Key Security Controls in Microsoft 365

TELASA | SECURITY

About Me

Brian Greidanus

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

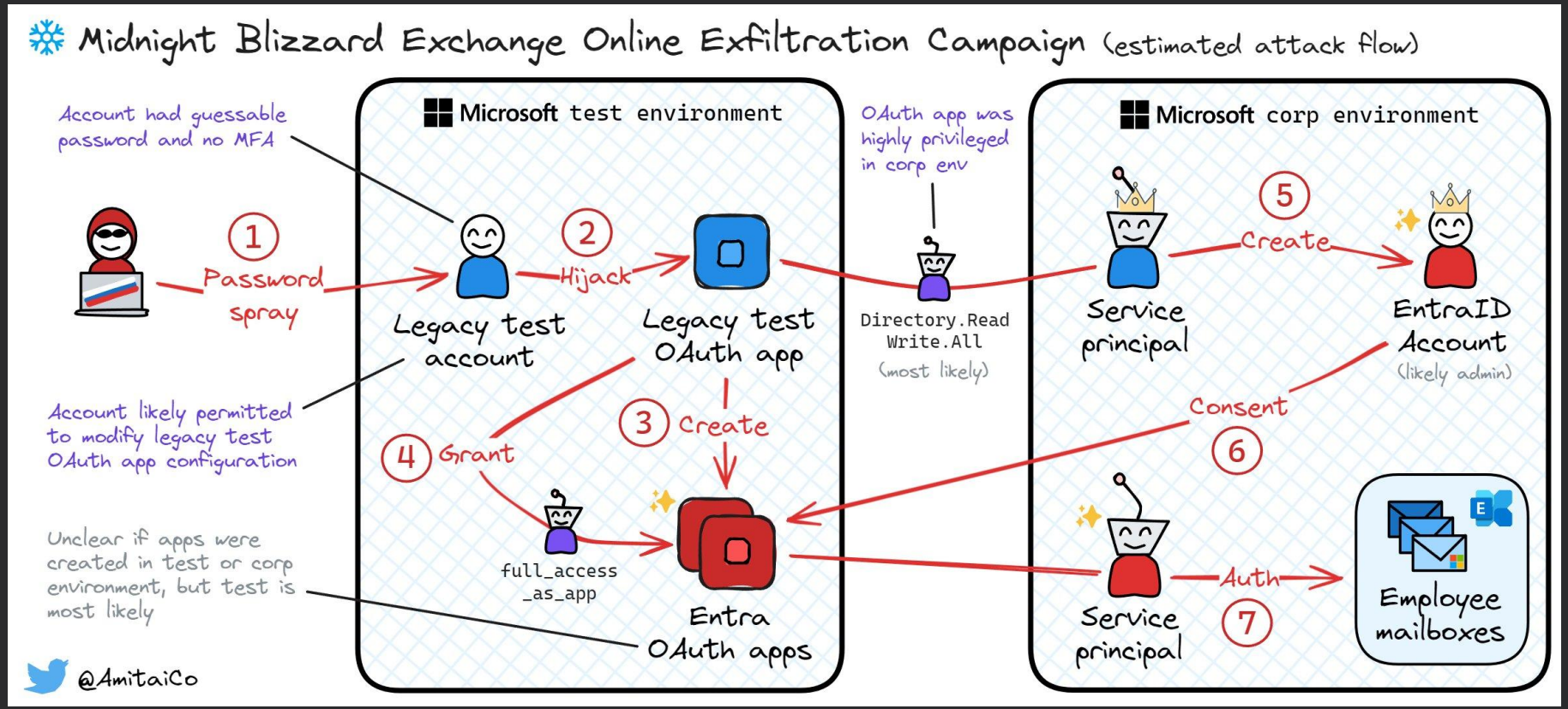
- https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

- 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)



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

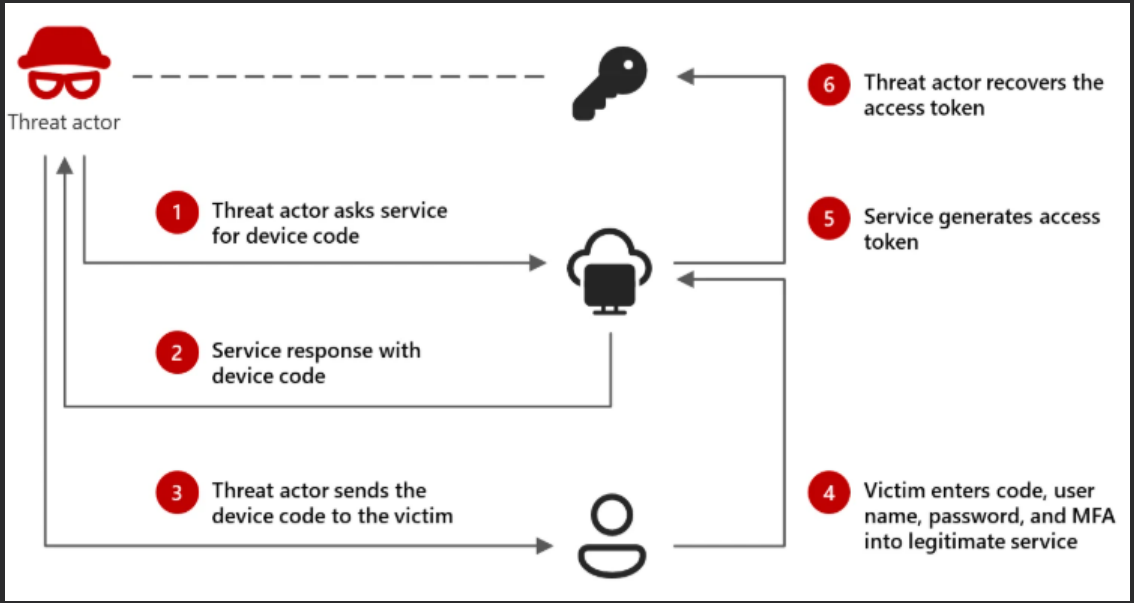
- Device code authentication uses a numeric or alphanumeric code to authenticate an account from an input-constrained device that can't perform interactive authentication on its own (e.g., smart TVs, other smart devices) and must authenticate on another device to sign-in.

- 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.

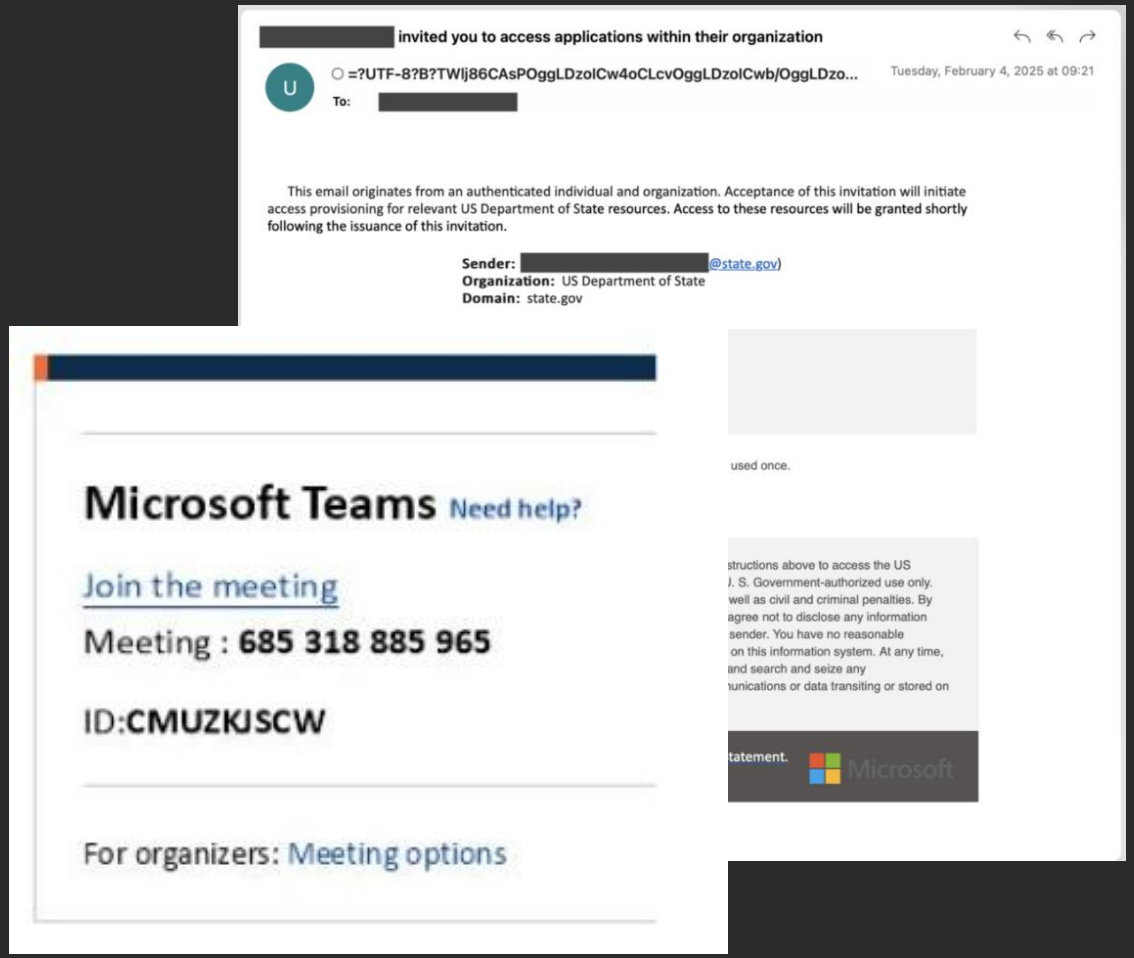
This grants the actor access and enables them to capture valid authentication tokens and use the tokens to access the target's accounts and data.



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 uses Microsoft 365 tenants owned by small businesses they have compromised to host and launch their social engineering attack.

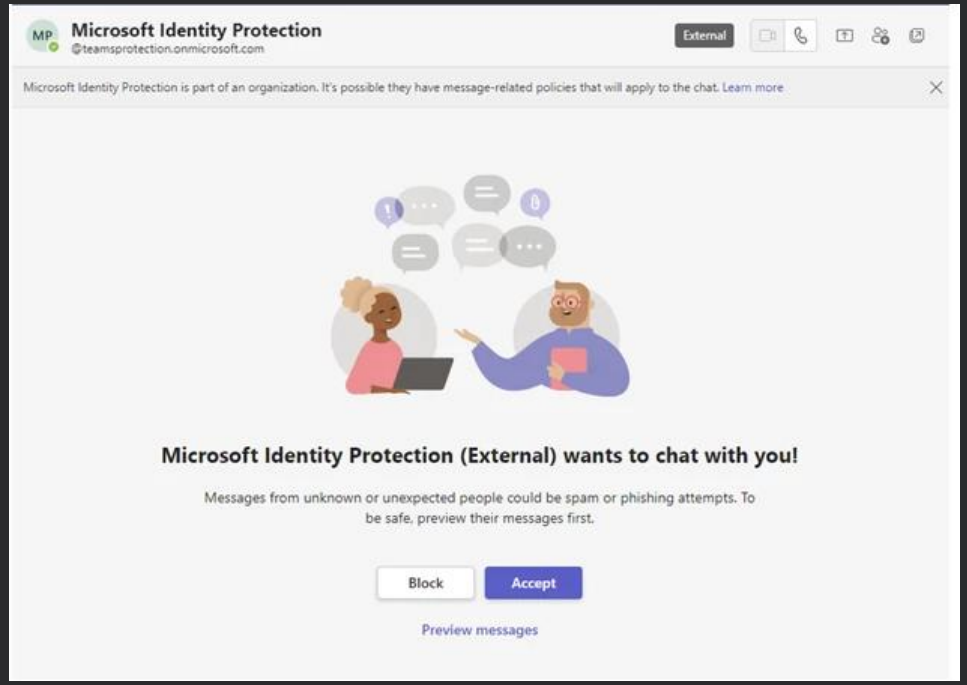
- Bad actor renames the compromised tenant, adds a new onmicrosoft.com subdomain, then sends messages from new subdomain.

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.

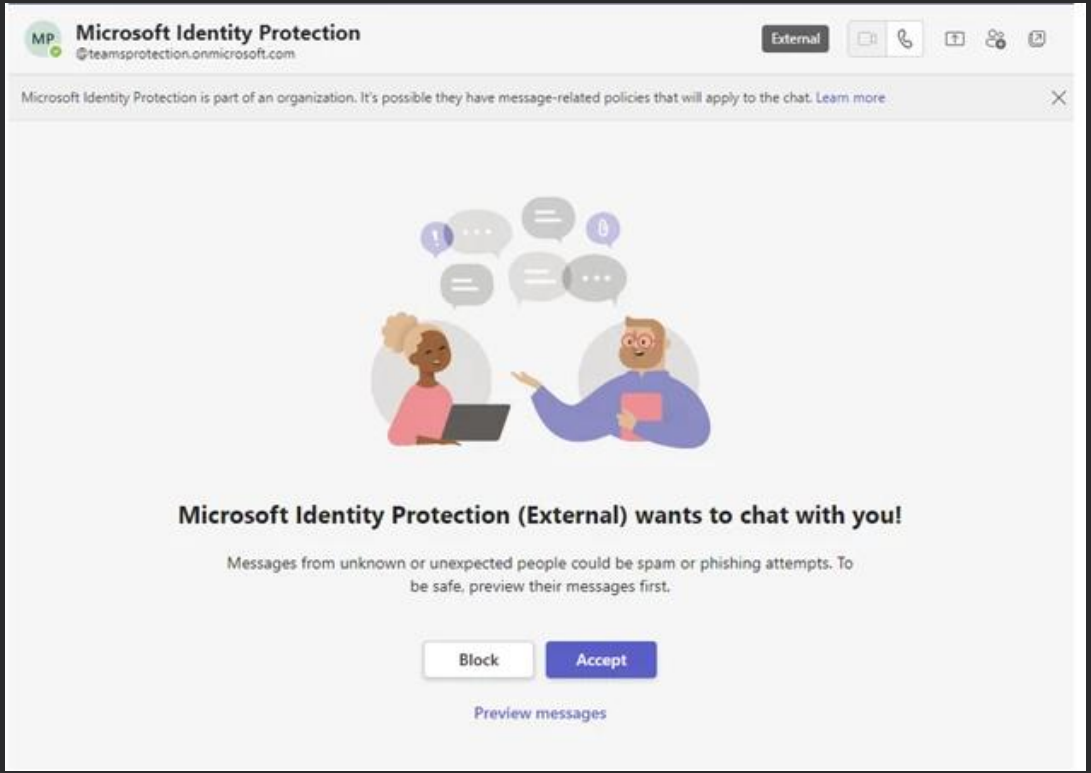


Midnight Blizzard – Teams-based Attacks

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

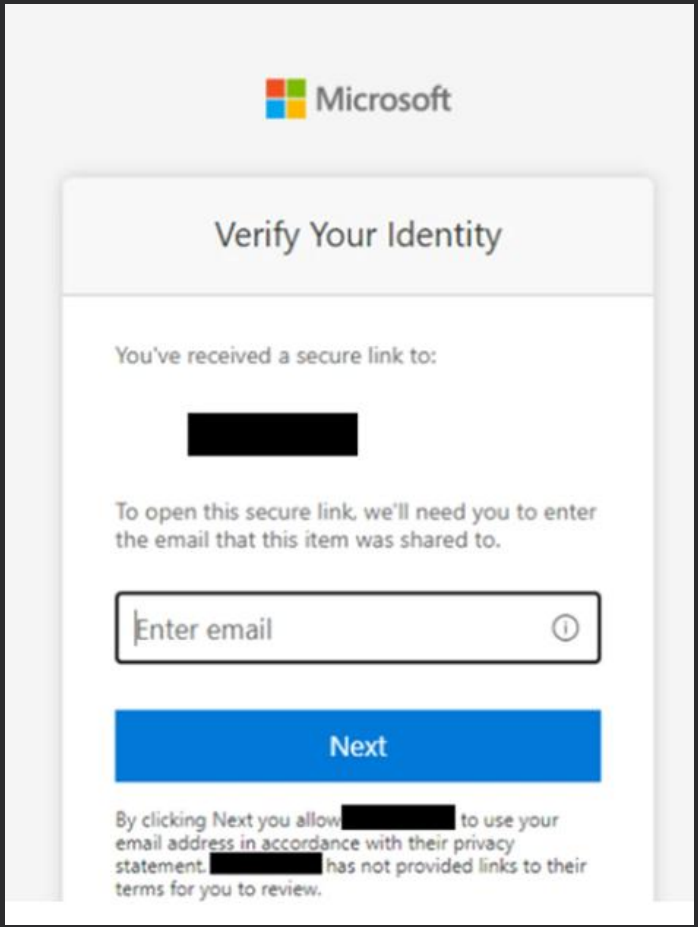
- Educate users about common phishing techniques. Sign-in prompts should clearly identify the application being authenticated to. As of 2021, Microsoft Azure interactions prompt the user to confirm ("Cancel" or "Continue") that they are signing in to the app they expect, which is an option frequently 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

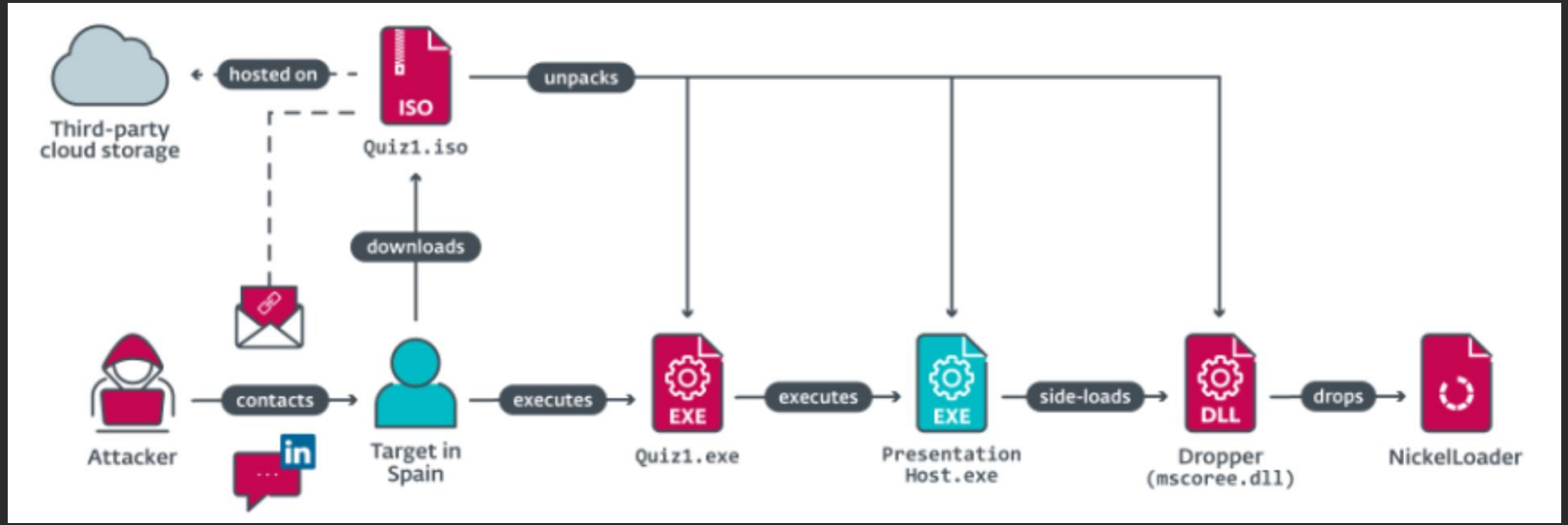
If you need assistance or suspect a security breach, visit: GitHub Security Support

Thank you for keeping your account secure.

GitHub Security Team

Phishing attacks via Fake Dev Recruiters on LinkedIn

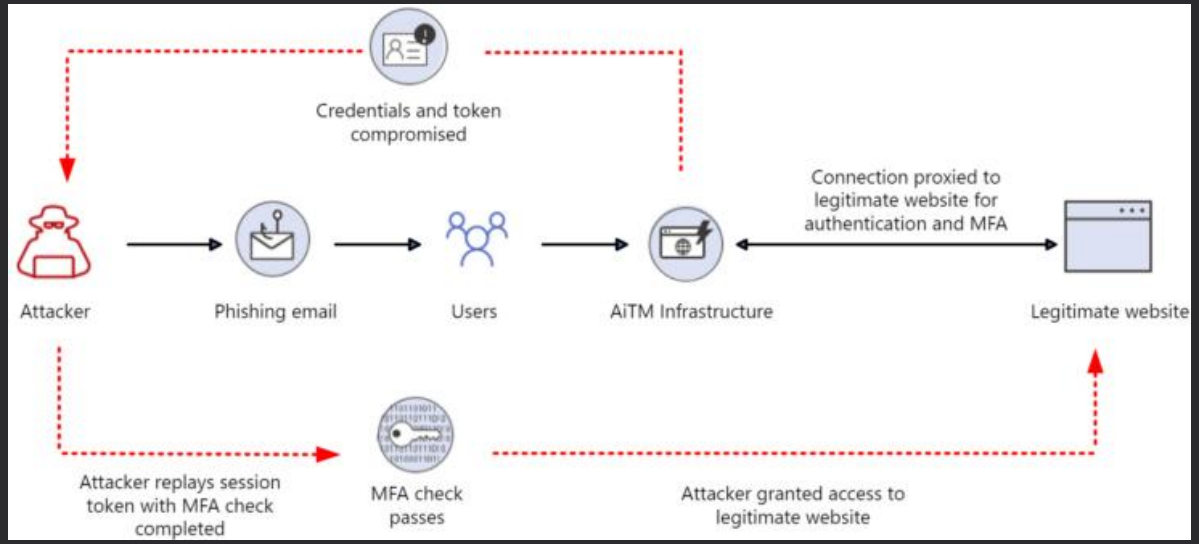
- Coding challenges as part of fake recruitment process are actually attacker backdoors.
- https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/



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

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: C**onfirm 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

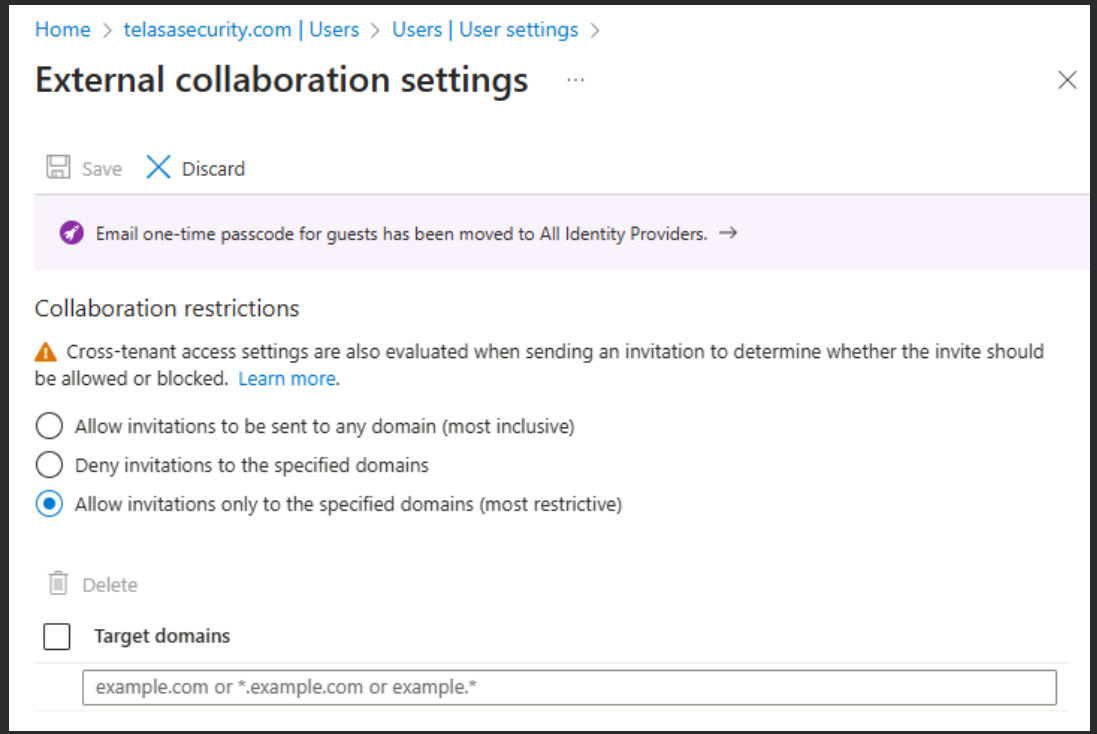
Emergency access or "break glass" accounts are intended for scenarios where normal administrative accounts are unavailable. Break glass accounts are not assigned to specific user and should have a combination of physical and technical controls to prevent them from being accessed outside of a true emergency, 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.

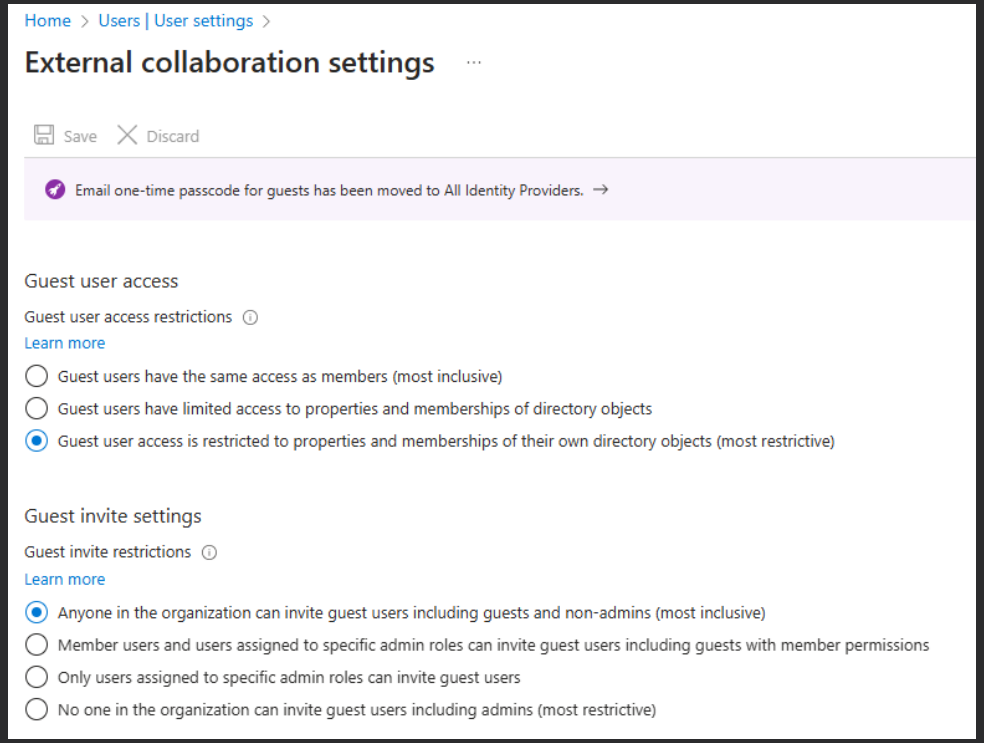
Users should only be permitted to send invitations to explicitly permitted domains. This prevents internal users from sending invitations to unknown external users.



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.

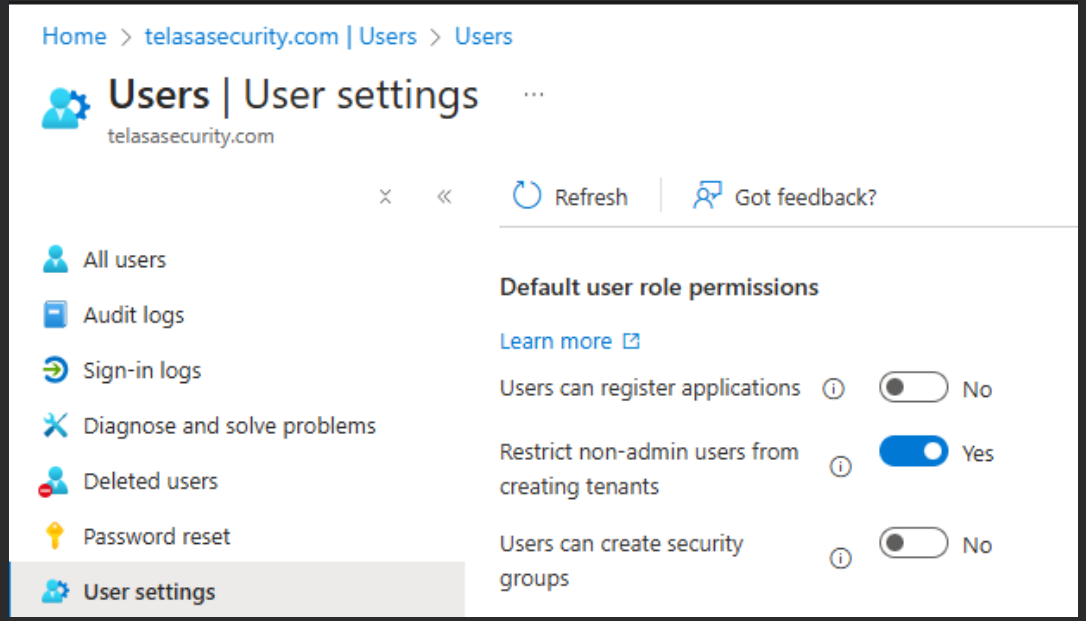


Application Registration / Tenant Creation / Security Group Creation

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.

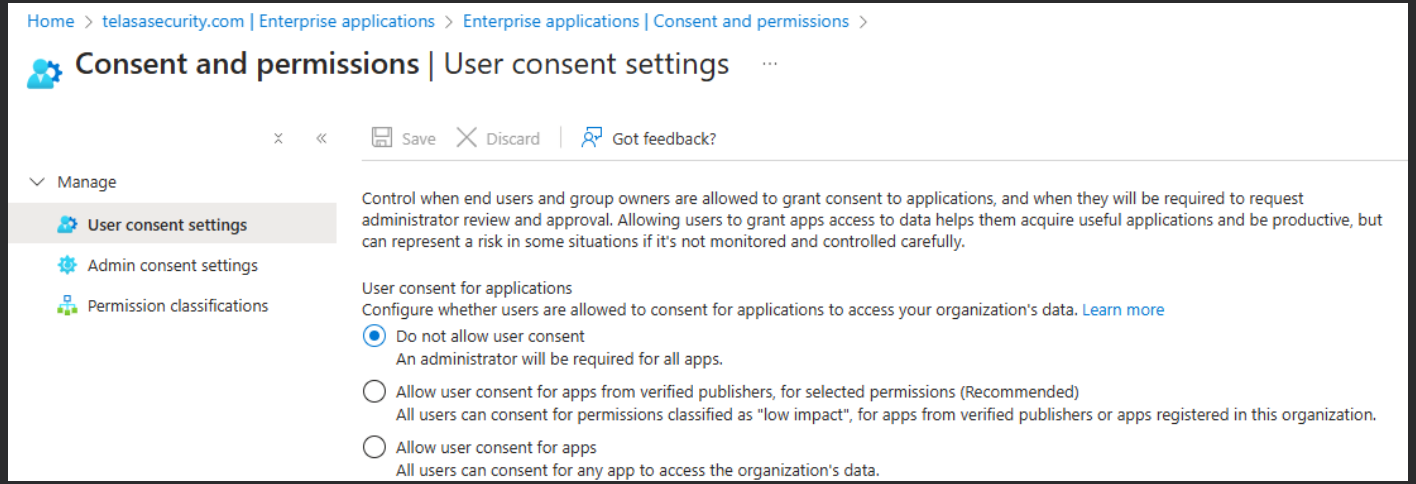


Entra ID – Enterprise Applications and OAUTH Consent

Restrict User Consent for Applications

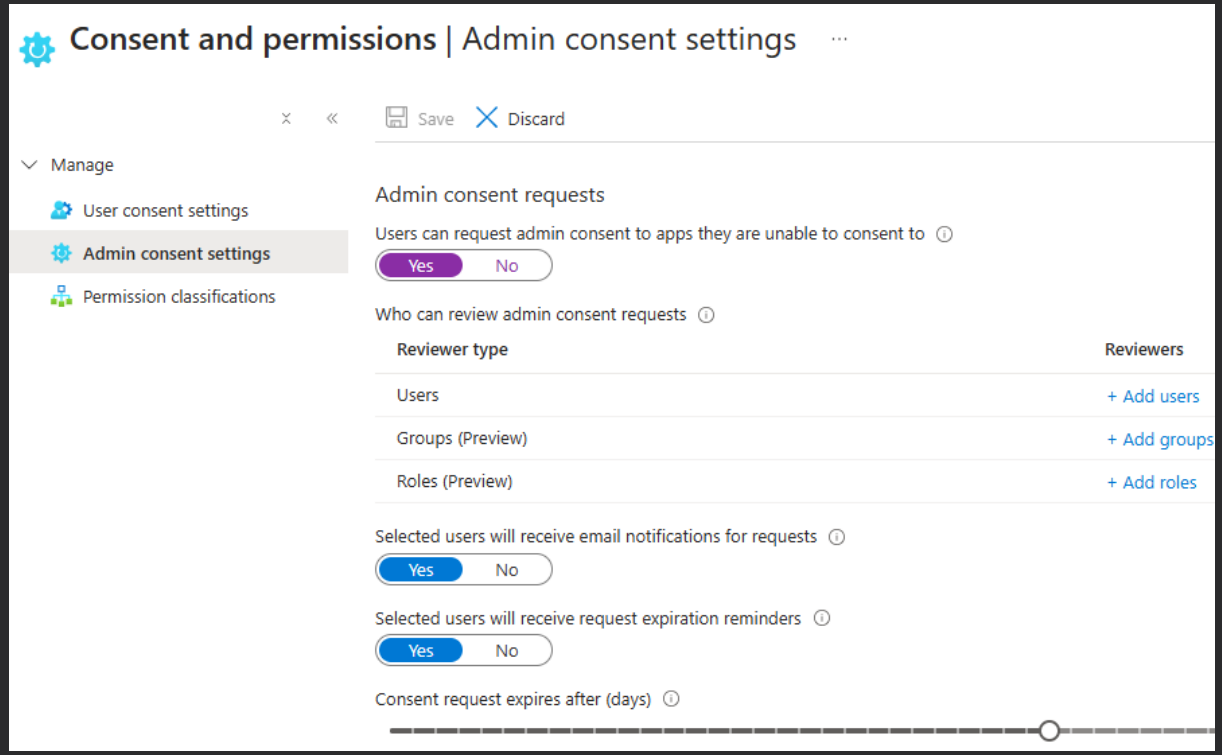
Users can grant consent to applications that can access organization data. Options for this setting, from least to most restrictive, include:

- 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**



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.



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)

Microsoft 365 Defender

Search

Brian Greid

- 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**
  - Investigations

App governance

What's new Learn mor

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

Overview | Apps | Alerts | Policies

63 items Search Customize column

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
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
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
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
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
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
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
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
Coronet	Enabled	Yes	Application	User (0)	Coronet Cyber Secu	Oct 25, 2022 1:03 AM	Jul 22, 2020 2:21 PM	Some unused	0 (0%)	High
Coronet	Enabled	Yes	Mixed	Admin (124)	Coronet Cyber Secu	Oct 25, 2022 1:03 AM	Nov 25, 2019 8:10 AM	Some unused	0 (0%)	High
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
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

Create policy

Create new policy Export

11 items Search

Filter Save the query Reset Filters

Policy name	Status	Severity	Active alerts	Total alerts	Last alert	Last modified	Source	Created by
Unusual activity from an app with priority account consent	Active	Medium	0	0	-	-	Predefined	Microsoft
New app with low consent rate	Active	Medium	0	0	-	-	Predefined	Microsoft
High volume of inbox rule creation activity by an app	Active	Medium	0	0	-	-	Predefined	Microsoft
Increase in data usage by an overprivileged or highly privileged app	Active	Medium	0	0	-	-	Predefined	Microsoft
Spike in Graph API calls made to SharePoint	Active	Medium	0	0	-	-	Predefined	Microsoft
Suspicious app with access to multiple M365 workloads	Active	Medium	0	0	-	-	Predefined	Microsoft
Access to sensitive data	Active	Medium	0	0	-	-	Predefined	Microsoft
Spike in Graph API calls made to Exchange	Active	Medium	0	0	-	-	Predefined	Microsoft
High volume of email sending activities by an app	Active	Medium	0	0	-	-	Predefined	Microsoft
Spike in Graph API calls made to OneDrive	Active	Medium	0	0	-	-	Predefined	Microsoft
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
SK Sarah ...	Yes	0	0
CM Corey ...	Yes	0	0
SI Steve I...	Yes	0	0
MH Micha...	Yes	0	0

Disable app

Entra ID – Conditional Access Policies

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.

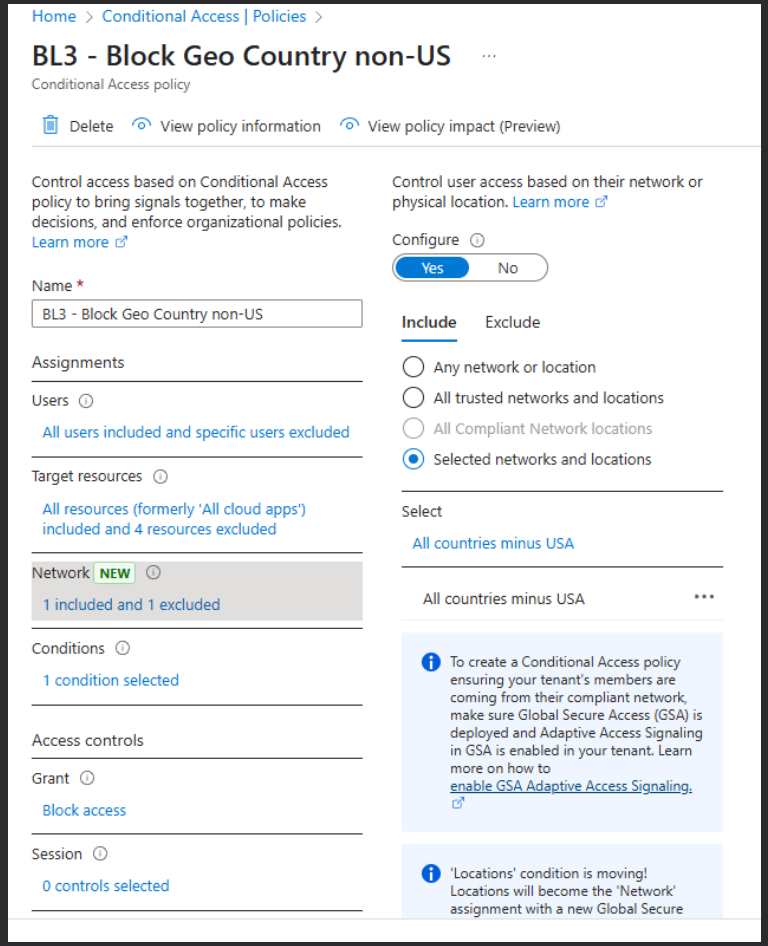
Conditional Access Policies for Legacy Authentication

- 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.



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+/)

Home
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Roles & admins
Roles & admins
Admin units

Home > Roles and administrators

Roles and administrators | Protected actions

Woodgrove - Azure AD for workforce

All roles
Protected actions
Diagnose and solve problems
Activity
Access reviews
Audit logs
Troubleshooting + Support
New support request

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

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
microsoft.directory/conditionalAccessPolicies/basic/update	Update basic properties for conditional access policies	Phishing-resistant MFA required
microsoft.directory/conditionalAccessPolicies/delete	Delete conditional access policies	Phishing-resistant MFA required
microsoft.directory/namedLocations/basic/update	Update basic properties of custom rules that define network locations	Phishing-resistant MFA required
microsoft.directory/namedLocations/create	Create custom rules that define network locations	Phishing-resistant MFA required
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	Microsoft-managed policies
12	0
Total	out of 12

Search

Add filter

12 out of 12 policies found

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

Entra ID – Authentication Methods and Requirements

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

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.

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).

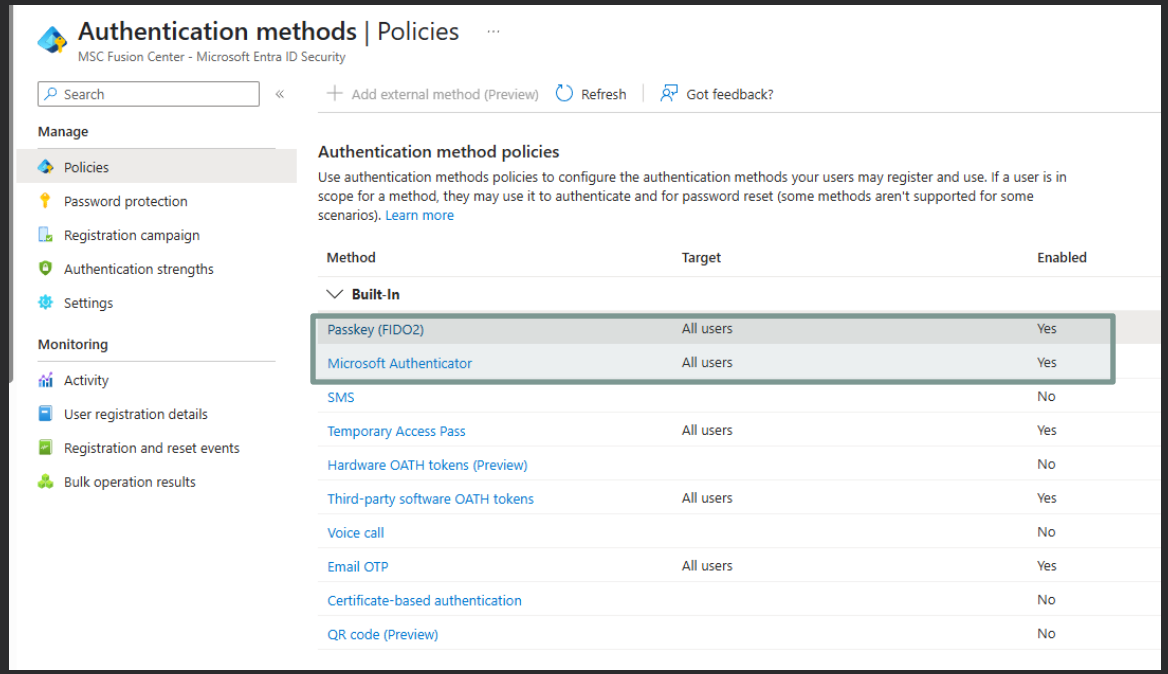
If Unicode characters are accepted in passwords, the verifier **SHOULD** apply the normalization process for stabilized strings using either the NFKC or NFKD normalization defined in Sec. 12.1 of *Unicode Normalization Forms* [UAX15]. This process is applied before hashing the byte string that represents 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.

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.



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:

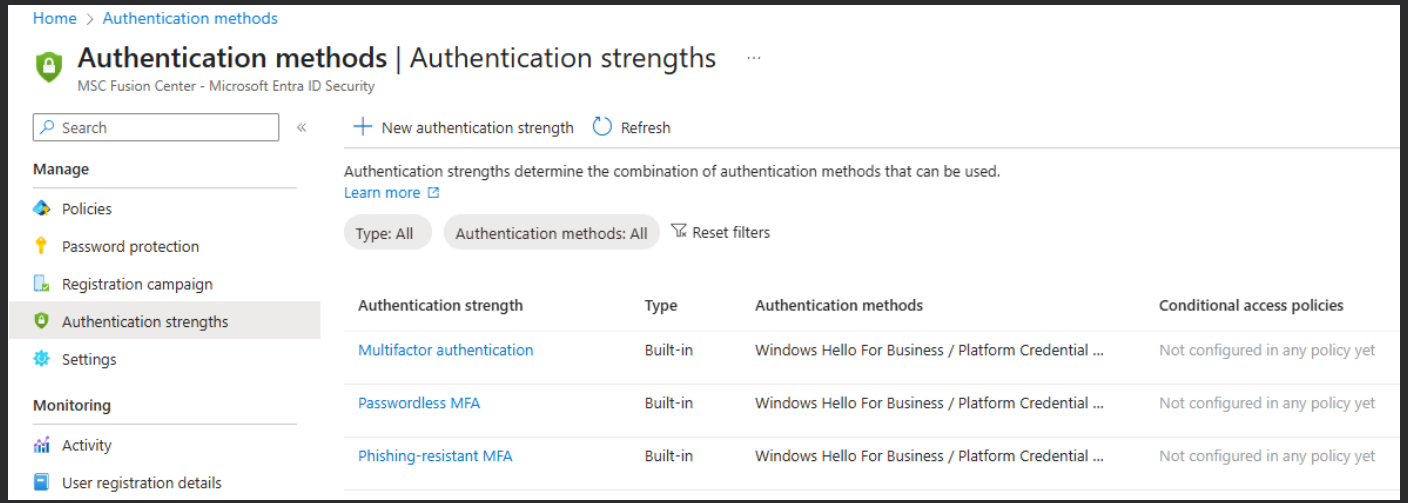
  - MFA number matching requires the user to input a two-digit number presented on the device requesting access into the device performing two-factor authentication. This setting requires the user to have access to both the device requesting the app as well as the device performing MFA, reducing the risk 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)

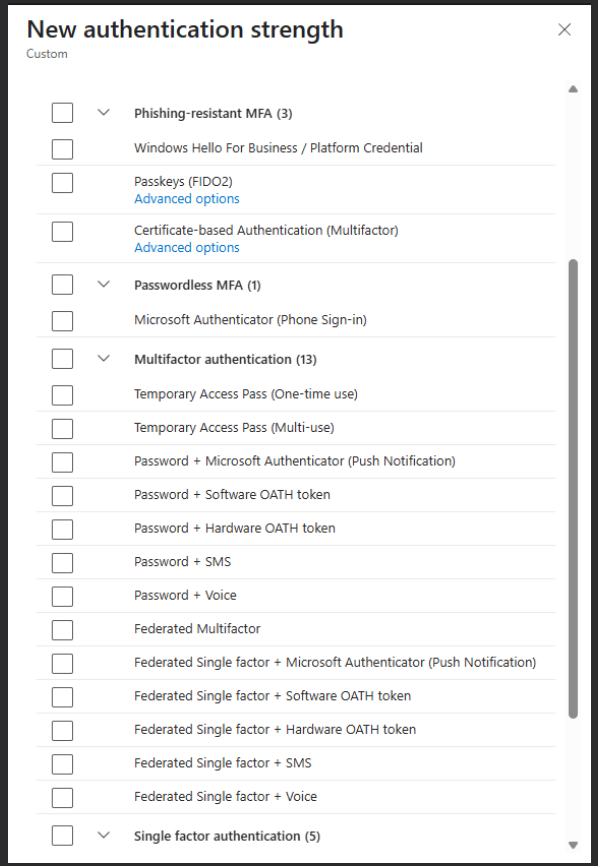
Authentication Strengths Menu allows configuration of sets of authentication factors – three built in policies:

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



Authentication Strengths (2 of 3)

20 different authentication strengths can be defined in policies:



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...

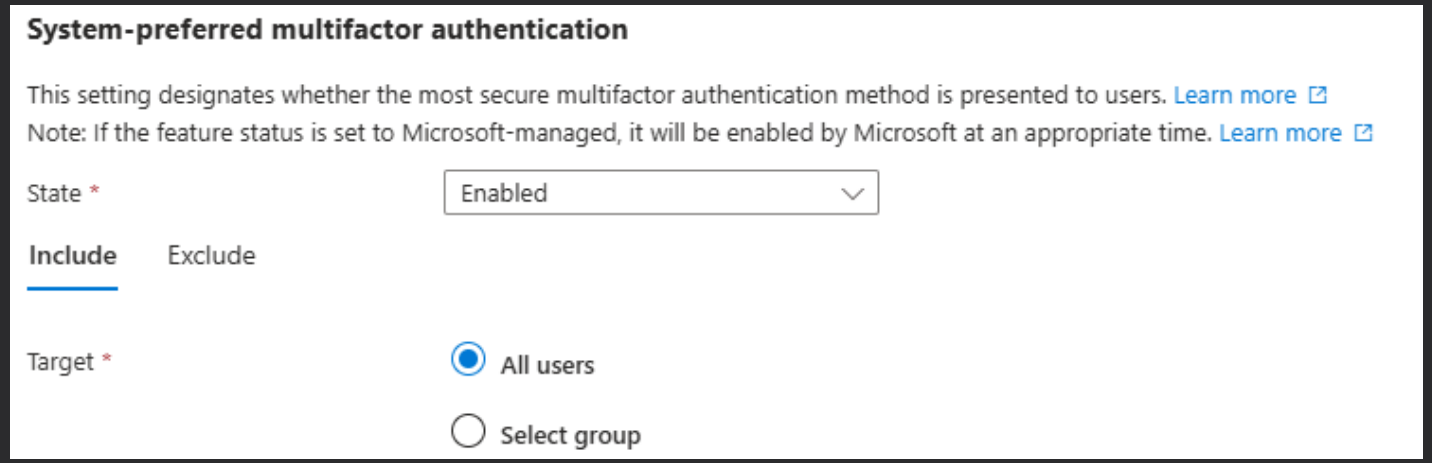
To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. Learn more

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.



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.

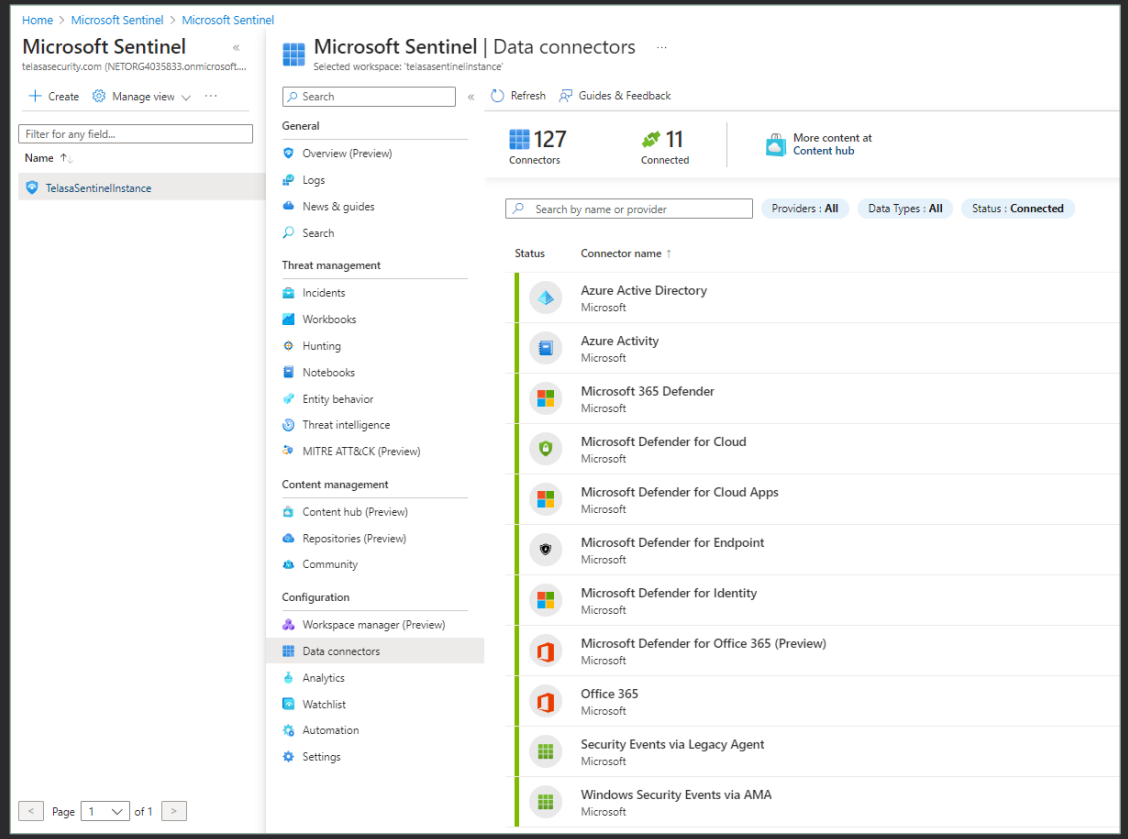
Entra ID – Auditing and Monitoring

Implement Microsoft Sentinel

- Microsoft Sentinel is a recommended SIEM platform for Entra ID and Azure IaaS/PaaS environments for several reasons, including:

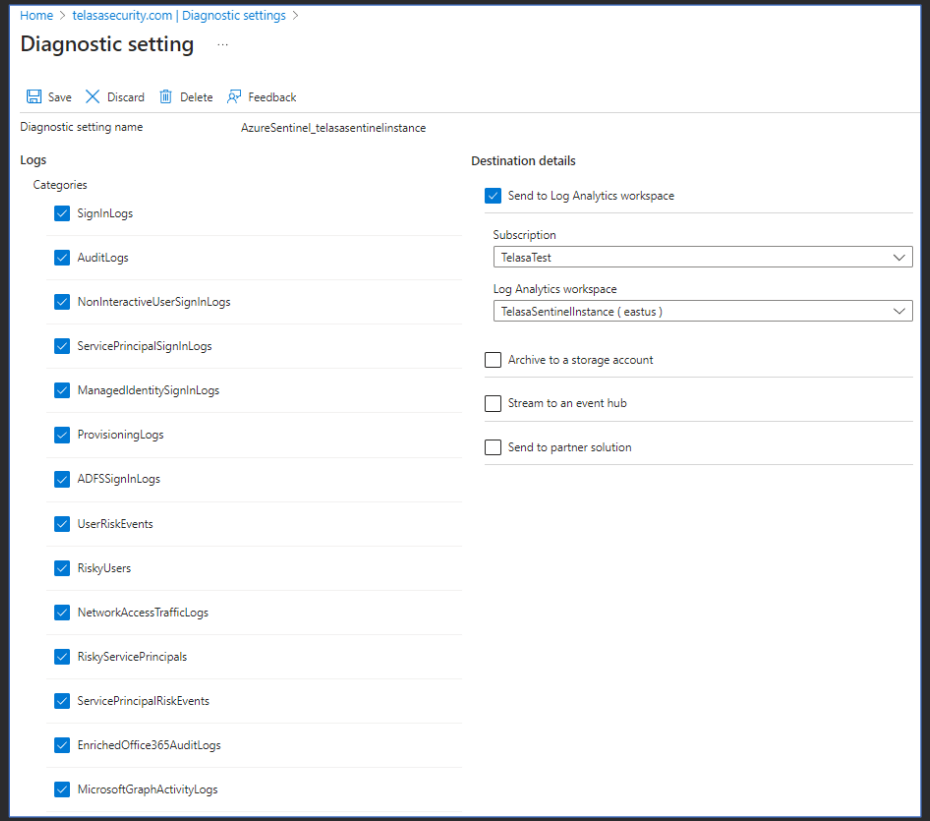
- Sentinel is a native Azure service and ingests logs from Azure Log Analytics workspaces.

- 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

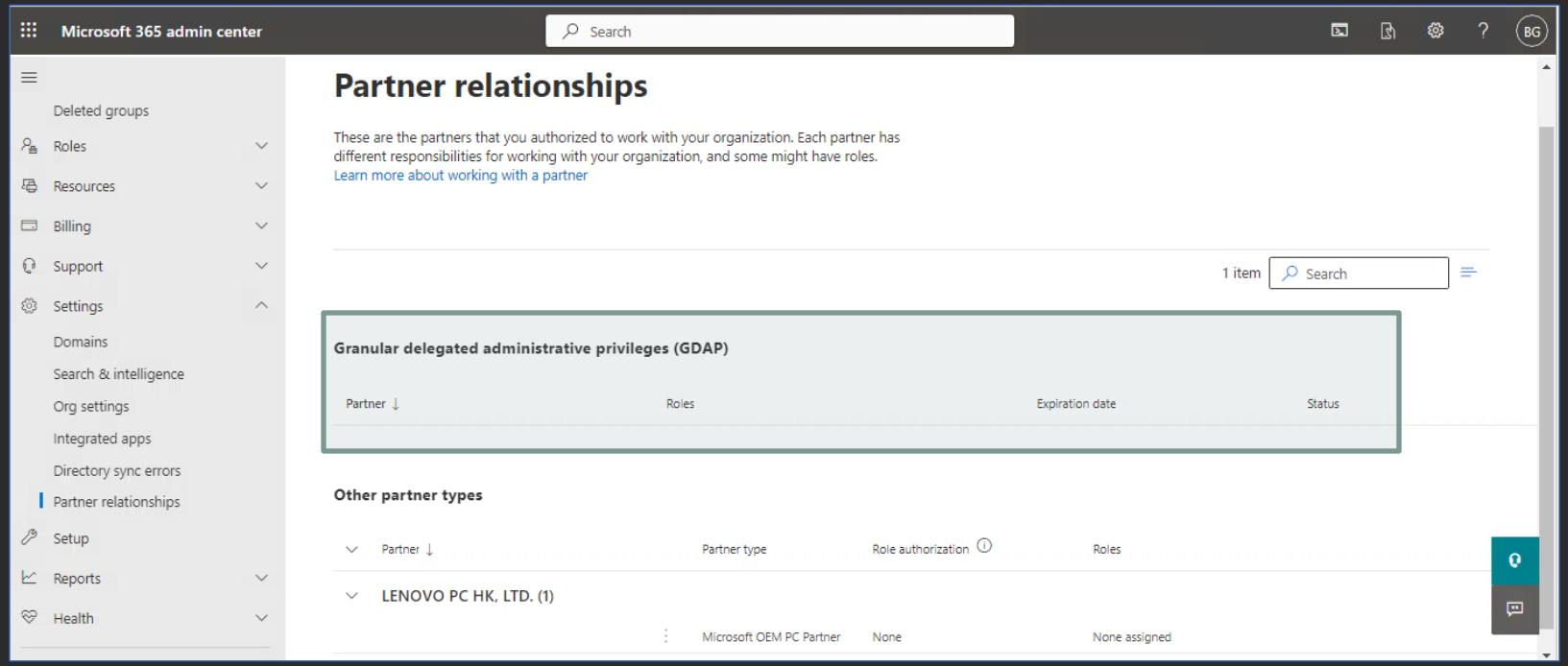
- All Azure AD authentication and audit activity should be logged and analyzed to detect anomalous activity or potentially unauthorized access. Numerous audit tables associated with Azure AD authentication activity are available, as presented in the following screen shot.



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.



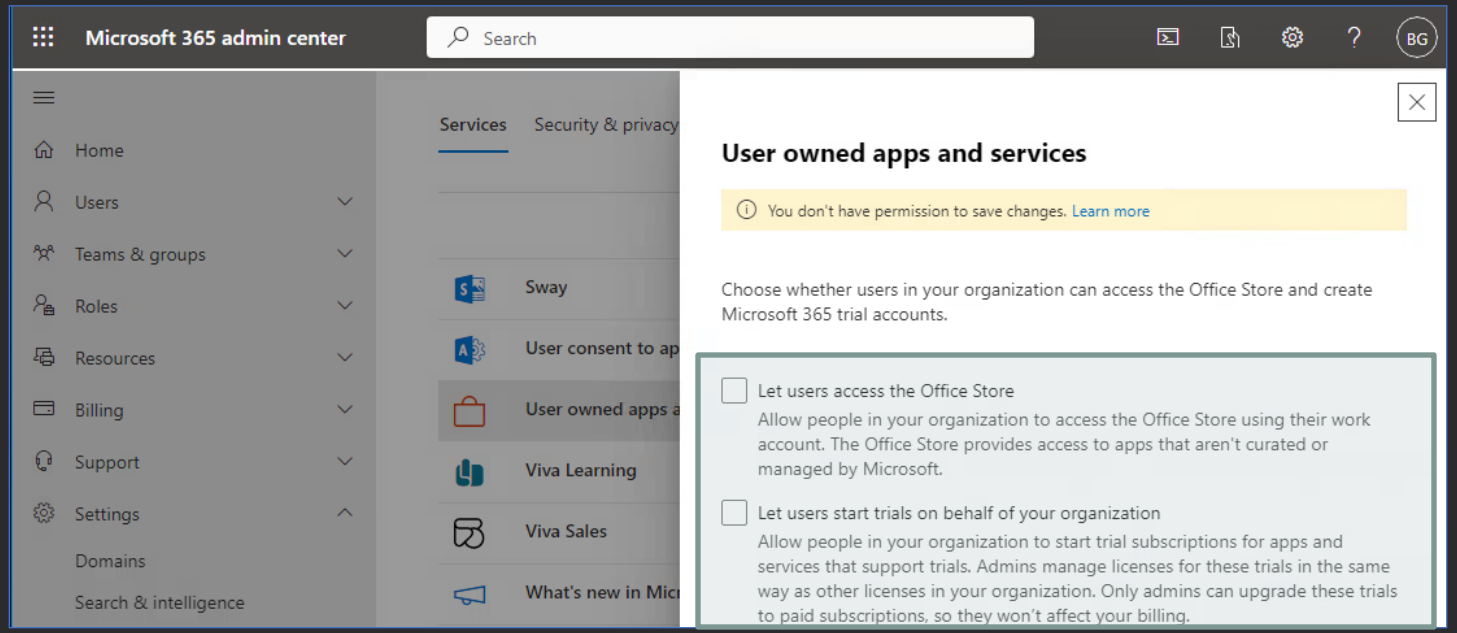
Azure AD Connect Configuration

- 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

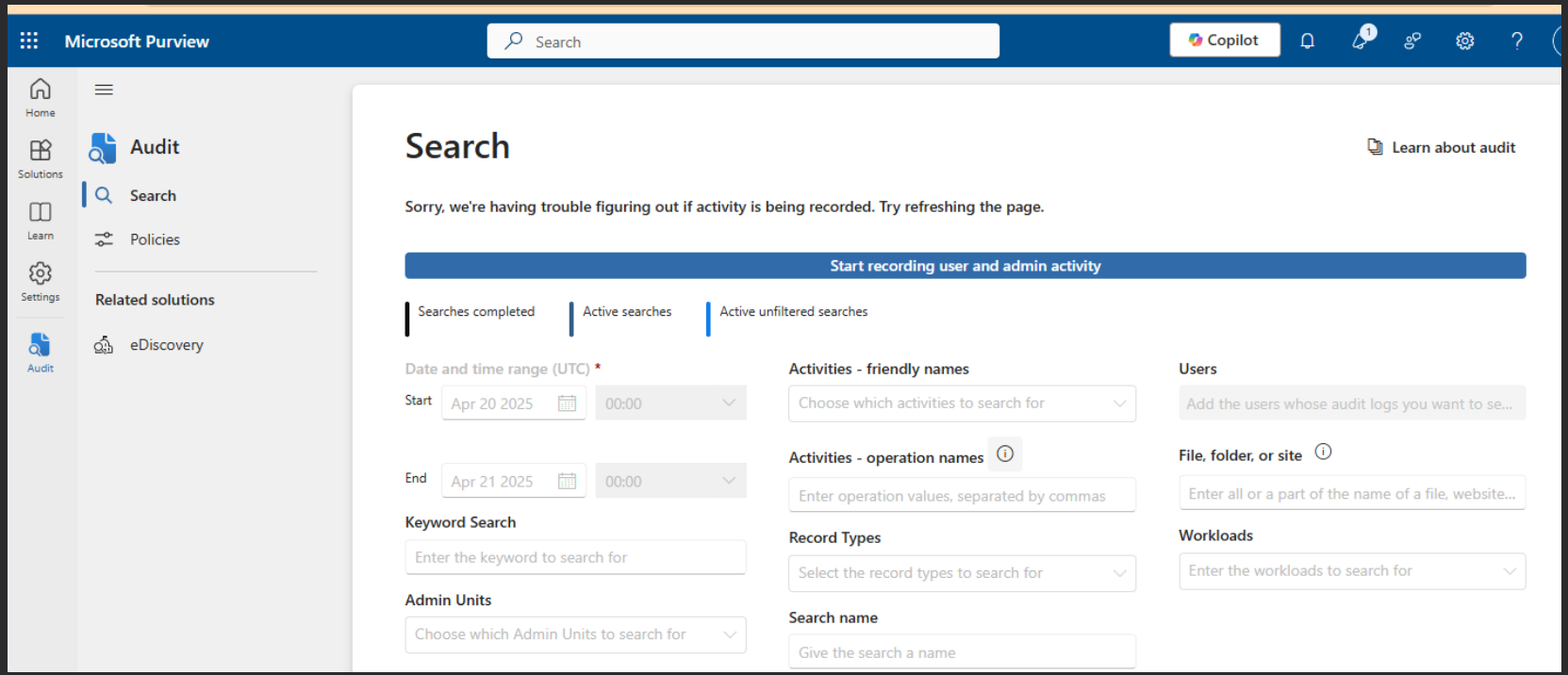
- By default, users can install add-ins in Outlook, Word, Excel, and PowerPoint, enabling the add-ins to access data contained within each file type

- 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

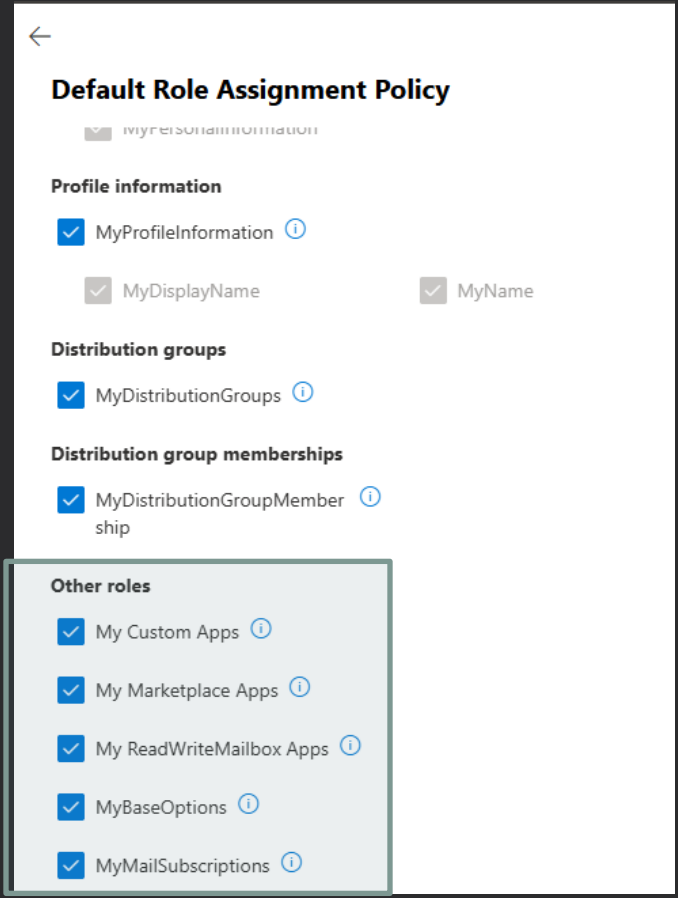
Enabling audit log search in the Microsoft Purview compliance portal can help organizations improve their security posture, meet regulatory compliance requirements, respond to security incidents, and gain valuable operational insights.



Key Security Controls in Exchange

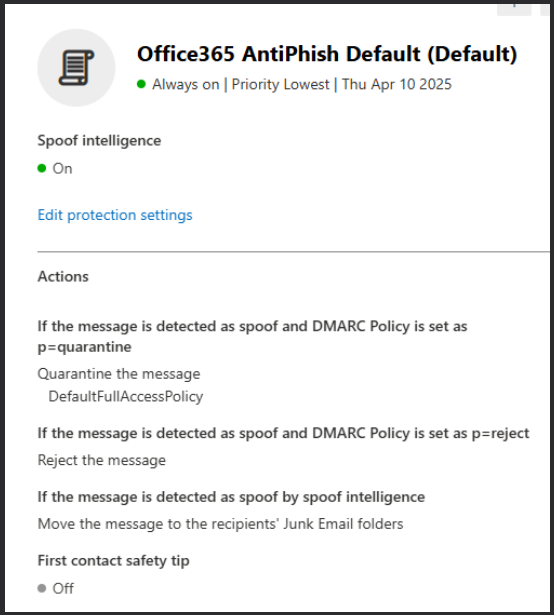
Prohibit installation of Outlook add-ins

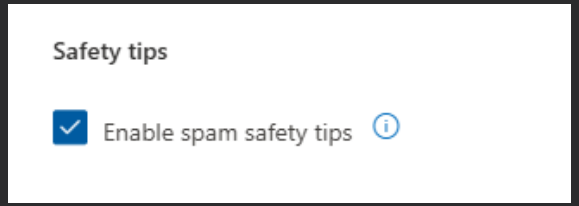
- By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application. Attackers could exploit vulnerable or custom add-ins to access user data. Disabling user-installed add-ins in Microsoft Outlook reduces this threat surface.



Ensure Mailbox Auditing and MailTips are Enabled

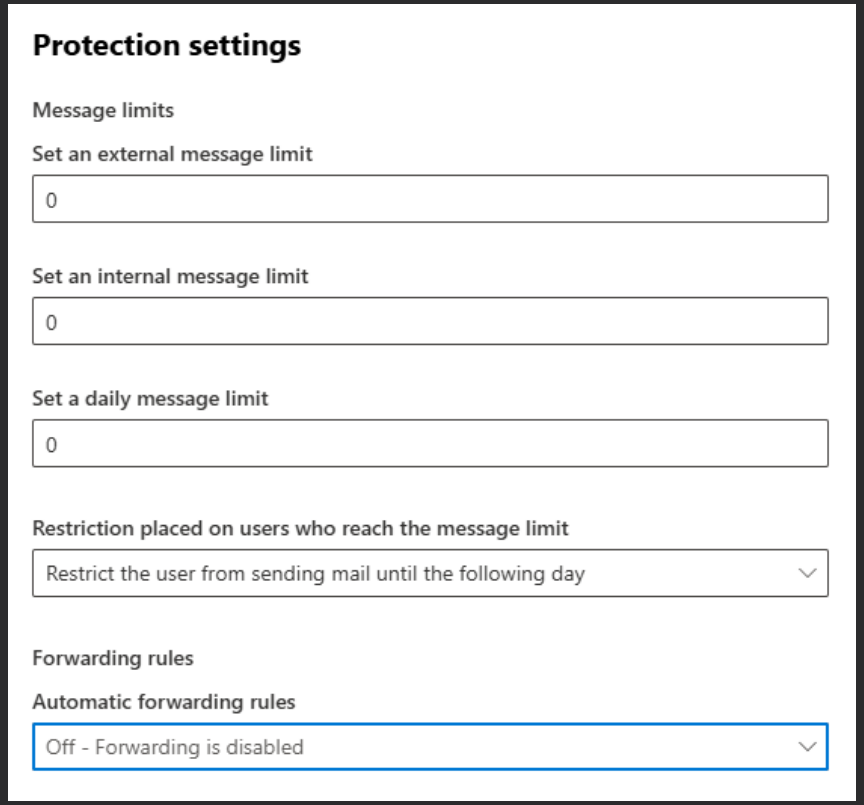
- Mailbox auditing now enabled by default, but exceptions can be implemented for accounts.
- **Audit task:** Periodically review mailbox audit settings for organization to confirm that auditing is enabled appropriately for all accounts and ensure that all exceptions are authorized.
- Ensure MailTips 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.



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.

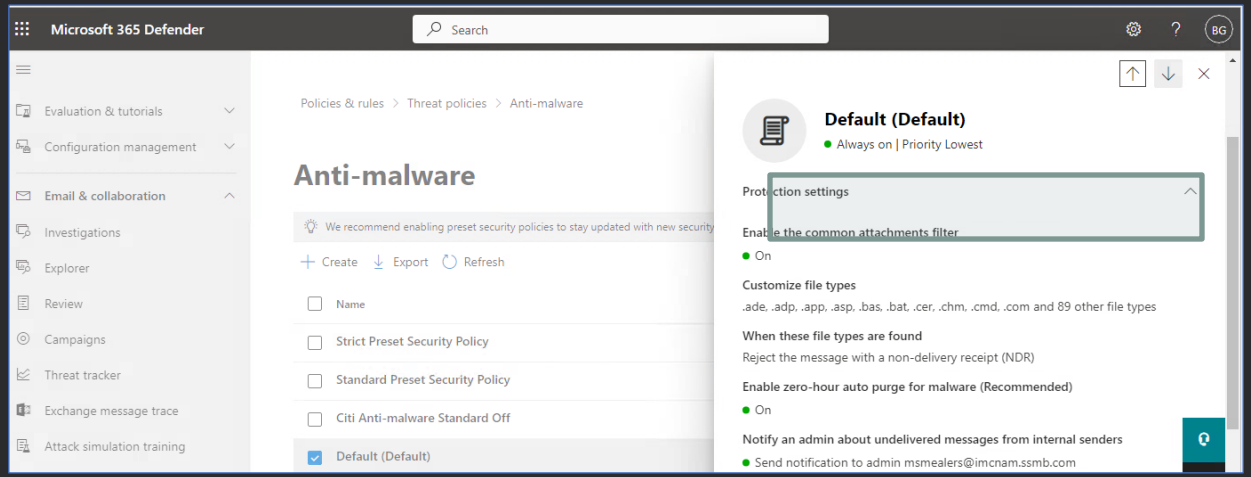
- Off

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.

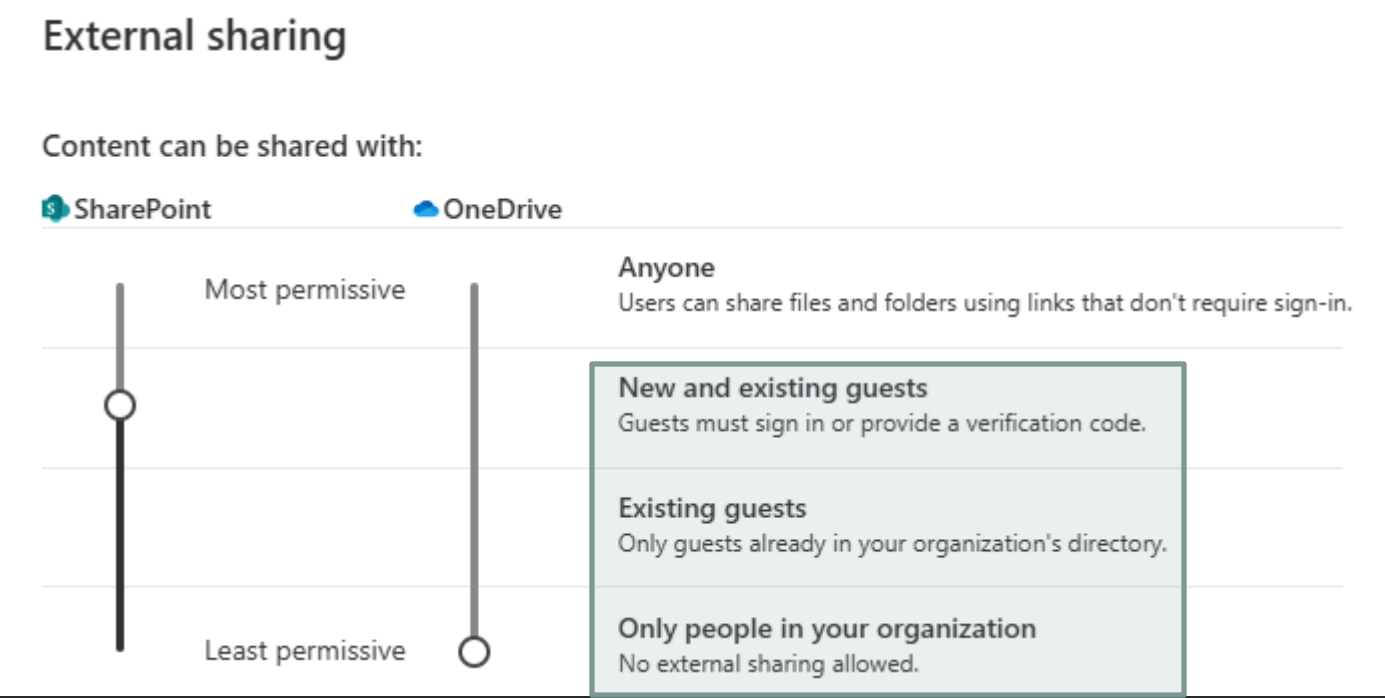
- DKIM lets an organization add a digital signature to outbound email messages in the message header. When DKIM is configured, the organization authorizes it's domain to associate, or sign, its name to an email message using cryptographic authentication. Email systems that get email from this domain 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

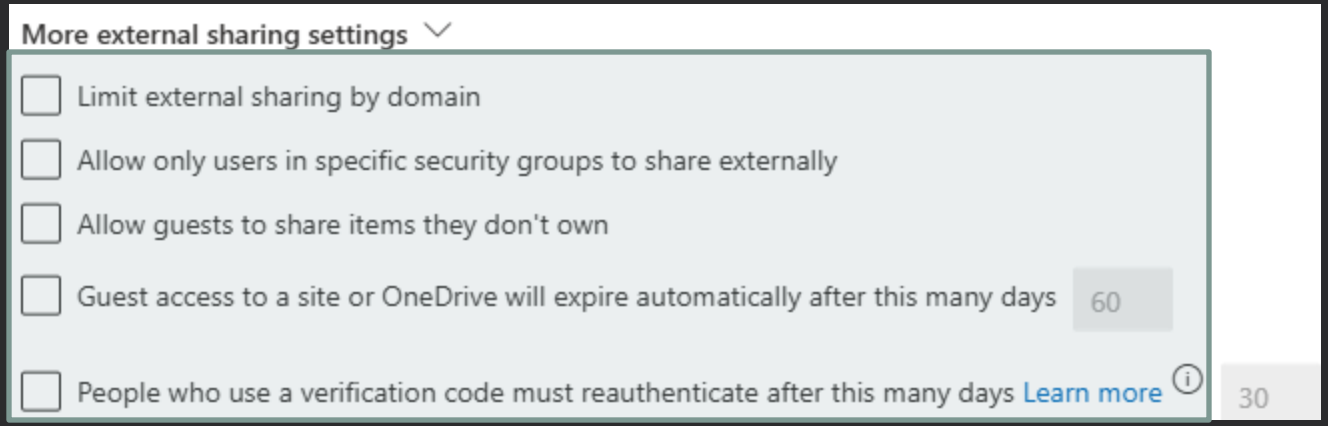
Restrict External SharePoint and OneDrive Content Sharing

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



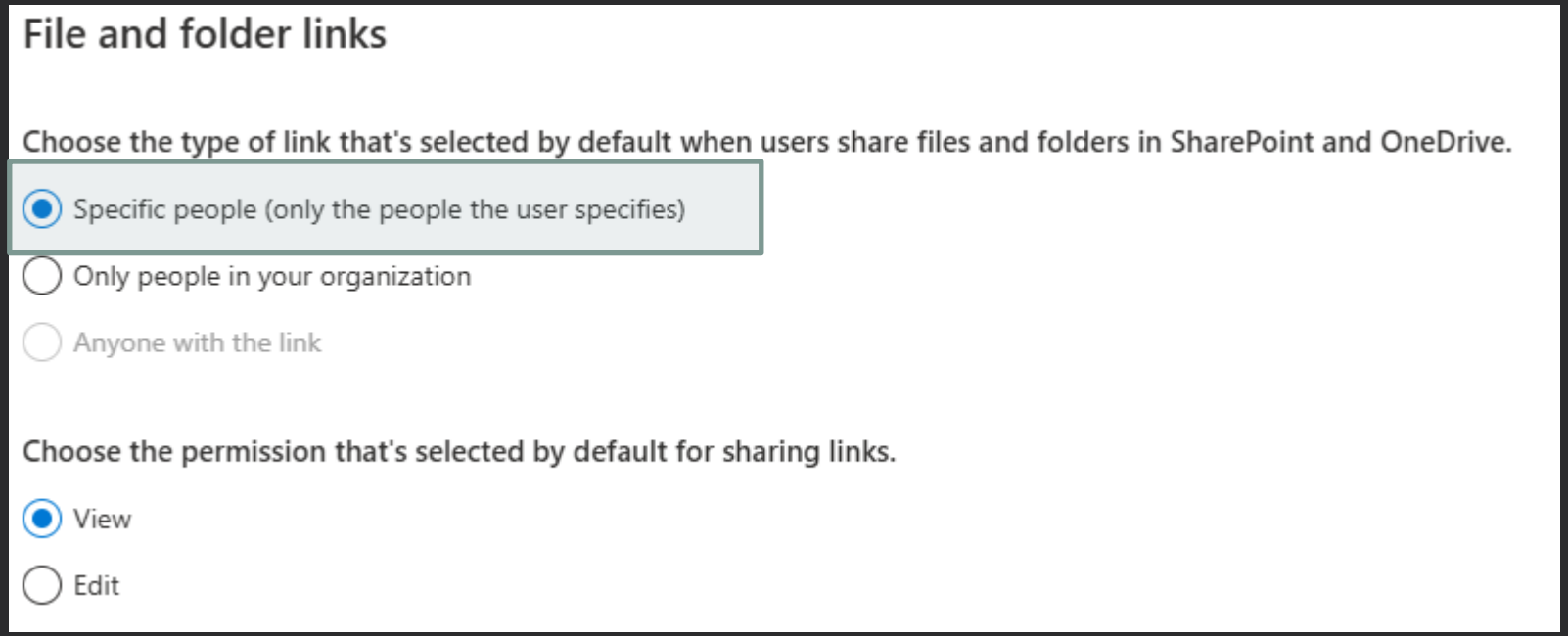
Additional External Sharing Options

- 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



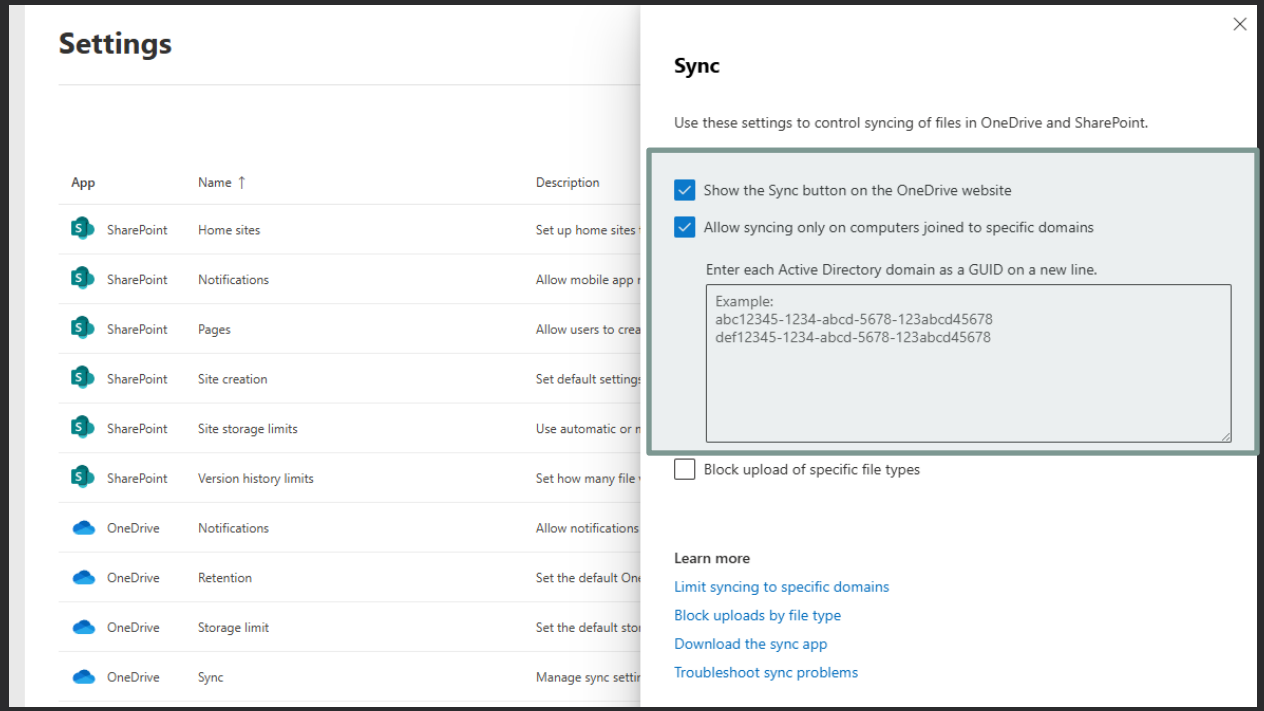
Link Sharing

- 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.



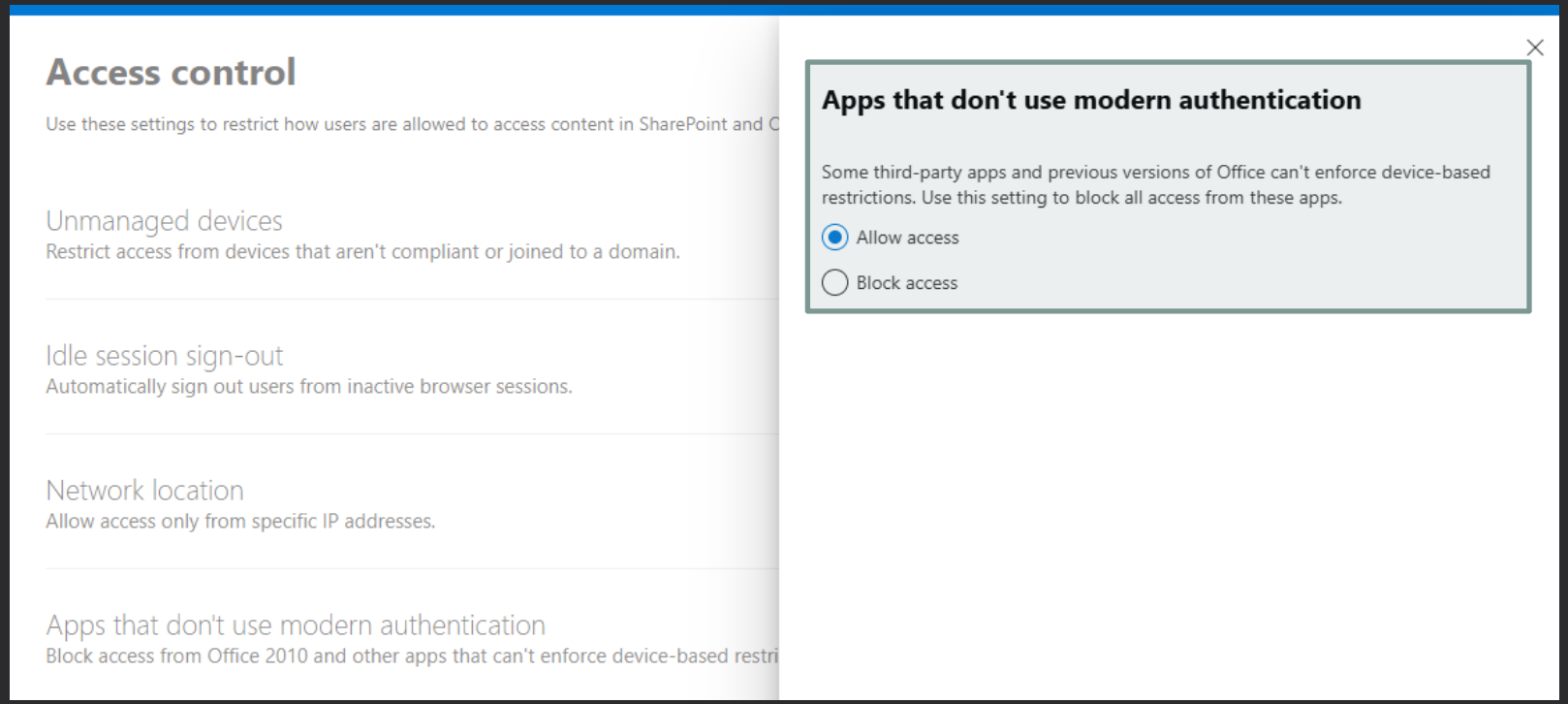
Restrict OneDrive Syncing

- 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.



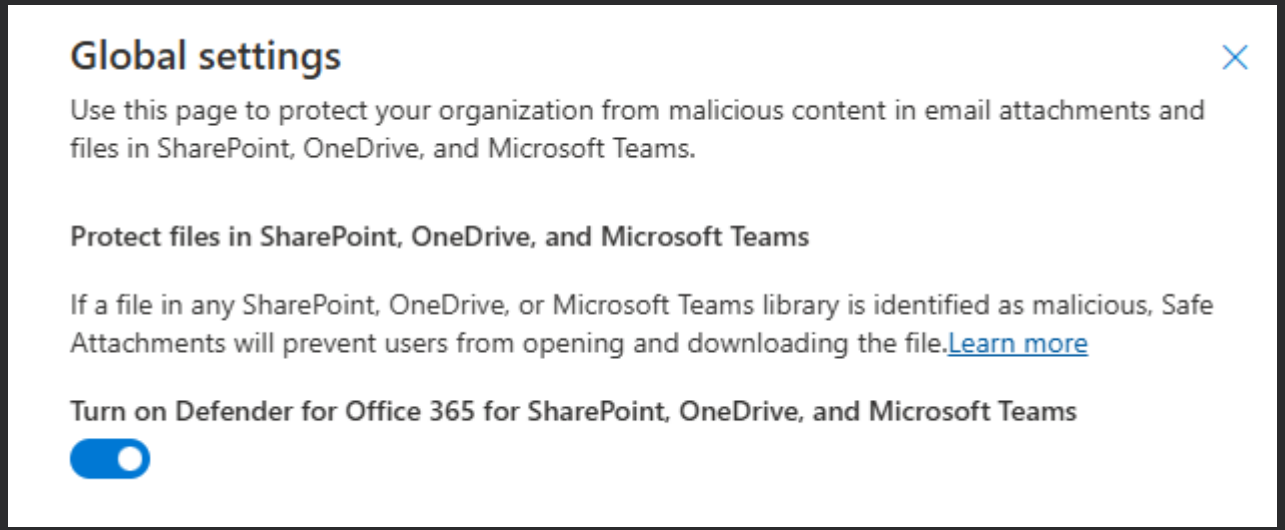
Block access to apps that do not use Modern Authentication

- SharePoint environment should enforce strong authentication requirements.



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.



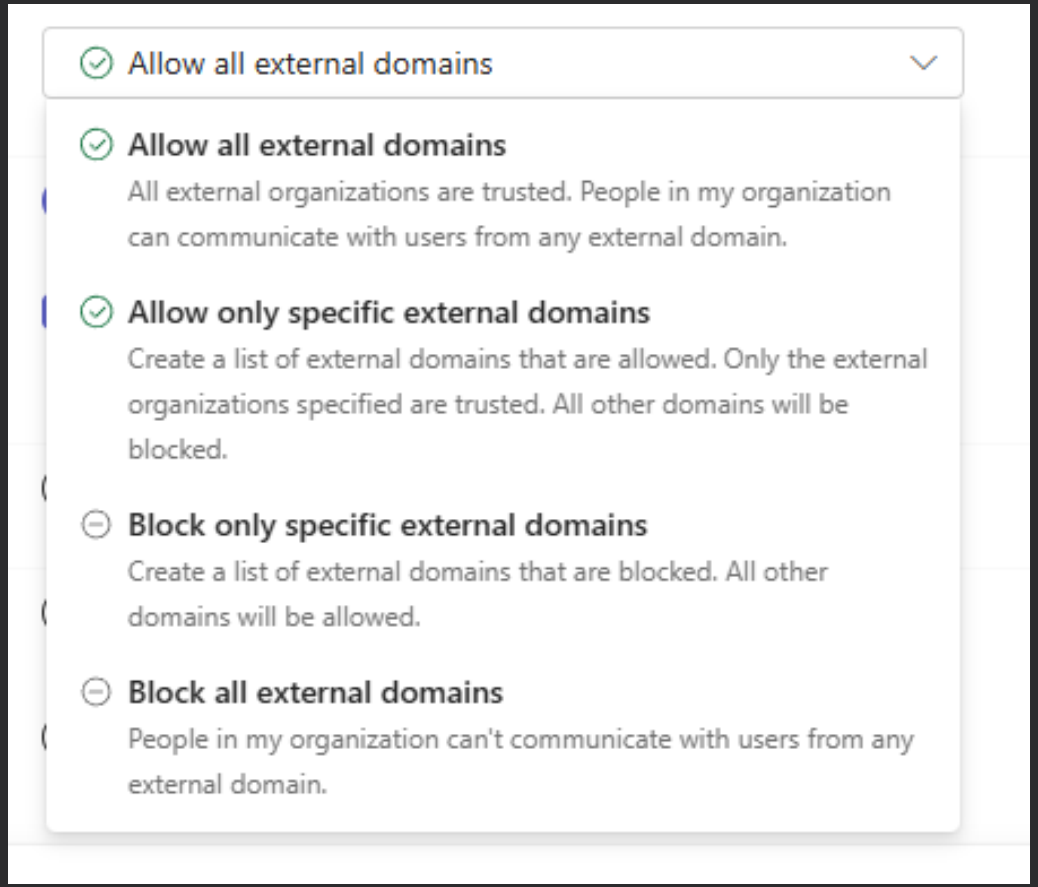
Key Security Controls in Microsoft Teams

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:

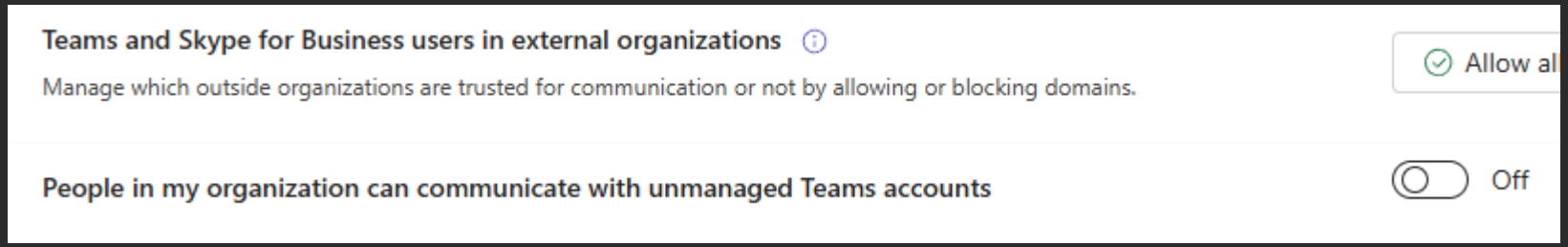
- Allow only specific external domains
- Block all external domains



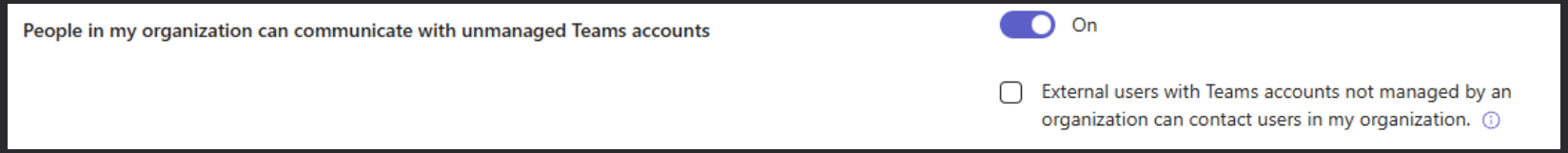
Restrict Communication with Unmanaged Teams Users

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.

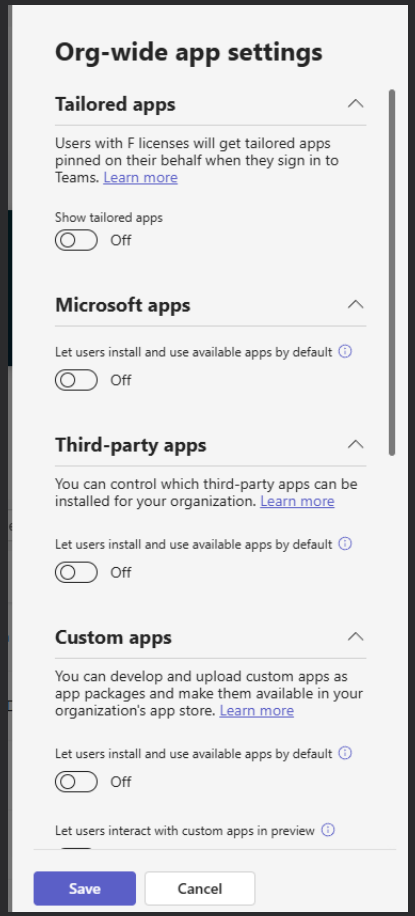


At minimum, don't let external users initiate conversations.



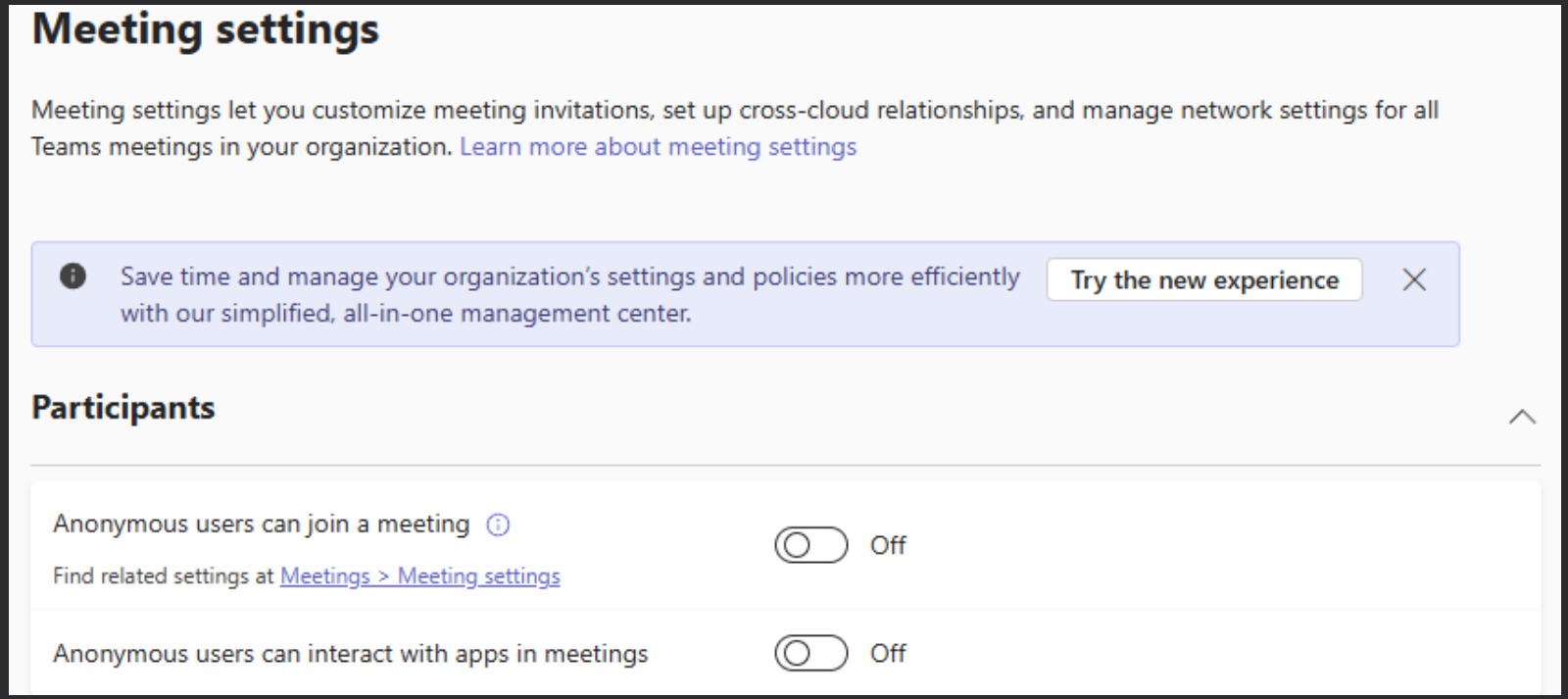
Organization App Settings

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



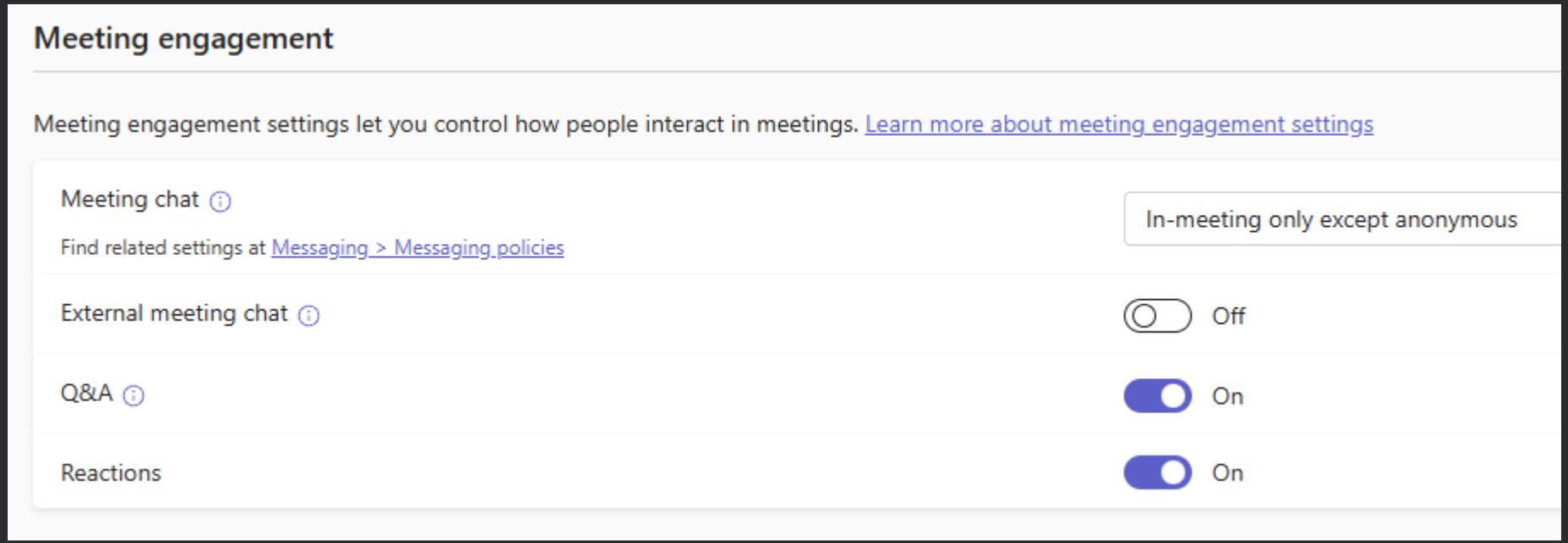
Block Anonymous User Access

- 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.



Restrict External Meeting Chat

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



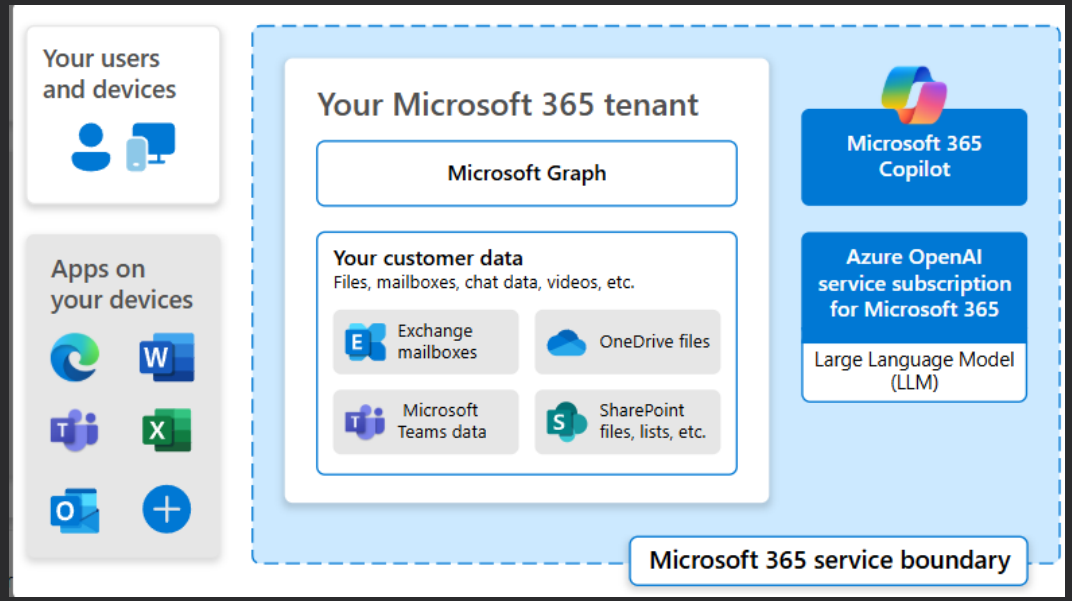
Key Security Controls in Microsoft Copilot

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.

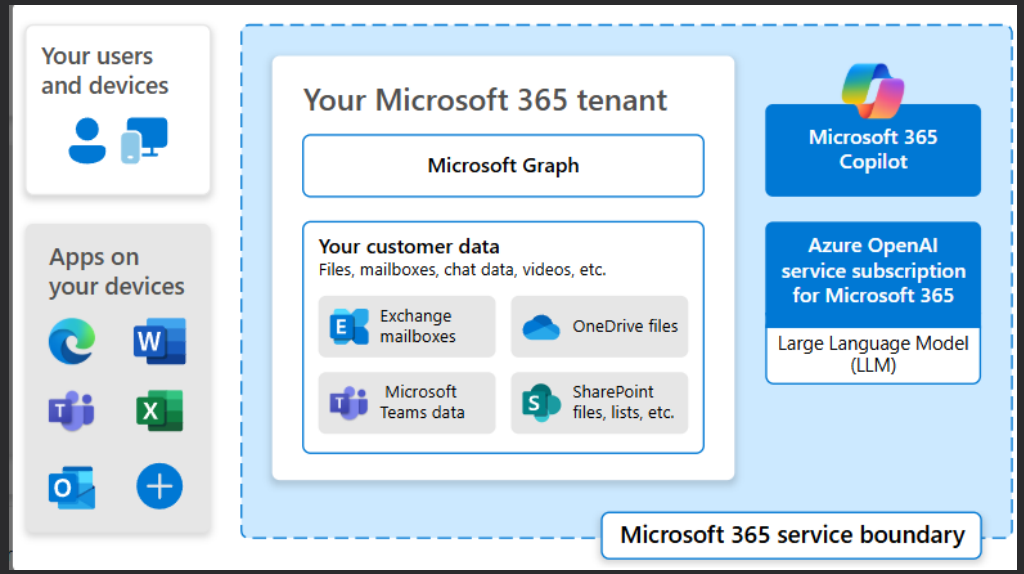


What is Microsoft 365 Copilot?

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.



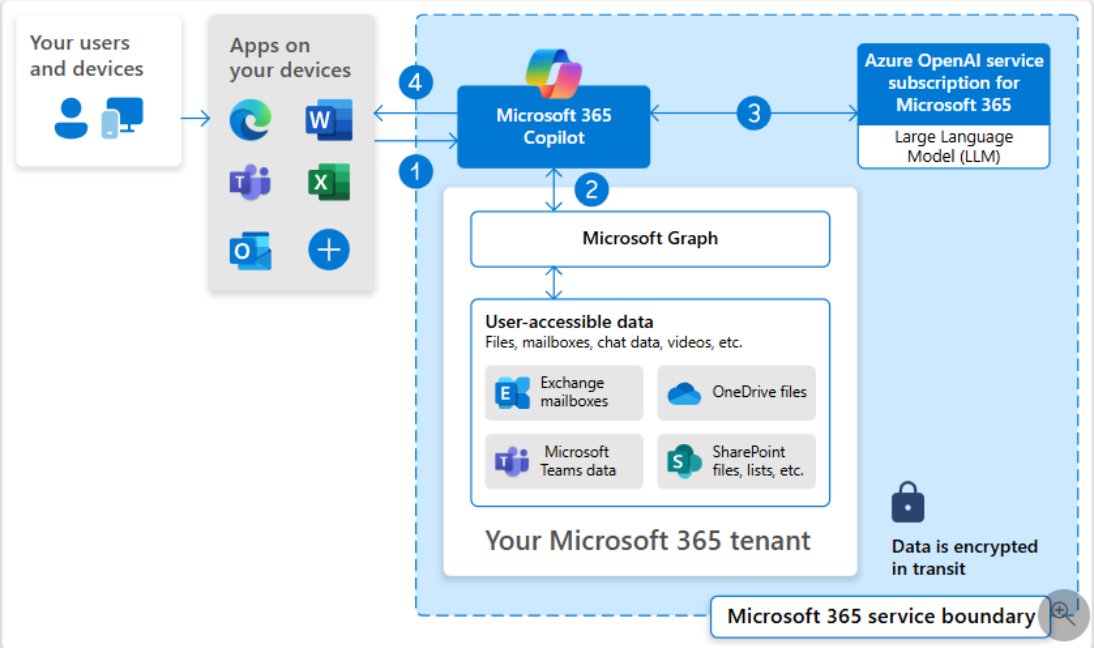
How Does a Copilot Request Work?

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

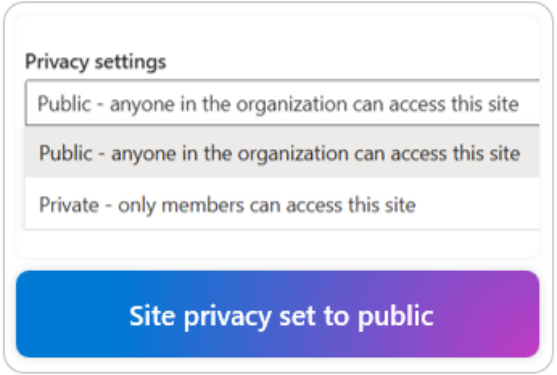
- Copilot only accesses data that an individual user is authorized to access, based on, for example, existing Microsoft 365 role-based access controls. This user data includes emails, chats, and documents that the user has permission to access. Copilot doesn't access data that the user doesn't have permission 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, you Copilot environment will not be secure

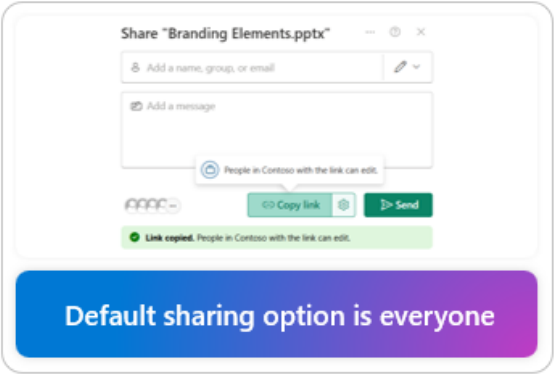
- There are Microsoft 365 services that help control access and security to your organization's data. These services include Restricted SharePoint Search (RSS), SharePoint Advanced Management (SAM), and Microsoft Purview.

Oversharing in Microsoft Copilot

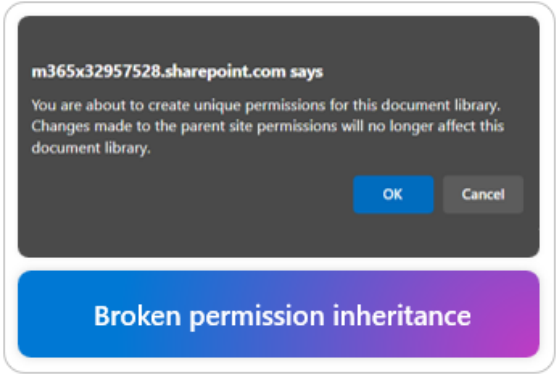
Common causes of Copilot oversharing in SharePoint



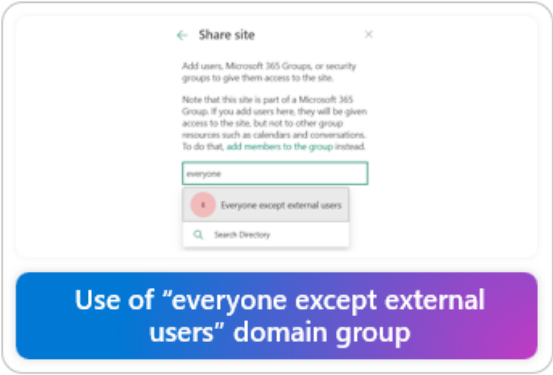
Site privacy set to public



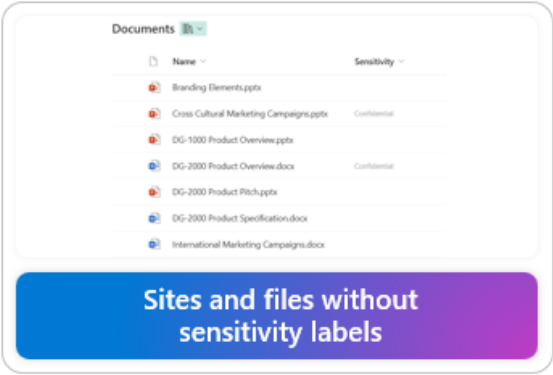
Default sharing option is everyone



Broken permission inheritance



Use of "everyone except external users" domain group



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

Cloud Command Line

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

Home | [cmd.ms]

cmd.ms

[cmd.ms]

- Home
- Microsoft Portals
  - Azure
  - Azure Active Directory
  - Defender
  - Intune
  - Microsoft 365
  - My Pages
- Docs
  - Power User Tips
  - Contributing
  - Related

Home

Home

[cmd.ms] the Microsoft Cloud command line!

Are you tired of clicking around in Microsoft portals to get to a blade?

🚀 Use the power of your browser's address bar to quickly get to your favorite blade in Azure, Microsoft 365, Azure AD, Intune...

Try it out. Open a new tab and type **{command}.cmd.ms** using any of the commands or alias from the list below.

Remember to check out the browser extensions that add support for auto-complete in the address bar.

All Microsoft Portals | Search commands...

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

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

113

Questions / Discussion