Microsoft 365 Assessment

MSFT

Introduction

In today's dynamic digital landscape, safeguarding your organization's data and infrastructure against emerging threats is paramount. As businesses increasingly rely on cloud-based solutions like Microsoft 365, ensuring robust security configurations becomes imperative.

This report has been meticulously designed to comb through the intricacies of your Microsoft 365 environment, meticulously analyzing configurations to identify potential security vulnerabilities. By leveraging industry best practices, it meticulously scans your settings to pinpoint areas warranting attention.

In this report, we present you with a detailed overview of the security settings within your Microsoft 365 ecosystem, highlighting any potential risks and offering clear, actionable remediation steps. Our aim is not only to detect potential vulnerabilities but also to empower you with the insights needed to fortify your defenses effectively.

This report is an assessment of the Microsoft 365 environment at MSFT. The assessment is based on the following areas:

- Security
- Compliance
- Identity
- Device management
- Information protection
- Threat protection
- Application management
- Collaboration
- Productivity

Executive Summary

This Executive Summary encapsulates the comprehensive security assessment conducted within your Microsoft 365 environment across key domains. Each category has been meticulously evaluated to provide insights into your organization's security posture:

- **Security**: Our assessment delved into the security settings of your Microsoft 365 environment, identifying potential vulnerabilities and recommending remediation steps to fortify your defenses against cyber threats.
- **Compliance**: We examined compliance configurations to ensure adherence to regulatory standards and internal policies, highlighting any gaps that may pose risks to data integrity and regulatory compliance.
- **Identity**: Analysis of identity management settings revealed areas for optimization in user authentication, access controls, and privilege management to mitigate the risk of unauthorized access and identity-related attacks.
- **Information Protection**: Our review of information protection settings focused on safeguarding sensitive data through encryption, data loss prevention (DLP) policies, and classification mechanisms, strengthening your data protection measures.
- **Threat Protection**: We scrutinized threat protection configurations to identify potential gaps in malware protection, email filtering, and threat detection capabilities, providing recommendations to bolster your defense against evolving cyber threats.
- **Application Management**: Analysis of application management settings aimed to optimize the security and governance of applications accessing your Microsoft 365 environment, enhancing control and visibility over application usage and permissions.
- **Collaboration**: Evaluation of collaboration settings focused on securing collaboration tools and platforms within Microsoft 365, ensuring safe and efficient communication and collaboration among users while mitigating the risk of data breaches.

This summary provides a glimpse into the comprehensive assessment conducted, highlighting areas of strength and opportunities for improvement across critical domains within your Microsoft 365 environment. Addressing the identified areas will reinforce your organization's resilience against emerging cyber threats and enhance overall security posture.

Review Secure Score

The overall review secure score for the Microsoft 365 environment is **56** (100 is maximum).

Overview

Category	Subcategory	Title
Microsoft 365 Admin Center	Users	1. Ensure Administrative accounts are separate and cloud-only
Microsoft 365 Admin Center	Users	2. Ensure Guest Users are reviewed
Microsoft 365 Admin Center	Teams and groups	3. Ensure that only organizationally managed/approved public groups exist
Microsoft 365 Admin Center	Teams and groups	4. Ensure sign-in to shared mailboxes is blocked
Microsoft 365 Admin Center	Settings	5. Ensure 'External sharing' of calendars is not available
Microsoft 365 Admin Center	Settings	6. Ensure the customer lockbox feature is enabled
Microsoft 365 Admin Center	Settings	7. Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web'
Microsoft 365 Admin Center	Settings	8. Ensure that Sways cannot be shared with people outside of your organization
Microsoft 365 Defender	Email and collaboration	9. Ensure Safe Links for Office Applications is Enabled
Microsoft 365 Defender	Email and collaboration	10. Ensure notifications for internal users sending malware is Enabled
Microsoft 365 Defender	Email and collaboration	11. Ensure Exchange Online Spam Policies are set to notify administrators
Microsoft 365 Defender	Email and collaboration	12. Ensure that an anti-phishing policy has been created
Microsoft 365 Defender	Email and collaboration	13. Ensure that DKIM is enabled for all Exchange Online Domains
Microsoft 365 Defender	Settings	14. Ensure Priority account protection is enabled and configured
Microsoft Purview	Audit	15. Ensure Microsoft 365 audit log search is Enabled
Microsoft Purview	Data Loss Prevention	16. Ensure DLP policies are enabled
Microsoft Entra Admin Center	Identity	17. Ensure third-party integrated applications are not allowed
Microsoft Entra Admin Center	Identity	18. Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'
Microsoft Entra Admin Center	Identity	19. Ensure the option to remain signed in is hidden
Microsoft Entra Admin Center	Identity	20. Ensure the Application Usage report is reviewed at least weekly
Microsoft Entra Admin Center	Identity	21. Ensure user consent to apps accessing company data on their behalf is not allowed

Category	Subcategory	Title
Microsoft Entra Admin Center	Protection	22. Ensure Microsoft Authenticator is configured to protect against MFA fatigue
Microsoft Entra Admin Center	Protection	23. Ensure custom banned passwords lists are used
Microsoft Entra Admin Center	Protection	24. Ensure 'Self service password reset enabled' is set to 'All'
Microsoft Entra Admin Center	Identity Governance	25. Ensure 'Privileged Identity Management' is used to manage roles
Microsoft Entra Admin Center	Identity Governance	26. Ensure 'Access reviews' for high privileged Azure AD roles are configured
Microsoft Exchange Admin Center	Audit	27. Ensure mailbox auditing for users is Enabled
Microsoft Exchange Admin Center	Mail Flow	28. Ensure all forms of mail forwarding are blocked and/or disabled
Microsoft Exchange Admin Center	Mail Flow	29. Ensure email from external senders is identified
Microsoft Exchange Admin Center	Roles	30. Ensure users installing Outlook add-ins is not allowed
Microsoft Exchange Admin Center	Settings	31. Ensure MailTips are enabled for end users
Microsoft SharePoint Admin Center	Policies	32. Ensure modern authentication for SharePoint applications is required
Microsoft SharePoint Admin Center	Policies	33. Ensure external content sharing is restricted
Microsoft SharePoint Admin Center	Policies	34. Ensure OneDrive content sharing is restricted
Microsoft SharePoint Admin Center	Policies	35. Ensure that SharePoint guest users cannot share items they don't own
Microsoft SharePoint Admin Center	Policies	36. Ensure SharePoint external sharing is managed through domain whitelist/blacklists
Microsoft SharePoint Admin Center	Policies	37. Ensure link sharing is restricted in SharePoint and OneDrive
Microsoft SharePoint Admin Center	Policies	38. Ensure external sharing is restricted by security group
Microsoft SharePoint Admin Center	Policies	39. Ensure guest access to a site or OneDrive will expire automatically
Microsoft SharePoint Admin Center	Policies	40. Ensure reauthentication with verification code is restricted
Microsoft SharePoint Admin Center	Settings	41. Ensure Office 365 SharePoint infected files are disallowed for download
Microsoft Teams Admin Center	Teams	42. Ensure external file sharing in Teams is enabled for only approved cloud storage services
Microsoft Teams Admin Center	Teams	43. Ensure users can't send emails to a channel email address
Microsoft Teams Admin Center	Users	44. Ensure 'external access' is restricted in the Teams admin center

Category	Subcategory	Title
Microsoft Teams Admin Center	Meetings	45. Ensure anonymous users can't join a meeting
Microsoft Teams Admin Center	Meetings	46. Ensure only people in my org can bypass the lobby
Microsoft Teams Admin Center	Meetings	47. Ensure meeting chat does not allow anonymous users
Microsoft Teams Admin Center	Meetings	48. Ensure only organizers and co-organizers can present
Microsoft Teams Admin Center	Messaging	49. Ensure users can report security concerns in Teams
Microsoft Fabric Admin Center	Tenant Settings	50. Ensure guest user access is restricted
Microsoft Fabric Admin Center	Tenant Settings	51. Ensure external user invitations are restricted
Microsoft Fabric Admin Center	Tenant Settings	52. Ensure 'Interact with and share R and Python' visuals is 'Disabled'
Microsoft Fabric Admin Center	Tenant Settings	53. Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'
Microsoft Fabric Admin Center	Tenant Settings	54. Ensure shareable links are restricted
Microsoft Fabric Admin Center	Tenant Settings	55. Ensure enabling of external data sharing is restricted
Microsoft Fabric Admin Center	Tenant Settings	56. Ensure 'Block ResourceKey Authentication' is 'Enabled'

1. Ensure Administrative accounts are separate and cloud-only

2024-03-15

1.1. Information

ID	Category	Subcategory	Review
289efa41-e17f-43e7-a6b8-9ff8868d3511	Microsoft 365 Admin Center	Users	True

1.2. Description

Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings. Regular user accounts should never be utilized for administrative tasks and care should be taken, in the case of a hybrid environment, to keep administrative accounts separated from on-prem accounts. Administrative accounts should not have applications assigned so that they have no access to potentially vulnerable services (EX. email, Teams, SharePoint, etc.) and only access to perform tasks as needed for administrative purposes. Ensure administrative accounts are licensed without attached applications and cloud-only.

1.3. Technical explanation

Ensuring administrative accounts are cloud-only, without applications assigned to them will reduce the attack surface of high privileged identities in your environment. In order to participate in Microsoft 365 security services such as Identity Protection, PIM and Conditional Access an administrative account will need a license attached to it. Ensure that the license used does not include any applications with potentially vulnerable services by using either Microsoft Entra ID P1 or Microsoft Entra ID P2 for the cloud-only account with administrator roles. In a hybrid environment, having separate accounts will help ensure that in the event of a breach in the cloud, that the breach does not affect the on-prem environment and vice versa.

1.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand **Users** select **Active users**
3. Click **Add a user**.
4. Fill out the appropriate fields for Name, user, etc.
5. When prompted to assign licenses select as needed **Microsoft Entra ID P1** or **Microsoft Entra ID P2**, then click Next.
6. Under the Option settings screen you may choose from several types of Administrative access roles. Choose Admin center access followed by the appropriate role then click **Next**.
7. Select **Finish** adding.

1.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide
- https://learn.microsoft.com/en-us/microsoft-365/enterprise/protect-your-global-administrator-accounts?view=o365-worldwide
- https://learn.microsoft.com/en-us/azure/active-directory/roles/best-practices#9-use-cloud-native-accounts-for-azure-ad-roles
- https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whatis

1.6. Data

Id	UserPrincipalName	DisplayName	CloudOnly	Roles	Licenses	AccountEnabled
04de8899-452a-40f6-bfdd-d6f75e37bc76	GradyA@04nxg.onmicrosoft.com	Grady Archie	True	Application Administrator	Microsoft 365 E5 Developer (without Windows and Audio Conferencing)	True
8aa0819b-4298-4b7c-a4a5-70522afe48cc	systemadmins@04nxg.onmicrosoft.com	Alex Ørving Toftegaard Hansen	True	Global Administrator	Microsoft 365 E5 Developer (without Windows and Audio Conferencing)	True

2. Ensure Guest Users are reviewed

2024-03-15

2.1. Information

ID	Category	Subcategory	Review
7fe4d30e-42bd-44d4-8066-0b732dcbda4c	Microsoft 365 Admin Center	Users	True

2.2. Description

Guest users can be set up for those users not in the organization to still be granted access to resources. It is important to maintain visibility for what guest users are established in the tenant.
Ensure Guest Users are reviewed no less frequently than biweekly.

2.3. Technical explanation

Periodic review of guest users ensures proper access to resources.

2.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com/.
2. Click to expand **Users** and select **Guest Users**.
3. Review the list of users.

2.5. More information

N/A

2.6. Data

Id	UserPrincipalName	GivenName	Surname	DisplayName	Roles	CreatedDateTime	LastSignIn	AccountEnabled
c9d55b3a-07b5-4ff4-a398-a6248caf1660	ath_toft e-it.dk#EXT#@04nxg.onmicrosoft.com			Alex Hansen	Global Administrator	23-01-2024 10:38:46	23-01-2024 11:11:03	True

3. Ensure that only organizationally managed/approved public groups exist

2024-03-15

3.1. Information

ID	Category	Subcategory	Review
90295b64-2528-4c22-aa96-a606633bc705	Microsoft 365 Admin Center	Teams and groups	True

3.2. Description

Microsoft 365 Groups is the foundational membership service that drives all teamwork across Microsoft 365. With Microsoft 365 Groups, you can give a group of people access to a collection of shared resources. While there are several different group types this recommendation concerns **Microsoft 365 Groups**.
In the Administration panel, when a group is created, the default privacy value is "Public".

3.3. Technical explanation

Ensure that only organizationally managed and approved public groups exist. When a group has a "public" privacy, users may access data related to this group (e.g. SharePoint), through three methods:

- By using the Azure portal, and adding themselves into the public group
- By requesting access to the group from the Group application of the Access Panel
- By accessing the SharePoint URL

Administrators are notified when a user uses the Azure Portal. Requesting access to the group forces users to send a message to the group owner, but they still have immediate access to the group. The SharePoint URL is usually guessable and can be found from the Group application of the Access Panel. If group privacy is not controlled, any user may access sensitive information, according to the group they try to access.

3.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand Teams & groups select Active teams & groups..
3. On the **Active teams and groups page**, select the group's name that is public.
4. On the popup groups name page, Select **Settings**.
5. Under Privacy, select **Private**.

3.5. More information

- https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-self-service-management
- https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

3.6. Data

Id	DisplayName	Visibility	SecurityEnabled	Mail	CreatedDateTime
18cd696e-8029-47e9-85d0-3ebe261af759	MSFT	Public	False	MSFT@04nxg.onmicrosoft.com	17-01-2024 03:55:27
2f6ac046-6bf0-4611-8e50-ee1faf66abc6	Sales and Marketing	Public	False	SalesandMarketing@04nxg.onmicrosoft.com	17-01-2024 17:57:36
32fa2f54-b64b-4b07-a3d9-9b3755a550ea	Digital Initiative Public Relations	Public	False	DigitalInitiativePublicRelations666@04nxg.onmicrosoft.com	17-01-2024 17:54:24
41bd9612-517d-47c2-bba2-e165df2bdc85	Sample Team Site	Public	False	SampleTeamSite@04nxg.onmicrosoft.com	17-01-2024 20:58:19
6db5dea1-5fa1-4868-94f6-873831d45740	Mark 8 Project Team	Public	False	Mark8ProjectTeam784@04nxg.onmicrosoft.com	17-01-2024 17:55:32
7272165a-22b3-4e8c-90f5-894d1c147186	U.S. Sales	Public	False	U.S.Sales@04nxg.onmicrosoft.com	17-01-2024 17:58:07
9139e39c-2847-429d-9389-1f37fdc967c9	Retail	Public	False	Retail@04nxg.onmicrosoft.com	17-01-2024 17:57:11

4. Ensure sign-in to shared mailboxes is blocked

2024-03-15

4.1. Information

ID	Category	Subcategory	Review
dc6727fe-333d-46ad-9ad6-f9b0ae23d03b	Microsoft 365 Admin Center	Teams and groups	True

4.2. Description

Shared mailboxes are used when multiple people need access to the same mailbox, such as a company information or support email address, reception desk, or other function that might be shared by multiple people.
Users with permissions to the group mailbox can send as or send on behalf of the mailbox email address if the administrator has given that user permissions to do that. This is particularly useful for help and support mailboxes because users can send emails from "Contoso Support" or "Building A Reception Desk."
Shared mailboxes are created with a corresponding user account using a system generated password that is unknown at the time of creation.
The recommended state is Sign in blocked for Shared mailboxes.

4.3. Technical explanation

The intent of the shared mailbox is the only allow delegated access from other mailboxes. An admin could reset the password or an attacker could potentially gain access to the shared mailbox allowing the direct sign-in to the shared mailbox and subsequently the sending of email from a sender that does not have a unique identity. To prevent this, block sign-in for the account that is associated with the shared mailbox.

4.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com/
2. Click to expand **Teams & groups** and select Shared mailboxes.
3. Take note of all shared mailboxes.
4. Click to expand **Users** and select Active users.
5. Select a shared mailbox account to open it's properties pane and then select **Block sign-in**.
6. Check the box for **Block this user from signing in**.
7. Repeat for any additional shared mailboxes.

4.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/admin/email/about-shared-mailboxes?view=o365-worldwide
- https://learn.microsoft.com/en-us/microsoft-365/admin/email/create-a-shared-mailbox?view=o365-worldwide#block-sign-in-for-the-shared-mailbox-account
- https://learn.microsoft.com/en-us/microsoft-365/enterprise/block-user-accounts-with-microsoft-365-powershell?view=o365-worldwide#block-individual-user-accounts
- https://learn.microsoft.com/en-us/powershell/module/azuread/set-azureaduser?view=azureadps-2.0

4.6. Data

Id	UserPrincipalName	GivenName	Surname	DisplayName	CreatedDateTime	LastSignIn	AccountEnabled	PrimarySmtpAddress	CloudOnly
d5bc5133-ab7e-451a-8e81-9febc0f1de55	testt@04nxg.onmicrosoft.com			test	12-02-2024 14:27:58		True	testt@04nxg.onmicrosoft.com	True

5. Ensure 'External sharing' of calendars is not available

2024-03-15

5.1. Information

ID	Category	Subcategory	Review
489b0b3d-cf78-46a5-8366-84908dc05d5a	Microsoft 365 Admin Center	Settings	True

5.2. Description

lExternal calendar sharing allows an administrator to enable the ability for users to share calendars with anyone outside of the organization. Outside users will be sent a URL that can be used to view the calendar.

5.3. Technical explanation

Attackers often spend time learning about organizations before launching an attack. Publicly available calendars can help attackers understand organizational relationships and determine when specific users may be more vulnerable to an attack, such as when they are traveling.

5.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand **Settings** select **Org settings**.
3. In the Services section click **Calendar**.
4. Uncheck **Let your users share their calendars with people outside of your organization who have Office 365 or Exchange**.
5. Click **Save**.

5.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/admin/manage/share-calendars-with-external-users?view=o365-worldwide

5.6. Data

Name	Domains	Enabled	Default
Default Sharing Policy	Anonymous:CalendarSharingFreeBusyReviewerl*:CalendarSharingFreeBusySimple	True	True

6. Ensure the customer lockbox feature is enabled

2024-03-15

6.1. Information

ID	Category	Subcategory	Review
f4cf24ca-cd8f-4ded-bfe0-6f45f3bcfed0	Microsoft 365 Admin Center	Settings	True

6.2. Description

Customer Lockbox is a security feature that provides an additional layer of control and transparency to customer data in Microsoft 365. It offers an approval process for Microsoft support personnel to access organization data and creates an audited trail to meet compliance requirements.

6.3. Technical explanation

Enabling this feature protects organizational data against data spillage and exfiltration.

6.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand **Settings** then select **Org settings**.
3. Select **Security & privacy** tab.
4. Click **Customer lockbox**.
5. Check the box **Require approval for all data access requests**.
6. Click **Save**.

6.5. More information

- https://learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

6.6. Data

Enabled
False

7. Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web'

2024-03-15

7.1. Information

ID	Category	Subcategory	Review
54b612c6-5306-45d4-b948-f3e75e09ab3b	Microsoft 365 Admin Center	Settings	True

7.2. Description

Third-party storage can be enabled for users in Microsoft 365, allowing them to store and share documents using services such as Dropbox, alongside OneDrive and team sites.
Ensure Microsoft 365 on the web third-party storage services are restricted.

7.3. Technical explanation

By using external storage services an organization may increase the risk of data breaches and unauthorized access to confidential information. Additionally, third-party services may not adhere to the same security standards as the organization, making it difficult to maintain data privacy and security.

7.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com
2. Go to **Settings** > **Org Settings** > **Services** > **Microsoft 365 on the web**
3. Uncheck **Let users open files stored in third-party storage services in Microsoft 365 on the web**

7.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/admin/setup/set-up-file-storage-and-sharing?view=o365-worldwide#enable-or-disable-third-party-storage-services

7.6. Data

Enabled
True

8. Ensure that Sways cannot be shared with people outside of your organization

2024-03-15

8.1. Information

ID	Category	Subcategory	Review
d10b85ac-05df-4c78-91a5-5bc03f799ea2	Microsoft 365 Admin Center	Settings	True

8.2. Description

Sway is a new app from Microsoft Office that allows users to create and share interactive reports, personal stories, presentations, and more.
This setting controls user Sway sharing capability, both within and outside of the organization. By default, Sway is enabled for everyone in the organization.

8.3. Technical explanation

Disable external sharing of Sway documents that can contain sensitive information to prevent accidental or arbitrary data leaks.

8.4. Advised solution

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand **Settings** then select **Org settings**.
3. Under Services select **Sway**
   - Uncheck **Let people in your organization share their sways with people outside your organization**.
4. Click Save.

8.5. More information

- https://support.microsoft.com/en-us/office/administrator-settings-for-sway-d298e79b-b6ab-44c6-9239-aa312f5784d4

8.6. Data

Enabled
True

9. Ensure Safe Links for Office Applications is Enabled

2024-03-15

9.1. Information

ID	Category	Subcategory	Review
b29a3b32-4042-4ce6-86f6-eb85b183b4b5	Microsoft 365 Defender	Email and collaboration	True

9.2. Description

Enabling Safe Links policy for Office applications allows URL's that exist inside of Office documents and email applications opened by Office, Office Online and Office mobile to be processed against Defender for Office time-of-click verification and rewritten if required.

9.3. Technical explanation

Safe Links for Office applications extends phishing protection to documents and emails that contain hyperlinks, even after they have been delivered to a user.

9.4. Advised solution

1. Navigate to Microsoft 365 Defender https://security.microsoft.com
2. Under Email & collaboration select **Policies & rules**
3. Select **Threat policies** then **Safe Links**
4. Click on **+Create**
5. Name the policy then click **Next**
6. In Domains select all valid domains for the organization and **Next**
7. Ensure the following URL & click protection settings are defined:
   - **Email**
     - Checked **On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default**
     - Checked **Apply Safe Links to email messages sent within the organization**
     - Checked **Apply real-time URL scanning for suspicious links and links that point to files**
     - Checked **Wait for URL scanning to complete before delivering the message**
     - Unchecked **Do not rewrite URLs, do checks via Safe Links API only.**
   - **Teams**
     - Checked **On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten**
   - Office 365 Apps
     - Checked **On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten**
   - **Click protection settings**
     - Checked **Track user clicks**
     - Unchecked **Let users click through the original URL**
8. Click **Next** twice and finally **Submit**

9.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure?view=o365-worldwide
- https://learn.microsoft.com/en-us/powershell/module/exchange/set-safelinkspolicy?view=exchange-ps
- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies?view=o365-worldwide

9.6. Data

Guid	Id	Name	Valid	EnableSafeLinksForEmail	EnableSafeLinksForTeams	EnableSafeLinksForOffice	TrackClicks	AllowClickThrough	ScanUrls	EnableForInternalSenders	DeliverMessageAfterScan	DisableURLRewrite
92f931ce-344c-4906-867d-f328aa80242d	Built-In Protection Policy	Built-In Protection Policy	False	True	True	True	True	True	True	False	True	True
df0d5aec-4acb-4b17-aba0-b073a135ac3d	Strict Preset Security Policy1706550528770	Strict Preset Security Policy1706550528770	True	True	True	True	True	False	True	True	True	False

10. Ensure notifications for internal users sending malware is Enabled

2024-03-15

10.1. Information

ID	Category	Subcategory	Review
01f7327e-f8cf-4542-b12a-41b40d03415d	Microsoft 365 Defender	Email and collaboration	True

10.2. Description

Exchange Online Protection (EOP) is the cloud-based filtering service that protects organizations against spam, malware, and other email threats. EOP is included in all Microsoft 365 organizations with Exchange Online mailboxes. EOP uses flexible anti-malware policies for malware protection settings. These policies can be set to notify Admins of malicious activity.

10.3. Technical explanation

This setting alerts administrators that an internal user sent a message that contained malware. This may indicate an account or machine compromise that would need to be investigated.

10.4. Advised solution

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand **E-mail & Collaboration** select Policies & rules.
3. On the Policies & rules page select **Threat policies**.
4. Under Policies select Anti-malware.
5. Click on the **Default (Default)** policy.
6. Click on Edit protection settings and change the settings for **Notify an admin about undelivered messages from internal senders** to **On** and enter the email address of the administrator who should be notified under Administrator email address.
7. Click **Save**.

10.5. More information

N/A

10.6. Data

Guid	Id	Name	Valid	EnableInternalSenderAdminNotifications	InternalSenderAdminAddress
70e3c52e-ecd0-4561-9336-cc1554b12d29	Default	Default	False	False	
5327f9c8-fabd-4182-b413-4f5c5e80917a	Strict Preset Security Policy1706550526556	Strict Preset Security Policy1706550526556	False	False	

11. Ensure Exchange Online Spam Policies are set to notify administrators

2024-03-15

11.1. Information

ID	Category	Subcategory	Review
a019303a-3b0a-4f42-999d-0d76b528ae28	Microsoft 365 Defender	Email and collaboration	True

11.2. Description

In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, email messages are automatically protected against spam (junk email) by EOP. Configure Exchange Online Spam Policies to copy emails and notify someone when a sender in the organization has been blocked for sending spam emails.

11.3. Technical explanation

A blocked account is a good indication that the account in question has been breached and an attacker is using it to send spam emails to other people.

11.4. Advised solution

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand **Email & collaboration** select **Policies & rules** > **Threat policies**.
3. Under Policies select **Anti-spam**.
4. Click on the **Anti-spam outbound policy (default)**.
5. Select **Edit protection settings** then under **Notifications**
6. Check **Send a copy of outbound messages that exceed these limits to these users and groups then enter the desired email addresses**.
7. Check **Notify these users and groups if a sender is blocked due to sending outbound spam then enter the desired email addresses**.
8. Click **Save**.

11.5. More information

N/A

11.6. Data

Guid	Id	Name	Valid	BccSuspiciousOutboundMail	NotifyOutboundSpam	NotifyOutboundSpamRecipients	Enabled
610ef558-a3d8-4d9b-a3f3-5c45c6132a37	Default	Default	False	False	False		False

12. Ensure that an anti-phishing policy has been created

2024-03-15

12.1. Information

ID	Category	Subcategory	Review
13954bef-f9cd-49f8-b8c8-626e87de6ba2	Microsoft 365 Defender	Email and collaboration	True

12.2. Description

By default, Office 365 includes built-in features that help protect users from phishing attacks. Set up anti-phishing polices to increase this protection, for example by refining settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization and is a single view to fine-tune anti-phishing protection. Custom policies can be created and configured for specific users, groups or domains within the organization and will take precedence over the default policy for the scoped users.

12.3. Technical explanation

Protects users from phishing attacks (like impersonation and spoofing), and uses safety tips to warn users about potentially harmful messages.

12.4. Advised solution

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand **Email & collaboration** select **Policies & rules**
3. Select **Threat policies**.
4. Under Policies select **Anti-phishing**.
5. Select the **Office365 AntiPhish Default (Default)** policy and click **Edit protection settings**.
6. Set the Phishing email threshold to at least **2 - Aggressive**
    1. Under **Impersonation**
        - Check **Enable mailbox intelligence (Recommended)**
        - Check **Enable Intelligence for impersonation protection (Recommended)**
    2. Under **Spoof**
        - Check **Enable spoof intelligence (Recommended)**
7. Click **Save**.

12.5. More information

N/A

12.6. Data

Guid	Id	Name	Valid	Enabled	PhishThresholdLevel	EnableMailboxIntelligenceProtection	EnableMailboxIntelligence	EnableSpoofIntelligence
1422945e-61fa-4295-8b4e-4433717d9911	Office365 AntiPhish Default	Office365 AntiPhish Default	False	True	1	False	True	True
edcbf99c-a71f-4f1e-8b72-6759ef9122d9	Strict Preset Security Policy1706550523647	Strict Preset Security Policy1706550523647	True	True	4	True	True	True

13. Ensure that DKIM is enabled for all Exchange Online Domains

2024-03-15

13.1. Information

ID	Category	Subcategory	Review
92adb77c-a12b-4dee-8ce8-2b5f748f22ec	Microsoft 365 Defender	Email and collaboration	True

13.2. Description

DKIM is one of the trio of Authentication methods (SPF, DKIM and DMARC) that help prevent attackers from sending messages that look like they come from your domain.
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.
Use of DKIM in addition to SPF and DMARC to help prevent malicious actors using spoofing techniques from sending messages that look like they are coming from your domain.

13.3. Technical explanation

By enabling DKIM with Office 365, messages that are sent from Exchange Online will be cryptographically signed. This will allow the receiving email system to validate that the messages were generated by a server that the organization authorized and not being spoofed.

13.4. Advised solution

To setup DKIM records, first add the following records to your DNS system, for each domain in Exchange Online that you plan to use to send email with:
For each accepted domain in Exchange Online, two DNS (CNAME) entries are required.

```
Host name: selector1._domainkey
Points to address or value: selector1-<domainGUID>._domainkey.<initialDomain>
TTL: 3600

Host name: selector2._domainkey
```

```
Points to address or value: selector2-<domainGUID>._domainkey.<initialDomain>
TTL: 3600
```

For Office 365, the selectors will always be **selector1** or **selector2.domainGUID** is the same as the domainGUID in the customized MX record for your custom domain that appears before mail.protection.outlook.com.

For example, in the following MX record for the domain **contoso.com**, the domainGUID is **contoso-com**.

1. The initial domain is the domain that you used when you signed up for Office 365. Initial domains always end in on microsoft.com.
2. After the DNS records are created, enable DKIM signing in Defender.
3. Navigate to Microsoft 365 Defender https://security.microsoft.com/
4. Expand **Email & collaboration** > **Policies & rules** > **Threat policies**.
5. Under Rules section click **Email authentication settings**.
6. Select **DKIM**
7. Click on each domain and click **Enable** next to **Sign messages for this domain with DKIM signature**.

13.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dkim-configure?view=o365-worldwide

13.6. Data

Domain	Valid	IsDefault	IsVerified	AuthenticationType	DkimEnabled	DkimRecord1	DkimRecord2
04nxg.onmicrosoft.com	False	True	True	Managed	False		

14. Ensure Priority account protection is enabled and configured

2024-03-15

14.1. Information

ID	Category	Subcategory	Review
749ee441-71ea-4261-86da-1f1081c65bb3	Microsoft 365 Defender	Settings	True

14.2. Description

Identify priority accounts to utilize Microsoft 365's advanced custom security features. This is an essential tool to bolster protection for users who are frequently targeted due to their critical positions, such as executives, leaders, managers, or others who have access to sensitive, confidential, financial, or high-priority information.
Once these accounts are identified, several services and features can be enabled, including threat policies, enhanced sign-in protection through conditional access policies, and alert policies, enabling faster response times for incident response teams.

14.3. Technical explanation

Enabling priority account protection for users in Microsoft 365 is necessary to enhance security for accounts with access to sensitive data and high privileges, such as CEOs, CISOs, CFOs, and IT admins. These priority accounts are often targeted by spear phishing or whaling attacks and require stronger protection to prevent account compromise.
To address this, Microsoft 365 and Microsoft Defender for Office 365 offer several key features that provide extra security, including the identification of incidents and alerts involving priority accounts and the use of built-in custom protections designed specifically for them.

14.4. Advised solution

1. Navigate to Microsoft 365 Defender https://security.microsoft.com/
2. Select **Settings** > **E-mail & Collaboration** > **Priority account protection**
3. Ensure **Priority account protection** is set to **On**
4. Select **User tags**
5. Select the **PRIORITY ACCOUNT** tag and click **Edit**
6. Select **Add members** to add users, or groups. Groups are recommended.
7. Repeat the previous 2 steps for any additional tags needed, such as Finance or HR.
8. **Next** and **Submit**.
9. Expand **E-mail & Collaboration** on the left column.
10. Select **New Alert Policy**
11. Enter a valid policy Name & Description. Set **Severity** to **High** and **Category** to **Threat management**.
12. Set **Activity is** to **Detected malware in an e-mail message**
13. Mail direction is **Inbound**
14. Select **Add Condition** and **User: recipient tags are**
15. In the **Selection option** field add chosen priority tags such as Priority account.
16. Select **Every time an activity matches the rule**.
17. **Next** and Verify valid recipient(s) are selected.
18. **Next** and select **Yes**, turn it on right away. Click **Submit** to save the alert.
19. Repeat steps 10 - 18 for the Activity field **Activity is: Phishing email detected at time of delivery**

14.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/admin/setup/priority-accounts
- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/security-recommendations-for-priority-accounts

14.6. Data

PriorityAccountProtectionEnabled	PriorityAccountUsersExist	PriorityAccountProtectionPolicyExist
True	False	True

15. Ensure Microsoft 365 audit log search is Enabled

2024-03-15

15.1. Information

ID	Category	Subcategory	Review
55299518-ad01-4532-aa35-422fd962c881	Microsoft Purview	Audit	True

15.2. Description

When audit log search is enabled in the Microsoft Purview compliance portal, user and admin activity within the organization is recorded in the audit log and retained for 90 days. However, some organizations may prefer to use a third-party security information and event management (SIEM) application to access their auditing data. In this scenario, a global admin can choose to turn off audit log search in Microsoft 365.

15.3. Technical explanation

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.

15.4. Advised solution

1. Navigate to Microsoft Purview https://compliance.microsoft.com.
2. Select **Audit** to open the audit search.
3. Click **Start recording user and admin activity** next to the information warning at the top.
4. Click **Yes** on the dialog box to confirm.

15.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-log-enable-disable?view=o365-worldwide
- https://learn.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps

15.6. Data

Enabled
False

16. Ensure DLP policies are enabled

2024-03-15

16.1. Information

ID	Category	Subcategory	Review
b9caf88c-0c9c-42a8-b6be-14953a8b76c3	Microsoft Purview	Data Loss Prevention	True

16.2. Description

Data Loss Prevention (DLP) policies allow Exchange Online and SharePoint Online content to be scanned for specific types of data like social security numbers, credit card numbers, or passwords.

16.3. Technical explanation

Enabling DLP policies alerts users and administrators that specific types of data should not be exposed, helping to protect the data from accidental exposure.

16.4. Advised solution

1. Navigate to Microsoft Purview https://compliance.microsoft.com.
2. Under **Solutions** select **Data loss prevention** then **Policies**.
3. Click **Create policy**.

16.5. More information

- https://learn.microsoft.com/en-us/powershell/module/exchange/search-unifiedauditlog?view=exchange-ps

16.6. Data

Type	Name	DisplayName	Enabled	Workload
Dlp	Default policy for Teams	Default policy for Teams	True	Exchange, SharePoint, OneDriveForBusiness, Teams

17. Ensure third-party integrated applications are not allowed

2024-03-15

17.1. Information

ID	Category	Subcategory	Review
3caa1bff-bce3-4744-8898-00b0ebc49ff7	Microsoft Entra Admin Center	Identity	True

17.2. Description

App registrations allows users to register custom-developed applications for use within the directory.

17.3. Technical explanation

Third party integrated applications connection to services should be disabled, unless there is a very clear value and robust security controls are in place. While there are legitimate uses, attackers can grant access from breached accounts to third party applications to exfiltrate data from your tenancy without having to maintain the breached account.

17.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Identity** > **Users** select **Users settings**.
3. Set **Users can register applications** to **No**.
4. Click **Save**.

17.5. More information

- https://learn.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

17.6. Data

AllowedToCreateApps
True

18. Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'

2024-03-15

18.1. Information

ID	Category	Subcategory	Review
bf785c94-b3b4-4b1b-bf90-55031fdba42c	Microsoft Entra Admin Center	Identity	True

18.2. Description

Non-privileged users can create tenants in the Azure AD and Entra administration portal under Manage tenant. The creation of a tenant is recorded in the Audit log as category “DirectoryManagement” and activity “Create Company”. Anyone who creates a tenant becomes the Global Administrator of that tenant. The newly created tenant doesn't inherit any settings or configurations.

18.3. Technical explanation

Restricting tenant creation prevents unauthorized or uncontrolled deployment of resources and ensures that the organization retains control over its infrastructure. User generation of shadow IT could lead to multiple, disjointed environments that can make it difficult for IT to manage and secure the organization's data, especially if other users in the organization began using these tenants for business purposes under the misunderstanding that they were secured by the organization's security team.

18.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/
2. Click to expand **Identity** > **Users** > **User settings**.
3. Set **Restrict non-admin users from creating tenants** to **Yes** then **Save**.

18.5. More information

- https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions#restrict-member-users-default-permissions

18.6. Data

AllowedToCreateTenants
True

19. Ensure the option to remain signed in is hidden

2024-03-15

19.1. Information

ID	Category	Subcategory	Review
08798711-af3c-4fdc-8daf-947b050dca95	Microsoft Entra Admin Center	Identity	True

19.2. Description

The option for the user to Stay signed in or the Keep me signed in option will prompt a user after a successful login, when the user selects this option a persistent refresh token is created. Typically this lasts for 90 days and does not prompt for sign-in or Multi-Factor.

19.3. Technical explanation

Allowing users to select this option presents risk, especially in the event that the user signs into their account on a publicly accessible computer/web browser. In this case it would be trivial for an unauthorized person to gain access to any associated cloud data from that account.

19.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Identity** > **Users** > **User settings**.
3. Set **Show keep user signed in** to **No**.
4. Click **Save**.

19.5. More information

N/A

19.6. Data

HideKeepMeSignedIn
False

20. Ensure the Application Usage report is reviewed at least weekly

2024-03-15

20.1. Information

ID	Category	Subcategory	Review
95d55daa-d432-44f5-907a-eda61b57696f	Microsoft Entra Admin Center	Identity	True

20.2. Description

The Application Usage report includes a usage summary for all Software as a Service (SaaS) applications that are integrated with the organization's directory.

20.3. Technical explanation

Review the list of app registrations on a regular basis to look for risky apps that users have enabled that could cause data spillage or accidental elevation of privilege. Attackers can often get access to data illicitly through third-party SaaS applications.

20.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Identity** > **Applications** select **Enterprise applications**.
3. Under **Activity** select **Usage & insights**.
4. Review the information.

20.5. More information

N/A

20.6. Data

Id	AppDisplayName	FailedSignInCount	SuccessfulSignInCount	SuccessPercentage
fb78d390-0c51-40cd-8e17-fdbfab77341b	Microsoft Exchange REST API Based Powershell	0	56	100
d1ddf0e4-d672-4dae-b554-9d5bdfd93547	Microsoft Intune PowerShell	1	0	0
c44b4083-3bb0-49c1-b47d-974e53cbdf3c	Azure Portal	0	9	100
9b716afc-69e9-4f0c-9f66-781f1cee14a2	TimeMap - Integration	0	8	100
89bee1f7-5e6e-4d8a-9f3d-ecd601259da7	Office365 Shell WCSS-Client	0	12	100
7eadcef8-456d-4611-9480-4fff72b8b9e2	Microsoft Account Controls V2	0	35	100
5d9fff84-5b34-4204-bc91-3aaf5f298c5d	SharePointPnP.ProvisioningApp.Tenant	0	2	100
497effe9-df71-4043-a8bb-14cf78c4b63b	Exchange Admin Center	0	1	100
4765445b-32c6-49b0-83e6-1d93765276ca	OfficeHome	0	2	100
31359c7f-bd7e-475c-86db-fdb8c937548e	PnP Management Shell	6	44	88
2ddfbe71-ed12-4123-b99b-d5fc8a062a79	Microsoft Teams Admin Portal Service	0	3	100
2793995e-0a7d-40d7-bd35-6968ba142197	My Apps	0	1	100
1950a258-227b-4e31-a9cf-717495945fc2	Microsoft Azure PowerShell	1	61	98,39
14d82eec-204b-4c2f-b7e8-296a70dab67e	Microsoft Graph Command Line Tools	0	21	100
12128f48-ec9e-42f0-b203-ea49fb6af367	MS Teams Powershell Cmdlets	0	53	100
04b07795-8ddb-461a-bbee-02f9e1bf7b46	Microsoft Azure CLI	1	2	66,67
00000006-0000-0ff1-ce00-000000000000	Microsoft Office 365 Portal	0	5	100

21. Ensure user consent to apps accessing company data on their behalf is not allowed

2024-03-15

21.1. Information

ID	Category	Subcategory	Review
ca409d22-6638-48ff-ad7c-4a61e3488b94	Microsoft Entra Admin Center	Identity	True

21.2. Description

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.

21.3. Technical explanation

Attackers commonly use custom applications to trick users into granting them access to company data. Disabling future user consent operations setting mitigates this risk, and helps to reduce the threat-surface. If user consent is disabled previous consent grants will still be honored but all future consent operations must be performed by an administrator.

21.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Identity** > **Applications** select **Enterprise applications**.
3. Under **Security** select **Consent and permissions** > **User consent settings**.
4. Under **User consent for applications** select **Do not allow user consent**.
5. Click the **Save** option at the top of the window.

21.5. More information

- https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?tabs=azure-portal&pivots=portal

21.6. Data

UserConsentSetting
AllowUserConsentForSelectedPermissions

22. Ensure Microsoft Authenticator is configured to protect against MFA fatigue

2024-03-15

22.1. Information

ID	Category	Subcategory	Review
0c1ccf40-64f3-4300-96e4-2f7f3272bf9a	Microsoft Entra Admin Center	Protection	True

22.2. Description

Microsoft has released additional settings to enhance the configuration of the Microsoft Authenticator application. These settings provide additional information and context to users who receive MFA passwordless and push requests, such as geographic location the request came from, the requesting application and requiring a number match. Ensure the following are Enabled.

- Require number matching for push notifications
- Show application name in push and passwordless notifications
- Show geographic location in push and passwordless notifications

22.3. Technical explanation

As the use of strong authentication has become more widespread, attackers have started to exploit the tendency of users to experience "MFA fatigue." This occurs when users are repeatedly asked to provide additional forms of identification, leading them to eventually approve requests without fully verifying the source. To counteract this, number matching can be employed to ensure the security of the authentication process. With this method, users are prompted to confirm a number displayed on their original device and enter it into the device being used for MFA. Additionally, other information such as geolocation and application details are displayed to enhance the end user's awareness. Among these 3 options, number matching provides the strongest net security gain.

22.4. Advised solution

1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com.
2. Click to expand **Protection** > **Authentication methods** select **Policies**.
3. Select **Microsoft Authenticator**
4. Under **Enable and Target** ensure the setting is set to **Enable**.
5. Select **Configure**
6. Set the following Microsoft Authenticator settings:
   - **Require number matching for push notifications Status** is set to **Enabled**, Target **All users**
   - **Show application name in push and passwordless notifications** is set to **Enabled**, Target **All users**
   - **Show geographic location in push and passwordless notifications** is set to **Enabled**, Target **All users**

22.5. More information

- https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-default-enablement
- https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677
- https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match

22.6. Data

id	state	displayApp	displayLocation
MicrosoftAuthenticator	enabled	disabled	disabled

23. Ensure custom banned passwords lists are used

2024-03-15

23.1. Information

ID	Category	Subcategory	Review
bb23f25a-0c03-4607-a232-ef8902a0a899	Microsoft Entra Admin Center	Protection	True

23.2. Description

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support business and security needs, custom banned password lists can be defined. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.
A custom banned password list should include some of the following examples:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms
- Abbreviations that have specific company meaning

23.3. Technical explanation

Creating a new password can be difficult regardless of one's technical background. It is common to look around one's environment for suggestions when building a password, however, this may include picking words specific to the organization as inspiration for a password. An adversary may employ what is called a 'mangler' to create permutations of these specific words in an attempt to crack passwords or hashes making it easier to reach their goal.

23.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/
2. Click to expand **Protection** > **Authentication methods**
3. Select **Password protection**
4. Set **Enforce custom list** to **Yes**
5. In Custom banned password list create a list using suggestions outlined in this document.
6. Click **Save**

23.5. More information

- https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#custom-banned-password-list
- https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection

23.6. Data

Enabled
False

24. Ensure 'Self service password reset enabled' is set to 'All'

2024-03-15

24.1. Information

ID	Category	Subcategory	Review
2425f84f-76cf-441b-891e-86142f14ff9e	Microsoft Entra Admin Center	Protection	True

24.2. Description

Enabling self-service password reset allows users to reset their own passwords in Azure AD. When users sign in to Microsoft 365, they will be prompted to enter additional contact information that will help them reset their password in the future. If combined registration is enabled additional information, outside of multi-factor, will not be needed.

24.3. Technical explanation

Users will no longer need to engage the helpdesk for password resets, and the password reset mechanism will automatically block common, easily guessable passwords.

24.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Protection** > **Password reset** select **Properties**.
3. Set **Self service password reset enabled** to **All**

24.5. More information

N/A

24.6. Data

EnablementType
None

25. Ensure 'Privileged Identity Management' is used to manage roles

2024-03-15

25.1. Information

ID	Category	Subcategory	Review
99dcdd37-60f6-450e-be03-13a85fcc5776	Microsoft Entra Admin Center	Identity Governance	True

25.2. Description

Azure Active Directory Privileged Identity Management can be used to audit roles, allow just in time activation of roles and allow for periodic role attestation. Organizations should remove permanent members from privileged Office 365 roles and instead make them eligible, through a JIT activation workflow.

25.3. Technical explanation

Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of a malicious actor getting that access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD and Office 365. Organizations can give users just-in-time (JIT) privileged access to roles. There is a need for oversight for what those users are doing with their administrator privileges. PIM helps to mitigate the risk of excessive, unnecessary, or misused access rights.

25.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Identity Governance** select **Privileged Identity Management**.
3. Select **Azure AD Roles**.
4. Select **Roles** beneath **Manage**.
5. Inspect at a minimum the following sensitive roles. For each of the members that have an **ASSIGNMENT TYPE** of **Permanent**, click on the **...** and choose **Make eligible**:
   - Application Administrator
   - Authentication Administrator
   - Billing Administrator
   - Cloud Application Administrator
   - Cloud Device Administrator
   - Compliance Administrator
   - Customer LockBox Access Approver
   - Device Administrators
   - Exchange Administrators
   - Global Administrators
   - HelpDesk Administrator
   - Information Protection Administrator
   - Intune Service Administrator
   - Kaizala Administrator
   - License Administrator
   - Password Administrator
   - PowerBI Service Administrator
   - Privileged Authentication Administrator
   - Privileged Role Administrator
   - Security Administrator
   - SharePoint Service Administrator
   - Skype for Business Administrator
   - Teams Service Administrator
   - User Administrator

25.5. More information

N/A

25.6. Data

roleID	roleName	eligibleCount	activeCount
62e90394-69f5-4237-9190-012177145e10	Global Administrator	1	3
10dae51f-b6af-4016-8d66-8c2a99b929b3	Guest User	0	0
2af84b1e-32c8-42b7-82bc-daa82404023b	Restricted Guest User	0	0
95e79109-95c0-4d8e-aee3-d01accf2d47b	Guest Inviter	0	0
fe930be7-5e62-47db-91af-98c3a49a38b1	User Administrator	0	0
729827e3-9c14-49f7-bb1b-9608f156bbb8	Helpdesk Administrator	0	0
f023fd81-a637-4b56-95fd-791ac0226033	Service Support Administrator	0	0
b0f54661-2d74-4c50-afa3-1ec803f12efe	Billing Administrator	0	0
a0b1b346-4d3e-4e8b-98f8-753987be4970	User	0	0
4ba39ca4-527c-499a-b93d-d9b492c50246	Partner Tier1 Support	0	0
e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8	Partner Tier2 Support	0	0
88d8e3e3-8f55-4a1e-953a-9b9898b8876b	Directory Readers	0	1
9360feb5-f418-4baa-8175-e2a00bac4301	Directory Writers	0	0
29232cdf-9323-42fd-ade2-1d097af3e4de	Exchange Administrator	0	1
f28a1f50-f6e7-4571-818b-6a12f2af6b6c	SharePoint Administrator	0	0
75941009-915a-4869-abe7-691bff18279e	Skype for Business Administrator	0	0
d405c6df-0af8-4e3b-95e4-4d06e542189e	Device Users	0	0
9f06204d-73c1-4d4c-880a-6edb90606fd8	Azure AD Joined Device Local Administrator	0	0
9c094953-4995-41c8-84c8-3ebb9b32c93f	Device Join	0	0
c34f683f-4d5a-4403-affd-6615e00e3a7f	Workplace Device Join	0	0
17315797-102d-40b4-93e0-432062caca18	Compliance Administrator	0	0

d29b2b05-8046-44ba-8758-1e26182fcf32	Directory Synchronization Accounts	0	0
2b499bcd-da44-4968-8aec-78e1674fa64d	Device Managers	0	0
9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3	Application Administrator	1	1
cf1c38e5-3621-4004-a7cb-879624dced7c	Application Developer	0	0
5d6b6bb7-de71-4623-b4af-96380a352509	Security Reader	0	0
194ae4cb-b126-40b2-bd5b-6091b380977d	Security Administrator	0	0
e8611ab8-c189-46e8-94e1-60213ab1f814	Privileged Role Administrator	0	0
3a2c62db-5318-420d-8d74-23affee5d9d5	Intune Administrator	0	0
158c047a-c907-4556-b7ef-446551a6b5f7	Cloud Application Administrator	0	0
5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91	Customer LockBox Access Approver	0	0
44367163-eba1-44c3-98af-f5787879f96a	Dynamics 365 Administrator	0	0
a9ea8996-122f-4c74-9520-8edcd192826c	Fabric Administrator	0	0
b1be1c3e-b65d-4f19-8427-f6fa0d97feb9	Conditional Access Administrator	0	0
4a5d8f65-41da-4de4-8968-e035b65339cf	Reports Reader	0	0
790c1fb9-7f7d-4f88-86a1-ef1f95c05c1b	Message Center Reader	0	0
7495fdc4-34c4-4d15-a289-98788ce399fd	Azure Information Protection Administrator	0	0
38a96431-2bdf-4b4c-8b6e-5d3d8abac1a4	Desktop Analytics Administrator	0	0
4d6ac14f-3453-41d0-bef9-a3e0c569773a	License Administrator	0	0
7698a772-787b-4ac8-901f-60d6b08affd2	Cloud Device Administrator	0	0
c4e39bd9-1100-46d3-8c65-fb160da0071f	Authentication Administrator	0	0
7be44c8a-adaf-4e2a-84d6-ab2649e08a13	Privileged Authentication Administrator	0	0
baf37b3a-610e-45da-9e62-d9d1e5e8914b	Teams Communications Administrator	0	0
f70938a0-fc10-4177-9e90-2178f8765737	Teams Communications Support Engineer	0	0
fcf91098-03e3-41a9-b5ba-	Teams Communications	0	0

6f0ec8188a12	Support Specialist		
69091246-20e8-4a56-aa4d-066075b2a7a8	Teams Administrator	0	0
eb1f4a8d-243a-41f0-9fbd-c7cdf6c5ef7c	Insights Administrator	0	0
ac16e43d-7b2d-40e0-ac05-243ff356ab5b	Message Center Privacy Reader	0	0
6e591065-9bad-43ed-90f3-e9424366d2f0	External ID User Flow Administrator	0	0
0f971eea-41eb-4569-a71e-57bb8a3eff1e	External ID User Flow Attribute Administrator	0	0
aaf43236-0c0d-4d5f-883a-6955382ac081	B2C IEF Keyset Administrator	0	0
3edaf663-341e-4475-9f94-5c398ef6c070	B2C IEF Policy Administrator	0	0
be2f45a1-457d-42af-a067-6ec1fa63bc45	External Identity Provider Administrator	0	0
e6d1a23a-da11-4be4-9570-befc86d067a7	Compliance Data Administrator	0	0
5f2222b1-57c3-48ba-8ad5-d4759f1fde6f	Security Operator	0	0
74ef975b-6605-40af-a5d2-b9539d836353	Kaizala Administrator	0	0
f2ef992c-3afb-46b9-b7cf-a126ee74c451	Global Reader	0	1
0964bb5e-9bdb-4d7b-ac29-58e794862a40	Search Administrator	0	0
8835291a-918c-4fd7-a9ce-faa49f0cf7d9	Search Editor	0	0
966707d0-3269-4727-9be2-8c3a10f19b9d	Password Administrator	0	0
644ef478-e28f-4e28-b9dc-3fdde9aa0b1f	Printer Administrator	0	0
e8cef6f1-e4bd-4ea8-bc07-4b8d950f4477	Printer Technician	0	0
0526716b-113d-4c15-b2c8-68e3c22b9f80	Authentication Policy Administrator	0	0
fdd7a751-b60b-444a-984c-02652fe8fa1c	Groups Administrator	0	0
11648597-926c-4cf3-9c36-bcebb0ba8dcc	Power Platform Administrator	0	0
e3973bdf-4987-49ae-837a-ba8e231c7286	Azure DevOps Administrator	0	0
8ac3fc64-6eca-42ea-9e69-59f4c7b60eb2	Hybrid Identity Administrator	0	0
2b745bdf-0803-4d80-aa65-822c4493daac	Office Apps Administrator	0	0

d37c8bed-0711-4417-ba38-b4abe66ce4c2	Network Administrator	0	0
31e939ad-9672-4796-9c2e-873181342d2d	Insights Business Leader	0	0
3d762c5a-1b6c-493f-843e-55a3b42923d4	Teams Devices Administrator	0	0
c430b396-e693-46cc-96f3-db01bf8bb62a	Attack Simulation Administrator	0	0
9c6df0f2-1e7c-4dc3-b195-66dfbd24aa8f	Attack Payload Author	0	0
75934031-6c7e-415a-99d7-48dbd49e875e	Usage Summary Reports Reader	0	0
b5a8dcf3-09d5-43a9-a639-8e29ef291470	Knowledge Administrator	0	0
744ec460-397e-42ad-a462-8b3f9747a02c	Knowledge Manager	0	0
8329153b-31d0-4727-b945-745eb3bc5f31	Domain Name Administrator	0	0
8424c6f0-a189-499e-bbd0-26c1753c96d4	Attribute Definition Administrator	0	0
58a13ea3-c632-46ae-9ee0-9c0d43cd7f3d	Attribute Assignment Administrator	0	0
1d336d2c-4ae8-42ef-9711-b3604ce3fc2c	Attribute Definition Reader	0	0
ffd52fa5-98dc-465c-991d-fc073eb59f8f	Attribute Assignment Reader	0	0
31392ffb-586c-42d1-9346-e59415a2cc4e	Exchange Recipient Administrator	0	0
45d8d3c5-c802-45c6-b32a-1d70b5e1e86e	Identity Governance Administrator	0	0
892c5842-a9a6-463a-8041-72aa08ca3cf6	Cloud App Security Administrator	0	0
32696413-001a-46ae-978c-ce0f6b3620d2	Windows Update Deployment Administrator	0	0
11451d60-acb2-45eb-a7d6-43d0f0125c13	Windows 365 Administrator	0	0
3f1acade-1e04-4fbc-9b69-f0302cd84aef	Edge Administrator	0	0
810a2642-a034-447f-a5e8-41beaa378541	Yammer Administrator	0	0
25a516ed-2fa0-40ea-a2d0-12923a21473a	Authentication Extensibility Administrator	0	0
e300d9e7-4a2b-4295-9eff-f1c78b36cc98	Virtual Visits Administrator	0	0
25df335f-86eb-4119-b717-0ff02de207e9	Insights Analyst	0	0
1501b917-7653-4ff9-a4b5-	Microsoft Hardware Warranty	0	0

203eaf33784f	Administrator		
281fe777-fb20-4fbb-b7a3-ccebce5b0d96	Microsoft Hardware Warranty Specialist	0	0
112ca1a2-15ad-4102-995e-45b0bc479a6a	Tenant Creator	0	0
59d46f88-662b-457b-bceb-5c3809e5908f	Lifecycle Workflows Administrator	0	0
92b086b3-e367-4ef2-b869-1de128fb986e	Viva Goals Administrator	0	0
27460883-1df1-4691-b032-3b79643e5e63	User Experience Success Manager	0	0
af78dc32-cf4d-46f9-ba4e-4428526346b5	Permissions Management Administrator	0	0
507f53e4-4e52-4077-abd3-d2e1558b6ea2	Organizational Messages Writer	0	0
ac434307-12b9-4fa1-a708-88bf58caabc1	Global Secure Access Administrator	0	0
87761b17-1ed2-4af3-9acd-92a150038160	Viva Pulse Administrator	0	0
dd13091a-6207-4fc0-82ba-3641e056ab95	Extended Directory User Administrator	0	0
5b784334-f94b-471a-a387-e7219fc49ca2	Attribute Log Administrator	0	0
9c99539d-8186-4804-835f-fd51ef9e2dcd	Attribute Log Reader	0	0
963797fb-eb3b-4cde-8ce3-5878b3f32a3f	Dynamics 365 Business Central Administrator	0	0
8c8b803f-96e1-4129-9349-20738d9f9652	Microsoft 365 Migration Administrator	0	0
1a7d78b6-429f-476b-b8eb-35fb715fffd4	SharePoint Embedded Administrator	0	0
92ed04bf-c94a-4b82-9729-b799a7a4c178	Organizational Branding Administrator	0	0

26. Ensure 'Access reviews' for high privileged Azure AD roles are configured

2024-03-15

26.1. Information

ID	Category	Subcategory	Review
e8c91221-63d2-4797-8a86-7ef53c30a9d6	Microsoft Entra Admin Center	Identity Governance	True

26.2. Description

Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organization.
Ensure Access reviews for high privileged Azure AD roles are done no less frequently than weekly. These reviews should include at a minimum the roles listed below:

- Global Administrator
- Exchange Administrator
- SharePoint Administrator
- Teams Administrator
- Security Administrator

26.3. Technical explanation

Regular review of critical high privileged roles in Azure AD will help identify role drift, or potential malicious activity. This will enable the practice and application of "separation of duties" where even non-privileged users like security auditors can be assigned to review assigned roles in an organization. Furthermore, if configured these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review.

26.4. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/
2. Click to expand **Identity Governance** and select **Privileged Identity Management**
3. Select **Azure AD Roles** under **Manage**
4. Select **Access reviews** and click **New access review**.
5. Provide a name and description.
6. **Frequency** set to **Weekly** or more frequent.
7. **Duration (in days)** is set to at most **3**.
8. **End** set to **Never**.
9. Role select these roles:
   - Global Administrator
   - Exchange Administrator
   - SharePoint Administrator
   - Teams Administrator
   - Security Administrator
10. **Assignment type** set to **All active and eligible assignments**.
11. Reviewers set to **Selected user(s) or group(s)**
12. **Select reviewers** are member(s) responsible for this type of review.
13. **Auto apply results to resource** set to **Enable**
14. **If reviewers don't respond** is set to **No change**
15. **Show recommendations** set to **Enable**
16. **Require reason or approval** set to **Enable**
17. **Mail notifications** set to **Enable**
18. **Reminders** set to **Enable**
19. Click **Start** to save the review.

26.5. More information

- https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review
- https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

26.6. Data

NotConfigured

Global Administrator,SharePoint Administrator,Teams Administrator,Security Administrator,Exchange Administrator

27. Ensure mailbox auditing for users is Enabled

2024-03-15

27.1. Information

ID	Category	Subcategory	Review
2b849f34-8991-4a13-a6f1-9f7d0ea4bcef	Microsoft Exchange Admin Center	Audit	True

27.2. Description

Mailbox audit logging is turned on by default in all organizations. This effort started in January 2019, and means that certain actions performed by mailbox owners, delegates, and admins are automatically logged. The corresponding mailbox audit records are available for admins to search in the mailbox audit log. Mailboxes and shared mailboxes have actions assigned to them individually in order to audit the data the organization determines valuable at the mailbox level. The recommended state is AuditEnabled to True on all user mailboxes along with additional audit actions beyond the Microsoft defaults.
Due to some differences in defaults for audit actions this recommendation is specific to users assigned an E3 license only.

27.3. Technical explanation

Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing, and ensuring the proper mailbox actions are accounted for allows for Microsoft 365 teams to run security operations, forensics or general investigations on mailbox activities. The following mailbox types ignore the organizational default and must have AuditEnabled set to True at the mailbox level in order to capture relevant audit data.

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

27.4. Advised solution

1. Connect to Exchange Online using Connect-ExchangeOnline.
2. Run the following PowerShell command:

```
$AuditAdmin = @( 'ApplyRecord', 'Copy', 'Create', 'FolderBind', 'HardDelete',
'Move', 'MoveToDeletedItems', 'SendAs', 'SendOnBehalf', 'SoftDelete',
'Update', 'UpdateCalendarDelegation', 'UpdateFolderPermissions',
'UpdateInboxRules' )

$AuditDelegate = @( 'ApplyRecord', 'Create', 'FolderBind', 'HardDelete',
'Move', 'MoveToDeletedItems', 'SendAs', 'SendOnBehalf', 'SoftDelete',
'Update', 'UpdateFolderPermissions', 'UpdateInboxRules' )

$AuditOwner = @( 'ApplyRecord', 'Create', 'HardDelete', 'MailboxLogin',
'Move', 'MoveToDeletedItems', 'SoftDelete', 'Update',
'UpdateCalendarDelegation', 'UpdateFolderPermissions', 'UpdateInboxRules' )

$MBX = Get-EXOMailbox -ResultSize Unlimited | Where-Object {
$_.RecipientTypeDetails -eq 'UserMailbox' }

$MBX | Set-Mailbox -AuditEnabled $true -AuditLogAgeLimit 90 -AuditAdmin
$AuditAdmin -AuditDelegate $AuditDelegate -AuditOwner $AuditOwner
```

27.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-mailboxes?view=o365-worldwide

27.6. Data

Name	Alias	UserPrincipalName	PrimarySmtpAddress	AuditEnabled
DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}	DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}	DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@O4nxg.onmicrosoft.com	DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@O4nxg.onmicrosoft.com	False

28. Ensure all forms of mail forwarding are blocked and/or disabled

2024-03-15

28.1. Information

ID	Category	Subcategory	Review
45887263-5f2f-4306-946d-8f36acfb3691	Microsoft Exchange Admin Center	Mail Flow	True

28.2. Description

Exchange Online offers several methods of managing the flow of email messages. These are Remote domain, Transport Rules, and Anti-spam outbound policies. These methods work together to provide comprehensive coverage for potential automatic forwarding channels:

- Outlook forwarding using inbox rules
- Outlook forwarding configured using OOF rule
- OWA forwarding setting (ForwardingSmtpAddress)
- Forwarding set by the admin using EAC (ForwardingAddress)
- Forwarding using Power Automate / Flow

Ensure a Transport rule and Anti-spam outbound policy are used to block mail forwarding.

28.3. Technical explanation

Attackers often create these rules to exfiltrate data from your tenancy, this could be accomplished via access to an end-user account or otherwise. An insider could also use one of these methods as a secondary channel to exfiltrate sensitive data.

28.4. Advised solution

1. Open the Exchange admin center through https://admin.exchange.microsoft.com.
2. Select **Mail Flow** then **Rules**.
3. For each rule that redirects email to external domains, select the rule and click the '**Delete**' icon.
4. Navigate to Microsoft 365 Defender https://security.microsoft.com/
5. Expand **E-mail & collaboration** then select **Policies & rules**.
6. Select **Threat policies** > **Anti-spam**.
7. Inspect **Anti-spam outbound policy (default)** and ensure **Automatic forwarding** is set to **Off - Forwarding is disabled**
8. Inspect any additional custom outbound policies and ensure **Automatic forwarding is set** to **Off - Forwarding is disabled**, in accordance with the organization's exclusion policies.

28.5. More information

- https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/mail-flow-rule-procedures?view=exchserver-2019
- https://techcommunity.microsoft.com/t5/exchange-team-blog/all-you-need-to-know-about-automatic-email-forwarding-in/ba-p/2074888#:~:text=%20%20%20Automatic%20forwarding%20option%20%20,%
- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/outbound-spam-policies-external-email-forwarding?view=o365-worldwide

28.6. Data

TransportRules	OutboundSpamFilterPolicies
	Default

29. Ensure email from external senders is identified

2024-03-15

29.1. Information

ID	Category	Subcategory	Review
a73f7dd0-6c32-44d1-ae18-197b775e28bb	Microsoft Exchange Admin Center	Mail Flow	True

29.2. Description

External callouts provide a native experience to identify emails from senders outside the organization. This is achieved by presenting a new tag on emails called "External" (the string is localized based on the client language setting) and exposing related user interface at the top of the message reading view to see and verify the real sender's email address.
Once this feature is enabled via PowerShell, it might take 24-48 hours for users to start seeing the External sender tag in email messages received from external sources (outside of your organization), providing their Outlook version supports it.
The recommended state is ExternalInOutlook set to Enabled True

29.3. Technical explanation

Tagging emails from external senders helps to inform end users about the origin of the email. This can allow them to proceed with more caution and make informed decisions when it comes to identifying spam or phishing emails.

29.4. Advised solution

1. Connect to Exchange online using Connect-ExchangeOnline.
2. Run the following PowerShell command:

```
Set-ExternalInOutlook -Enabled $true
```

29.5. More information

- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/configuration-best-practices
- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

29.6. Data

Identity	Enabled	AllowList
d8b1b73e-e147-4d6f-b7e4-cf68b59c7224	False	

30. Ensure users installing Outlook add-ins is not allowed

2024-03-15

30.1. Information

ID	Category	Subcategory	Review
36ee88d3-0ab8-41ea-90e7-fd9b14ed6a03	Microsoft Exchange Admin Center	Roles	True

30.2. Description

Specify the administrators and users who can install and manage add-ins for Outlook in Exchange Online.
By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application.

30.3. Technical explanation

Attackers exploit vulnerable or custom add-ins to access user data. Disabling user-installed add-ins in Microsoft Outlook reduces this threat surface.

30.4. Advised solution

1. Navigate to Exchange admin center https://admin.exchange.microsoft.com.
2. Click to expand **Roles** select **User roles**.
3. Select **Default Role Assignment Policy**.
4. In the properties pane on the right click on **Manage permissions**.
5. Under Other roles uncheck **My Custom Apps**, **My Marketplace Apps** and **My ReadWriteMailboxApps**.
6. Click **Save changes**.

30.5. More information

- https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/add-ins-for-outlook/specify-who-can-install-and-manage-add-ins?source=recommendations
- https://learn.microsoft.com/en-us/exchange/permissions-exo/role-assignment-policies

30.6. Data

Name	AssignedRoles
Default Role Assignment Policy	MyBaseOptions, My ReadWriteMailbox Apps, MyProfileInformation, MyContactInformation, MyDistributionGroups, MyDistributionGroupMembership, MyMailSubscriptions, My Marketplace Apps, My Custom Apps, MyTextMessaging, MyRetentionPolicies, MyVoiceMail

31. Ensure MailTips are enabled for end users

2024-03-15

31.1. Information

ID	Category	Subcategory	Review
bed51aa7-e6de-4542-96fc-ffe9d699763c	Microsoft Exchange Admin Center	Settings	True

31.2. Description

MailTips are informative messages displayed to users while they're composing a message. While a new message is open and being composed, Exchange analyzes the message (including recipients). If a potential problem is detected, the user is notified with a MailTip prior to sending the message. Using the information in the MailTip, the user can adjust the message to avoid undesirable situations or non-delivery reports (also known as NDRs or bounce messages).

31.3. Technical explanation

Setting up MailTips gives a visual aid to users when they send emails to large groups of recipients or send emails to recipients not within the tenant.

31.4. Advised solution

1. Run the Microsoft Exchange Online PowerShell Module.
2. Connect to Exchange Online using Connect-ExchangeOnline.
3. Run the following PowerShell command:

```
$TipsParams = @{ MailTipsAllTipsEnabled   = $true;
    MailTipsExternalRecipientsTipsEnabled = $true;
    MailTipsGroupMetricsEnabled           = $true;
    MailTipsLargeAudienceThreshold        = '25'
}

Set-OrganizationConfig @TipsParams
```

31.5. More information

- https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/mailtips/mailtips
- https://learn.microsoft.com/en-us/powershell/module/exchange/set-organizationconfig?view=exchange-ps

31.6. Data

Valid	MailTipsAllTipsEnabled	MailTipsExternalRecipientsTipsEnabled	MailTipsGroupMetricsEnabled	MailTipsLargeAudienceThreshold
False	True	False	True	25

32. Ensure modern authentication for SharePoint applications is required

2024-03-15

32.1. Information

ID	Category	Subcategory	Review
a8f1139f-9e08-4da9-bfea-1ddd811e6d68	Microsoft SharePoint Admin Center	Policies	True

32.2. Description

Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers.

32.3. Technical explanation

Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by SharePoint applications. Requiring modern authentication for SharePoint applications ensures strong authentication mechanisms are used when establishing sessions between these applications, SharePoint, and connecting users.

32.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint.
2. Click to expand **Policies** select **Access control**.
3. Select **Apps that don't use modern authentication**.
4. Select the radio button for **Block access**.
5. Click **Save**.

32.5. More information

- https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps

32.6. Data

LegacyAuthProtocolsEnabled
True

33. Ensure external content sharing is restricted

2024-03-15

33.1. Information

ID	Category	Subcategory	Review
f30646cc-e1f1-42b5-a3a5-4d46db01e822	Microsoft SharePoint Admin Center	Policies	True

33.2. Description

The external sharing settings govern sharing for the organization overall. Each site has its own sharing setting that can be set independently, though it must be at the same or more restrictive setting as the organization.
The new and existing guests option requires people who have received invitations to sign in with their work or school account (if their organization uses Microsoft 365) or a Microsoft account, or to provide a code to verify their identity. Users can share with guests already in your organization's directory, and they can send invitations to people who will be added to the directory if they sign in.
The recommended state is New and existing guests or less permissive.

33.3. Technical explanation

Forcing guest authentication on the organization's tenant enables the implementation of controls and oversight over external file sharing. When a guest is registered with the organization, they now have an identity which can be accounted for. This identity can also have other restrictions applied to it through group membership and conditional access rules.

33.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Click to expand **Policies** > **Sharing.**
3. Locate the **External sharing section**.
4. Under **SharePoint**, move the slider bar to **New and existing guests or a less permissive level**.
   - OneDrive will also be moved to the same level and can never be more permissive than SharePoint.

33.5. More information

N/A

33.6. Data

SharingCapability
ExistingExternalUserSharingOnly

34. Ensure OneDrive content sharing is restricted

2024-03-15

34.1. Information

ID	Category	Subcategory	Review
fcf37f2f-6b1d-4616-85cd-0b5b33d8f028	Microsoft SharePoint Admin Center	Policies	True

34.2. Description

This setting governs the global permissiveness of OneDrive content sharing in the organization. OneDrive content sharing can be restricted independent of SharePoint but can never be more permissive than the level established with SharePoint.
The recommended state is Only people in your organization.

34.3. Technical explanation

OneDrive, designed for end-user cloud storage, inherently provides less oversight and control compared to SharePoint, which often involves additional content overseers or site administrators. This autonomy can lead to potential risks such as inadvertent sharing of privileged information by end users. Restricting external OneDrive sharing will require users to transfer content to SharePoint folders first which have those tighter controls.

34.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Click to expand **Policies** > **Sharing**.
3. Locate the **External sharing** section.
4. Under **OneDrive**, set the slider bar to **Only people in your organization**.

34.5. More information

N/A

34.6. Data

SharingCapability
ExistingExternalUserSharingOnly

35. Ensure that SharePoint guest users cannot share items they don't own

2024-03-15

35.1. Information

ID	Category	Subcategory	Review
1a27642f-0ab9-46ba-8d26-8e14a5b52994	Microsoft SharePoint Admin Center	Policies	True

35.2. Description

SharePoint gives users the ability to share files, folders, and site collections. Internal users can share with external collaborators, and with the right permissions could share to other external parties.

35.3. Technical explanation

Sharing and collaboration are key; however, file, folder, or site collection owners should have the authority over what external users get shared with to prevent unauthorized disclosures of information.

35.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Click to expand **Policies** then select **Sharing**.
3. Expand **More external sharing settings**, uncheck **Allow guests to share items they don't own**.
4. Click **Save**.

35.5. More information

- https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off
- https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview

35.6. Data

PreventExternalUsersFromResharing
False

36. Ensure SharePoint external sharing is managed through domain whitelist/blacklists

2024-03-15

36.1. Information

ID	Category	Subcategory	Review
2c6d9aa6-0698-468d-8b0f-8d40ba5daa7b	Microsoft SharePoint Admin Center	Policies	True

36.2. Description

Control sharing of documents to external domains by either blocking domains or only allowing sharing with specific named domains.

36.3. Technical explanation

Attackers will often attempt to expose sensitive information to external entities through sharing, and restricting the domains that users can share documents with will reduce that surface area.

36.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Expand **Policies** then click **Sharing**.
3. Expand **More external sharing settings** and check **Limit external sharing by domain**.
4. Select **Add domains** to add a list of approved domains.
5. Click **Save** at the bottom of the page.

36.5. More information

N/A

36.6. Data

SharingDomainRestrictionMode
None

37. Ensure link sharing is restricted in SharePoint and OneDrive

2024-03-15

37.1. Information

ID	Category	Subcategory	Review
c4b93e39-d8a1-459e-835e-e4545418c633	Microsoft SharePoint Admin Center	Policies	True

37.2. Description

This setting sets the default link type that a user will see when sharing content in OneDrive or SharePoint. It does not restrict or exclude any other options. The recommended state is Specific people (only the people the user specifies)

37.3. Technical explanation

By defaulting to specific people, the user will first need to consider whether or not the content being shared should be accessible by the entire organization versus select individuals. This aids in reinforcing the concept of least privilege.

37.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Expand **Policies** then click **Sharing**.
3. Scroll to **Files and folder links**.
4. Set **Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive** to **Specific people (only the people the user specifies)**

37.5. More information

- https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps

37.6. Data

SharePointLinkSharing	OneDriveLinkSharing
Internal	None

38. Ensure external sharing is restricted by security group

2024-03-15

38.1. Information

ID	Category	Subcategory	Review
d62a22ba-144b-44e6-8592-9e3692742a89	Microsoft SharePoint Admin Center	Policies	True

38.2. Description

External sharing of content can be restricted to specific security groups. This setting is global, applies to sharing in both SharePoint and OneDrive and cannot be set at the site level in SharePoint.
The recommended state is Enabled or Checked.

38.3. Technical explanation

Organizations wishing to create tighter security controls for external sharing can set this to enforce role-based access control by using security groups already defined in Microsoft Entra.

38.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Expand **Policies** then click **Sharing**.
3. Scroll to and expand **More external sharing settings**.
4. Set the following:
   - Check **Allow only users in specific security groups to share externally**
   - Define **Manage security groups** in accordance with company procedure.

38.5. More information

- https://learn.microsoft.com/en-us/sharepoint/manage-security-groups

38.6. Data

WhoCanShareAllowListInTenant	WhoCanShareAllowListInTenantByPrincipalIdentity

39. Ensure guest access to a site or OneDrive will expire automatically

2024-03-15

39.1. Information

ID	Category	Subcategory	Review
af231488-4ca8-4496-8d10-09b65110d1ee	Microsoft SharePoint Admin Center	Policies	True

39.2. Description

This policy setting configures the expiration time for each guest that is invited to the SharePoint site or with whom users share individual files and folders with. The recommended state is 30 or less.

39.3. Technical explanation

This setting ensures that guests who no longer need access to the site or link no longer have access after a set period of time. Allowing guest access for an indefinite amount of time could lead to loss of data confidentiality and oversight.

39.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Expand **Policies** then click **Sharing**.
3. Scroll to and expand **More external sharing settings**.
4. Set **Guest access to a site or OneDrive will expire automatically after this many days** to **30**

39.5. More information

- https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo#change-the-organization-level-external-sharing-setting
- https://learn.microsoft.com/en-us/microsoft-365/community/sharepoint-security-a-team-effort

39.6. Data

ExternalUserExpireInDays
32

40. Ensure reauthentication with verification code is restricted

2024-03-15

40.1. Information

ID	Category	Subcategory	Review
82712a94-8427-4871-8d09-f2b94e8e1bf1	Microsoft SharePoint Admin Center	Policies	True

40.2. Description

This setting configures if guests who use a verification code to access the site or links are required to reauthenticate after a set number of days.
The recommended state is 15 or less.

40.3. Technical explanation

By increasing the frequency of times guests need to reauthenticate this ensures guest user access to data is not prolonged beyond an acceptable amount of time.

40.4. Advised solution

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Expand **Policies** then click **Sharing**.
3. Scroll to and expand **More external sharing settings**.
4. Set **People who use a verification code must reauthenticate after this** to **15** or less.

40.5. More information

- https://learn.microsoft.com/en-US/sharepoint/what-s-new-in-sharing-in-targeted-release?WT.mc_id=365AdminCSH_spo
- https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo#change-the-organization-level-external-sharing-setting
- https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode

40.6. Data

EmailAttestationEnabled	EmailAttestationReAuthDays
False	30

41. Ensure Office 365 SharePoint infected files are disallowed for download

2024-03-15

41.1. Information

ID	Category	Subcategory	Review
7033c11e-71d9-407b-9a19-cde209d05426	Microsoft SharePoint Admin Center	Settings	True

41.2. Description

By default, SharePoint online allows files that Defender for Office 365 has detected as infected to be downloaded.

41.3. Technical explanation

Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams protects your organization from inadvertently sharing malicious files. When an infected 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.

41.4. Advised solution

1. Connect to SharePoint Online using Connect-SPOService.
2. Run the following PowerShell command

```
Set-SPOTenant -DisallowInfectedFileDownload $true
```

41.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-configure?view=o365-worldwide
- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection-for-spo-odfb-teams-about?view=o365-worldwide

41.6. Data

DisallowInfectedFileDownload
False

42. Ensure external file sharing in Teams is enabled for only approved cloud storage services

2024-03-15

42.1. Information

ID	Category	Subcategory	Review
36016fe3-30fe-4070-a446-441ae23cfe95	Microsoft Teams Admin Center	Teams	True

42.2. Description

Microsoft Teams enables collaboration via file sharing. This file sharing is conducted within Teams, using SharePoint Online, by default; however, third-party cloud services are allowed as well.

42.3. Technical explanation

Ensuring that only authorized cloud storage providers are accessible from Teams will help to dissuade the use of non-approved storage providers.

42.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com.
2. Click to expand **Teams** select **Teams settings**.
3. Set any unauthorized providers to **Off**.

42.5. More information

https://learn.microsoft.com/en-us/microsoft-365/enterprise/manage-skype-for-business-online-with-microsoft-365-powershell?view=o365-worldwide

42.6. Data

Dropbox	Box	GoogleDrive	ShareFile	Egnyte
True	True	True	True	True

43. Ensure users can't send emails to a channel email address

2024-03-15

43.1. Information

ID	Category	Subcategory	Review
4623807d-6c30-4906-a33e-1e55fbbdfdec	Microsoft Teams Admin Center	Teams	True

43.2. Description

Teams channel email addresses are an optional feature that allows users to email the Teams channel directly.

43.3. Technical explanation

Channel email addresses are not under the tenant's domain and organizations do not have control over the security settings for this email address. An attacker could email channels directly if they discover the channel email address.

43.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com.
2. Click to expand **Teams** select **Teams settings**.
3. Under email integration set **Users can send emails to a channel email address** to **Off**.

43.5. More information

- https://learn.microsoft.com/en-us/powershell/module/exchange/search-unifiedauditlog?view=exchange-ps

43.6. Data

AllowEmailIntoChannel
True

44. Ensure 'external access' is restricted in the Teams admin center

2024-03-15

44.1. Information

ID	Category	Subcategory	Review
1d4902a0-dcb6-4b1a-b77a-0662ba15a431	Microsoft Teams Admin Center	Users	True

44.2. Description

This policy setting controls chat with external unmanaged Skype and Teams users. Users in the organization will not be searchable by unmanaged Skype or Teams users and will have to initiate all communications with unmanaged users.

44.3. Technical explanation

Allowing users to communicate with Skype or Teams users outside of an organization presents a potential security threat as external users can interact with organization users over Skype for Business or Teams. While legitimate, productivity-improving scenarios exist, they are outweighed by the risk of data loss, phishing, and social engineering attacks against organization users via Teams. Therefore, it is recommended to restrict external communications in order to minimize the risk of security incidents.

44.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/.
2. Click to expand **Users** select **External access**.
3. Under **Teams and Skype for Business users in external organizations** Select **Block all external domains**
   - NOTE: If the organization's policy allows select any allowed external domains.
4. Under **Teams accounts not managed by an organization** move the slider to **Off**.
5. Under **Skype users** move the slider is to **Off**.
6. Click **Save**.

44.5. More information

- https://learn.microsoft.com/en-us/skypeforbusiness/set-up-skype-for-business-online/set-up-skype-for-business-online
- https://learn.microsoft.com/en-US/microsoftteams/manage-external-access?WT.mc_id=TeamsAdminCenterCSH

44.6. Data

AllowTeamsConsumer	AllowPublicUsers	AllowFederatedUsers	AllowedDomains
True	True	True	AllowAllKnownDomains

45. Ensure anonymous users can't join a meeting

2024-03-15

45.1. Information

ID	Category	Subcategory	Review
087cd766-1d44-444d-a572-21312ddfb804	Microsoft Teams Admin Center	Meetings	True

45.2. Description

This policy setting can prevent anyone other than invited attendees (people directly invited by the organizer, or to whom an invitation was forwarded) from bypassing the lobby and entering the meeting.

45.3. Technical explanation

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times.

45.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/.
2. Click to expand **Meetings** select **Meeting policies**.
3. Click **Global (Org-wide default)**
4. Under meeting join & lobby set **Anonymous users can join a meeting** to **Off**.

45.5. More information

- https://learn.microsoft.com/en-us/MicrosoftTeams/configure-meetings-sensitive-protection

45.6. Data

AllowAnonymousUsersToJoinMeeting
True

46. Ensure only people in my org can bypass the lobby

2024-03-15

46.1. Information

ID	Category	Subcategory	Review
5252f126-4d4e-4a1c-ab56-743f8efe2b3e	Microsoft Teams Admin Center	Meetings	True

46.2. Description

This policy setting controls who can join a meeting directly and who must wait in the lobby until they're admitted by an organizer, co-organizer, or presenter of the meeting.

46.3. Technical explanation

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times.

46.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/.
2. Click to expand **Meetings** select **Meeting policies**.
3. Click **Global (Org-wide default)**
4. Under meeting join & lobby set **Who can bypass the lobby** is set to **People in my org**.

46.5. More information

- https://learn.microsoft.com/en-US/microsoftteams/who-can-bypass-meeting-lobby?WT.mc_id=TeamsAdminCenterCSH
- https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

46.6. Data

AutoAdmittedUsers
EveryoneInCompany

47. Ensure meeting chat does not allow anonymous users

2024-03-15

47.1. Information

ID	Category	Subcategory	Review
61b9c972-bb4e-4768-8db4-89a62fc09877	Microsoft Teams Admin Center	Meetings	True

47.2. Description

This policy setting controls who has access to read and write chat messages during a meeting.

47.3. Technical explanation

Ensuring that only authorized individuals can read and write chat messages during a meeting reduces the risk that a malicious user can inadvertently show content that is not appropriate or view sensitive information.

47.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/.
2. Click to expand **Meetings** select **Meeting policies**.
3. Click **Global (Org-wide default)**
4. Under meeting engagement set **Meeting chat** to **On for everyone but anonymous users**.

47.5. More information

- https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps#-meetingchatenabledtype

47.6. Data

MeetingChatEnabledType
Enabled

48. Ensure only organizers and co-organizers can present

2024-03-15

48.1. Information

ID	Category	Subcategory	Review
8cd7d1c7-6491-433d-9d5b-68f1bf7bcfc3	Microsoft Teams Admin Center	Meetings	True

48.2. Description

This policy setting controls who can present in a Teams meeting.

48.3. Technical explanation

Ensuring that only authorized individuals are able to present reduces the risk that a malicious user can inadvertently show content that is not appropriate.

48.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/.
2. Click to expand **Meetings** select **Meeting policies**.
3. Click **Global (Org-wide default)**
4. Under content sharing set **Who can present** to **Only organizers and co-organizers**.

48.5. More information

- https://learn.microsoft.com/en-US/microsoftteams/meeting-who-present-request-control
- https://learn.microsoft.com/en-us/microsoftteams/meeting-who-present-request-control#manage-who-can-present
- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#configure-meeting-settings-restrict-presenters
- https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

48.6. Data

DesignatedPresenterRoleMode
EveryoneUserOverride

49. Ensure users can report security concerns in Teams

2024-03-15

49.1. Information

ID	Category	Subcategory	Review
3a107b4e-9bef-4480-b5c0-4aedd7a4a0bc	Microsoft Teams Admin Center	Messaging	True

49.2. Description

User reporting settings allow a user to report a message as malicious for further analysis. This recommendation is composed of 3 different settings and all be configured to pass:

- **In the Teams admin center:** On by default and controls whether users are able to report messages from Teams. When this setting is turned off, users can't report messages within Teams, so the corresponding setting in the Microsoft 365 Defender portal is irrelevant.
- **In the Microsoft 365 Defender portal:** On by default for new tenants. Existing tenants need to enable it. If user reporting of messages is turned on in the Teams admin center, it also needs to be turned on the Defender portal for user reported messages to show up correctly on the User reported tab on the Submissions page.
- **Defender - Report message destinations:** This applies to more than just Microsoft Teams and allows for an organization to keep their reports contained. Due to how the parameters are configured on the backend it is included in this assessment as a requirement.

49.3. Technical explanation

Users will be able to more quickly and systematically alert administrators of suspicious malicious messages within Teams. The content of these messages may be sensitive in nature and therefore should be kept within the organization and not shared with Microsoft without first consulting company policy.

49.4. Advised solution

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com.
2. Click to expand **Messaging** select **Messaging policies**.
3. Click **Global (Org-wide default)**.
4. Set **Report a security concern** to **On**.
5. Next, navigate to Microsoft 365 Defender https://security.microsoft.com/
6. Click on **Settings** > **Email & collaboration** > **User reported settings**.
7. Scroll to **Microsoft Teams**.
8. Check **Monitor reported messages in Microsoft Teams** and **Save**.
9. Set **Send reported messages to:** to **My reporting mailbox only** with reports configured to be sent to authorized staff.

49.5. More information

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/submissions-teams?view=o365-worldwide

49.6. Data

Valid	AllowSecurityEndUserReporting	ReportJunkToCustomizedAddress	ReportNotJunkToCustomizedAddress	ReportPhishToCustomizedAddress	ReportJunkAddresses	ReportNotJunkAddresses	ReportPhishAddresses	ReportChatMessageEnabled	ReportChatMessageToCustomizedAddressEnabled
False	True								

50. Ensure guest user access is restricted

2024-03-15

50.1. Information

ID	Category	Subcategory	Review
4d179407-ca60-4a37-981f-99584ea2d6ea	Microsoft Fabric Admin Center	Tenant Settings	True

50.2. Description

This setting allows business-to-business (B2B) guests access to Microsoft Fabric, and contents that they have permissions to. With the setting turned off, B2B guest users receive an error when trying to access Power BI.
The recommended state is Enabled for a subset of the organization or Disabled.

50.3. Technical explanation

Establishing and enforcing a dedicated security group prevents unauthorized access to Microsoft Fabric for guests collaborating in Azure that are new or assigned guest status from other applications. This upholds the principle of least privilege and uses role-based access control (RBAC). These security groups can also be used for tasks like conditional access, enhancing risk management and user accountability across the organization.

50.4. Advised solution

1. Navigate to Microsoft Fabric https://app.powerbi.com/admin-portal
2. Select **Tenant settings**.
3. Scroll to **Export and Sharing settings**.
4. Set **Allow Azure Active Directory guest users to access Microsoft Fabric** to one of these states:
   - State 1: **Disabled**
   - State 2: **Enabled with Specific security groups** selected and defined.

50.5. More information

- https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing

50.6. Data

Restricted
False

51. Ensure external user invitations are restricted

2024-03-15

51.1. Information

ID	Category	Subcategory	Review
da8daeae-fc77-4bff-9733-19e8fe73b87b	Microsoft Fabric Admin Center	Tenant Settings	True

51.2. Description

The Invite external users setting helps organizations choose whether new external users can be invited to the organization through Power BI sharing, permissions, and subscription experiences. This setting only controls the ability to invite through Power BI.
The recommended state is Enabled for a subset of the organization or Disabled.

51.3. Technical explanation

Establishing and enforcing a dedicated security group prevents unauthorized access to Microsoft Fabric for guests collaborating in Azure that are new or assigned guest status from other applications. This upholds the principle of least privilege and uses role-based access control (RBAC). These security groups can also be used for tasks like conditional access, enhancing risk management and user accountability across the organization.

51.4. Advised solution

1. Navigate to Microsoft Fabric https://app.powerbi.com/admin-portal
2. Select **Tenant settings**.
3. Scroll to **Export and Sharing settings**.
4. Set **Invite external users to your organization** to one of these states:
   - State 1: **Disabled**
   - State 2: **Enabled with Specific security groups** selected and defined.

51.5. More information

- https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing
- https://learn.microsoft.com/en-us/power-bi/enterprise/service-admin-azure-ad-b2b#invite-guest-users

51.6. Data

52. Ensure 'Interact with and share R and Python' visuals is 'Disabled'

2024-03-15

52.1. Information

ID	Category	Subcategory	Review
134ffbee-2092-42a7-9309-7b9b04c14b4b	Microsoft Fabric Admin Center	Tenant Settings	True

52.2. Description

Power BI allows the integration of R and Python scripts directly into visuals. This feature allows data visualizations by incorporating custom calculations, statistical analyses, machine learning models, and more using R or Python scripts. Custom visuals can be created by embedding them directly into Power BI reports. Users can then interact with these visuals and see the results of the custom code within the Power BI interface.

52.3. Technical explanation

Disabling this feature can reduce the attack surface by preventing potential malicious code execution leading to data breaches, or unauthorized access. The potential for sensitive or confidential data being leaked to unintended users is also increased with the use of scripts.

52.4. Advised solution

1. Navigate to Microsoft Fabric https://app.powerbi.com/admin-portal
2. Select **Tenant settings**.
3. Scroll to **R and Python visuals settings**.
4. 4.Set **Interact with and share R and Python visuals** to **Disabled**

52.5. More information

- https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-r-python-visuals
- https://learn.microsoft.com/en-us/power-bi/visuals/service-r-visuals
- https://www.r-project.org/

52.6. Data

Disabled
False

53. Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'

2024-03-15

53.1. Information

ID	Category	Subcategory	Review
6aa91139-4667-4d38-887b-a22905da5bcc	Microsoft Fabric Admin Center	Tenant Settings	True

53.2. Description

Information protection tenant settings help to protect sensitive information in the Power BI tenant. Allowing and applying sensitivity labels to content ensures that information is only seen and accessed by the appropriate users.
The recommended state is Enabled or Enabled for a subset of the organization.

53.3. Technical explanation

Establishing data classifications and affixing labels to data at creation enables organizations to discern the data's criticality, sensitivity, and value. This initial identification enables the implementation of appropriate protective measures, utilizing technologies like Data Loss Prevention (DLP) to avert inadvertent exposure and enforcing access controls to safeguard against unauthorized access.
This practice can also promote user awareness and responsibility in regard to the nature of the data they interact with. Which in turn can foster awareness in other areas of data management across the organization.

53.4. Advised solution

1. Navigate to Microsoft Fabric https://app.powerbi.com/admin-portal
2. Select **Tenant settings**.
3. Scroll to **Information protection**.
4. Set **Allow users to apply sensitivity labels for content** to one of these states:
   - State 1: **Enabled**
   - State 2: **Enabled** with **Specific security groups** selected and defined.

53.5. More information

- https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-enable-data-sensitivity-labels
- https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-dlp-policies-for-power-bi-overview
- https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-enable-data-sensitivity-labels#licensing-and-requirements

53.6. Data

Enabled
False

54. Ensure shareable links are restricted

2024-03-15

54.1. Information

ID	Category	Subcategory	Review
e9ec0d44-00a5-4305-9d15-a225f00a8364	Microsoft Fabric Admin Center	Tenant Settings	True

54.2. Description

Creating a shareable link allows a user to create a link to a report or dashboard, then add that link to an email or another messaging application. There are 3 options that can be selected when creating a shareable link:

- People in your organization
- People with existing access
- Specific people

This setting solely deals with restrictions to People in the organization. External users by default are not included in any of these categories, and therefore cannot use any of these links regardless of the state of this setting.
The recommended state is Enabled for a subset of the organization or Disabled.

54.3. Technical explanation

While external users are unable to utilize shareable links, disabling or restricting this feature ensures that a user cannot generate a link accessible by individuals within the same organization who lack the necessary clearance to the shared data. For example, a member of Human Resources intends to share sensitive information with a particular employee or another colleague within their department. The owner would be prompted to specify either People with existing access or Specific people when generating the link requiring the person clicking the link to pass a first layer access control list. This measure along with proper file and folder permissions can help prevent unintended access and potential information leakage.

54.4. Advised solution

1. Navigate to Microsoft Fabric https://app.powerbi.com/admin-portal
2. Select **Tenant settings**.
3. Scroll to **Export and Sharing settings**.
4. Set **Allow shareable links to grant access to everyone in your organization** to one of these states:
    1. State 1: **Disabled**
    2. State 2: **Enabled** with **Specific security groups** selected and defined.

54.5. More information

- https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-share-dashboards?wt.mc_id=powerbi_inproduct_sharedialog#link-settings
- https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing

54.6. Data

55. Ensure enabling of external data sharing is restricted

2024-03-15

55.1. Information

ID	Category	Subcategory	Review
832a0d52-55b7-4a27-a6c7-a90e04bdaa7a	Microsoft Fabric Admin Center	Tenant Settings	True

55.2. Description

Power BI admins can specify which users or user groups can share datasets externally with guests from a different tenant through the in-place mechanism. Disabling this setting prevents any user from sharing datasets externally by restricting the ability of users to turn on external sharing for datasets they own or manage.
The recommended state is Enabled for a subset of the organization or Disabled.

55.3. Technical explanation

Establishing and enforcing a dedicated security group prevents unauthorized access to Microsoft Fabric for guests collaborating in Azure that are new or from other applications. This upholds the principle of least privilege and uses role-based access control (RBAC). These security groups can also be used for tasks like conditional access, enhancing risk management and user accountability across the organization.

55.4. Advised solution

1. Navigate to Microsoft Fabric https://app.powerbi.com/admin-portal
2. Select **Tenant settings**.
3. Scroll to **Export and Sharing settings**.
4. Set **Allow specific users to turn on external data sharing** to one of these states:
    1. State 1: **Disabled**
    2. State 2: **Enabled** with **Specific security groups** selected and defined.

55.5. More information

- https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing

55.6. Data

Restricted
False

56. Ensure 'Block ResourceKey Authentication' is 'Enabled'

2024-03-15

56.1. Information

ID	Category	Subcategory	Review
bbcbdabf-221c-412e-92d5-67367053ff27	Microsoft Fabric Admin Center	Tenant Settings	True

56.2. Description

This setting blocks the use of resource key based authentication. The Block ResourceKey Authentication setting applies to streaming and PUSH datasets. If blocked users will not be allowed send data to streaming and PUSH datasets using the API with a resource key.
The recommended state is Enabled.

56.3. Technical explanation

Resource keys are a form of authentication that allows users to access Power BI resources (such as reports, dashboards, and datasets) without requiring individual user accounts. While convenient, this method bypasses the organization's centralized identity and access management controls. Enabling ensures that access to Power BI resources is tied to the organization's authentication mechanisms, providing a more secure and controlled environment.

56.4. Advised solution

1. Navigate to Microsoft Fabric https://app.powerbi.com/admin-portal
2. Select **Tenant settings**.
3. Scroll to **Developer settings**.
4. Set **Block ResourceKey Authentication** to **Enabled**.

56.5. More information

- https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-developer
- https://learn.microsoft.com/en-us/power-bi/connect-data/service-real-time-streaming

56.6. Data

Blocked
False