teams-based Attacks

Attacker has obtained valid account credentials for the users they are targeting, or they are targeting users with passwordless authentication configured on their account – both require the user to enter a code on the Microsoft Authenticator app on their mobile device.

The target user may receive a Microsoft Teams message request from an external user masquerading as a technical support or security team.

If a user accepts the message request, they then receive Teams message from attacker attempting to convince them to enter a code into the Microsoft Authenticator app on their mobile device.

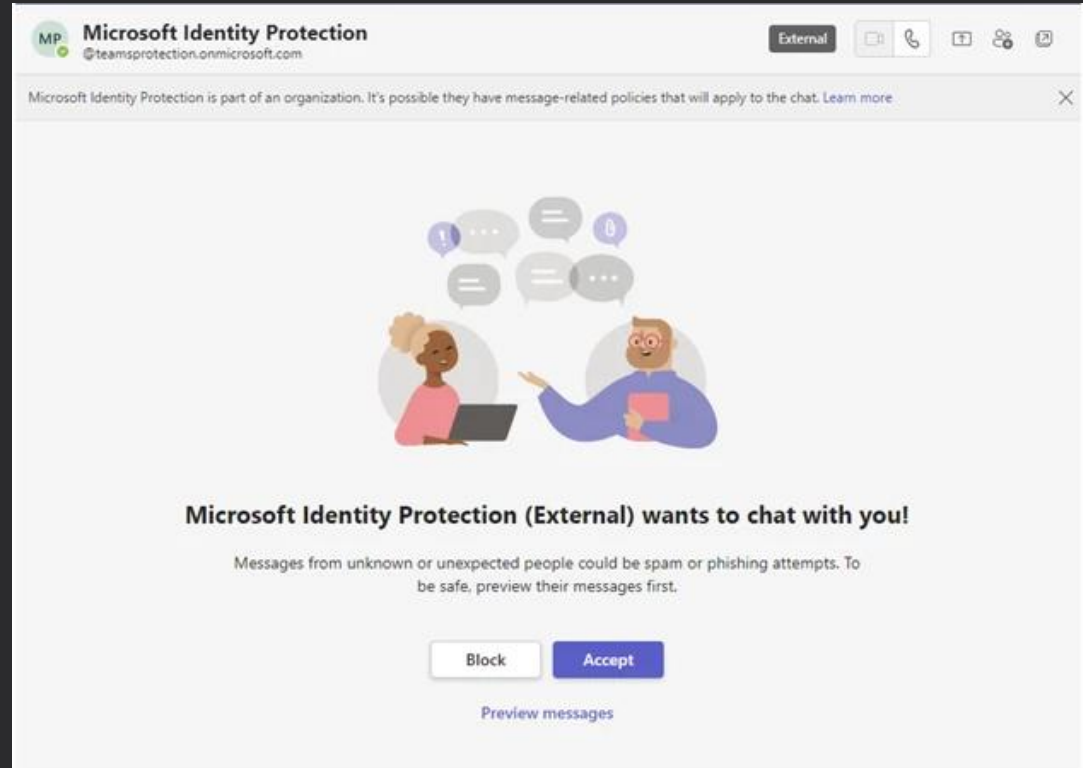


# Midnight Blizzard – Teams-based Attacks

Ensure users do not accept Teams invites from people they do not know.

Never share authentication credentials via Teams

Restrict Teams communication access as appropriate for environment

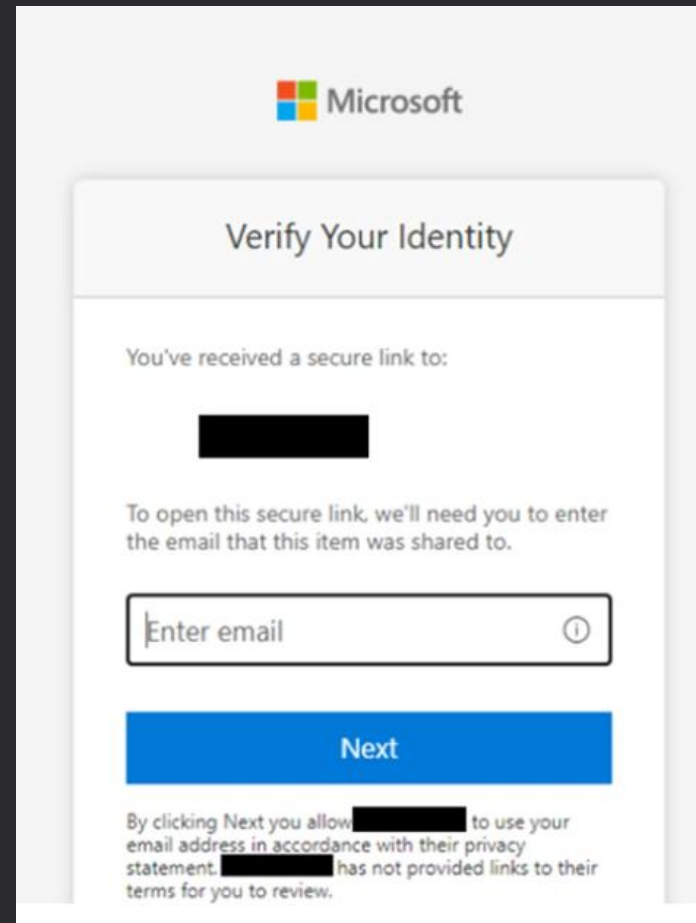


# Device Code Phishing Campaign – Mitigation

- Only allow device code flow where necessary. Microsoft recommends blocking device code flow wherever possible. Where necessary, configure Microsoft Entra ID's device code flow in Conditional Access policies :  
<https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows>
- Educate users about common phishing techniques. Sign-in prompts should clearly identify the application being authenticated to. As of 2021, Microsoft Azure interactions prompt the user to confirm ("Cancel" or "Continue") that they are signing in to the app they expect, which is an option frequently missing from phishing sign-ins.

# Legitimate File Hosting Services Used for Phishing

- <https://www.microsoft.com/en-us/security/blog/2024/10/08/file-hosting-services-misused-for-identity-phishing/>
- Microsoft observing an uptick in phishing attacks originating from trusted file sharing services – OneDrive, SharePoint, Dropbox - “living-off-trusted-sites” (LOTS)
- Access to documents is restricted to recipients and documents cannot be downloaded, making malicious detection more difficult.



# OneNote Attachment / RDP Attachment Campaigns

- **OneNote Campaigns** - OneNote attachments bypass file detection checks more readily than other office file types
- **RDP Campaigns** - Spear-phishing e-mails contained a signed Remote Desktop Protocol (RDP) configuration file that connected to an actor-controlled server.
- E-mails were sent from previously compromised legitimate organizations
- Malicious .RDP once target system compromised, it connected to actor-controlled server and mapped victim user's device resources to the server.



# Phishing Attackers Focused on Software Repositories

- Increase in phishing attempts targeting GitHub users
- Coming from GitHub accounts with names like "GitHub Notification"
- Fake logins authenticate rogue third party
- Ensure teams that use GitHub are aware of attack trend

## Security Alert: Unusual Access Attempt

We have detected a login attempt on your GitHub account that appears to be from a new location or device.

### Login Information

- **Location:** Reykjavik, Iceland
- **IP Address:** 53.253.117.8
- **Device:** Unrecognized

If you recognize this activity, no further action is required. However, if this was not you, we strongly recommend securing your account immediately.

### Steps to Secure Your Account

1. **Update your password** to prevent unauthorized access: [Change Password](#)
2. **Review and manage active sessions:** [Check Recent Activity](#)
3. **Enable Two-Factor Authentication (2FA)** for additional protection: [Set Up 2FA](#)

### Contact Support

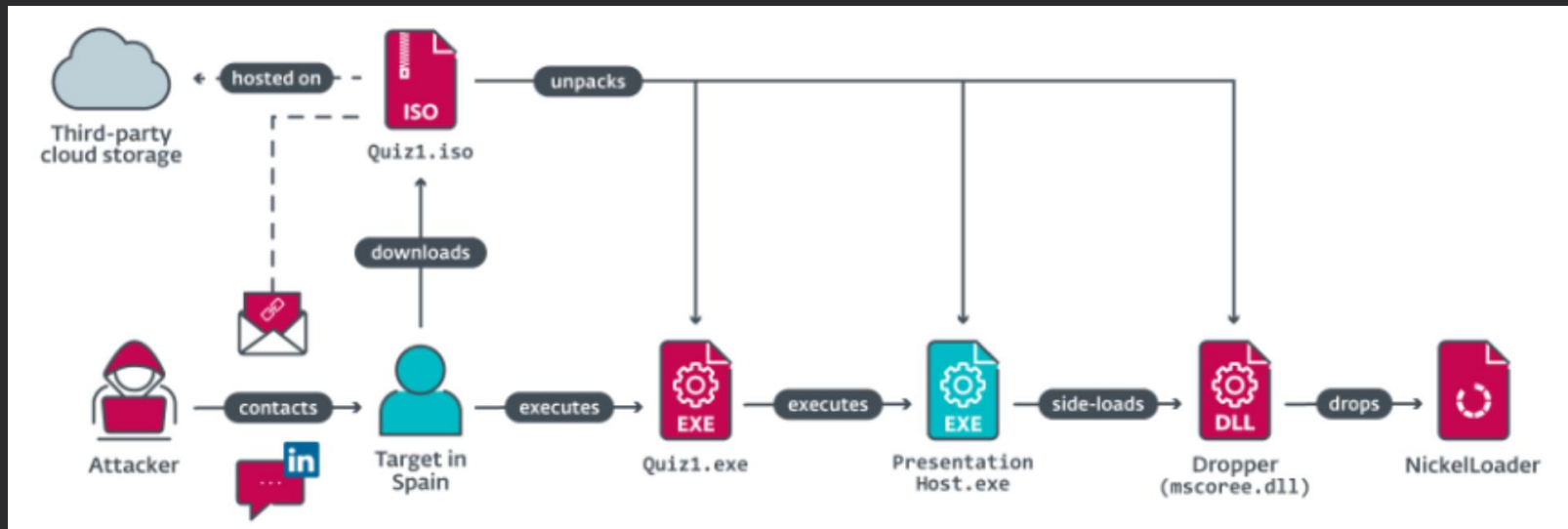
If you need assistance or suspect a security breach, visit: [GitHub Security Support](#)

Thank you for keeping your account secure.

**GitHub Security Team**

# Phishing attacks via Fake Dev Recruiters on LinkedIn

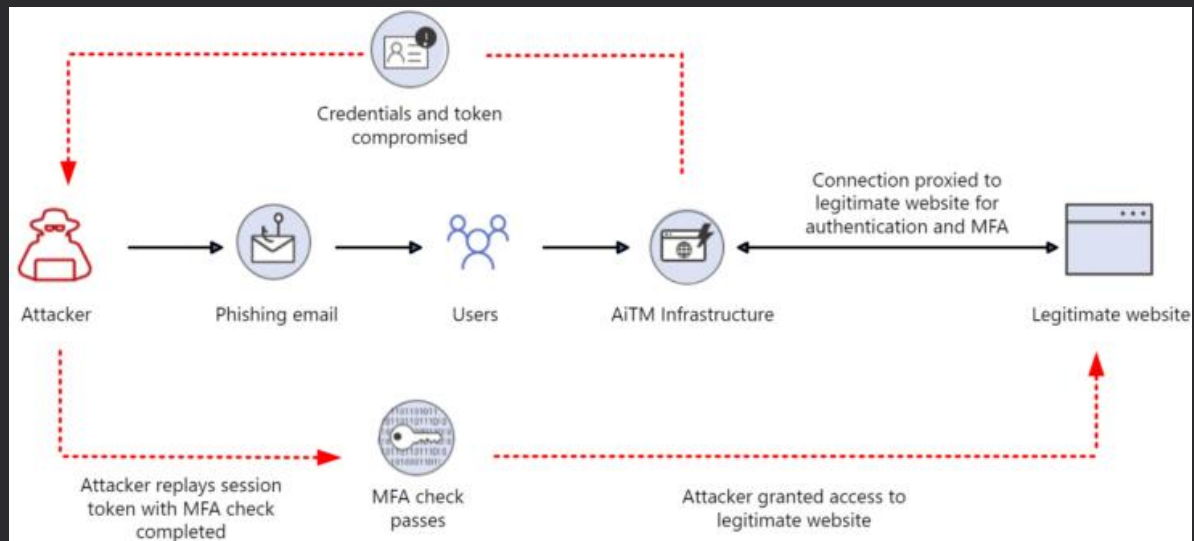
- Coding challenges as part of fake recruitment process are actually attacker backdoors.
- <https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/>



# Expanding Range of Attack Techniques Targeting MFA

## Attacks against MFA:

- Phishing
  - AITM Phishing Toolkits - man in the middle infrastructure to capture credentials AND session token
- Targeting SMS Providers to Steal Tokens
- Attempting MFA Reset via Customer Service / Tech Support
- Token Stealing Malware
- MFA Exhaustion Attacks
- SIM Swapping Attacks



# Key Security Controls in Entra ID

The background of the slide features a silhouette of a historic bridge, likely the Charles Bridge in Prague, with several statues and ornate street lamps. In the distance, a city skyline with various church spires and domes is visible. The sky is a gradient of green on the left and blue on the right, with some light clouds.

# Executive Summary

- What is Entra ID?
- Entra ID – General Configuration Settings
- Entra ID – Enterprise Applications and OAuth Consent
- Entra ID – Conditional Access Policies
- Entra ID – Authentication Methods and Requirements
- Entra ID – Privileged Identity Management
- Entra ID – Auditing and Monitoring

What is Entra ID?

# What is Entra ID?

- Formerly known as Azure Active Directory
- Microsoft Entra ID is a cloud-based identity and access management service that used to access external resources. Example resources include Microsoft 365, the Azure portal, and thousands of other SaaS applications.
- Whenever we access Office 365 applications or Azure resources, we are authenticating with an Entra ID identity.

# Why is Entra ID Important to M365 Security?

- Entra ID is the identity gatekeeper to all Microsoft 365 and Azure resources
- The first step of virtually every user interaction with M365 resources is authentication, which is managed by Entra ID.



# Entra ID – General Configuration Settings

# Limiting Number of Global Administrators

- Microsoft recommends that a maximum of five Global Administrators be permitted for most organizations.
- Wherever possible, lower-privileged roles should be assigned to users instead of Global Administrator.
- **Audit Item:** Confirm that users assigned the Global Administrator role in Entra ID tenant are reviewed regularly.
- **Audit Item:** Confirm that all users with privileged role eligibility in Entra ID tenant are reviewed regularly. Wherever possible, lower-privileged roles should be assigned to users.

# Cloud Only Administrative Accounts

Regular user accounts should not be utilized for administrative tasks - cloud administrative accounts should be separated from on-premise accounts.

Ensuring that cloud administrator accounts are cloud-only, without applications assigned, reduces the attack surface of those identities – protecting on-premise environment from a cloud-only account breach and vice versa.

To participate in Microsoft 365 security services such as Entra ID Identity Protection, PIM, and Conditional Access Policies, an administrative account will need a license attached. Ensure that the license does not include applications with potentially vulnerable services by using Azure Premium P1 or P2 for the cloud-only account.

# Create Break Glass Accounts

Emergency access or "break glass" accounts are intended for scenarios where normal administrative accounts are unavailable. Break glass accounts are not assigned to specific user and should have a combination of physical and technical controls to prevent them from being accessed outside of a true emergency, such as a technical failure of a cellular provider or service failures for key Microsoft services such as Conditional Access.

Break glass accounts should be cloud-only accounts that use the \*.onmicrosoft.com domain and are not federated or synchronized on-premise. Microsoft recommends exclusion of at least one of these accounts from all conditional access rules. Break glass account passwords must have sufficient entropy and length to protect against random guesses. FIDO2 security keys can be used instead of passwords.

# Restrict Collaboration to Trusted Domains

B2B collaboration is a feature within External Identities that allows guest invitations to be sent to users outside an organization.

Users should only be permitted to send invitations to explicitly permitted domains. This prevents internal users from sending invitations to unknown external users.

Home > telasasecurity.com | Users > Users | User settings >

## External collaboration settings

Save Discard

Email one-time passcode for guests has been moved to All Identity Providers. →

### Collaboration restrictions

⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. [Learn more.](#)

- ☐ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☒ Allow invitations only to the specified domains (most restrictive)

Delete

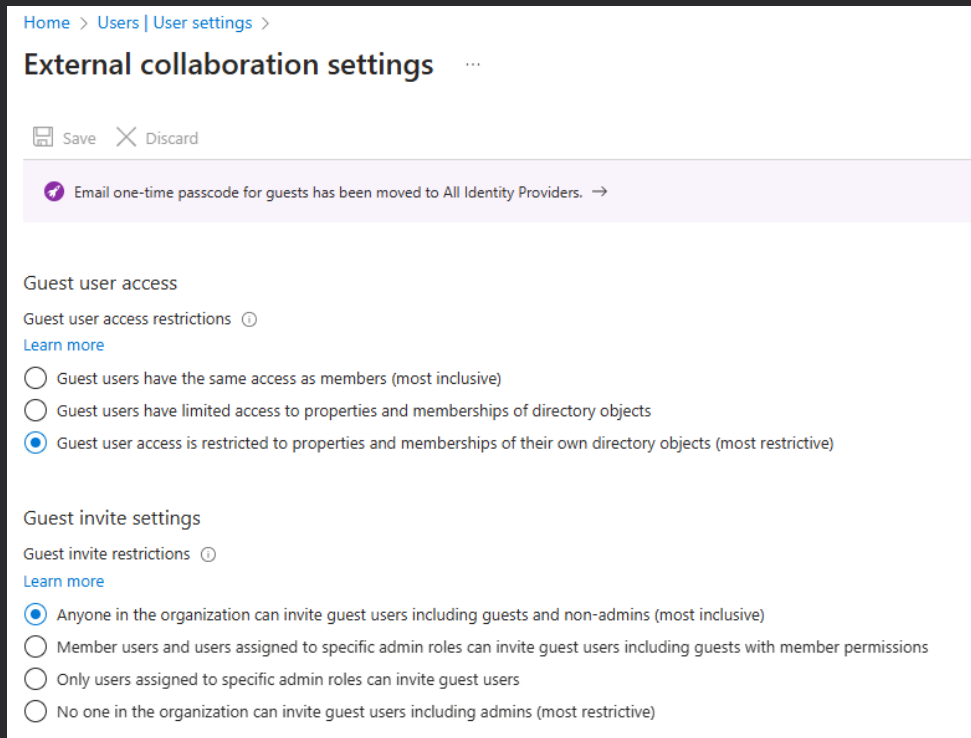
☐ Target domains

example.com or \*.example.com or example.\*

# Restrict Guest User Access

Guest user access provides access to users that are not part of an Entra ID tenant. Guest users are typically part of an external instance of Entra ID or another Microsoft or social account.

Restrict access as much as possible both in Guest user access and Guest invite settings.



The screenshot shows the 'External collaboration settings' page in the Microsoft Entra admin center. The breadcrumb trail at the top is 'Home > Users | User settings >'. Below the title, there are 'Save' and 'Discard' buttons. A purple notification bar states: 'Email one-time passcode for guests has been moved to All Identity Providers. →'. The main content is divided into two sections: 'Guest user access' and 'Guest invite settings'. Each section has a 'Learn more' link and a list of radio button options. In the 'Guest user access' section, the third option is selected: 'Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)'. In the 'Guest invite settings' section, the first option is selected: 'Anyone in the organization can invite guest users including guests and non-admins (most inclusive)'.

Home > Users | User settings >

## External collaboration settings

Save Discard

Email one-time passcode for guests has been moved to All Identity Providers. →

### Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☐ Guest users have limited access to properties and memberships of directory objects
- ☒ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

### Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

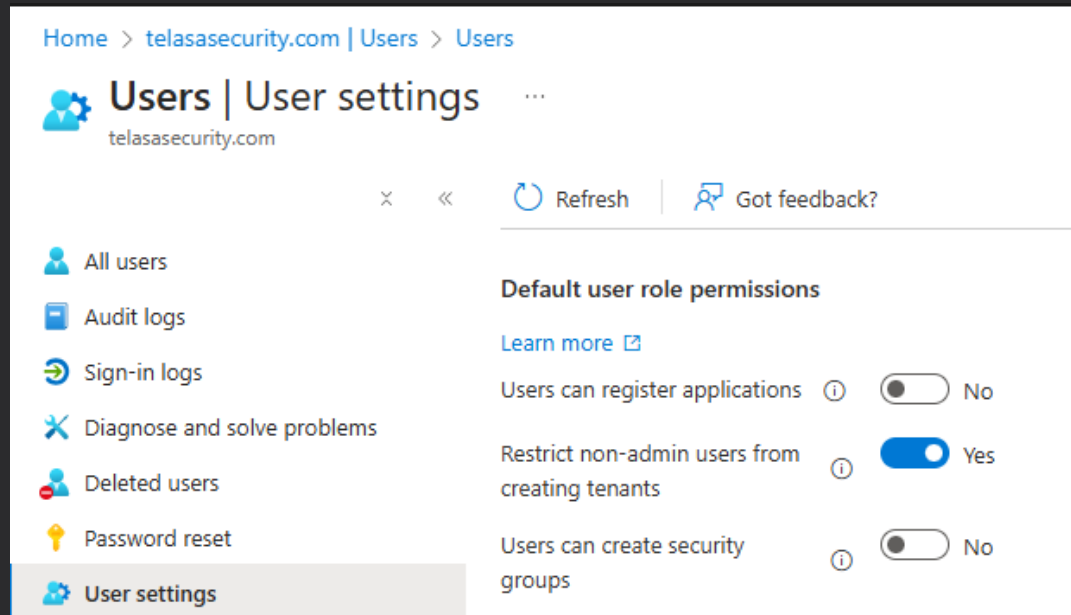
- ☒ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ☐ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ☐ Only users assigned to specific admin roles can invite guest users
- ☐ No one in the organization can invite guest users including admins (most restrictive)

# Application Registration / Tenant Creation / Security Group Creation

This setting restricts the ability for users to register applications in the environment. Application registration should be disabled.

Non-admin users can be granted permission to create tenants. Only administrators should be permitted to create new tenants.

Non-admin users should not have permission to create security groups in the tenant.







# Restrict User Consent for Applications

Users can grant consent to applications that can access organization data. Options for this setting, from least to most restrictive, include:

- Permit users to grant consent to applications from verified publishers that meet organizational criteria for risk (least restrictive).
- Allow users to request admin consent. Consent requests are routed to administrators who review and provide approval where appropriate.
- Do not permit users to request or grant consent (most restrictive) - **Recommended**

Home > telasasecurity.com | Enterprise applications > Enterprise applications | Consent and permissions >

## Consent and permissions | User consent settings

✕ ‹ Save ✕ Discard | 🗨️ Got feedback?

▼ Manage

- ⚙️ User consent settings
- ⚙️ Admin consent settings
- 👤 Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications  
Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- ☒ Do not allow user consent  
An administrator will be required for all apps.
- ☐ Allow user consent for apps from verified publishers, for selected permissions (Recommended)  
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- ☐ Allow user consent for apps  
All users can consent for any app to access the organization's data.

# Secure Admin Consent Workflow

Admin consent workflow gives admins a mechanism to grant access to applications that require admin approval. When a user is unable to provide consent, they submit a request for admin approval. The request is sent to designated reviewers, act on the request, and the user is notified of the response.

**Consent and permissions | Admin consent settings**

× << Save Discard

Manage

- User consent settings
- Admin consent settings**
- Permission classifications

**Admin consent requests**

Users can request admin consent to apps they are unable to consent to ①

Yes No

Who can review admin consent requests ①

Reviewer type	Reviewers
Users	+ Add users
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests ①

Yes No

Selected users will receive request expiration reminders ①

Yes No

Consent request expires after (days) ①

Progress bar: 0 days

# App Governance (1 of 3)

Deeper visibility, control and alerting over OAuth apps and permissions than previous interfaces in Entra ID and Defender for Cloud Apps (MCAS)

The screenshot displays the Microsoft 365 Defender App Governance interface. The left sidebar contains navigation options: Home, Incidents & alerts, Hunting, Actions & submissions, Threat analytics, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management, Email & collaboration, and Investigations. The main content area is titled 'App governance' and includes a search bar, a filter section, and a table of OAuth apps.

**App governance**

Get in-depth visibility and control over OAuth apps registered on Azure Active Directory.

Overview **Apps** Alerts Policies

63 items Search Customize columns

Filter Save the query Reset Filters

API access: Any Privilege level: Any Permission usage: Any Permission type: Any Publisher verified: Any Services accessed: Any Sensitivity labels accessed: Any

App name	App status	Graph API access	Permission type	Consent type	Publisher	Last modified	Added on	Permission usage	Data usage	Privilege level
<input type="checkbox"/> 3652sentinel	Enabled	Yes	Mixed	Admin (124)	N/A	Oct 25, 2022 1:03 AM	Jun 5, 2020 4:51 PM	N/A	0 (0%)	Low
<input type="checkbox"/> AddEvent.com	Enabled	Yes	Delegated	User (1)	N/A	Oct 25, 2022 1:03 AM	May 7, 2020 11:16 AM	Some unused	0 (0%)	Low
<input type="checkbox"/> AppConnectTestingGraph	Enabled	Yes	Mixed	Admin (124)	N/A	Oct 25, 2022 1:03 AM	Aug 23, 2021 7:58 AM	N/A	0 (0%)	High
<input type="checkbox"/> AtBot Logic	Enabled	Yes	Delegated	User (1)	N/A	Oct 25, 2022 1:03 AM	Jun 28, 2019 8:15 AM	N/A	0 (0%)	Low
<input type="checkbox"/> Azure Logic Apps - Azure AD	Enabled	Yes	Delegated	Admin (124)	N/A	Oct 25, 2022 1:03 AM	Jun 26, 2019 10:19 AM	N/A	0 (0%)	High
<input type="checkbox"/> Azure Notebooks	Enabled	Yes	Delegated	Admin (124)	N/A	Oct 25, 2022 1:03 AM	Jun 26, 2019 10:10 AM	N/A	0 (0%)	Low
<input type="checkbox"/> Cisco Webex Meetings	Enabled	Yes	Mixed	Admin (124)	Cisco	Oct 25, 2022 1:03 AM	Mar 11, 2019 9:18 AM	Some unused	0 (0%)	Low
<input type="checkbox"/> Coronet	Enabled	Yes	Application	User (0)	Coronet Cyber Sec	Oct 25, 2022 1:03 AM	Jul 22, 2020 2:21 PM	Some unused	0 (0%)	High
<input type="checkbox"/> Coronet	Enabled	Yes	Mixed	Admin (124)	Coronet Cyber Sec	Oct 25, 2022 1:03 AM	Nov 25, 2019 8:10 AM	Some unused	0 (0%)	High
<input type="checkbox"/> Docs Rendering Public	Enabled	Yes	Delegated	Admin (124)	N/A	Oct 25, 2022 1:03 AM	Nov 23, 2021 12:19 PM	N/A	0 (0%)	Low
<input type="checkbox"/> drawio	Enabled	Yes	Delegated	Admin (124)	N/A	Oct 25, 2022 1:03 AM	Apr 30, 2019 10:23 AM	Some unused	0 (0%)	High


# App Governance (2 of 3)

## Default and customizable alert policies for OAUTH application usage

Create policy									
<a href="#">Create new policy</a> <a href="#">Export</a> <span>11 items</span> <input type="text" value="Search"/>									
<b>Filter</b> <a href="#">Save the query</a> <a href="#">Reset</a> <a href="#">Filters</a>									
Policy name	Status ⓘ	Severity	Active alerts	Total alerts	Last alert ⓘ	Last modified ↓	Source	Created by	
<input type="checkbox"/> Unusual activity from an app with priority account consent	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> New app with low consent rate	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> High volume of inbox rule creation activity by an app	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> Increase in data usage by an overprivileged or highly privileged app	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> Spike in Graph API calls made to SharePoint	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> Suspicious app with access to multiple M365 workloads	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> Access to sensitive data	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> Spike in Graph API calls made to Exchange	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> High volume of email sending activities by an app	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> Spike in Graph API calls made to OneDrive	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	
<input type="checkbox"/> High volume of email search activity by an app	● Active	■ ■ ■ Medium	0	0	-	-	Predefined	Microsoft	

# App Governance (3 of 3)

Detailed usage and permissions history (App Governance does required Defender for Cloud Apps or E5 license)

**Graph explorer**  
Enabled

Summary | Data usage | Users | Permissions | Sensitivity labels

App name  
Graph explorer

App ID  
de8bc8b5-d9f9-48b1-a8ad-b748da725064  
[View in Azure AD](#)

Graph API access  
Yes

Consent type  
Admin

Added on  
9/4/2018


Last modified  
11/2/2022

Last action  
-

Publisher verification  
Microsoft  
[Learn more about publisher verification](#)

Certification  
No certification  
[Learn more about Microsoft 365 certification](#)

Disable app

**Graph explorer**  
Enabled

Summary | Data usage | Users | **Permissions** | ...

Permission summary

Total permissions  
43

High privilege  
12

Unused permissions  
10


Graph API permissions ⓘ

43 items

Permission	Privilege level	In use	Type
Calendars.ReadWrite	Low	No	Delegated
Chat.ReadBasic	Low	No	Delegated
Files.ReadWrite.All	High	No	Delegated
MailboxSettings.ReadWrite	High	No	Delegated
Contacts.ReadWrite	Low	No	Delegated

Show more

Disable app

**Graph explorer**  
Enabled





Summary | Data usage | **Users** | Permissions | Sensitivity labels

Summary ⓘ

Total consented users  
124

Priority accounts  
4

App users with the highest data usage ⓘ

Name	Priority account	Uploads ↑	Downloads
 Sarah ...	Yes	0	0
 Corey ...	Yes	0	0
 Steve I...	Yes	0	0
 Micha...	Yes	0	0

Disable app



# What is Conditional Access?

- Microsoft Entra ID Conditional Access (formerly Azure AD Conditional Access) is a policy-based access control system that lets organizations enforce security controls based on specific conditions when users attempt to access resources.
- Conditional Access enables building of flexible policies to align with organizational practices and risk appetite.
- Conditional Access is a cornerstone of a Zero Trust security strategy, allowing organizations to balance security and productivity by applying the right access controls under the right conditions rather than having a single approach for all situations.

# Conditional Access Policies for MFA

- **Require MFA for administrative users** - MFA should be enabled for all privileged accounts in Azure AD tenants.
- **Require MFA for all users** - MFA for all users, even those connecting from trusted IP addresses, can reduce risk from insider threats, and can limit unauthorized access windows in scenarios where an account compromise goes undetected. The sign in frequency for this Conditional Access Policy can be set to an interval that can limit the impact of the setting on users (e.g., users only authenticate with MFA once monthly).
- **Require MFA for Guests** - A Conditional Access Policy to enforce organizational authentication requirements for all guest users should be in place for all organizations that permit guest user access.



# What a Conditional Access Policy Looks Like

Home > Conditional Access | Policies >

## GR3 - Grant Require MFA

Conditional Access policy

Delete View policy information View policy impact (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

GR3 - Grant Require MFA

Assignments

Users

[All users included and specific users excluded](#)

Target resources

[All resources \(formerly 'All cloud apps'\)](#)

Network **NEW**

[Not configured](#)

Conditions

[0 conditions selected](#)

Access controls

Grant

[1 control selected](#)

Session

[Sign-in frequency - 7 days](#)

### Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication

"Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

☒ Require authentication strength

Strong Push - no SMS...

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more](#)

☐ Require device to be marked as compliant

## Conditional Access Policies for User Risk

- A Conditional Access Policy should exist that specifies automated actions when an Azure AD user is classified as high-risk by Azure AD Identity Protection.
- When triggered, this policy should invoke automation that blocks access to the user account until the user is reauthenticated with MFA and changes their password.
- This functionality requires an Azure AD Premium 2 (P2) license (e.g., E3+E5 Security or full E5 licensing), Azure AD Identity Protection is a high-fidelity detection capability that should be in place in all high-security Azure AD environments.

## Conditional Access Policies for Sign-in Risk

- A Conditional Access Policy should exist that specifies automation actions when an Azure AD sign-in is classified as Medium or High risk by Azure AD Identity Protection.
- When triggered, this policy should invoke automation that requires MFA authentication prior to account access being granted.
- This functionality requires an Azure AD Premium 2 license (e.g., E3+E5 Security or full E5 licensing). Azure AD Identity Protection is a high-fidelity detection capability that should be in place in all high-security Azure AD environments.

# Conditional Access Policies for Legacy Authentication

- A major historical risk associated with Entra ID is use of legacy authentication protocols, especially related to mail services, such as IMAP, POP, and SMTP. These applications do not support MFA. As a result, when organizations implement MFA, but do not restrict use of legacy protocols, they may still be vulnerable to brute force and password guessing attacks against the legacy protocols.
- Legacy authentication should be disabled in all Entra ID environments. The simplest approach to confirm that legacy authentication is disabled in an environment is to create a Conditional Access policy that blocks all legacy authentication use.

# Conditional Access Policies for Geographic Restrictions

- Conditional Access Policies can be used to prevent access from countries that are outside of an organization's scope of interest (e.g.: customers, suppliers). Blocking access from different countries can be utilized to reduce the attack surface of an organization's Entra ID tenant.

The screenshot shows the configuration page for a Conditional Access policy named 'BL3 - Block Geo Country non-US'. The page is divided into several sections for configuring the policy's scope and controls.

**Navigation:** Home > Conditional Access | Policies >

**Policy Name:** BL3 - Block Geo Country non-US

**Actions:** Delete, View policy information, View policy impact (Preview)

**Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)**

**Control user access based on their network or physical location. [Learn more](#)**

**Configure** (Yes/No toggle set to Yes)

**Include/Exclude:** **Include** (selected), Exclude

- ☐ Any network or location
- ☐ All trusted networks and locations
- ☐ All Compliant Network locations
- ☒ Selected networks and locations

**Select:** All countries minus USA

**Target resources:** All resources (formerly 'All cloud apps') included and 4 resources excluded

**Network:** NEW (1 included and 1 excluded)

**Conditions:** 1 condition selected

**Access controls:**

**Grant:** Block access

**Session:** 0 controls selected

**Informational messages:**

- To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. [Learn more on how to enable GSA Adaptive Access Signaling.](#)
- 'Locations' condition is moving! Locations will become the 'Network' assignment with a new Global Secure

# Conditional Access Policies for User Registration

- Securing user Azure AD MFA registration is possible with user actions in a Conditional Access Policy. This functionality allows organizations to treat the registration process like any application in a Conditional Access policy. Organizations can utilize trusted network location or device compliance to secure the registration process.

# Conditional Access Policies for Azure Management

- The Microsoft Azure Management application governs various Azure services and can be secured through the implementation of a Conditional Access Policy. This policy can restrict accounts from accessing Microsoft Azure Management portals and applications.
- When a Conditional Access Policy is targeted to Microsoft Azure Management, the policy will be enforced for application IDs of services bound to the portal, including:
  - Azure Resource Manager
  - Azure portal (including Microsoft Entra admin center)
  - Azure Data Lake
  - Application Insights API
  - Log Analytics API

# Conditional Access for Protected Actions

- Conditional Access Policies for Sensitive Actions
  - Admins require a privileged access workstation and a FIDO2 key to delete Conditional Access policies.
  - Admins need phishing-resistant MFA to define or modify custom rules that define network locations.

Microsoft Entra admin center

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

Home > Roles and administrators

## Roles and administrators | Protected actions

Woodgrove - Azure AD for workforce

+ Add protected actions Refresh Manage view Remove Preview features Got feedback?

All roles Protected actions Diagnose and solve problems

Activity

- Access reviews
- Audit logs
- Troubleshooting + Support
- New support request

Protected actions are role permissions with Conditional Access applied for added security. Conditional Access requirements are enforced when a user performs the protected action. [Learn more](#)

Search by name or description

5 actions found

Permission	Description	Conditional Access authentication context
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/basic/update	Update basic properties for conditional access policies	Phishing-resistant MFA required
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/delete	Delete conditional access policies	Phishing-resistant MFA required
<input type="checkbox"/> microsoft.directory/namedLocations/basic/update	Update basic properties of custom rules that define network locations	Phishing-resistant MFA required
<input type="checkbox"/> microsoft.directory/namedLocations/create	Create custom rules that define network locations	Phishing-resistant MFA required
<input type="checkbox"/> microsoft.directory/namedLocations/delete	Delete custom rules that define network locations	Phishing-resistant MFA required




## Conditional Access Policies for Device Code Flow


We recommend organizations get as close as possible to a unilateral block on device code flow. Organizations should consider creating a policy to audit the existing use of device code flow and determine if it is still necessary.

# End Result is a Conditional Access Policy Set

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

**All policies**  
**12**  
Total

**Microsoft-managed policies**  
 **0**  
out of 12

 Add filter

12 out of 12 policies found

Policy name	State	Creation date	Modified date
<a href="#">BL1 - Block access for unknown or unsupported device platform</a>	On	7/17/2023, 2:06:54 PM	11/17/2024, 9:24:11 PM
<a href="#">BL2 - Block legacy authentication</a>	On	8/24/2022, 4:01:03 PM	11/15/2024, 1:32:00 PM
<a href="#">BL3 - Block Geo Country non-US</a>	On	3/25/2021, 1:51:35 PM	3/3/2025, 1:55:09 PM
<a href="#">GR1 - Grant Action Require Device Compliance</a>	Report-only	7/17/2023, 2:13:36 PM	2/13/2025, 9:58:06 AM
<a href="#">GR2 - Grant With Acceptable Use Policy</a>	On	10/22/2021, 11:17:22 AM	11/14/2024, 11:04:47 AM
<a href="#">GR3 - Grant Require MFA</a>	On	2/2/2021, 2:01:48 PM	1/27/2025, 11:33:31 AM
<a href="#">GR4 - Grant PIM Group Strong Auth Managed Sentinel</a>	On	4/11/2023, 9:45:25 AM	9/18/2024, 3:06:57 PM
<a href="#">GR5 - Grant Travelers MFA</a>	On	4/18/2022, 9:24:48 AM	9/18/2024, 3:09:13 PM
<a href="#">GR6 - Grant with Password Change for Risky Users</a>	On	9/20/2024, 1:06:29 PM	11/15/2024, 1:36:11 PM
<a href="#">GR7 - Grant with MFA for Risky Signins</a>	On	9/20/2024, 1:08:43 PM	11/15/2024, 1:36:34 PM
<a href="#">GR8 - Grant GA MFA Every Time</a>	On	10/4/2024, 11:08:06 AM	2/19/2025, 5:22:50 PM

# Conditional Access Resources

## Baseline Policy References

- <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation>
- <https://danielchronlund.com/2020/11/26/azure-ad-conditional-access-policy-design-baseline-with-automatic-deployment-support/>



# Implement Password Protection

- Entra ID Password Protection provides global and custom banned password lists. A password change request will fail if the proposed password matches entries on either of the banned password lists. To protect on-premises Active Directory Domain Services (AD DS) environments, install and configure Azure AD Password Protection.
- With Entra ID Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. Custom banned password lists can also be defined. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.

# Password Expiration

Microsoft cloud-only accounts have a pre-defined password policy that cannot be changed. The only parameters that can change are the number of days until a password expires and whether passwords expire at all.

Organizations such as NIST and Microsoft have updated their password policy recommendations to not require users to change their passwords unless there is evidence the password is compromised, or the user forgot it.

When setting passwords not to expire it's important to have other controls to supplement this setting:

- Educate users to not reuse organization passwords anywhere else.
- Enforce Multi-Factor Authentication registration for all users.
- Ban common passwords.

# NIST Password Guidance - Highlights

- <https://pages.nist.gov/800-63-4/>
- Password verification method should no longer require passwords be changed at specific intervals (i.e. every 60 days) but in the following circumstances instead:
  - After a breach/compromise
  - User request
- Note the language – “shall not” – not a recommendation, but a requirement

NIST SP 800-63B-4 2pd  
August 2024

Digital Identity Guidelines  
Authentication and Authenticator Management

## 3.1.1.2. Password Verifiers

The following requirements apply to passwords:

1. Verifiers and CSPs **SHALL** require passwords to be a minimum of eight characters in length and **SHOULD** require passwords to be a minimum of 15 characters in length.
  2. Verifiers and CSPs **SHOULD** permit a maximum password length of at least 64 characters.
  3. Verifiers and CSPs **SHOULD** accept all printing ASCII [RFC20] characters and the space character in passwords.
  4. Verifiers and CSPs **SHOULD** accept Unicode [ISO/ISC 10646] characters in passwords. Each Unicode code point **SHALL** be counted as a single character when evaluating password length.
  5. Verifiers and CSPs **SHALL NOT** impose other composition rules (e.g., requiring mixtures of different character types) for passwords.
  6. Verifiers and CSPs **SHALL NOT** require users to change passwords periodically. However, verifiers **SHALL** force a change if there is evidence of compromise of the authenticator.
  7. Verifiers and CSPs **SHALL NOT** permit the subscriber to store a hint that is accessible to an unauthenticated claimant.
  8. Verifiers and CSPs **SHALL NOT** prompt subscribers to use knowledge-based authentication (KBA) (e.g., “What was the name of your first pet?”) or security questions when choosing passwords.
  9. Verifiers **SHALL** verify the entire submitted password (i.e., not truncate it).
- If Unicode characters are accepted in passwords, the verifier **SHOULD** apply the normalization process for stabilized strings using either the NFKC or NFKD normalization defined in Sec. 12.1 of *Unicode Normalization Forms* [UAX15]. This process is applied before hashing the byte string that represents the password. Subscribers choosing passwords that contain Unicode characters **SHOULD** be advised that some endpoints may represent some characters differently, which would affect their ability to authenticate successfully.

# NIST Password Guidance - Highlights

- <https://pages.nist.gov/800-63-4/>
- Also recommends migration away from password complexity rules
- Using complexity rules gets you the user psychology of:
  - Password1
  - Password2
- Use phrasing instead and allow for spaces, which is important. Humans type phrases with spaces.

NIST SP 800-63B-4 2pd  
August 2024

Digital Identity Guidelines  
Authentication and Authenticator Management

## 3.1.1.2. Password Verifiers

The following requirements apply to passwords:

1. Verifiers and CSPs **SHALL** require passwords to be a minimum of eight characters in length and **SHOULD** require passwords to be a minimum of 15 characters in length.
  2. Verifiers and CSPs **SHOULD** permit a maximum password length of at least 64 characters.
  3. Verifiers and CSPs **SHOULD** accept all printing ASCII [RFC20] characters and the space character in passwords.
  4. Verifiers and CSPs **SHOULD** accept Unicode [ISO/SC 10646] characters in passwords. Each Unicode code point **SHALL** be counted as a single character when evaluating password length.
  5. Verifiers and CSPs **SHALL NOT** impose other composition rules (e.g., requiring mixtures of different character types) for passwords.
  6. Verifiers and CSPs **SHALL NOT** require users to change passwords periodically. However, verifiers **SHALL** force a change if there is evidence of compromise of the authenticator.
  7. Verifiers and CSPs **SHALL NOT** permit the subscriber to store a hint that is accessible to an unauthenticated claimant.
  8. Verifiers and CSPs **SHALL NOT** prompt subscribers to use knowledge-based authentication (KBA) (e.g., "What was the name of your first pet?") or security questions when choosing passwords.
  9. Verifiers **SHALL** verify the entire submitted password (i.e., not truncate it).
- If Unicode characters are accepted in passwords, the verifier **SHOULD** apply the normalization process for stabilized strings using either the NFKC or NFKD normalization defined in Sec. 12.1 of *Unicode Normalization Forms* [UAX15]. This process is applied before hashing the byte string that represents the password. Subscribers choosing passwords that contain Unicode characters **SHOULD** be advised that some endpoints may represent some characters differently, which would affect their ability to authenticate successfully.

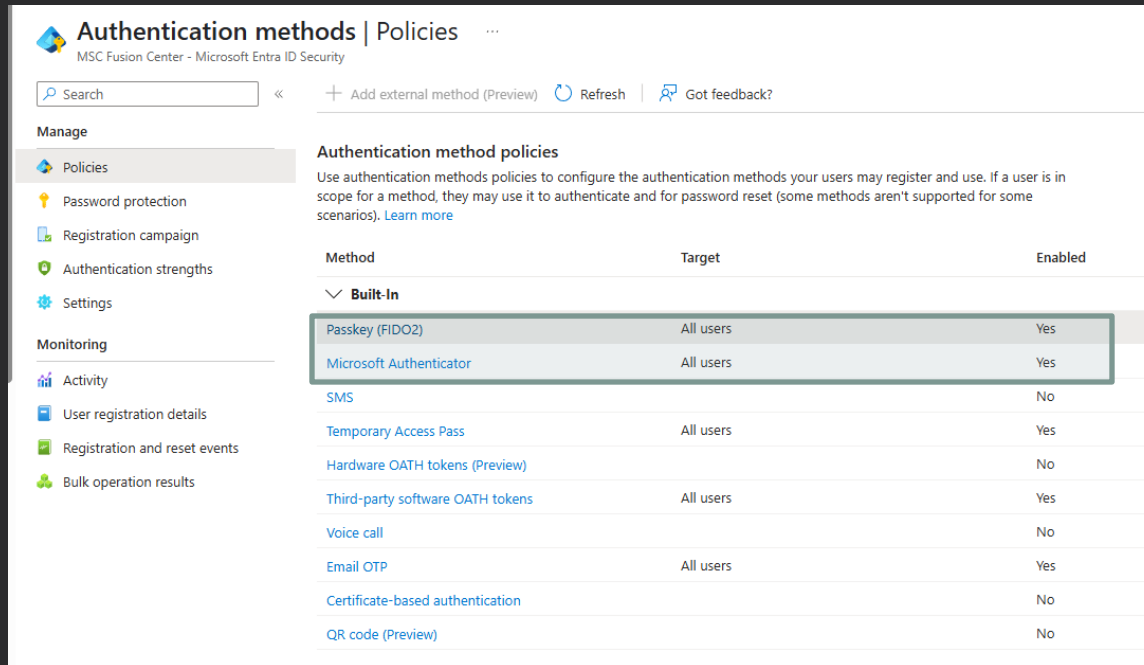


# Password Reset Notifications

Ensure that users are notified when account passwords are reset. User notification on password reset can help users to recognize potentially unauthorized password reset activities. Ensure that all administrators are notified if other administrators reset their password. This notification ensures that administrators can confirm if activity appears unusual or unauthorized.

# Restrict User Registration to Approved MFA Methods

- Restrict Authentication Methods to ensure users can only register for authentication methods approved by the organization. User should not be able to register weak authentication mechanisms, such as SMS and voice.



The screenshot shows the 'Authentication methods | Policies' page in the Microsoft Entra ID Security console. The left sidebar contains navigation links for 'Manage' (Policies, Password protection, Registration campaign, Authentication strengths, Settings) and 'Monitoring' (Activity, User registration details, Registration and reset events, Bulk operation results). The main content area is titled 'Authentication method policies' and includes a description: 'Use authentication methods policies 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 scenarios). [Learn more](#)'. Below this is a table with columns 'Method', 'Target', and 'Enabled'. The table lists various authentication methods, with 'Passkey (FIDO2)' and 'Microsoft Authenticator' highlighted in a blue box, indicating they are enabled for all users. Other methods like SMS, Temporary Access Pass, Hardware OATH tokens, Third-party software OATH tokens, Voice call, Email OTP, Certificate-based authentication, and QR code (Preview) are listed with their respective targets and enabled status.

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

# Authenticator Prompt Security

- Additional settings can enhance security of Microsoft Authenticator. These settings provide additional information and context to users who receive MFA passwordless and push requests:
  - **MFA number matching** requires the user to input a two-digit number presented on the device requesting access into the device performing two-factor authentication. This setting requires the user to have access to both the device requesting the app as well as the device performing MFA, reducing the risk of a successful MFA fatigue attack.
  - **Application Name** - in push and passwordless notifications can help end users confirm that the request is legitimate and to identify potential attempts at unauthorized access.
  - **Geographic Location** - Presentation of the **geographic location** associated with the authentication attempt in push and passwordless notifications can help alert end users to potential attempts at unauthorized access.
- In certain environments, such as those that rely on VPN use, or that route Internet traffic through proxies, or with certain cellular providers, geographic information presented in the MFA push response may be unreliable. As a result, the presentation of geographic location information could result in confusion for some users.

# Authentication Strengths (1 of 3)

Authentication Strengths Menu allows configuration of sets of authentication factors – three built in policies:

- MFA – All MFA types
- Passwordless MFA
- Phishing-resistant MFA – Windows Hello, Passkey, certificate auth only.

The screenshot shows the 'Authentication methods' page in the Microsoft Entra ID Security console. The page title is 'Authentication methods | Authentication strengths'. Below the title, there is a search bar and a '+ New authentication strength' button. The left sidebar contains a 'Manage' section with links to Policies, Password protection, Registration campaign, Authentication strengths (selected), and Settings. Below this is a 'Monitoring' section with links to Activity and User registration details. The main content area shows a table of authentication strengths. The table has four columns: Authentication strength, Type, Authentication methods, and Conditional access policies. There are three rows of data, all with a 'Built-in' type and 'Not configured in any policy yet' status.

Authentication strength	Type	Authentication methods	Conditional access policies
<a href="#">Multifactor authentication</a>	Built-in	Windows Hello For Business / Platform Credential ...	Not configured in any policy yet
<a href="#">Passwordless MFA</a>	Built-in	Windows Hello For Business / Platform Credential ...	Not configured in any policy yet
<a href="#">Phishing-resistant MFA</a>	Built-in	Windows Hello For Business / Platform Credential ...	Not configured in any policy yet

# Authentication Strengths (2 of 3)

20 different authentication strengths can be defined in policies:

The screenshot shows a 'New authentication strength' dialog box with a 'Custom' tab selected. It contains a scrollable list of 20 authentication strength options, each with an unchecked checkbox and a dropdown arrow. The options are grouped into five categories: Phishing-resistant MFA (3), Passwordless MFA (1), Multifactor authentication (13), and Single factor authentication (5). The last category, 'Single factor authentication (5)', is partially visible at the bottom of the list.

Category	Authentication Strength
Phishing-resistant MFA (3)	<input type="checkbox"/> Windows Hello For Business / Platform Credential
	<input type="checkbox"/> Passkeys (FIDO2) <a href="#">Advanced options</a>
	<input type="checkbox"/> Certificate-based Authentication (Multifactor) <a href="#">Advanced options</a>
Passwordless MFA (1)	<input type="checkbox"/> Microsoft Authenticator (Phone Sign-in)
Multifactor authentication (13)	<input type="checkbox"/> Temporary Access Pass (One-time use)
	<input type="checkbox"/> Temporary Access Pass (Multi-use)
	<input type="checkbox"/> Password + Microsoft Authenticator (Push Notification)
	<input type="checkbox"/> Password + Software OATH token
	<input type="checkbox"/> Password + Hardware OATH token
	<input type="checkbox"/> Password + SMS
	<input type="checkbox"/> Password + Voice
	<input type="checkbox"/> Federated Multifactor
	<input type="checkbox"/> Federated Single factor + Microsoft Authenticator (Push Notification)
	<input type="checkbox"/> Federated Single factor + Software OATH token
	<input type="checkbox"/> Federated Single factor + Hardware OATH token
	<input type="checkbox"/> Federated Single factor + SMS
	<input type="checkbox"/> Federated Single factor + Voice
Single factor authentication (5)	<input type="checkbox"/>
	<input type="checkbox"/>

# Authentication Strengths (3 of 3)

Authentication strength policies can be enforced within Conditional Access Policies

Home > Conditional Access | Policies >

## GR3 - Grant Require MFA

Conditional Access policy

[Delete](#) [View policy information](#) [View policy impact \(Preview\)](#)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

GR3 - Grant Require MFA

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All resources (formerly 'All cloud apps')

Network **NEW** ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Sign-in frequency - 7 days

### Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

☒ Require authentication strength ⓘ

Strong Push - no SMS... ▾

**i** To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more](#)

☐ Require device to be marked as compliant ⓘ

# Enable system-preferred MFA

- System-preferred MFA prompts user to sign in using the most secure method they have registered. Administrators can enable system-preferred MFA to discourage use of less secure sign-in methods.
- For example, if a user registered both SMS and Microsoft Authenticator push notifications for MFA, system-preferred MFA prompts the user to sign in using Microsoft Authenticator. The user can still choose to sign in using another method, but they are first prompted to try the most secure method.

**System-preferred multifactor authentication**

This setting designates whether the most secure multifactor authentication method is presented to users. [Learn more](#)

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time. [Learn more](#)

State \*

**Include**   Exclude

Target \* ☒ All users ☐ Select group

## Enable self-service password reset

- Self-service password reset (SSPR) enables users to reset their passwords on-demand instead of requiring administrator intervention. SSPR is available in hybrid environments, including those that utilize Azure AD Pass Through Authentication (PTA).
- SSPR can ensure the user's identity is confirmed with at least two separate methods of identification prior to permitting password reset. With multiple methods set, an attacker would have to compromise both methods before they could maliciously reset a user's password.



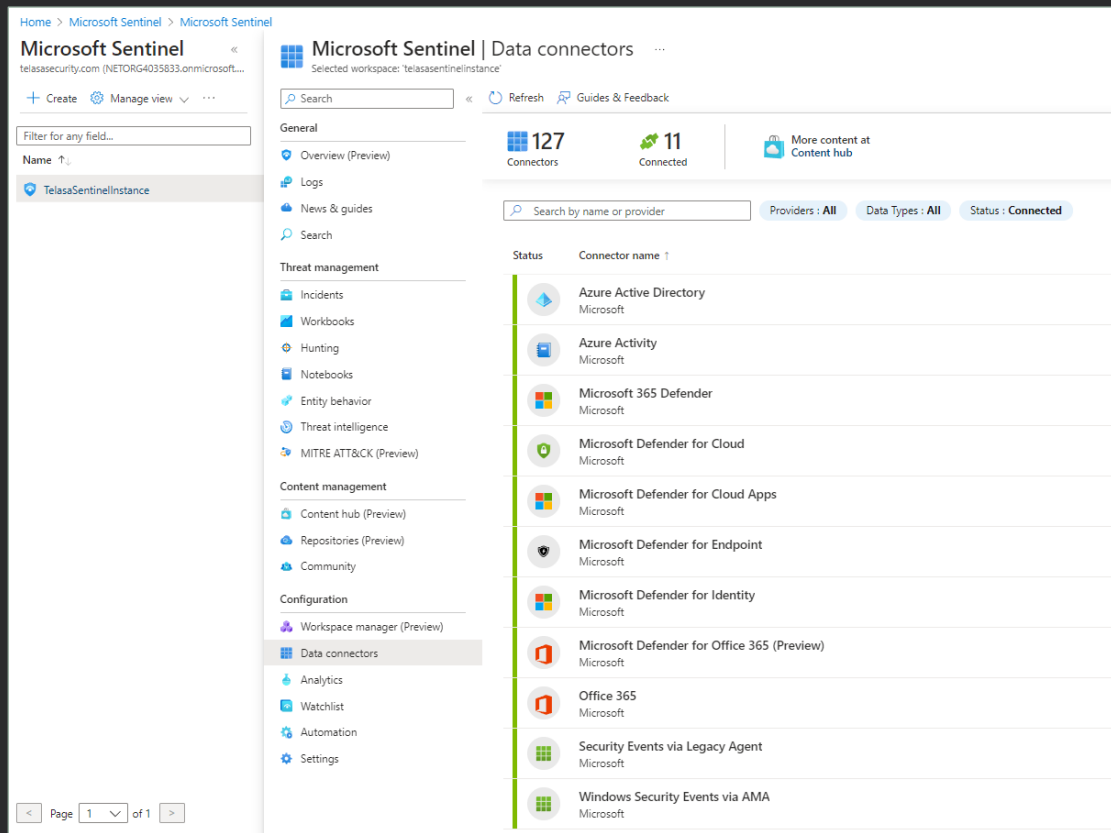
# Microsoft Admin Portals Mandatory MFA Requirements

- <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication>
- Workload identities, such as managed identities and service principals, aren't impacted by MFA enforcement. If user identities sign in as a service account to run automation (including scripts or other automated tasks), that identity needs to sign in with MFA. It's recommended to migrate these user-based service accounts to secure cloud-based service accounts with workload identities.
- Break glass or emergency access accounts are also required to sign in with MFA once enforcement begins. Update these accounts to use passkey (FIDO2) or certificate-based authentication for MFA. Both methods satisfy the MFA requirement.



# Implement Microsoft Sentinel

- Microsoft Sentinel is a recommended SIEM platform for Entra ID and Azure IaaS/PaaS environments for several reasons, including:
- Sentinel is a native Azure service and ingests logs from Azure Log Analytics workspaces.
- 365, Azure AD, and Azure IaaS/PaaS connectors are natively integrated. Ingestion of logging from Microsoft infrastructure is simple and comprehensive. A screen shot of native connectors implemented in a Sentinel instance is shown to right.



# Monitor Entra ID authentication and audit activity

- All Azure AD authentication and audit activity should be logged and analyzed to detect anomalous activity or potentially unauthorized access. Numerous audit tables associated with Azure AD authentication activity are available, as presented in the following screen shot.

The screenshot shows the 'Diagnostic setting' page in the Azure portal. The breadcrumb navigation at the top reads 'Home > telasasecurity.com | Diagnostic settings >'. The page title is 'Diagnostic setting' with a three-dot menu icon. Below the title are action buttons: 'Save', 'Discard', 'Delete', and 'Feedback'. The 'Diagnostic setting name' is 'AzureSentinel\_telasentinelinstance'.

The page is divided into two main sections: 'Logs' and 'Destination details'.

**Logs**

**Categories**

- ☒ SignInLogs
- ☒ AuditLogs
- ☒ NonInteractiveUserSignInLogs
- ☒ ServicePrincipalSignInLogs
- ☒ ManagedIdentitySignInLogs
- ☒ ProvisioningLogs
- ☒ ADFSSignInLogs
- ☒ UserRiskEvents
- ☒ RiskyUsers
- ☒ NetworkAccessTrafficLogs
- ☒ RiskyServicePrincipals
- ☒ ServicePrincipalRiskEvents
- ☒ EnrichedOffice365AuditLogs
- ☒ MicrosoftGraphActivityLogs

**Destination details**

- ☒ Send to Log Analytics workspace
- Subscription:
- Log Analytics workspace:
- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution

# General M365 Security Controls



# Confirm Partner Configuration

Any partners registered in a client environment should be approved, and any Granular Delegated Administrative Privileges (GDAP) should be limited to the minimum privileges required for fulfillment of partnership obligations.

The screenshot displays the Microsoft 365 admin center interface. The left-hand navigation pane includes links for Deleted groups, Roles, Resources, Billing, Support, Settings, Domains, Search & intelligence, Org settings, Integrated apps, Directory sync errors, Partner relationships (highlighted), Setup, Reports, and Health. The main content area is titled "Partner relationships" and contains an introductory paragraph about partner responsibilities, a search bar indicating "1 item", and a section for "Granular delegated administrative privileges (GDAP)". This section features a table with columns for Partner, Roles, Expiration date, and Status. Below this is a section for "Other partner types" with a table listing a partner named "LENOVO PC HK, LTD. (1)" with details for Partner type, Role authorization, and Roles. A red rectangle highlights the GDAP table.

**Microsoft 365 admin center**

Search

## Partner relationships

These are the partners that you authorized to work with your organization. Each partner has different responsibilities for working with your organization, and some might have roles. [Learn more about working with a partner](#)

1 item Search

### Granular delegated administrative privileges (GDAP)

Partner ↓	Roles	Expiration date	Status
-----------	-------	-----------------	--------

### Other partner types

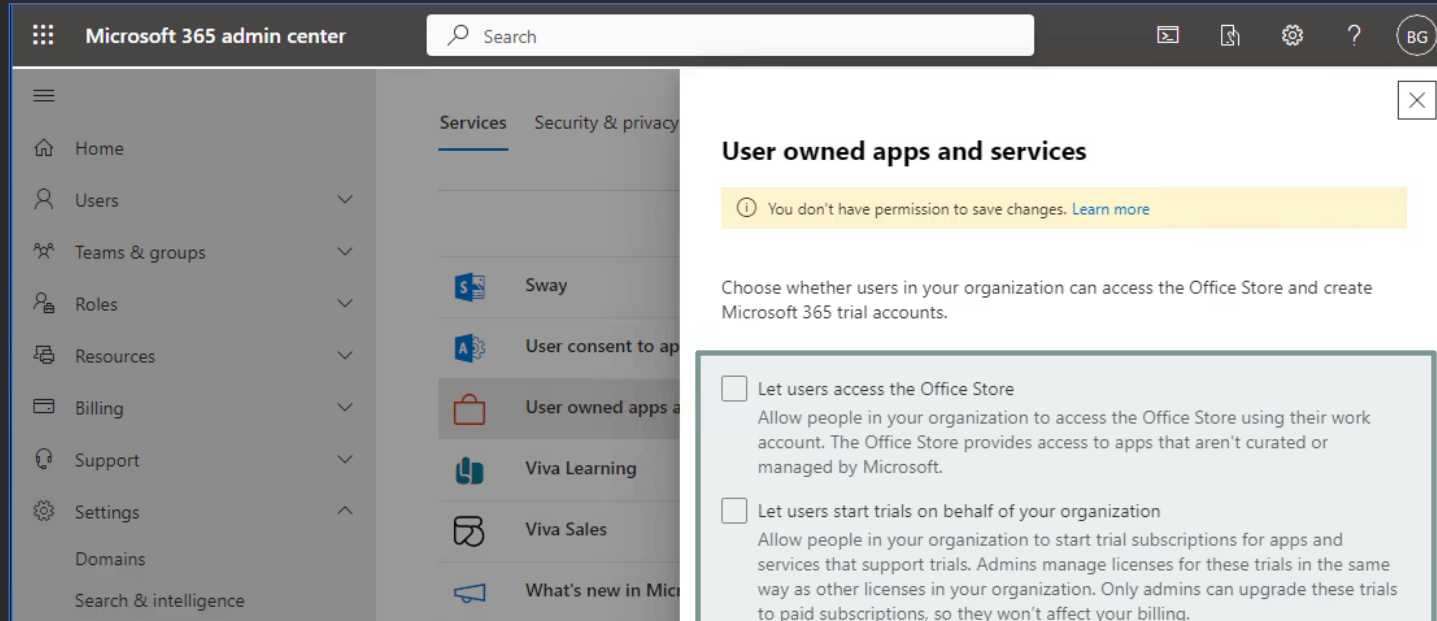
Partner ↓	Partner type	Role authorization ⓘ	Roles
LENOVO PC HK, LTD. (1)	Microsoft OEM PC Partner	None	None assigned

# Azure AD Connect Configuration

- Azure AD Connect is a tool for connecting on-premises identity infrastructure to Microsoft Azure AD.
- Azure AD Connect has been recently targeted by attackers in attempts to pivot from on-premise environments to cloud environments.
- Credentials stored in AD Connect could enable attackers to access cloud resources. The version of AD Connect in the environment should be kept up to date to minimize risks associated with vulnerabilities in AD Connect.

# Restrict Office store access

- By default, users can install add-ins in Outlook, Word, Excel, and PowerPoint, enabling the add-ins to access data contained within each file type
- To reduce risks associated with users installing potentially malicious add-ins, the ability for users to install add-ins should be limited.





# Ensure Purview Monitoring is Enabled

Enabling audit log search in the Microsoft Purview compliance portal can help organizations improve their security posture, meet regulatory compliance requirements, respond to security incidents, and gain valuable operational insights.

The screenshot displays the Microsoft Purview Search interface. The top navigation bar includes the Microsoft Purview logo, a search bar, and icons for Copilot, notifications, and settings. The left sidebar contains navigation links for Home, Solutions, Learn, Settings, and Audit. The main content area is titled "Search" and includes a message: "Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page." Below this message is a blue button labeled "Start recording user and admin activity". The search configuration section is divided into three columns: "Date and time range (UTC) \*", "Activities - friendly names", and "Users". The "Date and time range" column has fields for "Start" (Apr 20 2025, 00:00) and "End" (Apr 21 2025, 00:00). The "Activities - friendly names" column has a dropdown menu labeled "Choose which activities to search for". The "Users" column has a text input field labeled "Add the users whose audit logs you want to se...". Below these columns are sections for "Keyword Search" (text input), "Admin Units" (dropdown), "Activities - operation names" (text input), "Record Types" (dropdown), "File, folder, or site" (text input), and "Workloads" (dropdown). The "Search name" section at the bottom has a text input field labeled "Give the search a name".

Microsoft Purview

Search

Copilot

Home

Solutions

Learn

Settings

Audit

Audit

Search

Policies

Related solutions

eDiscovery

## Search

[Learn about audit](#)

Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page.

**Start recording user and admin activity**

Searches completed | Active searches | Active unfiltered searches

**Date and time range (UTC) \***

Start: Apr 20 2025 00:00

End: Apr 21 2025 00:00

**Keyword Search**

Enter the keyword to search for

**Admin Units**

Choose which Admin Units to search for

**Activities - friendly names**

Choose which activities to search for

**Activities - operation names**

Enter operation values, separated by commas

**Record Types**

Select the record types to search for

**Search name**

Give the search a name

**Users**

Add the users whose audit logs you want to se...

**File, folder, or site**

Enter all or a part of the name of a file, website...

**Workloads**

Enter the workloads to search for

# Key Security Controls in Exchange



# Prohibit installation of Outlook add-ins

- By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application. Attackers could exploit vulnerable or custom add-ins to access user data. Disabling user-installed add-ins in Microsoft Outlook reduces this threat surface.

←

## Default Role Assignment Policy

myPersonalInformation

**Profile information**

- ☒ MyProfileInformation ⓘ
- ☒ MyDisplayName ☒ MyName

**Distribution groups**

- ☒ MyDistributionGroups ⓘ

**Distribution group memberships**

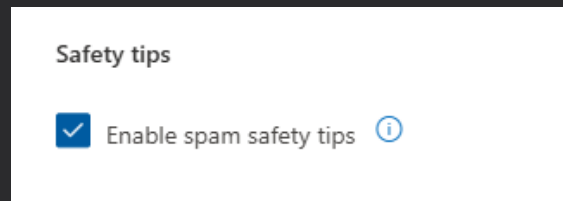
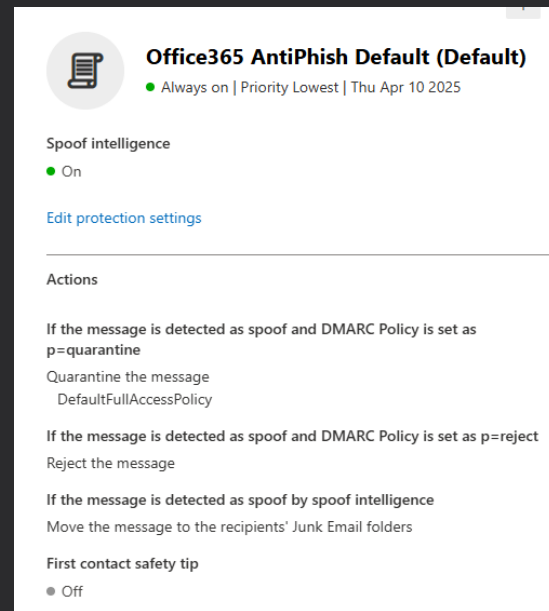
- ☒ MyDistributionGroupMember ship ⓘ

**Other roles**

- ☒ My Custom Apps ⓘ
- ☒ My Marketplace Apps ⓘ
- ☒ My ReadWriteMailbox Apps ⓘ
- ☒ MyBaseOptions ⓘ
- ☒ MyMailSubscriptions ⓘ

# Ensure Mailbox Auditing and MailTips are Enabled

- Mailbox auditing now enabled by default, but exceptions can be implemented for accounts.
- **Audit task:** Periodically review mailbox audit settings for organization to confirm that auditing is enabled appropriately for all accounts and ensure that all exceptions are authorized.
- Ensure MailTips are enabled so that users can see emails from outside the organization
- First time contact and spam safety tips should also be configured to provide users with notification.



# Ensure Appropriate Mail Transport and Forwarding is Configured

- Ensure a Transport rule and Anti-spam outbound policy are used to block mail forwarding.
- Do not whitelist domains in mail transport rules - whitelisting domains in transport rules bypasses regular malware and phishing scanning, which can enable an attacker to launch attacks against your users from a safe haven domain.

## Protection settings

### Message limits

#### Set an external message limit

#### Set an internal message limit

#### Set a daily message limit

#### Restriction placed on users who reach the message limit

### Forwarding rules

#### Automatic forwarding rules

# Safe Links for Office Applications

- Safe Links are available for Exchange, Teams, Office Apps
- URL clicks performs check prior to permitting user to access site
- Requires Defender for Office Licensing

## 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

● On

### Apply real-time URL scanning for suspicious links and links that point to files

● On

### Wait for URL scanning to complete before delivering the message

● On

### Do not rewrite URLs, do checks via Safe Links API only.

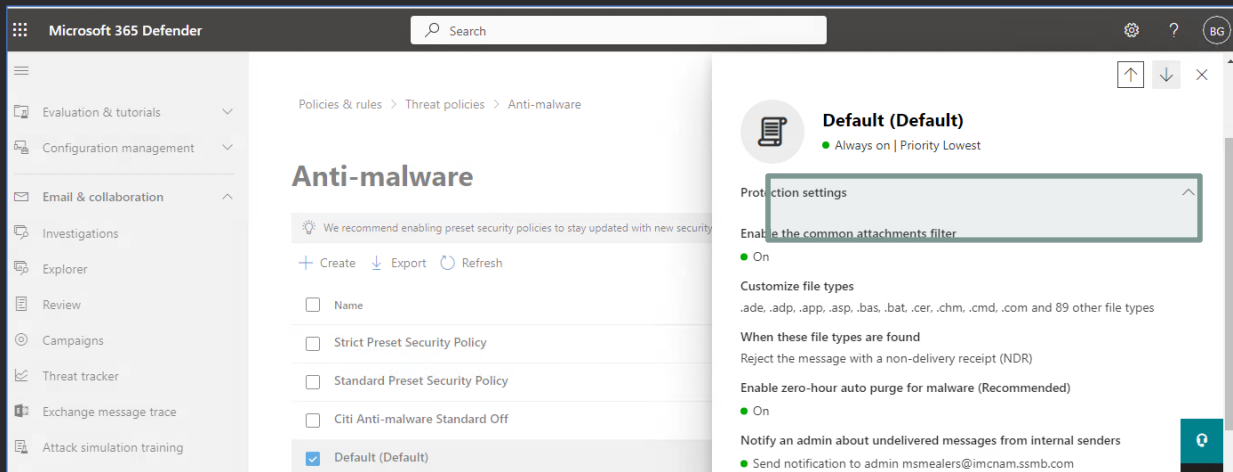
● Off

### Do not rewrite the following URLs in email (0)

-

# Enable Common Attachments Filter

- The common attachments filter blocks known and custom malicious file types from being attached to emails. Blocking known malicious file types can help prevent malware-infected files from infecting a host.



# Ensure SPF, DKIM, DMARC records are published for Exchange Domains

- SPF records allow Exchange Online Protection and other mail systems to know where messages from domains are allowed to originate. This information can be used by that system to determine how to treat the message based on if it is being spoofed or is valid.
- DKIM lets an organization add a digital signature to outbound email messages in the message header. When DKIM is configured, the organization authorizes its domain to associate, or sign, its name to an email message using cryptographic authentication. Email systems that get email from this domain can use a digital signature to help verify whether incoming email is legitimate.
- DMARC, or Domain-based Message Authentication, Reporting, and Conformance, assists recipient mail systems in determining the appropriate action to take when messages from a domain fail to meet SPF or DKIM authentication criteria.



# Key Security Controls in SharePoint

The background of the slide is a photograph of the Charles Bridge in Prague, viewed from a low angle looking down the bridge. The bridge is covered in cobblestones and has several statues and ornate street lamps along its sides. In the distance, the silhouettes of various European-style buildings and domes are visible against a hazy sky. The entire image is overlaid with a color gradient that transitions from a vibrant green on the left side to a deep blue on the right side.

# Restrict External SharePoint and OneDrive Content Sharing

- Content sharing should be as restrictive as possible for the environment.
- Anyone access should not be permitted.

**External sharing**

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

**Anyone**  
Users can share files and folders using links that don't require sign-in.

**New and existing guests**  
Guests must sign in or provide a verification code.

**Existing guests**  
Only guests already in your organization's directory.

**Only people in your organization**  
No external sharing allowed.

# Additional External Sharing Options

- If possible, limit sharing by domain
- If possible allow only users in specific groups to share externally
- Do not allow guests to share items that they do not own
- Where possible, set automatic expiration to SharePoint and OneDrive
- Force users that utilize a verification code to reauthenticate

More external sharing settings ▾

- ☐ Limit external sharing by domain
- ☐ Allow only users in specific security groups to share externally
- ☐ Allow guests to share items they don't own
- ☐ Guest access to a site or OneDrive will expire automatically after this many days
- ☐ People who use a verification code must reauthenticate after this many days [Learn more](#) ⓘ

# Link Sharing

- Set sharing to specific people by default - By defaulting to specific people, the user will first need to consider whether the content being shared should be accessible by select individuals or a wider range. This configuration aids in reinforcing the concept of least privilege.

## File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

☒ Specific people (only the people the user specifies)

☐ Only people in your organization

☐ Anyone with the link

Choose the permission that's selected by default for sharing links.

☒ View

☐ Edit

# Restrict OneDrive Syncing

- If possible, restrict OneDrive syncing only to devices joined to domain. Enabling this feature will prevent users from using the OneDrive for Business Sync client on devices that are not joined to the domains that were defined.

**Settings**

App	Name ↑	Description
SharePoint	Home sites	Set up home sites
SharePoint	Notifications	Allow mobile app r
SharePoint	Pages	Allow users to crea
SharePoint	Site creation	Set default settings
SharePoint	Site storage limits	Use automatic or n
SharePoint	Version history limits	Set how many file
OneDrive	Notifications	Allow notifications
OneDrive	Retention	Set the default On
OneDrive	Storage limit	Set the default stor
OneDrive	Sync	Manage sync settin

**Sync**

Use these settings to control syncing of files in OneDrive and SharePoint.

- ☒ Show the Sync button on the OneDrive website
- ☒ Allow syncing only on computers joined to specific domains

Enter each Active Directory domain as a GUID on a new line.

Example:  
abc12345-1234-abcd-5678-123abcd45678  
def12345-1234-abcd-5678-123abcd45678

☐ Block upload of specific file types

**Learn more**

- [Limit syncing to specific domains](#)
- [Block uploads by file type](#)
- [Download the sync app](#)
- [Troubleshoot sync problems](#)

# Block access to apps that do not use Modern Authentication

- SharePoint environment should enforce strong authentication requirements.

## Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

### Unmanaged devices

Restrict access from devices that aren't compliant or joined to a domain.

### Idle session sign-out

Automatically sign out users from inactive browser sessions.

### Network location

Allow access only from specific IP addresses.

### Apps that don't use modern authentication

Block access from Office 2010 and other apps that can't enforce device-based restrictions.

#### Apps that don't use modern authentication

Some third-party apps and previous versions of Office can't enforce device-based restrictions. Use this setting to block all access from these apps.

☒ Allow access

☐ Block access

# Enable Safe Attachments for Office

- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams protect organizations from inadvertently sharing malicious files. When a malicious file is detected, that file is blocked so that no one can open, copy, move, or share it until further actions are taken by the organization's security team.

## 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

☒

# Key Security Controls in Microsoft Teams

The background of the slide is a dark, atmospheric photograph of the Charles Bridge in Prague. The bridge's cobblestone surface leads the eye into the distance, flanked by stone balustrades and ornate statues. In the background, the silhouettes of historic buildings and church spires are visible against a hazy, teal-colored sky. The overall mood is mysterious and sophisticated.

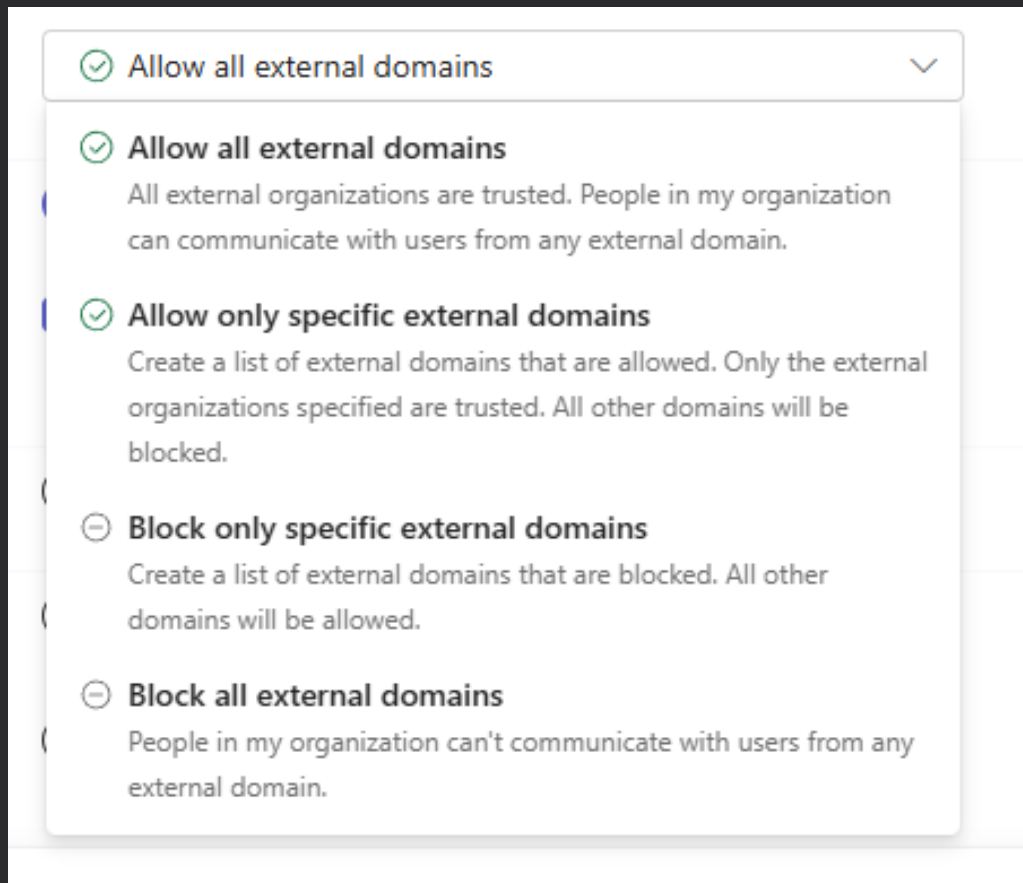


# Restrict Communication with External Organizations

Restrict communication according to organization policies and operations.

There is no universal configuration for this setting – organizations use Teams differently. Two recommended settings are:

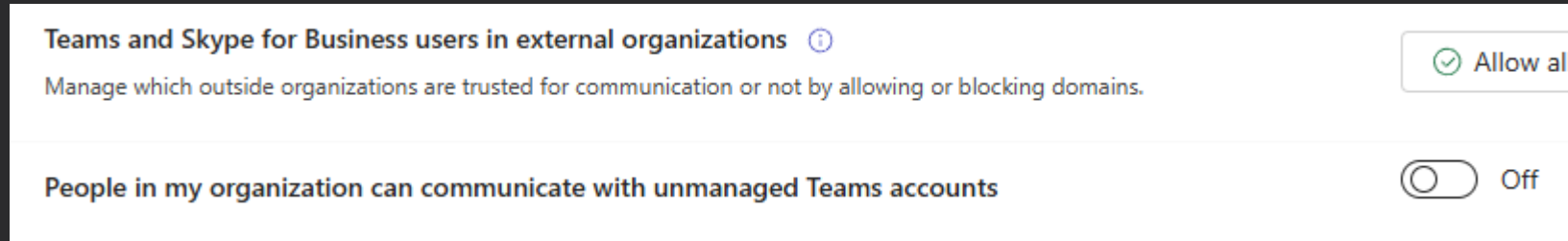
- Allow only specific external domains
- Block all external domains



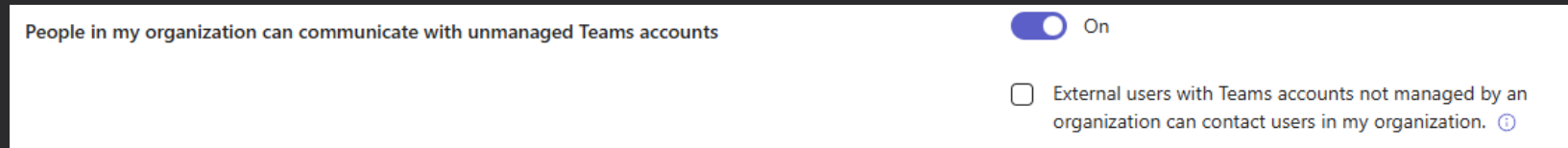
# Restrict Communication with Unmanaged Teams Users

This policy setting controls chats and meetings with external unmanaged Teams users (those not managed by an organization, such as Microsoft Teams (free)).

Recommended setting is: People in my organization can communicate with Teams users whose accounts aren't managed by an organization set to Off.



At minimum, don't let external users initiate conversations.



# Organization App Settings

- Restrict user permissions for adding applications as much as possible.

**Org-wide app settings**

**Tailored apps** ^

Users with F licenses will get tailored apps pinned on their behalf when they sign in to Teams. [Learn more](#)

Show tailored apps ☐ Off

**Microsoft apps** ^

Let users install and use available apps by default [?](#) ☐ Off

**Third-party apps** ^

You can control which third-party apps can be installed for your organization. [Learn more](#)

Let users install and use available apps by default [?](#) ☐ Off

**Custom apps** ^

You can develop and upload custom apps as app packages and make them available in your organization's app store. [Learn more](#)

Let users install and use available apps by default [?](#) ☐ Off

Let users interact with custom apps in preview [?](#)

**Save** **Cancel**

# Block Anonymous User Access

- Microsoft Teams provides an option to block Anonymous users from joining and interacting with apps during meetings. If possible, anonymous users should be restricted from joining meetings.

## Meeting settings

Meeting settings let you customize meeting invitations, set up cross-cloud relationships, and manage network settings for all Teams meetings in your organization. [Learn more about meeting settings](#)



Save time and manage your organization's settings and policies more efficiently with our simplified, all-in-one management center.

Try the new experience



## Participants



Anonymous users can join a meeting ⓘ



Off

Find related settings at [Meetings > Meeting settings](#)

Anonymous users can interact with apps in meetings



Off

# Restrict External Meeting Chat

- Restricting chat access in meetings hosted by external organizations limits possibility of malicious attachments being opened by users.

## Meeting engagement

Meeting engagement settings let you control how people interact in meetings. [Learn more about meeting engagement settings](#)

Meeting chat ⓘ

Find related settings at [Messaging > Messaging policies](#)

In-meeting only except anonymous

External meeting chat ⓘ

☐ Off

Q&A ⓘ

☒ On

Reactions

☒ On

# Key Security Controls in Microsoft Copilot

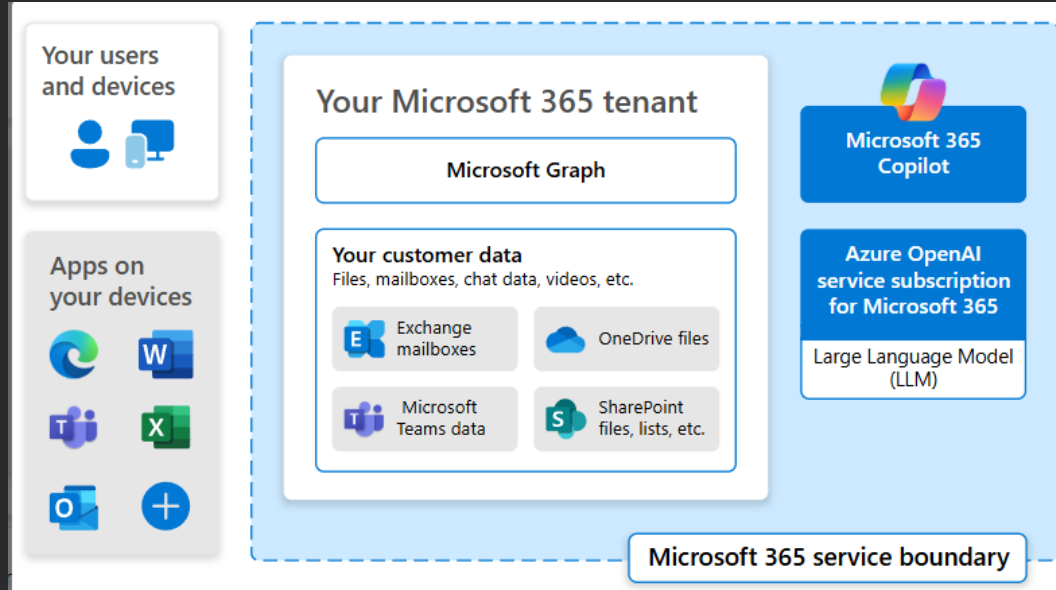
The background image is a dark, atmospheric photograph of a historic bridge, likely the Charles Bridge in Prague, featuring statues and a city skyline in the background. The image is overlaid with a green-to-blue gradient.

# What is Microsoft 365 Copilot?

Microsoft 365 Copilot works with Microsoft 365 apps like Word, Excel, PowerPoint, Outlook, Teams - use Copilot in Word to help create a document, in Excel to get suggestions for formulas, in Outlook to summarize an email thread, and in Teams to summarize meetings.

Uses content in Microsoft Graph to personalize the responses with a user's work emails, chats, and documents. Copilot only shows the data that users have permission to access.

Coordinates large language models (LLMs) to understand, summarize, predict, and generate content.

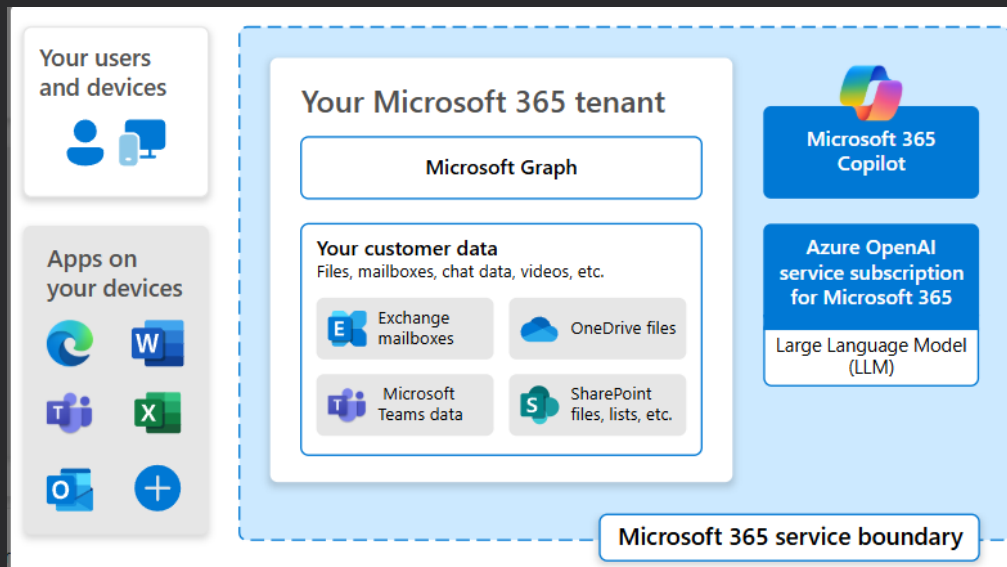


# What is Microsoft 365 Copilot?

When you create a Microsoft 365 subscription, a tenant is automatically created for you. Your tenant sits inside the Microsoft 365 service boundary, where Microsoft 365 Copilot can access organization's data.

Copilot is a shared service, just like many other services in Microsoft 365. When using Copilot:

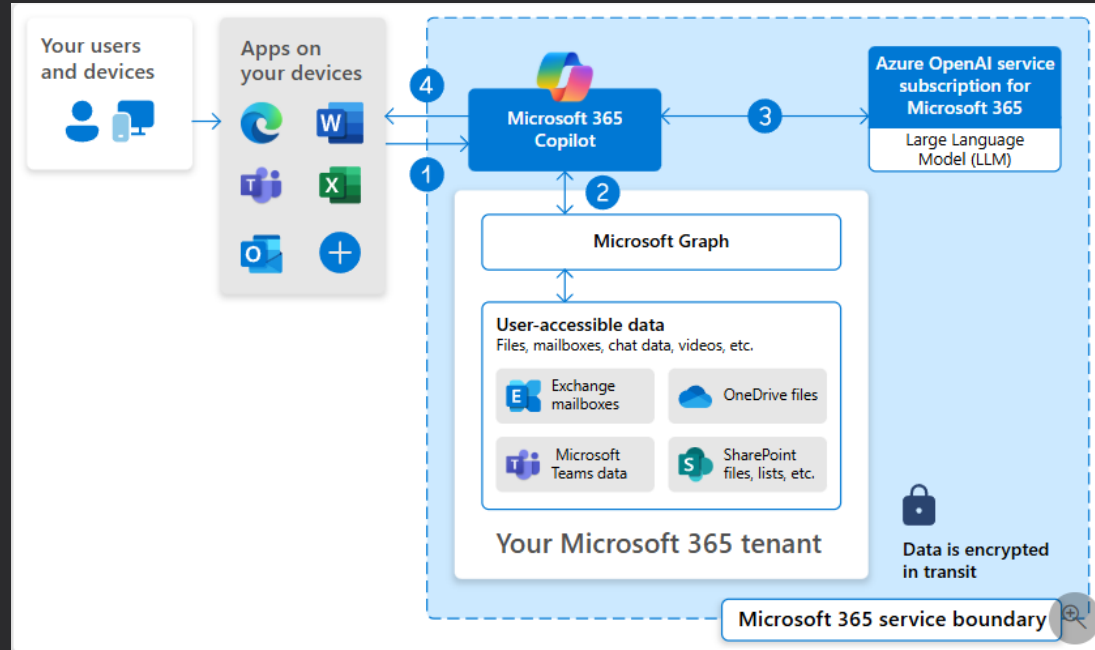
- Customer data stays within the Microsoft 365 service boundary.
- Data is secured based on existing security, compliance, and privacy policies already deployed by your organization.
- Microsoft 365 Copilot uses Azure OpenAI for processing, not OpenAI's public services – when an organization enables Copilot, an instance of OpenAI is created in their tenant.





# How Does a Copilot Request Work?

1. In a Microsoft 365 app, a user enters a prompt in Copilot.
2. Copilot preprocesses the input prompt using **grounding** and accesses Microsoft Graph in the user's tenant. Grounding improves the specificity of prompt, and helps get relevant and actionable answers specific task. The prompt can include text from input files or other content Copilot discovers.
3. Copilot sends the grounded prompt to the LLM. The LLM uses the prompt to generate a response that is contextually relevant to the user's task.
4. Copilot returns the response to the app and the user.



## Built-in Copilot Security

- Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft 365 Copilot.
- Microsoft 365 Copilot uses Azure OpenAI for processing, not OpenAI's public services – when an organization enables Copilot, an instance of OpenAI is created in their tenant.
- Copilot data storage - user's prompt and Copilot's response, including citations to any information used to ground Copilot's response stored in user's Copilot activity history.
  - Can be accessed by admins in Content Search or Purview

# Organizational Actions to Secure Microsoft Copilot

- Copilot only accesses data that an individual user is authorized to access, based on, for example, existing Microsoft 365 role-based access controls. This user data includes emails, chats, and documents that the user has permission to access. Copilot doesn't access data that the user doesn't have permission to access.
- Security of Copilot is dependent on security of underlying services - If your SharePoint environment is not secure, your Copilot environment will not be secure. If your Teams environment is not secure, your Copilot environment will not be secure
- There are Microsoft 365 services that help control access and security to your organization's data. These services include Restricted SharePoint Search (RSS), SharePoint Advanced Management (SAM), and Microsoft Purview.

# Oversharing in Microsoft Copilot

## Common causes of Copilot oversharing in SharePoint

### Privacy settings

Public - anyone in the organization can access this site

Public - anyone in the organization can access this site

Private - only members can access this site

Site privacy set to public

### Share "Branding Elements.pptx"

Add a name, group, or email

Add a message

People in Contoso with the link can edit.



Copy link

Send

Link copied. People in Contoso with the link can edit.

Default sharing option is everyone

m365x32957528.sharepoint.com says

You are about to create unique permissions for this document library. Changes made to the parent site permissions will no longer affect this document library.

OK

Cancel

Broken permission inheritance

### Share site

Add users, Microsoft 365 Groups, or security groups to give them access to the site.

Note that this site is part of a Microsoft 365 Group. If you add users here, they will be given access to the site, but not to other group resources such as calendars and conversations. To do that, add members to the group instead.

everyone

Everyone except external users

Search Directory

Use of "everyone except external users" domain group

### Documents

Name	Sensitivity
Branding Elements.pptx	
Cross Cultural Marketing Campaigns.pptx	Confidential
DG-1000 Product Overview.pptx	
DG-2000 Product Overview.docx	Confidential
DG-2000 Product Pitch.pptx	
DG-2000 Product Specification.docx	
International Marketing Campaigns.docx	

Sites and files without sensitivity labels

# Mitigation of Oversharing in Microsoft Copilot

- Microsoft has published guidance to help organizations secure their environment as they are deploying Copilot. Key tasks in this guidance include:
  - Identify the most popular sites & assess oversharing
  - Grant Copilot access to popular, low risk sites
  - Turn on proactive audit and protection
    - Turn off EEEU (everyone except external users) at the tenant level. If content is shared using this type of user group, it is likely overshared and should be reviewed.
  - Discover oversharing risk
  - Restrict sensitive info from Copilot access and/or processing

# Microsoft Copilot References

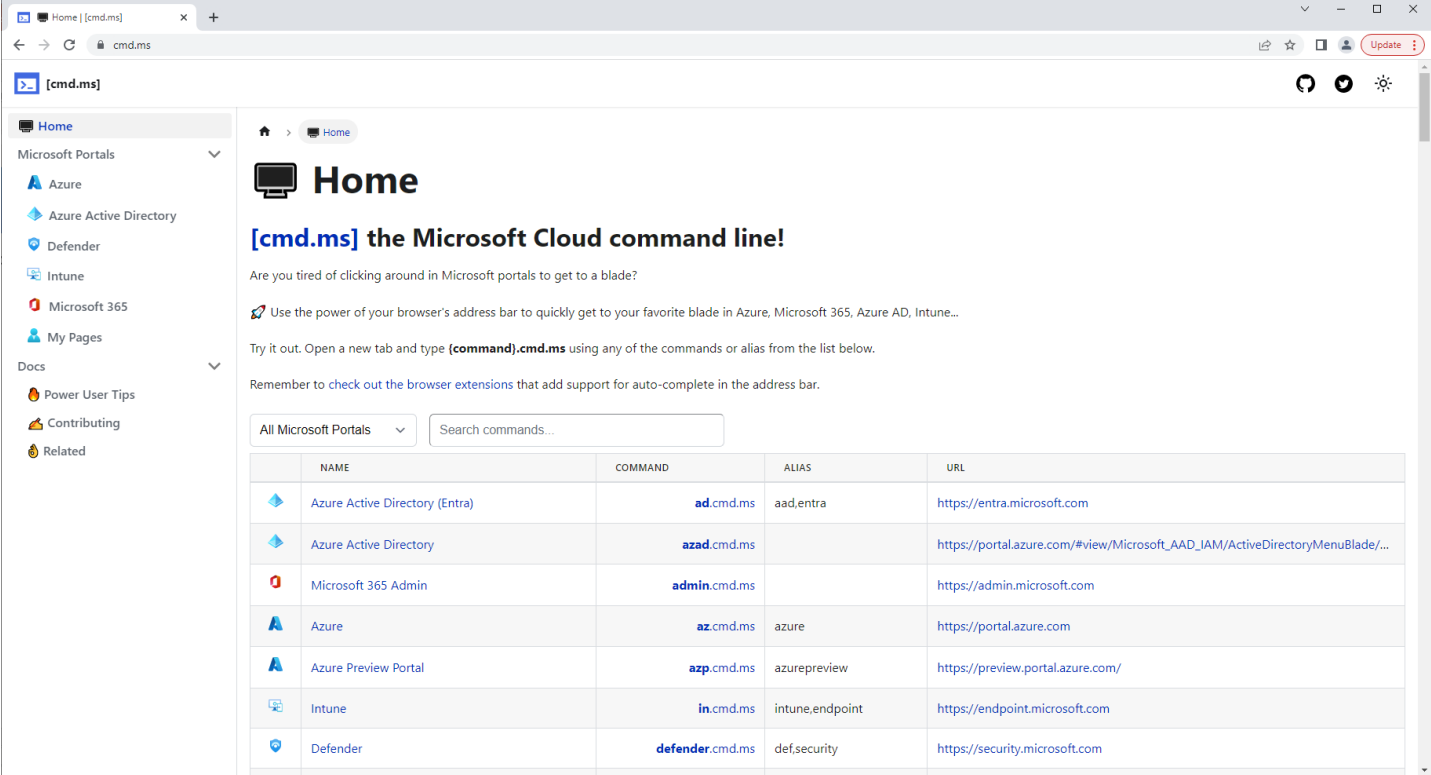
- <https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture>
- <https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-page>

# Appendix – Useful Resources








A teal-tinted photograph of the Charles Bridge in Prague. The bridge's cobblestone path leads towards the city skyline, with several statues and ornate street lamps visible along its length. The background features various church spires and domes under a hazy sky.

# Cloud Command Line

cmd.ms provides quick links to all Microsoft Cloud Portals – over 100 portals!



The screenshot shows the cmd.ms website in a web browser. The page has a sidebar on the left with a list of Microsoft Portals: Azure, Azure Active Directory, Defender, Intune, Microsoft 365, My Pages, Docs, Power User Tips, Contributing, and Related. The main content area is titled "Home" and features a heading "[cmd.ms] the Microsoft Cloud command line!". Below the heading, there is a paragraph explaining the service and a table listing various Microsoft Cloud Portals with their corresponding command-line shortcuts and URLs.

	NAME	COMMAND	ALIAS	URL
	Azure Active Directory (Entra)	<a href="#">aad.cmd.ms</a>	aad,entra	<a href="https://entra.microsoft.com">https://entra.microsoft.com</a>
	Azure Active Directory	<a href="#">azad.cmd.ms</a>		<a href="https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/...">https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/...</a>
	Microsoft 365 Admin	<a href="#">admin.cmd.ms</a>		<a href="https://admin.microsoft.com">https://admin.microsoft.com</a>
	Azure	<a href="#">az.cmd.ms</a>	azure	<a href="https://portal.azure.com">https://portal.azure.com</a>
	Azure Preview Portal	<a href="#">azp.cmd.ms</a>	azurepreview	<a href="https://preview.portal.azure.com/">https://preview.portal.azure.com/</a>
	Intune	<a href="#">in.cmd.ms</a>	intune,endpoint	<a href="https://endpoint.microsoft.com">https://endpoint.microsoft.com</a>
	Defender	<a href="#">defender.cmd.ms</a>	def,security	<a href="https://security.microsoft.com">https://security.microsoft.com</a>



# Least Privileged Roles by Task

Resource for confirming that least privilege roles are being assigned to users:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

Task	Least privileged role	Additional roles
Add user to directory role	Privileged Role Administrator	
Add user to group	User Administrator	
Assign license	License Administrator	User Administrator
Create guest user	Guest Inviter	User Administrator
Reset guest user invite	User Administrator	Global Administrator
Create user	User Administrator	
Delete users	User Administrator	
Invalidate refresh tokens of limited admins	User Administrator	
Invalidate refresh tokens of non-admins	Password Administrator	User Administrator
Invalidate refresh tokens of privileged admins	Privileged Authentication Administrator	
Read basic configuration	Default user role	
Reset password for limited admins	User Administrator	
Reset password of non-admins	Password Administrator	User Administrator
Reset password of privileged admins	Privileged Authentication Administrator	
Revoke license	License Administrator	User Administrator
Update all properties except User Principal Name	User Administrator	
Update User Principal Name for limited admins	User Administrator	
Update User Principal Name property on privileged admins	Global Administrator	
Update user settings	Global Administrator	
Update Authentication methods	Authentication Administrator	Privileged Authentication Administrator Global Administrator

# Questions / Discussion