Security Findings Report

August 05, 2026

Prepared for
accuknox-tech

Prepared by
AccuKnox
support@accuknox.com

Security Findings Report

Table of Contents

Benchmarks

CIS Microsoft 365 Foundations Benchmark v6.0.1

RULE ID	RULE NAME	STATUS
ms365-cis-1.1.1	Ensure Administrative accounts are cloud-only	PASS
ms365-cis-1.1.2	Ensure two emergency access accounts have been defined	MANUAL
ms365-cis-1.1.3	Ensure there are between 2 and 4 Global Administrators	PASS
ms365-cis-1.1.4	Ensure administrative accounts use reduced-footprint licenses	FAIL
ms365-cis-1.2.1	Ensure that only organizationally approved public groups exist	FAIL
ms365-cis-1.2.2	Ensure sign-in to shared mailboxes is blocked	PASS
ms365-cis-1.3.1	Ensure the 'Password expiration policy' is set to 'Set passwords to never expire'	PASS
ms365-cis-1.3.2	Ensure idle session timeout for unmanaged devices is set to 3 hours or less	FAIL
ms365-cis-1.3.3	Ensure 'External sharing' of calendars is not available	FAIL
ms365-cis-1.3.4	Ensure user owned apps and services are restricted	FAIL
ms365-cis-1.3.5	Ensure internal phishing protection for Forms is enabled	PASS
ms365-cis-1.3.6	Ensure the customer lockbox feature is enabled	FAIL
ms365-cis-1.3.7	Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web'	FAIL
ms365-cis-1.3.8	Ensure Sways cannot be shared with people outside of your organization	MANUAL
ms365-cis-1.3.9	Ensure shared bookings pages are restricted to select users	FAIL
ms365-cis-2.1.1	Ensure Safe Links for Office Applications is Enabled	FAIL
ms365-cis-2.1.2	Ensure the Common Attachment Types Filter is enabled	PASS
ms365-cis-2.1.3	Ensure notifications for internal users sending malware is Enabled	FAIL
ms365-cis-2.1.4	Ensure Safe Attachments policy is enabled	PASS
ms365-cis-2.1.5	Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled	PASS

Security Findings Report

ms365-cis-2.1.6	Ensure Exchange Online Spam Policies are set to notify administrators	FAIL
ms365-cis-2.1.7	Ensure that an anti-phishing policy has been created	FAIL
ms365-cis-2.1.8	Ensure that SPF records are published for all Exchange Domains	FAIL
ms365-cis-2.1.9	Ensure that DKIM is enabled for all Exchange Online Domains	PASS
ms365-cis-2.1.10	Ensure DMARC Records for all Exchange Online Domains are Published	FAIL
ms365-cis-2.1.11	Ensure comprehensive attachment filtering is applied	FAIL
ms365-cis-2.1.12	Ensure the connection filter IP allow list is not used	PASS
ms365-cis-2.1.13	Ensure the connection filter safe list is off	PASS
ms365-cis-2.1.14	Ensure inbound anti-spam policies do not contain allowed domains	PASS
ms365-cis-2.1.15	Ensure outbound anti-spam message limits are in place	FAIL
ms365-cis-2.2.1	Ensure that activity monitoring of emergency access accounts is configured	MANUAL
ms365-cis-2.4.1	Ensure Priority account protection is enabled and configured	SKIPPED
ms365-cis-2.4.2	Ensure Priority accounts have 'Strict protection' presets applied	SKIPPED
ms365-cis-2.4.3	Ensure Microsoft Defender for Cloud Apps is enabled	MANUAL
ms365-cis-2.4.4	Ensure Zero-hour auto purge for Microsoft Teams is on	PASS
ms365-cis-3.1.1	Ensure Microsoft 365 audit log search is Enabled	PASS
ms365-cis-3.2.1	Ensure DLP policies are enabled	FAIL
ms365-cis-3.2.2	Ensure DLP policies are enabled for Microsoft Teams	FAIL
ms365-cis-3.3.1	Ensure sensitivity label policies are published	FAIL
ms365-cis-4.1	Ensure that devices without a compliance policy are marked as not compliant	FAIL
ms365-cis-4.2	Ensure that personal device enrollment is blocked in Microsoft Intune	FAIL
ms365-cis-5.1.2.1	Ensure 'Per-user MFA' is disabled	PASS
ms365-cis-5.1.2.2	Ensure third party integrated applications are not allowed	FAIL
ms365-cis-5.1.2.3	Ensure non-admin users cannot create tenants	FAIL
ms365-cis-5.1.2.4	Ensure access to the Entra administration portal is restricted	MANUAL

ms365-cis-5.1.2.5	Ensure the option to remain signed in is hidden	MANUAL
ms365-cis-5.1.2.6	Ensure LinkedIn account connections are disabled	MANUAL
ms365-cis-5.1.3.1	Ensure a dynamic group for guest users is created	FAIL
ms365-cis-5.1.3.2	Ensure users can not create security groups	FAIL
ms365-cis-5.1.4.1	Ensure the ability to join devices is restricted	FAIL
ms365-cis-5.1.4.2	Ensure the maximum number of devices per user is limited	PASS
ms365-cis-5.1.4.3	Ensure Global Administrator is not added as a local administrator during Entra join	FAIL
ms365-cis-5.1.4.4	Ensure local administrator assignment is limited during Entra join	FAIL
ms365-cis-5.1.4.5	Ensure Local Admin Password Solution (LAPS) is enabled	FAIL
ms365-cis-5.1.4.6	Ensure users are restricted from recovering BitLocker keys	FAIL
ms365-cis-5.1.5.1	Ensure user consent to apps accessing company data on their behalf is not allowed	FAIL
ms365-cis-5.1.5.2	Ensure the admin consent workflow is enabled	FAIL
ms365-cis-5.1.6.1	Ensure that collaboration invitations are sent to allowed domains only	FAIL
ms365-cis-5.1.6.2	Ensure guest user access is restricted	PASS
ms365-cis-5.1.6.3	Ensure guest invitations are limited to the Guest Inviter role	FAIL
ms365-cis-5.1.8.1	Ensure password hash synchronization is enabled for hybrid environments	MANUAL
ms365-cis-5.2.2.1	Ensure multifactor authentication is enabled for all users in administrative roles	FAIL
ms365-cis-5.2.2.2	Ensure multifactor authentication is enabled for all users	FAIL
ms365-cis-5.2.2.3	Ensure legacy authentication is blocked via Conditional Access	FAIL
ms365-cis-5.2.2.4	Ensure sign-in frequency and persistent browser session for admins is configured	FAIL
ms365-cis-5.2.2.5	Ensure phishing-resistant MFA is required for admins	FAIL
ms365-cis-5.2.2.6	Ensure Identity Protection user risk policies are configured	FAIL
ms365-cis-5.2.2.7	Ensure Identity Protection sign-in risk policies are configured	FAIL
ms365-cis-5.2.2.8	Ensure sign-in risk is blocked for medium and high risk	FAIL

ms365-cis-5.2.2.9	Ensure a managed device is required for authentication	FAIL
ms365-cis-5.2.2.10	Ensure managed device is required to register security info	FAIL
ms365-cis-5.2.2.11	Ensure sign-in frequency for Intune Enrollment is set to every time	FAIL
ms365-cis-5.2.2.12	Ensure the device code sign-in flow is blocked	FAIL
ms365-cis-5.2.3.1	Ensure Microsoft Authenticator MFA fatigue protections are enabled	FAIL
ms365-cis-5.2.3.2	Ensure custom banned passwords lists are used	FAIL
ms365-cis-5.2.3.3	Ensure password protection is enabled for on-prem Active Directory	FAIL
ms365-cis-5.2.3.4	Ensure all member users are MFA capable	PASS
ms365-cis-5.2.3.5	Ensure weak authentication methods are disabled	PASS
ms365-cis-5.2.3.6	Ensure system-preferred MFA is enabled	FAIL
ms365-cis-5.2.3.7	Ensure email-based OTP is disabled	FAIL
ms365-cis-5.2.4.1	Ensure 'Self service password reset enabled' is set to 'All'	MANUAL
ms365-cis-5.3.1	Ensure Privileged Identity Management is used to manage roles	FAIL
ms365-cis-5.3.2	Ensure access reviews for guest users are configured	FAIL
ms365-cis-5.3.3	Ensure access reviews for privileged roles are configured	FAIL
ms365-cis-5.3.4	Ensure approval is required for Privileged Role Administrator activation	SKIPPED
ms365-cis-5.3.5	Ensure approval is required for Privileged Role Administrator activation	SKIPPED
ms365-cis-6.1.1	Ensure 'AuditDisabled' organizationally is set to 'False'	PASS
ms365-cis-6.1.2	Ensure mailbox audit actions are configured	PASS
ms365-cis-6.1.3	Ensure 'AuditBypassEnabled' is not enabled on mailboxes	PASS
ms365-cis-6.2.1	Ensure all forms of mail forwarding are blocked and/or disabled	FAIL
ms365-cis-6.2.2	Ensure mail transport rules do not whitelist specific domains	PASS
ms365-cis-6.2.3	Ensure email from external senders is identified	FAIL
ms365-cis-6.3.1	Ensure users installing Outlook add-ins is not allowed	FAIL
ms365-cis-6.5.1	Ensure modern authentication for Exchange Online is enabled	PASS

Security Findings Report

ms365-cis-6.5.2	Ensure MailTips are enabled for end users	FAIL
ms365-cis-6.5.3	Ensure additional storage providers are restricted in Outlook on the web	FAIL
ms365-cis-6.5.4	Ensure SMTP AUTH is disabled	PASS
ms365-cis-6.5.5	Ensure Direct Send submissions are rejected	FAIL
ms365-cis-7.2.1	Ensure modern authentication for SharePoint applications is required	FAIL
ms365-cis-7.2.2	Ensure SharePoint and OneDrive integration with Microsoft Entra B2B is enabled	SKIPPED
ms365-cis-7.2.3	Ensure external content sharing is restricted	FAIL
ms365-cis-7.2.4	Ensure OneDrive content sharing is restricted	FAIL
ms365-cis-7.2.5	Ensure that SharePoint external users cannot share items they don't own	FAIL
ms365-cis-7.2.6	Ensure SharePoint external sharing is restricted	FAIL
ms365-cis-7.2.7	Ensure the default sharing link type is not set to 'Anyone with the link'	SKIPPED
ms365-cis-7.2.8	Ensure external sharing is restricted by security group	MANUAL
ms365-cis-7.2.9	Ensure guest access to SharePoint and OneDrive expires automatically	SKIPPED
ms365-cis-7.2.10	Ensure guest access to SharePoint and OneDrive expires automatically	SKIPPED
ms365-cis-7.2.11	Ensure the default sharing link permission is set to View	SKIPPED
ms365-cis-7.3.1	Ensure SharePoint infected files are prevented from being downloaded	SKIPPED
ms365-cis-7.3.2	Ensure OneDrive sync is restricted for unmanaged devices	FAIL
ms365-cis-8.1.1	Ensure external file sharing in Teams is enabled for only approved cloud storage services	FAIL
ms365-cis-8.1.2	Ensure users can't send emails to a channel email address	FAIL
ms365-cis-8.2.1	Ensure external domains are restricted in the Teams admin center	FAIL
ms365-cis-8.2.2	Ensure communication with unmanaged Teams users is disabled	FAIL
ms365-cis-8.2.3	Ensure external Teams users cannot initiate conversations	FAIL
ms365-cis-8.2.4	Ensure the organization cannot communicate with accounts in trial Teams tenants	PASS
ms365-cis-8.4.1	Ensure Teams app permission policies are configured	MANUAL

ms365-cis-8.5.1	Ensure anonymous users can't join a meeting	FAIL
ms365-cis-8.5.2	Ensure anonymous users and dial-in callers can't start a meeting	PASS
ms365-cis-8.5.3	Ensure only people in my org can bypass the lobby	FAIL
ms365-cis-8.5.4	Ensure users dialing in can't bypass the lobby	PASS
ms365-cis-8.5.5	Ensure meeting chat does not allow anonymous users	FAIL
ms365-cis-8.5.6	Ensure only organizers and co-organizers can present	FAIL
ms365-cis-8.5.7	Ensure external participants can't give or request control	PASS
ms365-cis-8.5.8	Ensure external meeting chat is off	FAIL
ms365-cis-8.5.9	Ensure meeting recording is off by default	FAIL
ms365-cis-8.6.1	Ensure users can report security concerns in Teams	FAIL
ms365-cis-9.1.1	Ensure guest user access is restricted	FAIL
ms365-cis-9.1.2	Ensure external user invitations are restricted	FAIL
ms365-cis-9.1.3	Ensure guest access to content is restricted	PASS
ms365-cis-9.1.4	Ensure 'Publish to web' is restricted	SKIPPED
ms365-cis-9.1.5	Ensure 'Interact with and share R and Python' visuals is 'Disabled'	FAIL
ms365-cis-9.1.6	Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'	FAIL
ms365-cis-9.1.7	Ensure shareable links are restricted	FAIL
ms365-cis-9.1.8	Ensure enabling of external data sharing is restricted	FAIL
ms365-cis-9.1.9	Ensure 'Block ResourceKey Authentication' is 'Enabled'	FAIL
ms365-cis-9.1.10	Ensure access to APIs by service principals is restricted	FAIL
ms365-cis-9.1.11	Ensure service principals cannot create and use profiles	PASS
ms365-cis-9.1.12	Ensure service principals ability to create workspaces, connections and deployment pipelines is restricted	PASS

Compliance Details

ms365-cis-1.1.1 Ensure Administrative accounts are cloud-only

[PASS]

Vulnerability Name	All administrative accounts are cloud-only (checked 2 privileged role members).
Section	1.1 Users
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	N/A
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings. In a hybrid environment, administrative accounts should not have On-premises sync enabled, keeping them separate from on-premises accounts to prevent lateral movement between cloud and on-prem.

Privileged Member Count:

- 2

Description

Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings. In a hybrid environment, administrative accounts should not have On-premises sync enabled, keeping them separate from on-premises accounts to prevent lateral movement between cloud and on-prem.

Details

Rationale: In a hybrid environment, having separate accounts will help ensure that in the event of a breach in the cloud, the breach does not affect the on-prem environment and vice versa.

Impact: Administrative users will need to utilize login/logout functionality to switch accounts when performing administrative tasks, losing SSO benefit. A migration process from the 'daily driver' account to a dedicated admin account is required.

Audit Procedure:

Using Microsoft Graph:

Get all directory roles and identify privileged roles (roles with 'Administrator' in the name or 'Global Reader').

Get members of those roles.

For each member, check if OnPremisesSyncEnabled is True.

Any user with OnPremisesSyncEnabled = True in a privileged role is non-compliant.

Remediation:

Identify privileged accounts that are synced from on-premises.

Create a new cloud-only admin account for each.

Migrate M365 and Azure RBAC roles to the new cloud-only account.

Reduce the hybrid account to a non-privileged user or remove it.

Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users

---

- **ms365-cis-1.1.2 Ensure two emergency access accounts have been defined**

  [MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure two emergency access accounts have been defined

Security Findings Report

Section	1.1 Users
Severity	High
Profiles	E3 Level 1, E5 Level 1
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Emergency access ('break glass') accounts are limited for emergency scenarios where normal administrative accounts are unavailable. They must not be assigned to a specific user, must use .onmicrosoft.com domain, be cloud-only, unlicensed, and assigned the Global Administrator role. At least one must be excluded from all Conditional Access policies.

Description

Emergency access ('break glass') accounts are limited for emergency scenarios where normal administrative accounts are unavailable. They must not be assigned to a specific user, must use .onmicrosoft.com domain, be cloud-only, unlicensed, and assigned the Global Administrator role. At least one must be excluded from all Conditional Access policies.

Details

Rationale: In the event of losing access to administrative functions, an organisation may experience significant loss in its ability to provide support, lose insight into its security posture, and potentially suffer financial losses.

Impact: Failure to implement emergency access accounts can weaken security posture. Microsoft recommends FIDO2 security keys or certificate-based authentication for MFA compliance (required from 10/15/2024).

Audit Procedure:

Step 1 – Verify organisational policy:

• Confirm a documented policy authorises emergency access accounts.
• FIDO2 keys should be locked in a secure fireproof location.
• Passwords ≥ 16 characters, randomly generated.

Step 2 – Verify two accounts exist (Microsoft 365 admin center):
• Navigate to https://admin.microsoft.com → Users > Active Users.
• Confirm two designated emergency access accounts with:
  • Names that do NOT identify a specific person.
  • Default .onmicrosoft.com domain.
  • Cloud-only (no on-premises sync).
  • Unlicensed.
  • Global Administrator role assigned.

Step 3 – Conditional Access exclusion:
• In Entra admin center → Protection > Conditional Access.
• Confirm at least one emergency account is excluded from ALL CA rules.

Remediation:

Create two cloud-only, unlicensed accounts using the .onmicrosoft.com domain with names that do not identify a specific person.

Assign the Global Administrator role to each.

Configure FIDO2 passkey or certificate-based MFA.

Exclude at least one account from all Conditional Access policies.

Store credentials securely (fireproof vault, split across trustees).

Document and test break-glass procedures quarterly.

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

---

- **ms365-cis-1.1.3 Ensure there are between 2 and 4 Global Administrators**

  [PASS]

Security Findings Report

Vulnerability Name	Global Administrator count is 2, which is within the compliant range of 2–4.
Section	1.1 Users
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	N/A
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The number of Global Administrators should be between 2 and 4. Having fewer than 2 creates a single point of failure; having more than 4 unnecessarily expands the attack surface for the most privileged role in the tenant.

Memberids:

- 4421062b-5c25-4d1d-914e-7e343d55816d
- 11550c26-c64a-425e-987a-cda288cf1990

Globaladmincount:

- 2

Description

The number of Global Administrators should be between 2 and 4. Having fewer than 2 creates a single point of failure; having more than 4 unnecessarily expands the attack surface for the most privileged role in the tenant.

Details

Rationale: Designating at least 2 Global Administrators ensures that administrative tasks can still be performed if one account is unavailable. Limiting to no more than 4 reduces the blast radius should a Global Administrator account be compromised.

Impact: If the current number of Global Administrators is outside the 2–4 range, accounts must be added or removed. Removing Global Admin from existing users may impact their ability to perform tasks.

Audit Procedure:

Using Microsoft Graph:

GET /directoryRoles and find the role with displayName = 'Global Administrator'.

GET /directoryRoles/{id}/members

Count the members. Compliant if count is between 2 and 4 (inclusive).

Remediation:

Microsoft 365 admin center → Users > Active Users.

Assign or remove the Global Administrator role until there are between 2 and 4 Global Administrators.

Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles

---

- **ms365-cis-1.1.4 Ensure administrative accounts use reduced-footprint licenses**
  [FAIL]

Vulnerability Name	1 privileged account(s) have assigned licenses. Verify that none are full E3/E5 productivity suites.
Section	1.1 Users
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	N/A
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Administrative accounts should use reduced-footprint licenses such as Microsoft Entra ID P1 or P2 only. Full productivity suite licenses (E3/E5) include email, Office apps, and Teams which increase the attack surface of high-privileged accounts.

Id:

- 4421062b-5c25-4d1d-914e-7e343d55816d

Skuids:

- 2bc9d149-a1dc-4d8f-bcd8-e9c5750a59b5
- b49494c3-64d5-42da-9e32-ca44cb37f259
- 6fd2c87f-b296-42f0-b197-1e91e994b900
- 5821f2cb-338b-484d-bbe9-488efefad568
- a403ebcc-fae0-4ca2-8c8c-7a907fd6c235
- 3dd6cf57-d688-4eed-ba52-9e40b5468c3e
- 05e9a617-0261-4cee-bb44-138d3ef5d965

Userprincipalname:

- ayushaggarwal1136@ayushaggarwal1136gmail.onmicrosoft.com

Assignedlicensecount:

- 7

Description

Administrative accounts should use reduced-footprint licenses such as Microsoft Entra ID P1 or P2 only. Full productivity suite licenses (E3/E5) include email, Office apps, and Teams which increase the attack surface of high-privileged accounts.

Details

Rationale: Dedicated admin accounts that only have identity/governance licenses cannot receive phishing emails (no mailbox), cannot be used to open malicious attachments (no Office apps), and generally have a smaller attack surface than accounts with full E3/E5 licenses.

Impact: Administrative accounts will not have Exchange mailboxes, Office apps, or Teams. Admins will need a separate day-to-day account for productivity tasks.

Audit Procedure:

Using Microsoft Graph:

- Get all privileged role members.
- For each privileged user, check assignedLicenses.
- The account is non-compliant if any assigned SKU part number is in the high-footprint set (E3, E5, Business Premium, etc.).

Compliant accounts should have no licenses OR only Entra ID P1/P2.

Remediation:

- Create dedicated cloud-only admin accounts without productivity licenses.
- Assign only Microsoft Entra ID P1 or P2 licenses to admin accounts.
- Remove full E3/E5 licenses from dedicated admin accounts.

Reference: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices#4-use-dedicated-admin-accounts

---

- **ms365-cis-1.2.1 Ensure that only organizationally approved public groups exist** **[FAIL]**

Vulnerability Name	2 public Microsoft 365 Group(s) found. Verify each is organisationally approved.
Section	1.2 Groups
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Groups can be created as Public by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft 365 Groups with 'Public' visibility allow any tenant user to join and access group content (email, files, calendar) without owner approval. Groups should use 'Private' visibility unless there is a specific business justification for public access.

Id:

- 1e2703f0-3dd2-44a8-b5b0-811382a472d5

Visibility:

- Public

Displayname:

- All Company

Id:

- e9ee2463-da4d-4654-a93c-5be2838ab6b7

Visibility:

- Public

Displayname:

- Default Directory

Description

Microsoft 365 Groups with 'Public' visibility allow any tenant user to join and access group content (email, files, calendar) without owner approval. Groups should use 'Private' visibility unless there is a specific business justification for public access.

Details

Rationale: Public groups expose sensitive business information to all employees by default. Restricting groups to 'Private' ensures that only approved members can access group content.

Impact: Changing existing public groups to private will prevent non-members from joining without owner approval and may disrupt users who relied on self-service join functionality.

Audit Procedure:

Using Microsoft Graph:

GET /groups?$filter=groupTypes/any(c:c eq 'Unified')&$select=id,displayName,visibility&$top=999

Check visibility field for each group.

Any group with visibility = 'Public' is potentially non-compliant (unless organisationally approved).

Remediation:

For each public group that lacks business justification:

Microsoft 365 admin center → Groups > Active groups.

Select the group → Settings → Privacy → change to Private.

Or via PowerShell:

Set-UnifiedGroup -Identity <group> -AccessType Private

Reference: https://learn.microsoft.com/en-us/microsoft-365/solutions/groups-teams-access-governance

---

● ms365-cis-1.2.2 Ensure sign-in to shared mailboxes is blocked

[PASS]

Vulnerability Name	No unlicensed member accounts with sign-in enabled found. Shared mailbox accounts appear to have sign-in blocked.
Section	1.2 Groups
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Shared mailbox accounts have sign-in enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026

Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Shared mailboxes in Exchange Online have an associated user account. This account should have sign-in blocked (accountEnabled = false) to prevent it from being used as a direct sign-in account, which could bypass MFA and other controls.

Totaluserschecked:

- 2

Description

Shared mailboxes in Exchange Online have an associated user account. This account should have sign-in blocked (accountEnabled = false) to prevent it from being used as a direct sign-in account, which could bypass MFA and other controls.

Details

Rationale: Shared mailbox accounts often have weak or no password protections. Blocking sign-in ensures that only properly authenticated users who are delegates can access the shared mailbox through their own account.

Impact: Blocking sign-in to shared mailboxes prevents direct authentication as the shared mailbox account. Users must access the mailbox via delegation from their own account.

Audit Procedure:

Using Microsoft Graph:

GET /users?$filter=assignedLicenses/$count eq 0 and userType eq 'Member'&$select=id,displayName,userPrincipalName,accountEnabled,mail&$top=999

Also check: GET /users?$select=id,userPrincipalName,accountEnabled,assignedLicenses,onPremisesExtensionAttributes&$top=999

Shared mailboxes typically have no licenses assigned. Compliant: accountEnabled = false for shared mailbox accounts.

Remediation:

For each shared mailbox user with sign-in enabled:

Microsoft 365 admin center → Users > Active users.

Select the shared mailbox user → Block sign-in.

Or via PowerShell:

Get-Mailbox -RecipientTypeDetails SharedMailbox | ForEach-Object { Set-AzureADUser -ObjectId $_.ExternalDirectoryObjectId -AccountEnabled $false }

Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/email/about-shared-mailboxes

---

● ms365-cis-1.3.1 Ensure the 'Password expiration policy' is set to 'Set passwords to never expire'

[PASS]

Vulnerability Name	Password expiration policy is set to 'never expire' for all domains.
Section	1.3 Settings
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Passwords expire after 90 days (legacy default).
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft recommends setting passwords to never expire for cloud-managed accounts. NIST SP 800-63B guidance states that forcing periodic password changes actually reduces security by incentivising predictable patterns. MFA provides a stronger compensating control.

Id:

- ayushaggarwal1136gmail.onmicrosoft.com

Passwordvalidityperiodindays:

- 2147483647

Description

Microsoft recommends setting passwords to never expire for cloud-managed accounts. NIST SP 800-63B guidance states that forcing periodic password changes actually reduces security by incentivising predictable patterns. MFA provides a stronger compensating control.

Details

Rationale: Forcing users to change passwords regularly often results in weak, predictable password patterns (e.g. appending a number to the previous password). Setting passwords to never expire, combined with MFA and breach detection, is the current best practice.

Impact: Users will no longer receive password expiration reminders. Ensure MFA is enforced as a compensating control.

Audit Procedure:

Using Microsoft Graph:

GET /organization

Check: passwordPolicies property should NOT include 'DisablePasswordExpiration' at the user level, OR

GET /domains and check passwordNotificationWindowInDays / passwordValidityPeriodInDays.

Alternatively:

Microsoft 365 admin center → Settings > Org Settings > Security & privacy > Password expiration policy.

Confirm 'Set passwords to never expire (recommended)' is checked.

Remediation:

Navigate to Microsoft 365 admin center → Settings > Org Settings > Security & privacy > Password expiration policy.

Select 'Set passwords to never expire (recommended)' and save.

Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations

---

● ms365-cis-1.3.2 Ensure idle session timeout for unmanaged devices is set to 3 hours or less

[FAIL]

Vulnerability Name	No activity-based timeout policies found. Idle session timeout for unmanaged devices is not configured.
Section	1.3 Settings
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	No idle session timeout configured by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Configuring an idle session timeout for unmanaged devices ensures that browser sessions on shared or unmanaged devices are automatically signed out after a period of inactivity, reducing the risk of unauthorized access.

Description

Configuring an idle session timeout for unmanaged devices ensures that browser sessions on shared or unmanaged devices are automatically signed out after a period of inactivity, reducing the risk of unauthorized access.

Details

Rationale: Unmanaged devices may be used in shared environments (kiosks, shared PCs). Idle session timeouts ensure active sessions are terminated after inactivity, preventing unauthorized access to M365 services.

Impact: Users on unmanaged devices will be signed out after the configured idle period, requiring re-authentication.

Audit Procedure:

Using Microsoft Graph:

GET /policies/activityBasedTimeoutPolicies

Review each policy's definition property for web session timeout.

The timeout should be ≤ PT3H (3 hours) for web sessions.

Remediation:

Microsoft 365 admin center → Security & privacy → Idle session timeout.

Enable idle session timeout and set to 3 hours or less for unmanaged devices.

Or via Microsoft Entra admin center → Identity > Overview > Properties > Manage security defaults or Conditional Access.

Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/misc/idle-session-timeout-web-apps

---

● ms365-cis-1.3.3 Ensure 'External sharing' of calendars is not available

[FAIL]

Vulnerability Name	The Default Sharing Policy is enabled and grants full calendar detail sharing (not just free/busy) to: Anonymous:CalendarSharingFreeBusyReviewer

Security Findings Report

Section	1.3 Settings
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	External calendar sharing may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Sharing calendar details externally can expose sensitive information about employee schedules and business operations. External calendar sharing should be disabled unless there is a specific business need.

Id:

- Default Sharing Policy

Guid:

- a9482da4-b6b9-4393-99b7-7482a7e8cb3d

Name:

- Default Sharing Policy

Default:

- True

Domains:

- Anonymous:CalendarSharingFreeBusyReviewer
- *:CalendarSharingFreeBusySimple

Enabled:

- True

Isvalid:

- True

Identity:

- Default Sharing Policy

Objectclass:

- top
- msExchSharingPolicy

Objectstate:

- Changed

Whenchanged:

- 2026-03-10T04:20:29+00:00

Whencreated:

- 2026-03-09T05:04:48+00:00

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Sharing-Policy

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:29Z

Whencreatedutc:

- 2026-03-09T05:04:48Z

Exchangeversion:

- 0.10 (14.0.100.0)

Exchangeobjectid:

- a9482da4-b6b9-4393-99b7-7482a7e8cb3d

Distinguishedname:

- CN=Default Sharing Policy,CN=Federation,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Description

Sharing calendar details externally can expose sensitive information about employee schedules and business operations. External calendar sharing should be disabled unless there is a specific business need.

Details

Rationale: Calendar data can reveal meeting participants, meeting subjects, and availability patterns that could be leveraged by attackers for social engineering, spear phishing, or physical security attacks.

Impact: Users will not be able to share their full calendar details with external recipients. Free/busy information may still be shared based on configuration.

Audit Procedure:

Exchange admin center → Organization > Sharing.

Check Organization Sharing policies for external sharing with calendar details enabled.

Or via Exchange Online PowerShell:

Get-SharingPolicy | Select Name, Domains, Enabled

Look for policies with CalendarSharing or FreeBusySimple permissions applied to anonymous or external domains.

Remediation:

Exchange admin center → Organization > Sharing.

Edit or remove sharing policies that allow external calendar detail sharing.

PowerShell:

Set-SharingPolicy -Identity 'Default Sharing Policy' -Enabled $false

Or restrict to FreeBusySimple for external domains.

Reference: https://learn.microsoft.com/en-us/exchange/sharing/sharing-policies/sharing-policies

---

- **ms365-cis-1.3.4 Ensure user owned apps and services are restricted**
  [FAIL]

Vulnerability Name	User app restrictions not fully configured: allowedToSignUpEmailBasedSubscriptions = true; defaultUserRolePermissions.allowedToCreateApps = true

Section	1.3 Settings
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Users can sign up for email-based subscriptions and create apps by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Users should not be able to sign up for email-based subscriptions or consent to third-party applications on behalf of the organization. These capabilities should be restricted to administrators.

Allowedtocreateapps:

- True

Allowedtosignupemailbasedsubscriptions:

- True

Description

Users should not be able to sign up for email-based subscriptions or consent to third-party applications on behalf of the organization. These capabilities should be restricted to administrators.

Details

Rationale: Allowing users to sign up for email-based subscriptions or create apps introduces unmanaged SaaS services and potential data exposure. Centralized control ensures only approved applications are used.

Impact: Users will not be able to sign up for free trials of Microsoft services or other email-based subscriptions without admin approval.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy

Check:

• allowedToSignUpEmailBasedSubscriptions should be false

• defaultUserRolePermissions.allowedToCreateApps should be false

Remediation:

Microsoft 365 admin center → Settings > Org settings > Services > User owned apps and services.

Disable 'Let users access the Office Store' and 'Let users start trials on behalf of your organization'.

Or via Microsoft Graph:

PATCH /policies/authorizationPolicy

{ 'allowedToSignUpEmailBasedSubscriptions': false,

'defaultUserRolePermissions': { 'allowedToCreateApps': false } }

Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/misc/self-service-sign-up

---

- **ms365-cis-1.3.5 Ensure internal phishing protection for Forms is enabled**
  [PASS]

Vulnerability Name	Internal phishing protection for Forms is enabled.
Section	1.3 Settings
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Internal phishing protection for Forms is enabled by default.

Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft Forms has a built-in phishing detection capability that blocks forms containing phishing attempts from being shared. This protection should be enabled to prevent Microsoft Forms from being used as a phishing vector.

Isinorgformsphishingscanenabled:

- True

Description

Microsoft Forms has a built-in phishing detection capability that blocks forms containing phishing attempts from being shared. This protection should be enabled to prevent Microsoft Forms from being used as a phishing vector.

Details

Rationale: Attackers can use Microsoft Forms to create credential harvesting pages that appear legitimate due to the Microsoft branding. Internal phishing protection helps detect and block these forms.

Impact: Legitimate forms that happen to match phishing patterns may be incorrectly blocked. Administrators can review and unblock flagged forms.

Audit Procedure:

Microsoft Graph (beta):

GET /admin/forms/settings

Ensure isInOrgFormsPhishingScanEnabled is True.

Microsoft 365 admin center → Settings > Org settings > Forms.

Verify 'Add internal phishing protection' is checked under Phishing protection.

Remediation:

Microsoft 365 admin center → Settings > Org settings > Forms.

Enable the 'Internal phishing protection' option.

Reference: https://support.microsoft.com/en-us/office/phishing-protection-in-microsoft-forms

---

ms365-cis-1.3.6 Ensure the customer lockbox feature is enabled

[FAIL]

Vulnerability Name	Customer Lockbox is not enabled (CustomerLockBoxEnabled=None).
Section	1.3 Settings
Severity	Medium
Profiles	E5 Level 2
Default Value	Customer Lockbox is disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Customer Lockbox provides an additional layer of control by requiring explicit customer approval before Microsoft support engineers can access tenant data to resolve a service request.

Description

Customer Lockbox provides an additional layer of control by requiring explicit customer approval before Microsoft support engineers can access tenant data to resolve a service request.

Details

Rationale: Customer Lockbox ensures that Microsoft access to customer data is auditable and requires customer approval, supporting compliance requirements around data access controls.

Impact: When Microsoft needs to access tenant data to resolve a support case, a Global Administrator must approve the request within 12 hours. If not approved, Microsoft cannot access the data.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-OrganizationConfig | Select-Object CustomerLockBoxEnabled

Verify the value is True.

Microsoft 365 admin center → Settings > Org settings > Security & privacy > Customer Lockbox → verify 'Require approval for all data access requests' is checked.

Remediation:

Microsoft 365 admin center → Settings > Org settings > Security & privacy.

Enable 'Customer Lockbox'.

Requires Microsoft 365 E5 or Microsoft 365 E5 Compliance add-on.

Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests

---

● **ms365-cis-1.3.7 Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web'**

[FAIL]

Security Findings Report

Vulnerability Name	Third-party storage services in Microsoft 365 on the web are not restricted (service principal does not exist).
Section	1.3 Settings
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	Third-party storage may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft 365 web apps (Word, Excel, PowerPoint Online) can connect to third-party storage services. This should be restricted to prevent data from being saved to unapproved cloud storage providers.

Description

Microsoft 365 web apps (Word, Excel, PowerPoint Online) can connect to third-party storage services. This should be restricted to prevent data from being saved to unapproved cloud storage providers.

Details

Rationale: Third-party storage services are not subject to the same governance and compliance controls as OneDrive. Restricting storage options ensures data stays within approved and governed storage systems.

Impact: Users will not be able to open or save files directly to third-party storage services like Dropbox or Box from Office web apps.

Audit Procedure:

Microsoft Graph:

$SP = Get-MgServicePrincipal -Filter "appId eq 'c1f33bc0-bdb4-4248-ba9b-096807ddb43e'"

Passes if the service principal does not exist, or exists with AccountEnabled = False.

Microsoft 365 admin center → Settings > Org settings > Microsoft 365 on the web.

Verify 'Let users open files stored in third-party storage services in Microsoft 365 on the web' is not checked.

Remediation:

Microsoft 365 admin center → Settings > Org settings > Office on the web.

Disable 'Allow users to open files stored in third-party storage services in Office on the web'.

Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/misc/third-party-storage

---

● ms365-cis-1.3.8 Ensure Sways cannot be shared with people outside of your organization

[MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure Sways cannot be shared with people outside of your organization
Section	1.3 Settings
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	Sway external sharing may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026

Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft Sway is a presentation and newsletter tool. External sharing of Sways could expose sensitive business content to unauthorized external parties.

Description

Microsoft Sway is a presentation and newsletter tool. External sharing of Sways could expose sensitive business content to unauthorized external parties.

Details

Rationale: Sway content can include sensitive business information. Restricting sharing to internal users only prevents accidental data exposure through publicly accessible Sway links.

Impact: Users will not be able to share Sway content publicly or with external recipients.

Audit Procedure:

Microsoft 365 admin center → Settings > Org settings > Sway.

Verify that 'Let people in your organization share their sways with people outside your organization' is disabled.

There is no Microsoft Graph API for Sway settings.

Remediation:

Microsoft 365 admin center → Settings > Org settings > Sway.

Disable external sharing for Sway.

Reference: https://support.microsoft.com/en-us/office/administrator-settings-for-microsoft-sway

---

- **ms365-cis-1.3.9 Ensure shared bookings pages are restricted to select users**
  [FAIL]

Vulnerability Name	BookingsMailboxCreationEnabled is True on OwaMailboxPolicy-Default, and Bookings is not disabled at the organization level.
Section	1.3 Settings
Severity	Low
Profiles	E3 Level 1, E5 Level 1
Default Value	BookingsMailboxCreationEnabled is True by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Shared Bookings allows you to invite your team members and create booking pages and let your customers book time with you and your team. The recommended state is to restrict the OwaMailboxPolicy-Default policy or disable Bookings at the organization level.

Bookingsmailboxcreationenabled:

- True

Description

Shared Bookings allows you to invite your team members and create booking pages and let your customers book time with you and your team. The recommended state is to restrict the OwaMailboxPolicy-Default policy or disable Bookings at the organization level.

Details

Rationale: Shared Bookings pages can be exploited by threat actors to impersonate legitimate users using convincing internal email addresses. A compromised low-privilege account could be used to mimic high-profile identities (e.g., the CEO) and bypass impersonation filters to initiate fraudulent actions like fund transfers.

Impact: Users will not be able to create new Bookings calendars/pages unless explicitly permitted, and external customers will not be able to book appointments if Bookings is disabled at the organization level.

Audit Procedure:

Ensure Shared Bookings is turned off in the OWA Default policy. If booking is disabled at the tenant (OrganizationConfig) level this is also a compliant state.

To audit using PowerShell:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default | fl BookingsMailboxCreationEnabled

Ensure BookingsMailboxCreationEnabled is set to False.

Optionally: Get-OrganizationConfig | fl BookingsEnabled — if False, also compliant.

Remediation:

Exchange Online PowerShell:

Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -BookingsMailboxCreationEnabled $false

Or disable Bookings entirely at the organization level:

Set-OrganizationConfig -BookingsEnabled $false

Reference: https://learn.microsoft.com/en-us/microsoft-365/bookings/bookings-faq

---

- **ms365-cis-2.1.1 Ensure Safe Links for Office Applications is Enabled**

  [FAIL]

Vulnerability Name	No Safe Links policy has all required settings enabled. Found 1 policy(ies), none matching the compliant configuration.
Section	2.1 Microsoft Defender for Office 365
Severity	High
Profiles	E5 Level 1
Default Value	Safe Links is not enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Safe Links in Microsoft Defender for Office 365 provides URL scanning and rewriting of email messages and Office documents in real time. It should be enabled for Office applications including Word, Excel, PowerPoint, and Teams.

Id:

- Built-In Protection Policy

Guid:

- d97ceace-2e22-4d1c-a1cb-2fb656d1b0fc

Name:

- Built-In Protection Policy

Isvalid:

- True

Identity:

- Built-In Protection Policy

Scanurls:

- True

Objectclass:

- top
- msExchSmartLinksProtectionConfig

Objectstate:

- Unchanged

Trackclicks:

- True

Whenchanged:

- 2026-07-14T16:15:34+00:00

Whencreated:

- 2026-07-14T16:15:27+00:00

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Smart-Links-Protection-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-07-14T16:15:34Z

Whencreatedutc:

- 2026-07-14T16:15:27Z

Exchangeversion:

- 0.20 (15.0.0.0)

Exchangeobjectid:

- d97ceace-2e22-4d1c-a1cb-2fb656d1b0fc

Allowclickthrough:

- True

Disableurlrewrite:

- True

Distinguishedname:

- CN=Built-In Protection Policy,CN=Safe Links,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Isbuiltinprotection:

- True

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Delivermessageafterscan:

- True

Enablesafelinksforemail:

- True

Enablesafelinksforteams:

- True

Enablesafelinksforoffice:

- True

Description

Safe Links in Microsoft Defender for Office 365 provides URL scanning and rewriting of email messages and Office documents in real time. It should be enabled for Office applications including Word, Excel, PowerPoint, and Teams.

Details

Rationale: Safe Links protects users from clicking malicious URLs that may have changed since email delivery. Real-time scanning and blocking of malicious links significantly reduces the risk of phishing attacks.

Impact: URLs in emails and Office documents will be rewritten and checked before users are allowed to navigate to them. This adds latency to link clicks.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-SafeLinksPolicy | Select-Object Identity, EnableSafeLinksForEmail, EnableSafeLinksForTeams, EnableSafeLinksForOffice, TrackClicks, AllowClickThrough, ScanUrls, EnableForInternalSenders, DeliverMessageAfterScan, DisableUrlRewrite

Verify at least one policy has:

- EnableSafeLinksForEmail = True
- EnableSafeLinksForTeams = True
- EnableSafeLinksForOffice = True
- TrackClicks = True
- AllowClickThrough = False
- ScanUrls = True
- EnableForInternalSenders = True
- DeliverMessageAfterScan = True

• DisableUrlRewrite = False

Remediation:

Microsoft Defender portal (https://security.microsoft.com):

Email & Collaboration > Policies & Rules > Threat policies > Safe Links.

Create or edit a Safe Links policy:

• Enable Safe Links for Email, Teams, and Office apps

• Apply to all recipients

PowerShell:

Set-SafeLinksPolicy -Identity 'Default' -EnableSafeLinksForEmail $true -EnableSafeLinksForTeams $true -EnableSafeLinksForOffice $true -TrackClicks $true -AllowClickThrough $false -ScanUrls $true -EnableForInternalSenders $true -DeliverMessageAfterScan $true -DisableUrlRewrite $false

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-about

---

● ms365-cis-2.1.2 Ensure the Common Attachment Types Filter is enabled

[PASS]

Vulnerability Name	The Common Attachment Types Filter is enabled on: Default.
Section	2.1 Microsoft Defender for Office 365
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Common Attachment Types Filter is disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026

Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The Common Attachment Types Filter in Exchange Online Protection blocks email messages that contain file types commonly used in malware attacks (e.g., .exe, .vbs, .js). This filter should be enabled on anti-malware policies.

Id:

- Default

Guid:

- 16ad84a0-e2cf-4889-b99d-aeb15b65b809

Name:

- Default

Isvalid:

- True

Identity:

- Default

Filetypes:

- ace
- apk
- app
- appx
- ani
- arj
- bat
- cab
- cmd
- com
- deb
- dex
- dll
- docm
- elf
- exe
- hta

- img
- iso
- jar
- jnlp
- kext
- lha
- lib
- library
- lnk
- lzh
- macho
- msc
- msi
- msix
- msp
- mst
- pif
- ppa
- ppam
- reg
- rev
- scf
- scr
- sct
- sys
- uif
- vb
- vbe
- vbs
- vxd
- wsc
- wsf
- wsh
- xll
- xz
- z

Isdefault:

- True

Zapenabled:

- True

Objectclass:

- top
- msExchMalwareFilterConfig

Objectstate:

- Unchanged

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:26+00:00

Quarantinetag:

- AdminOnlyAccessPolicy

Filetypeaction:

- Reject

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Malware-Filter-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:26Z

Exchangeversion:

- 0.20 (15.0.0.0)

Enablefilefilter:

- True

Exchangeobjectid:

- 16ad84a0-e2cf-4889-b99d-aeb15b65b809

Distinguishedname:

- CN=Default,CN=Malware Filter,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Description

The Common Attachment Types Filter in Exchange Online Protection blocks email messages that contain file types commonly used in malware attacks (e.g., .exe, .vbs, .js). This filter should be enabled on anti-malware policies.

Details

Rationale: Common attachment types used in malware distribution include executable files, scripts, and other dangerous file types. Blocking these at the email gateway prevents them from reaching end users.

Impact: Emails with blocked attachment types will be quarantined or rejected. Users who legitimately need to send/receive these file types will need alternative delivery methods.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-MalwareFilterPolicy -Identity Default | Select-Object EnableFileFilter

Verify EnableFileFilter is True.

Remediation:

Microsoft Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Anti-malware.

Edit the default anti-malware policy:

- Enable 'Common attachments filter'

PowerShell:

Set-MalwareFilterPolicy -Identity Default -EnableFileFilter $true

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure

---

- **ms365-cis-2.1.3 Ensure notifications for internal users sending malware is Enabled** **[FAIL]**

Vulnerability Name	No malware filter policy has both EnableInternalSenderAdminNotifications=True and a defined InternalSenderAdminAddress (checked 1 policy(ies)).
Section	2.1 Microsoft Defender for Office 365
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Internal sender admin notifications are disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Anti-malware policies should be configured to notify administrators when internal users send messages containing malware. This provides early warning of compromised internal accounts.

Id:

- Default

Guid:

- 16ad84a0-e2cf-4889-b99d-aeb15b65b809

Name:

- Default

Isvalid:

- True

Identity:

- Default

Filetypes:

- ace
- apk
- app
- appx
- ani
- arj
- bat
- cab
- cmd
- com
- deb
- dex
- dll
- docm
- elf
- exe
- hta
- img
- iso
- jar
- jnlp
- kext
- lha
- lib
- library
- lnk
- lzh
- macho
- msc
- msi
- msix
- msp
- mst
- pif
- ppa
- ppam
- reg

- rev
- scf
- scr
- sct
- sys
- uif
- vb
- vbe
- vbs
- vxd
- wsc
- wsf
- wsh
- xll
- xz
- z

Isdefault:

- True

Zapenabled:

- True

Objectclass:

- top
- msExchMalwareFilterConfig

Objectstate:

- Unchanged

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:26+00:00

Quarantinetag:

- AdminOnlyAccessPolicy

Filetypeaction:

- Reject

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Malware-Filter-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:26Z

Exchangeversion:

- 0.20 (15.0.0.0)

Enablefilefilter:

- True

Exchangeobjectid:

- 16ad84a0-e2cf-4889-b99d-aeb15b65b809

Distinguishedname:

- CN=Default,CN=Malware Filter,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Description

Anti-malware policies should be configured to notify administrators when internal users send messages containing malware. This provides early warning of compromised internal accounts.

Details

Rationale: When an internal user sends malware, it typically indicates a compromised account or endpoint. Timely notifications allow security teams to investigate and respond before significant damage occurs.

Impact: Administrators will receive notifications when malware is detected in messages sent by internal users. This may increase alert volume.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-MalwareFilterPolicy | fl Identity, EnableInternalSenderAdminNotifications, InternalSenderAdminAddress

Ensure EnableInternalSenderAdminNotifications is True and InternalSenderAdminAddress is defined.

Remediation:

Microsoft Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Anti-malware.

Edit the default policy to enable notifications for internal senders.

PowerShell:

Set-MalwareFilterPolicy -Identity Default -EnableInternalSenderAdminNotifications $true -InternalSenderAdminAddress admin@contoso.com

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure

---

● ms365-cis-2.1.4 Ensure Safe Attachments policy is enabled

[PASS]

Vulnerability Name	Found compliant Safe Attachments policy(ies)
Section	2.1 Microsoft Defender for Office 365
Severity	High
Profiles	E5 Level 1
Default Value	Safe Attachments is not enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026

Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Found compliant Safe Attachments policy(ies): Built-In Protection Policy (Enable=True, Action=Block, QuarantineTag=AdminOnlyAccessPolicy). Rule priority/scope was not verified (Get-SafeAttachmentRule data is not collected) — confirm it applies to all recipients.

Id:

- Built-In Protection Policy

Guid:

- 78c7c543-39c1-4b28-a7c3-1181418bd01f

Name:

- Built-In Protection Policy

Action:

- Block

Enable:

- True

Isvalid:

- True

Identity:

- Built-In Protection Policy

Objectclass:

- top
- msExchSafeAttachmentProtectionConfig

Objectstate:

- Unchanged

Whenchanged:

- 2026-07-14T16:15:34+00:00

Whencreated:

- 2026-07-14T16:15:28+00:00

Quarantinetag:

- AdminOnlyAccessPolicy

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Safe-Attachment-Protection-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-07-14T16:15:34Z

Whencreatedutc:

- 2026-07-14T16:15:28Z

Exchangeversion:

- 0.20 (15.0.0.0)

Exchangeobjectid:

- 78c7c543-39c1-4b28-a7c3-1181418bd01f

Distinguishedname:

- CN=Built-In Protection Policy,CN=Safe Attachment,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Isbuiltinprotection:

- True

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Quarantinetagforblockingencryptedattachments:

- DefaultFullAccessWithNotificationPolicy

Description

Safe Attachments in Microsoft Defender for Office 365 provides advanced malware protection for email attachments by opening them in a virtual sandbox environment before delivery.

Details

Rationale: Safe Attachments provides protection against zero-day threats and unknown malware in email attachments by detonating attachments in a sandbox before delivering them to recipients.

Impact: Email delivery may be delayed slightly while attachments are scanned. The delay is typically a few minutes but can vary based on file type and size.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-SafeAttachmentPolicy | ft Identity, Enable, Action, QuarantineTag

The highest-priority policy that applies to all users should have Enable = True, Action = Block, and QuarantineTag = AdminOnlyAccessPolicy.

Remediation:

Microsoft Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Safe Attachments.

Create or edit a Safe Attachments policy:

• Enable the policy

• Set action to 'Block'

• Apply to all recipients

PowerShell:

Set-SafeAttachmentPolicy -Identity Default -Enable $true -Action Block -QuarantineTag AdminOnlyAccessPolicy

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

---

● ms365-cis-2.1.5 Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled

[PASS]

Vulnerability Name	Safe Attachments for SharePoint/OneDrive/Teams is enabled (EnableATPForSPOTeamsODB=True, EnableSafeDocs=True, AllowSafeDocsOpen=False).
Section	2.1 Microsoft Defender for Office 365
Severity	High

Profiles	E5 Level 1
Default Value	Safe Attachments for SPO/ODB/Teams is disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Safe Attachments for SharePoint, OneDrive, and Teams scans files stored in these services for malware. When a malicious file is detected, it is blocked from download and the file owner is notified.

Id:

- Default

Guid:

- 801f7758-842c-415f-a5a7-d8502f9a6409

Name:

- Default

Isvalid:

- True

Identity:

- Default

Objectclass:

- top
- msExchHostedContentFilterConfig

Objectstate:

- Unchanged

Whenchanged:

- 2026-07-14T16:15:34+00:00

Whencreated:

- 2026-07-14T16:15:24+00:00

Enablesafedocs:

- True

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Hosted-Content-Filter-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-07-14T16:15:34Z

Whencreatedutc:

- 2026-07-14T16:15:24Z

Exchangeversion:

- 0.20 (15.0.0.0)

Exchangeobjectid:

- 801f7758-842c-415f-a5a7-d8502f9a6409

Distinguishedname:

- CN=Default,CN=Atp Policy For O365,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Enableatpforspoteamsodb:

- True

Description

Safe Attachments for SharePoint, OneDrive, and Teams scans files stored in these services for malware. When a malicious file is detected, it is blocked from download and the file owner is notified.

Details

Rationale: Files shared via SharePoint, OneDrive, and Teams can spread malware if not scanned. Enabling Safe Attachments for these services provides protection against malware propagation through collaboration tools.

Impact: Files identified as malicious will be blocked. Users who uploaded an infected file will be notified.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-AtpPolicyForO365 | fl Name, EnableATPForSPOTeamsODB, EnableSafeDocs, AllowSafeDocsOpen

Verify EnableATPForSPOTeamsODB = True, EnableSafeDocs = True, and AllowSafeDocsOpen = False.

Remediation:

Microsoft Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Safe Attachments.

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

PowerShell:

Set-AtpPolicyForO365 -EnableATPForSPOTeamsODB $true -EnableSafeDocs $true -AllowSafeDocsOpen $false

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-configure

---

- **ms365-cis-2.1.6 Ensure Exchange Online Spam Policies are set to notify administrators** **[FAIL]**

Vulnerability Name	Admin notifications for outbound spam are not fully enabled
Section	2.1 Microsoft Defender for Office 365
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Admin notifications for outbound spam may not be configured.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Admin notifications for outbound spam are not fully enabled: BccSuspiciousOutboundMail=False, NotifyOutboundSpam=False.

Id:

- Default

Guid:

- 3c971a05-d238-4ad5-bb1d-b2cfd6bbfc25

Name:

- Default

Isvalid:

- True

Identity:

- Default

Isdefault:

- True

Objectclass:

- top
- msExchHygieneConfiguration

Objectstate:

- Unchanged

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:26+00:00

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Hygiene-Configuration

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:26Z

Exchangeversion:

- 0.20 (15.0.0.0)

Exchangeobjectid:

- 3c971a05-d238-4ad5-bb1d-b2cfd6bbfc25

Configurationtype:

- HostedOutboundSpamFilterPolicy

Distinguishedname:

- CN=Default,CN=Outbound Spam Filter,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Autoforwardingmode:

- Automatic

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Actionwhenthresholdreached:

- BlockUserForToday

Description

The outbound spam filter policy should be configured to notify administrators when a user is detected sending suspicious outbound email, allowing security teams to identify and respond to compromised accounts.

Details

Rationale: Admin notifications for suspicious outbound spam help security teams identify and respond to compromised accounts before they can be used to send large volumes of spam or phishing emails.

Impact: Administrators will receive notification emails when outbound spam is detected. This may increase email volume for admin accounts.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-HostedOutboundSpamFilterPolicy | Select-Object Bcc, *Notify*

Verify BccSuspiciousOutboundMail = True and NotifyOutboundSpam = True, with correctly configured notification email addresses.

Remediation:

Microsoft Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Anti-spam > Outbound spam filter policy.

Enable notifications for suspicious outbound activity.

PowerShell:

Set-HostedOutboundSpamFilterPolicy -Identity Default -BccSuspiciousOutboundMail $true -BccSuspiciousOutboundAdditionalRecipients admin@contoso.com -NotifyOutboundSpam $true -NotifyOutboundSpamRecipients admin@contoso.com

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/outbound-spam-policies-configure

---

- **ms365-cis-2.1.7 Ensure that an anti-phishing policy has been created**
  [FAIL]

Vulnerability Name	No anti-phishing policy has all required protections enabled (checked 1 policy(ies)).
Section	2.1 Microsoft Defender for Office 365
Severity	High
Profiles	E5 Level 1
Default Value	Only the default anti-phishing policy exists.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

A custom anti-phishing policy should be created in Microsoft Defender for Office 365 to protect users from impersonation attacks and provide advanced anti-phishing protection beyond the default settings.

Id:

- Office365 AntiPhish Default

Guid:

- c7ddb673-3d15-4d62-b21d-1d19d9104649

Name:

- Office365 AntiPhish Default

Enabled:

- True

Isvalid:

- True

Identity:

- Office365 AntiPhish Default

Isdefault:

- True

Objectclass:

- top
- msExchHostedContentFilterConfig

Objectstate:

- Unchanged

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:26+00:00

Enableviatag:

- True

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Hosted-Content-Filter-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:26Z

Exchangeversion:

- 0.20 (15.0.0.0)

Exchangeobjectid:

- c7ddb673-3d15-4d62-b21d-1d19d9104649

Honordmarcpolicy:

- True

Distinguishedname:

- CN=Office365 AntiPhish Default,CN=AntiPhish,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Dmarcrejectaction:

- Reject

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Spoofquarantinetag:

- DefaultFullAccessPolicy

Phishthresholdlevel:

- 1

Dmarcquarantineaction:

- Quarantine

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Enablespoofintelligence:

- True

Authenticationfailaction:

- MoveToJmf

Enablemailboxintelligence:

- True

Targeteduserquarantinetag:

- DefaultFullAccessPolicy

Enableunauthenticatedsender:

- True

Targeteddomainquarantinetag:

- DefaultFullAccessPolicy

Impersonationprotectionstate:

- Automatic

Targeteduserprotectionaction:

- NoAction

Targeteddomainprotectionaction:

- NoAction

Mailboxintelligencequarantinetag:

- DefaultFullAccessPolicy

Mailboxintelligenceprotectionaction:

- NoAction

Description

A custom anti-phishing policy should be created in Microsoft Defender for Office 365 to protect users from impersonation attacks and provide advanced anti-phishing protection beyond the default settings.

Details

Rationale: Anti-phishing policies provide protection against impersonation attacks where attackers spoof trusted senders or domains. Custom policies allow organizations to protect their own domains and key users from spoofing.

Impact: Emails that appear to impersonate protected users or domains will be quarantined or tagged, which may cause false positives for legitimate forwarded emails.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-AntiPhishPolicy | fl <fields> and Get-AntiPhishRule.

Verify a custom policy exists with: Enabled=True, PhishThresholdLevel=3, EnableTargetedUserProtection=True, EnableOrganizationDomainsProtection=True, EnableMailboxIntelligence=True, EnableMailboxIntelligenceProtection=True, EnableSpoofIntelligence=True, TargetedUserProtectionAction=Quarantine, TargetedDomainProtectionAction=Quarantine, MailboxIntelligenceProtectionAction=Quarantine,

EnableFirstContactSafetyTips=True, EnableSimilarUsersSafetyTips=True, EnableSimilarDomainsSafetyTips=True, EnableUnusualCharactersSafetyTips=True, HonorDmarcPolicy=True.

Remediation:

Microsoft Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Anti-phishing.

Create a new anti-phishing policy:

• Enable impersonation protection for key users and domains

• Enable mailbox intelligence and spoof intelligence

• Enable safety tips

• Configure action to quarantine

PowerShell:

New-AntiPhishPolicy -Name 'Custom Anti-Phish' -EnableMailboxIntelligence $true -EnableMailboxIntelligenceProtection $true -EnableSpoofIntelligence $true -HonorDmarcPolicy $true

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-mdo-configure

---

- **ms365-cis-2.1.8 Ensure that SPF records are published for all Exchange Domains**
  [FAIL]

Vulnerability Name	1 domain(s) are missing SPF records:
Section	2.1 Microsoft Defender for Office 365
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	No SPF record is published by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Sender Policy Framework (SPF) records specify which mail servers are authorized to send email on behalf of a domain. SPF records should be published for all Exchange Online verified domains.

Error:

- Client error '400 Bad Request' for url 'https://dns.google/resolve?name=&type=TXT'
  For more information check: https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/400

Description

Sender Policy Framework (SPF) records specify which mail servers are authorized to send email on behalf of a domain. SPF records should be published for all Exchange Online verified domains.

Details

Rationale: Without an SPF record, attackers can spoof the organization's domain in phishing emails. SPF records allow receiving mail servers to verify that email claiming to come from the domain was sent from an authorized server.

Impact: Incorrect SPF records can cause legitimate emails to be rejected. Ensure the SPF record includes all authorized sending sources before publishing.

Audit Procedure:

For each verified domain:

Query DNS TXT records for the domain

Look for a record starting with 'v=spf1'

Verify it includes 'include:spf.protection.outlook.com'

Using DNS-over-HTTPS:

GET https://dns.google/resolve?name={domain}&type=TXT

Remediation:

For each Exchange domain without an SPF record:

Add a DNS TXT record:

v=spf1 include:spf.protection.outlook.com -all

This should be done through your domain registrar's DNS management.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-spf-configure

---

- **ms365-cis-2.1.9 Ensure that DKIM is enabled for all Exchange Online Domains**
  [PASS]

Vulnerability Name	No custom verified domains found. DKIM is enabled by default for .onmicrosoft.com domains.
Section	2.1 Email & collaboration
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	DKIM is enabled by default for .onmicrosoft.com but not custom domains.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

DomainKeys Identified Mail (DKIM) should be enabled for all Exchange Online domains to digitally sign outbound mail and prevent spoofing. DKIM is a critical component of an email authentication stack alongside SPF and DMARC.

Description

DomainKeys Identified Mail (DKIM) should be enabled for all Exchange Online domains to digitally sign outbound mail and prevent spoofing. DKIM is a critical component of an email authentication stack alongside SPF and DMARC.

Details

Rationale: Without DKIM, attackers can more easily spoof your domain to send fraudulent emails that appear legitimate to recipients. DKIM signing also provides non-repudiation for outbound messages.

Impact: Minimal operational impact. Some third-party email services that send on behalf of your domain may need DKIM key updates.

Audit Procedure:

Using Microsoft Graph domains API:

GET /domains

For each verified domain, check the DKIM signing status via:

Exchange Online PowerShell: Get-DkimSigningConfig | Select-Object Domain, Enabled

All domains should have Enabled = True.

Note: The Graph API does not expose DKIM configuration directly. Full automated verification requires Exchange Online PowerShell or the Exchange Online REST API.

Remediation:

Exchange Online PowerShell:

Enable-DkimSigning -DomainName <domain>

Or via Defender portal:

Microsoft Defender portal → Email & collaboration > Policies & rules > Threat policies > Email authentication settings > DKIM.

Enable signing for each domain.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dkim-configure

● ms365-cis-2.1.10 Ensure DMARC Records for all Exchange Online Domains are Published

[FAIL]

Vulnerability Name	DMARC issues found: 1 domain(s) missing DMARC:
Section	2.1 Microsoft Defender for Office 365
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	No DMARC record is published by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Domain-based Message Authentication, Reporting, and Conformance (DMARC) records should be published for all Exchange Online verified domains. DMARC builds on SPF and DKIM to give email receivers instructions on how to handle emails that fail authentication.

Description

Domain-based Message Authentication, Reporting, and Conformance (DMARC) records should be published for all Exchange Online verified domains. DMARC builds on SPF and DKIM to give email receivers instructions on how to handle emails that fail authentication.

Details

Rationale: DMARC prevents domain spoofing by telling receiving mail servers what to do with email that fails SPF and DKIM checks. A DMARC policy of 'reject' or 'quarantine' prevents spoofed emails from reaching recipients.

Impact: Incorrect DMARC policies can cause legitimate emails to be rejected. Start with 'p=none' for monitoring before moving to 'p=quarantine' or 'p=reject'.

Audit Procedure:

For each verified domain:

- Query DNS TXT records for _dmarc.{domain}
- Look for a record starting with 'v=DMARC1'
- Check the policy (p=) value

Using DNS-over-HTTPS:

GET https://dns.google/resolve?name=_dmarc.{domain}&type=TXT

Remediation:

For each domain without a DMARC record:

Add a DNS TXT record for _dmarc.{domain}:

v=DMARC1; p=reject; rua=mailto:dmarc-reports@yourdomain.com

Start with p=none for monitoring, then move to p=quarantine, then p=reject.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dmarc-configure

---

- **ms365-cis-2.1.11 Ensure comprehensive attachment filtering is applied**
  [FAIL]

Vulnerability Name	No malware filter policy defines at least 120 file extensions with EnableFileFilter=True (checked 1 policy(ies)).
Section	2.1 Microsoft Defender for Office 365
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Default file type filtering includes common types but may not be comprehensive.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The anti-malware policy should have comprehensive file type filtering that goes beyond the default set. Additional dangerous file types such as .ps1, .bat, .cmd, and others should be blocked.

Id:

- Default

Guid:

- 16ad84a0-e2cf-4889-b99d-aeb15b65b809

Name:

- Default

Isvalid:

- True

Identity:

- Default

Filetypes:

- ace

- apk
- app
- appx
- ani
- arj
- bat
- cab
- cmd
- com
- deb
- dex
- dll
- docm
- elf
- exe
- hta
- img
- iso
- jar
- jnlp
- kext
- lha
- lib
- library
- lnk
- lzh
- macho
- msc
- msi
- msix
- msp
- mst
- pif
- ppa
- ppam
- reg
- rev
- scf

- scr
- sct
- sys
- uif
- vb
- vbe
- vbs
- vxd
- wsc
- wsf
- wsh
- xll
- xz
- z

Isdefault:

- True

Zapenabled:

- True

Objectclass:

- top
- msExchMalwareFilterConfig

Objectstate:

- Unchanged

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:26+00:00

Quarantinetag:

- AdminOnlyAccessPolicy

Filetypeaction:

- Reject

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Malware-Filter-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:26Z

Exchangeversion:

- 0.20 (15.0.0.0)

Enablefilefilter:

- True

Exchangeobjectid:

- 16ad84a0-e2cf-4889-b99d-aeb15b65b809

Distinguishedname:

- CN=Default,CN=Malware Filter,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Description

The anti-malware policy should have comprehensive file type filtering that goes beyond the default set. Additional dangerous file types such as .ps1, .bat, .cmd, and others should be blocked.

Details

Rationale: Attackers use many file types to deliver malware. Comprehensive filtering ensures that less common but equally dangerous file types are also blocked at the email gateway.

Impact: Legitimate emails with the blocked file types will be quarantined. Users will need to use alternative methods to share these file types.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-MalwareFilterPolicy and Get-MalwareFilterRule.

A comprehensive policy must: define at least 120 of CIS's reference list of 184 file extensions (a 90% threshold), have the corresponding rule's State = Enabled, and EnableFileFilter = True.

Remediation:

Exchange Online PowerShell:

Set-MalwareFilterPolicy -Identity Default -EnableFileFilter $true

Set-MalwareFilterPolicy -Identity Default -FileTypes 'ace','ani','app','cab','cmd','com','exe','gz','hta','img','iso','jar','jnlp','js','mde','msi','msp','ps1','ps2','reg','scr','tar','uue','vbe','vbs','wsc','wsf','wsh',... (through the full CIS reference list of 184 extensions)

Enable-MalwareFilterRule -Identity Default

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure

---

- **ms365-cis-2.1.12 Ensure the connection filter IP allow list is not used**
  [PASS]

Vulnerability Name	The connection filter IP allow list is empty.
Section	2.1 Microsoft Defender for Office 365
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	IP allow list is empty by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The connection filter IP allow list allows emails from specified IP addresses to bypass spam filtering. This should not be used as it can allow spam and malware from those IP addresses.

Description

The connection filter IP allow list allows emails from specified IP addresses to bypass spam filtering. This should not be used as it can allow spam and malware from those IP addresses.

Details

Rationale: IP addresses in the connection filter allow list bypass spam and malware filtering. This creates a potential attack vector if any of those IP addresses become compromised or are used by attackers.

Impact: Removing IP addresses from the allow list means their emails will be subject to normal spam and malware filtering.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-HostedConnectionFilterPolicy -Identity Default | fl IPAllowList

Ensure IPAllowList is empty.

Remediation:

Exchange Online PowerShell:

Set-HostedConnectionFilterPolicy -Identity Default -IPAllowList @()

If specific IPs need to be trusted, use the Enhanced Filtering for Connectors feature instead.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/connection-filter-policies-configure

---

- **ms365-cis-2.1.13 Ensure the connection filter safe list is off**

  [PASS]

Vulnerability Name	The connection filter safe list is disabled (EnableSafeList=False).
Section	2.1 Microsoft Defender for Office 365
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	EnableSafeList is disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The connection filter safe list allows Microsoft to periodically update a list of IP addresses considered safe. This should be disabled as it can bypass spam filtering for IPs that may be compromised.

Description

The connection filter safe list allows Microsoft to periodically update a list of IP addresses considered safe. This should be disabled as it can bypass spam filtering for IPs that may be compromised.

Details

Rationale: The safe list is a shared Microsoft list that can allow IPs used by spammers to bypass filtering. Disabling it ensures all email goes through your configured filtering policies.

Impact: Disabling the safe list means emails from those IP addresses will be subject to normal spam filtering.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-HostedConnectionFilterPolicy -Identity Default | fl EnableSafeList

Ensure EnableSafeList is False.

Remediation:
Exchange Online PowerShell:
Set-HostedConnectionFilterPolicy -Identity Default -EnableSafeList $false

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/connection-filter-policies-configure

---

- **ms365-cis-2.1.14 Ensure inbound anti-spam policies do not contain allowed domains**
  [PASS]

Vulnerability Name	AllowedSenderDomains is empty/undefined on all 1 inbound anti-spam policy(ies).
Section	2.1 Microsoft Defender for Office 365
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	AllowedSenderDomains is empty by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Allowed domains in the inbound anti-spam policy cause all emails from those domains to bypass spam filtering. This creates a risk if the domain is compromised or used by attackers to send phishing emails.

Id:

- Default

Guid:

- b6c326ea-52f1-46de-9793-c1c8ac8cbf9c

Name:

- Default

Isvalid:

- True

Identity:

- Default

Isdefault:

- True

Spamaction:

- MoveToJmf

Zapenabled:

- True

Objectclass:

- top
- msExchHostedContentFilterConfig

Objectstate:

- Unchanged

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:23+00:00

Bulkthreshold:

- 7

Bulkspamaction:

- MoveToJmf

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Hosted-Content-Filter-Config

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Spamzapenabled:

- True

Testmodeaction:

- None

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:23Z

Exchangeversion:

- 0.20 (15.0.0.0)

Phishspamaction:

- MoveToJmf

Phishzapenabled:

- True

Bulkmovesenabled:

- NotSet

Exchangeobjectid:

- b6c326ea-52f1-46de-9793-c1c8ac8cbf9c

Bulkquarantinetag:

- DefaultFullAccessPolicy

Distinguishedname:

- CN=Default,CN=Hosted Content Filter,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Spamquarantinetag:

- DefaultFullAccessPolicy

Markasspambulkmail:

- On

Phishquarantinetag:

- DefaultFullAccessPolicy

Intraorgfilterstate:

- Default

Recommendedpolicytype:

- Custom

Markasspamframesinhtml:

- Off

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Inlinesafetytipsenabled:

- True

Markasspamemptymessages:

- Off

Markasspamwebbugsinhtml:

- Off

Highconfidencespamaction:

- MoveToJmf

Markasspamformtagsinhtml:

- Off

Markasspamndrbackscatter:

- Off

Highconfidencephishaction:

- Quarantine

Markasspamembedtagsinhtml:

- Off

Quarantineretentionperiod:

- 15

Markasspamjavascriptinhtml:

- Off

Markasspamobjecttagsinhtml:

- Off

Increasescorewithimagelinks:

- Off

Increasescorewithnumericips:

- Off

Markasspamsensitivewordlist:

- Off

Markasspamspfrecordhardfail:

- Off

Markasspamfromaddressauthfail:

- Off

Increasescorewithbizorinfourls:

- Off

Highconfidencespamquarantinetag:

- DefaultFullAccessPolicy

Highconfidencephishquarantinetag:

- AdminOnlyAccessPolicy

Increasescorewithredirecttootherport:

- Off

Description

Allowed domains in the inbound anti-spam policy cause all emails from those domains to bypass spam filtering. This creates a risk if the domain is compromised or used by attackers to send phishing emails.

Details

Rationale: Domains in the allowed domains list bypass spam filtering entirely. Attackers who know a domain is whitelisted can spoof it or compromise an account in that domain to send phishing emails that bypass all filtering.

Impact: Emails from the removed domains will be subject to normal spam filtering. This may cause some legitimate emails to be marked as spam initially.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-HostedContentFilterPolicy | ft Identity, AllowedSenderDomains

Ensure AllowedSenderDomains is undefined for each inbound policy.

Remediation:

Exchange Online PowerShell:

Set-HostedContentFilterPolicy -Identity Default -AllowedSenderDomains @()

Remove any domains from the allowed senders list in the anti-spam policy.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-policies-configure

---

- **ms365-cis-2.1.15 Ensure outbound anti-spam message limits are in place**
  [FAIL]

Vulnerability Name	Outbound anti-spam recipient rate limits are not sufficiently restrictive
Section	2.1 Microsoft Defender for Office 365
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	RecipientLimitExternalPerHour=500, RecipientLimitInternalPerHour=1000, RecipientLimitPerDay=1000, ActionWhenThresholdReached=BlockUser by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Outbound anti-spam recipient rate limits are not sufficiently restrictive: RecipientLimitExternalPerHour=0 (max 500), RecipientLimitInternalPerHour=0 (max 1000), RecipientLimitPerDay=0 (max 1000), ActionWhenThresholdReached='BlockUserForToday' (must be BlockUser).

Id:

- Default

Guid:

- 3c971a05-d238-4ad5-bb1d-b2cfd6bbfc25

Name:

- Default

Isvalid:

- True

Identity:

- Default

Isdefault:

- True

Objectclass:

- top
- msExchHygieneConfiguration

Objectstate:

- Unchanged

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:26+00:00

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-Hygiene-Configuration

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:26Z

Exchangeversion:

- 0.20 (15.0.0.0)

Exchangeobjectid:

- 3c971a05-d238-4ad5-bb1d-b2cfd6bbfc25

Configurationtype:

- HostedOutboundSpamFilterPolicy

Distinguishedname:

- CN=Default,CN=Outbound Spam Filter,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Autoforwardingmode:

- Automatic

Recommendedpolicytype:

- Custom

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Actionwhenthresholdreached:

- BlockUserForToday

Description

The outbound spam filter policy should set recipient rate limits and an action to take once the threshold is reached, so that a compromised account cannot be used to send large volumes of spam.

Details

Rationale: Attackers who compromise email accounts often use them to send large volumes of spam or phishing emails. Recipient rate limits with an automatic block action contain the damage a compromised account can do.

Impact: Legitimate high-volume senders may be blocked if they exceed the configured recipient limits. Organizations must evaluate limits against legitimate business needs.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-HostedOutboundSpamFilterPolicy -Identity Default | fl RecipientLimitExternalPerHour, RecipientLimitInternalPerHour, RecipientLimitPerDay, ActionWhenThresholdReached

Recommended: External <= 500, Internal <= 1000, Daily <= 1000, ActionWhenThresholdReached = BlockUser. Microsoft's Strict preset values of 400/800/800 are also compliant (equal or more restrictive passes). Also verify NotifyOutboundSpamRecipients contains a monitored mailbox.

Remediation:

Exchange Online PowerShell:

Set-HostedOutboundSpamFilterPolicy -Identity Default -RecipientLimitExternalPerHour 500 -RecipientLimitInternalPerHour 1000 -RecipientLimitPerDay 1000 -ActionWhenThresholdReached BlockUser -NotifyOutboundSpamRecipients admin@contoso.com

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/outbound-spam-policies-configure

ms365-cis-2.2.1 Ensure that activity monitoring of emergency access accounts is configured

[MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure that activity monitoring of emergency access accounts is configured
Section	2.2 Microsoft 365 Defender
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	No monitoring is configured for emergency access accounts by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Emergency access accounts (break-glass accounts) should be monitored for any sign-in activity. Any use of these accounts should trigger immediate alerts to security administrators.

Description

Emergency access accounts (break-glass accounts) should be monitored for any sign-in activity. Any use of these accounts should trigger immediate alerts to security administrators.

Details

Rationale: Emergency access accounts are highly privileged accounts that should only be used in dire circumstances. Monitoring for their use helps detect unauthorized access and ensures accountability when they are used.

Impact: Security team will receive alerts when emergency access accounts are used, requiring investigation to verify whether the use was legitimate.

Audit Procedure:

Verify monitoring configuration:

Microsoft Entra admin center → Identity > Monitoring & health > Workbooks > Sign-ins

Azure Monitor / Log Analytics:

Create an alert rule for sign-in events from emergency access accounts

Microsoft Sentinel:

Configure analytic rules for break-glass account sign-ins

Verify that alerts are configured for all emergency access account UPNs.

Remediation:

Azure Monitor → Alerts > Create alert rule:

• Signal type: Log (Log Analytics)

• Signal: SigninLogs

• Condition: UserPrincipalName == '<emergency-account-upn>'

• Action group: Notify security team immediately

Or use Microsoft Sentinel with a custom analytic rule.

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

---

- **ms365-cis-2.4.1 Ensure Priority account protection is enabled and configured**
  [SKIPPED]

Vulnerability Name	Priority account protection has no Microsoft Graph API or PowerShell cmdlet published by CIS, so it cannot be collected. Verify in the Microsoft 365 Defender portal
Section	2.4 Microsoft Defender
Severity	Medium
Profiles	E5 Level 1
Default Value	Priority account protection is not enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

Priority account protection has no Microsoft Graph API or PowerShell cmdlet published by CIS, so it cannot be collected. Verify in the Microsoft 365 Defender portal: Settings > Email & collaboration > Priority account protection (confirm it is turned on), User tags (confirm priority accounts are tagged), and Alert policies (confirm priority-account alerts are enabled).

Description

Priority account protection in Microsoft Defender for Office 365 provides enhanced protection for accounts that are designated as priority accounts (executives, key financial personnel, etc.).

Details

Rationale: Priority accounts are high-value targets for attackers. Enhanced protection ensures that these accounts receive additional scrutiny and tighter security policies.

Impact: Priority account users may experience more aggressive filtering and more frequent authentication challenges.

Audit Procedure:

Microsoft 365 Defender portal (https://security.microsoft.com):

Settings > Email & collaboration > Priority account protection.

Verify priority account protection is turned on.

Also review:

Settings > Email & collaboration > User tags — confirm accounts are tagged as 'Priority account'.

Email & collaboration > Policies & rules > Alert policy — confirm priority-account alert policies are enabled.

Note: CIS publishes no PowerShell or Microsoft Graph audit method for this control; it is Defender portal (UI) only.

Remediation:

Microsoft 365 Defender portal → Settings > Email & collaboration > Priority account protection:

Turn on priority account protection.

Tag key accounts as priority accounts (User tags).

Enable the related alert policies.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/priority-accounts-turn-on-priority-account-protection

---

ms365-cis-2.4.2 Ensure Priority accounts have 'Strict protection' presets applied

[SKIPPED]

Vulnerability Name	Strict Preset Security Policy assignment for priority accounts has no Microsoft Graph API or PowerShell cmdlet published by CIS, so it cannot be collected. Verify in the Microsoft 365 Defender portal
Section	2.4 Microsoft Defender

Security Findings Report

Severity	Low
Profiles	E5 Level 2
Default Value	Priority accounts do not have Strict protection by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

Strict Preset Security Policy assignment for priority accounts has no Microsoft Graph API or PowerShell cmdlet published by CIS, so it cannot be collected. Verify in the Microsoft 365 Defender portal: Email & Collaboration > Policies & Rules > Threat policies > Preset security policies, confirming each of Anti-phishing, Anti-spam, Anti-malware, Safe Attachments, and Safe Links includes the priority accounts/groups under the Strict preset.

Description

Priority accounts should be assigned the 'Strict protection' preset security policy in Microsoft Defender for Office 365, which applies the most aggressive email security settings.

Details

Rationale: The Strict protection preset applies the most aggressive anti-spam, anti-malware, anti-phishing, Safe Links, and Safe Attachments settings, providing the highest level of email security for high-value accounts.

Impact: Strict protection settings may cause more false positives and quarantine more legitimate emails. Priority account users should be prepared for occasional false positives.

Audit Procedure:

Microsoft 365 Defender portal (https://security.microsoft.com):

Email & Collaboration > Policies & Rules > Threat policies.

For each of: Anti-phishing, Anti-spam, Anti-malware, Safe Attachments, and Safe Links, open the policy and confirm a 'Strict Preset Security Policy' exists whose recipient conditions include the priority accounts/groups.

Note: CIS publishes no PowerShell or Microsoft Graph audit method for this control; it is Defender portal (UI) only.

Remediation:

Microsoft 365 Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Preset security policies:

Edit the Strict protection preset.

Add the priority accounts/groups to the policy recipients for each of Anti-phishing, Anti-spam, Anti-malware, Safe Attachments, and Safe Links.

Save the configuration.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies

---

ms365-cis-2.4.3 Ensure Microsoft Defender for Cloud Apps is enabled

[MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure Microsoft Defender for Cloud Apps is enabled
Section	2.4 Microsoft Defender
Severity	Low
Profiles	E5 Level 2
Default Value	Defender for Cloud Apps is not enabled by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft Defender for Cloud Apps (formerly MCAS) provides Cloud Access Security Broker (CASB) capabilities including visibility into cloud app usage, threat detection, and data protection.

Description

Microsoft Defender for Cloud Apps (formerly MCAS) provides Cloud Access Security Broker (CASB) capabilities including visibility into cloud app usage, threat detection, and data protection.

Details

Rationale: Defender for Cloud Apps provides visibility into shadow IT, enforces data protection policies across cloud apps, and detects threats like unusual access patterns and potential account compromises.

Impact: Enabling Defender for Cloud Apps requires E5 licensing and initial configuration effort. Some features require additional licensing.

Audit Procedure:

Microsoft Defender portal (https://security.microsoft.com):

Navigate to Cloud apps section

Verify Defender for Cloud Apps is connected and active

Microsoft Defender for Cloud Apps portal (https://portal.cloudappsecurity.com):

Verify the portal is accessible and configured.

Remediation:

Microsoft 365 Defender portal:

Settings > Cloud apps > Defender for Cloud Apps

Enable Defender for Cloud Apps and configure the initial settings.

Reference: https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

---

ms365-cis-2.4.4 Ensure Zero-hour auto purge for Microsoft Teams is on

[PASS]

Vulnerability Name	Zero-hour auto purge for Teams is enabled on: ayushaggarwal1136gmail.onmicrosoft.com\Default Teams Protection Policy. Rule-level exclusions (Get-TeamsProtectionPolicyRule ExceptIf*) were not verified — this data is not collected.
Section	2.4 Microsoft Defender
Severity	Low
Profiles	E5 Level 2
Default Value	ZAP for Teams is not enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Zero-hour auto purge (ZAP) for Teams automatically removes malicious messages from Teams conversations after delivery, similar to how email ZAP works for Exchange Online.

Id:

- ayushaggarwal1136gmail.onmicrosoft.com\Default Teams Protection Policy

Guid:

- 00000000-0000-0000-0000-000000000000

Name:

- Default Teams Protection Policy

Isvalid:

- True

Identity:

- ayushaggarwal1136gmail.onmicrosoft.com\Default Teams Protection Policy

Zapenabled:

- True

Objectclass:

- msExchHostedContentFilterConfig

Objectstate:

- New

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Exchangeversion:

- 0.20 (15.0.0.0)

Exchangeobjectid:

- 63c45761-173a-4043-8acb-1777390ddb92

Distinguishedname:

- CN=Default Teams Protection Policy,CN=ATP Teams Protection,CN=Transport Settings,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Malwarequarantinetag:

- AdminOnlyAccessPolicy

Organizationalunitroot:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com

Highconfidencephishquarantinetag:

- AdminOnlyAccessPolicy

Description

Zero-hour auto purge (ZAP) for Teams automatically removes malicious messages from Teams conversations after delivery, similar to how email ZAP works for Exchange Online.

Details

Rationale: Malicious URLs and files can be shared in Teams messages. ZAP for Teams ensures that messages identified as malicious after delivery are automatically removed, reducing the window of exposure.

Impact: Messages identified as malicious will be automatically removed from Teams conversations, which may cause confusion if users saw the message before it was removed.

Audit Procedure:

Connect to Exchange Online using Connect-ExchangeOnline.

Run: Get-TeamsProtectionPolicy | fl ZapEnabled

Run: Get-TeamsProtectionPolicyRule | fl ExceptIf*

Ensure ZapEnabled is True and review any exclusions configured on the rule (ExceptIf* conditions).

Remediation:

Microsoft Defender portal → Email & Collaboration > Policies & Rules > Threat policies > Zero-hour auto purge, enable ZAP for Microsoft Teams.

Or via Exchange Online PowerShell:

Set-TeamsProtectionPolicy -Identity Default -ZapEnabled $true

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge

---

● ms365-cis-3.1.1 Ensure Microsoft 365 audit log search is Enabled

[PASS]

Vulnerability Name	The Microsoft 365 unified audit log is enabled (UnifiedAuditLogIngestionEnabled=True).
Section	3.1 Audit
Severity	High

Profiles	E3 Level 1, E5 Level 1
Default Value	Enabled by default in new tenants since 2019.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The Microsoft 365 unified audit log records user and administrator activity across Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, and other services. It must be enabled for effective security monitoring and incident investigation.

Unifiedauditlogingestionenabled:

- True

Description

The Microsoft 365 unified audit log records user and administrator activity across Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, and other services. It must be enabled for effective security monitoring and incident investigation.

Details

Rationale: Without audit logging, security teams cannot investigate incidents, detect malicious activity, or meet compliance requirements that mandate audit trails of administrative and user actions.

Impact: Minimal. Audit logging has negligible performance impact.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-AdminAuditLogConfig | Select-Object UnifiedAuditLogIngestionEnabled

Ensure UnifiedAuditLogIngestionEnabled is True.

Microsoft Purview (https://purview.microsoft.com) → Solutions > Audit → verify search results are returned for a recent activity.

Remediation:

Exchange Online PowerShell:

Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true

Or in Microsoft Purview compliance portal:

Audit → Turn on auditing.

Reference: https://learn.microsoft.com/en-us/purview/audit-log-enable-disable

---

- **ms365-cis-3.2.1 Ensure DLP policies are enabled**

  [FAIL]

Vulnerability Name	No DLP policies are configured. Sensitive data may be shared without restriction.
Section	3.2 Data Loss Prevention
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	No DLP policies are configured by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Resource Type	tenant

Finding Details

Data Loss Prevention (DLP) policies should be created and enabled to protect sensitive information from unauthorized sharing. At minimum, policies protecting common sensitive data types (PII, financial data, health information) should be in place.

Description

Data Loss Prevention (DLP) policies should be created and enabled to protect sensitive information from unauthorized sharing. At minimum, policies protecting common sensitive data types (PII, financial data, health information) should be in place.

Details

Rationale: DLP policies prevent accidental or intentional sharing of sensitive information such as credit card numbers, Social Security numbers, and health data. Without DLP policies, users may inadvertently share sensitive data through email, Teams, or SharePoint.

Impact: DLP policies may block or restrict some email messages and file sharing operations that contain sensitive data. Users may need to provide business justification to override DLP restrictions.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/security/informationProtection/sensitivityLabels

Or check Purview compliance portal:

https://compliance.microsoft.com → Data loss prevention > Policies

Compliant: At least one DLP policy is enabled.

Remediation:

Microsoft Purview compliance portal → Data loss prevention > Policies.

Create DLP policies for:

• U.S. Personally Identifiable Information (PII)

• U.S. Financial Data

• Health Insurance Portability and Accountability Act (HIPAA)

Or use industry-specific templates.

Reference: https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

---

ms365-cis-3.2.2 Ensure DLP policies are enabled for Microsoft Teams

[FAIL]

Vulnerability Name	No DLP policies found. Microsoft Teams DLP protection is not configured.
Section	3.2 Data Loss Prevention
Severity	High
Profiles	E5 Level 1
Default Value	DLP policies do not include Teams by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

DLP policies should be extended to cover Microsoft Teams chat and channel messages to prevent sensitive data from being shared through Teams conversations.

Description

DLP policies should be extended to cover Microsoft Teams chat and channel messages to prevent sensitive data from being shared through Teams conversations.

Details

Rationale: As Teams adoption increases, users may share sensitive information through chat messages and channels. DLP policies for Teams ensure that sensitive data is detected and protected in Teams conversations.

Impact: Teams messages containing sensitive data will be blocked or flagged. Users will receive policy tips when they attempt to share sensitive data.

Audit Procedure:

Microsoft Purview compliance portal:

Data loss prevention > Policies

Check each policy's location settings for Teams coverage.

Compliant: At least one DLP policy includes Teams as a location.

Remediation:

Microsoft Purview compliance portal → Data loss prevention > Policies.

Edit existing DLP policies or create new ones that include:

• Location: Microsoft Teams chat and channel messages

• Apply appropriate sensitive information type rules

Reference: https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams

---

● ms365-cis-3.3.1 Ensure sensitivity label policies are published

[FAIL]

Vulnerability Name	No sensitivity labels found. Content classification and protection via sensitivity labels is not configured.
Section	3.3 Information Protection
Severity	High

Profiles	E3 Level 1, E5 Level 1
Default Value	No sensitivity labels are configured by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Sensitivity labels allow users and administrators to classify and protect content based on its sensitivity. Sensitivity label policies must be published to make labels available to users.

Description

Sensitivity labels allow users and administrators to classify and protect content based on its sensitivity. Sensitivity label policies must be published to make labels available to users.

Details

Rationale: Sensitivity labels help protect sensitive data by enabling encryption, access controls, and content markings. Publishing label policies makes them available in Office apps, Teams, SharePoint, and Exchange.

Impact: Users will be prompted or required to apply sensitivity labels to content they create. This may require user training and change management.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/informationProtection/policy/labels

Check if labels exist and are configured.

Compliant: At least one sensitivity label policy is published.

Remediation:

Microsoft Purview compliance portal → Information protection > Labels.

Create sensitivity labels (e.g., Public, Internal, Confidential, Highly Confidential)

Create a label policy to publish the labels to users

Assign the policy to all users or specific groups

Reference: https://learn.microsoft.com/en-us/purview/sensitivity-labels

---

● ms365-cis-4.1 Ensure that devices without a compliance policy are marked as not compliant

[FAIL]

Vulnerability Name	No device compliance policies found in Intune. Devices may be considered compliant by default.
Section	4 Microsoft Intune
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Devices without compliance policy are marked as compliant by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft Intune should be configured so that devices without a compliance policy assigned are automatically marked as non-compliant. This ensures that all devices must meet compliance requirements to access corporate resources via Conditional Access.

Description

Microsoft Intune should be configured so that devices without a compliance policy assigned are automatically marked as non-compliant. This ensures that all devices must meet compliance requirements to access corporate resources via Conditional Access.

Details

Rationale: If devices without compliance policies are considered compliant, they can access corporate resources without meeting any security requirements. Marking them as non-compliant ensures no device can bypass compliance checks.

Impact: Devices that have not been assigned a compliance policy will be marked as non-compliant and may lose access to corporate resources if Conditional Access is enforced.

Audit Procedure:

Microsoft Intune admin center → Devices > Compliance policies > Compliance policy settings.

Verify 'Mark devices with no compliance policy assigned as' is set to 'Not compliant'.

Or via Microsoft Graph:

GET /deviceManagement/settings

Check deviceComplianceCheckinThresholdDays and secureByDefault (or equivalent) fields.

Remediation:

Microsoft Intune admin center → Devices > Compliance policies > Compliance policy settings.

Set 'Mark devices with no compliance policy assigned as' to 'Not compliant'.

Reference: https://learn.microsoft.com/en-us/intune/intune-service/protect/device-compliance-get-started

---

- **ms365-cis-4.2 Ensure that personal device enrollment is blocked in Microsoft Intune**
  [FAIL]

Vulnerability Name	No enrollment restriction policy found that blocks personal device enrollment.
Section	4 Microsoft Intune
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Personal device enrollment is allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Personal device enrollment in Microsoft Intune should be blocked to ensure only corporate-owned and managed devices can enroll. This prevents unmanaged personal devices from accessing corporate resources.

Odatatype:

- #microsoft.graph.deviceEnrollmentLimitConfiguration

Displayname:

- All users and all devices

Odatatype:

- #microsoft.graph.deviceEnrollmentPlatformRestrictionsConfiguration

Displayname:

- All users and all devices

Description

Personal device enrollment in Microsoft Intune should be blocked to ensure only corporate-owned and managed devices can enroll. This prevents unmanaged personal devices from accessing corporate resources.

Details

Rationale: Personal devices may not meet corporate security standards and could expose corporate data to risk. Restricting enrollment to corporate devices ensures all enrolled devices are under organizational control.

Impact: Employees will not be able to enroll personal devices into Intune or access corporate resources from personal devices via Intune-protected apps.

Audit Procedure:

Using Microsoft Graph:

GET /deviceManagement/deviceEnrollmentConfigurations

Look for enrollment restriction configuration with type 'singlePlatformRestriction' or 'defaultDeviceEnrollmentRestrictions'

Check platformRestrictions[windows].personalDeviceEnrollmentBlocked = true

Microsoft Intune admin center → Devices > Enrollment > Enrollment restrictions

Remediation:

Microsoft Intune admin center → Devices > Enrollment > Enrollment restrictions.

Edit the Default enrollment restriction:

• Device type restrictions: Block personal Windows devices

• Or: Block personal devices for all platforms based on requirements

Reference: https://learn.microsoft.com/en-us/intune/intune-service/enrollment/enrollment-restrictions-set

---

● ms365-cis-5.1.2.1 Ensure 'Per-user MFA' is disabled

[PASS]

Vulnerability Name	Per-user MFA is not enabled for any user. MFA should be enforced via Conditional Access policies.
Section	5.1.2 Users

Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Disabled (per-user MFA is off by default in new tenants with CA).
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Per-user MFA is a legacy method of enforcing MFA that should be replaced by Conditional Access or Security Defaults. When Conditional Access is in use, per-user MFA settings are ignored and can create confusion.

Users Checked:

- 2

Description

Per-user MFA is a legacy method of enforcing MFA that should be replaced by Conditional Access or Security Defaults. When Conditional Access is in use, per-user MFA settings are ignored and can create confusion.

Details

Rationale: Mixing per-user MFA with Conditional Access can result in users being prompted for MFA unexpectedly or bypassing intended security controls. Centralising MFA enforcement in Conditional Access provides consistent policy application.

Impact: Disabling per-user MFA requires that MFA is enforced via Conditional Access or Security Defaults. Ensure CA policies are in place before disabling.

Audit Procedure:

Using Microsoft Graph:
GET /users?$select=id,userPrincipalName,strongAuthenticationRequirements
(beta endpoint required)
Check: no user should have strongAuthenticationRequirements.state = 'enabled' or 'enforced'.

Alternatively via portal:
Azure portal → Microsoft Entra ID → Security > MFA > Per-user MFA.
Confirm no users have MFA Status of 'Enabled' or 'Enforced'.

Remediation:

Ensure Conditional Access MFA policies are in place.

Navigate to Microsoft Entra admin center → Users > All Users > Per-user MFA.

Select all users and disable per-user MFA.

Note: Do not disable per-user MFA until CA policies enforcing MFA are confirmed to be active.

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userstates

---

- **ms365-cis-5.1.2.2 Ensure third party integrated applications are not allowed**
  [FAIL]

Vulnerability Name	Users are allowed to register applications (allowedToCreateApps = True). Third-party apps can be registered without IT approval.
Section	5.1.2 Account Management
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Users can register applications by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Users should not be allowed to register or consent to third-party applications. This prevents unvetted applications from gaining access to organizational data through OAuth consent grants.

Allowedtocreateapps:

- True

Description

Users should not be allowed to register or consent to third-party applications. This prevents unvetted applications from gaining access to organizational data through OAuth consent grants.

Details

Rationale: Third-party applications registered by users can access organizational data with the permissions the user grants. Restricting app registration ensures only IT-approved applications can access organizational data.

Impact: Users will not be able to register new applications or consent to third-party applications. Applications needed by users must be pre-approved and deployed by IT administrators.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy

Check: defaultUserRolePermissions.allowedToCreateApps should be false

Remediation:

Microsoft Entra admin center → Identity > Users > User settings.

Set 'Users can register applications' to No.

Or via Microsoft Graph:

PATCH /policies/authorizationPolicy

{ 'defaultUserRolePermissions': { 'allowedToCreateApps': false } }

Reference: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/prevent-domain-hints-with-home-realm-discovery

---

ms365-cis-5.1.2.3 Ensure non-admin users cannot create tenants

[FAIL]

Vulnerability Name	Non-admin users are allowed to create tenants (allowedToCreateTenants = None).
Section	5.1.2 Account Management
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Non-admin users can create tenants by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Non-administrator users should not be allowed to create new Microsoft Entra ID tenants. Tenant creation should be restricted to administrators to prevent unauthorized tenant sprawl.

Description

Non-administrator users should not be allowed to create new Microsoft Entra ID tenants. Tenant creation should be restricted to administrators to prevent unauthorized tenant sprawl.

Details

Rationale: Allowing non-admin users to create tenants can result in shadow IT environments where organizational data is stored outside of governed and managed tenants.

Impact: Non-admin users will not be able to create new Entra ID tenants. All new tenants must be created by IT administrators.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy

Check: allowedToCreateTenants should be false

Remediation:

Microsoft Entra admin center → Identity > Users > User settings.

Set 'Restrict non-admin users from creating tenants' to Yes.

Or via Microsoft Graph:

PATCH /policies/authorizationPolicy

{ 'allowedToCreateTenants': false }

Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions

---

- **ms365-cis-5.1.2.4 Ensure access to the Entra administration portal is restricted**

  [MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure access to the Entra administration portal is restricted
Section	5.1.2 Account Management

Security Findings Report

Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Non-admin users can access the Entra admin portal by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Access to the Microsoft Entra administration portal should be restricted to administrators only. Non-admin users should not be able to access the Entra admin portal.

Description

Access to the Microsoft Entra administration portal should be restricted to administrators only. Non-admin users should not be able to access the Entra admin portal.

Details

Rationale: Restricting portal access reduces the information available to potential attackers who may compromise a regular user account. Non-admin users do not need access to the administrative portal.

Impact: Non-admin users will not be able to access the Microsoft Entra admin center portal.

Audit Procedure:

Microsoft Entra admin center → Identity > Users > User settings.

Check 'Restrict access to Microsoft Entra admin center' setting.

The setting 'Restrict non-admins from accessing the Entra admin portal' should be set to Yes.

Remediation:

Microsoft Entra admin center → Identity > Users > User settings.

Set 'Restrict access to Microsoft Entra admin center' to Yes.

Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions

---

ms365-cis-5.1.2.5 Ensure the option to remain signed in is hidden

[MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure the option to remain signed in is hidden
Section	5.1.2 Account Management
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	The 'Stay signed in?' prompt is shown by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The 'Stay signed in?' prompt allows users to maintain persistent browser sessions. This should be hidden to prevent long-lived sessions on shared or unmanaged devices.

Description

The 'Stay signed in?' prompt allows users to maintain persistent browser sessions. This should be hidden to prevent long-lived sessions on shared or unmanaged devices.

Details

Rationale: Persistent browser sessions on shared devices allow subsequent users to access corporate resources without re-authenticating. Hiding the 'Stay signed in?' option reduces the risk of session hijacking.

Impact: Users will not be prompted to stay signed in and will have shorter session lifetimes, requiring more frequent re-authentication.

Audit Procedure:

Microsoft Entra admin center (https://entra.microsoft.com) → Entra ID > Users > User settings.

Ensure 'Show keep user signed in' is set to No.

No Microsoft Graph or PowerShell field exposes this setting; CIS classifies this control as Manual.

Remediation:

Microsoft Entra admin center → Identity > Overview > Company branding.

Edit the default branding:

Set 'Show option to remain signed in' to No.

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

---

ms365-cis-5.1.2.6 Ensure LinkedIn account connections are disabled

[MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure LinkedIn account connections are disabled
Section	5.1.2 Account Management
Severity	Low

Profiles	E3 Level 2, E5 Level 2
Default Value	LinkedIn account connections are enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

LinkedIn account connections allow users to connect their Microsoft work account with their LinkedIn profile, sharing profile data between the two services. This should be disabled to prevent data leakage.

Description

LinkedIn account connections allow users to connect their Microsoft work account with their LinkedIn profile, sharing profile data between the two services. This should be disabled to prevent data leakage.

Details

Rationale: LinkedIn connections can expose employee data to LinkedIn's data processing and may allow data to flow between Microsoft 365 and LinkedIn, a third-party service not under organizational control.

Impact: Users will not be able to connect their Microsoft work account to LinkedIn or see LinkedIn profile information within Microsoft apps.

Audit Procedure:

Microsoft Entra admin center → Identity > Users > User settings.

Check 'LinkedIn account connections' setting.

Compliant: 'No' (disabled for all users).

Remediation:

Microsoft Entra admin center → Identity > Users > User settings.

Set 'LinkedIn account connections' to 'No'.

Reference: https://learn.microsoft.com/en-us/entra/identity/users/linkedin-user-consent

---

ms365-cis-5.1.3.1 Ensure a dynamic group for guest users is created

[FAIL]

Vulnerability Name	No dynamic group targeting guest users found. Guest users cannot be consistently targeted by policies.
Section	5.1.3 Groups
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	No dynamic group for guests exists by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

A dynamic group should be created that automatically includes all guest users in the tenant. This group can then be used in Conditional Access policies and access reviews to manage guest user access.

Totalgroupschecked:

- 3

Description

A dynamic group should be created that automatically includes all guest users in the tenant. This group can then be used in Conditional Access policies and access reviews to manage guest user access.

Details

Rationale: A dynamic group for guests enables consistent policy enforcement across all guest accounts without manual group maintenance. This group can be used as the target for stricter Conditional Access policies and access reviews.

Impact: Creating a dynamic group requires Azure AD Premium P1 licensing. The group membership is automatically maintained by the dynamic membership rule.

Audit Procedure:

Using Microsoft Graph:

GET /groups?$filter=membershipRule ne null&$select=id,displayName,membershipRule,membershipRuleProcessingState

Look for a group with membershipRule that includes user.userType -eq 'Guest'.

Remediation:

Microsoft Entra admin center → Identity > Groups > New group.

- Group type: Security or Microsoft 365
- Membership type: Dynamic User
- Dynamic query: user.userType -eq 'Guest'

This group can then be used in Conditional Access and access reviews.

Reference: https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership

---

● ms365-cis-5.1.3.2 Ensure users can not create security groups

[FAIL]

Vulnerability Name	Users are allowed to create security groups (allowedToCreateSecurityGroups = True).

Security Findings Report

Section	5.1.3 Groups
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Users can create security groups by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Non-administrator users should not be able to create security groups. Group creation should be restricted to administrators to maintain control over group-based access assignments.

Allowedtocreatesecuritygroups:

- True

Description

Non-administrator users should not be able to create security groups. Group creation should be restricted to administrators to maintain control over group-based access assignments.

Details

Rationale: Unrestricted security group creation can lead to group sprawl and make it difficult to manage access control. Restricting creation to administrators ensures groups are created with proper governance.

Impact: Users will not be able to create security groups. They must request group creation from IT administrators.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy
Check: defaultUserRolePermissions.allowedToCreateSecurityGroups should be false

Remediation:
Microsoft Entra admin center → Identity > Groups > General.
Set 'Users can create security groups in Microsoft Entra admin centers, API or PowerShell' to No.

Or via Microsoft Graph:
PATCH /policies/authorizationPolicy
{ 'defaultUserRolePermissions': { 'allowedToCreateSecurityGroups': false } }

Reference: https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management

---

- **ms365-cis-5.1.4.1 Ensure the ability to join devices is restricted**
  [FAIL]

Vulnerability Name	Device join to Entra ID is not restricted. All users may be able to join devices.
Section	5.1.4 Devices
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	All users can join devices to Entra ID by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Resource Type	tenant

Finding Details

The ability to join devices to Microsoft Entra ID should be restricted to administrators or specific approved groups. Unrestricted device join allows any user to join their personal devices to the tenant.

Description

The ability to join devices to Microsoft Entra ID should be restricted to administrators or specific approved groups. Unrestricted device join allows any user to join their personal devices to the tenant.

Details

Rationale: Restricting device join prevents users from adding unmanaged personal devices to the tenant's Entra ID, which would allow those devices to access corporate resources through device-based Conditional Access.

Impact: Users will not be able to join their personal devices to Entra ID without administrator involvement or being in an approved group.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/policies/deviceRegistrationPolicy

Check azureADJoin.allowedToJoin.@odata.type:

• 'AllowedToJoinAllUsersOrGroups' with specific groups = partial restriction

• 'AllowedToJoinNoUsers' or admin-only = compliant

• 'AllowedToJoinAllUsersOrGroups' with all users = non-compliant

Remediation:

Microsoft Entra admin center → Identity > Devices > Device settings.

Set 'Users may join devices to Microsoft Entra' to:

• 'None' (only administrators) or

• 'Selected' (specific groups only)

Reference: https://learn.microsoft.com/en-us/entra/identity/devices/device-join-plan

ms365-cis-5.1.4.2 Ensure the maximum number of devices per user is limited

[PASS]

Vulnerability Name	Maximum devices per user is limited to 50.
Section	5.1.4 Devices
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Maximum devices per user is set to 50 by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The maximum number of devices a user can register in Microsoft Entra ID should be limited. Unlimited device registration allows users to register many personal devices.

Userdevicequota:

- 50

Description

The maximum number of devices a user can register in Microsoft Entra ID should be limited. Unlimited device registration allows users to register many personal devices.

Details

Rationale: Limiting device registration reduces the number of unmanaged devices that can gain access through device-based policies and reduces the attack surface by limiting the number of registered devices per user.

Impact: Users who have already registered the maximum number of devices will be unable to register additional devices.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/policies/deviceRegistrationPolicy

Check userDeviceQuota field.

Compliant: userDeviceQuota is not Unlimited (e.g., 5 or fewer).

Remediation:

Microsoft Entra admin center → Identity > Devices > Device settings.

Set 'Maximum number of devices per user' to a specific limit (e.g., 5 or fewer).

Reference: https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities

---

● ms365-cis-5.1.4.3 Ensure Global Administrator is not added as a local administrator during Entra join

[FAIL]

Vulnerability Name	Global Administrators are added as local admins on Entra-joined devices (enableGlobalAdmins = true).
Section	5.1.4 Devices
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Global Admins are added as local admins during Entra join by default.

Security Findings Report

Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

During Microsoft Entra join, the Global Administrator role members should not be automatically added as local administrators on the joined devices. This reduces the attack surface by limiting local admin access.

Azureadjoin.Localadmins.Enableglobaladmins:

- True

Description

During Microsoft Entra join, the Global Administrator role members should not be automatically added as local administrators on the joined devices. This reduces the attack surface by limiting local admin access.

Details

Rationale: If Global Administrators are automatically added as local admins on Entra-joined devices, compromising one device could be used to escalate privileges or harvest credentials of the local admin account.

Impact: Global Administrators will not be local admins on Entra-joined devices. Alternative management approaches (LAPS, Intune policies) should be used.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/policies/deviceRegistrationPolicy

Check azureADJoin.localAdmins.enableGlobalAdmins.

Ensure enableGlobalAdmins is False.

Microsoft Entra admin center → Identity > Devices > Device settings:

'Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)' should be No.

Remediation:

Microsoft Entra admin center → Identity > Devices > Device settings.

In 'Additional local administrators on all Microsoft Entra joined devices':

Do not include Global Administrator role.

Use LAPS or Intune for local admin management instead.

Reference: https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin

---

- **ms365-cis-5.1.4.4 Ensure local administrator assignment is limited during Entra join** **[FAIL]**

Vulnerability Name	Registering users are added as local administrators on Entra-joined devices by default (localAdminType = None).
Section	5.1.4 Devices
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Registering user is added as local administrator by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Resource Type	tenant

Finding Details

During Microsoft Entra join, the user who joins the device is automatically added as a local administrator. This should be restricted so that only designated accounts have local admin rights.

Description

During Microsoft Entra join, the user who joins the device is automatically added as a local administrator. This should be restricted so that only designated accounts have local admin rights.

Details

Rationale: Automatic local admin assignment to joining users can result in a large number of devices with the user's account as local admin. This increases the attack surface and risk of privilege escalation.

Impact: Users will not automatically be local admins on devices they join. LAPS or Intune-managed local admin policies should be used instead.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/policies/deviceRegistrationPolicy

Check azureADJoin.localAdmins.registeringUsers.localAdminType

Compliant: localAdminType = 'None' or not set to 'Administrator'

Remediation:

Microsoft Entra admin center → Identity > Devices > Device settings.

Set 'Registering user is added as local administrator' to None/Disabled.

Use LAPS or Intune endpoint privilege management instead.

Reference: https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin

---

- **ms365-cis-5.1.4.5 Ensure Local Admin Password Solution (LAPS) is enabled**
  [FAIL]

Vulnerability Name	Microsoft Entra LAPS is disabled (localAdminPassword.isEnabled = false). Local admin passwords are not being managed and rotated automatically.
Section	5.1.4 Devices
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	LAPS is disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft Entra ID LAPS should be enabled to automatically manage and rotate local administrator passwords on Entra-joined and Entra-registered devices.

Description

Microsoft Entra ID LAPS should be enabled to automatically manage and rotate local administrator passwords on Entra-joined and Entra-registered devices.

Details

Rationale: LAPS ensures that each device has a unique, randomly generated local admin password that is rotated regularly. This prevents lateral movement if a local admin password is compromised on one device.

Impact: Enabling LAPS requires devices to be configured to use it. Existing local admin passwords will be replaced by LAPS-managed passwords.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/policies/deviceRegistrationPolicy

Check localAdminPassword.isEnabled = true

Remediation:

Microsoft Entra admin center → Identity > Devices > Device settings.

Enable 'Enable Microsoft Entra Local Administrator Password Solution (LAPS)'.

Then configure LAPS settings in Intune:

Microsoft Intune admin center → Endpoint security > Account protection > Create policy > Windows LAPS

Reference: https://learn.microsoft.com/en-us/entra/identity/devices/howto-manage-local-admin-passwords

---

- **ms365-cis-5.1.4.6 Ensure users are restricted from recovering BitLocker keys**
  [FAIL]

Vulnerability Name	Users can recover BitLocker keys for their owned devices (allowedToReadBitlockerKeysForOwnedDevice = true).
Section	5.1.4 Devices
Severity	High
Profiles	E3 Level 2, E5 Level 2
Default Value	Users can retrieve BitLocker keys by default.
Asset Label	universal
Date Discovered	Aug 05, 2026

Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Regular users should not be able to retrieve BitLocker recovery keys from the Microsoft Entra portal. Access to recovery keys should be restricted to IT administrators.

Defaultuserrolepermissions.Allowedtoreadbitlockerkeysforowneddevice:

- True

Description

Regular users should not be able to retrieve BitLocker recovery keys from the Microsoft Entra portal. Access to recovery keys should be restricted to IT administrators.

Details

Rationale: BitLocker recovery keys allow bypassing full disk encryption. If a non-admin user can retrieve their device's recovery key, they could share it with an attacker or use it to access data on a stolen device.

Impact: End users who have lost access to their devices and need to recover them will need to contact IT support for BitLocker recovery assistance.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy

(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions

Ensure AllowedToReadBitlockerKeysForOwnedDevice is False.

Microsoft Entra admin center → Identity > Devices > Device settings:

'Restrict users from recovering the BitLocker key(s) for their owned devices' should be Yes.

Remediation:

Microsoft Entra admin center → Identity > Devices > Device settings.

Set 'Restrict users from recovering the BitLocker key(s) for their owned devices' to Yes.

Reference: https://learn.microsoft.com/en-us/entra/identity/devices/device-management-azure-portal

---

● ms365-cis-5.1.5.1 Ensure user consent to apps accessing company data on their behalf is not allowed

[FAIL]

Vulnerability Name	Users are allowed to consent to application permissions. Permissive grant policies found
Section	5.1.5 Applications
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Users can consent to apps from verified publishers by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Users are allowed to consent to application permissions. Permissive grant policies found: ['ManagePermissionGrantsForSelf.microsoft-user-default-recommended', 'ManagePermissionGrantsForSelf.microsoft-user-default-allow-consent-apps']

Permissiongrantpoliciesassigned:

- ManagePermissionGrantsForSelf.microsoft-user-default-recommended
- ManagePermissionGrantsForSelf.microsoft-user-default-allow-consent-apps

- ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-team
- ManagePermissionGrantsForOwnedResource.microsoft-dynamically-managed-permissions-for-chat

Description

Users should not be allowed to consent to applications accessing company data on their behalf. Only administrators should be able to grant application permissions to prevent unauthorized data access.

Details

Rationale: User consent to apps can result in third-party applications gaining access to organizational data. Restricting consent to admins ensures all app permissions are reviewed and approved by IT.

Impact: Users will not be able to consent to new application permissions. They must request admin consent for applications they need.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy

Check: defaultUserRolePermissions.permissionGrantPoliciesAssigned

Compliant: empty array or no permissive grant policies

Remediation:

Microsoft Entra admin center → Identity > Enterprise applications > Consent and permissions > User consent settings.

Set 'User consent for applications' to 'Do not allow user consent'.

Enable admin consent workflow so users can request consent:

Identity > Enterprise applications > Consent and permissions > Admin consent settings > Enable admin consent requests

Reference: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent

---

- **ms365-cis-5.1.5.2 Ensure the admin consent workflow is enabled**
  [FAIL]

Security Findings Report

Vulnerability Name	Admin consent workflow is disabled (isEnabled = false). Users cannot request admin approval for applications.
Section	5.1.5 Applications
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Admin consent workflow is disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The admin consent workflow should be enabled to allow users to request admin approval for applications they need. Without this workflow, users may try to work around consent restrictions.

Description

The admin consent workflow should be enabled to allow users to request admin approval for applications they need. Without this workflow, users may try to work around consent restrictions.

Details

Rationale: When user consent is disabled, users still need to use applications. The admin consent workflow provides a formal process for users to request access, maintaining security while avoiding friction.

Impact: Users will be able to submit requests for application consent to administrators. Admins will need to review and approve or deny requests.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/policies/adminConsentRequestPolicy

Check: isEnabled = true

Remediation:

Microsoft Entra admin center → Identity > Enterprise applications > Consent and permissions > Admin consent settings.

Enable 'Users can request admin consent to apps they are unable to consent to' and configure reviewers.

Reference: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-admin-consent-workflow

---

- **ms365-cis-5.1.6.1 Ensure that collaboration invitations are sent to allowed domains only** **[FAIL]**

Vulnerability Name	No B2B invitation domain policy is configured, so the tenant is at its default of allowing collaboration invitations to be sent to any domain.
Section	5.1.6 Guest Access
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Invitations can be sent to all external domains by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026

Security Findings Report

Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External collaboration invitations should be restricted to approved domains. This prevents users from inviting external users from unapproved or potentially risky domains.

Description

External collaboration invitations should be restricted to approved domains. This prevents users from inviting external users from unapproved or potentially risky domains.

Details

Rationale: Restricting collaboration to approved domains reduces the risk of data being shared with unauthorized external parties and ensures that collaboration only happens with trusted partners.

Impact: Users will not be able to invite external users from non-approved domains. Only users from approved partner domains can be invited.

Audit Procedure:

Using Microsoft Graph:

GET /beta/legacy/policies

Filter for type == 'B2BManagementPolicy'; parse the JSON-encoded 'definition' field for B2BManagementPolicy.InvitationsAllowedAndBlockedDomainsPolicy.

Compliant: an AllowedDomains property is present (empty, or listing only approved domains) AND no BlockedDomains property is present.

Non-compliant: a BlockedDomains property is present.

Microsoft Entra admin center → Identity > External Identities > External collaboration settings → 'Allow invitations only to the specified domains' with approved Target domains.

Remediation:

Microsoft Entra admin center → Identity > External identities > External collaboration settings.

In 'Collaboration restrictions', select 'Allow invitations only to the specified domains' and add approved domains.

Reference: https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list

---

ms365-cis-5.1.6.2 Ensure guest user access is restricted

[PASS]

Vulnerability Name	Guest user access is set to Restricted Guest (most restrictive). guestUserRoleId = 10dae51f-b6af-4016-8d66-8c2a99b929b3
Section	5.1.6 Guest Access
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Guest user access is set to Guest User level by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Guest user access should be restricted to 'Restricted Guest User' permissions to minimize the amount of directory information guest users can access and enumerate.

Guestuserroleid:

- 10dae51f-b6af-4016-8d66-8c2a99b929b3

Description

Guest user access should be restricted to 'Restricted Guest User' permissions to minimize the amount of directory information guest users can access and enumerate.

Details

Rationale: By default, guest users have the same permissions as regular users to enumerate directory objects. Restricting guest access prevents guests from enumerating all users, groups, and other directory objects.

Impact: Guest users will have limited access to the directory and may not be able to enumerate other users or groups. Some integration scenarios may need to be adjusted.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy

Check guestUserRoleId:

• 10dae51f-b6af-4016-8d66-8c2a99b929b3 = Restricted Guest (compliant)

• bf6e4e74-7941-46e8-9c5a-fef2b3e9d6dd = Guest User (partially compliant)

• Other/null = Member-like access (non-compliant)

Remediation:

Microsoft Entra admin center → Identity > External identities > External collaboration settings.

Set 'Guest user access' to 'Guest users have limited access to properties and memberships of directory objects' (most restrictive).

Reference: https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure

---

● ms365-cis-5.1.6.3 Ensure guest invitations are limited to the Guest Inviter role

[FAIL]

Vulnerability Name	Guest invitations are not properly restricted (allowInvitesFrom = everyone). Should be 'adminsAndGuestInviters' or more restrictive.
Section	5.1.6 Guest Access

Security Findings Report

Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Members can invite guest users by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Only users with the Guest Inviter role or administrators should be allowed to invite external users. This prevents any user from inviting external guests without proper approval.

Allowinvitesfrom:

- everyone

Description

Only users with the Guest Inviter role or administrators should be allowed to invite external users. This prevents any user from inviting external guests without proper approval.

Details

Rationale: Allowing all users to invite guests can result in uncontrolled guest access to organizational resources. Restricting invitations ensures that guest access is properly governed and tracked.

Impact: Regular users will not be able to invite external guests. Only users with the Guest Inviter role or admin roles can send invitations.

Audit Procedure:

Using Microsoft Graph:

GET /policies/authorizationPolicy

Check allowInvitesFrom:

• 'adminsAndGuestInviters' = compliant
• 'admins' = compliant (most restrictive)
• 'none' = compliant (no invitations allowed)
• 'everyone' = non-compliant

Remediation:
Microsoft Entra admin center → Identity > External identities > External collaboration settings.
Set 'Guest invite settings' to 'Only users assigned to specific admin roles can invite guest users'.

Reference: https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure

---

● ms365-cis-5.1.8.1 Ensure password hash synchronization is enabled for hybrid environments

[MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure password hash synchronization is enabled for hybrid environments
Section	5.1.8 Identity Security
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Depends on hybrid configuration choices during Entra Connect setup.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Resource Type	tenant

Finding Details

For hybrid environments using Microsoft Entra Connect, password hash synchronization should be enabled. This allows leaked credential detection and provides a fallback authentication mechanism.

Description

For hybrid environments using Microsoft Entra Connect, password hash synchronization should be enabled. This allows leaked credential detection and provides a fallback authentication mechanism.

Details

Rationale: Password hash synchronization enables Entra ID Protection to detect leaked credentials by comparing synchronized password hashes against known compromised password lists. It also provides authentication resilience if federation services are unavailable.

Impact: Enabling password hash sync may require changes to the Entra Connect configuration and on-premises infrastructure.

Audit Procedure:

On the Microsoft Entra Connect server:

Open Microsoft Entra Connect configuration wizard

Check if 'Password hash synchronization' is enabled

Or via Microsoft Entra Connect Health:

Azure portal → Microsoft Entra Connect Health

Verify Password Hash Sync is shown as active

Remediation:

On the Microsoft Entra Connect server:

Run the Microsoft Entra Connect configuration wizard

Under Optional features, enable 'Password hash synchronization'

Complete the wizard and verify sync is working

Reference: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization

● ms365-cis-5.2.2.1 Ensure multifactor authentication is enabled for all users in administrative roles

[FAIL]

Vulnerability Name	No enabled Conditional Access policy found that requires MFA for administrative roles. (0 total policies found, 0 enabled)
Section	5.2.2 Risk-based Conditional Access
Severity	Critical
Profiles	E3 Level 1, E5 Level 1
Default Value	No MFA policy by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

MFA for privileged accounts is one of the most impactful security controls available. A Conditional Access policy must be enabled that targets users in administrative directory roles and requires MFA as a grant control.

Description

MFA for privileged accounts is one of the most impactful security controls available. A Conditional Access policy must be enabled that targets users in administrative directory roles and requires MFA as a grant control.

Details

Rationale: Administrative accounts with elevated privileges are high-value targets. Enforcing MFA dramatically reduces the risk of account compromise from phishing, password spray, or credential theft attacks.

Impact: Administrative users will be required to complete MFA on every sign-in (unless a 'sign-in frequency' policy manages session lifetime). Ensure MFA methods are registered before enforcing.

Audit Procedure:

Using Microsoft Graph:

GET /identity/conditionalAccess/policies

Look for an enabled policy that:

• Targets 'All' users OR explicitly includes directory role members.

• Has grantControls.builtInControls containing 'mfa'.

• Is not in 'reportOnly' mode (state must be 'enabled').

Remediation:

Create a Conditional Access policy:

Entra admin center → Protection > Conditional Access > New policy.

Assignments: Users → Select roles → All administrator roles.

Target resources: All cloud apps.

Grant: Require multifactor authentication.

Enable the policy.

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa

---

- **ms365-cis-5.2.2.2 Ensure multifactor authentication is enabled for all users**

  [FAIL]

Vulnerability Name	No enabled Conditional Access policy requires MFA for ALL users. Reviewed 0 policies.

Security Findings Report

Section	5.2.2 Risk-based Conditional Access
Severity	Critical
Profiles	E3 Level 1, E5 Level 1
Default Value	No MFA policy by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

All users, not just administrators, should be required to complete MFA. This is enforced via a Conditional Access policy targeting all cloud apps and requiring MFA as a grant control.

Description

All users, not just administrators, should be required to complete MFA. This is enforced via a Conditional Access policy targeting all cloud apps and requiring MFA as a grant control.

Details

Rationale: Non-administrative accounts are also targeted by attackers. Enforcing MFA for all users significantly reduces the risk of successful credential-based attacks such as phishing and password spraying.

Impact: All users will be required to register and use MFA. Allow time for MFA registration before enforcing the policy. Consider a staged rollout.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy where:

• conditions.users.includeUsers = ['All'] (or equivalent)

• conditions.applications.includeApplications = ['All']
• grantControls.builtInControls contains 'mfa'
• state = 'enabled' (not 'reportOnly')

Remediation:

Create a Conditional Access policy:

Entra admin center → Protection > Conditional Access > New policy.

Assignments: Users → All users (exclude emergency access accounts).

Target resources: All cloud apps.

Grant: Require multifactor authentication.

Enable the policy.

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-all-users-mfa

---

● ms365-cis-5.2.2.3 Ensure legacy authentication is blocked via Conditional Access [FAIL]

Vulnerability Name	No enabled Conditional Access policy found that blocks legacy authentication. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Critical
Profiles	E3 Level 1, E5 Level 1
Default Value	Legacy authentication is allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026

Security Findings Report

Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

A Conditional Access policy should block legacy authentication protocols. Legacy auth (Basic Auth, POP, IMAP, SMTP, MAPI, EAS without MFA) cannot enforce MFA and should be blocked.

Description

A Conditional Access policy should block legacy authentication protocols. Legacy auth (Basic Auth, POP, IMAP, SMTP, MAPI, EAS without MFA) cannot enforce MFA and should be blocked.

Details

Rationale: Legacy authentication protocols do not support modern authentication methods like MFA. Password spraying and brute force attacks primarily target legacy auth endpoints. Blocking legacy auth forces users to use modern, MFA-capable authentication.

Impact: Legacy email clients and apps that use Basic Authentication will no longer be able to connect. Users must migrate to OAuth-capable email clients.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy that:

• state = 'enabled'

• grantControls.builtInControls contains 'block'

• conditions.clientAppTypes includes legacy auth protocols:

exchangeActiveSync, other, or similar legacy types

Remediation:

Create a Conditional Access policy:

Entra admin center → Protection > Conditional Access > New policy

Users: All users (with no exclusions except break-glass)

Cloud apps: All cloud apps

Conditions: Client apps → Exchange ActiveSync clients + Other clients

Grant: Block access

Enable the policy

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/block-legacy-authentication

---

● ms365-cis-5.2.2.4 Ensure sign-in frequency and persistent browser session for admins is configured

[FAIL]

Vulnerability Name	No enabled Conditional Access policy with sign-in frequency configured for admin roles found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	No session frequency restriction on admin sessions by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Administrative accounts should have a sign-in frequency policy that requires re-authentication after a set period (e.g., every hour) and should not allow persistent browser sessions.

Description

Administrative accounts should have a sign-in frequency policy that requires re-authentication after a set period (e.g., every hour) and should not allow persistent browser sessions.

Details

Rationale: Limiting session lifetime for admins reduces the risk of session hijacking. Short sign-in frequency ensures admins frequently re-authenticate, reducing the window of opportunity for attackers.

Impact: Administrative users will be required to re-authenticate more frequently and browser sessions will not persist, requiring re-authentication when reopening the browser.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy targeting admin roles with:

• sessionControls.signInFrequency.isEnabled = true

• sessionControls.persistentBrowser.isEnabled = true (and mode = never)

Remediation:

Create a Conditional Access policy:

Target: Admin directory roles

Session: Sign-in frequency = every 1 hour

Session: Persistent browser session = never persistent

Enable the policy

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-session-lifetime

---

- **ms365-cis-5.2.2.5 Ensure phishing-resistant MFA is required for admins**
  [FAIL]

Vulnerability Name	No enabled CA policy with phishing-resistant authentication strength for admin roles found. Reviewed 0 policies.

Security Findings Report

Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E5 Level 2
Default Value	No phishing-resistant MFA requirement by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Administrative accounts should be required to use phishing-resistant MFA methods (FIDO2 security keys or Windows Hello for Business) via a Conditional Access policy with authentication strength.

Description

Administrative accounts should be required to use phishing-resistant MFA methods (FIDO2 security keys or Windows Hello for Business) via a Conditional Access policy with authentication strength.

Details

Rationale: Standard MFA methods like SMS OTP are susceptible to real-time phishing attacks (AiTM). Phishing-resistant MFA methods eliminate this risk by binding authentication to the legitimate site.

Impact: Administrative users must register phishing-resistant MFA methods (FIDO2 keys or Windows Hello). This may require device and hardware investments.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy targeting admin roles with:

• grantControls.authenticationStrength.displayName containing 'Phishing-resistant' or a custom strength requiring FIDO2/WHfB

Remediation:

Create a Conditional Access policy:

Target: All administrator roles

Grant: Require authentication strength

Select: Phishing-resistant MFA

Enable the policy

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa

---

● ms365-cis-5.2.2.6 Ensure Identity Protection user risk policies are configured [FAIL]

Vulnerability Name	No enabled CA policy with user risk level conditions found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E5 Level 2
Default Value	No user risk policies configured by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Security Findings Report

Resource Type	tenant

Finding Details

A Conditional Access policy should be configured that uses Identity Protection user risk signals to require MFA or block access for high-risk users.

Description

A Conditional Access policy should be configured that uses Identity Protection user risk signals to require MFA or block access for high-risk users.

Details

Rationale: Identity Protection user risk policies detect compromised credentials and risky user behavior. Requiring remediation for high-risk users helps prevent account compromise from spreading.

Impact: Users flagged as high risk will be required to change their password or complete MFA before accessing resources.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy with:

• conditions.userRiskLevels = ['high'] or ['medium', 'high']

Remediation:

Create a Conditional Access policy:

Users: All users

Conditions: User risk = High

Grant: Require password change + MFA

Enable the policy

Requires Microsoft Entra ID P2 (E5) licensing.

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

- **ms365-cis-5.2.2.7 Ensure Identity Protection sign-in risk policies are configured [FAIL]**

Vulnerability Name	No enabled CA policy with sign-in risk level conditions found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E5 Level 2
Default Value	No sign-in risk policies configured by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

A Conditional Access policy should use Identity Protection sign-in risk signals to require MFA for risky sign-ins.

Description

A Conditional Access policy should use Identity Protection sign-in risk signals to require MFA for risky sign-ins.

Details

Rationale: Sign-in risk policies detect anomalous sign-in behaviors like impossible travel, anonymous IP usage, and malware-linked IPs. Requiring MFA for risky sign-ins helps prevent unauthorized access.

Impact: Users with risky sign-in patterns will be required to complete MFA or have their sign-in blocked.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy with:

• conditions.signInRiskLevels = ['high'] or ['medium', 'high']

Remediation:

Create a Conditional Access policy:

Users: All users

Conditions: Sign-in risk = High

Grant: Require MFA

Enable the policy

Requires Microsoft Entra ID P2 (E5) licensing.

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

---

- **ms365-cis-5.2.2.8 Ensure sign-in risk is blocked for medium and high risk**
  [FAIL]

Vulnerability Name	No enabled CA policy that blocks/requires MFA for both medium and high sign-in risk found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E5 Level 2
Default Value	No sign-in risk blocking policy configured by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

A Conditional Access policy should block or require strong remediation for medium and high sign-in risk levels detected by Identity Protection.

Description

A Conditional Access policy should block or require strong remediation for medium and high sign-in risk levels detected by Identity Protection.

Details

Rationale: Medium and high sign-in risk indicates a high probability that the sign-in is not from the legitimate user. Blocking or requiring immediate remediation for these sign-ins prevents unauthorized access.

Impact: Users with medium or high sign-in risk will be blocked or required to complete additional verification before accessing resources.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy with:

• conditions.signInRiskLevels includes both 'medium' and 'high'

• grantControls.builtInControls contains 'block' or 'mfa'

Remediation:

Create a Conditional Access policy:

Users: All users

Conditions: Sign-in risk >= Medium

Grant: Block access (or Require MFA)

Enable the policy

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

---

ms365-cis-5.2.2.9 Ensure a managed device is required for authentication

[FAIL]

Vulnerability Name	No enabled CA policy requiring a managed device found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	No device compliance requirement for authentication by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

A Conditional Access policy should require that users authenticate only from managed (Intune-compliant or Hybrid Entra joined) devices to access corporate resources.

Description

A Conditional Access policy should require that users authenticate only from managed (Intune-compliant or Hybrid Entra joined) devices to access corporate resources.

Details

Rationale: Requiring managed devices ensures that corporate data is only accessed from devices that meet security compliance requirements, reducing the risk from unmanaged personal devices.

Impact: Users accessing corporate resources from personal or non-compliant devices will be blocked. All users must have a compliant managed device.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy with:

• grantControls.builtInControls contains 'compliantDevice' or 'domainJoinedDevice'

Remediation:

Create a Conditional Access policy:

Users: All users

Cloud apps: All cloud apps

Grant: Require device to be marked as compliant OR Require Hybrid Entra joined device

Enable the policy

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-compliant-device

---

- **ms365-cis-5.2.2.10 Ensure managed device is required to register security info**
  [FAIL]

Vulnerability Name	No enabled CA policy requiring managed device for security info registration found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E3 Level 2, E5 Level 2

Default Value	No device requirement for security info registration by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Users should only be able to register MFA security information (phone numbers, authenticator apps) from managed, compliant devices. This prevents attackers who compromise credentials from registering new MFA methods.

Description

Users should only be able to register MFA security information (phone numbers, authenticator apps) from managed, compliant devices. This prevents attackers who compromise credentials from registering new MFA methods.

Details

Rationale: If users can register MFA methods from any device, an attacker with stolen credentials can register their own MFA method and gain full account access. Requiring a managed device for registration prevents this.

Impact: Users must use a compliant device to register or update MFA methods. IT must assist users who need to register from a new device.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy that:

• targets the MFA registration app (or uses userActions registerSecurityInfo)

• requires compliantDevice or domainJoinedDevice

Remediation:

Create a Conditional Access policy:

Users: All users

Target resources: User actions > Register security information

Grant: Require device to be marked as compliant

Enable the policy

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-registration

---

- **ms365-cis-5.2.2.11 Ensure sign-in frequency for Intune Enrollment is set to every time [FAIL]**

Vulnerability Name	No enabled CA policy with 'every time' sign-in frequency for Intune enrollment found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	No sign-in frequency for Intune enrollment by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

A Conditional Access policy should require re-authentication every time for Microsoft Intune Enrollment to prevent device enrollment from cached credentials.

Description

A Conditional Access policy should require re-authentication every time for Microsoft Intune Enrollment to prevent device enrollment from cached credentials.

Details

Rationale: Requiring authentication at every Intune enrollment prevents enrollment using cached or stolen credentials, ensuring only the legitimate device owner can enroll their device.

Impact: Users must authenticate each time they enroll a device in Intune. This prevents bulk enrollment without active user consent.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy that:

• targets Intune Enrollment app (d4ebce55-015a-49b5-a083-c84d1797ae8c)

• sessionControls.signInFrequency.type = 'everyTime'

Remediation:

Create a Conditional Access policy:

Target resources: Select apps > Microsoft Intune Enrollment

Session: Sign-in frequency = Every time

Enable the policy

Reference: https://learn.microsoft.com/en-us/intune/intune-service/enrollment/multi-factor-authentication

---

- **ms365-cis-5.2.2.12 Ensure the device code sign-in flow is blocked**

  [FAIL]

Vulnerability Name	No enabled CA policy blocking device code flow found. Reviewed 0 policies.
Section	5.2.2 Conditional Access
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Device code flow is allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The device code flow authentication method should be blocked via Conditional Access. Device code flow is used by phishing attacks (device code phishing) to steal authentication tokens.

Description

The device code flow authentication method should be blocked via Conditional Access. Device code flow is used by phishing attacks (device code phishing) to steal authentication tokens.

Details

Rationale: Device code flow phishing tricks users into entering a device code provided by an attacker, allowing the attacker to obtain access tokens without needing the user's credentials.

Impact: Legitimate use cases for device code flow (e.g., TV apps, input-limited devices) will be blocked. Alternative authentication methods must be used.

Audit Procedure:

GET /identity/conditionalAccess/policies

Look for an enabled policy with:

• conditions.authenticationFlows.transferMethods includes 'deviceCodeFlow'

• grantControls.builtInControls contains 'block'

Remediation:

Create a Conditional Access policy:

Users: All users

Conditions: Authentication flows > Device code flow

Grant: Block access

Enable the policy

Reference: https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-conditions-authentication-flows

---

- **ms365-cis-5.2.3.1 Ensure Microsoft Authenticator MFA fatigue protections are enabled [FAIL]**

Vulnerability Name	Microsoft Authenticator MFA fatigue protections are not fully enabled: Additional context (displayAppInfo) state = 'default' (should be 'enabled')
Section	5.2.3 Authentication Methods
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Number matching may be enabled but additional context may not be.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Microsoft Authenticator should be configured with MFA fatigue protections: number matching (shows a number the user must match) and additional context (shows application name and location). These features prevent MFA push bombing attacks.

State:

- enabled

Numbermatchingrequiredstate:

- enabled

Displayappinformationrequiredstate:

- default

Description

Microsoft Authenticator should be configured with MFA fatigue protections: number matching (shows a number the user must match) and additional context (shows application name and location). These features prevent MFA push bombing attacks.

Details

Rationale: MFA fatigue attacks flood users with push notifications until they accidentally approve one. Number matching and additional context require users to actively verify the sign-in request, defeating these attacks.

Impact: Users will need to look at a number on the sign-in screen and enter it in the Authenticator app, adding a small amount of friction to MFA.

Audit Procedure:

GET /policies/authenticationMethodsPolicy

In authenticationMethodConfigurations:

Find microsoftAuthenticator method

Check featureSettings.numberMatchingRequiredState.state = 'enabled'

Check featureSettings.displayAppInformationRequiredState.state = 'enabled'

Remediation:
Microsoft Entra admin center → Protection > Authentication methods > Microsoft Authenticator.
Enable 'Require number matching' and 'Show additional context in notifications'.

PATCH /policies/authenticationMethodsPolicy
Update microsoftAuthenticator configuration with numberMatchingRequiredState = enabled

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-number-match

---

- **ms365-cis-5.2.3.2 Ensure custom banned passwords lists are used**
  [FAIL]

Vulnerability Name	No custom banned password list is configured for this tenant (Password Rule Settings group setting does not exist).
Section	5.2.3 Authentication Methods
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Custom banned passwords are not configured by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Security Findings Report

Resource Type	tenant

Finding Details

Microsoft Entra Password Protection should be configured with a custom banned password list specific to the organization. This prevents users from using company-specific weak passwords.

Description

Microsoft Entra Password Protection should be configured with a custom banned password list specific to the organization. This prevents users from using company-specific weak passwords.

Details

Rationale: Default banned password lists may not include organization-specific terms (company name, product names, locations) that attackers commonly use in password spray attacks. Custom lists enhance protection.

Impact: Users attempting to set passwords that match custom banned terms will be rejected and must choose a different password.

Audit Procedure:

Microsoft Graph:

GET /groupSettings, filter templateId == 5cf42378-d67d-4f36-ba46-e8b86229381d (Password Rule Settings)

Ensure EnableBannedPasswordCheck is True and BannedPasswordList is populated.

Microsoft Entra admin center → Protection > Authentication methods > Password protection.

Verify:

• 'Enforce custom list' is set to 'Yes'

• Custom banned password list contains organization-relevant terms

Remediation:

Microsoft Entra admin center → Protection > Authentication methods > Password protection.

Enable 'Enforce custom list' and add organization-specific terms:

• Company name and abbreviations

• Product names

• Office locations

• Common patterns used by your organization

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad

---

- **ms365-cis-5.2.3.3 Ensure password protection is enabled for on-prem Active Directory** **[FAIL]**

Vulnerability Name	On-premises Active Directory password protection is not configured for this tenant (Password Rule Settings group setting does not exist). Note: this control only applies to hybrid tenants with on-premises AD.
Section	5.2.3 Authentication Methods
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	On-premises password protection is not installed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

For hybrid environments, Microsoft Entra Password Protection agents should be installed on on-premises Active Directory domain controllers to enforce the same banned password policies on-premises.

Description

For hybrid environments, Microsoft Entra Password Protection agents should be installed on on-premises Active Directory domain controllers to enforce the same banned password policies on-premises.

Details

Rationale: Without on-premises password protection, users can set weak passwords in on-premises AD that may be synced to Entra ID, bypassing cloud password protection policies.

Impact: Requires installation of the Microsoft Entra Password Protection proxy service and DC agent on on-premises infrastructure.

Audit Procedure:

Microsoft Graph:

GET /groupSettings, filter templateId == 5cf42378-d67d-4f36-ba46-e8b86229381d (Password Rule Settings)

Ensure EnableBannedPasswordCheckOnPremises is True and BannedPasswordCheckOnPremisesMode is 'Enforce'.

Microsoft Entra admin center → Protection > Authentication methods > Password protection.

Ensure 'Enable password protection on Windows Server Active Directory' is Yes and Mode is Enforced.

Note: This recommendation applies to hybrid deployments only and has no impact without on-premises Active Directory.

Remediation:

Download the Microsoft Entra Password Protection proxy installer

Install on a domain-joined server with connectivity to Entra ID

Install DC agents on all domain controllers

Configure enforcement mode in Entra admin center

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises

---

- **ms365-cis-5.2.3.4 Ensure all member users are MFA capable**

  [PASS]

Vulnerability Name	All 2 member users are MFA capable.
Section	5.2.3 Authentication Methods
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	No MFA registered for new users by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

All member (non-guest) users should have at least one MFA method registered to be MFA capable. Users without MFA registered cannot comply with MFA enforcement policies.

Mfacapablecount:

- 2

Totalmemberusers:

- 2

Description

All member (non-guest) users should have at least one MFA method registered to be MFA capable. Users without MFA registered cannot comply with MFA enforcement policies.

Details

Rationale: MFA enforcement policies only protect users who have registered MFA methods. Users without registered MFA methods are at risk if their passwords are compromised.

Impact: Users without MFA registered may be blocked from accessing resources when MFA enforcement policies take effect.

Audit Procedure:

GET /reports/authenticationMethods/userRegistrationDetails

Filter by userType = 'member'

Check isMfaCapable = true for all member users

Remediation:

Identify users who are not MFA capable using the report

Contact those users and require MFA registration

Run an MFA registration campaign

Use the Entra ID MFA Registration Campaign feature:

Microsoft Entra admin center → Protection > Authentication methods > Registration campaign

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-methods-activity

---

- **ms365-cis-5.2.3.5 Ensure weak authentication methods are disabled**
  [PASS]

Vulnerability Name	Weak authentication methods (SMS, Voice) are disabled.
Section	5.2.3 Authentication Methods
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	SMS and Voice authentication methods may be enabled.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Weak authentication methods such as SMS OTP and voice call should be disabled in favor of stronger methods like Microsoft Authenticator and FIDO2. SMS and voice calls are susceptible to SIM swapping and social engineering attacks.

Methodschecked:

- sms
- voice

Description

Weak authentication methods such as SMS OTP and voice call should be disabled in favor of stronger methods like Microsoft Authenticator and FIDO2. SMS and voice calls are susceptible to SIM swapping and social engineering attacks.

Details

Rationale: SMS and voice call OTP are vulnerable to SIM swapping, phone number porting, and social engineering attacks. Disabling these methods forces users to adopt more secure authentication options.

Impact: Users currently using SMS or voice call for MFA must register a stronger method before the weak methods are disabled.

Audit Procedure:

GET /policies/authenticationMethodsPolicy

In authenticationMethodConfigurations:

Find SMS method (id = 'sms') - state should be 'disabled'

Find Voice method (id = 'voice') - state should be 'disabled'

Remediation:

Microsoft Entra admin center → Protection > Authentication methods.

Disable SMS and Voice call methods.

Ensure users have stronger methods registered before disabling.

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

---

ms365-cis-5.2.3.6 Ensure system-preferred MFA is enabled

[FAIL]

Vulnerability Name	System-preferred MFA state is 'default' (Microsoft managed) — it has not been explicitly enabled by the tenant admin, so this control is not satisfied.
Section	5.2.3 Authentication Methods
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	System-preferred MFA state may vary by tenant.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

System-preferred MFA (credential preferences) should be enabled to ensure users are prompted to use the most secure MFA method they have registered, rather than a weaker method they may prefer.

Includetargets:

- {'id': 'all_users', 'targetType': 'group'}

Systemcredentialpreferences.State:

- default

Description

System-preferred MFA (credential preferences) should be enabled to ensure users are prompted to use the most secure MFA method they have registered, rather than a weaker method they may prefer.

Details

Rationale: Users may have both weak (SMS) and strong (Authenticator) MFA methods registered. System-preferred MFA ensures the system prompts for the strongest available method rather than deferring to user preference.

Impact: Users may be prompted for a different MFA method than they are accustomed to using.

Audit Procedure:

GET /beta/policies/authenticationMethodsPolicy

(Invoke-MgGraphRequest ...).systemCredentialPreferences

Ensure includeTargets contains 'all_users' and state is 'enabled'.

Remediation:

Microsoft Entra admin center → Protection > Authentication methods > Authentication methods policy.

Enable 'System-preferred multifactor authentication'.

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-system-preferred-multifactor-authentication

---

● ms365-cis-5.2.3.7 Ensure email-based OTP is disabled

[FAIL]

Vulnerability Name	Email OTP authentication method is not disabled (state = 'enabled'). Disable email OTP in favor of stronger authentication methods.

Section	5.2.3 Authentication Methods
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Email OTP may be enabled for guest users by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Email one-time passcode (OTP) should be disabled as an authentication method. Email OTP is a weaker authentication method that can be compromised if the user's email is compromised.

Emailotp.State:

- enabled

Description

Email one-time passcode (OTP) should be disabled as an authentication method. Email OTP is a weaker authentication method that can be compromised if the user's email is compromised.

Details

Rationale: Email OTP relies on the security of the email account. If a user's email is compromised, attackers can intercept OTPs and bypass MFA. Stronger methods should be used instead.

Impact: External users (B2B guests) who rely on email OTP for authentication will need to use alternative authentication methods.

Audit Procedure:

GET /policies/authenticationMethodsPolicy
In authenticationMethodConfigurations:
Find email method (id = 'email') - state should be 'disabled'

Remediation:
Microsoft Entra admin center → Protection > Authentication methods.
Disable 'Email OTP' authentication method.

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

---

- **ms365-cis-5.2.4.1 Ensure 'Self service password reset enabled' is set to 'All'**

  [MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure 'Self service password reset enabled' is set to 'All'
Section	5.2.4 Password Reset
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	SSPR is disabled by default or set to 'None'.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Self-service password reset (SSPR) should be enabled for all users to allow them to reset their own passwords without contacting IT helpdesk, reducing support burden and enabling faster password recovery.

Description

Self-service password reset (SSPR) should be enabled for all users to allow them to reset their own passwords without contacting IT helpdesk, reducing support burden and enabling faster password recovery.

Details

Rationale: SSPR reduces helpdesk ticket volume for password resets and allows users to quickly regain access to their accounts. SSPR can be configured to require MFA verification for identity verification.

Impact: Users will be able to reset their own passwords using registered authentication methods. Requires users to register SSPR methods.

Audit Procedure:

Microsoft Entra admin center → Entra ID > Password reset > Properties.

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

Remediation:

Microsoft Entra admin center → Protection > Password reset > Properties.

Set 'Self-service password reset enabled' to 'All'.

Configure methods and require 2 methods for strong verification.

Reference: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment

---

● ms365-cis-5.3.1 Ensure Privileged Identity Management is used to manage roles

[FAIL]

Vulnerability Name	No PIM role assignments found. Roles may be permanently assigned without using Privileged Identity Management.

Security Findings Report

Section	5.3 Privileged Identity Management
Severity	Medium
Profiles	E5 Level 2
Default Value	Roles are permanently assigned without PIM by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Privileged Identity Management (PIM) should be used to manage directory role assignments, providing just-in-time (JIT) privileged access with approval workflows and time limits.

Description

Privileged Identity Management (PIM) should be used to manage directory role assignments, providing just-in-time (JIT) privileged access with approval workflows and time limits.

Details

Rationale: PIM replaces permanent role assignments with time-limited, just-in-time access that requires explicit activation. This dramatically reduces the window of opportunity for attackers who compromise privileged accounts.

Impact: Administrators will need to activate their roles before performing privileged tasks. Permanent assignments should be moved to eligible assignments in PIM.

Audit Procedure:

Using Microsoft Graph (beta):

GET /beta/privilegedAccess/aadRoles/roleAssignments
Look for 'Eligible' assignments (not just 'Active' permanent ones)

Microsoft Entra admin center → Identity governance > Privileged Identity Management

Remediation:

Enable PIM for the tenant (requires Entra ID P2)
Configure role settings with activation requirements
Convert permanent role assignments to eligible assignments
Require MFA and justification for role activation

Reference: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

---

● ms365-cis-5.3.2 Ensure access reviews for guest users are configured

[FAIL]

Vulnerability Name	No active access reviews targeting guest users found. Total access reviews in tenant: 0.
Section	5.3 Privileged Identity Management
Severity	Medium
Profiles	E5 Level 2
Default Value	No access reviews configured by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026

Security Findings Report

Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Access reviews should be configured for guest users to ensure that guest access is periodically reviewed and revoked when no longer needed.

Description

Access reviews should be configured for guest users to ensure that guest access is periodically reviewed and revoked when no longer needed.

Details

Rationale: Guest users are often added for specific projects and may retain access long after it is no longer needed. Regular access reviews ensure guest access is periodically validated and inappropriate access is removed.

Impact: Reviewers (typically group owners or managers) must periodically review and approve or deny guest access. This requires time commitment from reviewers.

Audit Procedure:

GET /identityGovernance/accessReviews/definitions

Look for active access review definitions that:

• Target guest users (userType = 'Guest')

• Are scheduled (not one-time)

• Are in 'active' state

Remediation:

Microsoft Entra admin center → Identity governance > Access reviews.

Create a new access review:

• Scope: Guest users

• Recurrence: Quarterly or more frequent

• Reviewers: Group owners or specific reviewers

• Auto-apply results: enabled

Reference: https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

---

ms365-cis-5.3.3 Ensure access reviews for privileged roles are configured

[FAIL]

Vulnerability Name	No active access reviews targeting privileged roles found. Total access reviews in tenant: 0.
Section	5.3 Privileged Identity Management
Severity	Medium
Profiles	E5 Level 2
Default Value	No access reviews for privileged roles by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Access reviews should be configured for privileged roles (especially Global Administrator) to ensure that role assignments are periodically reviewed and excessive access is removed.

Description

Access reviews should be configured for privileged roles (especially Global Administrator) to ensure that role assignments are periodically reviewed and excessive access is removed.

Details

Rationale: Privileged role assignments can accumulate over time as users change roles or leave the organization. Regular access reviews ensure that privileged access is periodically validated.

Impact: Role assignment reviewers must periodically review and confirm or deny existing role assignments.

Audit Procedure:

GET /identityGovernance/accessReviews/definitions

Look for access reviews targeting directory roles:

• scope.@odata.type referencing directoryRoles

• Status: active or scheduled

Remediation:

Microsoft Entra admin center → Identity governance > Access reviews.

Create access reviews for:

• Global Administrator

• Privileged Role Administrator

• Other high-privilege roles

Set recurrence to quarterly or more frequent.

Reference: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-create-roles-and-resource-roles-review

---

● ms365-cis-5.3.4 Ensure approval is required for Privileged Role Administrator activation [SKIPPED]

Vulnerability Name	Could not retrieve PIM role management policies: Privileged Identity Management is not provisioned in this tenant. It requires a Microsoft Entra ID P2 or Microsoft Entra ID Governance licence.
Section	5.3 Privileged Identity Management
Severity	Medium

Profiles	E5 Level 2
Default Value	Approval is not required for role activation by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

The Global Administrator role in Privileged Identity Management (PIM) should require explicit approval before activation. This adds an additional human verification layer to the most privileged role.

Description

The Privileged Role Administrator role in PIM should require approval before activation. This role can modify all other PIM role settings, making it critical to protect.

Details

Rationale: The Privileged Role Administrator can grant themselves or others any directory role. Requiring approval for its activation prevents unauthorized privilege escalation.

Impact: Privileged Role Administrator activation will require an approver, adding latency to PIM management tasks.

Audit Procedure:

GET /policies/roleManagementPolicies

Filter for Privileged Role Administrator role

Check approval rules: isApprovalRequired = true

Remediation:

Microsoft Entra admin center → Identity governance > PIM > Microsoft Entra roles > Privileged Role Administrator > Role settings:

• Enable approval for activation

• Add approvers

Reference: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings

---

ms365-cis-5.3.5 Ensure approval is required for Privileged Role Administrator activation [SKIPPED]

Vulnerability Name	Could not retrieve PIM role management policies: Privileged Identity Management is not provisioned in this tenant. It requires a Microsoft Entra ID P2 or Microsoft Entra ID Governance licence.
Section	5.3 Privileged Identity Management
Severity	Medium
Profiles	E5 Level 2
Default Value	Approval is not required for role activation by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

The Privileged Role Administrator role in PIM should require approval before activation. This role can modify all other PIM role settings, making it critical to protect.

Description

The Privileged Role Administrator role in PIM should require approval before activation. This role can modify all other PIM role settings, making it critical to protect.

Details

Rationale: The Privileged Role Administrator can grant themselves or others any directory role. Requiring approval for its activation prevents unauthorized privilege escalation.

Impact: Privileged Role Administrator activation will require an approver, adding latency to PIM management tasks.

Audit Procedure:

GET /policies/roleManagementPolicies

Filter for Privileged Role Administrator role

Check approval rules: isApprovalRequired = true

Remediation:

Microsoft Entra admin center → Identity governance > PIM > Microsoft Entra roles > Privileged Role Administrator > Role settings:

• Enable approval for activation

• Add approvers

Reference: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings

---

- **ms365-cis-6.1.1 Ensure 'AuditDisabled' organizationally is set to 'False'**
  [PASS]

Vulnerability Name	AuditDisabled is False organizationally; mailbox auditing is enabled by default.
Section	6.1 Audit
Severity	High

Profiles	E3 Level 1, E5 Level 1
Default Value	AuditDisabled = False by default in new tenants.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The AuditDisabled organization configuration in Exchange Online should be set to False to ensure mailbox auditing is enabled at the organization level.

Description

The AuditDisabled organization configuration in Exchange Online should be set to False to ensure mailbox auditing is enabled at the organization level.

Details

Rationale: Organization-level audit settings control the default audit behavior for all mailboxes. If AuditDisabled is True, mailbox audit logging is disabled by default, impeding security investigations.

Impact: Minimal - enables audit logging which is generally desirable.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-OrganizationConfig | Format-List AuditDisabled

Compliant: AuditDisabled is False.

Remediation:

Exchange Online PowerShell:

Set-OrganizationConfig -AuditDisabled $false

Reference: https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging

---

ms365-cis-6.1.2 Ensure mailbox audit actions are configured

[PASS]

Vulnerability Name	No user mailboxes were found to evaluate for audit action configuration.
Section	6.1 Audit
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Mailbox auditing is enabled by default in Exchange Online.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Mailbox audit logging should be enabled for all user mailboxes, and the AuditAdmin, AuditDelegate, and AuditOwner action sets should include the full recommended list of actions to record.

Description

Mailbox audit logging should be enabled for all user mailboxes, and the AuditAdmin, AuditDelegate, and AuditOwner action sets should include the full recommended list of actions to record.

Details

Rationale: Mailbox audit logs record who accessed a mailbox and what actions they performed. This is essential for detecting unauthorized access and supporting forensic investigations.

Impact: Minimal - enables audit logging which uses additional storage.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-EXOMailbox -PropertySets Audit,Minimum -ResultSize Unlimited | Where-Object { $_.RecipientTypeDetails -eq 'UserMailbox' }

For each mailbox verify:

AuditEnabled = True

AuditAdmin includes: ApplyRecord, Copy, Create, FolderBind, HardDelete, MailItemsAccessed, Move, MoveToDeletedItems, SendAs, SendOnBehalf, Send, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

AuditDelegate includes: ApplyRecord, Create, FolderBind, HardDelete, Move, MailItemsAccessed, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateFolderPermissions, UpdateInboxRules

AuditOwner includes: ApplyRecord, Create, HardDelete, MailboxLogin, Move, MailItemsAccessed, MoveToDeletedItems, Send, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

Remediation:

Exchange Online PowerShell:

Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled $true

Also configure comprehensive audit actions:

Set-Mailbox -AuditAdmin @{Add='Copy','Create','FolderBind',...}

Set-Mailbox -AuditOwner @{Add='MailboxLogin','Move','MoveToDeletedItems',...}

Reference: https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable

---

ms365-cis-6.1.3 Ensure 'AuditBypassEnabled' is not enabled on mailboxes

[PASS]

Vulnerability Name	No mailboxes have AuditBypassEnabled set to True.
Section	6.1 Audit
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Audit bypass is disabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

No mailboxes should have audit bypass enabled. Audit bypass allows specific accounts to access mailboxes without generating audit log entries, which could be used to hide unauthorized access.

Description

No mailboxes should have audit bypass enabled. Audit bypass allows specific accounts to access mailboxes without generating audit log entries, which could be used to hide unauthorized access.

Details

Rationale: Audit bypass provides a way to access mailboxes without leaving an audit trail. This can be abused by attackers or malicious insiders to cover their tracks when accessing sensitive mailboxes.

Impact: Removing audit bypass ensures all mailbox access is logged.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-MailboxAuditBypassAssociation -ResultSize unlimited | where AuditBypassEnabled -eq $true | select Name,AuditBypassEnabled

Compliant: no accounts are returned (no accounts bypass auditing).

Remediation:

Exchange Online PowerShell:

Get-MailboxAuditBypassAssociation -ResultSize Unlimited | Where-Object {$_.AuditBypassEnabled} | ForEach-Object { Set-MailboxAuditBypassAssociation -Identity $_.Identity -AuditBypassEnabled $false }

Reference: https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/bypass-mailbox-audit-logging

---

- **ms365-cis-6.2.1 Ensure all forms of mail forwarding are blocked and/or disabled**
  [FAIL]

Vulnerability Name	Mail forwarding is not fully blocked: AutoForwardingMode is 'Automatic' (must be 'Off')
Section	6.2 Mail flow
Severity	High
Profiles	E3 Level 1, E5 Level 1

Default Value	AutoForwardingMode is 'Automatic' (allows forwarding) by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Automatic email forwarding to external addresses is a well-known data exfiltration technique, frequently used by attackers who have compromised a mailbox. Blocking auto-forwarding via transport rules prevents sensitive data from leaving the organisation silently.

Autoforwardingmode:

- Automatic

Description

Automatic email forwarding to external addresses is a well-known data exfiltration technique, frequently used by attackers who have compromised a mailbox. Blocking auto-forwarding via transport rules prevents sensitive data from leaving the organisation silently.

Details

Rationale: Compromised accounts configured to silently forward mail to an attacker-controlled address can exfiltrate sensitive data for extended periods without detection. Blocking external forwarding reduces this risk.

Impact: Legitimate use-cases such as personal forwarding rules will be blocked. Users who require external forwarding for business purposes will need an approved exception documented in the transport rule.

Audit Procedure:

Exchange Online PowerShell:

Get-TransportRule | Where-Object {$_.RedirectMessageTo -ne $null -or $_.BlindCopyTo -ne $null}

Or check outbound spam policy:

Get-HostedOutboundSpamFilterPolicy | Select-Object AutoForwardingMode
AutoForwardingMode should be 'Off'.

Via admin portal:
Exchange admin center → Mail flow > Rules.
Verify a rule exists that blocks forwarding to external recipients.
Also check: Exchange admin center → Policies > Anti-spam > Outbound policy > Automatic forwarding rules = Off.

Remediation:
Option 1 – Outbound anti-spam policy (recommended):
Exchange admin center → Policies > Anti-spam > Outbound policy.
Set 'Automatic forwarding rules' to 'Off - Forwarding is disabled'.

Option 2 – Transport rule:
Create a transport rule that rejects messages where:
• The message was auto-forwarded (message type is auto-forward).
• The recipient is outside the organisation.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/outbound-spam-policies-configure

---

- **ms365-cis-6.2.2 Ensure mail transport rules do not whitelist specific domains**
  [PASS]

Vulnerability Name	No transport rule sets SCL to -1 (bypassing spam filtering) for a specific sender domain.
Section	6.2 Mail flow
Severity	High
Profiles	E3 Level 1, E5 Level 1

Default Value	No domain whitelist transport rules exist by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Mail transport rules should not be configured to whitelist entire domains from spam and malware filtering. Domain whitelisting bypasses security controls and can allow malicious emails to reach users.

Description

Mail transport rules should not be configured to whitelist entire domains from spam and malware filtering. Domain whitelisting bypasses security controls and can allow malicious emails to reach users.

Details

Rationale: Domain whitelist transport rules bypass all spam and malware filters for that domain. If a whitelisted domain is compromised, or the rule uses an attacker-controlled domain, malicious emails can reach users.

Impact: Removing domain whitelist rules means email from those domains will be filtered.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-TransportRule | Where-Object { $_.setscl -eq -1 -and $_.SenderDomainIs -ne $null } | ft Name,SenderDomainIs,SetSCL

Compliant: no rule sets SCL to -1 (bypass spam filtering) for a specific sender domain; no output is returned.

Remediation:

Exchange Online PowerShell:
Get-TransportRule | Where-Object {$_.SetSCL -eq -1} | Remove-TransportRule

Review and remove transport rules that bypass spam/malware filtering.

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

---

- **ms365-cis-6.2.3 Ensure email from external senders is identified**
  [FAIL]

Vulnerability Name	External sender identification is not enabled for: 825a7bf3-be45-47e9-86d5-565d24b0a7fb
Section	6.2 Mail flow
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	External sender identification may not be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External sender identification should be enabled to show Outlook users a visual warning when receiving email from external senders. This helps users identify potential phishing emails.

Identity:

- 825a7bf3-be45-47e9-86d5-565d24b0a7fb

Description

External sender identification should be enabled to show Outlook users a visual warning when receiving email from external senders. This helps users identify potential phishing emails.

Details

Rationale: Visual cues that an email comes from an external sender help users be more cautious about clicking links or opening attachments in those messages, reducing the risk of successful phishing attacks.

Impact: Users will see a visual indicator on emails from external senders.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-ExternalInOutlook

For each identity verify Enabled = True and that AllowList only contains explicitly permitted addresses/domains.

Remediation:

Exchange Online PowerShell:

Set-ExternalInOutlook -Enabled $true

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-junk-email-settings-on-exo-mailboxes

---

- **ms365-cis-6.3.1 Ensure users installing Outlook add-ins is not allowed**
  [FAIL]

Vulnerability Name	One or more role assignment policies allow users to install Outlook add-ins
Section	6.3 Add-ins
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	Users can install Outlook add-ins by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

One or more role assignment policies allow users to install Outlook add-ins: Default Role Assignment Policy: My Custom Apps, My Marketplace Apps, My ReadWriteMailbox Apps

Id:

- Default Role Assignment Policy

Guid:

- 12f22534-41e8-4c9c-9bf7-0e335c86c986

Name:

- Default Role Assignment Policy

Isvalid:

- True

Identity:

- Default Role Assignment Policy

Isdefault:

- True

Description:

- This policy grants end users the permission to set their options in Outlook on the web and perform other self-administration tasks.

Objectclass:

- top
- msExchRBACPolicy

Objectstate:

- Changed

Whenchanged:

- 2026-03-10T04:20:31+00:00

Whencreated:

- 2026-03-09T05:05:03+00:00

Assignedroles:

- My ReadWriteMailbox Apps
- MyDistributionGroups
- MyRetentionPolicies
- MyBaseOptions
- My Custom Apps
- MyDistributionGroupMembership
- My Marketplace Apps
- MyTextMessaging
- MyContactInformation
- MyVoiceMail
- MyProfileInformation
- MyMailSubscriptions

Objectcategory:

- indp287a011.prod.outlook.com/Configuration/Schema/ms-Exch-RBAC-Policy

Organizationid:

- indp287a011.prod.outlook.com/Microsoft Exchange Hosted Organizations/ayushaggarwal1136gmail.onmicrosoft.com - indp287a011.prod.outlook.com/ConfigurationUnits/ayushaggarwal1136gmail.onmicrosoft.com/Configuration

Whenchangedutc:

- 2026-03-10T04:20:31Z

Whencreatedutc:

- 2026-03-09T05:05:03Z

Exchangeversion:

- 0.11 (14.0.509.0)

Roleassignments:

- My ReadWriteMailbox Apps-Default Role Assignment Policy
- MyDistributionGroups-Default Role Assignment Policy

- MyRetentionPolicies-Default Role Assignment Policy
- MyBaseOptions-Default Role Assignment Policy
- My Custom Apps-Default Role Assignment Policy
- MyDistributionGroupMembership-Default Role Assignment Policy
- My Marketplace Apps-Default Role Assignment Policy
- MyTextMessaging-Default Role Assignment Policy
- MyContactInformation-Default Role Assignment Policy
- MyVoiceMail-Default Role Assignment Policy
- MyProfileInformation-Default Role Assignment Policy
- MyMailSubscriptions-Default Role Assignment Policy

Exchangeobjectid:

- 12f22534-41e8-4c9c-9bf7-0e335c86c986

Distinguishedname:

- CN=Default Role Assignment Policy,CN=Policies,CN=RBAC,CN=Configuration,CN=ayushaggarwal1136gmail.onmicrosoft.com,CN=ConfigurationUnits,DC=indp287a011,DC=prod,DC=outlook,DC=com

Originatingserver:

- MAYP287A11DC002.indp287a011.prod.outlook.com

Organizationalunitroot:

- ayushaggarwal1136gmail.onmicrosoft.com

Description

Users should not be allowed to install Outlook add-ins from the Office Store without administrator approval. Unrestricted add-in installation can introduce malicious or data-exfiltrating plugins.

Details

Rationale: Outlook add-ins have access to email data and can exfiltrate sensitive information. Restricting installation to admin-approved add-ins ensures only vetted tools access email data.

Impact: Users must request admin deployment of Outlook add-ins.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-EXOMailbox -PropertySets Policy | Select-Object -Unique RoleAssignmentPolicy

For each policy returned: Get-RoleAssignmentPolicy -Identity <policy>

Compliant: 'My Custom Apps', 'My Marketplace Apps', and 'My ReadWriteMailbox Apps' are NOT present in AssignedRoles for any policy.

Remediation:

Exchange Online PowerShell:

$policy = Get-RoleAssignmentPolicy 'Default Role Assignment Policy'

Set-RoleAssignmentPolicy -Identity $policy.Identity -Roles (($policy.AssignedRoles) -notlike 'My*Apps*')

Reference: 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

---

ms365-cis-6.5.1 Ensure modern authentication for Exchange Online is enabled

[PASS]

Vulnerability Name	OAuth2ClientProfileEnabled is True; modern authentication for Exchange Online is enabled.
Section	6.5 Client Access
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Modern authentication is enabled by default in Exchange Online.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Modern authentication (OAuth 2.0) for Exchange Online should be enabled to allow MFA and Conditional Access policies to apply to email clients. Without modern auth, older clients use Basic Authentication which cannot enforce MFA.

Oauth2Clientprofileenabled:

- True

Description

Modern authentication (OAuth 2.0) for Exchange Online should be enabled to allow MFA and Conditional Access policies to apply to email clients. Without modern auth, older clients use Basic Authentication which cannot enforce MFA.

Details

Rationale: Modern authentication enables MFA, Conditional Access, and other advanced security features for Exchange Online connections. Basic Authentication bypasses these controls.

Impact: Older email clients that only support Basic Auth will not be able to connect.

Audit Procedure:

Using Microsoft Graph:

GET /admin/exchange/settings

Check: isModernAuthentication = true

Or Exchange Online PowerShell:

Get-OrganizationConfig | Select-Object OAuth2ClientProfileEnabled

Remediation:

Exchange Online PowerShell:

Set-OrganizationConfig -OAuth2ClientProfileEnabled $true

Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online

ms365-cis-6.5.2 Ensure MailTips are enabled for end users

[FAIL]

Vulnerability Name	MailTips are not fully enabled: MailTipsExternalRecipientsTipsEnabled is not True
Section	6.5 Client Access
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	MailTips settings may vary.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

MailTips should be enabled to provide users with informational messages when composing emails that may indicate issues or potential problems, such as sending to external recipients or large distribution lists.

Mailtipsalltipsenabled:

- True

Mailtipsgroupmetricsenabled:

- True

Mailtipslargeaudiencethreshold:

- 25

Description

MailTips should be enabled to provide users with informational messages when composing emails that may indicate issues or potential problems, such as sending to external recipients or large distribution lists.

Details

Rationale: MailTips warn users before sending emails that might be sent to the wrong recipient, contain sensitive data recipients shouldn't see, or indicate other potential issues, reducing accidental data exposure.

Impact: No negative impact; MailTips provide helpful reminders to users.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-OrganizationConfig | fl MailTips*

Compliant: MailTipsAllTipsEnabled = True, MailTipsExternalRecipientsTipsEnabled = True, MailTipsGroupMetricsEnabled = True, and MailTipsLargeAudienceThreshold is set to an acceptable value (default 25).

Remediation:

Exchange Online PowerShell:

Set-OrganizationConfig -MailTipsAllTipsEnabled $true -MailTipsExternalRecipientsTipsEnabled $true -MailTipsGroupMetricsEnabled $true -MailTipsLargeAudienceThreshold 25

Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/mailtips/mailtips

---

● ms365-cis-6.5.3 Ensure additional storage providers are restricted in Outlook on the web

[FAIL]

Vulnerability Name	AdditionalStorageProvidersAvailable is True; users can connect third-party cloud storage providers in Outlook on the web.
Section	6.5 Client Access

Security Findings Report

Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	Additional storage providers are enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Outlook on the web (OWA) should be configured to prevent users from connecting to third-party cloud storage providers like Dropbox, Box, and Google Drive.

Additionalstorageprovidersavailable:

- True

Description

Outlook on the web (OWA) should be configured to prevent users from connecting to third-party cloud storage providers like Dropbox, Box, and Google Drive.

Details

Rationale: Third-party storage providers are not subject to organizational governance and compliance controls. Restricting access ensures data stays within approved storage systems.

Impact: Users will not be able to attach files from third-party storage in OWA.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default | fl AdditionalStorageProvidersAvailable

Compliant: AdditionalStorageProvidersAvailable = False

Remediation:

Exchange Online PowerShell:

Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -AdditionalStorageProvidersAvailable $false

Reference: https://learn.microsoft.com/en-us/powershell/module/exchange/set-owamailboxpolicy

---

ms365-cis-6.5.4 Ensure SMTP AUTH is disabled

[PASS]

Vulnerability Name	SmtpClientAuthenticationDisabled is True.
Section	6.5 Client Access
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	SMTP AUTH may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

SMTP Authentication (SMTP AUTH) should be disabled at the organization level to prevent legacy clients from sending email using Basic Authentication over SMTP port 587.

Smtpclientauthenticationdisabled:

- True

Description

SMTP Authentication (SMTP AUTH) should be disabled at the organization level to prevent legacy clients from sending email using Basic Authentication over SMTP port 587.

Details

Rationale: SMTP AUTH uses Basic Authentication which cannot enforce MFA. Attackers who compromise credentials can use SMTP AUTH to send emails from compromised accounts without triggering MFA challenges.

Impact: Devices and applications that send mail via SMTP AUTH will be unable to authenticate. They must use Microsoft 365 connectors or modern auth methods instead.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-TransportConfig | Format-List SmtpClientAuthenticationDisabled

Compliant: SmtpClientAuthenticationDisabled = True

Remediation:

Exchange Online PowerShell:

Set-TransportConfig -SmtpClientAuthenticationDisabled $true

For specific applications that require SMTP AUTH, enable it per-mailbox:

Set-CASMailbox -Identity <mailbox> -SmtpClientAuthenticationDisabled $false

Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

---

- **ms365-cis-6.5.5 Ensure Direct Send submissions are rejected**

  [FAIL]

Vulnerability Name	RejectDirectSend is not True; unauthenticated Direct Send submissions are still accepted.
Section	6.5 Client Access
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	RejectDirectSend may be False by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Direct Send allows devices and applications on the organization's network to submit mail directly to Exchange Online without authenticating, using the tenant's default domain. The RejectDirectSend organization setting should be enabled to reject these unauthenticated submissions.

Description

Direct Send allows devices and applications on the organization's network to submit mail directly to Exchange Online without authenticating, using the tenant's default domain. The RejectDirectSend organization setting should be enabled to reject these unauthenticated submissions.

Details

Rationale: Direct Send (unauthenticated SMTP submission using the tenant's accepted domain) can be abused by attackers to spoof internal senders and bypass authentication-based security controls. Rejecting Direct Send submissions forces devices to use authenticated methods instead.

Impact: Devices using Direct Send (printers, scanners, network appliances) must be reconfigured to use authenticated SMTP (SMTP AUTH) or an Microsoft 365 SMTP relay connector.

Audit Procedure:

Exchange Online PowerShell:

Connect-ExchangeOnline

Get-OrganizationConfig | fl RejectDirectSend

Compliant: RejectDirectSend = True

Remediation:

Exchange Online PowerShell:

Set-OrganizationConfig -RejectDirectSend $true

Reconfigure devices to use authenticated SMTP submission:

- Use SMTP AUTH with a licensed mailbox
- Or use a Microsoft 365 SMTP relay connector

Reference: https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365

- **ms365-cis-7.2.1 Ensure modern authentication for SharePoint applications is required** **[FAIL]**

Vulnerability Name	Legacy authentication is enabled for SharePoint (isLegacyAuthProtocolsEnabled = true). Modern authentication is not being enforced.
Section	7.2 Policies
Severity	High
Profiles	E3 Level 1, E5 Level 1

Default Value	Legacy authentication may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

SharePoint Online should require modern authentication to enable MFA and Conditional Access policies to apply to SharePoint connections. Legacy authentication should be blocked for SharePoint.

Islegacyauthprotocolsenabled:

- True

Description

SharePoint Online should require modern authentication to enable MFA and Conditional Access policies to apply to SharePoint connections. Legacy authentication should be blocked for SharePoint.

Details

Rationale: Legacy authentication bypasses MFA and Conditional Access, making SharePoint resources accessible with just a password. Modern auth enables comprehensive security controls.

Impact: Legacy SharePoint clients that don't support modern auth will be blocked.

Audit Procedure:

GET /admin/sharepoint/settings

Check: isLegacyAuthProtocolsEnabled = false (legacy auth disabled)

Remediation:

SharePoint admin center → Settings > SharePoint > Restrict access to legacy authentication.

Or via PowerShell:

Set-SPOTenant -LegacyAuthProtocolsEnabled $false

Reference: https://learn.microsoft.com/en-us/sharepoint/control-access-based-on-network-location

---

● ms365-cis-7.2.2 Ensure SharePoint and OneDrive integration with Microsoft Entra B2B is enabled

[SKIPPED]

Vulnerability Name	This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually: Get-SPOTenant | fl EnableAzureADB2BIntegration
Section	7.2 Policies
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	B2B integration setting may vary.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

SharePoint and OneDrive should be integrated with Microsoft Entra B2B to ensure external users are managed through Entra ID's identity governance features rather than SharePoint's own guest management.

Description

SharePoint and OneDrive should be integrated with Microsoft Entra B2B to ensure external users are managed through Entra ID's identity governance features rather than SharePoint's own guest management.

Details

Rationale: Entra B2B integration for SharePoint ensures external users are properly governed as Entra ID guest accounts with consistent access controls, MFA requirements, and lifecycle management.

Impact: Existing SharePoint-only external users may need to be migrated to Entra B2B guest accounts.

Audit Procedure:

Connect to SharePoint Online using Connect-SPOService, then:

Get-SPOTenant | ft EnableAzureADB2BIntegration

Ensure the returned value is True.

Remediation:

SharePoint admin center → Settings > External collaboration.

Enable Microsoft Entra B2B integration for SharePoint and OneDrive.

Reference: https://learn.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration

---

● ms365-cis-7.2.3 Ensure external content sharing is restricted

[FAIL]

Vulnerability Name	SharePoint external sharing is too permissive: sharingCapability = externalUserAndGuestSharing
Section	7.2 Policies
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	ExternalUserAndGuestSharing (any external user, guest links enabled).

Security Findings Report

Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

SharePoint and OneDrive tenant-level external sharing settings should be restricted to 'Existing external users' or 'Only people in your organisation' to prevent unrestricted data exposure via sharing links.

@Odata.Context:

- https://graph.microsoft.com/v1.0/$metadata#admin/sharepoint/settings/$entity

Sharingcapability:

- externalUserAndGuestSharing

Imagetaggingoption:

- basic

Ismacsyncappenabled:

- True

Issitecreationenabled:

- True

Tenantdefaulttimezone:

- (UTC-08:00) Pacific Time (US and Canada)

Issitecreationuienabled:

- True

Issitepagescreationenabled:

- True

Islegacyauthprotocolsenabled:

- True

Issitesstoragelimitautomatic:

- True

Sharingdomainrestrictionmode:

- none

Iscommentingonsitepagesenabled:

- True

Sitecreationdefaultmanagedpath:

- /sites/

Isfileactivitynotificationenabled:

- True

Isresharingbyexternalusersenabled:

- True

Personalsitedefaultstoragelimitinmb:

- 1048576

Sitecreationdefaultstoragelimitinmb:

- 26214400

Availablemanagedpathsforsitecreation:

- /sites/
- /teams/

Issharepointmobilenotificationenabled:

- True

Deleteduserpersonalsiteretentionperiodindays:

- 30

Description

SharePoint and OneDrive tenant-level external sharing settings should be restricted to 'Existing external users' or 'Only people in your organisation' to prevent unrestricted data exposure via sharing links.

Details

Rationale: Unrestricted external sharing allows any user to share files with anyone, including unauthenticated 'Anyone with the link' access. This significantly increases the risk of unintended data disclosure.

Impact: Users will be unable to share content with new external users without additional configuration. Business processes relying on anonymous sharing links will need to be reviewed.

Audit Procedure:

Using Microsoft Graph:

GET /admin/sharepoint/settings

Check: sharingCapability should be 0 (Disabled) or 3 (Existing users only).

Or in SharePoint admin center:

https://admin.microsoft.com/sharepoint → Policies > Sharing.

External sharing slider should be at most 'Existing external users'.

Remediation:

SharePoint admin center → Policies > Sharing.

Set external sharing for SharePoint and OneDrive to 'Existing external users' or 'Only people in your organization'.

PowerShell: Set-SPOTenant -SharingCapability ExistingExternalUserSharingOnly

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

---

- **ms365-cis-7.2.4 Ensure OneDrive content sharing is restricted**
  [FAIL]

Vulnerability Name	OneDrive sharing is too permissive: externalUserAndGuestSharing
Section	7.2 Policies
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	OneDrive sharing may allow external sharing by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

OneDrive sharing should be restricted to existing external users or disabled entirely to prevent unrestricted sharing of personal files with unknown external parties.

Onedrivesharingcapability:

- externalUserAndGuestSharing

Description

OneDrive sharing should be restricted to existing external users or disabled entirely to prevent unrestricted sharing of personal files with unknown external parties.

Details

Rationale: Unrestricted OneDrive sharing can result in sensitive personal files being shared with anyone on the internet. Restricting sharing reduces the risk of unintended data disclosure.

Impact: Users will be unable to share OneDrive files with new external users.

Audit Procedure:

GET /admin/sharepoint/settings

Check: oneDriveDefaultShareLinkType and sharingCapability for OneDrive

Remediation:

SharePoint admin center → Policies > Sharing.

Set OneDrive sharing to 'Existing external users' or 'Only people in your organization'.

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

---

● ms365-cis-7.2.5 Ensure that SharePoint external users cannot share items they don't own

[FAIL]

Vulnerability Name	External users are allowed to re-share items they don't own (isResharingByExternalUsersEnabled (inverted)).

Security Findings Report

Section	7.2 Policies
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	External users can re-share by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External users should not be able to re-share content they don't own. This prevents external users from sharing organizational content with other unauthorized parties.

Isresharingbyexternalusersenabled:

- True

Description

External users should not be able to re-share content they don't own. This prevents external users from sharing organizational content with other unauthorized parties.

Details

Rationale: If external users can re-share items they have access to, content can spread to unapproved parties exponentially. Restricting re-sharing limits data exposure to explicitly authorized recipients.

Impact: External users will not be able to share content they access but don't own.

Audit Procedure:

Using Microsoft Graph:

GET /admin/sharepoint/settings

Check: isResharingByExternalUsersEnabled = false (Graph exposes the inverse of the Get-SPOTenant property).

Using SharePoint Online PowerShell:
Get-SPOTenant | ft PreventExternalUsersFromResharing → True

Remediation:
SharePoint admin center → Policies > Sharing.
Disable 'Allow guests to share items they don't own'.

PowerShell:
Set-SPOTenant -PreventExternalUsersFromResharing $true

Reference: https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview

---

- **ms365-cis-7.2.6 Ensure SharePoint external sharing is restricted**
  [FAIL]

Vulnerability Name	External sharing is not limited by domain (SharingDomainRestrictionMode = 'none'). Content can be shared with any external domain.
Section	7.2 Policies
Severity	High
Profiles	E3 Level 2, E5 Level 2
Default Value	'Limit external sharing by domain' is unchecked (SharingDomainRestrictionMode: None).
Asset Label	universal
Date Discovered	Aug 05, 2026

Security Findings Report

Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External sharing in SharePoint and OneDrive should be limited by domain, so that content can only be shared with an approved list of external domains. The recommended state is 'Limit external sharing by domain' > 'Allow only specific domains'.

Sharingdomainrestrictionmode:

- none

Description

External sharing in SharePoint and OneDrive should be limited by domain, so that content can only be shared with an approved list of external domains. The recommended state is 'Limit external sharing by domain' > 'Allow only specific domains'.

Details

Rationale: 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.

Impact: Users will be prevented from sharing documents with domains outside of the organization unless those domains are on the allow list.

Audit Procedure:

Using Microsoft Graph:

GET /admin/sharepoint/settings

Check: sharingDomainRestrictionMode = allowList and

sharingAllowedDomainList contains the approved domains.

Using SharePoint Online PowerShell:

Get-SPOTenant | fl SharingDomainRestrictionMode,SharingAllowedDomainList

Remediation:

SharePoint admin center → Policies > Sharing.

Expand 'More external sharing settings', check 'Limit external sharing by domain', and add the approved domains.

PowerShell:

Set-SPOTenant -SharingDomainRestrictionMode AllowList -SharingAllowedDomainList "domain1.com domain2.com"

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

---

- **ms365-cis-7.2.7 Ensure the default sharing link type is not set to 'Anyone with the link'** **[SKIPPED]**

Vulnerability Name	This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually: Get-SPOTenant | fl DefaultSharingLinkType
Section	7.2 Policies
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Default sharing link type may be set to Anyone.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

The default sharing link type in SharePoint and OneDrive should not be set to 'Anyone with the link' (anonymous access). The default should be set to 'Only people in your organization' or a more restrictive option.

Description

The default sharing link type in SharePoint and OneDrive should not be set to 'Anyone with the link' (anonymous access). The default should be set to 'Only people in your organization' or a more restrictive option.

Details

Rationale: When users create sharing links, the default link type pre-selects the sharing mode. If the default is 'Anyone', users may inadvertently create anonymous sharing links without considering the security implications.

Impact: Users will need to explicitly select 'Anyone' links if needed.

Audit Procedure:

GET /admin/sharepoint/settings

Check: defaultSharingLinkType

0 = None (users choose)

1 = Direct (specific people)

2 = Internal (organization)

3 = Anonymous (Anyone) - non-compliant

Remediation:

SharePoint admin center → Policies > Sharing.

Set default link type to 'Only people in your organization'.

PowerShell:

Set-SPOTenant -DefaultSharingLinkType Internal

Reference: https://learn.microsoft.com/en-us/sharepoint/change-default-sharing-link

---

- **ms365-cis-7.2.8 Ensure external sharing is restricted by security group**

  [MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure external sharing is restricted by security group
Section	7.2 Policies
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	All users can share externally by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External sharing in SharePoint should be limited to users in a specific security group, preventing all users from sharing externally by default.

Description

External sharing in SharePoint should be limited to users in a specific security group, preventing all users from sharing externally by default.

Details

Rationale: Restricting external sharing to a security group ensures only authorized users can share content with external parties, reducing the risk of accidental data exposure.

Impact: Most users will be unable to share content with external parties.

Audit Procedure:

SharePoint admin center → Policies > Sharing.
Check if external sharing is limited to members of a security group.

There is no Graph API for this specific SharePoint setting.

Remediation:
SharePoint admin center → Policies > Sharing.
Under 'Limit external sharing by domain', add the security group that is permitted to share externally.

Reference: https://learn.microsoft.com/en-us/sharepoint/manage-external-sharing

---

- **ms365-cis-7.2.9 Ensure guest access to SharePoint and OneDrive expires automatically** **[SKIPPED]**

Vulnerability Name	This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually
Section	7.2 Policies
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Guest access does not expire by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually: Get-SPOTenant | fl ExternalUserExpirationRequired,ExternalUserExpireInDays

Description

Guest access to SharePoint sites and OneDrive should be configured to expire automatically so that stale guest access is revoked.

Details

Rationale: Guest access that does not expire can persist indefinitely after the original business need is gone. Automatic expiration ensures guest access is regularly reviewed and renewed.

Impact: External users will need to request re-invitation after their access expires.

Audit Procedure:

GET /admin/sharepoint/settings

Check: externalUserExpirationRequired = true and externalUserExpireInDays

Remediation:

SharePoint admin center → Policies > Sharing.

Enable 'Guest access expires after this many days' and set to 30 days or fewer.

Reference: https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview

---

- **ms365-cis-7.2.10 Ensure guest access to SharePoint and OneDrive expires automatically** **[SKIPPED]**

Vulnerability Name	This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually

Security Findings Report

Section	7.2 Policies
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Guest access does not expire by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually: Get-SPOTenant | fl EmailAttestationRequired,EmailAttestationReAuthDays

Description

Guest access to SharePoint sites and OneDrive should be configured to expire automatically so that stale guest access is revoked.

Details

Rationale: Guest access that does not expire can persist indefinitely after the original business need is gone. Automatic expiration ensures guest access is regularly reviewed and renewed.

Impact: External users will need to request re-invitation after their access expires.

Audit Procedure:

GET /admin/sharepoint/settings

Check: externalUserExpirationRequired = true and externalUserExpireInDays

Remediation:

SharePoint admin center → Policies > Sharing.

Enable 'Guest access expires after this many days' and set to 30 days or fewer.

Reference: https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview

---

ms365-cis-7.2.11 Ensure the default sharing link permission is set to View

[SKIPPED]

Vulnerability Name	This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually: Get-SPOTenant | fl DefaultLinkPermission
Section	7.2 Policies
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Default link permission is Edit.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

The default permission for sharing links in SharePoint and OneDrive should be set to 'View' rather than 'Edit'. This ensures users who create sharing links don't inadvertently grant edit permissions.

Description

The default permission for sharing links in SharePoint and OneDrive should be set to 'View' rather than 'Edit'. This ensures users who create sharing links don't inadvertently grant edit permissions.

Details

Rationale: When the default link permission is 'Edit', users can modify shared content unless the sharer specifically selects 'View'. Setting the default to 'View' follows the principle of least privilege.

Impact: Users will need to explicitly select 'Edit' permission when creating sharing links.

Audit Procedure:

GET /admin/sharepoint/settings

Check: defaultLinkPermission

1 = View (compliant)

2 = Edit (non-compliant)

Remediation:

SharePoint admin center → Policies > Sharing.

Set default link permission to 'View'.

PowerShell:

Set-SPOTenant -DefaultLinkPermission View

Reference: https://learn.microsoft.com/en-us/sharepoint/change-default-sharing-link

---

ms365-cis-7.3.1 Ensure SharePoint infected files are prevented from being downloaded

[SKIPPED]

Vulnerability Name	This property is only exposed by SharePoint Online PowerShell, which requires the certificate-based bridge (--ms365-cert-path) that is not configured for this scan. Verify manually: Get-SPOTenant | fl DisallowInfectedFileDownload

Security Findings Report

Section	7.3 Security
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Infected file downloads may be allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

SharePoint Online should be configured to prevent users from downloading files that have been detected as infected with malware.

Description

SharePoint Online should be configured to prevent users from downloading files that have been detected as infected with malware.

Details

Rationale: Allowing downloads of infected files can spread malware to user devices. Blocking infected file downloads protects users from accidentally downloading and executing malware.

Impact: Users will not be able to download files detected as infected.

Audit Procedure:

GET /admin/sharepoint/settings

Check: disallowInfectedFileDownload = true

Remediation:

SharePoint admin center → Settings > Allow or prevent the download of infected files.

PowerShell:

Set-SPOTenant -DisallowInfectedFileDownload $true

Reference: https://learn.microsoft.com/en-us/sharepoint/virus-detection-in-sharepoint-and-onedrive

---

- **ms365-cis-7.3.2 Ensure OneDrive sync is restricted for unmanaged devices**
  [FAIL]

Vulnerability Name	OneDrive sync is allowed on unmanaged devices (isUnmanagedSyncAppForTenantRestricted = false). Corporate data can be synced to personal devices.
Section	7.3 Security
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	OneDrive sync is not restricted by device management status by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

OneDrive sync should be restricted to domain-joined devices. Preventing sync to unmanaged personal devices reduces the risk of corporate data being stored on unmanaged endpoints.

Description

OneDrive sync should be restricted to domain-joined devices. Preventing sync to unmanaged personal devices reduces the risk of corporate data being stored on unmanaged endpoints.

Details

Rationale: When OneDrive sync is allowed on any device, users can sync corporate data to personal devices that may not have appropriate security controls (encryption, antivirus, remote wipe capability).

Impact: Users will not be able to sync OneDrive to personal unmanaged devices.

Audit Procedure:

GET /admin/sharepoint/settings

Check: isUnmanagedSyncAppForTenantRestricted = true

Remediation:

SharePoint admin center → Settings > OneDrive sync.

Enable 'Allow syncing only on computers joined to specific domains'.

PowerShell:

Set-SPOTenant -IsUnmanagedSyncAppForTenantRestricted $true

Reference: https://learn.microsoft.com/en-us/sharepoint/allow-syncing-only-on-specific-domains

---

● ms365-cis-8.1.1 Ensure external file sharing in Teams is enabled for only approved cloud storage services

[FAIL]

Vulnerability Name	Third-party cloud storage providers are enabled for Teams file sharing

Section	8.1 Teams Client Configuration
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Third-party storage is allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Third-party cloud storage providers are enabled for Teams file sharing: AllowDropBox, AllowBox, AllowGoogleDrive, AllowShareFile, AllowEgnyte. Disable any that are not organizationally approved.

Allowbox:

- True

Allowegnyte:

- True

Allowdropbox:

- True

Allowsharefile:

- True

Allowgoogledrive:

- True

Description

Microsoft Teams should be configured to only allow file sharing through approved cloud storage services (SharePoint/OneDrive). Third-party storage services like Dropbox and Box should be disabled.

Details

Rationale: Third-party cloud storage services are outside organizational governance. Restricting Teams to use only SharePoint/OneDrive ensures files are stored in governed storage with appropriate compliance controls.

Impact: Users will only be able to share files stored in SharePoint and OneDrive.

Audit Procedure:

Connect-MicrosoftTeams.

Get-CsTeamsClientConfiguration -Identity Global | fl AllowDropbox, AllowBox, AllowGoogleDrive, AllowShareFile, AllowEgnyte

Verify that only organizationally-approved third-party storage providers are set to True; all others should be False.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsClientConfiguration -Identity Global -AllowDropbox $false -AllowBox $false -AllowGoogleDrive $false -AllowShareFile $false -AllowEgnyte $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/teams-client-configuration

---

- **ms365-cis-8.1.2 Ensure users can't send emails to a channel email address**
  [FAIL]

Vulnerability Name	AllowEmailIntoChannel is True; users can send emails to a channel email address.
Section	8.1 Teams Client Configuration
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	Email into channel may be enabled by default.

Security Findings Report

Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The ability to email a Teams channel address should be disabled to reduce the attack surface and prevent use of channel emails for spam or phishing.

Allowemailintochannel:

- True

Description

The ability to email a Teams channel address should be disabled to reduce the attack surface and prevent use of channel emails for spam or phishing.

Details

Rationale: Channel email addresses can be exploited to inject content into Teams channels. Disabling this feature reduces the risk of malicious content being posted via email.

Impact: Users will not be able to send email messages to Teams channels.

Audit Procedure:

Connect-MicrosoftTeams.

Get-CsTeamsClientConfiguration -Identity Global | fl AllowEmailIntoChannel

Verify that AllowEmailIntoChannel is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsClientConfiguration -Identity Global -AllowEmailIntoChannel $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/email-management

---

- **ms365-cis-8.2.1 Ensure external domains are restricted in the Teams admin center** **[FAIL]**

Vulnerability Name	AllowFederatedUsers is True with no AllowedDomains list, so Teams users may communicate with every known external domain.
Section	8.2 Teams External Access
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	All external domains may be allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Teams external access should be configured to restrict communication to only approved external domains. Communication with all external Teams tenants should not be allowed by default.

Description

Teams external access should be configured to restrict communication to only approved external domains. Communication with all external Teams tenants should not be allowed by default.

Details

Rationale: Unrestricted external Teams access allows users to communicate with anyone in any Teams tenant, increasing phishing and social engineering risks. Restricting to approved domains limits exposure.

Impact: Users will only be able to communicate with users in approved external domains.

Audit Procedure:

Connect-MicrosoftTeams.

Get-CsExternalAccessPolicy -Identity Global — ensure EnableFederationAccess is False.

OR (the organization-level setting takes precedence and is also a passing state):

Get-CsTenantFederationConfiguration | fl AllowFederatedUsers, AllowedDomains — passing if AllowFederatedUsers is False, OR AllowFederatedUsers is True AND AllowedDomains is restricted to specific authorized domains (not AllowAllKnownDomains).

Remediation:

Microsoft Teams admin center → External access.

Configure to allow only specific external domains:

Change to 'Allow only specific external domains'

Add approved partner domains

Teams PowerShell:

Set-CsTenantFederationConfiguration -AllowedDomainsAsAList @('partner.com')

Reference: https://learn.microsoft.com/en-us/microsoftteams/manage-external-access

---

- **ms365-cis-8.2.2 Ensure communication with unmanaged Teams users is disabled** **[FAIL]**

Vulnerability Name	Communication with unmanaged (consumer) Teams users is enabled (EnableTeamsConsumerAccess=True, AllowTeamsConsumer=True).

Security Findings Report

Section	8.2 Teams External Access
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Communication with unmanaged Teams users may be enabled.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Communication with unmanaged Teams users (those who use Teams without a work or school account) should be disabled to prevent data leakage to consumer accounts.

Allowteamsconsumer:

- True

Enableteamsconsumeraccess:

- True

Description

Communication with unmanaged Teams users (those who use Teams without a work or school account) should be disabled to prevent data leakage to consumer accounts.

Details

Rationale: Unmanaged Teams accounts (personal/consumer) don't have the same governance as organizational accounts. Disabling communication with them prevents sensitive business data from being shared with consumer accounts.

Impact: Users will not be able to communicate with personal/consumer Teams accounts.

Audit Procedure:

Connect-MicrosoftTeams.

Get-CsExternalAccessPolicy -Identity Global — ensure EnableTeamsConsumerAccess is False.

OR (the organization-level setting takes precedence and is also a passing state):

Get-CsTenantFederationConfiguration | fl AllowTeamsConsumer — ensure it is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsExternalAccessPolicy -Identity Global -EnableTeamsConsumerAccess $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/manage-external-access

---

- **ms365-cis-8.2.3 Ensure external Teams users cannot initiate conversations**
  [FAIL]

Vulnerability Name	External Teams users can initiate conversations with internal users (EnableTeamsConsumerInbound=True, AllowTeamsConsumerInbound=True).
Section	8.2 Teams External Access
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	External users may be able to initiate conversations.
Asset Label	universal
Date Discovered	Aug 05, 2026

Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External Teams users should not be able to initiate conversations with internal users. Internal users should be the ones initiating external communications.

Allowteamsconsumerinbound:

- True

Enableteamsconsumerinbound:

- True

Description

External Teams users should not be able to initiate conversations with internal users. Internal users should be the ones initiating external communications.

Details

Rationale: Allowing external users to initiate conversations opens the door to social engineering and phishing via Teams chat. Restricting initiation to internal users reduces unsolicited external contact.

Impact: External Teams users will not be able to initiate chats with internal users.

Audit Procedure:

Connect-MicrosoftTeams.

Get-CsExternalAccessPolicy -Identity Global — ensure EnableTeamsConsumerInbound is False.

OR (the organization-level setting takes precedence and is also a passing state):

Get-CsTenantFederationConfiguration | fl AllowTeamsConsumerInbound — ensure it is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsExternalAccessPolicy -Identity Global -EnableTeamsConsumerInbound $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/manage-external-access

● ms365-cis-8.2.4 Ensure the organization cannot communicate with accounts in trial Teams tenants

[PASS]

Vulnerability Name	ExternalAccessWithTrialTenants is Blocked.
Section	8.2 Teams External Access
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Trial tenant communication may be allowed if external access is open.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Communication with Teams trial tenants (free or trial accounts) should be disabled. Trial tenants may be created by attackers for phishing or social engineering attacks.

Externalaccesswithtrialtenants:

- Blocked

Description

Communication with Teams trial tenants (free or trial accounts) should be disabled. Trial tenants may be created by attackers for phishing or social engineering attacks.

Details

Rationale: Trial Teams tenants have lower accountability and may be used by attackers to impersonate legitimate organizations. Blocking communication with trial tenants reduces this risk.

Impact: Communication with free/trial Teams tenants will be blocked.

Audit Procedure:

Connect-MicrosoftTeams.

Get-CsTenantFederationConfiguration — ensure ExternalAccessWithTrialTenants is set to Blocked.

Remediation:

Microsoft Teams PowerShell:

Set-CsTenantFederationConfiguration -ExternalAccessWithTrialTenants Blocked

Reference: https://learn.microsoft.com/en-us/microsoftteams/manage-external-access

---

ms365-cis-8.4.1 Ensure Teams app permission policies are configured

[MANUAL] — *Manual check required.*

Vulnerability Name	Manual: Ensure Teams app permission policies are configured
Section	8.4 Teams Apps
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	All apps may be allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026

Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Teams app permission policies should be configured to restrict which apps users can install in Teams. Third-party apps should require admin approval before users can install them.

Description

Teams app permission policies should be configured to restrict which apps users can install in Teams. Third-party apps should require admin approval before users can install them.

Details

Rationale: Third-party Teams apps can access organizational data and conversations. Requiring admin approval ensures apps are reviewed before deployment and prevents users from installing unapproved data-accessing apps.

Impact: Users must request admin approval to install third-party Teams apps.

Audit Procedure:

Microsoft Teams admin center → Teams apps > Permission policies.

Teams PowerShell:

Get-CsTeamsAppPermissionPolicy | Select-Object Identity, DefaultCatalogApps, PrivateCatalogApps, GlobalCatalogApps

Compliant: Third-party apps are blocked or require approval.

Remediation:

Microsoft Teams admin center → Teams apps > Permission policies.

Create or modify the global policy:

• Microsoft apps: Allow all

• Third-party apps: Block all or Allow specific

• Custom apps: Block or Allow specific

Reference: https://learn.microsoft.com/en-us/microsoftteams/teams-app-permission-policies

---

ms365-cis-8.5.1 Ensure anonymous users can't join a meeting

[FAIL]

Vulnerability Name	AllowAnonymousUsersToJoinMeeting is True; anonymous users are allowed to join Teams meetings.
Section	8.5 Meetings
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	Enabled (anonymous join is on by default).
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Anonymous meeting join allows anyone who has a meeting link to join without authenticating. This should be disabled to prevent uninvited participants from joining sensitive meetings.

Allowanonymoususerstojoinmeeting:

- True

Description

Anonymous meeting join allows anyone who has a meeting link to join without authenticating. This should be disabled to prevent uninvited participants from joining sensitive meetings.

Details

Rationale: Allowing anonymous users to join meetings increases the risk of eavesdropping on sensitive discussions, meeting bombing, and social engineering attacks.

Impact: External guests must be authenticated before joining meetings. B2B guest users can still join; only truly anonymous users are blocked.

Audit Procedure:

Teams PowerShell:

Get-CsTeamsMeetingPolicy -Identity Global | Select-Object AllowAnonymousUsersToJoinMeeting

Expected: AllowAnonymousUsersToJoinMeeting = False

Or Teams admin center → Meetings > Meeting policies > Global > Participants & guests > Allow anonymous users to join a meeting.

Remediation:

Teams admin center:

Meetings > Meeting policies > Global > Participants & guests.

Set 'Allow anonymous users to join a meeting' to Off.

PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToJoinMeeting $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-settings-in-teams

---

- **ms365-cis-8.5.2 Ensure anonymous users and dial-in callers can't start a meeting**
  [PASS]

Vulnerability Name	AllowAnonymousUsersToStartMeeting is False.

Security Findings Report

Section	8.5 Meetings
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Anonymous users cannot start meetings by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Anonymous users and dial-in callers should not be able to start Teams meetings. Only authenticated users should be able to initiate meetings.

Description

Anonymous users and dial-in callers should not be able to start Teams meetings. Only authenticated users should be able to initiate meetings.

Details

Rationale: Allowing anonymous or unauthenticated users to start meetings creates opportunities for unauthorized meeting sessions that could be used for eavesdropping or social engineering.

Impact: Meetings must be started by authenticated meeting participants.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl AllowAnonymousUsersToStartMeeting

Ensure AllowAnonymousUsersToStartMeeting is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToStartMeeting $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-participants-and-guests

---

● ms365-cis-8.5.3 Ensure only people in my org can bypass the lobby

[FAIL]

Vulnerability Name	AutoAdmittedUsers is 'EveryoneInCompany', which allows more than InvitedUsers/organization members to bypass the lobby.
Section	8.5 Teams Meetings
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	AutoAdmittedUsers may allow everyone to bypass lobby.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Only users from the organization should be able to bypass the meeting lobby. External users and guests should wait in the lobby for an organizer or presenter to admit them.

Autoadmittedusers:

- EveryoneInCompany

Description

Only users from the organization should be able to bypass the meeting lobby. External users and guests should wait in the lobby for an organizer or presenter to admit them.

Details

Rationale: The meeting lobby acts as a security gate, ensuring unauthorized users don't join meetings without explicit admission. External users should not automatically bypass this control.

Impact: External users must wait in the lobby before being admitted to meetings.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl AutoAdmittedUsers

Ensure AutoAdmittedUsers is InvitedUsers or a more restrictive value (EveryoneInCompanyExcludingGuests, OrganizerOnly).

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -AutoAdmittedUsers InvitedUsers

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-participants-and-guests

---

● ms365-cis-8.5.4 Ensure users dialing in can't bypass the lobby

[PASS]

Vulnerability Name	AllowPSTNUsersToBypassLobby is False.
Section	8.5 Teams Meetings
Severity	Medium

Profiles	E3 Level 1, E5 Level 1
Default Value	Dial-in callers bypass lobby by default when organizer is in meeting.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Dial-in callers should not be able to bypass the meeting lobby. They should wait in the lobby until an organizer admits them.

Description

Dial-in callers should not be able to bypass the meeting lobby. They should wait in the lobby until an organizer admits them.

Details

Rationale: Dial-in callers cannot be authenticated the same way as Teams users. Requiring them to wait in the lobby for admission ensures an authenticated meeting participant approves their access.

Impact: Dial-in callers must be admitted by a meeting organizer or presenter.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl AllowPSTNUsersToBypassLobby

Ensure AllowPSTNUsersToBypassLobby is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -AllowPSTNUsersToBypassLobby $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-participants-and-guests

---

ms365-cis-8.5.5 Ensure meeting chat does not allow anonymous users

[FAIL]

Vulnerability Name	MeetingChatEnabledType is 'Enabled', which allows anonymous users to use meeting chat.
Section	8.5 Teams Meetings
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Meeting chat settings vary by policy.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Meeting chat should be configured to prevent anonymous users from posting in chat, limiting chat participation to authenticated users.

Meetingchatenabledtype:

- Enabled

Description

Meeting chat should be configured to prevent anonymous users from posting in chat, limiting chat participation to authenticated users.

Details

Rationale: Anonymous users in meeting chat cannot be held accountable for their communications. Restricting anonymous chat participation prevents abuse and potential social engineering through chat.

Impact: Anonymous users will not be able to post in meeting chat.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl MeetingChatEnabledType

Ensure MeetingChatEnabledType is EnabledExceptAnonymous or a more restrictive value (EnabledInMeetingOnlyForAllExceptAnonymous, Disabled).

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -MeetingChatEnabledType EnabledExceptAnonymous

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-in-teams-general

---

● ms365-cis-8.5.6 Ensure only organizers and co-organizers can present

[FAIL]

Vulnerability Name	DesignatedPresenterRoleMode is 'EveryoneUserOverride', not OrganizerOnlyUserOverride; participants other than organizers/co-organizers may be able to present by default.
Section	8.5 Teams Meetings
Severity	Low

Profiles	E3 Level 2, E5 Level 2
Default Value	Everyone can present by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Meeting presentation rights should be configured so only the organizer and co-organizers can present by default. This prevents external attendees or others from unexpectedly presenting screen shares.

Designatedpresenterrolemode:

- EveryoneUserOverride

Description

Meeting presentation rights should be configured so only the organizer and co-organizers can present by default. This prevents external attendees or others from unexpectedly presenting screen shares.

Details

Rationale: Limiting presenter rights to organizers and co-organizers prevents external attendees from sharing potentially malicious content during meetings.

Impact: Meeting participants who need to present must be explicitly promoted by the organizer.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl DesignatedPresenterRoleMode

Ensure DesignatedPresenterRoleMode is OrganizerOnlyUserOverride.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -DesignatedPresenterRoleMode OrganizerOnlyUserOverride

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-participants-and-guests

---

ms365-cis-8.5.7 Ensure external participants can't give or request control

[PASS]

Vulnerability Name	AllowExternalParticipantGiveRequestControl is False.
Section	8.5 Teams Meetings
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	External control may be allowed by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External participants in Teams meetings should not be able to give or request control of a presenter's desktop or application. This prevents external parties from controlling internal computers.

Description

External participants in Teams meetings should not be able to give or request control of a presenter's desktop or application. This prevents external parties from controlling internal computers.

Details

Rationale: Allowing external users to control screen shares gives them direct control of internal computers, which can be exploited to install malware or access sensitive data.

Impact: External meeting participants will not be able to use remote control features.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl AllowExternalParticipantGiveRequestControl

Ensure AllowExternalParticipantGiveRequestControl is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -AllowExternalParticipantGiveRequestControl $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-content-sharing

---

- **ms365-cis-8.5.8 Ensure external meeting chat is off**
  [FAIL]

Vulnerability Name	AllowExternalNonTrustedMeetingChat is True; external participants can use meeting chat.
Section	8.5 Teams Meetings
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	External participants can use meeting chat by default.

Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Meeting chat should be restricted so that external participants (guests and federated users) cannot use the meeting chat to communicate with internal participants.

Allowexternalnontrustedmeetingchat:

- True

Description

Meeting chat should be restricted so that external participants (guests and federated users) cannot use the meeting chat to communicate with internal participants.

Details

Rationale: External participants in meeting chat can send malicious links or attempt social engineering through meeting chat. Restricting external chat reduces this attack vector.

Impact: External participants will not be able to use meeting chat.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl AllowExternalNonTrustedMeetingChat

Ensure AllowExternalNonTrustedMeetingChat is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -AllowExternalNonTrustedMeetingChat $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-in-teams-general

ms365-cis-8.5.9 Ensure meeting recording is off by default

[FAIL]

Vulnerability Name	AllowCloudRecording is True; meeting recording is enabled by default.
Section	8.5 Teams Meetings
Severity	Low
Profiles	E3 Level 2, E5 Level 2
Default Value	Meeting recording may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Meeting recording should be disabled by default to prevent sensitive meeting content from being recorded and stored without explicit consent from all participants.

Allowcloudrecording:

- True

Description

Meeting recording should be disabled by default to prevent sensitive meeting content from being recorded and stored without explicit consent from all participants.

Details

Rationale: Meeting recordings can contain sensitive business discussions. Disabling recording by default ensures recordings are made intentionally and not without participants' knowledge.

Impact: Users must explicitly enable recording for each meeting.

Audit Procedure:

Get-CsTeamsMeetingPolicy -Identity Global | fl AllowCloudRecording

Ensure AllowCloudRecording is False.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMeetingPolicy -Identity Global -AllowCloudRecording $false

Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-recording-and-transcription

---

● ms365-cis-8.6.1 Ensure users can report security concerns in Teams

[FAIL]

Vulnerability Name	Users cannot fully report security concerns in Teams: no report submission policy was returned by Get-ReportSubmissionPolicy.
Section	8.6 Teams Messaging
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Security concern reporting may be enabled by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Users should be able to report security concerns (phishing, malware, inappropriate content) in Microsoft Teams. This feature should be enabled to facilitate incident reporting.

Description

Users should be able to report security concerns (phishing, malware, inappropriate content) in Microsoft Teams. This feature should be enabled to facilitate incident reporting.

Details

Rationale: Enabling users to report suspicious content in Teams creates a simple mechanism for early detection of phishing or social engineering attempts targeting the organization through Teams.

Impact: Minimal; this is an additive capability that enables security reporting.

Audit Procedure:

Connect-MicrosoftTeams.

Get-CsTeamsMessagingPolicy -Identity Global | fl AllowSecurityEndUserReporting

Ensure AllowSecurityEndUserReporting is True.

ALSO Connect-ExchangeOnline.

Get-ReportSubmissionPolicy | fl Report*

Ensure ReportJunkToCustomizedAddress = True, ReportNotJunkToCustomizedAddress = True, ReportPhishToCustomizedAddress = True, ReportJunkAddresses / ReportNotJunkAddresses / ReportPhishAddresses are set to the organization's SOC address, ReportChatMessageEnabled = False, and ReportChatMessageToCustomizedAddressEnabled = True.

Remediation:

Microsoft Teams PowerShell:

Set-CsTeamsMessagingPolicy -Identity Global -AllowSecurityEndUserReporting $true

Exchange Online PowerShell:

Set-ReportSubmissionPolicy -ReportJunkToCustomizedAddress $true -ReportNotJunkToCustomizedAddress $true -ReportPhishToCustomizedAddress $true -ReportJunkAddresses <SOC address> -ReportNotJunkAddresses <SOC address> -ReportPhishAddresses <SOC address> -ReportChatMessageEnabled $false -ReportChatMessageToCustomizedAddressEnabled $true

Reference: https://learn.microsoft.com/en-us/microsoftteams/messaging-policies-in-teams

---

- **ms365-cis-9.1.1 Ensure guest user access is restricted**
  [FAIL]

Vulnerability Name	Guest user access to Microsoft Fabric is enabled for the entire organization (not scoped to specific security groups).
Section	9.1 Microsoft Fabric
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Guest access to Fabric may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Guest user access to Microsoft Fabric should be restricted to prevent external users from accessing sensitive data analytics and BI content without proper authorization.

Title:

- Guest users can access Microsoft Fabric

Enabled:

- True

Settingname:

- AllowGuestUserToAccessSharedContent

Tenantsettinggroup:

- Export and sharing settings

Canspecifysecuritygroups:

- True

Description

Guest user access to Microsoft Fabric should be restricted to prevent external users from accessing sensitive data analytics and BI content without proper authorization.

Details

Rationale: Microsoft Fabric may contain sensitive business data in datasets, reports, and dashboards. Restricting guest access prevents unauthorized external access to potentially sensitive analytical data.

Impact: Guest users will not be able to access Fabric content without explicit approval.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Export and sharing settings.

Ensure 'Guest users can access Microsoft Fabric' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName AllowGuestUserToAccessSharedContent.

Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings:

Disable 'Allow Azure Active Directory guest users to access Microsoft Fabric'

Reference: https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-export-sharing

---

ms365-cis-9.1.2 Ensure external user invitations are restricted

[FAIL]

Vulnerability Name	External user invitations to Microsoft Fabric are enabled for the entire organization (not scoped to specific security groups).
Section	9.1 Microsoft Fabric
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	External user invitations may be enabled by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

The ability to invite external users to Microsoft Fabric content should be restricted to prevent unauthorized sharing of analytical content with external parties.

Title:

- Users can invite guest users to collaborate through item sharing and permissions

Enabled:

- True

Settingname:

- ExternalSharingV2

Tenantsettinggroup:

- Export and sharing settings

Canspecifysecuritygroups:

- True

Description

The ability to invite external users to Microsoft Fabric content should be restricted to prevent unauthorized sharing of analytical content with external parties.

Details

Rationale: Unrestricted external user invitations can result in sensitive business intelligence content being shared with external parties without proper authorization.

Impact: Users will not be able to invite external users to Fabric content directly.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Export and sharing settings.

Ensure 'Users can invite guest users to collaborate through item sharing and permissions' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName ExternalSharingV2.

Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings:

Disable 'Invite external users to your organization through Microsoft Fabric'

Reference: https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-export-sharing

---

ms365-cis-9.1.3 Ensure guest access to content is restricted

[PASS]

Vulnerability Name	Guest access to Microsoft Fabric content is restricted.
Section	9.1 Microsoft Fabric
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Guest access settings may vary.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Guest users should not have unrestricted access to Microsoft Fabric workspaces and content. Access should be limited to specifically shared items.

Title:

- Guest users can browse and access Fabric content

Settingname:

- ElevatedGuestsTenant

Tenantsettinggroup:

- Export and sharing settings

Canspecifysecuritygroups:

- True

Description

Guest users should not have unrestricted access to Microsoft Fabric workspaces and content. Access should be limited to specifically shared items.

Details

Rationale: Broad guest access to Fabric workspaces could expose sensitive business intelligence data and analytics to external parties.

Impact: Guest users will only access content explicitly shared with them.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Export and sharing settings.

Ensure 'Guest users can browse and access Fabric content' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName ElevatedGuestsTenant.

Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings:

Restrict guest user access to specific shared content only

Reference: https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-export-sharing

---

- **ms365-cis-9.1.4 Ensure 'Publish to web' is restricted**

  [SKIPPED]

Security Findings Report

Vulnerability Name	The Microsoft Fabric admin API did not return a PublishToWebPublishToWeb setting for this tenant. Verify manually in the Fabric admin portal > Tenant settings > Export and sharing settings.
Section	9.1 Microsoft Fabric
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Publish to web may be enabled for all users by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Finding Details

The 'Publish to web' feature in Microsoft Fabric (Power BI) allows reports to be published publicly on the internet. This should be disabled or restricted to prevent accidental public exposure of sensitive data.

Description

The 'Publish to web' feature in Microsoft Fabric (Power BI) allows reports to be published publicly on the internet. This should be disabled or restricted to prevent accidental public exposure of sensitive data.

Details

Rationale: 'Publish to web' creates anonymous, publicly accessible links to reports. If a user accidentally publishes a sensitive report, the data is exposed to anyone on the internet.

Impact: Users will not be able to publish reports to the public web.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Export and sharing settings.

Ensure 'Publish to web' is Disabled, or Enabled with 'Choose how embed codes work' set to 'Only allow existing codes' AND specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName PublishToWebPublishToWeb.

Pass if enabled=false, or enabled=true AND properties.createP2w=false AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings:

Disable 'Publish to web' or restrict to specific security groups

Reference: https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-publish-to-web

---

- **ms365-cis-9.1.5 Ensure 'Interact with and share R and Python' visuals is 'Disabled'** **[FAIL]**

Vulnerability Name	Interact with and share R and Python visuals is enabled.
Section	9.1 Microsoft Fabric
Severity	Medium
Profiles	E3 Level 2, E5 Level 2
Default Value	R and Python visuals may be enabled by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

R and Python visuals in Microsoft Fabric execute code that runs server-side. These should be disabled unless explicitly needed, as they could be used to execute malicious code.

Title:

- Interact with and share R and Python visuals

Enabled:

- True

Settingname:

- RScriptVisual

Tenantsettinggroup:

- R and Python visuals settings

Description

R and Python visuals in Microsoft Fabric execute code that runs server-side. These should be disabled unless explicitly needed, as they could be used to execute malicious code.

Details

Rationale: R and Python code execution in Fabric visuals can access data and potentially exfiltrate it or perform unintended operations. Disabling these reduces the attack surface.

Impact: Users will not be able to use R or Python visuals in Power BI reports.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > R and Python visuals settings.

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

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):
GET https://api.fabric.microsoft.com/v1/admin/tenantsettings
Locate settingName RScriptVisual. Pass if enabled=false.

Remediation:
Microsoft Fabric admin portal → Tenant settings:
Disable R visuals and Python visuals

Reference: https://learn.microsoft.com/en-us/power-bi/visuals/service-r-visuals

---

- **ms365-cis-9.1.6 Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'** **[FAIL]**

Vulnerability Name	Users are not allowed to apply sensitivity labels for content.
Section	9.1 Microsoft Fabric
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Sensitivity label integration may not be configured.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Sensitivity labels should be enabled for Microsoft Fabric content to classify and protect analytics content based on its sensitivity.

Title:

- Allow users to apply sensitivity labels for content

Settingname:

- EimInformationProtectionEdit

Tenantsettinggroup:

- Information protection

Canspecifysecuritygroups:

- True

Description

Sensitivity labels should be enabled for Microsoft Fabric content to classify and protect analytics content based on its sensitivity.

Details

Rationale: Sensitivity labels on Fabric content ensure consistent classification and protection policies apply to analytical data and reports, extending information protection to the BI layer.

Impact: Content creators will be required to apply sensitivity labels to Fabric items.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Information protection.

Ensure 'Allow users to apply sensitivity labels for content' is Enabled (optionally restricted to specific security groups).

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName EimInformationProtectionEdit.

Pass if enabled=true.

Remediation:

Microsoft Fabric admin portal → Tenant settings > Information protection:

Enable sensitivity labels for Microsoft Fabric

Reference: https://learn.microsoft.com/en-us/fabric/governance/information-protection

---

ms365-cis-9.1.7 Ensure shareable links are restricted

[FAIL]

Vulnerability Name	Shareable links can grant access to everyone in the organization (not scoped to specific security groups).
Section	9.1 Microsoft Fabric
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	Shareable links may be available to all users by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Shareable links in Microsoft Fabric should be restricted to prevent users from creating publicly accessible links to reports and dashboards containing potentially sensitive data.

Title:

- Allow shareable links to grant access to everyone in your organization

Enabled:

- True

Settingname:

- ShareLinkToEntireOrg

Tenantsettinggroup:

- Export and sharing settings

Canspecifysecuritygroups:

- True

Description

Shareable links in Microsoft Fabric should be restricted to prevent users from creating publicly accessible links to reports and dashboards containing potentially sensitive data.

Details

Rationale: Shareable links allow any person with the link to access reports without authentication. Restricting this feature prevents accidental public disclosure of business intelligence data.

Impact: Users will not be able to create shareable links for Fabric content.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Export and sharing settings.

Ensure 'Allow shareable links to grant access to everyone in your organization' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName ShareLinkToEntireOrg.

Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings > Export and sharing:

Disable or restrict shareable links feature

Reference: https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-share-dashboards

ms365-cis-9.1.8 Ensure enabling of external data sharing is restricted

[FAIL]

Vulnerability Name	Any user can turn on external data sharing (not scoped to specific security groups).
Section	9.1 Microsoft Fabric
Severity	Low
Profiles	E3 Level 1, E5 Level 1
Default Value	External data sharing settings may vary.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

External data sharing in Microsoft Fabric allows workspace data to be shared with external organizations' Fabric workspaces. This should be restricted to prevent uncontrolled data sharing.

Title:

- Allow specific users to turn on external data sharing

Enabled:

- True

Settingname:

- EnableDatasetInPlaceSharing

Tenantsettinggroup:

- Export and sharing settings

Canspecifysecuritygroups:

- True

Description

External data sharing in Microsoft Fabric allows workspace data to be shared with external organizations' Fabric workspaces. This should be restricted to prevent uncontrolled data sharing.

Details

Rationale: External data sharing can result in live connections to organizational datasets from external organizations' Fabric environments, creating ongoing data access that may be difficult to revoke.

Impact: Users will not be able to set up cross-tenant data sharing for Fabric.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Export and sharing settings.

Ensure 'Allow specific users to turn on external data sharing' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName EnableDatasetInPlaceSharing.

Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings:

Disable or restrict external data sharing

Reference: https://learn.microsoft.com/en-us/fabric/governance/external-data-sharing-overview

---

- **ms365-cis-9.1.9 Ensure 'Block ResourceKey Authentication' is 'Enabled'**
  [FAIL]

Security Findings Report

Vulnerability Name	ResourceKey authentication is not blocked.
Section	9.1 Microsoft Fabric
Severity	High
Profiles	E3 Level 1, E5 Level 1
Default Value	ResourceKey authentication may not be blocked by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

ResourceKey authentication in Microsoft Fabric allows access to datasets and reports using resource keys instead of Azure AD tokens. This should be blocked to enforce proper authentication.

Title:

- Block ResourceKey Authentication

Settingname:

- BlockResourceKeyAuthentication

Tenantsettinggroup:

- Developer settings

Description

ResourceKey authentication in Microsoft Fabric allows access to datasets and reports using resource keys instead of Azure AD tokens. This should be blocked to enforce proper authentication.

Details

Rationale: ResourceKey authentication bypasses Azure AD-based authentication and conditional access. Blocking it ensures all access goes through proper identity verification and MFA enforcement.

Impact: Applications using ResourceKey authentication will need to migrate to Azure AD.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Developer settings.

Ensure 'Block ResourceKey Authentication' is Enabled.

Via the Fabric admin REST API (app-only; the tenant must enable 'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName BlockResourceKeyAuthentication.

Pass if enabled=true.

Remediation:

Microsoft Fabric admin portal → Tenant settings > Developer settings:

Enable 'Block ResourceKey Authentication'

Reference: https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-developer

---

- **ms365-cis-9.1.10 Ensure access to APIs by service principals is restricted**
  [FAIL]

Vulnerability Name	Any service principal can call Fabric public APIs (not scoped to specific security groups).
Section	9.1 Microsoft Fabric
Severity	High
Profiles	E3 Level 1, E5 Level 1

Default Value	Service principal access to Fabric API may be restricted by default.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Service principals should not have access to the Microsoft Fabric API unless specifically needed. Broad service principal access can be exploited if a service principal's credentials are compromised.

Title:

- Service principals can call Fabric public APIs

Enabled:

- True

Settingname:

- ServicePrincipalAccessPermissionAPIs

Tenantsettinggroup:

- Developer settings

Canspecifysecuritygroups:

- True

Description

Service principals should not have access to the Microsoft Fabric API unless specifically needed. Broad service principal access can be exploited if a service principal's credentials are compromised.

Details

Rationale: Service principals have persistent, often unmonitored access to Fabric resources. Restricting API access to service principals reduces the attack surface and potential for unauthorized data access.

Impact: Applications using service principals for Fabric API access will need to be reviewed.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Developer settings.

Ensure 'Service principals can call Fabric public APIs' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName ServicePrincipalAccessPermissionAPIs.

Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings > Developer settings:

Disable 'Allow service principals to use Fabric APIs' or restrict to specific groups

Reference: https://learn.microsoft.com/en-us/power-bi/developer/embedded/embed-service-principal

---

ms365-cis-9.1.11 Ensure service principals cannot create and use profiles

[PASS]

Vulnerability Name	Service principals cannot create and use profiles for the entire organization.
Section	9.1 Microsoft Fabric
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Profile creation by service principals may be enabled by default.
Asset Label	universal

Security Findings Report

Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com
Resource Type	tenant

Finding Details

Service principals should not be allowed to create service principal profiles in Microsoft Fabric. This limits the potential for privilege escalation through profile creation.

Title:

- Allow service principals to create and use profiles

Settingname:

- AllowServicePrincipalsCreateAndUseProfiles

Tenantsettinggroup:

- Developer settings

Canspecifysecuritygroups:

- True

Description

Service principals should not be allowed to create service principal profiles in Microsoft Fabric. This limits the potential for privilege escalation through profile creation.

Details

Rationale: Service principal profiles in Fabric can be used to access workspace data. Preventing service principals from creating profiles reduces the risk of unauthorized data access through compromised service principals.

Impact: Service principals will not be able to create new profiles.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Developer settings.

Ensure 'Allow service principals to create and use profiles' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable
'Service principals can access read-only admin APIs'):
GET https://api.fabric.microsoft.com/v1/admin/tenantsettings
Locate settingName AllowServicePrincipalsCreateAndUseProfiles.
Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:
Microsoft Fabric admin portal → Tenant settings > Developer settings:
Disable 'Service principals can create and use profiles'

Reference: https://learn.microsoft.com/en-us/power-bi/developer/embedded/embed-multi-tenancy

---

● ms365-cis-9.1.12 Ensure service principals ability to create workspaces, connections and deployment pipelines is restricted

[PASS]

Vulnerability Name	Service principal ability to create workspaces, connections, and deployment pipelines is restricted.
Section	9.1 Microsoft Fabric
Severity	Medium
Profiles	E3 Level 1, E5 Level 1
Default Value	Workspace creation restrictions may vary by tenant.
Asset Label	universal
Date Discovered	Aug 05, 2026
Last Seen	Aug 05, 2026
Asset / Resource	ms365://ayushaggarwal1136gmail.onmicrosoft.com

Security Findings Report

Resource Type	tenant

Finding Details

Service principals should not be able to create Fabric workspaces. Workspace creation by service principals can lead to uncontrolled workspace proliferation and makes governance more difficult.

Title:

- Service principals can create workspaces, connections, and deployment pipelines

Settingname:

- ServicePrincipalAccessGlobalAPIs

Tenantsettinggroup:

- Developer settings

Canspecifysecuritygroups:

- True

Description

Service principals should not be able to create Fabric workspaces. Workspace creation by service principals can lead to uncontrolled workspace proliferation and makes governance more difficult.

Details

Rationale: Restricting workspace creation to humans or authorized service principals maintains governance over Fabric workspace proliferation and ensures workspaces are created with proper ownership and purpose.

Impact: Service principals will not be able to create new Fabric workspaces.

Audit Procedure:

Microsoft Fabric admin portal (app.powerbi.com/admin-portal):

Tenant settings > Developer settings.

Ensure 'Service principals can create workspaces, connections, and deployment pipelines' is Disabled, or Enabled with specific security groups selected.

Via the Fabric admin REST API (app-only; the tenant must enable

'Service principals can access read-only admin APIs'):

GET https://api.fabric.microsoft.com/v1/admin/tenantsettings

Locate settingName ServicePrincipalAccessGlobalAPIs.

Pass if enabled=false, or enabled=true AND enabledSecurityGroups is non-empty.

Remediation:

Microsoft Fabric admin portal → Tenant settings > Workspace settings:

Restrict workspace creation to specific users/groups only

Reference: https://learn.microsoft.com/en-us/fabric/admin/portal-workspace