WhiteRook Cyber

Microsoft 365 Assessment

Sample Client

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 sampleclient.com.au. 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 **36** (100 is maximum).

Issues Discovered

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 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices
Microsoft 365 Admin Center	Settings	6. Ensure 'External sharing' of calendars is not available
Microsoft 365 Admin Center	Settings	7. Ensure that Sways cannot be shared with people outside of your organization
Microsoft 365 Defender	Email and collaboration	8. Ensure notifications for internal users sending malware is Enabled
Microsoft 365 Defender	Email and collaboration	9. Ensure Exchange Online Spam Policies are set to notify administrators
Microsoft 365 Defender	Email and collaboration	10. Ensure that an anti-phishing policy has been created
Microsoft 365 Defender	Email and collaboration	11. Ensure that DKIM is enabled for all Exchange Online Domains
Microsoft 365 Defender	Email and collaboration	12. Ensure DMARC Records for all Exchange Online domains are published
Microsoft 365 Defender	Email and collaboration	13. Ensure the spoofed domains report is reviewed weekly
Microsoft Purview	Data Loss Prevention	14. Ensure DLP policies are enabled
Microsoft Purview	Data Loss Prevention	15. Ensure DLP policies are enabled for Microsoft Teams
Microsoft Purview	Information Protection	16. Ensure SharePoint Online Information Protection policies are set up and used
Microsoft Entra Admin Center	Identity	17. Ensure Security Defaults is disabled on Azure Active Directory
Microsoft Entra Admin Center	Identity	18. Ensure third-party integrated applications are not allowed
Microsoft Entra Admin Center	Identity	19. Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'
Microsoft Entra Admin Center	Identity	20. Ensure 'Restrict access to the Azure AD administration portal' is set to 'Yes'
Microsoft Entra Admin Center	Identity	21. Ensure the option to remain signed in is hidden

Category	Subcategory	Title
Microsoft Entra Admin Center	Identity	22. Ensure 'LinkedIn account connections' is disabled
Microsoft Entra Admin Center	Identity	23. Ensure a dynamic group for guest users is created
Microsoft Entra Admin Center	Identity	24. Ensure the Application Usage report is reviewed at least weekly
Microsoft Entra Admin Center	Identity	25. Ensure user consent to apps accessing company data on their behalf is not allowed
Microsoft Entra Admin Center	Identity	26. Ensure the admin consent workflow is enabled
Microsoft Entra Admin Center	Protection	27. Ensure Microsoft Authenticator is configured to protect against MFA fatigue
Microsoft Entra Admin Center	Protection	28. Ensure custom banned passwords lists are used
Microsoft Entra Admin Center	Protection	29. Ensure 'Self service password reset enabled' is set to 'All'
Microsoft Exchange Admin Center	Audit	30. Ensure mailbox auditing for users is Enabled
Microsoft Exchange Admin Center	Mail Flow	31. Ensure all forms of mail forwarding are blocked and/or disabled
Microsoft Exchange Admin Center	Mail Flow	32. Ensure mail transport rules do not whitelist specific domains
Microsoft Exchange Admin Center	Mail Flow	33. Ensure email from external senders is identified
Microsoft Exchange Admin Center	Roles	34. Ensure users installing Outlook add-ins is not allowed
Microsoft Exchange Admin Center	Reports	35. Ensure mail forwarding rules are reviewed at least weekly
Microsoft Exchange Admin Center	Settings	36. Ensure MailTips are enabled for end users
Microsoft Exchange Admin Center	Settings	37. Ensure additional storage providers are restricted in Outlook on the web
Microsoft SharePoint Admin Center	Policies	38. Ensure modern authentication for SharePoint applications is required
Microsoft SharePoint Admin Center	Policies	39. Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled
Microsoft SharePoint Admin Center	Policies	40. Ensure external content sharing is restricted
Microsoft SharePoint Admin Center	Policies	41. Ensure OneDrive content sharing is restricted
Microsoft SharePoint Admin Center	Policies	42. Ensure SharePoint external sharing is managed through domain whitelist/blacklists
Microsoft SharePoint Admin Center	Policies	43. Ensure external sharing is restricted by security group
Microsoft SharePoint Admin Center	Policies	44. Ensure guest access to a site or OneDrive will expire automatically

Category	Subcategory	Title
Microsoft SharePoint Admin Center	Policies	45. Ensure reauthentication with verification code is restricted
Microsoft SharePoint Admin Center	Settings	46. Ensure Office 365 SharePoint infected files are disallowed for download
Microsoft Teams Admin Center	Teams	47. Ensure external file sharing in Teams is enabled for only approved cloud storage services
Microsoft Teams Admin Center	Teams	48. Ensure users can't send emails to a channel email address
Microsoft Teams Admin Center	Users	49. Ensure 'external access' is restricted in the Teams admin center
Microsoft Teams Admin Center	Meetings	50. Ensure anonymous users can't join a meeting
Microsoft Teams Admin Center	Meetings	51. Ensure only people in my org can bypass the lobby
Microsoft Teams Admin Center	Meetings	52. Ensure meeting chat does not allow anonymous users
Microsoft Teams Admin Center	Meetings	53. Ensure only organizers and co-organizers can present
Microsoft Teams Admin Center	Meetings	54. Ensure external participants can't give or request control

1. Ensure Administrative accounts are separate and cloud-only

2024-11-30

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
023d2786-44ea-422b-aef6-e5bdabc8b32a	alex@samplecclient.com.au	Alex Sample	True	Global Administrator	Microsoft 365 Business Premium, Microsoft Fabric (Free), Microsoft Power Automate Free	True
2603bc99-3de9-4901-a7d0-583481d9544e	Mary@sampleclient.com.au	Mary Smith	True	Global Administrator	Office 365 E3, Microsoft Power Automate Free	True
5495eddc-0731-40d7-ad39-d8052da298be	John@sampleclient.com.au	John Bollard	True	Global Administrator	Microsoft Power Automate Free, Microsoft Fabric (Free), Microsoft 365 Business Premium	

2. Ensure Guest Users are reviewed

2024-11-30

2.7. Information

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

2.8. 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.

2.9. Technical explanation

Periodic review of guest users ensures proper access to resources.

2.10. 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.

2.11. More information

N/A

2.12. Data

Id	UserPrincipalName	GivenName	Surname	DisplayName	Roles	CreatedDateTime	LastSignIn	AccountEnabled
8a59989a-4d75-47f8-8097-51460edcc423	raspberrymango877_gmail.com#EXT#@samplecomau.onmicrosoft.com			raspberrymango877@gmail.com		15/11/2024 2:11:05 AM		True
0ac65668-3983-477c-8411-67a761104fc7	roba_tkc.wa.edu.au#EXT#@samplecomau.onmicrosoft.com			roba@tkc.wa.edu.au		15/11/2024 2:11:12 AM		True

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

2024-11-30

3.13. Information

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

3.14. 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".

3.15. 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.

3.16. 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**.

3.17. 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

3.18. Data

Id	DisplayName	Visibility	SecurityEnabled	Mail	CreatedDateTime
6601503e-d958-4cf2-8dfc-a5dcd774a1be	All Company	Public	False	AllCompany.13703077888.ypmtyvum@sampleclient.com.au	12/05/2020 5:34:33 AM
d9d7a935-bb23-497d-a21c-e23b948d5f45	Sample Team	Public	False	SampleIT@sampleclient.com.au	23/03/2020 11:43:39 PM

4. Ensure sign-in to shared mailboxes is blocked

2024-11-30

4.19. Information

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

4.20. 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.

4.21. 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.

4.22. 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.

4.23. 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

4.24. Data

Id	UserPrincipalName	GivenName	Surname	DisplayName	CreatedDateTime	LastSignIn	AccountEnabled	PrimarySmtpAddress	CloudOnly
580294d7-54cf-4e8a-939e-4bb3d9f81c78	accounts@sampleclient.com.au	Sample	Accounts	Accounts Sample	13/11/2019 1:38:09 PM	18/07/2023 12:10:30 PM	True	accounts@sampleclient.com.au	True
fa176e5b-1ec2-475f-ad66-e8b82f00fcb7	edwin@sampleclient.com.au	Edwin	Edwardo	Edwin Edwardo	1/12/2022 11:40:30 AM	22/11/2024 3:35:47 AM	True	edwin@sampleclient.com.au	True

5. Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices

2024-11-30

5.25. Information

ID	Category	Subcategory	Review
645b1886-5437-43e5-8b8a-84c033173ff3	Microsoft 365 Admin Center	Settings	True

5.26. Description

Idle session timeout allows the configuration of a setting which will timeout inactive users after a pre-determined amount of time. When a user reaches the set idle timeout session, they'll get a notification that they're about to be signed out. They have to select to stay signed in or they'll be automatically signed out of all Microsoft 365 web apps. Combined with a Conditional Access rule this will only impact unmanaged devices. A managed device is considered a device managed by Intune MDM.

The following Microsoft 365 web apps are supported.

- Outlook Web App
- OneDrive for Business
- SharePoint Online (SPO)
- Office.com and other start pages
- Office (Word, Excel, PowerPoint) on the web
- Microsoft 365 Admin Center

NOTE: Idle session timeout doesn't affect Microsoft 365 desktop and mobile apps.

The recommended setting is 3 hours (or less) for unmanaged devices.

5.27. Technical explanation

Ending idle sessions through an automatic process can help protect sensitive company data and will add another layer of security for end users who work on unmanaged devices that can potentially be accessed by the public. Unauthorized individuals onsite or remotely can take advantage of systems left unattended over time. Automatic timing out of sessions makes this more difficult.

5.28. Advised solution

To configure Idle session timeout:

1. Navigate to the Microsoft 365 admin center https://admin.microsoft.com/.
2. Click to expand **Settings** Select Org settings.
3. Click **Security & Privacy** tab.
4. Select **Idle session timeout**.
5. Check the box **Turn on to set the period of inactivity for users to be signed off of Microsoft 365 web apps**
6. Set a maximum value of **3 hours**.
7. Click **save**.

Ensure the Conditional Access policy is in place:

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/
2. Expand **Azure Active Directory** > **Protect & secure** > **Conditional Access**
3. Click New policy and give the policy a name.
4. Select **Users** > **All users**.
5. Select **Cloud apps or actions** > Select **apps** and select Office 365
6. Select **Conditions** > Client apps > Yes check only **Browser** unchecking all other boxes.
7. Select **Sessions** and check **Use app enforced**

5.29. More information

- https://learn.microsoft.com/en-us/microsoft-365/admin/manage/idle-session-timeout-web-apps?view=o365-worldwide

5.30. Data

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

2024-11-30

6.31. Information

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

6.32. Description

IExternal 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.

6.33. 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.

6.34. 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**.

6.35. More information

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

6.36. Data

Name	Domains	Enabled	Default
Default Sharing Policy	Anonymous:CalendarSharingFreeBusyReviewer|*:CalendarSharingFreeBusySimple	True	True

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

2024-11-30

7.37. Information

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

7.38. 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.

7.39. Technical explanation

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

7.40. 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.

7.41. More information

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

7.42. Data

Enabled
True

8. Ensure notifications for internal users sending malware is Enabled

2024-11-30

8.43. Information

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

8.44. 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.

8.45. 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.

8.46. 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**.

8.47. More information

N/A

8.48. Data

Guid	Id	Name	Valid	EnableInternalSenderAdminNotifications	InternalSenderAdminAddress
54f8e5bd-2ecc-4d71-bb33-3b94c2085d2f	Default	Default	False	False	

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

2024-11-30

9.49. Information

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

9.50. 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.

9.51. 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.

9.52. 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**.

9.53. More information

N/A

9.54. Data

Guid	Id	Name	Valid	BccSuspiciousOutboundMail	NotifyOutboundSpam	NotifyOutboundSpamRecipients	Enabled
060b0923-2e3b-471d-8362-edb79d125bf2	Accounts Allow Fwd	Accounts Allow Fwd	False	False	False		False
43b8790d-c599-401f-84fb-b30124cf12eb	Default	Default	False	False	False		False

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

2024-11-30

10.55. Information

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

10.56. 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.

10.57. Technical explanation

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

10.58. 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**.

10.59. More information

N/A

10.60. Data

Guid	Id	Name	Valid	Enabled	PhishThresholdLevel	EnableMailboxIntelligenceProtection	EnableMailboxIntelligence	EnableSpoofIntelligence
3f4caf54-de4f-4955-87f3-d28e60ec7799	Office365 AntiPhish Default	Office365 AntiPhish Default	False	True	1	False	True	True

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

2024-11-30

11.61. Information

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

11.62. 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.

11.63. 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.

11.64. 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**.

11.65. More information

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

11.66. Data

Domain	Valid	IsDefault	IsVerified	AuthenticationType	DkimEnabled	DkimRecord1	DkimRecord2
Sample.com.au	False	False	True	Managed	False		
sampleclient.com.au	True	True	True	Managed	True	selector1-Sampleit-com-au._domainkey.samplecomau.onmicrosoft.com.	selector2-Sampleit-com-au._domainkey.samplecomau.onmicrosoft.com.
samplecomau.onmicrosoft.com	False	False	True	Managed	False		
Samplewa.com.au	False	False	True	Managed	False		

12. Ensure DMARC Records for all Exchange Online domains are published

2024-11-30

12.67. Information

ID	Category	Subcategory	Review
7f46d070-097f-4a6b-aad1-118b5b707f41	Microsoft 365 Defender	Email and collaboration	True

12.68. Description

DMARC, or Domain-based Message Authentication, Reporting, and Conformance, assists recipient mail systems in determining the appropriate action to take when messages from a domain fail to meet SPF or DKIM authentication criteria.

12.69. Technical explanation

DMARC strengthens the trustworthiness of messages sent from an organization's domain to destination email systems. By integrating DMARC with SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail), organizations can significantly enhance their defenses against email spoofing and phishing attempts.

12.70. Advised solution

1. For each Exchange Online Accepted Domain, add the following record to DNS:

```
Record: _dmarc.contoso.com
Type: TXT Value: v=DMARC1; p=none;
```

2. This will create a basic DMARC policy that audits compliance.

12.71. More information

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

12.72. Data

Domain	Valid	IsDefault	IsVerified	AuthenticationType	Record
Sample.com.au	False	False	True	Managed	
sampleclient.com.au	True	True	True	Managed	v=DMARC1; p=none; pct=100; rua=mailto:Mary@sampleclient.com.au; ruf=mailto:Mary@sampleclient.com.au; fo=1
Samplewa.com.au	True	False	True	Managed	v=DMARC1; p=none
Sampledigital.com.au	True	False	True	Managed	v=DMARC1; p=none

13. Ensure the spoofed domains report is reviewed weekly

2024-11-30

13.73. Information

ID	Category	Subcategory	Review
c7d90aa7-bcb3-403c-96f4-bc828e6246ff	Microsoft 365 Defender	Email and collaboration	True

13.74. Description

Use spoof intelligence in the Security Center on the Anti-spam settings page to review all senders who are spoofing either domains that are part of the organization, or spoofing external domains. Spoof intelligence is available as part of Office 365 Enterprise E5 or separately as part of Defender for Office 365 and as of October 2018 Exchange Online Protection (EOP).

13.75. Technical explanation

Bad actors spoof domains to trick users into conducting actions they normally would not or should not via phishing emails. Running this report will inform the message administrators of current activities, and the phishing techniques used by bad actors. This information can be used to inform end users and plan against future campaigns.

13.76. Advised solution

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Under Email & collaboration click on **Policies & rules** then select **Threat policies**.
3. Under Rules click on **Tenant Allow / Block Lists** then select **Spoofed senders**.
4. Review.

13.77. More information

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-spoof-intelligence?view=o365-worldwide
- https://learn.microsoft.com/en-us/powershell/module/exchange/get-spoofintelligenceinsight?view=exchange-ps

13.78. Data

SpoofedUser	SendingInfrastructure	MessageCount	LastSeen	SpoofType	Action
test.com.au	samplenet.com.au	93	27/11/2024 11:30:17 AM	External	Allow
domain2.com.au	ains.net.au	27	26/11/2024 4:06:21 PM	External	Block

14. Ensure DLP policies are enabled

2024-11-30

14.79. Information

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

14.80. 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.

14.81. 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.

14.82. Advised solution

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

14.83. More information

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

14.84. Data

15. Ensure DLP policies are enabled for Microsoft Teams

2024-11-30

15.85. Information

ID	Category	Subcategory	Review
48d970b5-a31b-41e9-9d66-eb8e02e0546d	Microsoft Purview	Data Loss Prevention	True

15.86. Description

The default Teams Data Loss Prevention (DLP) policy rule in Microsoft 365 is a preconfigured rule that is automatically applied to all Teams conversations and channels. The default rule helps prevent accidental sharing of sensitive information by detecting and blocking certain types of content that are deemed sensitive or inappropriate by the organization.
By default, the rule includes sensitive information types, such as credit card numbers and social security numbers, and applies to all users in the organization.

15.87. Technical explanation

Enabling the default Teams DLP policy rule in Microsoft 365 helps protect an organization's sensitive information by preventing accidental sharing or leakage of that information in Teams conversations and channels.

15.88. Advised solution

1. Navigate to Microsoft Purview compliance portal https://compliance.microsoft.com.
2. Under **Solutions** select **Data loss prevention** then **Policies**.
3. Click **Policies** tab.
4. Check **Default policy for Teams** then click **Edit policy**.
5. The edit policy window will appear click **Next**
6. At the **Choose locations to apply the policy** page, turn the status toggle to **On for Teams chat and channel messages** location and then click **Next**.
7. On Customized advanced DLP rules page, ensure the **Default Teams DLP policy rule Status is On** and click **Next**.
8. On the Policy mode page, select the radial for **Turn it on right away** and click **Next**.
9. Review all the settings for the created policy on the Review your policy and create it page, and then click **submit**.
10. Once the policy has been successfully submitted click **Done**.

15.89. More information

- https://learn.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps
- https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#turn-on-basic-authentication-in-winrm
- https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps

15.90. Data

16. Ensure SharePoint Online Information Protection policies are set up and used

2024-11-30

16.91. Information

ID	Category	Subcategory	Review
b01a1187-5921-4b29-95fd-73e1af3c5285	Microsoft Purview	Information Protection	True

16.92. Description

SharePoint Online Data Classification Policies enables organizations to classify and label content in SharePoint Online based on its sensitivity and business impact. This setting helps organizations to manage and protect sensitive data by automatically applying labels to content, which can then be used to apply policy-based protection and governance controls.

16.93. Technical explanation

By categorizing and applying policy-based protection, SharePoint Online Data Classification Policies can help reduce the risk of data loss or exposure and enable more effective incident response if a breach does occur.

16.94. Advised solution

1. Navigate to Microsoft Purview compliance portal https://compliance.microsoft.com.
2. Under **Solutions** select **Information protection**.
3. Click on the **Label policies** tab.
4. Click **Create a label** to create a label.
5. Select the label and click on the **Publish label**.
6. Fill out the forms to create the policy.

16.95. More information

- https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-overview?view=o365-worldwide#top-sensitivity-labels-applied-to-content

16.96. Data

17. Ensure Security Defaults is disabled on Azure Active Directory

2024-11-30

17.97. Information

ID	Category	Subcategory	Review
bf8c7733-8ec0-4c86-9c4e-28bf4812a57a	Microsoft Entra Admin Center	Identity	True

17.98. Description

Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect the organization. Security defaults contain preconfigured security settings for common attacks.
By default, Microsoft enables security defaults. The goal is to ensure that all organizations have a basic level of security enabled. The security default setting is manipulated in the Azure Portal.
The use of security defaults, however, will prohibit custom settings which are being set with more advanced settings from this benchmark.

17.99. Technical explanation

Security defaults provide secure default settings that are managed on behalf of organizations to keep customers safe until they are ready to manage their own identity security settings. For example, doing the following:

- Requiring all users and admins to register for MFA.
- Challenging users with MFA - mostly when they show up on a new device or app, but more often for critical roles and tasks.
- Disabling authentication from legacy authentication clients, which can't do MFA.

17.100. Advised solution

1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com.
2. Click to expand **Identity** select **Overview**
3. Click **Properties**.
4. Click **Manage security defaults**.
5. Set the **Security defaults** dropdown to **Disabled**.
6. Select **Save**.

17.101. More information

- https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
- https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414

17.102. Data

Enabled
True

18. Ensure third-party integrated applications are not allowed

2024-11-30

18.103. Information

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

18.104. Description

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

18.105. 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.

18.106. 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**.

18.107. More information

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

18.108. Data

AllowedToCreateApps
True

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

2024-11-30

19.109. Information

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

19.110. 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.

19.111. 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.

19.112. 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**.

19.113. More information

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

19.114. Data

AllowedToCreateTenants
True

20. Ensure 'Restrict access to the Azure AD administration portal' is set to 'Yes'

2024-11-30

20.115. Information

ID	Category	Subcategory	Review
591c821b-52ca-48f3-806e-56a98d25c041	Microsoft Entra Admin Center	Identity	True

20.116. Description

Restrict non-privileged users from signing into the Azure Active Directory portal.

20.117. Technical explanation

The Azure AD administrative (AAD) portal contains sensitive data and permission settings, which are still enforced based on the user's role. However, an end user may inadvertently change properties or account settings that could result in increased administrative overhead. Additionally, a compromised end user account could be used by a malicious attacker as a means to gather additional information and escalate an attack.

20.118. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/
2. Click to expand **Identity** > **Users** > **User settings**.
3. Set **Restrict access to Microsoft Entra ID administration portal** to **Yes** then **Save**.

20.119. More information

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

20.120. Data

RestrictNonAdminUsers
False

21. Ensure the option to remain signed in is hidden

2024-11-30

21.121. Information

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

21.122. 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.

21.123. 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.

21.124. 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**.

21.125. More information

N/A

21.126. Data

HideKeepMeSignedIn
False

22. Ensure 'LinkedIn account connections' is disabled

2024-11-30

22.127. Information

ID	Category	Subcategory	Review
23d22457-f5e2-4f55-9aba-e483e8cbb11d	Microsoft Entra Admin Center	Identity	True

22.128. Description

LinkedIn account connections allow users to connect their Microsoft work or school account with LinkedIn. After a user connects their accounts, information and highlights from LinkedIn are available in some Microsoft apps and services.

22.129. Technical explanation

Disabling LinkedIn integration prevents potential phishing attacks and risk scenarios where an external party could accidentally disclose sensitive information.

22.130. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Identity** > **Users** select **User settings**.
3. Under **LinkedIn account connections** select **No**.
4. Click **Save**.

22.131. More information

- https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/linkedin-integration
- https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/linkedin-user-consent

22.132. Data

BlockLinkedInConnection
False

23. Ensure a dynamic group for guest users is created

2024-11-30

23.133. Information

ID	Category	Subcategory	Review
a15e2ff5-2a03-495d-a4f2-4935742395d5	Microsoft Entra Admin Center	Identity	True

23.134. Description

A dynamic group is a dynamic configuration of security group membership for Azure Active Directory. Administrators can set rules to populate groups that are created in Azure AD based on user attributes (such as userType, department, or country/region). Members can be automatically added to or removed from a security group based on their attributes.

23.135. Technical explanation

Dynamic groups allow for an automated method to assign group membership. Guest user accounts will be automatically added to this group and through this existing conditional access rules, access controls and other security measures will ensure that new guest accounts are restricted in the same manner as existing guest accounts.

23.136. Advised solution

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand **Identity** > **Groups** select **All groups**.
3. Select **New group** and assign the following values:
   - **Group type:** Security
   - **Azure AD Roles can be assigned:** No
   - **Membership type:** Dynamic User
4. Select **Add dynamic query**.
5. Above the Rule syntax text box, select **Edit**.
6. Place the following expression in the box:
   (user.userType -eq "Guest")
7. Select **OK** and **Save**

23.137. More information

- https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule
- https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership
- https://learn.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups

23.138. Data

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

2024-11-30

24.139. Information

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

24.140. 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.

24.141. 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.

24.142. 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.

24.143. More information

N/A

24.144. Data

Id	AppDisplayName	FailedSignInCount	SuccessfulSignInCount	SuccessPercentage
38aa3b87-a06d-4817-b275-7a316988d93b	Windows Sign In	90	196	68.53
cbc6b050-0dc7-45dd-a203-75fdd4314121	TacticalRMM	6	66	91.67
54746c02-fd4f-4d74-97b3-b18ad2f1ecc3	SystemAdmins.M365Assessment.PnPPowerShell	5	13	72.22
cb1056e2-e479-49de-ae31-7812af012ed8	Microsoft Azure Active Directory Connect	4	0	0
d3590ed6-52b3-4102-aeff-aad2292ab01c	Microsoft Office	3	0	0
1b730954-1685-4b74-9bfd-dac224a7b894	Azure Active Directory PowerShell	3	0	0
4765445b-32c6-49b0-83e6-1d93765276ca	OfficeHome	2	64	96.97
29d9ed98-a469-4536-ade2-f981bc1d605e	Microsoft Authentication Broker	2	4	66.67
1950a258-227b-4e31-a9cf-717495945fc2	Microsoft Azure PowerShell	1	18	94.74
04b07795-8ddb-461a-bbee-02f9e1bf7b46	Microsoft Azure CLI	1	0	0
4345a7b9-9a63-4910-a426-35363201d503	O365 Suite UX	1	0	0
14d82eec-204b-4c2f-b7e8-296a70dab67e	Microsoft Graph Command Line Tools	1	26	96.3
c44b4083-3bb0-49c1-b47d-974e53cbdf3c	Azure Portal	1	20	95.24
9ea1ad79-fdb6-4f9a-8bc3-2b70f96e34c7	Bing	1	13	92.86
4683bdb1-c807-4e5c-8c51-624fa1a5b420	Guardz	0	13	100
2793995e-0a7d-40d7-bd35-6968ba142197	My Apps	0	1	100
fb78d390-0c51-40cd-8e17-fdbfab77341b	Microsoft Exchange REST API Based Powershell	0	9	100
1dee7b72-b80d-4e56-933d-8b6b04f9a3e2	RemoteAssistanceService	0	1	100
12128f48-ec9e-42f0-b203-ea49fb6af367	MS Teams Powershell Cmdlets	0	14	100
10fa57ef-4895-4ab2-872c-8c3613d4f7fb	Cascade Authentication	0	4	100
08e18876-6177-487e-b8b5-cf950c1e598c	SharePoint Online Web Client Extensibility	0	15	100

08362ab3-4561-4fb4-a85a-69615042b327	Cisco Business Dashboard	0	1	100
00000006-0000-0ff1-ce00-000000000000	Microsoft Office 365 Portal	0	9	100
243c63a3-247d-41c5-9d83-7788c43f1c43	Office Online Core SSO	0	22	100
481504a4-a89a-4be0-ad19-626bf2b2b8a9	GhostWriter	0	6	100
5e3ce6c0-2b1f-4285-8d4b-75ee78787346	Microsoft Teams Web Client	0	26	100
499bf591-13ab-41f2-849e-ae9226f55b87	Pax8 Website	0	1	100
fabfbdc4-5751-471c-ac43-3826fa1afc31	Microsoft Partner Center	0	2	100
ee272b19-4411-433f-8f28-5c13cb6fd407	Microsoft 365 Support Service	0	23	100
d7b530a4-7680-4c23-a8bf-c52c121d2e87	Microsoft Edge Enterprise New Tab Page	0	1	100
d46ecdff-bc8c-4d98-a863-7b496bbb4321	AFI backup	0	3	100
d414ee2d-73e5-4e5b-bb16-03ef55fea597	Azure Static Web Apps	0	4	100
c9a559d2-7aab-4f13-a6ed-e7e9c52aec87	Microsoft Forms	0	4	100
c8c384c1-2c29-44db-966a-4a7f15dab965	DuoPortalSSO	0	6	100
b803a633-fdb1-43c6-ae85-a208a0bdbb23	HaloAzureSSO	0	2	100
b48906b1-451f-46f6-953c-244e0330bdd4	bitwarden-sso	0	2	100
afa5a19a-a047-457f-8321-6df35d11f56a	Leader Cloud Single Sign On	0	3	100
a81d90ac-aa75-4cf8-b14c-58bf348528fe	Microsoft Community v2	0	21	100
a146732d-16eb-4525-8650-4f3b3b0e1f66	Teamviewer SSO	0	9	100
89bee1f7-5e6e-4d8a-9f3d-ecd601259da7	Office365 Shell WCSS-Client	0	363	100
7eadcef8-456d-4611-9480-4fff72b8b9e2	Microsoft Account Controls V2	0	57	100
69f6c859-3456-44a0-9dab-a79aa1b22ad3	Xen Orchestra	0	10	100
6204c1d1-4712-4c46-a7d9-3ed63d992682	Microsoft Flow Portal	0	1	100
00000003-0000-0ff1-ce00-000000000000	Office 365 SharePoint Online	0	16	100

497effe9-df71-4043-a8bb-14cf78c4b63b	Exchange Admin Center	0	11	100
00000002-0000-0ff1-ce00-000000000000	Office 365 Exchange Online	0	37	100

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

2024-11-30

25.145. Information

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

25.146. 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.

25.147. 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.

25.148. 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.

25.149. More information

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

25.150. Data

UserConsentSetting
AllowUserConsentForApps

26. Ensure the admin consent workflow is enabled

2024-11-30

26.151. Information

ID	Category	Subcategory	Review
7bd57849-e98c-48c0-bd98-5c337fb7bc32	Microsoft Entra Admin Center	Identity	True

26.152. Description

The admin consent workflow gives admins a secure way to grant access to applications that require admin approval. When a user tries to access an application but is unable to provide consent, they can send a request for admin approval. The request is sent via email to admins who have been designated as reviewers. A reviewer takes action on the request, and the user is notified of the action.

26.153. Technical explanation

The admin consent workflow (Preview) gives admins a secure way to grant access to applications that require admin approval. When a user tries to access an application but is unable to provide consent, they can send a request for admin approval. The request is sent via email to admins who have been designated as reviewers. A reviewer acts on the request, and the user is notified of the action.

26.154. 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**.
4. Under **Manage** select **Admin consent settings**.
5. Set **Users can request admin consent to apps they are unable to consent to** to **Yes** under **Admin consent requests**.
6. Under the **Reviewers** choose the **Roles and Groups** that will review user generated app consent requests.
7. Set **Selected users will receive email notifications for requests** to **Yes**
8. Select **Save** at the top of the window.

26.155. More information

- https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

26.156. Data

Enabled
False

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

2024-11-30

27.157. Information

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

27.158. 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

27.159. 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.

27.160. 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**

27.161. 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

27.162. Data

id	state	displayApp	displayLocation
MicrosoftAuthenticator	disabled	default	default

28. Ensure custom banned passwords lists are used

2024-11-30

28.163. Information

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

28.164. 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

28.165. 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.

28.166. 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**

28.167. 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

28.168. Data

Enabled
False

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

2024-11-30

29.169. Information

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

29.170. 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.

29.171. 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.

29.172. 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**

29.173. More information

N/A

29.174. Data

EnablementType
None

30. Ensure mailbox auditing for users is Enabled

2024-11-30

30.175. Information

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

30.176. 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.

30.177. 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

30.178. 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;

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

30.179. More information

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

30.180. Data

Name	Alias	UserPrincipalName	PrimarySmtpAddress	AuditEnabled
DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}	DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}	DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@samplecomau.onmicrosoft.com	DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@samplecomau.onmicrosoft.com	False
ESCO Ipads_113aa8710b	ESCOIpads	ESCOIpads@sampleclient.com.au	ESCOIpads@sampleclient.com.au	False
Porting Calendar	porting	porting@sampleclient.com.au	porting@sampleclient.com.au	False
SL Test Bookings_97cfbe7af2	SLTestBookings	SLTestBookings@sampleclient.com.au	SLTestBookings@sampleclient.com.au	False
Test Booking Page_7ab4687b35	TestBookingPage	TestBookingPage@sampleclient.com.au	TestBookingPage@sampleclient.com.au	False
Training Room	Training	Training@sampleclient.com.au	Training@sampleclient.com.au	False
WA Conference	WAConference	WAConference@sampleclient.com.au	WAConference@sampleclient.com.au	False

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

2024-11-30

31.181. Information

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

31.182. 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.

31.183. 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.

31.184. 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.

31.185. 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

31.186. Data

TransportRules	OutboundSpamFilterPolicies
	Accounts Allow Fwd

32. Ensure mail transport rules do not whitelist specific domains

2024-11-30

32.187. Information

ID	Category	Subcategory	Review
8bf19b9f-7c76-4cb6-8d9a-2a327db4d7d3	Microsoft Exchange Admin Center	Mail Flow	True

32.188. Description

Mail flow rules (transport rules) in Exchange Online are used to identify and take action on messages that flow through the organization.

32.189. Technical explanation

Whitelisting domains in transport rules bypasses regular malware and phishing scanning, which can enable an attacker to launch attacks against your users from a safe haven domain.

32.190. Advised solution

1. Navigate to Exchange admin center https://admin.exchange.microsoft.com..
2. Click to expand **Mail Flow** and then select **Rules**.
3. Review the rules and verify that none of them whitelist any specific domains.

32.191. 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

32.192. Data

Name	Priority	State	Identity	SenderDomainIs	SetSCL
Email Security Domains Blocklist (id: 9e4b37-e402649e-e5e9-0)	0	Enabled	Email Security Domains Blocklist (id: 9e4b37-e402649e-e5e9-0)	toplead.info	
Support@ disable SPAM filter	7	Enabled	Support@ disable SPAM filter		-1

33. Ensure email from external senders is identified

2024-11-30

33.193. Information

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

33.194. 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

33.195. 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.

33.196. Advised solution

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

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

33.197. 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

33.198. Data

Identity	Enabled	AllowList
4687e1a9-56f1-4821-927f-4d6dc2da1e9d	False	

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

2024-11-30

34.199. Information

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

34.200. 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.

34.201. 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.

34.202. 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**.

34.203. 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

34.204. Data

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

35. Ensure mail forwarding rules are reviewed at least weekly

2024-11-30

35.205. Information

ID	Category	Subcategory	Review
b2798cfb-c5cc-41d4-9309-d1bd932a4a91	Microsoft Exchange Admin Center	Reports	True

35.206. Description

The Exchange Online environment can be configured in a way that allows for automatic forwarding of e-mail. This can be done using Transport Rules in the Admin Center, Auto Forwarding per mailbox, and client-based rules in Outlook. Administrators and users both are given several methods to automatically and quickly send e-mails outside of your organization.

35.207. Technical explanation

Reviewing mail forwarding rules will provide the Messaging Administrator with insight into possible attempts to exfiltrate data from the organization. Weekly review helps create a recognition of baseline, legitimate activity of users. This will aid in helping identify the more malicious activity of bad actors when/if they choose to use this side-channel.

35.208. Advised solution

1. Navigate to Exchange admin center https://admin.exchange.microsoft.com.
2. Expand **Reports** then select **Mail flow**.
3. Click on **Auto forwarded messages report**.
4. Review.

35.209. 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

35.210. Data

Id	Primary SmtpAddress	Alias	RuleIdentity	RuleName	RuleEnabled	ForwardTo	RedirectTo	ForwardAsAttachmentTo
Mary	Mary@sampleclient.com.au	Mary	Mary\156770724107863982 09	Slack	True			"Alex Sample" [EX:/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=734d46ba8af34d0a982d77707a5436a5-alex] "Accounts Sample" [EX:/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0e168bd362a54ebcb489026f0268afa4-accounts]

36. Ensure MailTips are enabled for end users

2024-11-30

36.211. Information

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

36.212. 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).

36.213. 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.

36.214. 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
```

36.215. 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

36.216. Data

Valid	MailTipsAllTipsEnabled	MailTipsExternalRecipientsTipsEnabled	MailTipsGroupMetricsEnabled	MailTipsLargeAudienceThreshold
False	True	False	True	25

37. Ensure additional storage providers are restricted in Outlook on the web

2024-11-30

37.217. Information

ID	Category	Subcategory	Review
d576ebed-fe29-44a7-9fdf-bb8b3c484894	Microsoft Exchange Admin Center	Settings	True

37.218. Description

This setting allows users to open certain external files while working in Outlook on the web. If allowed, keep in mind that Microsoft doesn't control the use terms or privacy policies of those third-party services.
Ensure **AdditionalStorageProvidersAvailable** are restricted.

37.219. Technical explanation

By default additional storage providers are allowed in Office on the Web (such as Box, Dropbox, Facebook, Google Drive, OneDrive Personal, etc.). This could lead to information leakage and additional risk of infection from organizational non-trusted storage providers. Restricting this will inherently reduce risk as it will narrow opportunities for infection and data leakage.

37.220. Advised solution

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

```
Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -
AdditionalStorageProvidersAvailable $false
```

37.221. More information

- https://learn.microsoft.com/en-us/powershell/module/exchange/set-owamailboxpolicy?view=exchange-ps
- https://support.microsoft.com/en-us/topic/3rd-party-cloud-storage-services-supported-by-office-apps-fce12782-eccc-4cf5-8f4b-d1ebec513f72

37.222. Data

Name	AdditionalStorageProvidersAvailable
OwaMailboxPolicy-Default	True

38. Ensure modern authentication for SharePoint applications is required

2024-11-30

38.223. Information

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

38.224. 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.

38.225. 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.

38.226. 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**.

38.227. More information

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

38.228. Data

LegacyAuthProtocolsEnabled
True

39. Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled

2024-11-30

39.229. Information

ID	Category	Subcategory	Review
68e99561-878a-4bcd-bce1-d69a6c0e2282	Microsoft SharePoint Admin Center	Policies	True

39.230. Description

Azure AD B2B provides authentication and management of guests. Authentication happens via one-time passcode when they don't already have a work or school account or a Microsoft account. Integration with SharePoint and OneDrive allows for more granular control of how guest user accounts are managed in the organization's AAD, unifying a similar guest experience already deployed in other Microsoft 365 services such as Teams.

39.231. Technical explanation

External users assigned guest accounts will be subject to Azure AD access policies, such as multi-factor authentication. This provides a way to manage guest identities and control access to SharePoint and OneDrive resources. Without this integration, files can be shared without account registration, making it more challenging to audit and manage who has access to the organization's data.

39.232. Advised solution

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

```
Set-SPOTenant -EnableAzureADB2BIntegration $true
```

39.233. More information

- https://learn.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration#enabling-the-integration
- https://learn.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b
- https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps

39.234. Data

EnableAzureADB2BIntegration
False

40. Ensure external content sharing is restricted

2024-11-30

40.235. Information

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

40.236. 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.

40.237. 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.

40.238. 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.

40.239. More information

N/A

40.240. Data

SharingCapability
ExternalUserAndGuestSharing

41. Ensure OneDrive content sharing is restricted

2024-11-30

41.241. Information

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

41.242. 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.

41.243. 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.

41.244. 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**.

41.245. More information

N/A

41.246. Data

SharingCapability
ExternalUserAndGuestSharing

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

2024-11-30

42.247. Information

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

42.248. Description

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

42.249. 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.

42.250. 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.

42.251. More information

N/A

42.252. Data

SharingDomainRestrictionMode
None

43. Ensure external sharing is restricted by security group

2024-11-30

43.253. Information

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

43.254. 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.

43.255. 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.

43.256. 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.

43.257. More information

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

43.258. Data

GuestSharingGroupAllowListInTenant	GuestSharingGroupAllowListInTenantByPrincipalIdentity

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

2024-11-30

44.259. Information

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

44.260. 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.

44.261. 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.

44.262. 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**

44.263. 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

44.264. Data

ExternalUserExpireInDays
90

45. Ensure reauthentication with verification code is restricted

2024-11-30

45.265. Information

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

45.266. 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.

45.267. 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.

45.268. 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.

45.269. 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

45.270. Data

EmailAttestationEnabled	EmailAttestationReAuthDays
False	30

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

2024-11-30

46.271. Information

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

46.272. Description

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

46.273. 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.

46.274. Advised solution

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

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

46.275. 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

46.276. Data

DisallowInfectedFileDownload
False

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

2024-11-30

47.277. Information

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

47.278. 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.

47.279. Technical explanation

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

47.280. 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**.

47.281. More information

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

47.282. Data

Dropbox	Box	GoogleDrive	ShareFile	Egnyte
True	True	True	True	True

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

2024-11-30

48.283. Information

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

48.284. Description

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

48.285. 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.

48.286. 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**.

48.287. More information

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

48.288. Data

AllowEmailIntoChannel
True

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

2024-11-30

49.289. Information

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

49.290. 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.

49.291. 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.

49.292. 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**.

49.293. 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

49.294. Data

AllowTeamsConsumer	AllowPublicUsers	AllowFederatedUsers	AllowedDomains
True	True	True	AllowAllKnownDomains

50. Ensure anonymous users can't join a meeting

2024-11-30

50.295. Information

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

50.296. 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.

50.297. 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.

50.298. 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**.

50.299. More information

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

50.300. Data

AllowAnonymousUsersToJoinMeeting
True

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

2024-11-30

51.301. Information

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

51.302. 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.

51.303. 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.

51.304. 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**.

51.305. 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

51.306. Data

AutoAdmittedUsers
EveryoneInCompany

52. Ensure meeting chat does not allow anonymous users

2024-11-30

52.307. Information

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

52.308. Description

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

52.309. 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.

52.310. 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**.

52.311. More information

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

52.312. Data

MeetingChatEnabledType
Enabled

53. Ensure only organizers and co-organizers can present

2024-11-30

53.313. Information

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

53.314. Description

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

53.315. 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.

53.316. 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**.

53.317. 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

53.318. Data

DesignatedPresenterRoleMode
EveryoneUserOverride

54. Ensure external participants can't give or request control

2024-11-30

54.319. Information

ID	Category	Subcategory	Review
89773e80-9004-4d41-bf8b-80d4dcbb141b	Microsoft Teams Admin Center	Meetings	True

54.320. Description

This policy setting allows control of who can present in meetings and who can request control of the presentation while a meeting is underway.

54.321. Technical explanation

Ensuring that only authorized individuals and not external participants are able to present and request control reduces the risk that a malicious user can inadvertently show content that is not appropriate.
External participants are categorized as follows: external users, guests, and anonymous users.

54.322. 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 **External participants can give or request control** to **Off**.

54.323. More information

- https://learn.microsoft.com/en-us/microsoftteams/meeting-who-present-request-control
- https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

54.324. Data

AllowExternalParticipantGiveRequestControl
True